IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 22, 2021, accepted December 10, 2021, date of publication December 16, 2021,
date of current version January 7, 2022.

*Digital Object Identifier 10.1109/ACCESS.2021.3136328*

# Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges

**SUHYEON LEE, (Member, IEEE), AND SEUNGJOO KIM, (Member, IEEE)**
School of Cybersecurity, Institute of Cyber Security and Privacy (ICSP), Korea University, Seoul 02841, South Korea

Corresponding author: Seungjoo Kim (skim71@korea.ac.kr)

This work was supported by Institute for Information and communications Technology Promotion (IITP) Grant by the Korean Government through MSIT [Development of High-Assurance (≥EAL6) Secure Microkernel] under Grant 2018-0-00532.

**ABSTRACT** Targets of cyber crime are not exclusive to the private sector. Successful cyber attacks on nation-states have proved that cyber threats can jeopardize significant national interests. In response, nation-states have begun to handle cyber threats at the national defense level, which is titled 'cyber defense.' The cyber defense sector is related to national security, therefore requires robust security technology. Contrary to normal systems, blockchain provides strong security properties without a centralized control entity, and as such its application in the cyber defense field is under the spotlight. In this paper, we present opportunities blockchain provides for cyber defense, research and national projects, and limitations. We constructed a survey of government documents, interviews, related news, technical reports, and research papers from 2016 to 2021. As a result, our research contributes to reducing the gap in blockchain for cyber defense by systematically conducting research and analysis. In our research, we found that not only research but also government-led plans are actively promoting blockchain, which demonstrates that blockchain will play a remarkable role in cyber defense. This paper concludes with suggestions for future research in aspects of the blockchain technology, evaluation, and survey.

**INDEX TERMS** Blockchain, cyber security, cyber defense, military, survey.

## I. INTRODUCTION

Cyber defense is a matter of ensuring the survival of a state from cyber threats. We have continued rapid digital transformation over the past decades. The surging cyber threats, perhaps, are payment for efficiency that we have benefited from the digital transition. Numerous IT systems were designed and used without enough consideration on security. Furthermore, new type of security vulnerabilities are found over time. This issue should be treated as significant because the target of cyber threats has become a primary function of the state, not a single service or company. National energy power plants, medical facilities, and even military networks are continuously infiltrated. One article insisted that nuclear submarines are hackable [1]. The fact that some national infrastructures' systems cannot be updated or re-designed in a short time makes it worse. Nation states require powerful security technologies for their cyber defense.

Against this backdrop, a 2021 U.S. Defense Authorization Act amendment was passed to designate blockchain technology as an emerging technology in the defense sector [2]–[4]. It shows that the strong security characteristics of blockchain are attracting attention in the field of cyber defense. Blockchain technology was first introduced to implement a cryptocurrency termed Bitcoin [5]. The other name of the blockchain is a distributed ledger technology because several ledgers record the same content and verify it in a decentralized process. This structure prevents data manipulation unless any attacker monopolizes more than half of the resources. Blockchain technology can provide secure computation using smart contracts [6] that are Turing-complete. Therefore, blockchain technology works as a platform for various decentralized applications.

Blockchain projects, including cryptocurrency, have demonstrated strong security characteristics. For this reason, various blockchain projects are being promoted at the level of cyber defense in at least several countries. Applications can be categorized into multiple domains based on their use, from data integrity to a decentralized military network, a reliable supply chain for weapons systems, swarming drones, and members' authorization.

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

**TABLE 1.** Comparison with previous research.

| Research | Topic | Main Contribution | Limitation |
|---|---|---|---|
| Taylor et al. [7] | Blockchain for cyber security | Systematic literature review on blockchain for cyber security | Limitations of the role of blockchain are not discussed. |
| Zhu et al. [8] | Blockchain for defense | Introduction to various blockchain applications combined with the latest technologies | Existing cases or studies are not thoroughly investigated. |
| Lilly and Lilly [9] | The weaponization of blockchain in the US, China, and Russia | Specific case studies of the three countries and a strategical analysis on them | Since it is case-oriented, related research is not sufficiently handled. |
| Bansal et al. [10] | Blockchain for cybersecurity | Conceptual investigation on the use of blockchain for various applications of cybersecurity | It focuses on detailed topics such as private messages, DDoS, and DNS. |
| Ahmed et al. [11] | Blockchain for aerospace and defense | State-of-the-art survey on blockchain aerospace and defense and detailed examples | The research domain is focused on border protection, battlefield, swarm, and supply chain management. |
| Our research | Blockchain for cyber defense | The first blockchain survey with the approach of cyber defense, and plenty of the latest research and application cases | Due to linguistic limitations, national projects are not surveyed in a balanced manner. |

Several studies have investigated the role of blockchain related to cyber defense. Table 1 presents related research's topic, main contributions, and limitations. Taylor *et al.* [7] systematically reviewed blockchain applications for cyber security. Zhu *et al.* [8] studied blockchain applications for the use of cyber security. Lilly and Lilly [9]'s study focused on real-world military blockchain projects in three countries including the US, China, and Russia. Bunsal *et al.* [10] studied specific cyber security applications using blockchain. Ahmad *et al.* [11] investigated blockchain for defense and aerospace, which are strongly related domains. Their study provides detailed architecture of blockchain applications.

However, to the best of our knowledge, no papers approached a survey in blockchain applications that can be covered at the notion of cyber defense. Cyber defense is not limited to the use of the military but also covers national security. When we consider recent cyber threats and the significance of national security, blockchain for cyber defense needs to be studied. Therefore, in this paper, our study is based on the research about the role of blockchain in the domain of cyber defense. It is embodied in the following three research questions.

**RQ1.** What are the main benefits of cyber defense's use of blockchain technology?

**RQ2.** What types of blockchain applications are used in the field of cyber defense, and what applications have actually been promoted?

**RQ3.** Compared to the private sector, what are the limitations or challenges of blockchain technology in the field of cyber defense?

According to research questions, in the process of conducting the study, we identified the characteristics of the blockchain that were not found in other studies and built a new knowledge system of blockchain for cyber defense. In addition, the limitations of the blockchain technology we have performed consider policy factors not only in terms of technology but also in terms of practice and policy. Our contributions are as the following:

- We provide crucial roles of blockchain technology to cyber defense in aspects of visibility, verifiability, eliminating a single point of failure, and auditability.
- We conduct the first systematic survey on blockchain systems for cyber defense. We surveyed at least 40 blockchain projects concerning cyber defense including research and government projects.
- We analyze domain-specific challenges which consist of battlefield environments, air-gaps, and resource shortage when applying blockchain technology to cyber defense.

The rest of this paper is organized as follows: Section II provides an overview of blockchain technology. Section III, which covers **RQ1**, provides the definition of cyber defense and discusses the benefits of blockchain implementations in cyber defense. Section IV, which answers to **RQ2**, presents up-to-date blockchain research, projects, and applications in cyber defense. Section V answers to **RQ3** by identifying open challenges in blockchain under national infrastructure and military circumstances. Finally, Section VI concludes the paper with future recommendations.

## II. BLOCKCHAIN TECHNOLOGY

In this section, we provide an overview of blockchain technology. The notion of a blockchain has seen wide use since the first successful cryptocurrency, Bitcoin, appeared in 2009. The blockchain is the essential data structure of Bitcoin, and it allows Bitcoin to work as e-cash in trustless environments by avoiding double-spending. A Bitcoin transaction is a record that includes the amount, senders, receivers, and signature. A block can contain a number of transactions, and the word 'blockchain' explicitly describes Bitcoin's data structure, as illustrated in Fig. 1. Excluding the genesis block, which is the first block, every block is linked to its previous block by containing the previous block's hash. Every block contains the Merkle root hash of the transactions to prevent modification, blocks linked to each other guarantee the integrity of the block. In other words, to modify the data of this block, such as the transaction information, it is inevitable to modify the value of all blocks behind it. The process to generate blocks is determined on Bitcoin's decentralized network, and it has its own consensus mechanism that uses Proof-of-Work (PoW). Bitcoin's structure is, however, not the only form of a blockchain. Other cryptocurrencies like Ethereum, Zcash, Ripple, and IOTA use modified or fairly different structures compared to Bitcoin.

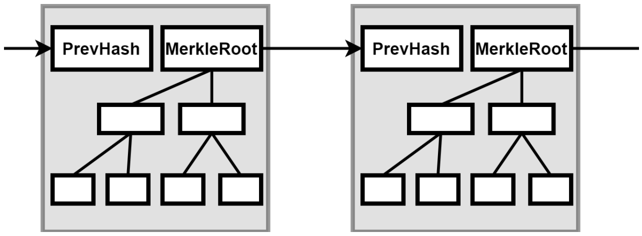


**FIGURE 1. Bitcoin data structure.**

Fig. 2 (a) illustrates Bitcoin's longest chain rule. Blocks are generated via Proof-of-Work (PoW), which needs to prove that a sufficient amount of computing power has been consumed. Each block is singly linked, but there can be a fork, which means that more than one block would refer to the same previous block. Bitcoin thus accepts the longest chain as the valid chain. Because of the PoW, the longest chain implies that the most computing power has been devoted to it.

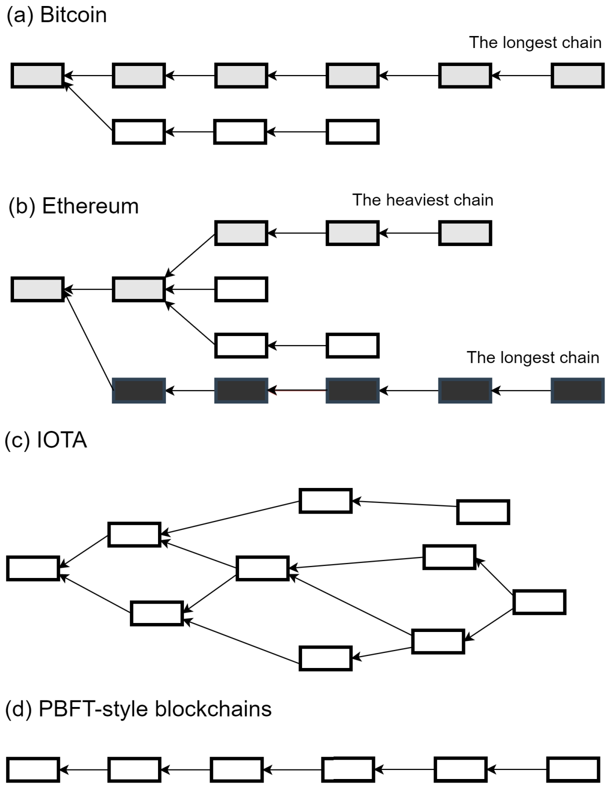


**FIGURE 2. Hash chain structures.**

Blockchain does not use only the same data structure which is used by Bitcoin. Ethereum [6]'s PoW has a multiply linked list structure. Ethereum can rapidly generate a block every 15 seconds, and as a result, it can easily have multiple blocks that link to the same block. To solve such issues, Ethereum accepts the heaviest chain as the legitimate chain rather than the longest chain, which is referred to as the Greedy Heaviest-Observed Sub-Tree (GHOST) protocol. For example, Fig. 2 (b) shows that the gray chain becomes the heaviest and, therefore, the legitimate chain as opposed to the black and longest chain. Since many blocks are not included in the heaviest chain, the uncle blocks' miners obtain a reward. IOTA [12] uses the tangle, which is likened to a directed graph. A transaction is approved in the tangle only when two transactions reference it. Even though a node selects transactions to verify and refer in a random sense, this structure has several centralization issues. In Practical Byzantine Fault Tolerance (PBFT)-style blockchains, the block generation mechanism is deterministic. As far as they can make a consensus, they generate only one block at the same height. Therefore, they remain forkless as one single chain. A PBFT-style blockchain is usually used in private blockchains because it requires to recognize blockchain nodes in advance.

Another essential property of blockchains is the decentralization of their networks, which requires a Sybil control mechanism to prevent malicious participants from controlling the block generation. Bitcoin implemented its decentralized Sybil control mechanism using a Proof-of-Work (PoW) scheme. Simply, PoW requires sufficient computational effort from the participants. The PoW concept was proposed by Dwork to prevent spam mails [13]. In Bitcoin, a block can be confirmed when the block contains a hash value that is difficult enough to find, and the Bitcoin network controls the difficulty. Though Bitcoin uses PoW as its Sybil control mechanism, we do not recognize PoW as a blockchain's essential property because other cryptocurrencies and blockchain solutions use different decentralized Sybil control mechanisms like Proof-of-Stake (PoS), Proof-of-Burn (PoB), Delegate Proof-of-Stake (DPoS), and PBFT.

From the perspective of operation, blockchains can be categorized into four types. As seen in Table 2, these include public (permissionless), public permissioned, consortium, and private blockchain. Bitcoin is a public blockchain, or public permissionless, in which anyone can be a participant. In other words, in the public blockchain, everyone can suggest a block and everyone can validate data. Most cryptocurrencies are public blockchains and anyone can suggest a new block, make a transaction, or validate transaction data. In a private blockchain, all participants are authorized in a particular group, such as a company, and the network is not accessible for public use. Naturally, a private blockchain is less decentralized than a public one. In a consortium blockchain, participants are limited as its network is built or owned only for multiple entities. Therefore, it has medium characteristics of a public blockchain and a private blockchain.

In addition, depending on the authentication of the participants, blockchains can be categorized into permissioned blockchain or permissionless blockchain. As we mentioned above, a public blockchain is generally a permissionless blockchain. On the other hand, we can construct a public permissioned blockchain with a permissioned writership system while anyone can see and verify blockchain data for decentralized governance. In this case, it has medium characteristics between a public blockchain and consortium blockchain.

**TABLE 2.** **Blockchain operation types.**

| Blockchain Type | Write | Read | Owner |
|---|---|---|---|
| Public chain | Public | Public | N/A |
| Public permissioned chain | Limited | Public | Single/Multiple |
| Consortium chain | Limited | Limited | Multiple |
| Private chain | Limited | Limited | Single |

Lastly, smart contract, which is introduced by Ethereum, is one of the biggest advances in the blockchain technology. Over simplified scripts for e-cash transactions, Ethereum provides a Turing-complete smart contract environment that can implement any computable code, including recursion, with user-friendly languages like Solidity. Similar to multiparty computation, nodes in decentralized networks implement smart contracts and verify the computations together in a blockchain. If the nodes achieve the same results of a smart contract's code execution, the nodes store the resulting state on the blockchain. By using smart contracts, people can use various applications with trustworthy computations.

## III. BENEFITS OF USING A BLOCKCHAIN FOR CYBER DEFENSE

In this section, we explain cyber defense using the definition of cyber security. Then, we discuss how a blockchain can provide benefits for cyber defense.

### A. CYBER DEFENSE

Cyber defense is a relatively new norm as a result of recent cyber attacks on various governments throughout the world. Cyber attacks on countries have become a severe issue. The following cyber attacks have made governments realize that a 'cyber war' is already in progress: the attacks on Estonia in 2007, on Georgia in 2008, on South Korea in 2009, on the Iranian nuclear facility in 2010, as well as various conflicts between the US and China. In addition to these obvious threats from other countries, insider threats also pose a big risk to national security. In a system for critical infrastructure, a single insider threat can force systems to collapse. Betrayal or unintentional human mistakes are difficult to foresee. In addition, supply chains are complex with multiple stakeholders because a complex supply chain structure may involve a potential enemy. For example, software or hardware backdoors that are not clearly visible could infiltrate systems. Political intervention via cyber space, such as social media, has also been pointed out repeatedly. Cyber defense is the practice of responding to everyday threats against national interests and to large-scale adversarial acts of cyber warfare. To comprehend cyber defense clearly, an accurate understanding of cyber security is key.

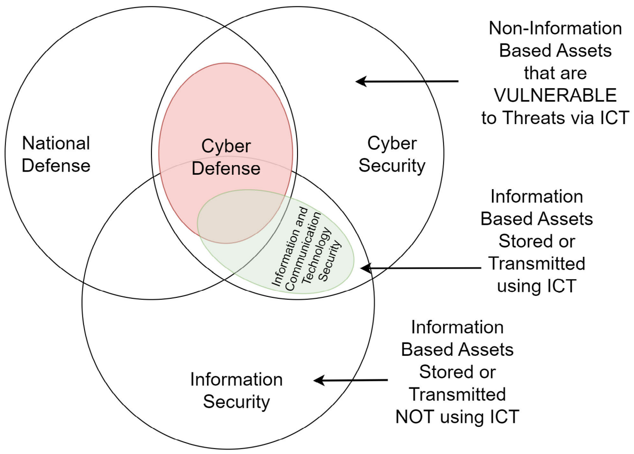


**FIGURE 3.** **Relationship between information security, cyber security, and national defense. By adding national defense to the figure in von Solms and van Niekerk [14], cyber defense is defined.**

Fig. 3 illustrates cyber defense and its relationships with national security (defense), cyber security, and information security. It is clear that cyber defense is the shared domain of national security and cyber security. Though we have discussed cyber defense, it is still ambiguous as to whether cyber security, one of the key foundations of cyber defense, can be adequately defined. Unlike national security, cyber security is easily misconstrued for information security. Von Solms and Van Niekerk [14] pointed out that the definition of cyber security varies, even in official and standard documents. However, the authors provided a sound definition themselves based on a threat's source. Protecting assets from threats via/using Information and Communication Technology (ICT) is the at cyber security's very core. Although when their discussions of information and non-information based assets seem vague, we consider their definition to be the finest among past reasons. Therefore, with the help of their work, we have divided the notion of cyber defense into the following three categories:

*Definition 1: Cyber security* is the practice of protecting assets from threats via Information and Communication Technology (ICT).

Cyber defense derives from merging cyber security and traditional defense techniques so it is important that we clarify the term 'defense' in this particular context. If we use 'defense' to describe security in a national sense, it is clear that the expressions 'national defense' and 'national security' can be used interchangeably.

*Definition 2: National defense* or *national security* is the practice of protecting a nation state and its structures from inner and outer threats.

By combining the two aforementioned concepts, the following is constructed.

*Definition 3: Cyber defense* is the practice of protecting national assets from inner and outer threats coming via Information and Communication Technology (ICT).

### B. ADVANTAGES OF BLOCKCHAIN IN CYBER DEFENSE

#### 1) VISIBILITY

Due to its distributed and shared ledger structure, blockchain improves the visibility of data which, in turn, can provide greater security. Since militaries are becoming more modernized and digitized thanks to the rapid advancement of technology, there are now plenty of data producers and consumers. Excessive data can create challenges in terms of proper capability for efficient processing. This can cause disruptions when attempting to deal with threats. A recent survey in Balbix's enterprise security report [15] shows that 52% of cyber security professionals do not have continuous visibility on their risk area, which is, therefore, one of the significant difficulties in treating threats. In a blockchain, the data's history is shown from generation to process, transformation and ending. Therefore, all participants are able to see who generated or who processed data. Such visibility creates opportunities to easily locate threats in the early stages and develop systems to eradicate them quickly.

It has also been suggested that businesses could financially benefit from this visibility. A recent report by PricewaterhouseCoopers (PwC) [16] analyzes that applying blockchain to the aviation industry's supply chain would result in about 4% profit because of data efficiency. A study shows that blockchain's information sharing positively affects the allocation of available industrial resources, which results in an economic advantage. However, unlike general industries, the application of blockchain in the defense sector may be limited. For example, data classified as secret may be challenging to share between participants. In this case, It is possible to apply blockchain by processing specific data in an off-chain and including only the relevant metadata in the blockchain.

#### 2) VERIFIABILITY

The advantages of blockchain are not solely based around providing visible data but also span to verifiability to enchance cyber security. For example, an adversary can interfere with data processes if it was processed by multiple entities. The entities can adopt blockchain on the data processed. By validating data before a process and after a process by entities, we can guarantee data is valid. The validity depends on what kinds of data and processes are expressed and validated on the blockchain. Besides, smart contracts also provide a validated data process environment.

According to a Lockheed Martin's report [17], more than 1,900 top-tier suppliers worldwide supply parts for F-35 fighter jets. A wide variety of contributors are involved in the defense industry due to globalization. However, among them, there can be countries that may not have as close relations as others, especially in supply chains. In particular, there have been significant issues whereby microchips that were undisclosed in original blueprint documents have been discovered. In this situation, the application of blockchain throughout complex manufacturing processes like these can provide a solution. Although absence of defects from suppliers is not completely guaranteed, blockchain significantly reduces any possibility of deceit within the defense industry because of a higher verifiability of data.

#### 3) ELIMINATING A SINGLE POINT OF FAILURE

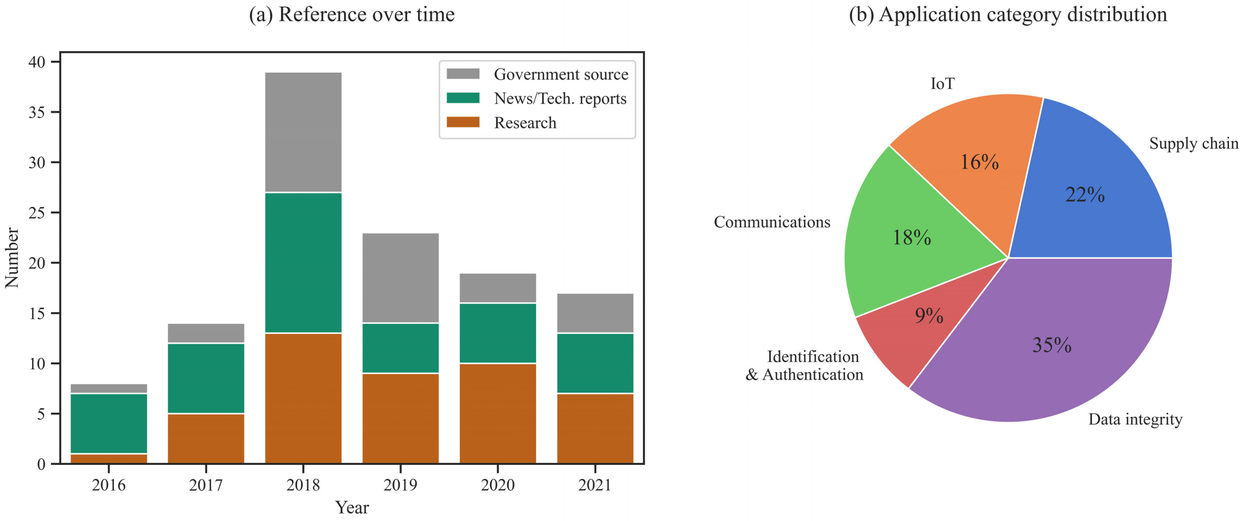
The motivation for the first development of the blockchain was to implement e-cash without a centralized control. In order for e-cash to be used as a normal currency, strong reliability of transaction data must be guaranteed. In a structure with one centralized control server, such as an existing digital banking system, the server becomes a problem to be a single point of failure. However, this problem rarely exists in a decentralized blockchain environment.

In fact, the problem that Bitcoin tried to solve through the blockchain is called Sybil attack [18] on a distributed network. Sybil attack refers to an attack that adversely affects decision-making by controlling multiple nodes on the network in a way that deceives one attacker as if there were actually multiple attackers. It means that blockchain systems considered multiple points of failure. For example, PBFT requires two-thirds or more node voting to generate blocks, so if an attacker controls more than one-third of nodes, the system can fail. By adopting PoW, a Bitcoin attacker must occupy more than half of the computing power of the entire network to successfully perform a Sybil attack, making it very challenging to succeed in reality.

Therefore, when applying the blockchain to the national system for cyber defense purposes, it is possible to solve the single point of failure and respond to situations in which attackers occupy multiple nodes. This characteristic is useful for core infrastructure such as military networks and power plants, which should never fail, directly related to the survival of the country. However, the defensive effect may vary depending on which Sybil control mechanism is used and how resources can be distributed. For example, PBFT has the right to participate in decision-making in proportion to the number of nodes participating, and PoW is proportional to computing power, and PoS is proportional to stake it has. For instance, if one node occupies overwhelming computing power in PoW, even in a blockchain, the node can be a single point of failure. A more detailed discussion of the cyber defense environment and the decentralized environment is covered in Section V.

#### 4) AUDITABILITY

The blockchain data structure consists of a continuous hash-chain. It is almost impossible to erase or modify data in the middle of the blocks. Thus, the participants can retain auditability of the system data for cyber defense. For example, we can assume that a nuclear power plant went through cyber attacks and was subjected to a certain damage. Systematic state-sponsored cyber attacks also attempted


(a) Reference over time

(b) Application category distribution

**FIGURE 4.** The two charts illustrate our system of survey. Fig. (a) shows references over year and sources. Fig. (b) is what we classified references according to the application domains.

remove every trace of evidence. Removing or distorting data for the purpose of interfering with cyber intelligence analysis is becoming part of sophisticated attacks, and if the logs that were generated during the cyber attacks involving nuclear power plants are systematically removed, then the affected country will have difficulty in identifying the attack process and the target. In addition, countries already have problems in securing legal evidence to ascertain the responsibility to the cyber attacks. We believe that the blockchain-applied system provides excellent auditability for this issue.

## IV. ANALYSIS OF BLOCKCHAIN R&D TRENDS IN CYBER DEFENSE

In this section, we analyze blockchain research and development trends, including government policy directions. First of all, we transparently describe the system of our survey. Then, we show the results of investigation and analysis on blockchain applications in order of supply chain, IoT, communication, identification & authentication, and data integrity service.

### A. SYSTEM OF OUR SURVEY

We conducted an extensive survey on the application of blockchain to cyber defense. First of all, according to the second research question (RQ2), our aim is not only to find relevant research but also to identify the trends in blockchain applications by identifying projects that are actually promoted by the government. Secondly, based on the aim, references used in the survey are primarily divided into two categories. One is a reference of research, and the other is a practical project reference. We further divided project references into formal government documents or sources from web pages, technical reports from companies, and news. In many cases, information on military-related or national security-related projects is not preferably disclosed, so there were inevitable news references. In addition, we took care not to overlap when projects found in government source documents pointed to the news. Lastly, we mainly used Google and Google Scholar search engines as the primary survey method. We could also find related references using the references and keywords cited in the primarily obtained references.

Fig. 4 (a) shows the sources we used by year by classifying them by type. Starting in 2017, when the cryptocurrency boom occurred, we found plenty of references on related projects this year. Fig. 4 (b) illustrates what types of projects. We categorized the blockchain projects into five major categories: supply chain management in Section IV-B, Internet-of-Things (IoT) in Section IV-C, communications in Section IV-D, identification & authentication in Section IV-E, and data integrity in Section IV-F. According to the categorization, the blockchain projects are listed in Table 3. Some projects were classified repeatedly according to their characteristics. For example, applications for authentication between IoT are classified into both IoT and authentication applications. In addition, data integrity is a concept that basically enters the purpose of blockchain, so it was used as a concept that includes a wide range of applications that are not appropriate for the remaining four classifications.

We stress that it is challenging to investigate the details of such projects since military projects are often partially disclosed or undisclosed. Furthermore, we found that various basic studies are currently being conducted. For example, the Russian military research lab [53] and the Small Business Innovation Research (SBIR) program on provenance using blockchain on disconnected networks [42] are such cases.

### B. SUPPLY CHAIN MANAGEMENT (SCM)

Supply Chain Management (SCM) is the most notable domain of blockchain applications in cyber defense. As a

**TABLE 3. Government-led blockchain projects in cyber defense.**

| Blockchain Projects | Domain | | | | |
|---|---|---|---|---|---|
| Related to Cyber Defense | Supply Chain | IoT | Comms. | I&A | Integrity |
| Formally Verify Blockchain-Based Integrity Monitoring System (Glois) [19] | | | | | ✔ |
| Military Encrypted Messaging App Built on Blockchain [20] | | | ✔ | | |
| Blockdata: An assessment of various blockchain technologies [21] | | ✔ | ✔ | | ✔ |
| Blockchain on Naval Aviation Enterprise with Indiana-Based Company [22] | ✔ | | | | |
| DHS Grant For Blockchain IoT in Critical Infrastructures (Factom) [23] | | ✔ | | | |
| MOD's Laboratory to create blockchain enabled smart documents (Crossword) [24] | | | | | ✔ |
| Blockchain-based system to record intelligence in Australia [25] | | | | | ✔ |
| Blockchain to help secure aerospace and defense (A&D) supply chains [26] | ✔ | | | | |
| Blockchain for Secret Management [27, 28] | | | | | ✔ |
| French Military Police Finds Use Case for Tezos Blockchain [29] | | | | | ✔ |
| Blockchain-Based Military Digital IDentification (DID) [30] | | | | ✔ | |
| Military Acquisitions Agency's Blockchain-Based Procurement Contract [31] | | | | | ✔ |
| On Blockchain Technology and Its Potential Application in Tactical Networks [32] | ✔ | ✔ | ✔ | ✔ | ✔ |
| Military Blockchain for Supply Chain Management [33] | ✔ | | | | |
| Blockchain Technology in Military Strategy formulation [34] | | | | | ✔ |
| Research on Missile Data Security Based on Blockchain [35] | | | | | ✔ |
| Study on Trends and Strategies for Defense Blockchain and ICT Technologies [36] | | | | | ✔ |
| Navy's Approved Multi-Factor Authentication for Personal Mobile Devices [37] | | | | ✔ | |
| SOCOM's Automated Processing, Exploitation and Dissemination Project [38] | | | | | ✔ |
| BlockChain Supply Chain Enhancement for Trusted and Assured FPGA and ASICs [39] | ✔ | | | | |
| Decentralized Key Management using Blockchain [40] | | | | ✔ | |
| Army Innovation Network - Information System [41] | | | | | ✔ |
| Provenance using Blockchain on Disconnected Networks [42] | | | ✔ | | ✔ |
| Supporting Continuity of Operations (COOP) [43] | | | ✔ | | ✔ |
| Sharing of Defense R&D Data Distribution using Blockchain [44] | | | | | ✔ |
| Clearinghouse for Subsistence Ordering & Receipt (CSOR) [45] | | | ✔ | | |
| Information Trust Technology for Communication [46] | | | ✔ | | ✔ |
| Improving Understanding of Blockchain and Exploring Opportunities [47, 48] | | | | | ✔ |
| Dynamic Management on Unmanned Aerial Systems [49–51] | | ✔ | | | ✔ |
| Global Data Integration [52] | | | | | ✔ |

brief definition, supply chain management manages all processes related to the supply of goods from producers to consumers. To be concrete, SCM includes planning, sourcing, making, delivering, and returning. Barnas [54], Wrona and Jaroza [55] discussed SCM as one of the core blockchain applications in defense. Wrona and Jaroza [55] proposed a detailed blockchain data structure considering confidentiality in a NATO standard agreement so that their research could be practically applicable.

Cyber attacks on SCM processes are attractive for attackers. Assume that an attacker wants to affect a weapon systems, which is an air-launch vehicle. When the weapons system is launched, the time window before the strike is terribly limited for the attacker to corrupt. Furthermore, direct access to the weapons system is not easy physically or logically due to multiple security layers. On the other hand, if the attacker infiltrates into the SCM process of the weapons system, the attacker can modify the system before the weapon's use. In addition, the SCM process is complex with a variety of subprocesses. This implies that the attack surface of the SCM process exposes plenty of attack vectors that are not managed properly.

A testimony from Semiconductor Industry Association (SIA) [56] states that as many as 15% of the parts purchased by the Pentagon are counterfeit. It is therefore challenging to identify whether a counterfeit part is just introduced for economic reasons or with malicious intent. This uncertainty implies that threats to SCM can become much more severe than expected. Bloomberg [57] discussed a real-world spy chip issue. Software update processes are also included in the SCM. The hacking of the department of defense in South Korea can be considered to be a supply chain attack [58]. In this case, the hacker exploited anti-virus update servers to take over the personal computers of the users. In general, an anti-virus update is transferred to most personal computers, so it is an attractive vector for attackers. A recent attack on

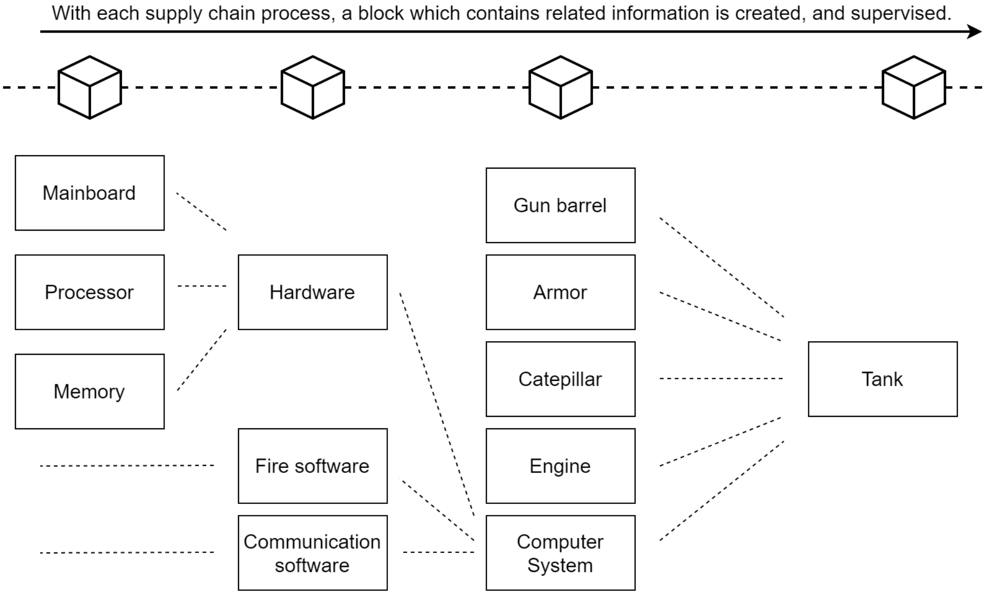


**FIGURE 5.** **Blockchain-based supply chain example. To manufacture a tank, there are a lot of components are needed. From a certain level of component, a block is created with the related information. Therefore, we can supervise the supply process of every single tank. Especially, tracking and monitoring of each part prevent the inclusion of fake parts in the tank.**

the US government and a security vendor, FireEye, occurred when attackers targeted SolarWinds, which is a widely used and trusted network administration tool. By interfering with the update process of SolarWinds, the attackers could access sensitive data [59]. This is also considered a supply chain attack.

Blockchain can provide protection from unintended modifications of the information in the SCM. Based on access to information with high integrity, SCM processes cannot be easily corrupted. Therefore, by applying blockchain throughout the SCM process, it is expected for this threat to be suppressed by contributing to the process of accurately acquiring the desired defense system.

For example, Fig. 5 shows a blockchain-based supply chain for a tank manufacturer. There are major components, including barrels, armors, an engine, and a computer system. The major components are comprised of smaller components. When a component is produced, a block including its relevant information is created so that it can be transparently monitored by the related suppliers and authorities. We believe this process can prevent counterfeit components with rigorous records on the blockchain.

One of the technologies in the spotlight in SCM is a digital twin. Several studies show that the blockchain will provide secure data management capabilities in a complex multilateral digital twin process [60], [61]. For industrial management, digital twins are their cyber representation of the physical assets to understand, simulate, predict, analyze, and optimize. By constructing the same digital twin corresponding to the real physical product, a manufacturer can trace and examine the product in the computer and in the information systems. As the physical product moves along in manufacturing progress, its digital twin follows with the same history. In the process, all records exist as immutable digital records. In particular, Putz *et al.* [61] used Ethereum to provide a full-featured open source prototype for a digital twin, suggesting that a blockchain can immediately be applied to the digital twin.

For this reason, the R&D projects directly related to the SCM and cyber defense were carried out in several respects. Hsieh and Ravich [63] studied blockchain use for the supply chain domain. They discussed how a blockchain can be a solution for supply chain attacks for cyber-enabled warfare with an economic perspective. Rahayu *et al.* [33] studied blockchain use for military supply chains, focusing on shipment. However, quantitative or explicit effects were not presented in the research. The Department of Defense (DoD) of the United States launched a project to develop an affordable and highly secure supply chain risk management system that is enhanced by blockchain technology using the uniqueness of Physically Unclonable Functions (PUFs) [39]. A PUF is a kind of digital fingerprint of the hardware and depends on the physical microstructure during manufacturing. It provides a unique id on the hardware so that, for example, people can trace a chip efficiently in a supply chain using the blockchain. Indiana Technology and Manufacturing Companies (ITAMCO) announced that they had started cooperation to help track aviation parts throughout their life-cycle with the US Navy [22]. Article [26] showed that a pilot project using blockchain technology in aerospace and defense (A&D) supply chains demonstrated successfully, and companies are still finding new projects using blockchain implementations.

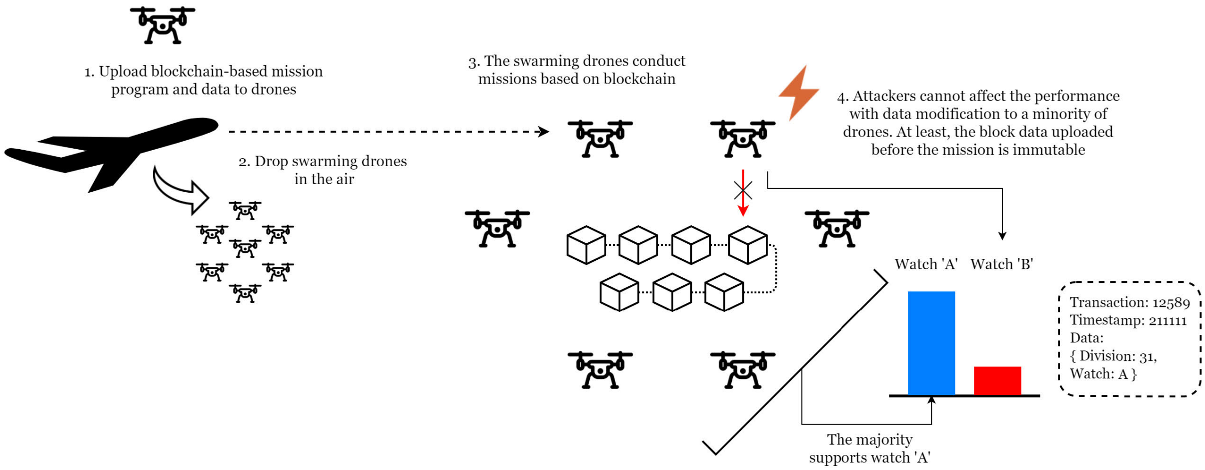

1. Upload blockchain-based mission program and data to drones
2. Drop swarming drones in the air
3. The swarming drones conduct missions based on blockchain
4. Attackers cannot affect the performance with data modification to a minority of drones. At least, the block data uploaded before the mission is immutable
Watch 'A'
Watch 'B'
Transaction: 12589
Timestamp: 211111
Data:
{ Division: 31,
Watch: A }
The majority supports watch 'A'

**FIGURE 6.** **Blockchain-based swarming drone operation example [62]. The swarming drones carry out their mission with pre-installed blockchain data. Mission data recording and decision-making are made through the blockchain. Attackers have difficulty in intervening in the already-recorded context of the mission performance.**

Notably, the need for blockchain applications was also discussed in the military Additive Manufacturing (AM) field, which requires accurate production based on design [64].

### C. INTERNET-OF-THINGS

Government agencies are paying close attention to the convergence of IoT and blockchain. The Department of Homeland Security (DHS) developed a blockchain solution for IoT sensors in critical infrastructures [23], [65]. It tries to provide programs to help understand blockchain technology for other departments. The blockdata project [66] shows multiple assessment projects to adopt blockchain on defense domains, including IoT. However, further details are not disclosed. Other government documents [67] and research studies funded by government, for example, Willink [32], imply that defense domains are still finding uses of blockchain technology in IoT.

The Internet of Things (IoT) is a system of devices that communicate in cooperative relationships. IoT refers to a new type of network between devices, not human-to-human or human-to-device connections. The number of active devices is increasing rapidly. More sensors gain more information, enabling efficient operational support. The devices may now be smaller than ever before thanks to advances in hardware. Conventional weapons and vehicles in defense are becoming digitalized and have communication functions inside and outside.

IoT in the defense domain is referred to as the Internet of Military Things (IoMT), Internet of Battlefield Things (IoBT), or tactical IoT. [68]. IoBT performs offensive/defensive operations directly as well as supporting roles. For example, drones can be employed for possibly hazardous activities, including surveillance & reconnaissance, destruction, assassination, rescue in difficult-to-access areas, removal of mines, and detoxification of contaminated zones.

From an operational aspect, IoT swarm systems [62], [69] are in the limelight. The IoT swarm system refers to group-operated drones that can be utilized in places where there is a lot of communication infrastructure and accurate operation is required. By managing IoT devices in swarms, not only we can expect efficient execution of the operations, but mission domains can also be expanded. Nevertheless, for IoT swarm systems, the system control and communications must be precise and secure. However, at the same time, an IoT swarm system can collapse due to a cyber attack to the central control. Sensors and their connection can be a vulnerable attack surface from the perspective of security. Security applications mainly target personal computers, servers, or mobile phones, not tiny devices. Small devices are also under threat, but they are often not adequately managed. Occasionally, too little functionality can be performed on a small embedded system, which is sometimes ignored in terms of its needed security. Attacks on IoT devices, in the context of cyber defense, by state-sponsored hackers were already detected [70]. Hacked devices for the soldiers raised the suspicion of armed intervention that Ukrainian soldiers would also be under a physical attack [71]. In this context, the UK and the US had military training in situations with hacked IoT devices [72], [73].

Blockchain can provide security-enhanced IoT environments. Related research [74]–[77] pointed out that blockchain can cover security problems for IoT. Together with an integration with the blockchain, at first, makes the control of IoT devices decentralized so that it prevents the single point of failure problem. Second, a decentralized system with blockchain increases the reliability of the data. Data on the blockchain is hard to tamper with for attackers. Third, the decentrality of the blockchain doubles the cost of an attacker to compromise a system since the attacker should take control of multiple devices, at least. Finally, reliable data provided by a blockchain can be used to identify and authorize IoT devices in a network. Fig. 6 shows an example blockchain-based swarming drone operation. Drones perform based on pre-installed blockchain data, collecting data from the battlefield, and receiving data from their command center. Even if cyberattacks are successful on some drones, conceptually, there is no significant impact on the mission performance of the blockchain-based swarming drones.

Since the need to combine blockchain with IoT is being examined, blockchain for IoT in defense research focuses on usability. The adoption of blockchain for IoT is evaluated according to the performance and scalability [78], [79]. In another case, Won *et al.* [80] proposed a decentralized IoT-PKI structure for IoT security in the context of the military use. In the US Air Force documents [49]–[51], a project includes dynamic management on unmanned aerial systems using blockchain. Also, the fact that the project is continuously promoted implies the significance of blockchain's role in drone swarm systems.

### D. COMMUNICATIONS

It is always critical for national defense to build secure communication platforms. The absence of a proper tactical network can lead to tactical isolation of a unit, which can lead to annihilation. Tampering in communications can lead to significant failures in defense. Eavesdropping on communications can also expose defense tactics. As a result, communications have always been strategically crucial, and challenges to these communications are canonical. Communications have various applications that depend on various levels. For example, at a low level, tactical networks have various data links that primarily use Ethernet connections. Communications in defense also include email and chat applications.

Blockchain can provide secure and reliable communications capabilities, which are the nature of the blockchain. Empirically, Bitcoin has already demonstrated communications capabilities without a trust base. Since 2009, the Bitcoin blockchain system has worked successfully in cryptocurrency transactions. Though financial institutions have financial fundamentals, Bitcoin systems do not have any financial fundamentals. The value of Bitcoin only relies on trust in the system. Crucially, people found that a Bitcoin system with a decentralized structure is nearly immutable and available all the time in a defined capacity.

For such reasons, the government has backed a number of initiatives that use blockchain to facilitate military communications. A Canadian military research group discussed potential blockchain applications for communications in a tactical network [32]. The US Department of Defense (DoD) introduced blockchain technology as a cyber security shield in a trustless environment [81]. The document also shows that the Defense Advanced Research Projects Agency (DARPA) started experiments for an efficient, robust, and secure platform to transmit secure messages or process transactions.

Another blockchain project with the keyword 'unhackable code' was introduced to transmit secure messages or process transactions [81]. A similar project named information trust technology [46] concerns to securing messages on distributed ledgers. There are two more DoD projects related to blockchain adoption in communications. One is an applicative project, Supporting Continuity of Operations (COOP), through resilient blockchain frameworks [43]. The other is the development of a private blockchain in challenging situations to assess provenance using blockchain on disconnected networks [42]. A disjointed network is not commonly discussed in the private sector because network disconnections are temporary or not typical. However, we consider it to be a severe problem in cyber defense. Thus we will discuss this in Section V.

In a research context, Barnas [54] addressed the use of blockchain for robust defense communications at a fundamental level, and blockchain technology was studied for use in network-enabled military operations. Sudhan and Nene [82] proposed for blockchain to maintain the sustainability of networks for military operations. Even though military networks are not an untrusted environment, research has considered that a part of the networks can be compromised. Wrona and Jarosz [55] pointed out that confidentiality can be an issue in military blockchain applications. They proposed a data structure to achieve confidentiality within a standard NATO agreement. As was discussed in the former part, communications techniques using blockchain in IoT devices were also studied. Rivera *et al.* [79] proposed a scalable blockchain implementation using edge computing, and they demonstrated the scalability and security of their architecture, combining edge computing with a blockchain architecture. Menagay *et al.* [83] proposed concrete communications applications, including email, chat, and a military interdepartmental purchases. They proposed that blockchain enhances the security of the system backend.

### E. IDENTIFICATION AND AUTHENTICATION

Identification and authentication are not only intuitive features to implement with blockchain, since these require public verification, but also are essential for other domains of cyber defense. This is an area where blockchain is being implemented in the real world [30], [31], [37], [40], [65]. The user, the device, and the application are the objects for identification and authentication from conventional methods such as passwords to recently improved methods, including biometrics. In addition, our discussion in this part includes key management.

Blockchain can provide strong identification and authentication for cyber defense environments. At first, Bitcoin's blockchain system has been based on authentication with public-key cryptography. Furthermore, data on the blockchain is nearly immutable and consistently available. The factors needed for identification or authentication on the blockchain can be useful, and as if to prove the point, many cryptocurrencies have been created to address identification features. One cryptocurrency information website introduces 32 coins (e.g. Project Pai [84], Civic [85], Metaverse

ETP [86], Metadium [87], CryptoVerificationCoin [88], V-ID [89], and so on) as identity-specific blockchain cryptocurrency implementations.

In that context, the following blockchain R&D projects were conducted. Won *et al.* [80] studied decentralized public key infrastructure for IoT. Their study detailed in the blockchain protocol, public key structure, and corresponding evaluation. As for real applications in defense, South Korea has adopted a blockchain Digital IDentifier (DID) for military manpower administration [30]. It has already been provided as a service for average citizens, and the US Navy also started a project for multi-factor authentication for personal mobile devices using a blockchain implementation [37]. The DHS's decentralized key management project is another blockchain project in the cyber defense domain, and it was developed for privacy-respecting identity management  [40], [65].

### F. DATA INTEGRITY

Data integrity refers to maintaining the correctness and consistency of data over its life cycle. Almost all operations in a system are based on data, such as data fetch, data store, and data delete. Thus, the issue of data integrity can affect the confidentiality and authorization beyond simple data processing errors. Data integrity is the most fundamental property in a blockchain. As shown in Fig. 4 (c), the data integrity provided by blockchain is the basis of the other four application categories. Nevertheless, data integrity was classified into an independent category because a number of projects used blockchain technology to protect the integrity of the specific data, not to build new application schemes through a blockchain.

In Bitcoin, all transactions are hash-chained so that people can trust the integrity of the transactions. Contrary to a distributed database, we can track every single state as well as the changes in data. The structure of the blockchain is costly in terms of the needed resources, but it guarantees data integrity. Thus, blockchain applications for data integrity are the most fundamental and reliable for use. Barnas [54] of the Air University of the US Air Force expected blockchain to enhance data integrity in defense applications. This study placed an emphasis on the role of a blockchain, but no specific application design nor experiment was presented.

Other studies that proposed more specific applications are as the following. Sudhan and Nene [82] suggested blockchain technology as a viable solution to ensure the integrity and provenance of data to suit military operations using networks. They proposed four kinds of employability potentials, including secure messaging, logistics, supply chains, and patient records. Wrona and Jarosz [55] focused on information management using the federated mission environment of NATO. Their work is remarkable since they chose this application in two conditions: mistrust existence and Trusted Third Party (TTP) non-existence. Not directly for military use, but still in the cyber defense context, Patel *et al.* [90] proposed border control and immigration information on the blockchain. Wang *et al.* [35], in which the first author belongs to the People's Liberation Army, suggested a blockchain data model specifically for aviation missile data.

Protection against cyber threats targeting private data also falls within the scope of cyber defense in some cases. Areas of particular attention from this point of view are medical facilities and medical data protection. The hacking of vaccine companies in connection with the 2019 Corona Pandemic has also become a problem. In 2020, there was also the first case in which a patient died from a hospital ransomware infection. Concerning here, multiple studies were conducted for access control of patient information using blockchain. Wu *et al.* [91] proposed a health information system based on blockchain to manage privacy and access control in medical information on the cloud. They provided a security and privacy analysis of the system.

As a government-led project, we found the US army started three projects related to blockchain technology. A project within the army innovation network [41] addresses the development of an innovative network but without detailed blockchain use. Another project regarding provenance uses blockchain on disconnected objects [42] in a manner strongly related to blockchain. This aims to develop capabilities to maintain data integrity in challenging situations rather than direct applications. A project, which is named Global data integration [52], aims to support data governance, provenance, and discoverability related to artificial intelligence. The US Special Operations COMmand (SOCOM) mentioned that blockchain should be included in the development of automated Processing, Exploitation, and Dissemination (PED) systems. The US DoD started a blockchain project to share defense research, and development data [44]. The US Navy announced a plan to develop an information system for the subsistence of total order and receipt, which is also related to supply chain management. It does not directly mention using blockchain implementations, but its keywords implies that a consideration of the use of such.

The Ministry of Defense in South Korea had two projects addressing data integrity. One is a military acquisition agency project to use a blockchain for procurement [92]. The other is a blockchain for managing secrets [27]. Even though a blockchain is expected to provide traceability and integrity of a secret, this project was criticized by technology experts in that it is unnecessary or inappropriate to keep information on secrets across distributed nodes [28]. In France, military police started to record information relevant to investigations on a blockchain to ensure integrity  [29]. Even though a blockchain may provide better security properties relative to existing platforms, some of these projects are questionable in whether their systems have in fact been implemented to address practical threats through their introduction of blockchain technology.

## V. ANALYSIS OF PROBLEMS WHEN APPLYING BLOCKCHAIN TO CYBER DEFENSE

This section focuses on three domain-specific challenges that are highly relevant to the subject of cyber defense rather than general concerns that were mentioned in the earlier literature.

### A. DYNAMIC BATTLEFIELD ENVIRONMENT

Battlefield environments can be more dynamic compared to commercial applications that were previously assumed. Military operations on battlefields require networks to be tolerant under extreme situations. In wartime, physical damage, as well as software failures, often occur. Extreme situations include, for example, two problems: frequent network partitioning and network expansion/shrinkage.

Resolving a fork in the blockchain is complicated. When the whole network is divided into two network partitions, the blockchain on each network works independently, and this results in a fork in the blockchain. A fork includes two kinds of notions: a hard fork and a soft fork. The soft fork refers to a situation where a logical change was made in a blockchain protocol or in a data structure. The hard fork refers to a situation in which two or more chains grow from a specific block. In general, a hard fork creates confusion through data inconsistency, so it should be resolved as quickly as possible. In public blockchains like Bitcoin [5] and Ethereum [6], a hard fork sometimes occurs when miners find blocks at the same time. They have a clear rule to resolve a hard fork by a long-chain rule based on a block height and resource consumption. Practical Byzantine Fault Tolerance (PBFT), [93] which generally is used for private blockchain consensus like with Hyperledger [94] is deterministic so that a hard fork does not occur.

In a partitioned network situation, the fork should be resolved. Assuming there is an algorithm to choose one legitimate chain, one of the chains will then be chosen. However, for example, assuming nodes are sensors to collect data in the battlefield at each location, it is not proper to choose a chain from only one partition. In this case, we need to keep all data from all partial chains. We should consider approaches to keep fork chains, not only choosing just one right chain depending on the situation. Then, a deterministic Sybil control mechanism, for example PBFT, can be considered to avoid a fork. This raises another problem below.

**TABLE 4. Block generation rate of blockchain consensus under challenging situations when assuming the throughput is 1 before the situation. The symbol *e* indicates a positive number to describe an extra change.**

| Given Situation | PoW | PoS | PoA | PBFT |
|---|---|---|---|---|
| Network Split (1/2, 1/2) | $(1/2-1, 1/2-1)$ | $(1+e, 1+e)$ | $(1+e, 1+e)$ | $(0, 0)$ |
| Network Split (2/3, 1/3) | $(2/3-1, 1/3-1)$ | $(1+e, 1+e)$ | $(1+e, 1+e)$ | $(1+e, 0)$ |
| Network Shrinkage (1/2) | $1/2-1$ | $1-e$ | $1+e$ | $1+e$ |
| Network Expansion (3/2) | $1-2/3$ | $1-e$ | $1-e$ | $1-e$ |

Second, changes in the blockchain network's shape or scale, especially sudden changes, cause problems. Table 4 presents the expected block generation rate of a blockchain in problematic situations caused by a dynamic battlefield environment. Four Sybil control Mechanisms are compared: PoW, PoS, PBFT, and Proof-of-Authority (PoA). We consider that PoA is considerable to use in military environments. It has the economy of PoS in that it can obtain block generation privileges via allocated authorities instead of tokens. First, looking at the situation in which the network is divided into 1/2 and 1/2, PoW does not instantaneously reduce the task difficulty, resulting in throughput halving in proportion to the resource halving. PoS and PoA are always dependent on relative resources and are therefore largely unaffected. PBFT requires at least 2/3 of the nodes to reach a consensus. As mentioned previously, the forks do not occur, but PBFT ''fails to generate any blocks.'' When a network is divided into 1/3 and 2/3, only the network part with 2/3 partition can generate blocks from the 2/3 partitions.

In addition to partitioned networks, we expect difficulties with a decrease or extension of the networks. PoS, PoA, and PBFT do not directly affect resource consumption because of the size of the network. On the contrary, PoW decides the difficulty of the block generation relative to the network resource size. Therefore, in the case of the shrunk network, block generation speed is reduced under the existing fixed difficulty level and recovers to normal speed as the difficulty is adjusted. When expanding, the block generation speed increases, but as the difficulty is adjusted, the block generation speed returns to a normal level.

### B. THE AIR GAPPED NETWORK ENVIRONMENT

It is common for military environments to have air gapped networks for cyber security. Likewise, many critical infrastructures have air gapped networks to protect systems from unknown cyber threats. There may even be double-triple air gaps that depend on a network structure. Even for private companies, there are often places with air gapped environments when requiring important updates to security. The air gapped network blocks the flow of information, and the most extreme case is that the flow of information does not form at all. Another case is the one-way flow of information. The least restricted one is the intermittent flow of information in both directions. Blockchain applications used in networks with air gaps may have an issue for consensus by controlling limited information. It makes the Blockchain Oracle problem [95] worse. For example, consider a software supply chain with periodic software patches. Although software inside the air gap relies on externally provided patches, it is not possible to construct a blockchain-based system with reliable information because it does not have direct access to external patches inside the network.

Another issue to consider is how network separation caused by air gaps impacts decentralization. The security characteristics of the blockchain are maximized when proper decentralization has been achieved. Gochhayat *et al.* [96] measured the centrality of blockchain-based systems. Measuring centrality helps understand the decentrality of the systems. In the study [96], the networks were mainly measured

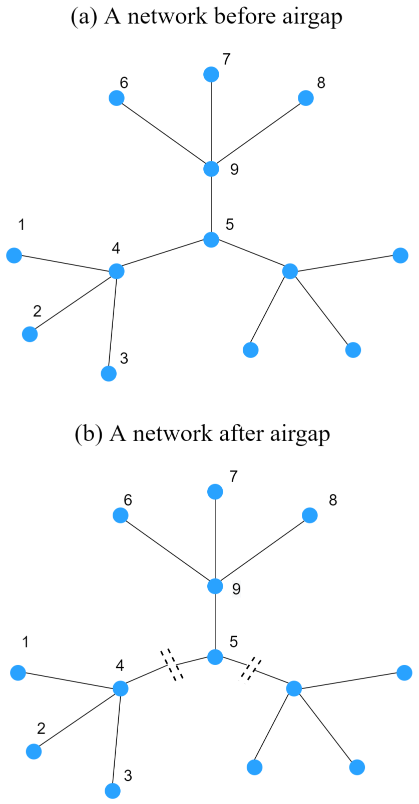


FIGURE 7. Network topology example with air gaps.

using three methods, which are degree centrality, betweenness centrality, and closeness centrality. The degree centrality implies the number of directly connected nodes to a node. The betweenness centrality implies the number of shortest paths through a node. When $\sigma_{st}$ is the total number of shortest paths from node $s$ to node $t$, and $\sigma_{st}(v)$ is the number of paths through $v$ among them, the definition of betweenness centrality is

$$C_{betweenness}(v) = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}}.$$

The closeness centrality indicates the closeness of distances to other nodes from a node. When $d(s, v)$ is the distance between the vertices $s$ and $v$, the definition of the closeness centrality is

$$C_{closeness}(x) = \frac{1}{\sum_s d(s, v)}.$$

There is an example of the network topology illustrated in Fig. 7. Assume that the network needs to adopt two air gaps to protect two subnetworks from potential threats. Fig. 8 shows the result. We can check the difference between the two networks' centralities in Fig. 8. We calculated the betweenness centrality and closeness centrality of nodes 1-9 in two networks. The centrality of the other nodes can be assumed by nodes 1-5. In the betweenness centrality graph, the nodes with a positive centrality value increased with the air gaps.

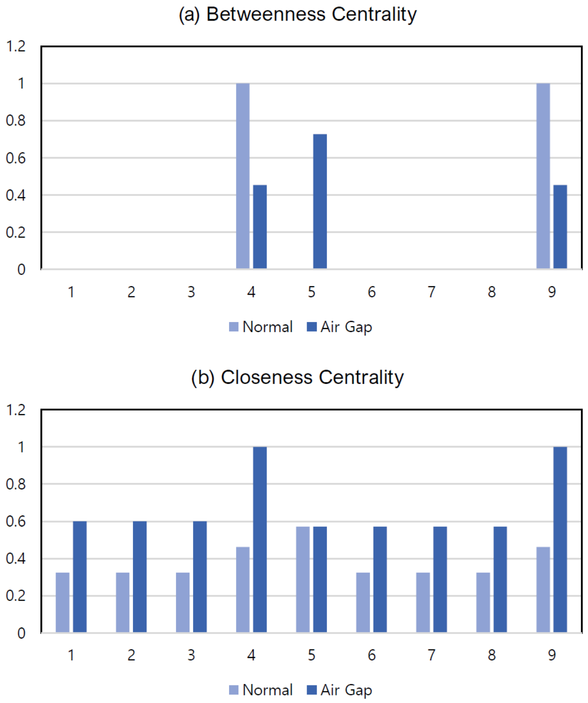


FIGURE 8. Centrality of the example network.

In the closeness centrality graph, the closeness centralities generally increased with the air gaps. The overall centrality of the networks increases with air gaps because the separation caused by the air gaps makes new centers in separate networks. It implies that a network with air gaps may not be as decentralized as its topology. Thus, if a defense system adopts blockchain technology for a network, the system should be examined to achieve sufficient decentralization.

### C. RESOURCE SHORTAGE & HEAVY DEVELOPMENT PROCESS

Resource shortages, including computing power, storage, and bandwidth, is a significant challenge in a tactical network. Nevertheless, blockchain structure needs redundant resources. To store every single state which produces strong integrity, a blockchain takes up several times the storage space of a typical storage format. In a decentralized consensus, nodes need to confirm the majority of the other nodes, and this can require, for example, in PBFT, $O(n^2)$ communications. Also, a previous work [97] pointed out that it is one of the issues for a blockchain-based adaptive resilient cyber-defense system.

Several studies provide blockchain performance evaluation data. Comparative testing on the performance of a blockchain and a database was systemically performed by Chen *et al.* [98]. Their study compared the performance of a private blockchain using Ethereum with 6 nodes and MySQL, which is a relational database. A part of the analysis is shown in Table 5. Even though the maximum data size in a transaction can be undoubtedly advanced, performance differences in throughput and execution time are substantial. The private blockchain using Ethereum is more than 1,000 times slower than MySQL.

**TABLE 5. Performance comparison of a blockchain and a database by Chen *et al.* [98].**

| | Private blockchain<br>(6 nodes Ethereum) | Database<br>(MySQL) |
|---|---|---|
| Maximum transaction size | 6,688 bytes | 65,535 bytes |
| Throughput | Around 3 bytes/ms | Under 1 second |
| Execution | Less than 2027 ms | 1.22 ms in average |

Furthermore, public blockchain mechanisms are slow, and this can be a severe problem for tactical IoT devices that use small, limited spaces. Thanks to recent developments in processors and flash memory, small devices can used with better resources than before. There are studies to improve the performance or scalability of blockchain systems. However, these produce some trade-offs. For example, a scalable PBFT method using network coding [99] requires a stable and delicate network environment.

Nevertheless, there is a lack of research on the performance of blockchains for defense. We cannot apply Chen *et al.* [98], which compared the performance of the relational database and the private blockchain, directly to military environments. As far as we know, for now, the three studied addressed the performance of a blockchain for defense. Table 6 presents a brief description of the environment and critical results in these studies. Unfortunately, all three studies include the simulation results for the environment but do not contain a comparative analysis between the performance of the networks before blockchain and after blockchain implementation. Furthermore, the three studies were applied with different blockchain technologies and different simulation environments. Therefore, a direct comparison is difficult.

**TABLE 6. Research on performance evaluation for blockchain in tactical networks.**

| Research | Environment | Description |
|---|---|---|
| Weston at al. [100] | 10 nodes<br>/ Ethereum | Heavy reliance on TCP and latency<br>7 seconds as block generation latency |
| Liu et al. [101] | 50 nodes<br>/ Weighted PBFT | 5.5 – 6 seconds<br>as block generation latency |
| Feng et al. [102] | 1000 nodes<br>/ B4SDC | 40 seconds for transaction confirmation<br>About 26 tx/s as throughput |

The noteworthy points for the three studies are as follows. Weston *et al.* [100] highlighted blockchain's excessive dependence on TCP. A network environment that is not TCP-supported may exist in a tactical network environment, and blockchains are not likely to be easily applied to these nodes. Liu *et al.* [101] studied that a blockchain system using weighted PBFT and show that higher performance than normal PBFT can be expected in a military environment. Feng *et al.* [102] conducted experiments in the most extensive network environment under a new mechanism named B4SDC. Given the scale, we believe that a 40-second transaction confirmation is acceptable in a public setting. Still, it is a matter of careful consideration depending on whether the mission is performed by a tactical network.

Furthermore, it is not easy to adapt state-of-the-art hardware support to a tactical environment because the defense acquisition process requires a high standard specification for military operation. Furthermore, the acquisition process takes a much longer than in the private sector. Heavy development processes in defense have already caused problems. This results in resource shortages that are more challenging. Blockchain technology should be used as a way to do it efficiently, not as a burden to cyber defense. As a result, blockchain applications should be considered with the current resources and available future resources that can be afforded through development.

## VI. CONCLUDING REMARKS AND FUTURE RECOMMENDATIONS

In this study, we focused on blockchain technology for cyber defense. With digital innovation on military and social infrastructure, cyber threats are not avoidable. Blockchain technology is one of the emerging technologies for security in defense. It has a decentralized nature, so a blockchain ensures data processing integrity. It significantly helps secure system reliability against cyber threats. We provided a scope of cyber defense and reviewed blockchain research and development trends under the defined cyber defense. And then, we explored the potential concerns in the use of blockchain based on recent research and blockchain methodologies. Therefore, this paper clearly shows opportunities, applications, and challenges in blockchain for cyber defense.

Lastly, our key concluding remarks along with future recommendations are as the following:

- It is recommended to improve the practicality of the blockchain, which is to overcome technological limitations. Since the blockchain has a decentralized decision-making process, it is slower than the centralized system and holds more extensive data. We need scalable solutions, such as Plasma, Lightning network, and optimistic roll-up, for this.
- To obtain evaluation data for cyber defense is necessary. As discussed in a previous section, there are additional restricted conditions in cyber defense, contrary to commercial networks, which will affect the blockchain. We introduced several studies related to this issue, but it is far from enough data to apply the blockchain in earnest. Therefore, it is a significant future work to obtain evaluated data from blockchain in defense environments.
- For future surveys, it is required to conduct a large-scale investigation into the government lead blockchain project that is underway. Our study was conducted mainly in the United States, and Lilly and Lilly conducted in-depth research on three countries in related fields. In addition to the three countries, additional

survey analysis is required. However, it is a challenging task due to linguistic limitations and information disclosure policies.

## REFERENCES

[1] E. MacAskill. (2017). *U.K.'s Trident Nuclear Submarines Vulnerable to Catastrophic Hack*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.theguardian.com/U.K.-news/2017/jun/01/uks-trident-nuclear-submarines-vulnerable-to-catastrophic-hack-cyber-attack

[2] *National Defense Authorization Act for Fiscal Year 2020*, United States Congr., Washington, DC, USA, 2020. [Online]. Available: https://www.congress.gov/116/cprt/HPRT40810/CPRT-116HPRT40810.pdf

[3] *Amendment to Rules Committee Print 116–57 Offered by Mr. Soto of Florida*, United States Congr., Washington, DC, USA, 2020. [Online]. Available: https://amendments-rules.house.gov/amendments/SOTO_052_xml713201215551555.pdf

[4] *Amendment to Rules Committee Print 116–57 Offered by Mr. Soto of Florida*, United States Congr., Washington, DC, USA, 2020. [Online]. Available: https://amendments-rules.house.gov/amendments/SOTO_051_xml71320121507157.pdf

[5] Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Oct. 19, 2021. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[6] V. Buterin. *A Next-Generation Smart Contract and Decentralized Application Platform*. Accessed: Oct. 19, 2021. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[7] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, "A systematic literature review of blockchain cyber security," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 147–156, May 2020.

[8] Y. Zhu, X. Zhang, Z. Y. Ju, and C. C. Wang, "A study of blockchain technology development and military application prospects," *J. Phys., Conf. Ser.*, vol. 1507, no. 5, Apr. 2020, Art. no. 052018.

[9] B. Lilly and S. Lilly, "Weaponising blockchain," *RUSI J.*, vol. 166, no. 3, pp. 46–56, 2021, doi: 10.1080/03071847.2021.1886871.

[10] P. Bansal, R. Panchal, S. Bassi, and A. Kumar, "Blockchain for cybersecurity: A comprehensive survey," in *Proc. IEEE 9th Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, Apr. 2020, pp. 260–265.

[11] R. W. Ahmad, H. Hasan, I. Yaqoob, K. Salah, R. Jayaraman, and M. Omar, "Blockchain for aerospace and defense: Opportunities and open research challenges," *Comput. Ind. Eng.*, vol. 151, Jan. 2021, Art. no. 106982.

[12] S. Popov. (2018). *The Tangle (Version 1.4.3)*. Accessed: Oct. 19, 2021. [Online]. Available: http://www.descryptions.com/Iota.pdf

[13] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1992, pp. 139–147.

[14] R. von Solms and J. van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013.

[15] Balbix. (2020). *2020 State of Enterprise Security Posture Report*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.balbix.com/app/uploads/2020-State-of-Enterprise-Security-Posture-Report.pdf

[16] PwC. (2020). *Blockchain in Aerospace*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.pwc.com/gx/en/industries/aerospace-defence/publications/blockchain-in-aerospace.html

[17] L. Martin. (2020). *F-35 Lightning II Program Status and Fast Facts*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.f35.com/content/dam/lockheed-Martin/aero/f35/documents/FG21-00000_001%20F35FastFacts6_2021.pdf

[18] J. R. Douceur, "The sybil attack," in *Proc. Int. Workshop Peer-Peer Syst.* Berlin, Germany: Springer, 2002, pp. 251–260.

[19] Galois, Portland, OR, USA. (2016). *Galois and Guardtime Federal Awarded $1.8 Million DARPA Contract to Formally Verify Blockchain-Based Integrity Monitoring System*. Accessed: Oct. 19, 2021. [Online]. Available: https://galois.com/news/galois-guardtime-formal-verification/

[20] S. Ranger. The U.S. Military wants its own encrypted messaging app built on blockchain, ZDNet. Accessed: Oct. 19, 2021. [Online]. Available: https://www.zdnet.com/article/the-us-military-wants-its-own-encrypted-messaging-app-that-uses-blockchain/

[21] *Department of Defense Fiscal Year (FY) 2019 Budget Estimates*, United States Congr., Washington, DC, USA, 2018. [Online]. Available: https://comptroller.defense.gov/portals/45/documents/defbudget/fy2019/fy19_green_book.pdf

[22] J. Neidig. Naval aviation enterprise exploring blockchain with Indiana-based company ITAMCO. Cision. Accessed: Oct. 19, 2021. [Online]. Available: https://www.prnewswire.com/news-releases/naval-aviation-enterprise-exploring-blockchain-with-indiana-based-company-itamco-300716633.html

[23] DHS S&T Press Office, Homeland Security, Washington, DC, USA. *DHS Awards Austin-Based Factom, Inc. $192k for Blockchain Tech*. Accessed: Oct. 19, 2021. [Online]. available: https://www:dhs:gov/scienceand-technology/news/2018/06/15/news-release-dhsawards-austin-based-factom-inc-192k

[24] Crossword Security, London, U.K. (2016). *Crossword Wins Contract With MOD's Defence Science and Technology Laboratory to Create Blockchain Enabled Smart Documents*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.crosswordcybersecurity.com/2016/05/25/2016-5-crossword-wins-contract-with-mods-defence-science-and-technology-laboratory-to-create-blockchain-enabled-smart-documents/

[25] J. Wagstaff and B. Kaye. (2017). For security agencies, blockchain Goes from suspect to potential solution. Reuters. Accessed: Oct. 19, 2021. [Online]. Available: https://www.reuters.com/article/us-tech-blockchain-security/for-security-agencies-blockchain-goes-from-suspect-to-potential-solution-idUSKBN1DX01A

[26] G. Cowan. Companies look to blockchain to secure supply chains. AIN. Accessed: Oct. 19, 2021. [Online]. Available: https://www.ainonline.com/aviation-news/aerospace/2018-07-12/companies-look-blockchain-secure-supply-chains

[27] J. Kang. (2018). The department of defense will prepare blockchain application plans till november. Digital Today. Accessed: Oct. 19, 2021. [Online]. Available: https://www.digitaltoday.co.kr/news/articleView.html?idxno=301229

[28] S. Han. (2018). Blockchain introduction to military secret management? Experts say negative. Coindesk Korea. Accessed: Oct. 19, 2021. [Online]. Available: https://www.coindeskkorea.com/news/articleView.html?idxno=30682

[29] E. Janus. (2019). French military police finds use case for tezos blockchain. Bitcoinist. Accessed: Oct. 19, 2021. [Online]. Available: https://bitcoinist.com/french-military-police-finds-use-case-for-tezos-blockchain/

[30] R. Martinez. South Korean military gets a blockchain-based upgrade. Bitcoinist. Accessed: Oct. 19, 2021. [Online]. Available: https://bitcoinist.com/south-korean-military-gets-a-blockchain-based-upgrade/

[31] Y. Khatri. South Korea's military acquisitions agency plans blockchain pilot. Coindesk. Accessed: Oct. 19, 2021. [Online]. Available: https://www.coindesk.com/south-koreas-military-acquisitions-agency-plans-blockchain-adoption/

[32] T. J. Willink, "On blockchain technology and its potential application in tactical networks," DRDC—Ottawa Res. Centre, Ottawa, ON, Canada, Tech. Rep. DRDC-RDDC-2018-R033, Apr. 2018.

[33] S. B. Rahayu, N. D. Kamarudin, and A. M. Azahari, "Military blockchain for supply chain management," *J. Educ. Social Sci.*, vol. 13, no. 1, pp. 9–14, 2019.

[34] C. Chedrawi and P. Howayeck, "The role of blockchain technology in military strategy formulation, a resource-based view on capabilities," in *Proc. Cogn. Anal. Manage. Conf. At.* Beirut, Lebanon: American Univ. Beirut Lebanon, 2018.

[35] Y. Wang, L. Cong, Y. Fang, J. Deng, and Y. Chen, "Research on missile data security based on blockchain," *J. Phys., Conf. Ser.*, vol. 1237, no. 2, Jun. 2019, Art. no. 022139, doi: 10.1088/1742-6596/1237/2/022139.

[36] K. H. Lee and H. S. Park, "Study on trends and strategies for defense blockchain and ICT technologies," *Electron. Telecommun. Trends*, vol. 35, no. 1, pp. 12–24, 2020.

[37] U.S. Small Business Administration, Washington, DC, USA. (2017). *Navy Approved Multi-Factor Authentication for Personal Mobile Devices*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.sbir.gov/sbirsearch/detail/1254599

[38] U.S. Small Business Administration, Washington, DC, USA. (2018). *Automated Processing, Exploitation and Dissemination*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.sbir.gov/node/1413791

[39] U.S. Small Business Administration, Washington, DC, USA. (2018). *Blockchain Supply Chain Enhancement for Trusted & Assured FPGA and ASICs*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.sbir.gov/node/1482583

[40] U.S. Small Business Administration, Washington, DC, USA. (2016). *Decentralized Key Management Using Blockchain*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.sbir.gov/sbirsearch/detail/1302463

[41] U.S. Small Business Administration, Washington, DC, USA. (2019). *Army Innovation Network—Information System*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.sbir.gov/node/1620861

[42] U.S. Small Business Administration, Washington, DC, USA. (2018). *Provenance Using Blockchain on Disconnected Networks*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.sbir.gov/node/1531629

[43] U.S. Small Business Administration, Washington, DC, USA. (2019). *Supporting Continuity of Operations (COOP) Through Resilient Blockchain Frameworks (SCOOP-RBF)*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.sbir.gov/sbirsearch/detail/1606125

[44] U.S. Small Business Administration, Washington, DC, USA. (2018). *Sharing of Defense Research, Development, Testing, and Evaluation (RDT&E) Data Distribution Using Distributed Ledger Technologies*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.sbir.gov/node/1508913

[45] U.S. Small Business Administration, Washington, DC, USA. (2018). *Clearinghouse for Subsistence Ordering & Receipt (CSOR)*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.sbir.gov/sbirsearch/detail/1604549

[46] *Department of Defense Fiscal Year (FY) 2021 Budget Estimates Research, Development, Test & Evaluation, Army RDT&E Volume I, Budget Activity 2*, Dept. Army, Arlington County, VA, USA, 2020. [Online]. Available: https://comptroller:defense:gov/Portals/45/Documents/defbudget/fy2021/budget_justification/pdfs/03_RDT_and_E/RDTE_Vol3_OSD_RDTE_PB21_Justification_Book:pdf

[47] *Department of Defense Fiscal Year (FY) 2020 Budget Estimates Defense-Wide Justification Book Volume 3 of 5*, Office Secretary Defense, Washington, DC, USA, 2019. [Online]. Available: https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2020/budget_justification/pdfs/03_RDT_and_E/RDTE_Vol3_OSD_RDTE_PB20_Justification_Book.pdf

[48] *Department of Defense Fiscal Year (FY) 2021 Budget Estimates Defense-Wide Justification Book Volume 3 of 5*, Office Secretary Defense, Washington, DC, USA, 2020. [Online]. Available: https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/budget_justification/pdfs/03_RDT_and_E/RDTE_Vol3_OSD_RDTE_PB21_Justification_Book.pdf

[49] *Department of Defense Fiscal Year (FY) 2020 Budget Estimates Research, Development, Test & Evaluation, Air Force VolI*, Dept. Air Force, Arlington County, VA, USA, 2019. [Online]. Available: https://www:saffm:hq:af:mil/Portals/84/documents/FY21/RDTE_/FY21%20Air%20Force%20Research%20Development%20Test%20and%20Evaluation%20Vol%20I:pdf?ver=2020-02-11-083544-793

[50] *Department of Defense Fiscal Year (FY) 2021 Budget Estimates Research, Development, Test & Evaluation, Air Force VolI*, Dept. Air Force, Arlington County, VA, USA, 2020. [Online]. Available: https://www.saffm.hq.af.mil/Portals/84/documents/FY20/RDTE/FY20_PB_RDTE_Vol-I.PDF?ver=2019-03-18-153506-463

[51] *Department of Defense Fiscal Year (FY) 2022 Budget Estimates Research, Development, Test & Evaluation, Air Force VolI*, Dept. Air Force, Arlington County, VA, USA, 2021. [Online]. Available: https://www.saffm.hq.af.mil/Portals/84/documents/FY22/RDTE_/FY22_PB_RDTE_Vol-I.pdf?ver=DGijGVofWq4jnTnOLuU5Bg%3d%3d

[52] *Department of Defense Fiscal Year (FY) 2022 Budget Estimates Research, Development, Test & Evaluation, Space Force*, Dept. Air Force, Arlington County, VA, USA, 2021. [Online]. Available: https://www.saffm.hq.af.mil/Portals/84/documents/FY22/RDTE_/FY22%20DAF%20J-Book%20-%203620%20-%20SF%20RDT%20and%20E.pdf

[53] M. Shen. (2018). The russian military is building a blockchain research lab. Coindesk. Accessed: Oct. 19, 2021. [Online]. Available: https://www.coindesk.com/the-russian-military-is-building-a-blockchain-research-lab

[54] N. B. Barnas, "Blockchains in national defense: Trustworthy systems in a trustless world," 2016. [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/Education/jpme_papers/barnas_n.pdf

[55] K. Wrona and M. Jarosz, "Does NATO need a blockchain?" in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2018, pp. 667–672.

[56] SIA Anti-Counterfeit Task Force, "Winning the battle against counterfeit semiconductor products," Semicond. Ind. Assoc., Washington, DC, USA, 2013.

[57] J. Robertson and M. Riley. The big hack: How China used a tiny chip to infiltrate U.S. Companies. Bloomberg. Accessed: Oct. 19, 2021. [Online]. Available: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[58] The Dong-A. (2016). *North Korea's Hacking of South Korean Military Cyber Command*. Accessed: Oct. 19, 2021. [Online]. Available: http://www.donga.com/en/article/all/20161207/796965/1/N-Korea-s-hacking-of-S-Korean-military-cyber-command

[59] FireEye. (2020). *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[60] S. Huang, G. Wang, Y. Yan, and X. Fang, "Blockchain-based data management for digital twin of product," *J. Manuf. Syst.*, vol. 54, pp. 361–371, Jan. 2020.

[61] B. Putz, M. Dietz, P. Empl, and G. Pernul, "EtherTwin: Blockchain-based secure digital twin information management," *Inf. Process. Manage.*, vol. 58, no. 1, Jan. 2021, Art. no. 102425.

[62] E. C. Ferrer, "The blockchain: A new framework for robotic swarm systems," in *Proc. Future Technol. Conf.* Cham, Switzerland: Springer, 2018, pp. 1037–1058.

[63] M. Hsieh and S. Ravich, "Leveraging blockchain technology to protect the national security industrial base from supply chain attacks," *Res. Memo, Found. Defense Democracies*, 2017. [Online]. Available: https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/MEMO_Leveraging_Blockchain.pdf

[64] Maritime Executive. *U.S. Navy Looks to Blockchain Revolution*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.maritime-executive.com/article/us-navy-looks-to-blockchain-revolution

[65] DHS S&T Press Office, Homeland Security, Washington, DC, USA. *S&T Leading Blockchain Solution R&D for DHS Components*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.dhs.gov/science-and-technology/blog/2018/05/22/st-leading-blockchain-solution-rd-dhs-components

[66] *Department of Defense Fiscal Year (FY) 2019 Budget Estimates Defense-Wide Justification Book Volume 3A of 5*, Office Secretary Defense, Washington, DC, USA, 2018. [Online]. Available: https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2019/budget_justification/pdfs/03_RDT_and_E/RDTE_DAs_Vol_3A_of_5_OSD_FY19PB-RDTE_Exhibits_BA1-3.pdf

[67] *National Defense Authorization Act for Fiscal Year 2020*, United States Congr., Washington, DC, USA, 2019. [Online]. Available: https://www.congress.gov/116/plaws/publ92/PLAW-116publ92.pdf

[68] Fujitsu Coportation. *Fujitsu Tactical IoT: Connecting Command & Control With the Battlespace*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.fujitsu.com/U.K./Images/Fujitsu-Tactical-IoT.pdf

[69] F. Ye, S. Shao, and Y. Tian, "Weapon target assignment based on improved artificial fish swarm algorithm," in *Proc. USNC-URSI Radio Sci. Meeting, Joint With AP-S Symp.*, Jul. 2018, pp. 15–16.

[70] C. Cimpanu. Microsoft: Russian state hackers are using IoT devices to breach enterprise networks. ZDNet. Accessed: Oct. 19, 2021. [Online]. Available: https://www.zdnet.com/article/microsoft-russian-state-hackers-are-using-iot-devices-to-breach-enterprise-networks/

[71] D. Volz. Russian hackers tracked Ukrainian artillery units using Android implant: Report. Reuters. Accessed: Oct. 19, 2021. [Online]. Available: https://www.reuters.com/article/us-cyber-ukraine/russian-hackers-tracked-ukrainian-artillery-units-using-android-implant-report-idUSKBN14B0CU

[72] J. Jay. IoT soldiers' communications intercepted and disrupted in mock cyber attack. Teiss. Accessed: Oct. 19, 2021. [Online]. Available: https://www.teiss.co.U.K./iot-soldiers-intercepted-cyber-attack/

[73] T. Hitchens. AFRL cyber center to train how to hack sensors (think IoT), Breaking Defense. Accessed: Oct. 19, 2021. [Online]. Available: https://breakingdefense.com/2019/10/afrl-cyber-center-to-train-how-to-hack-sensors-think-iot/

[74] M. A. Khan and K. Salah, ''IoT security: Review, blockchain solutions, and open challenges,'' *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[75] A. Dorri, S. S. Kanhere, and R. Jurdak, ''Towards an optimized BlockChain for IoT,'' in *Proc. 2nd Int. Conf. Internet-Things Design Implement.*, Apr. 2017, pp. 173–178.

[76] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, ''Blockchain and IoT integration: A systematic survey,'' *Sensors*, vol. 18, no. 8, p. 2575, 2018.

[77] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, ''On blockchain and its integration with IoT. Challenges and opportunities,'' *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018.

[78] E. D. Buenrostro, A. O. G. Rivera, D. Tosh, J. C. Acosta, and L. Njilla, ''Evaluating usability of permissioned blockchain for internet-of-battlefield things security,'' in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2019, pp. 841–846.

[79] A. O. G. Rivera, D. K. Tosh, and L. Njilla, ''Scalable blockchain implementation for edge-based Internet of Things platform,'' in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2019, pp. 1–6.

[80] J. Won, A. Singla, E. Bertino, and G. Bollella, ''Decentralized public key infrastructure for Internet-of-Things,'' in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2018, pp. 907–913.

[81] D. L. Norquist, ''DoD digital modernization strategy: DoD information resources management strategic plan FY19-23,'' Office Secretary Defense, Washington, DC, USA, 2019.

[82] A. Sudhan and M. J. Nene, ''Employability of blockchain technology in defence applications,'' in *Proc. Int. Conf. Intell. Sustain. Syst. (ICISS)*, Dec. 2017, pp. 630–637.

[83] P. Menegay, J. Salyers, and G. College, ''Secure communications using blockchain technology,'' in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2018, pp. 599–604.

[84] Project PAI. *Project PAI Motivation Whitepaper*. Accessed: Oct. 19, 2021. [Online]. Available: https://projectpai.com/assets/files/whitepaper/projectpai_whitepaper.pdf

[85] Civic Technologies Inc., San Francisco, CA, USA. *Civic Whitepaper*. Accessed: Oct. 19, 2021. [Online]. Available: https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf

[86] H. Chen, E. Gu, and Y. Jiang. (2018). *Metaverse: New Reality*. Accessed: Oct. 19, 2021. [Online]. Available: http://newmetaverse.org/white-paper/Metaverse-white-paper-v2.1-EN.pdf

[87] *Metadium Whitepaper*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.metadium.com/whitepaper

[88] (2019). *CryptoVerificationCoin Whitepaper*. Accessed: Oct. 19, 2021. [Online]. Available: https://cryptoverificationcoin.com/CVCC_LiteWhitepaper.pdf

[89] (2019). *V-ID Whitepaper*. Accessed: Oct. 19, 2021. [Online]. Available: https://www.allcryptowhitepapers.com/wp-content/uploads/2019/04/V-ID-Whitepaper.pdf

[90] D. Patel and V. Mistry, ''Border control and immigration on blockchain,'' in *Proc. Int. Conf. Blockchain*. Cham, Switzerland: Springer, 2018, pp. 166–179.

[91] H. Wu, A. D. Dwivedi, and G. Srivastava, ''Security and privacy of patient information in medical systems based on blockchain technology,'' *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 17, no. 2s, pp. 1–17, Jun. 2021, doi: 10.1145/3408321.

[92] Defense Acquisition Program Administration, Gwacheon-Si, South Korea. (2019). *Raising Reliability of Defense Programs by Using Blockchain Technology*. Accessed: Oct. 19, 2021. [Online]. Available: http://www.dapa.go.kr/dapa/na/ntt/selectNttInfo.do?bbsId=326&nttSn=31690&menuId=678

[93] M. Castro and B. Liskov, ''Practical Byzantine fault tolerance,'' in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.

[94] Hyperledger Fabric. *A Blockchain Platform for the Enterprise*. Accessed: Oct. 19, 2021. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/

[95] G. Caldarelli, ''Understanding the blockchain Oracle problem: A call for action,'' *Information*, vol. 11, no. 11, p. 509, Oct. 2020.

[96] S. P. Gochhayat, S. Shetty, R. Mukkamala, P. Foytik, G. A. Kamhoua, and L. Njilla, ''Measuring decentrality in blockchain based systems,'' *IEEE Access*, vol. 8, pp. 178372–178390, 2020.

[97] G. Cybenko and R. Hallman, ''Resilient distributed adaptive cyber-defense using blockchain,'' in *Game Theory and Machine Learning for Cyber Security*. Hoboken, NJ, USA: Wiley, 2021, ch. 23, pp. 485–498. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119723950.ch23, doi: 10.1002/9781119723950.ch23.

[98] S. Chen, J. Zhang, R. Shi, J. Yan, and Q. Ke, ''A comparative testing on performance of blockchain and relational database: Foundation for applying smart technology into current business systems,'' in *Proc. Int. Conf. Distrib., Ambient, Pervasive Interact.* Cham, Switzerland: Springer, 2018, pp. 21–34.

[99] B. Choi, J.-Y. Sohn, D.-J. Han, and J. Moon, ''Scalable network-coded PBFT consensus algorithm,'' in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 857–861.

[100] N. Weston, J. Willard, and P. Wang, ''Performance of blockchain technology on DoD tactical networks,'' *Proc. SPIE*, vol. 11013, May 2019, Art. no. 110130O.

[101] G. Liu, H. Dong, Z. Yan, X. Zhou, and S. Shimizu, ''B4SDC: A blockchain system for security data collection in MANETs,'' *IEEE Trans. Big Data*, early access, Mar. 17, 2020, doi: 10.1109/TBDATA.2020.2981438.

[102] W. Feng, Y. Li, X. Yang, Z. Yan, and L. Chen, ''Blockchain-based data transmission control for tactical data link,'' *Digit. Commun. Netw.*, vol. 7, no. 3, pp. 285–294, Aug. 2021.

**SUHYEON LEE** (Member, IEEE) received the B.S. degree in cyber defense from Korea University, Seoul, South Korea, in 2016, where he is currently pursuing the Ph. D. degree with the School of Cybersecurity. He is currently working with the Korea Ministry of National Defense in the cybersecurity area. Before the current work, he has three years of research and development experience with the Agency for Defense Development (ADD) as a Researcher. His current research interests include model-driven security, network security, cyber defense, and blockchain.

**SEUNGJOO KIM** (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in information engineering from Sungkyunkwan University, South Korea, in 1994, 1996, and 1999, respectively. Since 2011, he has been a Professor with the School of Cybersecurity, Korea University. For the past seven years, he was an Associate Professor at Sungkyunkwan University and has five years of back ground of the Team Leader of the Cryptographic Technology Team and also IT Security Evaluation Team of the Korea Internet and Security Agency (KISA). In addition to being a Professor, he is positioning the Head of the Security Assessment and Engineering (SANE) Laboratory, an Adviser of undergraduate hacking club CyKor, and the Founder/Advisory Director of an international security and hacking conference SECUINSIDE. Since 2018, he has been a Review Board Member of Black Hat Asia. His main research interests include trustworthy system development methodology, such as secure SDLC, RMF, Common Criteria, CMVP, and blockchain.