A study of blockchain technology development and military application prospects

Y Zhu¹, X Zhang¹, Zh Y Ju¹,² and Ch Ch Wang¹

¹Beijing Institute of Special Electromechanical Technology, Beijing 100012, China
²School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China

Email: zhuying_0001@sina.com

Abstract. Once blockchain technology is successfully applied, it will certainly trigger revolutionary changes in the military development and combat mode, which are beyond the traditional military command and management scope. In the future, blockchain technology, by combining with military artificial intelligence, Internet of things, cloud computing and big data, will have priority to be applied in military management, support, security and even command. It is of great significance to excavate the military application potential of blockchain technology and scientifically predict its impact and influence on the military field, so as to improve the combat effectiveness of the army and promote its transformation and development.

1. Introduction
During the 18th collective study of the Political Bureau of the Central Committee held on October 24, 2019, President Xi Jinping noted that, “We must take the blockchain as an important breakthrough for independent innovation of core technologies, clarify the main direction, increase investment, focus on a number of key core technologies, and accelerate the development of blockchain technology and industrial innovation.” Following this on October 31, the 4th Plenary Session of the 19th Central Committee of the Communist Party of China (CPC) adopted the CPC Central Committee’s Decision on Some Major Issues Concerning Upholding and Improving the System of Socialism with Chinese Characteristics and Advancing the Modernization of China’s System and Capacity for Governance, which for the first time included data as an equal factor of production to labor, capital, land, knowledge, technology, and management in terms of allocation. This epoch-making decision well signals that China has made fundamental system preparations for digital economy, and blockchain technology would be one of the core technologies in promoting effective system implementation, and safeguarding justice and equality of China’s basic allocation mode. The integrated application of blockchain technology will play a pivotal role in the upcoming technological innovation and industrial revolution.

2. Overview of the blockchain technology
As its scale and openness continuously enhances, the Internet has already experienced the transition from Web1.0 to Web2.0. Represented by social networks, the Web2.0-based Internet is also an “internet of information”, which greatly advances the efficiency of information flow among businesses
and individuals, and enables effective information delivery among people. Nevertheless, under the limitation of Internet’s operating mechanism, information remains replicable, easy-to-tamper and hard-to-trace. Only through centralized third-party intermediaries could we ensure the relative reliability of data. Furthermore, as Internet application continues to extend, its inherent problems of value concentration, privacy leakage, data unreliability and interest distribution inequality seems to have become ever more prominent. Therefore, the distributed, intelligent and personalized Web3.0 is expected to lead the trend of Internet development (See Table 1 for a comparison of Web1.0, Web2.0 and Web3.0).

The blockchain technology is born out of the actual demands generated by Internet development. It is capable of offering direct technical support to artificial intelligence (AI) application as well as decentralized networks with supernodes, thus promoting the Internet to develop from single-way data transmission to joint construction, and then integrated growth involving multiple parties.

**Table 1. Comparison of Web1.0, Web2.0 and Web3.0.**

| Type            | Web1.0     | Web2.0     | Web3.0                     |
|-----------------|------------|------------|----------------------------|
| Transfer of files | Read only  | Read & Edit| Read & Edit & Execute      |
| Type of networks | Simple network | Social network | Semantic network          |
| User capacity   | Million    | Billion    | Trillion                   |
| Websites        | Static     | Dynamic    | Intelligent                |
| AI              | Non-applicable | Non-applicable | Applicable                 |
| Contents        | Experts-designed | Social network-based | Personalized information flow |
| Search engines  | Domain names | Search engine optimized | AI-based                  |
| Centralization  | Centralized | Centralized | Distributed                |
| Purpose         | Connect information | Connect users | Connect knowledge          |

2.1. **Development history and technical attributes**

Blockchain, also called distributed ledger technology, is a kind of user community-managed ledger technology that ensures transmission and access security with cryptography, enables consistent data storage, and prevents from any attempt to alter data or commit repudiation. A typical blockchain uses the chained block structure to verify and store data, avails the distributed node consensus mechanism to generate and update data, adopts smart contracts consisting of automated scripts to program and process data, and as mentioned above, ensures data transmission and access security with cryptography.

2.1.1. **Development history.** As a new type of computing paradigm and solution establishing a trust mechanism in an incredible and competitive online environment with low costs, blockchain is now changing the application scenarios and operating rules of various industries. In this sense, it is one of the indispensable technologies for the development of digital economy and the construction of a new trust system. Since its birth in 2008, the technology has upgraded from Blockchain1.0 to Blockchain2.0 and now Blockchain 3.0.

(1) Blockchain1.0: Digital currency
The creation of Bitcoin marks the inception of the era of Blockchain1.0. Bitcoin offers a solution to the double-spending flaw of digital currencies, and introduces a real-sense digital currency by way of blockchain-based distributed recording and storage, which is epoch-making.

Blockchain1.0 is mainly applied in areas closely related with digital currency, such as currency transfer, exchanges and payment. With Blockchain1.0, a chain structure of block units is established, which helps ensure the authenticity of ledger-contained information by sharing the ledger among all blocks, and verify information authenticity with asymmetric encryption algorithm and open source code, thus solving the problem of both currency-based payment and decentralized payment. In general, this generation of blockchain is characterized by such technical features of decentralization, anti-tampering, collective maintenance, traceability and security.

(2) Blockchain2.0: Smart contracts

At the initial stage of Blockchain1.0 design, only transaction attributes of a digital currency were taken into account. Therefore, Blockchain1.0 could only support the running of some simple sets of instructions under many a limitations. To address the problem, Blockchain2.0 emerged at a right moment. Closely related with the development of contract technologies, Blockchain2.0 was the most typically applied in Ethereum. Then, blockchain technologies started to be applied in various industries.

Ethereum is an open source blockchain-based underlying system capable of operating all blockchains and contracts, and supporting the rapid development of diversified blockchain applications. Specifically, smart contracts represent one of the most distinctive features of Ethereum. Smart contracts, as the fundamental technology of programmable currency and programmable finance, can store and transfer value in a highly effective way. Blockchain constructs a reliable environment for smart contract execution; and in turn, smart contracts support blockchain application expansion. The in-depth application of Blockchain2.0 has brought the technology well beyond the area of currencies with programmable characteristics. Currently, the development of Blockchain2.0 is still at an early stage, and scale application is yet to realize.

(3) Blockchain3.0: Comprehensive application

Blockchain3.0 will introduce an era of comprehensive blockchain technology application, in which the blockchain technology will evolve from the “Decentralized Application (DApp)” to “Decentralized Autonomous Corporation (DAC), then “Decentralized Autonomous Organization (DAO), and finally “Decentralized Autonomous Society (DAS).” At present, the blockchain operating system EOS is a typical infrastructure project under development. In the future, Blockchain3.0 will be widely adopted in industries including healthcare, the Internet of Things (IoT), sharing economy and so on. Capable of performing ownership recognition, measurement and storage of data on the Internet, Blockchain3.0 will make asset traceability, controllability and tradability along the blockchain a reality and ultimately ushers in a “programmable society” for all.

2.1.2. Technical attributes. In circumstances of information asymmetry, blockchain saves the effort of presenting mutually guaranteed trust or verified credibility certificates by a third party. Instead, based on the node trust mechanism created by big data-supported encryption algorithms, blockchain enables intelligently-built trust as well as value enhancement for all parties. The main attributes are as follows:

(1) Decentralized/Weakly centralized

Blockchain is a distributed data storage structure without centralized nodes. Each and every node along the chain stores totally the same information; and the verification, accounting, storage, maintenance and transmission of all blockchain data are all based on the distributed systematic structure. The structure adopts purely mathematical methods instead of central institutions to establish trust relationships among distributed nodes, so that in cases of information asymmetry, a decentralized and trusted distributed system could be formed. In special application scenarios, it can also flexibly adopt weakly centralized management nodes.

(2) Tamper-proof and traceable
Once the data is submitted, it will be permanent and cannot be destroyed or modified. The blockchain uses a chained block structure with time stamps to store data, thereby adding a time dimension to data, hence the strong verifiability and traceability.

(3) Transparent and trust-free
The operating rules of the blockchain technology and the data information carried in blockchains are transparent, and no identity verification is necessary among the nodes. In this way, both fraud risks and intermediary costs could be reduced, and trusted data transmission could be achieved in an untrusted network.

(4) Collectively maintained
The blockchain uses a specific economic incentive mechanism to ensure that all nodes in the distributed system participate in the verification process of data blocks (such as in the “mining” process of Bitcoin), and relies on a consensus mechanism to select specific nodes for the adding of new blocks into the chain, which gives the blockchain technology the property of self-maintenance and thus reduces network operation and maintenance costs.

(5) Programmable
The blockchain technology can provide a flexible script code system that supports users to create advanced smart contracts, currencies, or other decentralized applications, empowers the blockchain technology to be tightly integrated with existing technologies and then applied in various scenarios. For example, the Ethereum platform has provided complete scripting languages for users to build any smart contract or transaction type that can be precisely defined.

(6) Security enhanced
The blockchain technology uses asymmetric cryptography to encrypt data. At the same time, it avails consensus mechanisms such as the proof-of-work (PoW) consensus for each node in the distributed system to form a strong computing power to resist external attacks, and prevent data from tampering and forgery. Compared with traditional security methods, it boasts a naturally higher security and indestructibility.

2.1.3. Key technologies. Blockchain technology is a combination of a series of existing technologies, including distributed network, cryptographic technology, proof of work (a consensus mechanism), Byzantine fault tolerance protocol (an agreement that guarantees the consistency and activity of distributed systems even if there are malicious nodes), etc. These technologies have undergone more than ten years or even decades of development and evolution. Aside from a combination of existing technologies, new technologies have been integrated and innovation has been continuously conducted. The key technologies involved are mainly as follows:

1) Block + chain: This is a basic structure for data recording. The block is composed of a block header and a block body. The block body is responsible for recording data of the previous period, mainly quantity and details; and the data relies on asymmetric encryption to ensure information security and authenticity. The block header encapsulates the current version number, the former block’s address, the time stamp, the random number, the target hash value of the current block (with a certain hash algorithm, a long piece of data can be mapped shorter; and this short piece of data, or small data, is the hash value of the big data, which changes along with changes of the big data), as well as the root value of Merkle tree (a hash binary tree often used for rapid data inquiry in the field of computer science). Based on the hash of the previous block recorded in the current block, the blocks can form into an immutable blockchain.

2) Point-to-point communication: The blockchain uses a peer-to-peer (P2P) network network for communication, making each user in the network not only a node, but a server. The resources and services in the network are scattered on all the nodes; and the transmission of information and the realization of services are performed directly between the nodes without any intermediary participation or server intervention.

3) Consensus mechanism: In the peer-to-peer network, since each node has the right to package data and generate new blocks, in order for all nodes to agree on the newly generated blocks in the
blockchain, and ensure consistency of the node-recording blocks across the network, the blockchain network sets up a consensus mechanism. In the light of the mechanism, any node in the network can produce new blocks, only provided that the new block meets pre-set requirements of the consensus mechanism (Proof of Work [PoW], the mechanism of Proof of Stake [PoS], the mechanism of Delegated Proof of Stake [DPoS], the Raft protocol, as well as the Byzantine Fault Tolerance Algorithm (Practical Byzantine Fault-Tolerant, PBFT), that is, to be recognized by all nodes in the entire network and added to the shared blockchain with independent storage.

(4) Smart contract: It is a set of procedural rules and logics realized through decentralized, trusted, and shared script codes deployed on the blockchain. Generally, smart contracts are signed by relevant parties, and then attached to blockchain data in the form of program codes. They are then recorded into specific blocks in the blockchain after P2P network transmission and node verification. Smart contracts encapsulate a number of predefined states and transition rules, scenarios that could trigger contract execution, and response actions in specific scenarios. The blockchain can monitor the status of smart contracts in real time, and activate and execute the contract after checking external data sources and confirming that certain trigger conditions are met. Smart contracts can ensure traceability, irreversibility and transaction security in the absence of third parties.

2.2. Relationship between blockchain technology and AI, big data and other frontier technologies
The development and application of the blockchain technology would not be possible without the infrastructure support of next-generation information technologies such as AI, big data, cloud computing, and IoT. In turn, the blockchain technology has also promoted the advancement of these information technologies.

2.2.1. Blockchain + AI. AI and blockchain are expected to complement each other with respective advantages.

(1) AI can help solve the problems faced by blockchain in terms of autonomy, effectiveness, energy efficiency and intelligence, especially data credibility in AI applications, so that AI can focus more on algorithms. Furthermore, AI is capable of managing the autonomous organization of blockchain in a more effective manner, extending and improving the function and efficiency of smart contracts, as well as optimizing blockchain operation for greater security, effectiveness and energy efficiency.

(2) Blockchain can bring along distributed AI, realize the mutual call of diversified AI functions, accelerate AI development, break the currently closed development mode, and promote data sharing. Additionally, blockchain can also be used for audit trail data models, thus providing more reliable forecasts, etc.

2.2.2. Blockchain + Big data. The introduction of the blockchain technology has provided solutions to several problems in an open network environment, such as data opening, data sharing, low-quality data, and data leakage.

(1) The decentralized, open and autonomous nature of the blockchain helps remove data islands in an effective way, transfer information to all participants openly and transparently, and improve data risk control through information sharing.

(2) The openness, transparency, and security of the blockchain ameliorates quality of big data, and tackles such problems as diversified data formats, fragmented data forms, valid data deficiency, and data content incompleteness, thus fundamentally improving data quality and enhancing data verification capabilities.

(3) Boasting collective maintenance and enhanced security, the blockchain effectively prevents from data leakage. The blockchain database is a decentralized database, where any operation on data will be noticed by the other nodes, hence intensified monitoring on data leakage. Besides, the blockchain encrypts stored information to ensure data security. Any external attack on the blockchain would not be possible without having over 50% computing power of the blockchain. When the
number of nodes reaches a certain scale, the cost of attack would also be enormous, making the attack hard to realize. In this sense, the problem of data leakage will be solved effectively.

2.2.3. **Blockchain + Internet of things (IoT).** (1) The cost of IoT operation and maintenance is reduced significantly. With the blockchain technology, the IoT can transfer data through point-to-point direct interconnection without relying on any central processors. Distributed computing can be used to process hundreds of millions of transactions. What’s more, the computing power, storage capacity, and bandwidth of hundreds of millions of idle equipments will greatly reduce computing and storage costs.

(2) No third-party verification is required. The blockchain technology can help solve problems of scalability, single-point failure, time stamping, recording, privacy, trust, and reliability in a completely consistent manner. Under the fully decentralized trusted digital infrastructure, the IoT equipments can run independently without the need of receiving any centralized authorization.

(3) IoT security is guaranteed. Blockchain can record all behaviors of terminal devices. Since the information recorded can never be rewritten, data security and user privacy will be put under effective protection.

2.2.4. **Blockchain + Cloud computing.** Cloud computing services are characterized by large scale, high reliability, low cost, flexibility, and on-demand delivery. Combined with the decentralization and data tamper-proof characteristics of the blockchain, it has the potential of promoting widespread application of blockchain technology. In the future, based on infrastructure and services (IaaS), platform as a service (PaaS), and software as a service (SaaS), blockchain as a service (BaaS) will be created to integrate the blockchain technology framework into cloud computing platforms and build a cloud service market of BaaS, thus providing stable and reliable cloud computing platforms for decentralized applications.

3. **Military application prospects of blockchain technology**

3.1. **Military command**

The command information system is an important method and equipment to realize real-time, accurate and automatic battlefield command at war and help headquarters at all levels to implement scientific and efficient management of subordinate units and weapons at ordinary times. As an organic “human-machine” system, taking commanders as the core, and computers, and using computers and other information technology equipments as the prerequisite and material guarantee, the system organically combines various command-and-control methods and commanders to enable high-level automation in the collection, transmission, processing and usage of military command information. In this way, it ensures data integrity, availability, and security of the command information system, and basically guarantees the enhancement of combat effectiveness and the success in seizing initiatives in the war.

3.1.1. **Blockchain+Command information system.** Military requirements: First, the command information system has centralized networks and database. As an important target in wartime and even peacetime, it is vulnerable in front of enemies or hackers. They may use a variety of information means to conduct network and electrical attacks, causing the entire information system to paralyze, or to steal and falsify identity information, tampering with important data. Therefore, combatants face great risks in data authenticity, and even may make erroneous decisions with malicious data. Second, when the commanders rely on the command information system to make decisions, there will be risks of giving wrong commands or fake orders caused by the enemy’s tampering with data.

Technical principle: The command information system based on blockchain technology can be divided into data layer, network layer, consensus layer, incentive layer, contract layer and application layer. Among them, the data layer guarantees the data or intelligence reliability, credibility and security of military information system; the network layer guarantees self-organizing and
decentralized features of military information systems; the consensus layer encapsulates various types of consensus algorithms to achieve autonomous and credible decision-making; the incentive layer uses a programmable incentive mechanism to avoid all kinds of misbehaviors and achieve positive behavior incentives; the contract layer helps automate and intelligentize military information systems, reducing the uncertainty, diversity and complexity that human and other factors bring to battle command and military management.

Solution: Taking advantage of the decentralized and distributed features, consensus mechanism, autonomous characteristics and asymmetric encryption algorithm credit mechanism of the blockchain technology, we can establish an automatic and secure command and control system. By combining it with artificial intelligence and military IoT in the future, we can first change the combat control at the tactical level from a centralized mode to a decentralized mode. Credible combat command can also be achieved, which means that, command issued by commanders at all levels can be recorded completely, with rewritten data being evidencable and traceable. Only when the enemy or hackers modify more than 51% of the node information at the same time can the command information system data possibly be altered.

Thanks to time series data, collective maintenance, programmable and reliable features of the blockchain technology, the dynamic and permanent recording can be realized in networks or databases, and the false information and hacking can be effectively prevented. Thus, we can monitor in real time whether the database has been tampered with or whether the military system has been monitored, and eliminate the risk of enemy attacks inherent in command information systems.

Typical case: DARPA is trying to develop a secure and reliable information platform based on the blockchain technology. It would be a secure information service system capable of effectively protecting sensitive data and preventing from hacking.

3.1.2. Blockchain + UAV cluster operations. Military requirements: UAV cluster systems have five typical characteristics, namely decentralization, autonomous control, cluster recovery, function amplification and zero casualties. However, the current UAVs in the clusters lack overall perception of the external environment, and there is a lack of effective information sharing and action coordination among individual UAVs and UAV formations.

Solution: Using the consensus mechanism of blockchain technology, we can transform from personal trust and institutional trust to machine trust. In the future battlefield, the UAV cluster command and control system will share combat command data in a decentralized manner and thus unify operations. The ability of maintaining combat capability under any casualties is of great significance for the realization of a new “human-machine / machine-machine” command and control mode that matches unmanned operations.

The first is about security. Through the “public and private key encryption and decryption” and “digital signature” function of the blockchain technology, each UAV in the cluster can serve as a network node. All nodes share and maintain the same ledger, ensure the authenticity of communication data, and verify the identity of cluster members.

The second involves distributed decision-making. Distributed decision-making algorithm is the key to the effective work of UAV cluster systems, and the consensus mechanism ensures that all nodes in a distributed system agree on the objective of making decisions. In real combat, each entity in the cluster must agree on operational tasks and objectives such as grouping and formatting, path planning, and barrier avoidance.

The third is for formation control. The sidechain technology of blockchain allows multiple blockchains to be connected to each other in a hierarchical manner. On the one hand, UAVs on different chains can act according to the protocol preset on the chain where they are located; on the other hand, inter-chain collaboration makes it easier to switch among diverse cluster formations. In the process of coordinated search, reconnaissance and attack, the UAV cluster can change formations to protect itself and kill enemy.
The fourth is about decentralized autonomous cluster. In the future, each entity in the UAV cluster can be regarded as an autonomous agent with the function of perception, reasoning and decision-making. These agents will form various decentralized autonomous clusters through smart contracts to execute optimal decisions in an autonomous way.

3.2. Military management
The traditional military management structure is a top-down “command and control” system, which brings along such problems as bloated institutions, high management costs, unclear definition of responsibilities, inefficient management, redundant management, poor information transmission, and power concentrating at the top level while the lower levels having very limited autonomy and thus limited innovation potential.

3.2.1. Blockchain + Lifetime weapon management. Military requirements: Modern warfare requires the combat system to have better responsiveness and agility, but institutions featuring hierarchical management operate inefficiently. There is a large number of data to be recorded such as design plans, test results, and combat technology status during the whole lifecycle of weapons, from project demonstration, development, production, delivery to service to retirement. Information is easy to be lost or tampered with in the process.

Solution: Based on blockchain technology, we can build a lifecycle weapon and equipment management system jointly operated and mutually supervised by developers, producers and users. With the system, we can track and manage equipment design parameters, test data, combat technology status and maintenance records. No content can be manipulated or deleted, which improves information security, convenience and credibility. All management actions will rely on smart contracts for open and transparent decisions, reducing management hierarchy, forming a flat management mode, and finally improving efficiency. At the same time, every component of the weapons and equipment can be traced to the origin, which helps resolve disputes over procurement contracts, and constructs a complete unbreakable monitoring, management and control system, thus improving management security, convenience and credibility.

3.2.2. Blockchain + Sensitive data management. Using the “untamperable” feature of blockchain technology, we can provide a solution to the problem of “hard to maintain evidence” in sensitive data management in military inspection and supervision, human resources and medical and healthcare. “Truthful record” of all information can be realized through “whole-network witness”, thus avoiding document counterfeits, file missing and information tampering.

3.3. Military logistics.
Military requirements: It is difficult to solve problems related to networking, data storage, system maintenance, traceability and quality control during packaging, loading and unloading, transportation, and disassembly in military logistics.

Solution: By using blockchain technology, we can create a separated, secure, shared and permanent auditable record, track and audit transactions of various supply chains and among all operating partners, and perform effective lifecycle management on defense supply chain and the system of procurement and logistics.

By incorporating the blockchain technology into the military logistics network, we can build a decentralized autonomous network of personnel and materials in logistics systems. Data related to the production, procurement, transportation and distribution of materials in the systems can be stored in various blocks in a unified manner, which can greatly improve the security of military logistics information, and enable the military logistics equipment and energy to meet requirements of various services and departments, hence always in the best condition.

Modern military logistics involves intelligent warehousing, packaging, transportation and distribution. The different processes form into a small military IoT based on the dynamic autonomous
network of people and objects. By using the nodes, we can communicate directly or through relays to manage important data in the military logistics chain such as user needs, stored goods, loading, transportation, and distribution and transit. The maintenance of the blockchain will be supervised by all nodes across the network, and the illegal operation of some individual nodes will be rejected and resisted by most nodes. In this way, the security and convenience of transactions will be enhanced, and the time consumed by intelligent military logistics will be reduced. It can also help solve problems related to networking, communications, data storage, and system maintenance during packaging, loading, unloading, transportation and disassembly in military logistics, thus ensuring orderly and efficient system operation. This is considered to be the most promising military application of the blockchain.

Typical case: In April 2016, the U.S. Department of Defense and its NATO allies began to pay attention to the potential application of blockchain technology in defense, including automatic execution of smart contracts, secure storage of sensitive files, and reduction of errors and interruptions during defense contract execution. Furthermore, the blockchain technology can also be applied to emergency response when disasters occur, and improving the transparency of raw material procurement on the supply chain and barge transport in the logistics process.

In June 2017, the U.S. Navy availed the blockchain technology to improve the security of additive manufacturing systems. They recorded the entire process of component design, prototype manufacturing, testing, production and final processing, so that users could look into any specific data, and give alerts in cases of component damage or at the end of its lifecycle.

3.4. Military security

3.4.1. Quantum blockchain. Military requirements: Security of battlefield data transmission must be ensured, and problems of signal interception, deciphering and reconnaissance need to be solved.

Solution: By using quantum key distribution as a replacement of the original private key structure, and tapping into the anti-eavesdropping and anti-interception features of quantum cryptography in the blockchain network, we can greatly improve the defense ability of blockchain network, and exert disruptive influences on the problem of signal interception, deciphering and detection.

Typical case: The Russian Quantum Center and Russian Academy of Sciences successfully tested the first quantum blockchain system.

3.4.2. Blockchain + Resilient communication. Military requirements: The security of battlefield data transmission must be ensured.

Solution: Based on the distributed characteristics of the blockchain technology, a wide-coverage, disaster-resilient, and high-secure communication system can be constructed to achieve secure and resilient communication in a complex battlefield environment.

Typical case: In May 2017, the Indiana-based Technology and Manufacturing Company, funded by DARPA, used the blockchain technology to develop an “inaccessible messaging and trading platform” for the military. This platform separates information creation and information transmission to ensure the data sent and received cannot be cracked, and enable secure communication between the headquarters and ground forces, as well as between the Department of Defense and intelligence officials. In July 2019, as part of the DOD digital modernization strategy, DARPA began to leverage the blockchain technology to build a more efficient, powerful, and secure communication platform, in order to facilitate secure information transmission for any command, control and communication systems, allow the staff to track transactions through a distributed ledger channel, and guarantee communication security between the headquarters and ground forces, and between the Department of Defense and intelligence officials in the future.
4. The bottleneck of blockchain technology application in military

To some extent, blockchain is a new type of information technology that sacrifices storage space, access speed, and overall efficiency for data security and trust. It is mainly suitable for military application scenarios featuring low frequency of usage, high security requirements, low timeliness, and small amount of data. Its limitations and risks are mainly reflected in the following areas:

First, high redundancy and huge energy consumption makes it difficult to meet the requirements for light weight and expansion. Every node of the blockchain must synchronize all ledger data in real time, and duplicate data will be stored in each block. As the amount of data increases and new nodes are added in, the system will be more redundant, thus requiring more storage resources. This requires combat units or platform terminals to have great capacity in storage, computing and communication, which is inconsistent with the trend of light weight and miniaturization of equipment. As the number of nodes increases, the computing power, bandwidth and energy consumed by each node in data synchronization will also increase. With a larger number of nodes, the requirement for storage capacity for subsequent new nodes will be higher; the difficulty of accessing will augment; the time needed for synchronizing will increase; and the efficiency of overall operation will further decrease, all of which will hamper the large-scale and on-demand expansion of the combat system.

Second, it is hard to satisfy high-frequency rapid response requirements with a complex data synchronization mechanism. Every data modification in the blockchain requires all nodes in the system to update ledger data synchronously, which takes a long time. If the operation is too frequent within a short period of time, a lot of bandwidth will be consumed, hence the potential network congestion. Modern warfare has entered the era of “second kill”, especially at tactical and platform levels. This means that, situational information updates grow faster, and combat units and platform send information assistance applications at higher frequencies. It is hard for the blockchain technology to meet these real-time response requirements.

Third, the consensus mechanism and encryption algorithm still have security risks. The security of the blockchain technology consensus mechanism depends on the cryptographic algorithm. The cryptographic algorithm is not absolutely secure and there are still risks to be cracked. For example, the elliptic-curve-based cryptographic algorithm is widely used in blockchain. Although it is very difficult to crack with classic computers, the task is rather easy for quantum computers. At present, world powers are stepping up efforts to make breakthroughs in quantum computing technology. Once a reliable and practical quantum computer is developed, most blockchain technologies today will lose security guarantees.

Fourth, the small scale of the military blockchain reduces system security. From the perspective of the principle of blockchain technology, unless attackers modify more than 51% of the nodes at the same time, they would not be able to tamper with data contained in the blockchain. Therefore, the more nodes there are, the more difficult it is for an attacker to alter data. For blockchains used in military, the number of nodes is usually much smaller than that the number of nodes contained in Internet-based civil systems. During wartime, in the face of large-scale network attacks launched by the enemy with enormous computing power, it is still possible to modify more than half of the nodes and tamper with the data.

Fifth, the gaming of military blockchain nodes gives rise to problems in the incentive mechanism. Since the blockchain network is a decentralized distributed system, the game relationship featuring both competition and cooperation among nodes is inevitable in the interaction process. The design of a consensus mechanism compatible with military incentives has become a key issue for any military blockchain before it can turn practical. After all, only a well-designed consensus mechanism can enable the nodes in a decentralized system to simultaneously perform data verification and ledging, increase the cost of committing inappropriate behaviors in the system, and thus hindering attacks on and threats to security.

References

[1] Drescher D. 2018 Blockchain basics: a non-technical introduction in 25 steps. Posts & Telecom
Tapscott D. 2016 *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. China CITIC Press

Huang LJ, Wu SJ, and Cao F, et al. 2018 Blockchain Security Technology Guide. China Machine Press

Jing DWT, Wu YW, and Zhao GD, et al. 2017 *Block Chain and Big Data*. Posts & Telecom Press

Lian L, Zhu QC, and Zhao Z. 2016 *National Defense Science & Technology* 2 30-4

Sun Y, Lei Z, and Cui PZ. 2017 *China Computer & Communication* 19 142-4

Sun Y, Lei Z, and Zhan GY. 2018 *Journal of Command and Control* 4(03) 17-22

Yu MY, Yang CY, and Liu J, et al. 2018 *Logistics Sci-Tech*. 41(10) 144-6

Liu N, and He W. 2019 *National Defense* 395(01) 32-5

Lian L, and Zhu QC. 2019 Decoding military applications of blockchain technology. PLA Daily