A survey on military Applications of Blockchain Technology

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.

I. INTRODUCTION Blockchain technology (BCT) is one of the much-discussed technological advancements like AI and quantum technology. Its significance rose exponentially with its extensive usage in the financial sector. Bitcoin, Ethereum, are some of the virtual currencies which have become household names for all virtual currency enthusiasts. However, this technology has its applications spread out into the military. In general, this technology is about organizing and storing information in the most secure and trustable way with complex mathematical logic. For the military, BCT based systems provide secure and trustful communications, defence inventory management, tracking of the defence equipment imports etc. Going with its general applications, in the military space, BCT is wished to be used in the documentation, supply chain, logistics. Though they appear to be simple and easy applications to be adopted, they can increase the efficiency in the defence services and also in the budget spending. BCT application has become a common aspiration for militaries across the world. For India, its implementation has a bit more advantage compared to others. Here is one area to understand why it is more important. India has seen numerous scams (proved and alleged) anchored to military imports.

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.

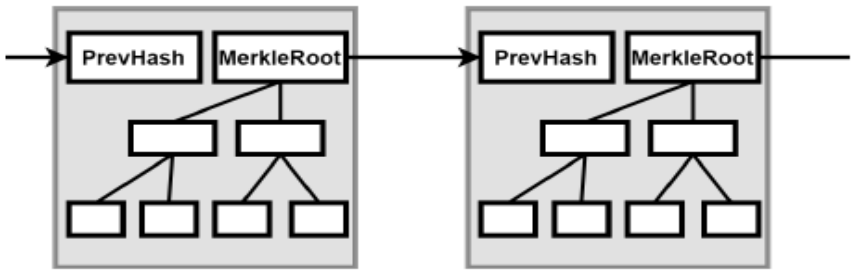

FIGURE 1. Bitcoin data structure.

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.

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.

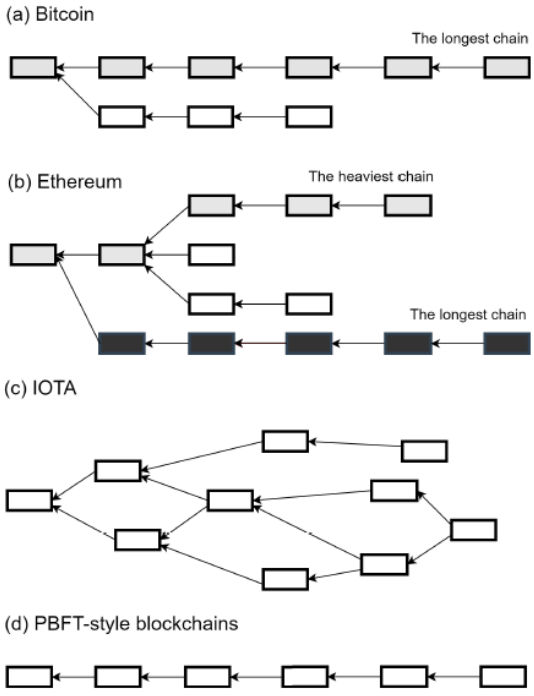

FIGURE 2. Hash chain structures.

Each block is singly linked, but there can be a fork, which means that more than one blockwould 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.

Blockchain does not use only the same data structure which is used by Bitcoin. Ethereum'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 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 networkcontrols 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), Proofof-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. 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. Blockchain applications in military

Blockchain would be particularly useful in defence. This technology has several advantages that stem from its decentralized nature. Firstly, the distributed structure of the blockchain ensures its availability. It also makes this technology less expensive. Secondly, its resilience, security and immutability are particularly useful to store the data and are a strong asset for many military applications. we have surveyed some of the applications in this section.

A. Blockchain as 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 in_ltrate 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.

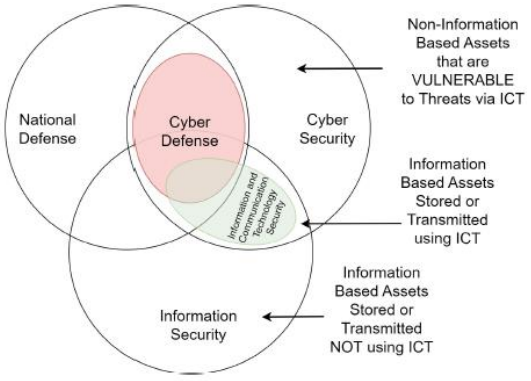

FIGURE 3. Relationship between information security, cyber security, and national defense. By adding national defense to the figure in von Solms and van Niekerk [14], cyber defense is defined.

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 defend. 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. Prehend cyber defense clearly, an accurate understanding of cyber security is key.

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

B. Smart contract management and supply chain auditing

Decentralized Smart Contract technology is emerging as an undertone of next-gen IT infrastructure. After banking and finance sector leveraging distributed ledgers to secure operations, now, other sectors are aggressive to implement this technology. One such vertical is defense and military applications. Smart contract technology in defense will revolutionize the sector. Top agencies including DARPA, and US Navy have caught the bandwagon. Not only in the US, this technology is also gaining global grounds. NATO is also ready to invest on it. Defense and military sector has integrated IT as a salient tool with advances in drones, smart weapon systems, and active monitoring.

Smart Contract technologies like blockchain impacted several aspects of military and defense. Real-time data collection using drones, decentralization of weapon control, military supply chain management can become highly optimized and effective using blockchain.

Blockchain-based smart contract technology has the potential to create a real-time supply chain in weapon administration. Blockchain is gaining a rapid adoption in governance, which can replicate in supply-chain management in the military as well. Distributed ledgers can let all roles in the chain to implement their parts in tandem with other stakeholders in real-time. Such chain will effectively work during an emergency period. Such decentralized networks will connect each weapon on the grid to administrations. This will augment the process of servicing and maintenance of high-tech weapons. Suppliers in the chain will know the requirement to replace any damaged part or machine in the weaponry on real-time. Thus, military logistics, procurement, and supply operations will enhance using decentralized applications.

Decentralized ledgers and smart contracts are emerging technologies. Blockchain-based technology has the potential to create innumerable innovative applications for defense, military, and security. SaaS Development, web-based applications are now pertinent in this industry. These systems will enhance dynamically with decentralization. Distributed ledgers are foolproof, immutable and uncollapsible, which make them apposite for military applications.

C. Enabling Drones in the Internet of Things with Decentralized Blockchain-based Security In recent years, drone technology has emerged as key aerial machinery with a wide range of

industrial, environmental, safety, and military applications. Some examples include surveillance, search and rescue operations, aerial photography, and disaster monitoring. The use of drones and drone technology will undoubtedly rise in our modern cyber run society. As is pertinent in current literature, drones have a considerable amount of benefits that can be realized for the human race. They enable us as a race to do things that are nearly impossible to do in remote parts of the physical world. From a more technical standpoint, the design and implementation of drone network models have challenges. These challenges mainly come from running a multitude of topologies and unstable connection issues. In particular, though, both drone movement and insufficient security may result in several problems that are yet to come into fruition. These include unauthorized access, excessive latency, and high energy usage in the drone's network. Moreover, there is widespread concern regarding using drones in the growing number of Internet of Things (IoT) enabled smart cities. One of the most important issues in smart cities nowadays is the issue of authentication of drones during flight. The conventional question arises here, whether all drones should be allowed to fly all over a given smart city or into particular zones. There is ongoing contention as to how moderators of drones as well as smart cities can respond to this question. Many people are of the opinion that only trusted drones should be allowed to fly airborne due to the fact that unauthorized drones can violate privacy and impose risks. To tackle this issue, the need for a secure drone network in each zone of the smart city is imperative. Most commercial drone-assisted application's require a low latency authentication mechanism with high security. Since preserving the quality of service and removing the effect of parameters may influence drones' authentication mechanism, we should have an efficient approach in drone networks that can handle time-sensitive tasks in a nearly real-time manner. Indeed, in some drone-based applications, the issue of latency is crucial. Take as an example using drones to monitor disasters, where any latency may be the difference between life and death. We can build a secure low latency authentication scheme for drones using blockchain-based security in a smart city that is suitable for networks of drones. Our approach is built upon blockchain technology through the creation of decentralized authentication using a zone-based architecture in a smart city which can be beneficial in a multitude of ways . a public blockchain can be applied so that all drones can have the ability to register to fly (become authorized) by authenticating on the blockchain. Drones in a given smart city are connected through P2P networks using a shared ledger. All connected drones can migrate to other city's zones through their disseminated identity quickly. In fact, we consider several zones which cover the specific area in each city. The movement of any drone that is already authenticated on the network from one zone to another zone will not require re-authentication of that drone to occur again. The cluster based approach originally proposed in is followed in our proposed zone architecture. Like a cluster-head in each cluster, we consider a drone controller in each zone of a smart city. The drone controller plays a management role in the authentication mechanism for drones and handles all operations that are related to the blockchain. This characteristic by itself has a significant influence on maximizing security and minimizing the time required for the authentication of drones.

D. Securing Internet of Things (IoT) by blockchain

Internet of Things (IoT) technology is emerging to advance the modern defense and warfare applications because the battlefield things, such as combat equipment, warfighters, and vehicles, can sense and disseminate information from the battlefield to enable real-time decision making on military operations and enhance autonomy in the battlefield. Since this Internet-of- Battlefield Things (IoBT) environment is highly heterogeneous in terms of devices, network standards, platforms, connectivity, and so on, it introduces trust, security, and privacy challenges when battlefield entities exchange information with each other. Blockchain as a distributed ledger system provides many needed features and functionalities needed for cyber operations, such as, auditability of historical information, assurance of data provenance, guaranteed variability of integrity violations of historical data, and information tampering detection. Besides, Blockchain has both cost effectiveness merits, as well as transparency features, making it an appealing system for military cyber operations as described in the following cases. Generation of cyber assets - Blockchain can be used to generate cyber assets that will enable applications which rely on direct interaction between customers and assets. The Blockchain system can aid in ensuring the issuance processes, transaction processing, and housing of cyber assets/identities. Transfer of ownership of cyber assets - A Blockchain system allows transfer of cyber assets between owners by leveraging the immutability property of Blockchain so that once a transaction is committed, it cannot be reversed. Any changes will have to be appended and will not alter an already validated transaction, thereby ensuring non-reversibility of transfer of ownership. Transparent and assured data provenance - Every operation on the cyber asset is encoded in the Blockchain transaction using a publicly available and immutable ledger. The Blockchain system ensures that provenance of every operation on the cyber asset is recorded and traceable. Verifiability and audit - The distributed ledger keeps track of transactions pertaining to creation and transfer of cyber assets. The tamper-resistant property of the ledger facilitates variability and audit of operations. Military cyber operations - Ensuring traceable and tamperevident accountability and auditability of C2, logistics, and other critical mission data among international partners is paramount as our future operations involve the convergence of multiple domains and a heavily contested cyberspace. Centralized or homogenous information systems and databases must evolve distributed, disintermediated, and secure capabilities. As such, trust with respect to operations involving international entities must not be rooted in one single entity. Trust must be decentralized and built around robust, innovative cryptographic paradigms transcending the traditional Public Key Infrastructure (PKI) typically used in most homogenous enterprises. An innovative, distributed trust and identity management mechanism is a crucial for enabling assured identification, authentication, and authorization in such a way that would further allow disintermediated accountability and auditability. Emerging Blockchain and distributed ledger technologies as a whole demonstrates the potential of a truly distributed and disintermediated mechanism for achieving above needs. The current production application of cryptocurrencies using public Blockchain has already shown the potential of decentralization to allow customers to perform monetary transactions seamlessly and maintain the ledger at the same time. The nuances of disintermediated international partnerships and information exchange involve some mutually exclusive research and development challenges distinct from the permissionless and public implementations of Blockchain. Given that Blockchain can be instrumental in offering many needed security services, in the following Section, we propose a multi-layered architecture of the Blockchain-enabled IoBT and describe in detail the

individual components along with their roles.

IV.CONCLUSION

Blockchain military use cases are mostly in Command and
Control (C2) fields like Anti-hacking, intrusion detection, Battle orders management, Network and data redundancy and Digital order-of-battle verification. We explained a brief use case of it in part B. other use cases are more about Communications, mostly the security and authentication parts relate to blockchain like Encrypted communications client and Credentialled identity management. In part C we had the example of drones. The other applications are in weapon supply chains which track the weapons distribution and trackability. Blockchain can used in Professional military education and Officer and NCO career tracking too. Also it can be used in Decentralized propaganda channels for Psychological Operations.

REFERENCES

[1] S. Lee and S. Kim, "Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges," in IEEE Access, vol. 10, pp. 2602-2618, 2022, doi: 10.1109/ACCESS.2021.3136328.

[2] Lilly, Bilyana & Lilly, Sale. (2021). Weaponising Blockchain: Military Applications of Blockchain Technology in the US, China and Russia. The RUSI Journal. 1-11. 10.1080/03071847.2021.1886871.

[3] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava and M. Aledhari, "Enabling Drones in the Internet of Things With Decentralized Blockchain-Based Security," in IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6406-6415, 15 April15, 2021, doi: 10.1109/JIOT.2020.3015382.

[4] D. K. Tosh, S. Shetty, P. Foytik, L. Njilla and C. A. Kamhoua, "Blockchain-Empowered Secure Internet -of- Battlefield Things (IoBT) Architecture," MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM), 2018, pp. 593-598, doi: 10.1109/MILCOM.2018.8599758.

[5] Tosh, Deepak & Shetty, Sachin & Foytik, Peter & Njilla, Laurent & Kamhoua, Charles. (2018). Blockchain-Empowered Secure Internet -of- Battlefield Things (IoBT) Architecture. 593-598. 10.1109/MILCOM.2018.8599758.

[6] M. Golam, J. -M. Lee and D. -S. Kim, "A UAV-assisted Blockchain Based Secure Device-to-Device Communication in Internet of Military Things," 2020 International Conference on Information and Communication Technology Convergence (ICTC), 2020, pp. 1896-1898, doi: 10.1109/ICTC49870.2020.9289282.