International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Blockchain Integration in Military Organizations: Addressing Energy Efficiency, Privacy, and Scalability Challenges

Sanskruti Pasalkar[1], Pratiksha Sawant[2]

[1]Student, Department of Computer Science, PVG's College of Science & Commerce
[2]Assistant Professor, Department of Computer Science, PVG's College of Science & Commerce

Abstract
Blockchain systems ensure to change defense operations by ensuring secure communication, enhancing cybersecurity, and increasing supply chain transparency through unchangeable ledgers and decentralized systems. This kind of study identifies the gaps and research needs in energy efficiency, privacy, and scalability and investigates the integration of blockchain systems into defense organizations. To solve these research gaps, solutions are suggested like energy-efficient consensus techniques, off-chain processing, and privacy-preserving protocols. This study shows how blockchain technology is used to protect drones used in defense operations and important communication networks and improve military logistics.

Keywords: Military, Blockchain, Cyber Defense, Unmanned Aerial Vehicles (UAVs), Consensus Processes, Zero-Knowledge Proofs (ZKPs), Off-chain Processing.

1. INTRODUCTION

Background

Blockchain was originally designed for digital currencies called "bitcoin. This technology is widely used in various industries and comes with a lot of benefits. Blockchain is primarily a decentralized distributed ledger that stores transactions securely without altering or manipulating them. Blockchain has different characteristics such as decentralization, immutability, and transparency. Decentralization contains peer-to-peer networking in which the centre server or authority is absent; it helps in resisting cyberattacks and guarantees security even if some network segments are hacked. Immutability ensures that no single transaction record can alter or change once it gets recorded in the system. It can only be removed or changed by the permission of all the peers or nodes, thus suitable for military operations where accurate planning and information are required in operations. As all the peers have equal access to the information and transparency, this openness helps in supply tracking and protects against fraud and poor management. Due to this characteristic, it becomes suitable for defense operations.

Motivation

Blockchain technology has great potential in defense operations, despite several challenges preventing its application. Modern defense systems are sensitive to security threats and cyberattacks because of their concentration. Although these issues are solved by the decentralized and secure nature of the blockchain systems, issues regarding privacy, scalability, and energy efficiency restrict its application. In defense

organizations where there are limited resources and time restrictions for the operations where drones need to make fast decisions, consensus algorithms like Proof of Work (PoW) are inefficient to work as they require high energy requirements. Additionally, processing and storing becomes limited due to the huge amount of data generated during operations; security of that classified data is also challenging. To ensure that blockchain is used to its optimal capabilities and overcome all the challenges and restrictions, this research will help in achieving those by investigating solutions to the problems.

Objectives

This paper's aim is to pick up the research gaps that are restricting military organizations from implementing blockchain systems. It will specifically address the issues of energy efficiency, scalability, and privacy in military usage. It will provide practical solutions to these specific problems by gaining additional knowledge about gaps and implementing effective solutions that will contribute to the implementation of blockchain technology in defense.

2. BLOCKCHAIN FUNDAMENTALS FOR MILITARY APPLICATIONS

Overview of Blockchain

Blockchain is basically a distributed ledger that uses peer-to-peer networks that allows secure and transparent transactions and communication that keeps records safe and secure due to its immutability. In blockchain, every block or entry relates to another block, linking together and making chains. In this architecture, every block has a cryptographic hash for the blocks before it such that an immutable sequence of records is created and changes are detectable [1].

Figure 1: Blockchain block structure[1].

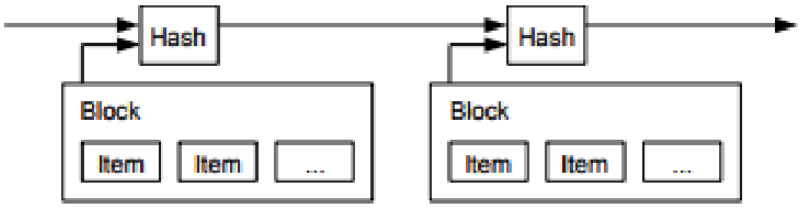
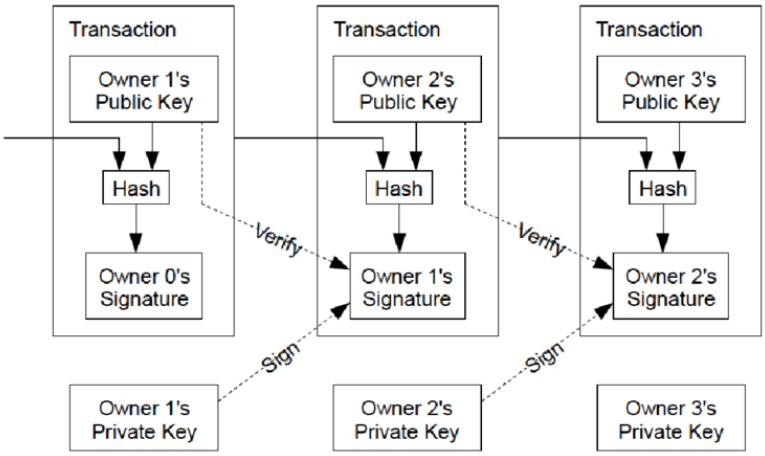


Figure 2: Blockchain working [1].



Important Blockchain Elements

Decentralization means in blockchain systems, a peer-to-peer network is used rather than a centralized system where there is a central database. Due to the decentralized nature, it helps in improving resilience against cyber-attacks and reduces the risks of single point failure [2]. There are various types of consensus mechanisms in blockchain that are used to validate transactions and help in maintaining the integrity of the ledger. Some of them are listed below:

1. Proof of Work (PoW): It is one of the consensus mechanisms where the users have to solve mathematical puzzles to validate records or transactions and then add them to the blockchain. This method is secure but consumes a lot of energy, so it is not the right choice to use in defense operations having limited resources [1].
2. Proof of Stake (PoS): PoS is more energy efficient than PoW because it uses coins they own and stakes them as collateral and validates transactions [4].
3. Proof of Authority (PoA): A small number of selected nodes called validators are selected to validate the transactions. This technique is mainly seen in permissioned blockchain networks [5].
4. Smart contracts: These are self-executing contracts that use cryptographic encryptions. They function as go-betweens to help, validate, or enforce contract negotiations and performance. We can use smart contracts in defense applications to effectively improve the efficiency of military operations and tasks such as resource allocation and procurement [6].

Relevance to Military Applications

Blockchain is suitable for its special characteristics:

Tamper-Resistance: Once the data is added to the record, it cannot be altered without all its members permission due to its immutable nature. This is essential in the military, where consistent data is important for troop movements, logistics, and intelligence reports [2].

Secure Communication: Unauthorized access is prevented by cryptographic techniques to secure communication channels [7].

Decentralized Control: Central data breaches and operational errors are avoided due to the decentralized nature. allows data sharing while maintaining security and privacy to many stakeholders, including commanders, field staff, and automated systems. [8].

Secure Data Sharing: Multiple parties can securely share data while maintaining records and responsibility. Military logistics requires real-time tracking of supplies and equipment.[9].

Considering all the above qualities they will help in improving defence operational capabilities and will give them a strong foundation.

Current Applications of Blockchain in Military and Defence

1. Blockchain in UAVs and Military Drones

Surveillance, targeted attacks, and reconnaissance: such tasks are performed by unmanned aerial vehicles (UAVs) and military drones in wartime combat. For successful operations, they must operate, coordinate, and communicate securely. For achieving this aim that will improve drone operations security and management, there are multiple ways as follows:

Secure Communication: Due to the decentralized nature of blockchain, authenticity and integrity of data are guaranteed. Communication from drones becomes secure due to blockchain protecting important

operational data from illegal authority. Smart contracts restrict access to the blockchain for specific users, and their commands are implemented, and it enables real-time decision-making [8].

Drone Swarm Management: Blockchain works as a backbone to coordinate swarms of drones; they have decentralized control, which enables fast speed and improves responsive time in dynamic environments that they communicate information with one another without relying on central authority [7].

Protecting Privacy: Blockchain cryptographic characteristics enable safe transactions and communication by hiding data of military activities. Verification strategies are used like zero-knowledge proofs, which protect sensitive mission information [9].

2. Blockchain and Cyber Defence

Due to the increase in cyberattacks, preventing them is a major task in which blockchain plays an important role in improving the cyber defense capabilities.

Defense Against Cyber Threats: Due to the decentralized blockchain systems that don't allow any data manipulation and unauthorized access, it helps in improving the military network's security. The integrity of the entire network is maintained even if a single node is affected [10].

Stopping Data Tampering: In blockchain, the records cannot be changed or manipulated; to do so, all the users or nodes must be approved, which makes it difficult for attackers to do so. Therefore, they can maintain the quality of operational data [7].

Maintaining System Integrity Military organizations verify that only authorized persons will be able to access the records and also to carry out software management and updates protecting against cyber-attacks and unauthorized access[8].

3. Blockchain in Military Supply Chain and Logistics

In defense operations, the mission's success greatly relies on supply chain management, where timely delivery of supplies and equipment is equally important. In this case, blockchain can help in numerous ways to improve logistics.

Monitoring Military Supplies: Due to decentralized systems, military supplies can be easily tracked and maintained in real-time. Also capable of tracking the flow of supplies [9].

Ensuring Transparency: Blockchain enables authorized people to see all the supply chain transactions that occur on blockchain. Due to the transparent nature of fraud, poor management, and the introduction of fake goods into the supply chain, all can be eliminated [7].

Preventing Unauthorized Access and Corruption: Due to the immutable nature of blockchain, the chances of corruption in military logistics drastically reduce. Due to the access control methods, it guarantees that the classified data can be accessed only by authorized persons [10].

4. Blockchain for UUVs, or underwater drones

There is an extensive use of Underwater Unmanned Vehicles (UUVs) in the detection of mines, security observations, and some naval operations. Following are the benefits of including UUVs in operations:

Secure Communication: Secure communication becomes important in dangerous environments. The decentralized framework of blockchain guarantees the security and integrity of commands and telemetry data [7].

Data Sharing and Coordination: Due to the blockchain integration, UUVs and command centres can share data securely and effectively that improves coordination of work. Smart contracts also enable allocating task automation on real-time data that ultimately maximizes the effectiveness of operations [8].

Enhanced Task Management: Blockchain also enables task management techniques for UUVs, enabling safe and reliable communication among several vehicles operating in harsh conditions. This becomes important for missions that require data processing and decision-making in real time [10].

3. RESEARCH GAPS IN BLOCKCHAIN ADOPTION IN MILITARY ORGANIZATIONS

Concerns about Scalability and Privacy in Drone Operations

There are some issues regarding security and privacy in drone fleet management systems. UAVs must transmit data safely and securely without disclosing important details regarding operations. But because of the transparency in the system, maintaining confidentiality might be challenging [11]. Additionally, when the number of drones increases, scalability issues become a concern. To handle the huge amount of data generated by various drones at a time, the system should be efficient enough to handle it; transactions must be processed quickly. The current blockchain's efficiency is limited, causing an inability to handle operational load [8].

Restrictions on the Existing Consensus Mechanisms

In defense, there are very restrictive consensus processes in various blockchain systems. An example is good for privacy but is more energy-consuming and needs more computational power, which might not be possible with limited resources [10]. Also, POWs validating transaction delays may slow the decision-making time, which is important in wartime situations. Military operations require high energy and performance requirements that may not be sufficiently addressed by proof of stake and other consensus techniques. So military organization needs more rapid and energy-efficient consensus processes[12].

Power Restrictions and Data Management in Underwater Environments

Underwater Unmanned Vehicles (UUVs) face restrictions on data management and power requirements while using blockchain technology. In underwater situations, UUVs face problems with limited energy supplies and data storage capacity. Data transmission is unreliable over water, and maintaining communication between UUVs and command centers can be difficult [7] There is a need to implement blockchain solutions that will ensure continuous connectivity and less electricity consumption [13].

4. PROPOSED SOLUTIONS TO IDENTIFIED RESEARCH GAPS

Solutions to Privacy and Security Challenges

Applying Zero-Knowledge Proofs (ZKPs) in the Military

A Zero-Knowledge Proof (ZKP) is a professional cryptographic technique that encourages one team to prove to another team that they know the information without telling the proof. ZKPs give a tool for defense organizations, which allows them to maintain privacy and security while communicating, and they can verify some sensitive operations without disclosing details. As a result, ZKPs are extremely useful in contexts where maintaining confidentiality is highly important and the disclosure of data could have serious security implications.

Importance of ZKPs in Military Operations

Deployments, target areas, and the location of base stations and camps are sensitive and classified data that must be protected from illegal access. Zero-Knowledge Proofs (ZKPs) help in protecting the information and proving the data's validity without disclosing it. People sensitive to national security have been trained from before Day 1 that cutting off the flow of information is essential when it would compromise the success or failure of military operations.

Intended Application Use Case—For example, one military unit may need to identify another while working together on a joint operation, however, without disclosing their own location or mission details. Zero-knowledge proofs could help them to confirm that this is the same person without giving up any more information about them [14].

ZKPs can also be useful in:

- **Authentication (institution):** Demonstrating that personnel or equipment are legitimate without revealing explicit knowledge of person/mission.
- **Communication:** Validating the messages exchanged between military units without revealing information within the message to potential threats [2].
- **Supply Chain Security:** Confirming the arrival of important material moments without disclosing things that are essential about both commodities.

How ZKPs can be implemented in Military Sector

Define Use Cases:

To start, defining critical military use cases for ZKPs listed below. Common areas include:

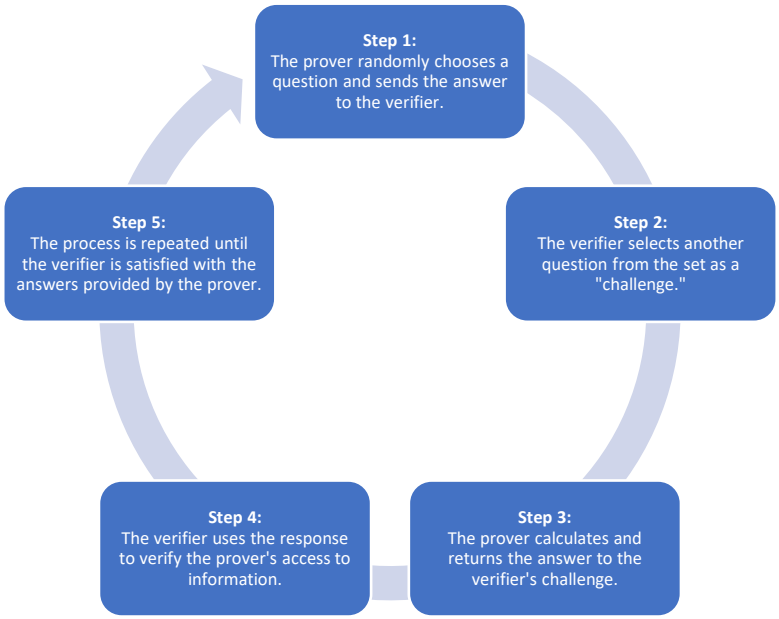
- **Identification:** Establishing who personnel are in a secure manner without letting out sufficient details to breach operational security [15].
- **Collateralized Communication**: Verified messages or commands for military units without the content of communication.
- **Supply Chain Transparency**: Maintaining the security and verifiability of military logistics while hiding sensitive details on what is in transit [16].

Selecting the ZKP Protocol:

Different ZKP protocols -Two of the most popular ZKP methods for military operations are:

- **zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge):** Highly efficient and with very short proof sizes, zk-SNARKs enable identity verification or secure communication without needing to send all the data used in the process, so they can save bandwidth consumption [14].
- **zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge):** zk-STARKs are significantly more scalable than zk-SNARK. NIZK can be utilized in large-scale applications, such as safeguarding communications and supply lines between multiple military units or even allied armies, because it is an algorithm specifically designed to scale. Which protocol a military organization chooses will depend on the specific requirements it has for speed, scalability, and transparency.

Figure 3: Working of Zero knowledge Proof



Integration of ZKPs in Use with Military Devices:

Select a ZKP protocol and incorporate it into today's military systems. This means working closely with current security protocols to provide a more complete, rather than disruptive, workflow.

- **Identity Verification:** Use ZKPs in identity verification systems to help military members prove their credentials without having to reveal private, personal data. However, ZKPs can be used to demonstrate some information about a soldier (e.g., they have clearance) without revealing much more detail [16].
- **Command and Control:** Combine ZKPs into reliable communication systems to secure the message origin between two military units. Each unit can then check that the message is valid without exposing it to eavesdroppers [17].
- **Supply Chain Management:** ZKPs are applied in blockchain-based supply chains to attest that equipment (or goods) delivery is authentic without revealing real information about the delivered supplies, e.g., nature and/or number, which guarantees transparency without disclosing operational security [2].

Test and Pilot Programs*:* After the integration of ZKPs, it has to be tested severely with real-world usage before going live. e.g., running pilot programs to assess how ZKPs apply in alternative military domains.

- **Field Communication:** ZKPs can also be used to secure field communications between units, proving such messages have been sent from an authenticated unit without revealing operationally critical details.
- **Logistics Verification**: Testing ZKP protocols in supply chain logistics to verify under zero knowledge that critical equipment and supplies are delivered while maintaining transaction privacy relevant for proving its legitimacy without revealing too much sensitive information.
- **Training Personnel:** Because cryptographic systems are difficult to comprehend, it is crucial for military personnel to be trained in the use of ZKPs. It includes training personnel who need to understand how ZKPs work, potentially written down as they are deployed and also when operational security is made imperative.

The advantages of implementing ZKP into military organizations

Enhanced Privacy: Zero-knowledge proofs enable military organizations to prove that they have data or identities without showing any underlying details. This secures the privacy of data, as revealing any information in a covert mission could mean causing security breaches [14]. Use case: A military unit can authenticate itself to an ally without divulging exactly where it is or what it might be doing.

Secure Data Verification: ZKPs allow you to authenticate a communication or transaction without exposing the content. Military communications are thus not readily decipherable to usual eavesdroppers. Example: A drone can confirm that it finished surveying an area without betraying what information was collected [16].

Scalability: More importantly, ZKPs in the form of zk-STARKs are so scalable that military organizations will be able to use them on a large-scale level. This is important to verify communications or logistics between different units and international forces [18].

Difficulties with ZKP Deployment

Computational Complexity*:* Even zk-SNARKs are computationally heavy, and ZKPs in general can suck up quite a bit of processing power. A common use case for ORAM is military environments where resources are scarce or a minimum latency in operation [16]-[11].

Legacy Systems Integration: Existing military systems may be built on legacy hardware that does not support modern cryptographic protocols like ZKPs. However, this is non-trivial to guarantee and requires careful planning that would not break existing workflow [15].

Training Requirements: Using Zero-Knowledge Proofs requires training military personnel to use and apply them. It can take some time, especially if the person is not acquainted with crypto.

Conclusion: For safeguarding plausible deniability of sensitive military operations, zero-knowledge proofs provide a powerful answer. Using ZKPs, military personnel can verify their identity as well as authenticate communications and secure supply chains without sharing sensitive data. Although there are problems related to using ZKPs (including computational overhead and integration with existing infrastructure), the improvements in privacy, scalability, and security outweigh these costs for military organizations. Against the backdrop of this evolving cryptographic landscape, ZKPs are slated to secure a spot in defense for some time.

Solutions to Energy Efficiency Challenges

Consensus: Energy-Efficient Structures

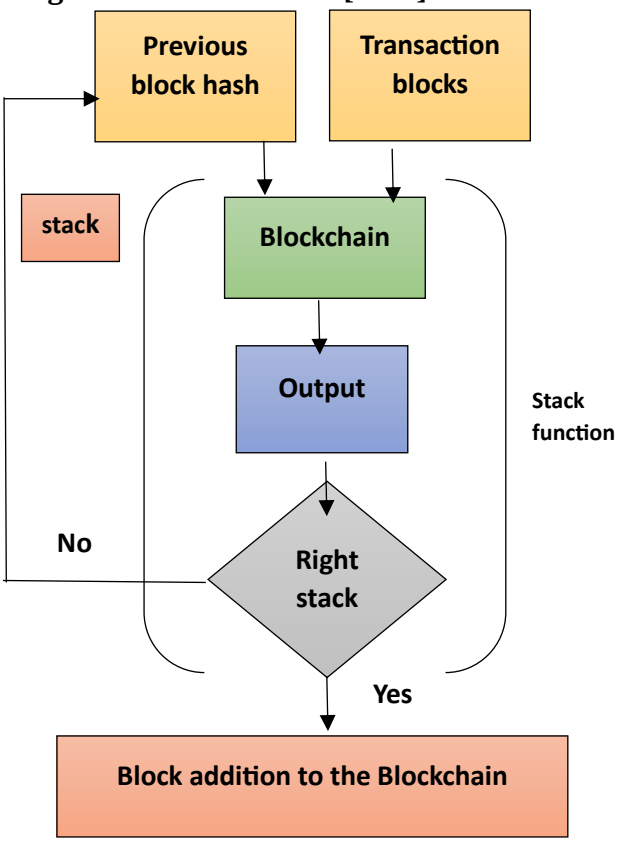
The consensus mechanism is the heart of any blockchain network that controls how transactions are validated and added to a ledger. Military applications need to have mechanisms that are safe and efficient in terms of energy. The main difference between the consensus algorithms of POW (Proof-of-Work) and POS (Proceed-to-Stake) is that staking participants need just relatively few coins to validate the nodes. Since this does not require heavy computation, it greatly reduces energy consumption [4]. PoS could process transactions very quickly in such a military setting while conserving energy. In PoA (Proof of Authority), a restricted number of nodes (or we can say validators) are granted authority to validate the transactions. This in turn lowers energy use and increases transaction speed, ideal for military applications requiring snap decision-making. In this design, the nodes are pre-chosen using a trust model to ensure the safety of the validation process as well [5].

Proof-of-Stake (PoS) military use case

Proof of Stake (PoS) is a less intensive version of the Proof of Work model employed by some blockchains. In PoS, validators are chosen to perform the transactions on their value or stake and not according to

computational power as in PoW. Because energy efficiency, security, and scalability are crucial issues for military organizations deploying blockchain-based systems, PoS is a more practical platform. Based upon these references, as well as in-line citations and explanations, this section then outlines the process of PoS implementation to other military settings.

Figure 4: Flow chart of [POS]Proof of Stake



Why do Military Organizations Matter in PoS?

Military operations require secure, reliable, and efficient communication systems for information management in the field of youth as well as logistics. In military bases or field operations where energy resources are limited, POS offered many advantages. It chooses validators who serve somewhat similar functions as miners to manage distributed consensus for blockchains based on their stake within the network in a way that is considerably less energy intensive than using computational puzzles [19].

PoS may be beneficial in military applications that need to support the following aspects:

Secure communication: This is to make sure that only the authorized nodes validate transactions and reduce any risk of malicious actors accessing the network.

Supply Chain Management: Tracking and auditing of military equipment and supplies over a decentralized, energy-efficient network.

Operational Scalability: Permitting the blockchain networks to grow without requiring substantial resources as in the case of PoW [20].

How to Implement PoS in Militaries?

PoS Military Use Cases

Military organizations must first determine where blockchain can provide value before rolling PoS out.

Applications of PoS in Military Context

Communication Safety: Protection of military communications using PoS, allowing only authorized nodes (those who have collateralized some stake) to validate transactions and messages.

Logistics and Supply Chain Management: Using PoS in blockchains to keep an auditable record of equipment & supplies without its high energy bill [21].

Drone & UAV Coordination: Drone & UAV Coordination: In drone operations, PoS can ensure trust among peers who communicate with each other and bridge between geographic distances, allowing checking command-and-control data securely in known trusted nodes [11].

Select a PoS Protocol

There are different levels of security and scalability depending on the PoS protocol, a must-have for military applications. Examples of popular PoS protocols include:

Casper (used in Ethereum 2.0): This protocol is designed to provide increased security and faster finality of transactions, allowing military communications such as data transfers to be confirmed more rapidly [22].

Tendermint: Tendermint has fast finality and high throughput; it can be used in military applications where low-latency communication is required, such as for coordination of UAVs or real-time battlefield logistics [4].

Deploy Validator Nodes

Validators in the PoS operate by entrusting validators who are chosen with regards to their stake in the network. For example, in a military organization, you can involve these validators:

Science-fiction use case: Validators as command centers or something akin to a trusted military unit that could verify transactions such as the delivery of supplies, equipment, and mission data. The validators simply entered promises with each other, where the consequences of failing to meet a promise were forfeiture by the validator stakeholders themselves (i.e., restricted access to military networks).

Allied Forces of Defense Contractors: Allied forces or defense contractors would also serve as validators in military operations and logistics across a secure transfer of supplies or intelligence via decentralized blockchain networks [21].

Consensus Rules and Penalties

Military organizations must establish procedures for validating transactions and create incentives to dissuade bad actors (entities trying to compromise the system). In PoS, validators can be slashed for not accurately validating, aka lying [22].

Consensus Rules: Define how validators should confirm military transactions; it will only consider valid messages or logistics updates. Economic penalties for Byzantine mechanisms that penalize nodes who try to validate fraudulent transactions or compromise the security of the network.

Deploy PoS with Current Military: The security, productivity, and transparency of existing military systems are increased by combining them with the PoS network. Some examples of key integration points are:

Communication Systems: PoS can become a component of hardened military communication networks to verify encrypted messages between command centres and units at little computational cost.

Logistics Platforms: Military logistics platforms can be linked to PoS-based blockchain systems that will allow decentralized supply and equipment tracking, such as for containers or weapons [11].

PoS consensus: There is at least one other blockchain use case that has a very positive impact on the drone market by using the PoS consensus mechanism to ensure immediately secure and efficient data processing

without draining energy resources, namely drones/UAVs for which mission commands can be received in real-time verification.

Conduct Pilot Testing

Once a PoS-based blockchain is deployed, you have to run pilot tests that require real-world performance analysis. Pilot projects might include:

Trials for Secure Communication: Validate PoS in communication among military units deployed on the ground, where data security and speed are paramount.

PoS Logistics Management: Develop a small-scale PoS blockchain with the goal of managing and tracking military supplies in terms of both quantity levels based on inventory for a specific base or unit to test how it can scale, reliability, etc. Pilot tests to consider factors such as speed, security, and energy efficiency versus traditional methods. Missions, Functions, and DIME Operations Scale

Global Operations: It rolls out PoS functionality for safe, accurate data sharing among allied forces.

Application of Large-Scale Logistics: As the earliest example, PoS networks can be used for tracking military supplies worldwide to guarantee security and improve efficiency without consuming massive energy [21].

Benefits of PoS within the Military Segment

Energy Efficiency

The primary benefit of PoS is that it requires much less energy than PoW. In the military setting, this is great as energy resources are scarce on deployments, especially in remote or field environments [19].

Scalability

Compared to PoW systems, the bottlenecks that are experienced when handling a high number of transactions can be dealt with by increasing transaction capacity. Example of the use case within military supply chain management where there might be thousands of transactions at once in real-time [22]

Enhanced Security

Preserving the adversarial dynamic between new token buyers and existing holders, PoS requires network participants to similarly have real skin in the game while utilizing sincere slashing for dishonest validators providing security against malignant actors who would seek to harm the network. This policy enhances security by allowing only authorized entities to interact with military blockchain networks [21].

Faster Transaction Times

This feature of PoS can allow faster validations against real-time military applications such as UAV control or battlefield communications [11].

Hurdles in executing PoS on Military organizations

Validator Selection: Selecting the legible bodies for validators holds a substantial stage in military foundations. Corrupting a validator would put the whole network at risk [19].

Resistance to Change: If it were deployed, PoS would likely face the same resistance associated with using any new technology that military personnel simply aren't familiar with. The key to success is training and education.

Integrating with Legacy Systems: Most of these military institutions are still on legacy platforms that may not readily plug into the blockchain networks. It will require careful planning and technical know-how to fit the pieces together.

Conclusion: Proof of Stake offers a way to start using blockchain within military organizations, ensuring the best levels of security/robustness, scalability, and energy efficiency. PoS can be easily integrated into communication systems, supply chain management, and drone coordination, and then military

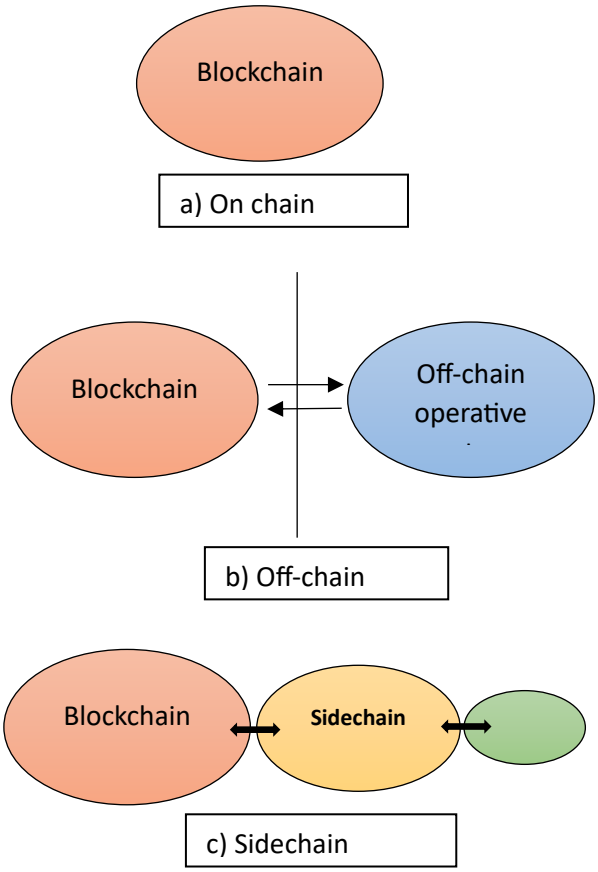
organizations can have their operations secured, streamlined, and energy conserved. While there are still relevant challenges, like the difficulty of selecting validators and interoperability into existing systems, these factors aside, PoS is tentatively an appealing choice for military 2.0 infrastructure requirements.

Solutions to Scalability Challenges

Off chain processing

In the military, this concept is applied by using off-chain processing solutions. Off-chain processing is designed to handle some data or transaction operations "off" (not within) one of the main blockchain networks; it can unload its load from a chain while keeping this chain integral, which is perfect for military organizations so that they can quickly and securely process tons of sensitive data without jamming the main blockchain network. Off-chain solutions make it possible for military operations to access the security and transparency features of blockchain without running into slowdowns due to computational or bandwidth limitations on a decentralized network.

Figure 5: Chain types



Why Off-Chain Processing Matters in Military Operations

The challenge is that real-time, massive data cannot be efficiently handled by blockchain itself owing to its slowness and scalability. The use of off-chain processing can help with this as it moves some operators from the blockchain itself, lightening data presses and enabling militaries to process information more quickly using fewer resources [2].

Scenario: A military drone fleet might want to share huge quantities of surveillance tapes or mission logs as they happen. On–chain components of it such as proof or data integrity may stay on–chain but the bulk will be processed off chain.

Although Off-chain solutions excel in following contexts:

Data-Intensive Operations: Mission-centric requirements such as real-time battlefield analytics or drone coordination, where disparities in processing time mean differences between mission success and failure [23]

Military supply chain management: Large scale military logistics data verification without blockchain network overloading

Foreign Military Partners: Sharing intelligence and operational data between allied forces in an off-chain capacity, while using blockchain for the final verification of that information.

Off-Chain Processing Solutions

Benefits of each off-chain solution that can be implemented in the military organizations:

State Channels: Allow parties to perform transactions with each other off-chain, and then have the final state settled on a blockchain. This supports the ability to have many interactions between military units or systems without overwhelming a given blockchain.

Defence command centres and army field units need fast and secure communication off-chain before updating the blockchain. This decreases blockchain overhead and quick decision-making[23].

Sidechains: These are the separate blockchain system that runs parallel to main blockchain. This is an independent chain containing its own set of transactions. This system can be made flexible and scalable by moving data from sidechain to main blockchain. Sidechain can run logistic operations, handling transactions such as equipment deliveries or troop movements. The data then transfer to main blockchain permanently after being verified [24].

Off-Chain Data Storage

However, large amounts of data are directed on-chain quickly becomes inefficient. This enables off-chain data storage for most military records (think video surveillance and supply chain) while proof of these external, independent operations is stored on-chain through cryptographic hashes accounting to its integrity.

Example: A military surveillance drone can store high-resolution video footage off-chain, while the blockchain stores a cryptographic hash of the video, ensuring that any tampering or manipulation of the footage can be detected without needing to store large files on-chain [25].

Steps for Implementing Off-Chain Processing in Military Organizations

- **Identify Data-Intensive Operations**: The first step is to identify specific military operations that generate large amounts of data and require real-time processing. These may include:
- **Surveillance and Reconnaissance**: Vast amount of data is produced from Drones and other intelligence-gathering systems that need to be processed quickly.
- **Logistics and Supply Chains**: Tracking military supplies in real-time can overwhelm on-chain systems, making off-chain processing a better fit.
- **Military communications networks:** Exchanging encrypted messages or rapid updates between command centres and local units may benefit from government channels outside the network.

Select an Off-Chain processing model

The selection of the appropriate off-chain processing model depends on the specific requirements of the defence organization

- **State Channel**: It is ideal for secure and repeatable interactions like synchronous real time communication between two units.

- **Sidechains:** It is suitable for operations that can be sharded or divided in units, such as supply chains or field operations, where sidechains can operate independently.
- **Offline storage**: It is best to deal with large files (such as CCTV footage, sensor data) by sequencing required integrity checks [24].

Integration with the Blockchain network

Off-chain solutions need to integrate seamlessly with an organization's existing blockchain infrastructure:

- **Government channels**: May connect to command-and-control systems or military units that require fast and secure interactions.
- **Sidechains:** May be placed in parallel with an existing blockchain network to allow local or independent data processing.
- **Offline storage:** A secure external storage solution (e.g., cloud or local server) must be integrated with the military blockchain system to ensure that data can be stored off-chain for a while that still maintains the integrity of the chain.

Use security protocols and encryption: Defense organizations handle highly sensitive information. Therefore, safety is essential. Data outside the network must be protected using encryption and authentication methods to prevent unauthorized access or tampering. Additionally, Zero-Knowledge Proofs (ZKP) can be used to ensure data integrity outside the network without revealing the content [25].

Test scale: After use Off-grid solutions should be rigorously tested in real-world conditions to ensure they meet operational requirements.

Pilot testing: Test off-chain processing in specific use cases, such as coordinating drone operations. or logistics management in the supply chain.

Performance Monitoring: Monitor off-chain solutions for processing speed, security, and overall performance. This is to ensure that it meets the real-time needs of military operations.

Scaling: Once tested, the solution can be scaled out of the chain to larger operations, such as joint military exercises or international cooperation, to increase safety and efficiency.

Important advantages of off-chain computing in military organizations

Increased scalability: Offline computing allows military operations to scale without overloading the blockchain. State channels and side chains allow multiple interactions or transactions to be processed quickly. It is then settled in the chain only when necessary [23]. Example: In military operations, drone fleets are used in which there are multiple data points and interactions per second. The data can be processed off-chain and later combined with the main blockchain.

Reduce costs and energy efficiency: Transaction costs and energy consumption can be reduced by collecting large amounts of data outside the network. This special characteristic helps in resource-constrained environments, such as battlefields or remote operations**.** [2]

Advanced security Off-network solution Off-chain processing can be combined with encryption and zero-knowledge proofs to ensure privacy and security from cyberattacks.[25]

Real-time determination Off-chain processing ensures that critical classified information like battlefield updates or logistical movement is processed outside the chain in real time without delay due to chain validations [23].

Challenges in using off-network solutions

Data security and integrity: Data security and integrity: off-chain communication must be secure to safeguard from unauthorized access. Strong encryption techniques need to be followed, and zero-knowledge proofing should be used to maintain good off-chain data integrity[25].

Integration with legacy systems: Most of the defense systems are constructed on old infrastructure; they may not be compatible with modern off-chain solutions. Combining off-chain solutions with existing systems or networks may require careful handling, planning, and technical expertise.

Complexity training: Off-chain solutions can be complex. This may require professional training for military personnel to handle and understand the network.

Conclusion: Off-chain networks provide defense organizations with a scalable solution. Powerful and secure for managing large amounts of data in real time. Reducing the load on the blockchain network while maintaining data integrity Off-grid solutions are ideal for data-intensive operations such as drone coordination, logistics, secure communications, etc., although challenges such as security and integration with legacy systems exist. By adding scalability, reduced costs, and improved real-time resolution, this makes it a valuable technology for modern military organizations.

5. CASE STUDIES AND REAL-WORLD APPLICATIONS

Examples and Practical Uses, in Real Life Situations

The use of technology in defense settings is being more widely investigated through different real-life examples. These practical applications showcase how the technology can boost efficiency in operations and security measures while also simplifying logistics processes. Here are some notable instances that showcase the advantages of employing blockchain in activities. The U.S. Department of Defense has been actively delving into the possibilities of technology for purposes with a focus on supply chain management and logistics improvement efforts in recent years. A notable project involves an effort between the DoE and tech companies to create a blockchain-powered system to monitor and verify resources, like aircraft components and ammunition. The platform's goal is to offer a clear way to track the origin and condition of resources seamlessly from start to finish using blockchain technology. The implementation of this project could boost the preparedness for operations by enhancing the accuracy and accountability of inventory management systems. Relying on technology also enables real-time tracking, which can result in the distribution of resources and more informed decision-making in crucial mission scenarios [9].

NATO is currently conducting research, on projects related to blockchain technology.

NATO has started initiatives to evaluate the potential use of blockchain technology in military settings with a specific project dedicated to utilizing blockchain for secure communication and information exchange among allied military units. The project's goal is to establish a communication system for NATO member countries to exchange intelligence and operational information securely using blockchain technologies security features, like immutability and encryption, to safeguard sensitive data from unauthorized access or alterations. This project aims to improve communication between NATO forces for coordination in combined missions by utilizing technology to share data securely and enhance situational awareness and operational efficiency during multinational military operations [8].

Use of Blockchain in Israeli Defence Forces (IDF)

The Israeli Defense Forces (IDC) are investigating the use of technology to improve cybersecurity and safeguard communications, with a special emphasis placed upon utilizing blockchain to secure important infrastructure and confidential information. The new blockchain system aims to establish a decentralized communication platform to protect information from risks effectively. It will maintain a record of all communications in a ledger to help the IDF improve accountability and trackability in its activities. The use of technology in this situation is intended to enhance the IDF's ability to defend against cyber threats and minimize the risk of cyberattacks affecting their operations significantly [10].

Pilot Programs in European Military Organizations

Numerous military entities in Europe are currently running test programs to explore how blockchain technology can be used in situations such as logistics and personnel administration. These initial initiatives aim to leverage technology for organizing employee records, authentically capturing work experience certifications, and training history. Furthermore, blockchain is for monitoring the movement of resources across borders to boost visibility and responsibility in missions. The use of blockchain in managing personnel is anticipated to decrease tasks and improve data integrity while also simplifying processes in an organization's workforce operation and promoting effective collaboration between European partners for better resource management during collaborative missions [2].

6. FUTURE PROSPECTS OF BLOCKCHAIN IN MILITARY ORGANIZATIONS

Military companies will be able to improve their cybersecurity, supply chain management, autonomous operations, and cross-border cooperation in the future thanks to blockchain technology. However, resolving challenges with scalability, energy efficiency, and regulatory compliance will be necessary for its widespread acceptance.

- **Strengthened Cybersecurity**: By establishing tamper-proof, decentralized systems that reduce the danger of cyberattacks, blockchain can strengthen cybersecurity. Future uses for smart contracts could include automatic threat detection and decentralized security frameworks, enhancing the resilience of military networks. [9]-[7].
- **Military Operations with Autonomy:** Blockchain has the potential to facilitate secure communication and real-time coordination amongst unmanned systems, such as UAVs and UUVs, in autonomous operations. Blockchain-based tamper-proof mission logs would improve the dependability of autonomous decision-making and guarantee accountability [11].
- **Optimization of the Supply Chain**: Blockchain's transparent, real-time asset monitoring can completely transform military supply chains. Smart contracts have the potential to simplify logistics, lower fraud, and automate procurement [9].
- **Command and Control Decentralized:** Blockchain technology may be used by command-and-control systems in the future to provide decentralized decision-making, enabling quicker and more adaptable operations. The transparent nature of blockchain enhances the military units' awareness and safeguards data exchange[2].
- **International Cooperation**: Interoperability and operational efficiency can be improved by implementing blockchain in international military cooperation like NATO that encourages secure information sharing and resource management [8].
- **Overcoming Obstacles:** Future studies need to be done to handle issues regarding energy efficiency and scalability. Technology will be in widespread use only by creating consensus techniques like Proof of Stake (PoS) and following international laws like GDPR**.** [20]-[4]- [9].

7. CONCLUSION

The vast potential of blockchain in defense is explained in this paper, which also pinpoints the important issues of energy efficiency, scalability, and privacy. This study shows us the present shortcomings for implementation, including the privacy dangers associated with drone operations, the energy inefficiency of the consensus algorithms, such as Proof of Work (PoW), and the scalability issues related to large-scale military network management. Given solutions cover all the related gaps. Solutions are off-chain

processing for scalability, Proof of Stake (PoS) for energy efficiency, and Zero-Knowledge Proofs (ZKPs) for privacy. Blockchain has a great potential to enhance military operations in offering secure communications, tamper-proof data management, and decentralized control of autonomous systems and supply chains. It is significant in the context of defense because it can protect critical infrastructure and offer transparency in military logistics and operations. By filling up these gaps and testing blockchain's usefulness in real-world scenarios, military organizations may better prepare for the challenges of modern combat.

REFERNCES

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.” [Online]. Available: www.bitcoin.org
2. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” in 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, Jun. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.
3. D. T. Alex Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin. 2016.
4. S. King and S. Nadal, “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,” 2012.
5. M. A. Manolache, S. Manolache, and N. Tapus, “Decision Making using the Blockchain Proof of Authority Consensus,” in Procedia Computer Science, Elsevier B.V., 2021, pp. 580–588. doi: 10.1016/j.procs.2022.01.071.
6. Melanie Swan, Swan, M. (2015). Blockchain: Blueprint for a New Economy. O’Reilly Media.
7. B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab, “Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment,” IEEE Trans Veh Technol, vol. 69, no. 8, pp. 9097–9111, Aug. 2020, doi: 10.1109/TVT.2020.3000576.
8. D. K. Tosh, S. Shetty, P. Foytik, L. Njilla, and C. A. Kamhoua, “Blockchain-Empowered Secure Internet -of- Battlefield Things (IoBT) Architecture,” in MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM), IEEE, Oct. 2018, pp. 593–598. doi: 10.1109/MILCOM.2018.8599758.
9. K. Shahzad, A. O. Aseeri, and M. A. Shah, “A Blockchain-Based Authentication Solution for 6G Communication Security in Tactile Networks,” Electronics (Basel), vol. 11, no. 9, p. 1374, Apr. 2022, doi: 10.3390/electronics11091374.
10. S. S. Et.al, “Consortium Blockchain for Military Supply Chain,” Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 3, pp. 1825–1831, Apr. 2021, doi: 10.17762/turcomat.v12i3.1011.
11. A. Islam, M. Masuduzzaman, A. Akter, and S. Young Shin, “MR-Block: A Blockchain-Assisted Secure Content Sharing Scheme for Multi-User Mixed-Reality Applications in Internet of Military Things,” in 2020 International Conference on Information and Communication Technology Convergence (ICTC), IEEE, Oct. 2020, pp. 407–411. doi: 10.1109/ICTC49870.2020.9289327.
12. L. Gambazzi, P. Schaller, A. Mermoud, and V. Lenders, “Blockchain in Cyberdefence: A Technology Review from a Swiss Perspective,” Mar. 2021.
13. A. Kumar et al., “Blockchain for unmanned underwater drones: Research issues, challenges, trends and future directions,” Journal of Network and Computer Applications, vol. 215, p. 103649, Jun. 2023, doi: 10.1016/j.jnca.2023.103649.

14. R. : Eike Kiltz, D. Stehlé, É. Normale, and S. De Lyon, "Gaussian Sampling in Lattice-Based Cryptography Vadim Lyubashevsky IBM Zürich Encadrant Industriel : Sylvain Lachartre Thales Communications & Security."
15. O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems," Journal of the ACM, vol. 38, no. 3, pp. 690–728, Jul. 1991, doi: 10.1145/116825.116852.
16. N. Narula, W. Vasquez, and M. Virza, Open access to the Proceedings of the 15th USENIX Symposium on Networked Systems Design and Implementation is sponsored by USENIX. zkLedger: Privacy-Preserving Auditing for Distributed Ledgers This paper is included in the Proceedings of the 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI '18). zkLedger: Privacy-Preserving Auditing for Distributed Ledgers. [Online]. Available: https://www.usenix.org/conference/nsdi18/presentation/narula
17. S. Goldwasser, S. Micali, and C. Rackoff, "The Knowledge Complexity of Interactive Proof-Systems."
18. E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable, transparent, and post-quantum secure computational integrity," 2018.
19. A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the Security and Performance of Proof of Work Blockchains," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA: ACM, Oct. 2016, pp. 3–16. doi: 10.1145/2976749.2978341.
20. V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform."
21. N. Kostopoulos, Y. C. Stamatiou, C. Halkiopoulos, and H. Antonopoulou, "Blockchain Applications in the Military Domain: A Systematic Review," Jan. 01, 2025, Multidisciplinary Digital Publishing Institute (MDPI). doi: 10.3390/technologies13010023.
22. V. Buterin and V. Griffith, "Casper the Friendly Finality Gadget," Oct. 2017, [Online]. Available: http://arxiv.org/abs/1710.09437
23. J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," 2016.
24. A. Back et al., "Enabling Blockchain Innovations with Pegged Sidechains," 2014.
25. G. Zyskind, O. Nathan, and A. "Sandy" Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in 2015 IEEE Security and Privacy Workshops, IEEE, May 2015, pp. 180–184. doi: 10.1109/SPW.2015.27.
26. Y. Chen, X. Xu, and M. Zhang, "Blockchain for secure and efficient data sharing in industrial IoT," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4156–4165, 2020, doi: 10.1109/TII.2020.2988551.
27. M. Swan, Blockchain: Blueprint for a New Economy (2nd Edition), O'Reilly Media, 2018.
28. M. Ali, R. Dhamija, and A. Benslimane, "Scalable blockchain for IoT applications," in Proceedings of the ACM SIGCOMM Workshop on Blockchain for IoT, 2019, pp. 21–26, doi: 10.1145/3356250.3356251.
29. W. Wang and D. T. Hoang, "Blockchain-based supply chain and logistics for the IoT industry," IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3562–3571, 2019, doi: 10.1109/TII.2019.2940201.
30. S. Huh, J. Kim, and S. Kim, "Managing IoT devices with blockchain platform," in Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT), 2017, pp. 464–467, doi: 10.23919/ICACT.2017.7890132.

31. X. Xu, L. Chen, and Y. Wang, "Exploring blockchain for trusted industrial IoT applications," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7596–7608, 2019, doi: 10.1109/JIOT.2019.2912296.
32. G. O. Karame and E. Androulaki, Bitcoin and Blockchain Security, Artech House, 2016.
33. N. Kshetri, "Blockchain's roles in meeting key supply chain management objectives," International Journal of Information Management, vol. 39, pp. 80–89, 2018, doi: 10.1016/j.ijinfomgt.2017.12.005.
34. K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
35. P. Zhang, X. Zhang, and M. H. Khan, "Blockchain technology use cases in healthcare, aerospace, and defense," in Proceedings of the International Conference on Digital Innovation in Healthcare and Aerospace, 2018, pp. 151–160.
36. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond Bitcoin," Applied Innovation Review, vol. 2, pp. 6–19, 2016.
37. E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in Proceedings of the Thirteenth EuroSys Conference, Apr. 2018, pp. 1–15, doi: 10.1145/3190508.3190538.
38. X. Xu, C. Pautasso, and L. Zhu, "A taxonomy of blockchain-based systems for architecture design," in Proceedings of the IEEE International Conference on Software Architecture (ICSA), 2016, pp. 243–252, doi: 10.1109/ICSA.2016.30.
39. S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," SIAM Journal on Computing, vol. 18, no. 1, pp. 186–208, 1989, doi: 10.1137/0218012.
40. E. Ben-Sasson and A. Chiesa, "Scalable transparent arguments of knowledge," Journal of Cryptology, vol. 32, no. 2, pp. 484–541, 2019, doi: 10.1007/s00145-018-9283-2.