MilChain: A Blockchain Network for Military Communication

Ikechi Saviour Igboanusi [1] and Dong-Seong Kim [*2]

[1]ICT Convergence Research Center, Kumoh National Institute of Technology, South Korea
[2]Department of IT Convergence Engineering, Kumoh National Institute of Technology, South Korea
(ikechisaviour, dskim)@kumoh.ac.kr

***Abstract*—This paper proposes MilChain, a permissioned blockchain network based on Hyperledger Besu, designed to enhance military communication and coordination within coalitions like NATO. MilChain addresses challenges related to trust, data integrity, and operational coordination by providing a secure, scalable, and interoperable infrastructure. The network incorporates a novel consensus mechanism, PoA^3, which integrates AI and PoA^2 for improved security and miner behavior, along with Smart Auto Mining (SAM) to increase mining efficiency. Performance evaluations demonstrate MilChain's potential to reduce storage overhead, improve energy efficiency, and ensure resilience in dynamic and contested environments.**

***Index Terms*—AI, Blockchain, consensus, MilChain, military network, security**

I. Introduction

Modern warfare's reliance on digital technologies presents significant challenges for coalitions like NATO, particularly regarding trust, data integrity, and operational coordination across diverse, sovereign networks [1], [2]. Adversarial threats and contested cyberspace further complicate this landscape [3]. Blockchain technology is being explored for military communications within NATO [4]–[6], offering potential benefits like immutability and decentralized trust [7]. However, existing proposals often lack practical suitability for large-scale coalition operations [8], [9], and there is no public confirmation of a fully implemented NATO-wide blockchain network. This work can inform proposals for new or improved blockchain systems for member states.

To address these challenges, this paper proposes *MilChain*, a permissioned blockchain network based on Hyperledger Besu, tailored for NATO-member military communication. MilChain is envisioned as a secure, scalable infrastructure for command dissemination, asset tracking, intelligence sharing, and policy enforcement. Hyperledger Besu's Ethereum compatibility and flexible consensus algorithms suit private defense environments requiring low latency and granular control [10].

Prior work on blockchain for military applications [11]–[13] highlights persistent gaps that MilChain aims to resolve:

1 Lightweight Consensus: Existing protocols (e.g., PoW) are often too resource-intensive for tactical nodes. MilChain leverages Hyperledger Besu's customizable PoA consensus for efficiency [14], [15].
2 Scalability: Edge IoBT networks face data saturation. MilChain uses parallel transaction execution and caching to support dynamic scaling, crucial for applications like unmanned reconnaissance coordination [7], [15].
3 Interoperability Access Control: Multinational coalitions require granular control across diverse security domains. MilChain implements attribute-based access control compatible with zero-trust principles [16], [17].
4 Real-time Smart Contracts: Many proposals lack low-latency execution for mission-critical tasks. MilChain integrates priority handling and hybrid triggers for time-sensitive logic [13], [18].
5 Cyber Resilience: Nodes are vulnerable in contested environments. MilChain adopts a blockmesh approach with localized verification and rotating validators to enhance continuity [16].

Building on prior research into secure battlefield IoT, drone communication, and NATO standards [12], [17]–[19], this work seeks to provide a unified, adaptable platform. Our objectives are to: 1) Propose the MilChain architecture tailored for coalition needs; 2) Design a novel consensus algorithm optimized for military constraints; and 3) Implement a validating prototype system.

Section 2 details MilChain's architecture and implementation. Performance evaluation is presented in Section III. Section IV concludes with discussions on implications, results, and future directions.

II. System Model

The use of blockchain for military purposes, although considered extensively, has not had a lot of instances of integration across an entire country's communication infrastructure. For instance, the Army, the Navy, the Air Force and any other relevant group can connect to the same blockchain network and share general information throughout the network to all the participants. However, information made of a specific group is shared through a private channel that only the member of

that channel can access the information. A military network is expected to be secure, have low latency, handle a large volume of transactions, and be light to accommodate military IoT devices. To achieve this, this model proposes the use of a modified version of a consortium blockchain network based on Hyperledger Besu, a new consensus algorithm and an efficient mining mechanism.

A. Blockchain network setup

Our system model leverages the inherent strengths of blockchain technology, employing a decentralized and distributed ledger architecture that operates across a peer-to-peer network of interconnected nodes. At the heart of this architecture lies a chain of blocks, each meticulously containing a batch of transactions secured through cryptographic hashing and timestamping. This chronological and cryptographically enforced linkage, typically employing hashing algorithms, guarantees the immutability and data integrity that are fundamental to the system's trustworthiness. To ensure agreement on the state of this distributed ledger and to validate new transaction entries, our model incorporates a robust consensus mechanism. Specifically, our system model utilizes the Clique Proof-of-Authority (PoA) consensus algorithm [20]. This choice is particularly well-suited for our permissioned network environment, where participant identities are known and a degree of trust exists among them.

Building upon this foundational blockchain layer, our system model is implemented using Hyperledger Besu [21], an open-source, enterprise-grade Ethereum client developed in Java. Besu's adherence to the Enterprise Ethereum Alliance (EEA) specification [22] ensures seamless interoperability and standardization within our enterprise blockchain solution. The modular design of Besu allows for the flexible integration and upgrading of essential blockchain functionalities, with the Clique consensus algorithm being a key component in our deployment. Clique operates as a Proof-of-Authority mechanism, where a set of authorized nodes, known as signers, take turns proposing and validating new blocks. This approach offers a balance between security and efficiency in permissioned settings, providing fault tolerance while maintaining relatively low computational overhead compared to Proof-of-Work systems. While Clique does not offer immediate finality, its resilience and suitability for environments with known participants make it a pragmatic choice for our system model.

Beyond the consensus mechanism, Hyperledger Besu provides a rich set of enterprise-focused features that are integral to our system model. We utilize Besu's sophisticated permissioning system to exert fine-grained control over network participation, ensuring that only authorized nodes and accounts can interact with the ledger. Furthermore, for sensitive data handling within our system, Besu's support for private transactions allows for confidential exchanges between specific parties. Fig. 1 shows how a private transaction can be made in the

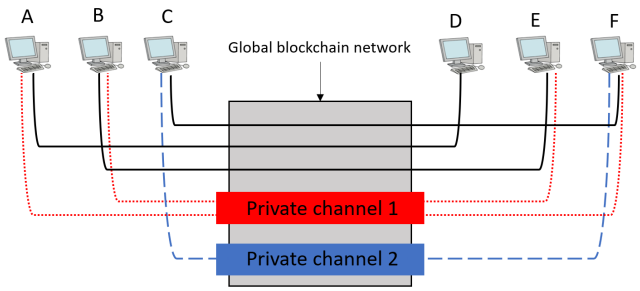

Fig. 1: A diagram of a private channel in a blockchain network

proposed network through the private channel. The efficient RocksDB key-value database underpins Besu's storage layer, ensuring reliable and performant data persistence. Communication between nodes within our network is facilitated by Ethereum's devp2p protocols, tailored to accommodate the specifics of the Clique consensus algorithm. To enable seamless integration with existing infrastructure and development tools, our system model exposes standard Ethereum and EEA JSON-RPC APIs over HTTP and WebSocket. Monitoring and performance analysis are facilitated through Besu's support for Prometheus, allowing us to maintain optimal system operation. The compatibility of Hyperledger Besu with the Ethereum Virtual Machine (EVM) [23] is also crucial, as it enables the deployment and execution of smart contracts written in Solidity, allowing for the automation of business logic and the creation of sophisticated decentralized applications within our enterprise ecosystem.

B. Proposed Blockchain Network Architecture

The MilChain blockchain network is engineered for high performance, robust security, and efficiency through the integration of cutting-edge blockchain features. The complete network architecture is visually depicted in Figure 2.

Users engage with the MilChain network through an Application Programming Interface (API), which acts as a secure entry point to the Blockchain network. This network consists of two primary node types: Miner nodes and Light nodes (IoT nodes). Miner nodes play a crucial role in validating transactions and appending new blocks to the blockchain, thereby maintaining the network's integrity. In contrast, Light nodes maintain a streamlined view of the blockchain, enabling them to efficiently query data and submit transactions. Both node types possess the capability to interact with the network.

At the core of the network reside Smart Contracts. These are self-executing agreements whose terms are directly encoded within them. Smart contracts can interact with miner nodes, light nodes, Oracles/External APIs, and the Ledger (Blockchain DB), the permanent and immutable record of all network transactions. Conversely, both miner and light nodes can trigger the execution of smart contracts and retrieve rele-

vant information. To extend the capabilities of smart contracts beyond the blockchain itself, Oracles/External APIs provide a conduit for real-world data integration. This allows smart contracts to react to and utilize information originating from external sources.

To optimize network operations, the system incorporates Smart Auto Mining. This feature automates the mining process, likely triggered by the presence of pending transactions within the network [24].

The network employs a sophisticated consensus mechanism denoted as PoA^3, which stands for Proof-of-Authority, Association, and AI. This mechanism leverages AI, a PoA² inactive node detection system [25], and a foundational PoA consensus algorithm to ensure network agreement. The PoA² component utilizes input from AI anomaly detection to identify and flag potentially malicious activities that could compromise the consensus process. The output of this anomaly detection and inactive node detection feeds into the overarching PoA consensus mechanism, ultimately safeguarding the integrity and security of the Ledger (Blockchain DB).

C. Genesis block

The genesis block configuration serves as the foundational blueprint for the entire MilChain network. It defines the initial state and core parameters that govern the blockchain's operation from its very inception. This crucial block typically includes a unique hash identifying it as the first block, and an initial nonce value. In the context of MilChain's PoA^3 consensus mechanism, the genesis block is paramount in establishing the initial set of trusted authority nodes responsible for validating transactions. Furthermore, it enshrines the starting parameters for the consensus algorithm, including any initial settings. If the network utilizes a native token, the genesis block could also dictate its initial allocation. In essence, the configuration of the genesis block acts as the immutable seed from which the entire MilChain blockchain and its subsequent evolution originate. The blockchain genesis block configuration is below.

```
{
  "config":0 {
    "chainId":0 1337,
    "homesteadBlock":0 0,
    "eip150Block":0 0,
    "eip155Block":0 0,
    "eip158Block":0 0,
    "byzantiumBlock":0 0,
    "constantinopleBlock":0 0,
    "petersburgBlock":0 0,
    "istanbulBlock":0 0,
    "muirGlacierBlock":0 0,
    "berlinBlock":0 0,
    "londonBlock":0 0,
    "zeroBaseFee":0 true,
    "clique":0 {
      "period":0 1,
      "epochlength":0 30000
    }
  },
  "difficulty":0 "0x1",
  "extraData":0 "0x0000000000000000000000000000000000000000
      000000000000000000000000000000<VALIDATOR_ADDRE
      SS_1>000000000000000000000000000000000000000000
      0000000000000000000<VALIDATOR_ADDRESS_2>00
      000000000000000000000000000000000000000000000000
      00000000000000",
  "gasLimit":0 "0x7fffffffffffffff",
  "mixHash":0 "0x0000000000000000000000000000000000000000
      0000000000000000000000000000",
  "nonce":0 "0x0000000000000000",
  "parentHash":0 "0x0000000000000000000000000000000000000000
      0000000000000000000000000000",
  "timestamp":0 "0x0",
  "alloc":0 {
    "<ACCOUNT_ADDRESS_1>":0 { "balance":0 "0xffffffff
        ffffffffffffffffffffffffffffffffffffffffffffffff
        fffffffff" },
    "<ACCOUNT_ADDRESS_2>":0 { "balance":0 "0xffffffff
        ffffffffffffffffffffffffffffffffffffffffffffffff
        fffffffff" }
    // Addmore pre-funded accounts as needed
  }
}
```

1) What Makes This Code Efficient for a Network Focused on Speed and Capacity:

1) **Clique Proof-of-Authority (PoA):** PoA is inherently more efficient for private or consortium networks compared to Proof-of-Work. Block creation is controlled by a set of pre-approved validators, eliminating the need for energy-intensive mining. This leads to faster and more predictable block times.

2) **Short Block Period (`period: 1 second`):** Setting a very short block period of 1 second directly contributes to a low block time, meaning transactions can be included in a block and confirmed much faster than on networks with longer block times.

3) **Zero Base Fee (`zeroBaseFee: true`):** Disabling the base fee mechanism makes transactions effectively free in terms of gas costs. This can significantly increase the willingness to transact and simplifies the transaction process, as users don't need to worry about gas prices.

4) **Extremely High Gas Limit (`gasLimit`):** A very high gas limit allows for a larger number of transactions, or transactions that consume more computational resources, to be included in each block. This directly translates to a higher transaction throughput (more transactions processed per second) and thus greater network capacity.

5) **Pre-allocation of Funds (`alloc`):** Pre-funding accounts in the genesis block streamlines the initial setup and testing phases. Participants have Ether available immediately to interact with smart contracts or send transactions without needing to mine or acquire funds through other means.

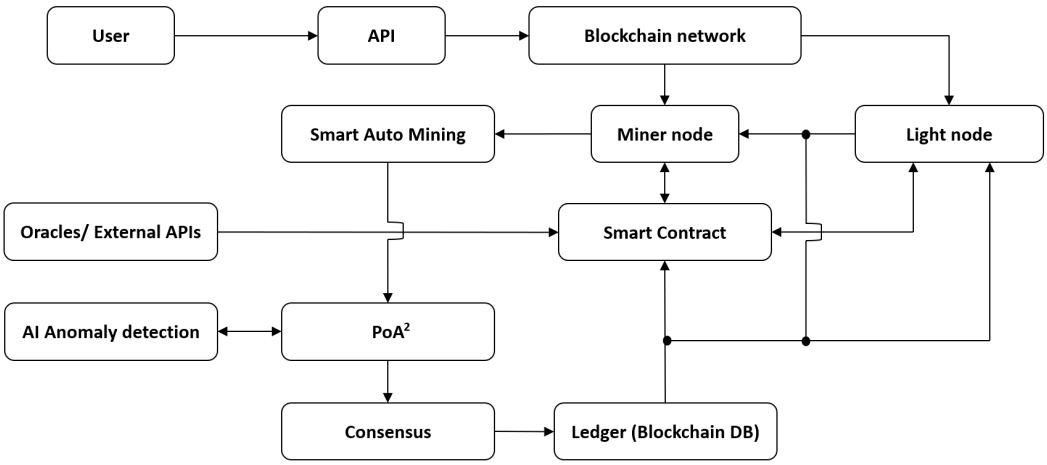

Fig. 2: A diagram of the Milchain blockchain network

6) **Latest Protocol Features Activated (`homesteadBlock: 0, ..., londonBlock: 0`):** By activating all the latest Ethereum protocol upgrades from the beginning, your private network benefits from the most recent performance improvements and features available in the Ethereum ecosystem.

While these Genesis block settings optimize for speed and capacity in a controlled environment, there is a need for resource efficiency and high security.

D. Efficiency

The Smart Auto Mining (SAM) model introduces a resource-efficient approach to blockchain mining, particularly beneficial for Internet of Things (IoT) network environments that include resource-constrained devices. The core idea is to automate the mining process dynamically based on transaction activity [24].

In traditional blockchain systems, miners continuously participate in the mining process, regardless of whether there are transactions to be processed. This leads to the creation of empty blocks, which consumes energy and computational resources without contributing to the network's transaction processing capacity. These empty blocks also occupy storage space over time and consume network bandwidth as they are distributed across the network.

MilChain addresses these inefficiencies by adopting SAM which enable miners to listen to the network for transaction requests and to start the mining process only when there is at least one pending transaction. Once all pending transactions are mined, the mining process is stopped. This on-demand mining approach minimizes the creation of empty blocks, leading to a reduction in energy consumption, computational overhead, storage usage, and network bandwidth.

E. PoA^3PoA3 consensus for Consortium Blockchain network

This MilChain blockchain network has the Cliuqe PoA as its basic consenstus algorithm, but there are the addition of PoA^2 an idle miner replacement mechanism and AI for anomaly detection.

1) Clique Proof-of-Authority (PoA): consensus mechanism, prominently featured in the Go Ethereum (geth) client and specifically tailored for the operational needs of permissioned blockchain environments. Within a Clique network, a pre-defined and limited group of trusted nodes, designated as signers or authorities, collaboratively manage the blockchain by sequentially proposing and validating new blocks of transactions. The privilege of block creation is typically distributed among these authorized participants through a deterministic process, often following a predictable round-robin schedule, ensuring a fair and orderly progression of the blockchain.

A distinguishing characteristic of the Clique algorithm lies in its integrated voting system, which empowers the existing set of signers to actively participate in the network's governance. Through this mechanism, authorized nodes can initiate proposals and cast votes on critical decisions, such as the inclusion of new reputable entities as signers or the removal of existing ones that may no longer be trusted or are underperforming. This built-in governance framework allows the network to adapt and evolve its set of authorities in a controlled manner. While Clique offers advantages in terms of transaction throughput and significantly lower computational demands compared to energy-intensive Proof-of-Work (PoW) algorithms, its security and overall resilience are fundamentally dependent on the integrity and continued trustworthiness of the carefully selected set of authorized signers.

2) PoA^2 idle miner replacement mechanism: To address the challenges of applying blockchain technology in IoT networks, we employ a novel consensus mechanism called Proof-of-

Authority-and-Association (PoA^2). PoA^2 is designed to enhance the efficiency and reliability of blockchain operations within consumer IoT applications.

Our PoA^2 model builds upon the Proof of Authority (PoA) consensus algorithm by introducing an association verification process and a redundancy mechanism. In PoA, a set of authorized nodes, known as signers, validate transactions and create new blocks. PoA^2 extends this by ensuring that each signer's authority is associated with their validated transactions, adding an extra layer of accountability.

Furthermore, PoA^2 incorporates redundant standby signers that monitor the activity of active signers. If a signer becomes inactive or exhibits abnormal behavior, the PoA^2 algorithm automatically triggers the replacement of that signer with a standby signer. This dynamic replacement mechanism ensures continuous network operation and improves fault tolerance.

F. AI for anomaly detection

Inactivity of miners is a fault in a blockahin network based on Clique PoA consensus; however, this is not the only anomaly that can occur. An abnormal miner could also ignore Smart Auto Mining, include invalid transactions in the block, etc. Since there are many anomalous behaviors and new ones could be discovered in the future, an AI anomaly detection model is used to identify potential traits in the blockchain network, and any compromised miner in the process is removed.

To enhance the resilience of the MilChain blockchain network against a spectrum of anomalies, we propose a hybrid AI model that combines the strengths of time-series analysis and supervised learning. This model is designed to detect deviations from normal miner behavior and identify patterns indicative of malicious activity. By integrating these two approaches, we aim to create a robust and adaptive anomaly detection system that can effectively safeguard the network's integrity.

The first component of our hybrid model employs time series analysis to establish a baseline of normal miner behavior. LSTM algorithm continuously monitor networks key performance indicators, including block creation timestamps, transaction inclusion rates, and SAM execution metrics. Deviations from these established patterns are quantified as anomaly scores, providing a measure of how much a miner's behavior has diverged from its typical operation.

In parallel, a supervised learning component is utilized to detect known attack vectors. A Support Vector Machine classification model is trained on a labeled dataset comprising both normal behavior and examples of specific attack scenarios. This model calculates the probability that a miner is exhibiting a particular type of malicious activity. By combining the anomaly score from the time series analysis with the attack probability from the supervised learning model, our hybrid approach provides a comprehensive assessment of miner behavior, enabling the identification and isolation of anomalous nodes.

III. RESULTS

A. Improvement by integrating Smart Auto Mining (SAM)

The performance of Smart Auto Mining (SAM) within a Proof of Authority (PoA) framework was assessed. SAM enhances efficiency by initiating mining only when transactions are pending and stopping when the queue is clear, thus preventing empty block generation.

Experiments on a private Ethereum network showed SAM significantly reduces unnecessary block creation. Over 12 hours without transactions, standard PoA generated 4934 blocks. SAM, activating only upon transaction events, drastically curtailed this.

This reduction directly impacts storage efficiency. Table I shows that processing 599,950 transactions over 12 hours required 112.2 MB storage with standard PoA (including overhead from empty blocks) versus only 83.5 MB with SAM. By eliminating empty block mining, SAM optimizes resources, inherently reducing the energy consumption and network bandwidth associated with creating and propagating superfluous blocks.

TABLE I: Performance Comparison of MilChain Network with and without SAM (12-hour duration, 599,950 transactions)

Metric	Standard PoA	SAM
Blocks Generated	4934	1022
Storage Consumption	112.2 MB	83.5 MB

B. Improvement by integrating PoA^2

1) Performance Evaluation of PoA^2: The PoA^2 consensus algorithm was tested in a simulated network of six Ethereum nodes (3 signers, 1 redundant signer, 2 ordinary nodes). Signer activity was monitored using the `protocol_signer` RPC method, where a `sealerActivity` of 0 identifies inactive signers. The PoA^2 algorithm successfully detected inactive signers and initiated their replacement with the designated redundant signer, demonstrating its fault tolerance mechanism.
2) Energy Consumption Analysis: Energy efficiency gains with PoA^2 were notable. An active signer node consumed 637 watt-hours over 10 minutes while mining. In contrast, a redundant standby node (operating as a full node but not mining) consumed only 157 watt-hours in the same period. This indicates that active mining nodes under this setup require over four times the energy compared to redundant standby nodes, highlighting the energy savings achieved when nodes are in a non-mining standby state.

IV. Conclusion

This paper introduced MilChain, a blockchain network designed for military coalition communications (e.g., NATO) using Hyperledger Besu. Key innovations, the PoA^3 consensus (integrating AI and PoA^2 for reliable signer behavior) and Smart Auto Mining (SAM for mining efficiency), address critical defense network challenges in scalability, efficiency, security, and responsiveness.

Performance evaluations demonstrated MilChain's ability to significantly reduce storage overhead, enhance energy efficiency, and maintain operational continuity. This resilient framework, adaptable to tactical scenarios, stems from its layered consensus and intelligent automation.

Future work will focus on optimizing the AI anomaly detection, scaling deployment, ensuring cross-domain interoperability, and integrating with emerging military standards. MilChain establishes a foundation for secure, decentralized, and efficient command and control systems for future digital warfare scenarios.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of IITP grant funded by the Korean government(MSIT) (IITP-2024-2020-0-01612, 50%) and by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003, 50%)

References

[1] R. Bielawski, "Development of security technologies by nato: Current status and development prospects," *Safety & Defense*, vol. 8, no. 1, 2022. [Online]. Available: https://doi.org/10.37105/sd.170

[2] S. Lucarelli, A. Marrone, and F. N. Moro, Eds., *NATO Decision-Making in the Age of Big Data and Artificial Intelligence*. NATO Allied Command Transformation, 2021.

[3] C. Chromyszak, S. Jacobson, E. Khosraw, S. Lavey, M. Lewis, S. Mabe, A. Olsen, C. Ryals, K. Sahagun, I. Williamson, and S. Winstead, "Navigating new threats: Nato's posture on emerging technologies," Henry M. Jackson School of International Studies, University of Washington, Tech. Rep. Task Force Report Winter 2022, March 2022, faculty Advisor: Dr. Sarah Lohmann.

[4] N. Kostopoulos, Y. C. Stamatiou, C. Halkiopoulos, and H. Antonopoulou, "Blockchain applications in the military domain: A systematic review," *Technologies*, vol. 13, no. 1, 2025. [Online]. Available: https://www.mdpi.com/2227-7080/13/1/23

[5] A. Cornella, L. Zamengo, A. Delepierre, and G. Clementz, "Blockchain in defence: A breakthrough?" https://www.finabel.org, 2020, finabel Food for Thought Paper, European Army Interoperability Centre.

[6] J. Álvaro González, A. M. S. García, and V. M. Baeza, "Blockchain-enabled management framework for federated coalition networks," 2025. [Online]. Available: https://arxiv.org/abs/2503.09666

[7] D. K. Tosh, S. Shetty, P. Foytik, L. Njilla, and C. A. Kamhoua, "Blockchain-empowered secure internet-of-battlefield things (iobt) architecture," in *2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 2018, pp. 593–598.

[8] V. S. Sokolović and G. B. Marković, "Internet of things in military applications," *Vojnotehnički glasnik / Military Technical Courier*, vol. 71, no. 4, pp. 1148–1171, 2023. [Online]. Available: https://doi.org/10.5937/vojtehg71-46785

[9] R. Kufakunesu, H. Myburgh, and A. D. Freitas, "The internet of battle things: a survey on communication challenges and recent solutions," *Discover Internet of Things*, vol. 5, no. 3, pp. 1–22, 2025.

[10] P. Praitheeshan, L. Pan, and R. Doss, "Private and trustworthy distributed lending model using hyperledger besu," *SN Computer Science*, vol. 2, no. 115, 2021.

[11] M. Golam, R. Akter, R. Naufal, V.-S. Doan, J.-M. Lee, and D.-S. Kim, "Blockchain inspired intruder uav localization using lightweight cnn for internet of battlefield things," in *2022 IEEE Military Communications Conference (MILCOM)*. IEEE, 2022, pp. 342–348.

[12] X. Liang, J. Zhao, S. Shetty, and D. Li, "Towards data assurance and resilience in iot using blockchain," in *2017 IEEE Military Communications Conference (MILCOM)*. IEEE, 2017, pp. 261–266.

[13] C. Maracchion, T. Woods, S. Furman, and A. L. Drozd, "The role of private blockchain architectures and smart contracts for decentralized 5g militarized networks," in *2022 IEEE Military Communications Conference (MILCOM)*. IEEE, 2022, pp. 535–540.

[14] E. D. Buenrostro, A. O. Gomez Rivera, D. Tosh, J. C. Acosta, and L. Njilla, "Evaluating usability of permissioned blockchain for internet-of-battlefield things security," in *2019 IEEE Military Communications Conference (MILCOM)*. IEEE, 2019, pp. 841–846.

[15] A. O. Gomez Rivera, D. K. Tosh, and L. Njilla, "Scalable blockchain implementation for edge-based internet of things platform," in *2020 IEEE Military Communications Conference (MILCOM)*. IEEE, 2020, pp. 342–347.

[16] J. Luo and A. Velazquez, "Blockmesh data security and trust framework for tactical networks," in *2024 IEEE Military Communications Conference (MILCOM)*. IEEE, 2024, pp. 536–541.

[17] K. Wrona and M. Jarosz, "Does nato need a blockchain?" in *2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 2018, pp. 667–672.

[18] E. Bandara, S. Shetty, A. Rahman, and R. Mukkamala, "Let'strace—blockchain, federated learning and tuf/in-toto enabled cyber supply chain provenance platform," in *2021 IEEE Military Communications Conference (MILCOM)*. IEEE, 2021, pp. 470–476.

[19] P. Menegay, J. Salyers, and C. Griffin, "Secure communications using blockchain technology," in *2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 2018, pp. 599–604.

[20] "Clique proof-of-authority consensus algorithm," description of the Clique consensus mechanism used in permissioned blockchain networks.

[21] "Hyperledger besu documentation," Hyperledger, official documentation for the Hyperledger Besu Ethereum client. [Online]. Available: https://besu.hyperledger.org/

[22] "Enterprise ethereum alliance specification," Enterprise Ethereum Alliance, specification outlining standards for enterprise Ethereum implementations. [Online]. Available: https://entethalliance.org/

[23] "Ethereum virtual machine (evm)," Ethereum Foundation, documentation on the Ethereum Virtual Machine and its functionality. [Online]. Available: https://ethereum.org/en/developers/docs/evm/

[24] I. S. Igboanusi, A. Allwinnaldo, R. N. Alief, M. R. R. Ansori, J.-M. Lee, and D.-S. Kim, "Smart auto mining (sam) for industrial iot blockchain network," *IET Communications*, vol. 16, no. 18, pp. 2123–2132, 2022. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/cmu2.12465

[25] D.-S. Kim, I. S. Igboanusi, L. A. Chijioke Ahakonye, and G. O. Anyanwu, "Proof-of-authority-and-association consensus algorithm for iot blockchain networks," in *2025 IEEE International Conference on Consumer Electronics (ICCE)*, 2025, pp. 1–6.