

PAPER

A Mobile Edge Computing and Blockchain Framework for Secure Cross-Island Critical Mineral Traceability

Musran Munizu¹  ,
Suraya Ainun Lestari¹ ,
Muhammad Asdar¹ ,
Adeel Akmal² ,
Danial Kasim¹ 

¹Hasanuddin University,
Makassar, Indonesia

²University of Iceland,
Reykjavík, Iceland

musran@fe.unhas.ac.id

ABSTRACT

Cloud-based traceability systems depend on continuous connectivity, limiting their reliability in geographically dispersed mineral supply chains where prolonged network outages may occur. This study proposes an offline-first architecture integrating Mobile Edge Computing (MEC) with a permissioned blockchain for secure cross-island critical-mineral traceability. Traceability events generated at mines, transport routes, ports, vessels, warehouses, and processing facilities are locally validated, digitally signed, encrypted, and queued at MEC gateways during connectivity loss before synchronization with the blockchain. The framework was evaluated using 12,384 synthetic traceability events derived from a critical-minerals dataset and six simulated attack categories. After a 24-hour outage, the proposed framework maintained 98.7% record completeness compared with 58.2% for the cloud-only baseline. It achieved an average attack-detection rate of 98.5% and reduced post-outage synchronization delay from 466 sec to 185 sec. These findings demonstrate the potential of an offline-first MEC blockchain architecture to improve traceability continuity, tamper detection, and shared verification in critical-mineral supply chains operating under intermittent connectivity.

KEYWORDS

mobile edge computing (MEC), permissioned blockchain, critical-mineral traceability, offline-first architecture, mobile logistics

1 INTRODUCTION

The transition toward low-carbon technologies is increasing demand for critical minerals such as nickel, lithium, cobalt, copper, graphite, and rare-earth elements (REEs), which are essential to electric vehicles, battery storage, renewable-energy systems, and related technologies [1]. Consequently, reliable traceability of mineral origin, movement, custody, and processing is increasingly important for responsible sourcing, regulatory compliance, and supply-chain resilience. Critical-mineral traceability is particularly challenging across geographically dispersed supply chains. In Indonesia, for example, mineral production and processing may span remote mines,

Munizu, M., Lestari, S. A., Asdar, M., Akmal, A., Kasim, D. (2026). A Mobile Edge Computing and Blockchain Framework for Secure Cross-Island Critical Mineral Traceability. *International Journal of Interactive Mobile Technologies (iJIM)*, 20(19), pp. 103–116. <https://doi.org/10.3991/ijim.v20i19.63193>

Article submitted 2026-06-12. Revision uploaded 2026-08-20. Final acceptance 2026-08-20.

© 2026 by the authors of this article. Published under CC-BY.

storage facilities, island ports, vessels, smelters, and export terminals. Multiple operators and information systems create risks of delayed, duplicated, incomplete, or manipulated records [2]. These risks are amplified by unreliable connectivity at remote mines, vessels, and small ports [3]. Cloud-based traceability systems generally depend on network access to transmit field data to centralized servers; prolonged outages can therefore create gaps between physical mineral movements and their digital records, weakening auditability and custody verification [4]. Mobile Edge Computing (MEC) can reduce this dependence by processing, validating, and temporarily storing traceability events near their source [5]. MEC gateways can capture operational information from sensors, identification systems, mobile applications, and authorized operators [6]. However, centralized edge or cloud storage alone may not provide sufficient shared trust among independent actors such as miners, transport operators, ports, processors, auditors, and regulators [7]. Permissioned blockchain can enhance Multi-access Edge Computing (MEC) by enabling distributed verification, digital identities, cryptographic signatures, and smart contract-based transaction validation. However, blockchain technology does not ensure the accuracy of source data [8], and many blockchain-based traceability solutions presuppose continuous connectivity.

While prior research has explored blockchain-based supply chain traceability, IoT monitoring, and edge computing [9], [10], there has been limited focus on offline-first integration of MEC and permissioned blockchain for cross-island critical mineral logistics during extended connectivity disruptions. This gap constitutes the primary research focus of the present study.

This study develops and evaluates an offline-first MEC blockchain framework designed to capture and validate mineral traceability events locally during network outages. The framework preserves event integrity using hashing, digital signatures, and encrypted storage. Upon restoration of connectivity, it synchronizes and verifies queued events through a permissioned blockchain. Evaluation metrics include record completeness, synchronization performance, transaction processing, resource utilization, and detection of simulated security attacks.

2 LITERATURE REVIEW

Security, trust, and processing efficiency are major challenges in distributed systems, and solutions such as MEC and blockchain are gaining traction to address these challenges [11]. MEC processes information close to its source, minimizing the delay in information communication and reliance on centralized cloud platforms. Edge devices, however, still can be accessed, tampered with, and compromised, and the cryptographic keys can be stolen. MEC systems have been suggested using blockchain to secure the communication between the edge devices and enhance trust in industrial IoT systems [12]. Inaccuracy of data is not a problem because it will not be reliable even if it is written on a blockchain. Other research has thus found ways to attest to data generated on the edges, detect storage errors, and secure distributed data from unauthorized modification [13].

Blockchain-based solutions can help in the generation, distribution, renewal, and revocation of keys [12]. To keep such sensitive data conveyed between the edge and blockchain system safe [14], privacy-preserving techniques have been implemented. Earlier research has demonstrated how blockchain can be utilized to address the business challenges of mineral provenance, responsible sourcing, transparency in operations, safety, regulation, and coordination of supply chain actors [15]. A distributed ledger could serve as a shared ledger for mining companies,

transport operators, port authorities, protein processors, auditors, and regulators to keep mineral-related transactions [8] [16]. Blockchain is employed to support responsible cobalt sourcing and prove mineral-origin [13]. There are also a number of proposals to use DLT and IoT-based systems to enhance transparency, sustainability, and inspection efforts in the mining industry [6], [17]. To ensure the authenticity of the data from the mining enterprises, blockchain can be linked with digital watermarking [4].

In coal mining, Consortium blockchain is used for security and information sharing applications [18]; In access control and mining-related transactions, smart contractors used for IoT applications [19] [20]. In terms of the security area, related topics involving zero-trust architectures, artificial intelligence, explainable threat detection, and optimization techniques to boost threat detection performance and scalability were investigated [7, 9, 10]. The research of Blockchain and MEC has also been explored in mobile and aerial networks in which the communication conditions vary [20].

To summarize, the existing studies validate the use of the MEC for local processing and temporary storage and the blockchain for data integrity and trust, access control, transparency, and traceability. There is, however, little research that merges all of these attributes (limited to offline-first edge processing, permissioned blockchain synchronization, cryptographically attached local records, replay detection, duplicate prevention, and custody validation) into one package for critical-mineral transportation between islands. A framework of MEC-blockchain, therefore, needs to be offline-first so as to be able to ensure a secure capture of the mineral events in disconnected areas and synchronization with the shared ledger when connectivity has been reestablished.

3 RESEARCH METHODOLOGY

3.1 Architecture of the proposed MEC–blockchain traceability framework

The proposed architecture integrates MEC with a permissioned blockchain for secure, offline-first critical-mineral traceability across geographically dispersed locations (see Figure 1). Traceability events from mines, transport routes, ports, vessels, warehouses, and processing facilities are captured from authorized users and devices, including GPS, sensors, QR/RFID systems, and mobile applications. Key attributes include batch identity, mineral type, origin, weight, location, timestamp, custody, and destination. MEC gateways locally validate and store events during connectivity loss before blockchain synchronization [1], [2]. Validation checks required fields, participant identity, event sequence, custody status, duplicates, and anomalous entries.

Once validated, each event receives a unique identifier and sequence number, is digitally signed, and is cryptographically linked to the preceding event to support tamper detection [11], [14]. Events remain locally stored with a defined synchronization status until blockchain confirmation. When connectivity is restored, the MEC gateway authenticates with the permissioned blockchain and submits queued events sequentially. The system checks for duplicate, replayed, out-of-sequence, and custody-conflicting transactions; valid events are recorded on the ledger, while invalid events are flagged for review [18], [19].

3.2 Cross-island supply-chain scenario and system actors

The proposed framework involves mineral batch transport across the Island starting at remote mining locations to ports, vessels, storage facilities, and

processing facilities. Each mineral batch (1) is given a specific mineral type, mineral origin, mineral creation time, and specific operator identification number at the mining site:

$$B_i = H(M_i || L_i || T_i || O_i) \quad (1)$$

Each will take the form of (B_i) for the batch identifier, (M_i) for the type of mineral, (L_i) for the location source, (T_i) for the date created, (O_i) for the operator performing the action, and (H) for an encryption hash function. The whole trip of a batch (2) can be represented as:

$$P(B_i) = \{S_1, S_2, \dots, S_n\} \quad (2)$$

The movement of batch (B_i) in the supply chain is represented by ($P(B_i)$), and the different stages of supply chain are represented by (S_1), (S_2), ..., (S_n). A representation of a custody-transfer event (3) is:

$$C_i = \{B_i, A_s, A_r, T_i, L_i, S_s, S_r\} \quad (3)$$

The (A_s) and (A_r) represent the actors who send and receive the message, and digital signatures (S_s) and (S_r) are used for their respective actors. The synchronization status (4) is given as:

$$\text{Sync}(E_i) = \begin{cases} 1, & \text{if network connectivity is available} \\ 0, & \text{if the gateway is offline} \end{cases} \quad (4)$$

If the value is set to zero, then the event will be left in the local transaction queue. The set of system access rules (5) controlled the access to the system:

$$\text{Access}(A_j, R_k) = \begin{cases} 1, & \text{if actor } A_j \text{ is authorized for role } R_k \\ 0, & \text{otherwise} \end{cases} \quad (5)$$

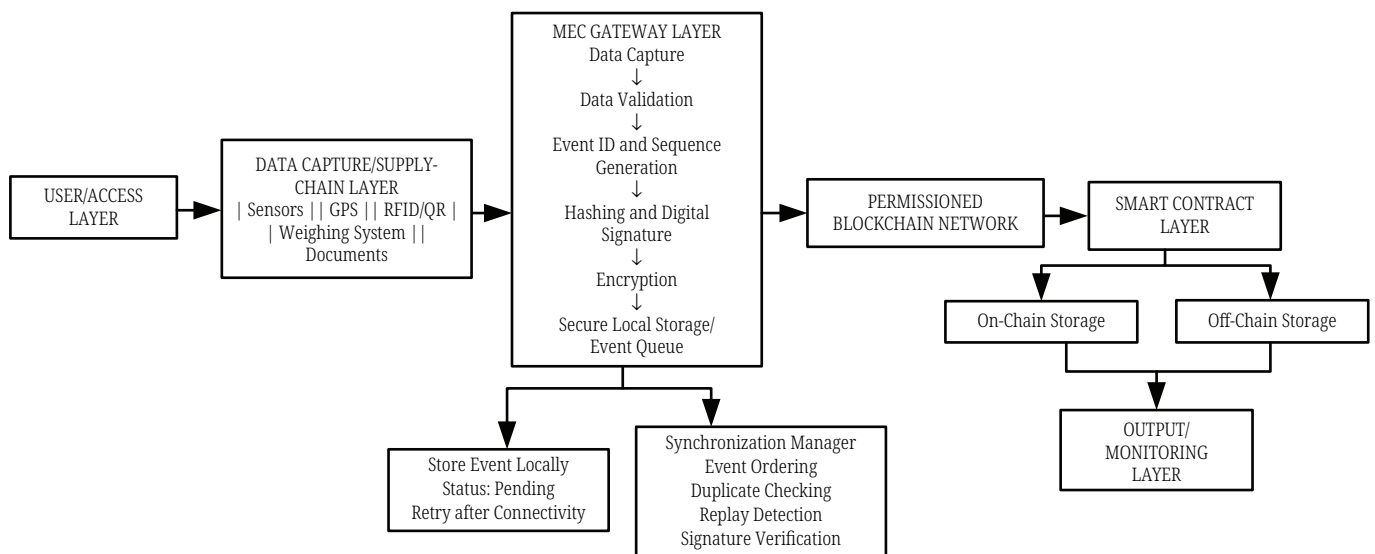


Fig. 1. Architecture of the proposed offline-first MEC–blockchain framework for cross-island critical-mineral traceability

3.3 Edge-based data capture, processing, and local storage

This proposed framework relies on the ability to store and process important traceability data for critical minerals closer to where supply-chain activities happen using MEC gateways, which can temporarily store and process the critical-mineral traceability data. The basic event structure (6) is shown as:

$$E_i = \{B_i, A_i, T_i, L_i, W_i, C_i, N_i\} \quad (6)$$

(E_i) is the (i)-th traceability event, (B_i) is the identifier of the mineral batch, (A_i) is the actor or the device identity, (T_i) is the time when the event took place, (L_i) is the location at which the event occurred, (W_i) is the recorded weight, (C_i) is the custody status at the event, and (N_i) is the event-sequence number. The result of the validation (7) should be expressed thus:

$$V(E_i) = \begin{cases} 1, & \text{if all validation requirements are satisfied} \\ 0, & \text{otherwise} \end{cases} \quad (7)$$

If ($V(E_i) = 1$), the event is taken to the next step for processing. When ($V(E_i) = 0$), it is either rejected or put under manual review. The Hash value of the event (8) is

$$H_i = H(E_i \parallel H_{i-1} \parallel S_i) \quad (8)$$

where (H_i) is the hash of the current event, (H_{i-1}) is the hash of the previous event, (S_i) is the digital signature. The event at time t , plus those events that are concurrent with t , but not yet completed, is shown by (9):

$$Q_t = \{E_i \mid V(E_i) = 1 \wedge \text{Sync}(E_i) = 0\} \quad (9)$$

where Q_t denotes the set of events that have been verified but not synchronized, and $\text{Sync}(E_i)$ denotes whether the event has been synchronized or not.

3.4 Permissioned blockchain and smart-contract design

The proposed framework includes a shared and immutable record of critical mineral movements—created on an encrypted blockchain but with a permissioned process for accessing it. The access decision (10) is written as:

$$A(u, r, o) = \begin{cases} 1, & \text{if user } u \text{ with role } r \text{ can perform operation } o \\ 0, & \text{otherwise} \end{cases} \quad (10)$$

A transaction (11) is accepted only if all the validation conditions are met:

$$\text{Valid}(T_i) = I_i \wedge R_i \wedge S_i \wedge B_i \wedge O_i \quad (11)$$

where (I_i) is a valid identity of the participant, (R_i) is a sufficient role, (S_i) is a valid digital signature, (B_i) is a valid batch, and (O_i) is a correct order in which events occur. The blockchain record (12) can be represented as:

$$L_i = H(ID_i \parallel B_i \parallel T_i \parallel A_i \parallel H_{i-1}) \quad (12)$$

where $[L_i]$ is the hash contained in the ledger, $[ID_i]$ is the identity of the event, $[B_i]$ is the identifier of the corresponding batch, $[T_i]$ is the time when the event was recorded and $[H_{i-1}]$ is the hash of the previous event in the same batch.

3.5 Edge-to-blockchain synchronization and security mechanism

The edge-to-blockchain synchronization mechanism allows sending traceability events to the permissioned blockchain when the network connection is established. The adopted events (13) waiting for synchronization are represented:

$$P_t = \{E_i \in Q_t \mid N_i > N_c\} \quad (13)$$

where (P_t) represents the set of pending events, (Q_t) represents a local event queue, (N_i) represents the sequence number of event (E_i) and (N_c) represents the sequence number of the most recent event from the blockchain confirmed by the corresponding service (E_c) . If any events are pending, they are sent in their original order, as they have to occur in a valid sequence for minerals (14) to be represented by the sequence-validation rule:

$$Seq(E_i) = \begin{cases} 1, & \text{if } N_i = N_{i-1} + 1 \\ 0, & \text{otherwise} \end{cases} \quad (14)$$

If $(Seq(E_i) = 0)$, the event is considered to be an ordering violation and is returned to consideration. The digital signature (15) is being verified with the public key of the participant/MEC gateway:

$$Verify(E_i) = Verify_{pki}(S_i, H(E_i)) \quad (15)$$

(Pki) is the participant's public key; (S_i) is a digital signature; and $(H(E_i))$ represents the cryptographic hash of the event. Every event has its own unique identifier, sequence number, timestamp, and nonce. The last transaction-acceptance condition (16) is expressed as:

$$Accept(E_i) = V_i \wedge Seq_i \wedge Sig_i \wedge Auth_i \wedge Dup_i \quad (16)$$

where (V_i) means that the event X_i is valid, (Sig_i) that the event signature is OK, (Seq_i) that the order of the events is OK, $(Auth_i)$ that the author of the event is OK, and (Dup_i) whether the event ID or nonce has already been recorded.

3.6 Algorithm of proposed Offline-First Mineral Traceability

Algorithm 1: Offline-First Mineral Traceability

Input: Traceability event (E_i), participant (A_i), batch (B_i), network status (Net)

Output: Confirmed, pending, or rejected event

BEGIN

```

1. Receive traceability event  $E_i$ 
2. IF required data are missing THEN
    Reject  $E_i$ 
    Store error message
3. ELSE IF participant  $A_i$  is unauthorized THEN
    Reject  $E_i$ 
    Store security alert
4. ELSE
    Assign event ID and sequence number
    Generate event hash  $H_i$ 
    Digitally sign  $E_i$ 
    Encrypt sensitive data
5.   IF network is unavailable THEN
    Store  $E_i$  in local MEC queue
    Set status  $\leftarrow$  "Pending Synchronization"
6.   ELSE
    Submit  $E_i$  to blockchain
    END IF
    END IF

7. WHILE local queue is not empty AND network is available DO
8.   Select the next event  $E_i$ 
9.   IF event sequence is incorrect THEN
    Set status  $\leftarrow$  "Sequence Conflict"
10.  ELSE IF event ID already exists THEN
    Set status  $\leftarrow$  "Duplicate Rejected"
11.  ELSE IF nonce was previously used THEN
    Set status  $\leftarrow$  "Replay Rejected"
12.  ELSE IF digital signature is invalid THEN
    Set status  $\leftarrow$  "Invalid Signature"
13.  ELSE IF participant lacks custody rights THEN
    Set status  $\leftarrow$  "Custody Conflict"
14.  ELSE
    Execute smart contract
    Store event hash on blockchain
    Store sensitive files off-chain
    Update custody status
    Set status  $\leftarrow$  "Blockchain Confirmed"
    Remove  $E_i$  from local queue
    END IF

15. END WHILE

16. Return event status

END

```

4 RESULT AND DISCUSSION

The proposed MEC–blockchain framework was evaluated in a simulated cross-island traceability testbed representing mines, ports, vessels, and processing facilities. The experiment used the Kaggle *Critical Minerals and Rare Earths (2015–2026)* dataset, comprising 1,548 records covering 24 minerals and 35 countries. Eight traceability events were generated per source record, producing 12,384 synthetic events. Four MEC gateways and a Hyperledger Fabric 2.5 permissioned blockchain were configured to evaluate normal, constrained, and complete network-outage conditions. During outages, events were retained locally and synchronized after connectivity was restored. Six security-attack categories were also simulated, with 100 injected events per category. The complete experimental configuration is summarized in Table 1.

Table 1. Experimental configuration of the proposed MEC–blockchain framework

Experimental Parameter	Configured Value
Dataset	Critical Minerals and Rare Earths (2015–2026), Kaggle
Original dataset records	1,548
Number of minerals	24
Countries represented	35
Dataset period	2015–2026
Events generated per record	8
Total normal events	12,384
Number of MEC gateways	4
Edge-node processor	Quad-core, 2.4 GHz
Edge-node memory	8 GB RAM
Edge-node storage	128 GB
Local database	SQLite
Blockchain platform	Hyperledger Fabric 2.5
Peer organizations	4
Ordering nodes	3
Consensus mechanism	Raft
Blockchain state database	CouchDB
Hashing algorithm	SHA-256
Average on-chain payload	Approximately 2 KB per event
Off-chain file size	50–500 KB
Normal network condition	20 Mbps and 40 ms latency
Constrained network condition	1 Mbps, 200 ms latency, and 2% packet loss
Simulated outages	1, 6, 12, and 24 hours
Events per attack type	100
Total injected attack events	600
Repetitions per scenario	30

4.1 Experimental results

Figure 2 compares record completeness under increasing network-outage durations. The proposed MEC-blockchain framework maintained high completeness, declining only from 99.9% at 1 hour to 98.7% at 24 hours. In comparison, the cloud-only system declined substantially to 58.2%, while the centralized offline-first system reached 95.2% after 24 hours. These results demonstrate the stronger resilience of the proposed framework under prolonged connectivity loss.

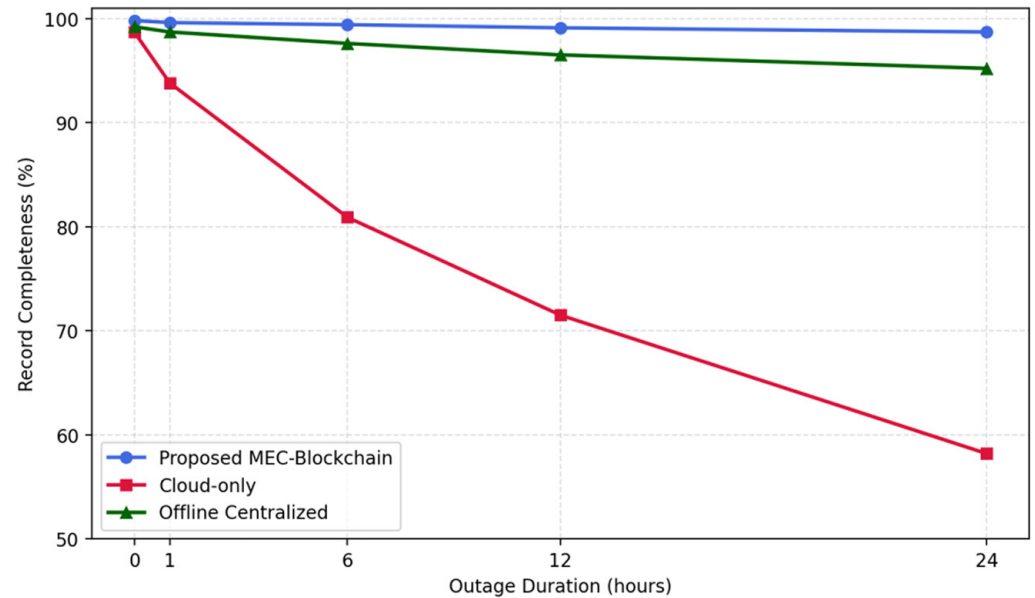


Fig. 2. Record completeness achieved under outage durations

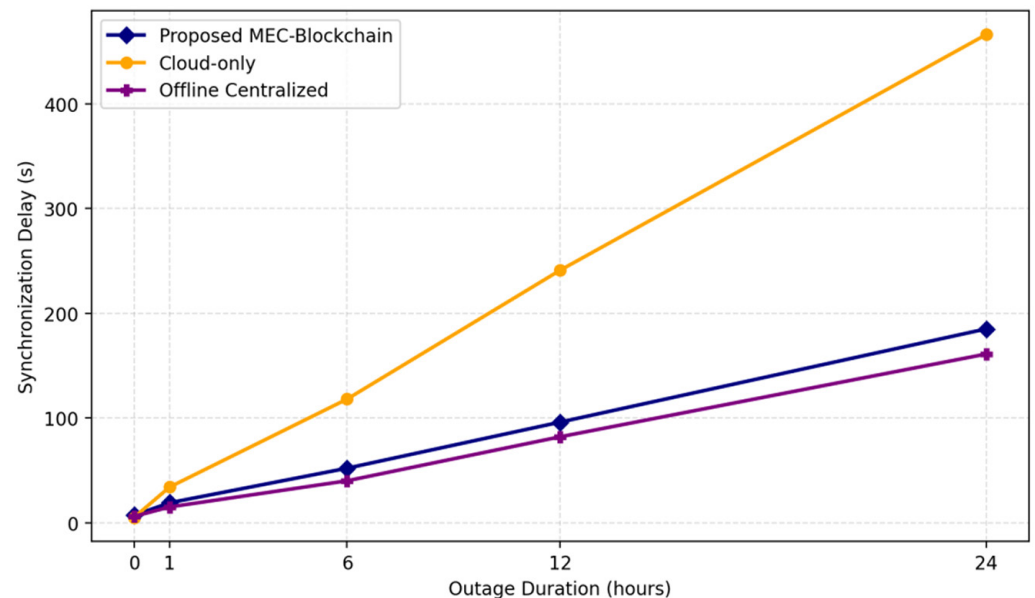


Fig. 3. Synchronization delay

Figure 3 presents the synchronization delay after network reconnection. The delay increased with outage duration as locally queued events accumulated. Following a 24-hour outage, the proposed framework synchronized in 185 s, compared with

466 s for the cloud-only system and 161 s for the centralized offline-first system. Although the centralized approach was slightly faster, the proposed framework substantially outperformed the cloud-only system. Transaction-confirmation time increased after prolonged outages; following a 24-hour outage, the proposed framework required 29.4 s, compared with 66.2 s for cloud-only and 27.8 s for centralized offline-first processing.

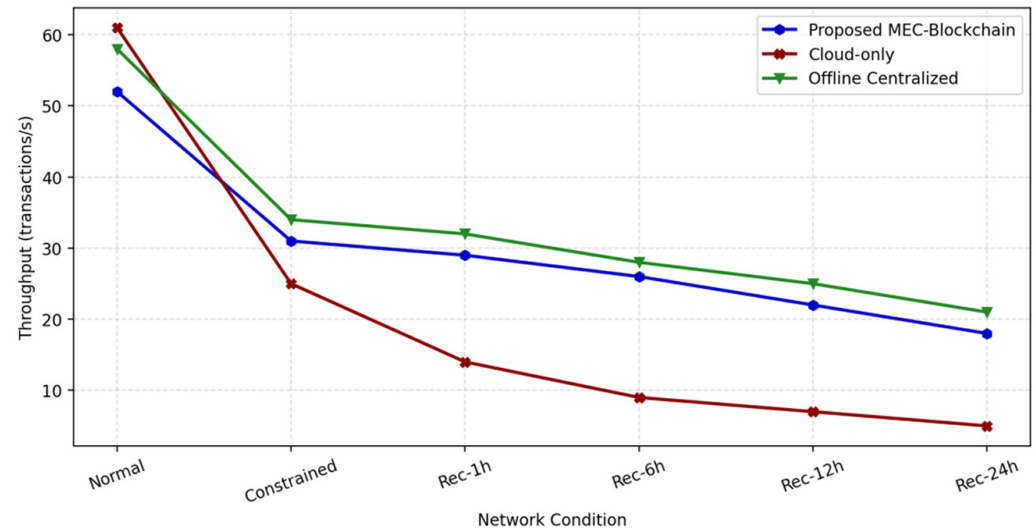


Fig. 4. Transaction throughput

Figure 4 compares transaction throughput across network conditions. Under normal connectivity, the proposed framework achieved 52 TPS, increasing to 31 TPS under constrained connectivity and declining to 18 TPS after a 24-hour outage. Although the centralized offline-first system achieved slightly higher throughput, the proposed framework substantially outperformed the cloud-only system during constrained connectivity and post-outage recovery.

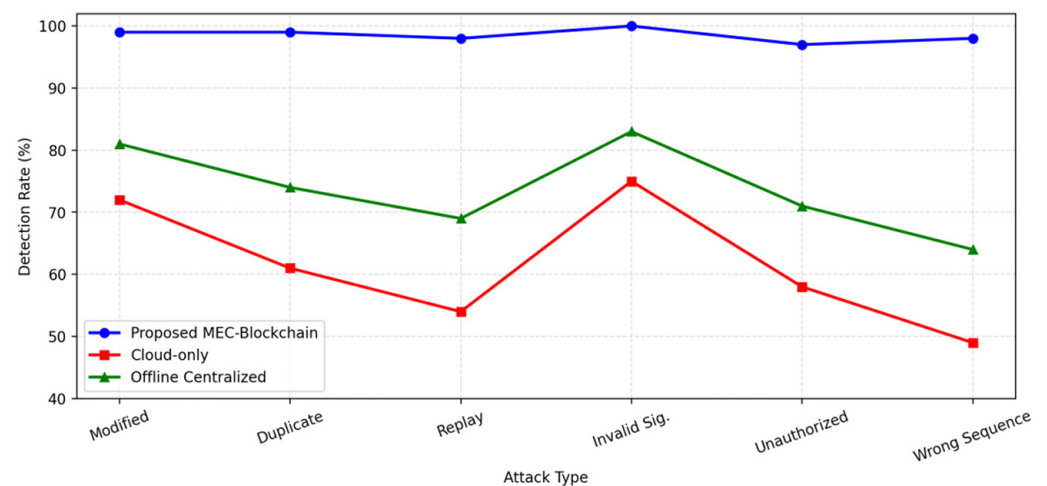


Fig. 5. Security-attack detection rates

Figure 5 compares security-attack detection across six simulated attack categories. The proposed framework achieved detection rates of 97–100%, with an overall rate of 98.5%, compared with 61.5% for the cloud-only and 73.7% for the centralized

offline-first system. Invalid signatures achieved the highest detection rate (100%), while unauthorized custody transfers recorded the lowest (97%).

4.2 Discussion

The findings demonstrate that the proposed MEC–blockchain framework can improve critical-mineral traceability under intermittent connectivity, particularly where cloud-dependent systems are vulnerable to prolonged network outages. After a 24-hour outage, the framework maintained 98.7% record completeness, compared with 58.2% for the cloud-only system and 95.2% for the centralized offline-first approach. This supports previous research highlighting the value of edge computing for localized processing and reduced dependence on continuous cloud connectivity [1], [2]. The results also extend blockchain-based mineral traceability studies [3], [6], [8], [13], [16] by explicitly addressing offline operation and post-outage synchronization.

The 98.5% average attack-detection rate further indicates that cryptographic hashing, digital signatures, sequencing, access control, and smart-contract validation can strengthen tamper detection and transaction integrity. This is consistent with previous MEC–blockchain security research emphasizing authenticated data exchange and integrity protection [11], [12], [14]. However, blockchain verification should not be interpreted as guaranteeing the accuracy of source data; incorrect sensor measurements or authorized but inaccurate inputs may still enter the system. Performance results also reveal an important trade-off. Although the proposed framework substantially reduced synchronization delay compared with the cloud-only baseline (185 versus 466 s after a 24-hour outage), the centralized offline-first system was slightly faster at 161 s and achieved higher transaction throughput. Edge CPU utilization also increased during recovery. These results suggest that blockchain-enabled distributed verification introduces computational overhead in exchange for stronger traceability, tamper evidence, and multi-organization verification.

Overall, the framework appears most relevant to geographically distributed mineral supply chains where continuity, shared verification, and security are prioritized over maximum processing efficiency.

5 CONCLUSION AND LIMITATION

This study proposed an offline-first MEC–permissioned blockchain framework for secure cross-island critical-mineral traceability under intermittent connectivity. MEC gateways enable local validation, signing, encryption, and storage of traceability events during network outages, while the permissioned blockchain supports distributed verification and tamper-evident records. Evaluation using 12,384 synthetic traceability events showed 98.7% record completeness after a 24-hour outage, an average attack-detection rate of 98.5%, and a reduction in post-outage synchronization delay from 466 s for the cloud-only baseline to 185 s. These findings demonstrate the framework’s potential to improve traceability continuity and security in geographically distributed mineral supply chains. However, the evaluation was simulation-based. Future research should prioritize field validation at mines, ports, and vessels, integration with calibrated weighing systems and digital product passports, hardware-secured MEC gateways, alternative connectivity such as satellite communication, and privacy-preserving blockchain mechanisms. The study is

limited by its simulation-based evaluation using synthetic traceability events and a four-gateway testbed. Future research should validate the framework in real mineral supply chains and examine larger networks, hardware-secured MEC gateways, and privacy-preserving mechanisms.

6 REFERENCES

- [1] J. A. Alzubi, O. A. Alzubi, A. Singh, and T. M. Alzubi, "A blockchain-enabled security management framework for mobile edge computing," *Int. J. Netw. Manage.*, vol. 33, no. 5, p. e2240, 2023. <https://doi.org/10.1002/nem.2240>
- [2] S. Asaithambi, S. Nallusamy, J. Yang, S. Prajapat, G. Kumar, and P. S. Rathore, "A secure and trustworthy blockchain-assisted edge computing architecture for industrial Internet of Things," *Sci. Rep.*, vol. 15, no. 1, 2025. <https://doi.org/10.1038/s41598-025-00337-3>
- [3] F. Díaz, N. Cerna, R. Liza, and B. Motta, "Blockchain in mining and mineral supply chains: A systematic mapping review of traceability, governance, and operational coordination," *Logistics*, vol. 10, no. 5, p. 118, 2026. <https://doi.org/10.3390/logistics10050118>
- [4] O. Evsutin and Y. Meshcheryakov, "The use of blockchain technology and digital watermarking to provide data authenticity on a mining enterprise," *Sensors*, vol. 20, no. 12, p. E3443, 2020. <https://doi.org/10.3390/s20123443>
- [5] K. Fiaz *et al.*, "A two-phase blockchain-enabled framework for securing Internet of Medical Things systems," *Internet Things*, vol. 28, p. 101335, 2024. <https://doi.org/10.1016/j.iot.2024.101335>
- [6] N. Gligorić, D. Escuín, L. Polo, A. Amditis, T. Georgakopoulos, and A. Fraile, "IOTA-based distributed ledger in the mining industry: Efficiency, sustainability and transparency," *Sensors*, vol. 24, no. 3, p. 923, 2024. <https://doi.org/10.3390/s24030923>
- [7] M. A. G. Hazber *et al.*, "A blockchain-enabled edge computing framework leveraging artificial neural network and Aquila optimization to enhance security and scalability of cloud-based IoT platforms," *Cluster Comput.*, vol. 28, 2025. <https://doi.org/10.1007/s10586-025-05518-3>
- [8] A. Jha, A. Young, and J. Sattarvand, "Blockchain technology and mining industry: A review," *Min. Metall. Explor.*, vol. 40, no. 6, pp. 2269–2280, 2023. <https://doi.org/10.1007/s42461-023-00874-3>
- [9] I. U. Khan, F. M. Khan, Z. A. Haider, and F. Alturise, "Integrating AI, blockchain, and edge computing for zero-trust IoT security: A comprehensive review of advanced cybersecurity frameworks," *Comput. Mater. Contin.*, vol. 85, no. 3, pp. 4307–4344, 2025. <https://doi.org/10.32604/cmc.2025.070189>
- [10] M. Yuan and N. Anurak, "A systematic review of TikTok, WeChat, and LINE: The impact of social media on Sino-Thai cross-cultural engagement," *J. Adv. Hum. Res.*, vol. 4, no. 1, pp. 61–76, 2025. <https://doi.org/10.56868/jadhur.v4i1.303>
- [11] S. K. Jha, B. H. Kumari, K. Anand, J. Kanjalkar, R. B. Gaddam, and S. Kumar, "Intelligent task prediction and partial computation offloading in mobile edge cloud computing," *International Journal of Interactive Mobile Technologies (IJIM)*, vol. 19, no. 18, pp. 106–117, 2025. <https://doi.org/10.3991/ijim.v19i18.57233>
- [12] Q. Tang, Z. Fei, J. Zheng, B. Li, L. Guo, and J. Wang, "Secure aerial computing: Convergence of mobile edge computing and blockchain for UAV networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 11, pp. 12073–12087, 2022. <https://doi.org/10.1109/TVT.2022.3189818>
- [13] J. A. Wise *et al.*, "Legal smart contracts for derivative trading in mining," *Knowl. Eng. Rev.*, vol. 35, p. e10, 2020. <https://doi.org/10.1017/S0269888920000144>

- [14] X. Yan, Q. Wu, and Y. Sun, "A homomorphic encryption and privacy protection method based on blockchain and edge computing," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–9, 2020. <https://doi.org/10.1155/2020/8832341>
- [15] M. Pincheira, M. Antonini, and M. Vecchio, "Integrating the IoT and blockchain technology for the next generation of mining inspection systems," *Sensors*, vol. 22, no. 3, p. 899, 2022. <https://doi.org/10.3390/s22030899>
- [16] Z. Qiang, Y. Wang, K. Song, and Z. Zhao, "Mine consortium blockchain: The application research of coal mine safety production based on blockchain," *Secur. Commun. Netw.*, vol. 2021, pp. 1–10, 2021. <https://doi.org/10.1155/2021/5553874>
- [17] T. Sultana, A. Almogren, M. Akbar, M. Zuair, I. Ullah, and N. Javaid, "Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices," *Appl. Sci.*, vol. 10, no. 2, p. 488, 2020. <https://doi.org/10.3390/app10020488>
- [18] A. Ramli, I. Ismail, and R. M. Idrus, "Mobile learning via SMS among distance learners: Does learning transfer occur?" *Int. J. Interact. Mob. Technol.*, vol. 4, no. 3, pp. 30–35, 2010. <https://doi.org/10.3991/ijim.v4i3.1180>
- [19] A. T. Nieto, "Blockchain, non-fungible tokens ownership certification of gold reserves and potential contribution to sustainable mining," *Earth Sci. Inform.*, vol. 18, 2025. <https://doi.org/10.1007/s12145-025-01835-8>
- [20] M. Onifade, J. A. Adebisi, and T. Zvarivadza, "Recent advances in blockchain technology: Prospects, applications and constraints in the minerals industry," *Int. J. Min. Reclam. Environ.*, vol. 38, no. 7, pp. 497–533, 2024. <https://doi.org/10.1080/17480930.2024.2319453>

7 AUTHORS

Prof. Dr. Musran Munizu, SE, M.Si, M.A.P, CIPM, is a senior Indonesian academic and Full Professor (Guru Besar) specializing in Operations and Strategic Management at the Faculty of Economics and Business, Hasanuddin University. Inaugurated as a professor in 2019, his extensive research focuses on supply chain management, total quality management (TQM), and small-to-medium enterprise (SME) development in Eastern Indonesia. Alongside his primary tenure at Unhas, he extends his academic leadership to Universitas Cokroaminoto Makassar, where he serves as the Director of the Postgraduate Program (E-mail: musran@fe.unhas.ac.id).

Suraya Ainun Lestari is affiliated with the Faculty of Economics and Business, Hasanuddin University, Indonesia. Her academic involvement in this project contributes to the examination of governance performance. This background is relevant to the study's focus on the strategic role of interactive mobile technologies in strengthening transparency, accountability, and coordination in infrastructure projects (E-mail: surayaal@unhas.ac.id).

Prof. Dr. H. Muhammad Asdar, SE, M.Si., is a prominent Indonesian academic, economist, and public official based in Makassar, South Sulawesi. He serves as a Full Professor (Guru Besar) at the Faculty of Economics and Business at Hasanuddin University (Unhas) (E-mail: muh.asdar@fe.unhas.ac.id).

Dr. Adeel Akmal is an Assistant Professor of Operations and Project Management at the Faculty of Industrial Engineering, Mechanical Engineering and Computer Science, University of Iceland, specializing in lean thinking, healthcare quality improvement, and operations management. Previously, he served as a Research Fellow and Coordinator at the University of Otago's Centre for Health Systems and Technology (CHeST) in New Zealand, where he published extensively in major international journals on organizational performance and workflow efficiency (E-mail: adeel@hi.is).

Danial Kasim is an academic affiliate and student at the Faculty of Economics and Business, University of Hasanuddin (UNHAS) in Makassar, Indonesia, with a research focus on economics, intervention strategies, and change management. He utilizes a personal contact email for professional and academic communication regarding his projects and research outputs. For more information, visit the University of Hasanuddin (E-mail: danial@student.unhas.ac.id).