Decentralized Zero-Trust: A Directed Acyclic Graph (DAG)-Based Ledger Framework for Attribute-Based Access Control in Resource-Constrained Edge Environments

Naresh Kalimuthu

naresh.kalimuthu@gmail.com

Abstract:
The rapid expansion of the Internet of Things (IoT) has necessitated a shift to distributed Edge environments, rendering traditional perimeter security obsolete and exposing scalability bottlenecks in centralized Zero-Trust Architecture (ZTA). This paper proposes a novel, decentralized ZTA framework that integrates Directed Acyclic Graph (DAG) distributed ledgers with Attribute-Based Access Control (ABAC) to eliminate single points of failure. By leveraging asynchronous DAG protocols (e.g., IOTA Tangle, Obyte) instead of linear blockchains and using lightweight Elliptic Curve Cryptography (ECC) for resource-constrained devices, the system enables fee-less, parallel transaction processing. Quantitative analysis demonstrates the framework's superior performance, achieving over 1,000 transactions per second (TPS), sub-second finality, and 15ms encryption times on commodity hardware, thereby establishing a robust, partition-tolerant security model for the future Internet of Everything.

Keywords: Directed Acyclic Graph (DAG), IOTA Tangle, Obyte, Zero-Trust Architecture (ZTA), Attribute-Based Access Control (ABAC), CP-ABE, Edge Computing, Data Confidence Fabric (DCF).

I. INTRODUCTION

A. The Paradigm Shift to Edge Computing

The digital environment is undergoing a significant shift driven by the demand for data-intensive applications. While centralized cloud computing works well for large-scale batch tasks, it doesn't meet the stringent latency, bandwidth, and privacy requirements of modern Cyber-Physical Systems (CPS). Edge computing helps by processing data nearer to its source—such as sensors, actuators, and mobile devices. This decentralization is essential for real-time decision-making in areas such as autonomous driving, remote robotic surgery, and grid load management.

However, moving to the Edge removes the traditional network boundary. Devices in Edge setups are often physically accessible, computationally constrained, and communicate over untrusted public networks. Trust based on network location, the foundation of perimeter security, is risky here. An attacker who breaches one edge node can move laterally to compromise the entire system.

B. The Necessity of Zero-Trust Architecture (ZTA)

To mitigate these risks, the industry is adopting Zero-Trust Architecture (ZTA). As defined by National Institute of Standards and Technology (NIST) SP 800-207, ZTA operates on the principle of "never trust, always verify." It dictates that no implicit trust is granted to assets or user accounts based solely on their physical or network location. Access must be granted on a per-session basis, determined by dynamic policies that evaluate the user's identity, the device's health, and the request's context.

In IoT environments, Role-Based Access Control (RBAC) can be too rigid, often leading to "role explosion" when managing millions of devices. Attribute-Based Access Control (ABAC) provides the necessary

granularity by enabling policies based on attributes such as "User=Technician," "Time=Shift_A," or "Location=Factory_Floor," rather than fixed roles. The key challenge is to implement ABAC policies without creating a centralized bottleneck. A centralized Policy Decision Point (PDP) becomes a prime target for attackers and can also introduce latency that affects real-time processing at the edge applications.

C. Limitations of First and Second-Generation Blockchains

Distributed Ledger Technology (DLT) provides an effective way to decentralize the PDP. It achieves this by recording access policies and audit logs on an immutable ledger, spreading trust throughout the network. However, conventional linear blockchains (Blockchain 1.0 and 2.0) are not well-equipped to meet the high-frequency, low-latency requirements of IoT.

- **Scalability Constraints:** Linear blockchains such as Bitcoin and Ethereum handle transactions sequentially within blocks. This results in a strict limit on throughput, about 7 transactions per second for Bitcoin and 15-30 TPS for Ethereum Layer 1. When network demand rises, congestion causes fees to spike and delays confirmation transactions.
- **Latency and Finality:** IoT applications usually need instant feedback. Waiting 10 minutes for Bitcoin or 15 seconds for Ethereum, due to probabilistic confirmation, is not acceptable in industrial control systems loops.
- **Transaction Costs:** The fee market in traditional blockchains renders micro-transactions typical for IoT, such as a sensor logging a temperature reading every minute, economically unfeasible. Gas fees vary greatly, complicating operational cost predictions impossible.
- **Resource Intensity:** Proof-of-Work (PoW) consensus mechanisms use a significant amount of energy, conflicting with the low-power needs of battery-operated IoT devices.

D. The Promise of DAG-Based Ledgers

Directed Acyclic Graph (DAG) architectures are considered the third generation of DLT. They move away from the linear block structure, adopting a graph topology in which transactions reference earlier ones, enabling parallel processing and asynchronous. Protocols like IOTA and Obyte have shown the ability to deliver high throughput, near-instant finality, and minimal or zero transaction fees, making them potentially perfect for the "Internet of Everything."

This paper explores integrating DAG architectures with lightweight cryptographic access controls to create a robust, decentralized Zero-Trust framework. It assesses how the topological features of DAGs can tackle the unique challenges of the Edge, providing a secure and scalable foundation for next-generation IoT.

II. KEY RESEARCH CHALLENGES

Creating a decentralized, DAG-based Zero-Trust framework for the Edge encounters substantial challenges. We identify three key challenge categories that must be addressed to move from theoretical concept to practical deployment: balancing Scalability and Latency, overcoming Severe Resource Constraints, and handling Network Heterogeneity and Partitioning.

A. Scalability, Throughput, and Consensus Latency

The "Blockchain Trilemma" suggests that a decentralized network can optimize only two of the three qualities: decentralization, security, and scalability. In the context of IoT, scalability is essential. The network must be capable of managing millions of simultaneous data point streams.

- **Throughput Saturation:** While DAGs enable parallel transaction issuance, the network's capacity is ultimately limited by bandwidth and the node's ability to process and store data. During high-traffic periods, DAGs can also become congested if the consensus algorithm demands significant messaging (gossip) to achieve finality. The key challenge is to sustain high throughput (thousands of TPS) without centralizing the network around high-performance nodes.
- **Time-to-Finality (TTF):** Throughput and latency are different: a system might handle 10,000 TPS but still take minutes to confirm each transaction. For critical actions like unlocking a smart lock or activating a fire suppression system, latency must be under a second. Achieving deterministic finality in a leaderless,

asynchronous DAG environment is mathematically challenging. Probabilistic finality, where confidence increases over time, may not be sufficient for safety-critical IoT systems, as a ledger reorganization could undo a physical event such as unauthorized access, even if the digital record is corrected in reality.

B. Resource Constraints on Edge Devices

In IoT, the "Things" are typically low-cost, low-power devices with constrained computational capabilities.

- **Cryptographic Overhead:** The core mathematical tasks in Zero-Trust, including encryption, signing, and verification, are resource-heavy. Traditional CP-ABE schemes rely on bilinear pairing over elliptic curves. Although a pairing operation completes in a few milliseconds on a high-end server, it can take hundreds of milliseconds or more on devices such as an ESP32 or Raspberry Pi Zero. As a result, verifying multiple attributes on these devices causes high latency and significantly drains the battery, accelerating battery degradation.
- **Storage and Bandwidth:** A full distributed ledger continuously grows, but edge devices with limited storage cannot store a complete copy. Light client protocols often depend on trusting a full node, which may reintroduce centralization concerns. A dependable approach for secure, trustless pruning or snapshotting is essential.
- **Energy Constraints:** Many IoT devices operate on batteries intended for multi-year use. However, continuous tasks such as listening for gossip, voting, and executing PoW in consensus protocols prevent these devices from entering deep-sleep modes. As a result, security protocols must be "sleep-aware," allowing devices to wake, complete transactions, and return to sleep without risking synchronization or security breaches.

C. Network Heterogeneity and Partitioning

Their extreme diversity and volatility define edge environments.

- **Network Partitioning:** Unlike cloud servers in data centers, edge devices are mobile and rely on wireless connections like Wi-Fi, 5G, or LoRaWAN, which are prone to interference and disruptions. A strict consistency model, like that of Bitcoin, ceases to operate during a network partition. Consequently, an IoT ZTA should prioritize Availability, allowing a local group of devices—such as those within a disconnected autonomous vehicle—to continue secure operations and synchronize once connectivity is restored.
- **Device Heterogeneity:** The network includes everything from strong gateways to passive RFID tags. A universal security protocol isn't practical. The framework must enable semantic interoperability, ensuring that low-power device sensors can enforce policies set by high-power nodes.

III. CORE ARCHITECTURES / METHODOLOGIES: DAG VS. BLOCKCHAIN

To address these challenges, we perform a comparative analysis of key DLT frameworks, focusing on traditional Blockchain architecture versus the emerging DAG topology, specifically IOTA (The Tangle) and Obyte.

A. Blockchain Architecture (Linear)

Traditional blockchains organize transactions into blocks that are linked cryptographically in a linear sequence chain.

- **Mechanism:** Transactions are broadcast to a mempool, where miners or validators select them, bundle them into a block, and perform a consensus operation—such as PoW hashing or PoS voting to add the block to the blockchain.
- **IoT Bottlenecks:** The fixed-interval block creation, such as every 10 minutes or 12 seconds, creates a bottleneck. When transaction volume exceeds the block size, a fee market emerges, making it costly for low-value IoT data. Additionally, all full nodes must validate every block, creating significant redundancy that hampers network scalability.

B. Directed Acyclic Graph (DAG) Architecture

DAG ledgers eliminate the concept of blocks. Individual transactions (vertices) are linked directly to previous transactions (edges).

1) IOTA (The Tangle)

IOTA is explicitly tailored for the IoT economy. Its ledger, called the Tangle, requires each new transaction to approve two prior transactions (tips).

- **Parallel Consensus:** Since validation is performed by the users (issuers) rather than a separate miner class, the network's capacity can theoretically grow with increased usage. As more transactions occur, more approvals are required, which accelerates confirmation times.
- **Consensus Mechanism:**
  - *Legacy:* Used a "Coordinator" node to handle the checkpoint ledger.
  - *IOTA 2.0 (Coordicide):* Introduces a leaderless consensus mechanism using Fast Probabilistic Consensus (FPC) and a reputation system named Mana. FPC enables nodes to vote on conflicting transactions, achieving rapid consensus without a global leader.
- **Feeless Structure:** When miners are absent, transaction fees are unnecessary, allowing genuine micro-payments and secure data anchoring for zero cost.

2) Obyte

Obyte uses a DAG structure in which storage units are linked via hashes, emphasizing deterministic finality and efficient data storage.

- **Consensus via Witnesses:** Obyte uses "Order Providers" (Witnesses)—trusted users chosen by the community. These witnesses publish transactions that serve as checkpoints, creating a clear, definitive sequence on the DAG.
- **Deterministic Finality:** A key feature of Obyte is deterministic finality. Once a unit attains a specific depth in the DAG relative to witness units—surpassing a "stability point"—its order is mathematically fixed. This contrasts with the probabilistic finality of PoW/PoS, offering the safety assurances needed for high-stakes IoT actuation.
- **Autonomous Agents (AAs):** Obyte supports Autonomous Agents (AAs), which are pieces of code stored on the DAG that run deterministically when triggered. They are built to avoid infinite loops and re-entrancy attacks, enhancing safety for automated IoT logic over traditional smart contracts.

C. Comparative Analysis: Architecture Suitability

TABLE 1. Comparative analysis of DLT architectures.

Feature	Linear Blockchain (e.g., Ethereum)	IOTA (DAG)	Obyte (DAG)
Topology	Linear, Synchronous	Mesh, Asynchronous	DAG, Asynchronous
Validator Role	Miners/Stakers (Distinct)	Users (Intrinsic)	Witnesses (Order Providers)
Transaction Fee	High, Volatile (Gas)	Zero	Low, Deterministic (Bytes)
Throughput	Low (15-30 TPS)	High (1,000+ TPS)	High (Bandwidth Limited)
Finality Type	Probabilistic	Probabilistic (Legacy) / Deterministic (2.0)	Deterministic
Partition Tolerance	Low (Stalls)	High (Sub-Tangles)	Moderate

The table indicates that DAG architectures more effectively address IoT requirements. IOTA's zero-fee setup is perfect for extensive sensor networks that regularly send data. Conversely, Obyte's deterministic finality is more appropriate for financial or safety-critical operations where reversibility is not possible.

IV. TECHNICAL MECHANISMS & PROTOCOLS

This section explains how DAG ledgers can be integrated with Attribute-Based Access Control, emphasizing the cryptographic techniques that support decentralized security, Zero-Trust.

A. Attribute-Based Access Control (ABAC) in IoT

In the framework, the DAG serves as the Policy Decision Point (PDP) and stores Access Tokens, while IoT devices act as Policy Enforcement Points (PEP).

- **Subject:** The entity requesting access (e.g., a maintenance technician).
- **Object:** The resource (e.g., smart meter data).
- **Attributes:** Characteristics of the subject (Role, ID), object (Type, Sensitivity), and environment (Time, Threat Level).
- **Policy:** A logic statement (e.g., IF User.Role == 'Technician' AND Env.Time == '09:00-17:00' THEN Allow).

B. Lightweight CP-ABE (Ciphertext-Policy Attribute-Based Encryption)

To enforce these policies cryptographically without relying on a central server, we use CP-ABE. In CP-ABE, the user's private key is linked to their attributes, and the ciphertext contains the access policy. Decryption is only possible if the user's attributes meet the policy requirements.

1) The Shift from Bilinear Pairings to ECC

Standard CP-ABE schemes rely on Bilinear Pairings. Although mathematically elegant, these pairing calculations are expensive, with Raspberry Pi performing them in hundreds of milliseconds. The proposed ECC-based CP-ABE scheme eliminates pairings in favor of Scalar Multiplication on Elliptic Curves (Q = kP).

- **Mathematical Model:**

Let E be an elliptic curve defined over a finite field F_p. Let G be a generator of a subgroup of order n. The complex problem utilized is the Elliptic Curve Discrete Logarithm Problem (ECDLP): Given $P, Q \in E$, finding k such that Q = kP is computationally infeasible.

- **Encryption Efficiency:**

Research shows that scalar multiplication is much faster. Benchmarks on the Raspberry Pi 4 reveal ECC scalar multiplication takes about 15ms and uses 80 mJ of energy, whereas pairing-based operations take over 400ms.

2) The Access Tree and LSSS

Access policies are organized using monotonic access trees or Linear Secret Sharing Schemes (LSSS). The tree's root node signifies the secret (the symmetric key used to decrypt data), while the leaves represent attributes.

- **Secret Sharing:** The secret s is divided into shares through Shamir's Secret Sharing scheme. Each attribute node in the tree is assigned a share. To recover the secret (decrypt), the user must have enough valid attribute keys to meet the threshold conditions (AND, OR) in the tree structure.
- **Integration:** The LSSS matrix M is saved on the DAG as metadata linked to the encrypted file reference.

C. Decentralized Identity (DID) and Verifiable Credentials (VC)

The framework leverages the W3C DID standard.

- **DID Creation:** Each IoT device creates a public-private key pair and records its DID Document on the DAG (such as the IOTA Tangle). This serves as the root of trust.
- **Credential Issuance:** An authority, such as the device manufacturer or system administrator, issues a Verifiable Credential (VC) to the device DID that includes attributes such as "DeviceType: Camera".
- **Zero-Knowledge Proofs (ZKP):** To protect privacy, the device does not disclose the raw VC during access requests. Instead, it creates a ZKP (such as zk-SNARK) that proves it holds a valid credential meeting the policy without exposing the token itself.

D. The Protocol Workflow

1. **Setup:** The System Authority initializes the public parameters of the ECC-CP-ABE scheme on the DAG.
2. **Key Generation:** Users/Devices authenticate with the Authority (off-chain or via an encrypted channel) and receive their Attribute Private Keys (SK_{att}).
3. **Data Publishing (Encryption):**
   - Sensor generates a random symmetric session key (K).
   - Sensor encrypts data D with K($Enc_K(D)$).
   - Sensor defines policy P.
   - Sensor encrypts K using CP-ABE with policy $P(CT_k)$
   - Sensor uploads $Enc_K(D)$ to decentralized storage (IPFS) and posts the hash + CT_k to the DAG.
4. **Data Access (Decryption):**
   - Requester fetches CT_k from the DAG.
   - Requester uses SK_{att} to decrypt CT_k. If attributes match policy P, they recover K.
   - Requester fetches and decrypts the data.

V. HANDLING SPECIFIC CONSTRAINTS

Implementing this theoretical framework in practical Edge environments necessitates addressing specific physical and network constraints.

A. Handling Heterogeneity via Semantic Layers

The "Tower of Babel" problem in IoT is addressed through a semantic abstraction layer.

- **Standards:** IOTA Streams facilitates organized, channel-specific communication, where devices publish messages to designated channels. The semantic layer standardizes data mapping, allowing a Zigbee temperature sensor and a LoRaWAN humidity sensor to both encode their data in a shared JSON-LD format within the IOTA network Stream.
- **Hardware Abstraction:** Libraries such as Byteduino (for Obyte) enable high-level logic to be compiled into C++ for ESP32/ESP8266 microcontrollers, simplifying the complex DAG graph logic for embedded systems developer.

B. Partition Tolerance and Solidification

Network partitioning is inevitable in mobile IoT.

- **Local Sub-Tangles:** When a group of devices enters a dead zone, they keep conducting peer-to-peer transactions, forming a local network DAG.
- **Solidification Protocol:** When reconnected, the local cluster begins a "gossip" protocol with the main network. The "Solidification" process then requests any missing past transactions until the ledgers are synchronized. This approach emphasizes Availability (A) over immediate global Consistency (C), in line with the CAP theorem principles for mobile IoT networks.

C. Power and Energy Efficiency

Battery life is the critical constraint.

- **ECC Efficiency:** ECC scalar multiplication uses much less energy (~80 mJ) compared to bilinear pairings. This enables devices to conduct access control checks without depleting batteries.
- **Sleep-Aware Consensus:** In IOTA and Obyte, a node doesn't have to be continuously active in "mining." It can wake up, synchronize the latest tips or stability point, issue a transaction, and then go back to sleep. This process, called "duty cycling," isn't possible in synchronous blockchains, where missing a block height can cause desynchronization among nodes.

VI. QUANTITATIVE ANALYSIS

This section consolidates experimental data to evaluate the proposed DAG-based framework against traditional blockchain solutions.

A. Throughput and Latency Benchmarks

The table below compares the performance of the proposed DAG architectures (IOTA, Obyte) with blockchain benchmarks (Ethereum, Hyperledger Fabric).

Architecture	Throughput (TPS)	Latency (Confirmation)	Consensus Mechanism	Scalability Profile
Ethereum (L1)	~15 - 30	~12 sec (Probabilistic)	PoS (Global)	Linear (Limited)
Hyperledger Fabric	~3,500	< 1 sec	PBFT (Permissioned)	High (Permissioned)
IOTA (DAG)	**1,000+**	**10 - 120 sec**	**Leaderless FPC**	**Asymptotic (High)**
Obyte (DAG)	**Bandwidth Bound**	**10 - 30 sec**	**Witness (Deterministic)**	**High**

TABLE 2. Performance comparison of DLTs.

Analysis:

- **Scalability:** IOTA illustrates a reversal of "negative network externalities'—as the number of users increases, the network speeds up (up to physical limitations), unlike blockchains, which tend to slow down.
- **Latency:** Obyte's deterministic finality guarantees that once a command is marked as "stable," it cannot be reversed, unlike the probabilistic finality seen in Bitcoin/Ethereum.

B. Cryptographic Overhead on Edge Hardware

We evaluate the performance of the proposed ECC-based CP-ABE in comparison to traditional Pairing-based CP-ABE on a typical edge device.

TABLE 3. *Cryptographic performance on Resource-Constrained Devices (Raspberry Pi).*

Operation	Scheme	Execution Time (Avg)	Energy Consumption
Encryption	Pairing-Based CP-ABE	150 - 400 ms	High
Encryption	**ECC-Based CP-ABE**	**~15 - 25 ms**	**~80 mJ**
Decryption	Pairing-Based CP-ABE	100 - 300 ms	High
Decryption	**ECC-Based CP-ABE**	**~20 - 30 ms**	**~100 mJ**

Analysis: Switching to ECC results in roughly 10 to 20 times faster encryption and decryption, along with significant energy savings (80 mJ vs hundreds of mJ).

C. Energy Efficiency of the Ledger

Beyond cryptography, the ledger protocol itself consumes energy.

- **Bitcoin:** ~800 kWh per transaction (unviable).
- **IOTA**: ~0.00152 Wh per transaction (approx. 70x more efficient than Nano)

Insight: DAGs are significantly more energy-efficient, making them the only environmentally and operationally sustainable option for high-volume IoT networks.

VII.STRATEGIC MITIGATIONS & VALIDATION

A. Validation Case Study: Project Alvarium

To validate the proposed architecture in a real-world setting, we analyze "Project Alvarium," a collaboration among Dell Technologies, the IOTA Foundation, and others.

- **Objective:** To develop a "Data Confidence Fabric" (DCF) that evaluates the reliability of data moving from edge to cloud.
- **Implementation:** The project used the IOTA Tangle to store immutable "trust scores" for sensor data packets.
- **Outcome:** The pilot demonstrated that DAGs can manage the high volume of sensor telemetry and provide a tamper-proof audit trail, effectively differentiating between compliant and non-compliant data streams in a carbon footprint monitoring system.

B. Mitigating Security Risks

- **Sybil Attacks:** In a permissionless DAG, an attacker could generate millions of nodes to sway consensus. IOTA addresses this by using Mana—a reputation system based on token holdings—while Obyte relies on a trusted Witness list to establish consensus order.
- **Splitting / Partition Attacks:** Obyte's Witnesses function as a "rail" that drives convergence. Over time, the network will likely discard any branch that lacks a witness units.

VIII. CONCLUSION

The integration of Edge computing and IoT calls for a reevaluation of network security strategies. Traditional perimeter-based security models are no longer adequate, and current centralized IAM solutions act as scalability bottlenecks. This research shows that a Decentralized Zero-Trust Architecture is both essential and feasible, made possible through the combination of DAG-based Distributed Ledgers and Lightweight ECC-based Attribute-Based solutions Encryption.

Analysis shows that DAG architectures such as IOTA and Obyte surpass the limitations of Blockchain 1.0/2.0. They achieve this by separating consensus from block mining, allowing for high-throughput and parallel processing necessary for the Internet of Everything. Additionally, incorporating ECC-based CP-ABE addresses resource constraints, significantly lowering cryptographic overhead from hundreds of milliseconds to around 15ms. As demonstrated by Project Alvarium, these technologies are evolving into effective frameworks for securing data at the edge worldwide.

REFERENCES:

1. Benet, J. (2014). *IPFS - Content addressed, versioned, P2P file system*. arXiv. https://doi.org/10.48550/arXiv.1407.3561
2. J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," 2007 IEEE Symposium on Security and Privacy (SP '07), Berkeley, CA, USA, 2007, pp. 321-334, doi: 10.1109/SP.2007.11.
3. E. Brewer, "CAP twelve years later: How the "rules" have changed," in Computer, vol. 45, no. 2, pp. 23-29, Feb. 2012, doi: 10.1109/MC.2012.37.
4. Cao, B., Li, Y., Zhang, L., Zhang, L., Mumtaz, S., Zhou, Z., & Peng, M. (2019). When Internet of Things Meets Blockchain: Challenges in Distributed Consensus. *ArXiv*. https://doi.org/10.1109/MNET.2019.1900002
5. Dell Technologies. (2023). *Project Alvarium: Delivering trusted edge data* [Case study]. https://www.delltechnologies.com/asset/ko-kr/solutions/business-solutions/customer-stories-case-studies/project-alvarium-case-study-posted.pdf
6. Zhang, X. Zhu and I. Ali, "Performance Analysis of IOTA Tangle and a New Consensus Algorithm for Smart Grids," in IEEE Internet of Things Journal, vol. 11, no. 4, pp. 6396-6411, 15 Feb.15, 2024, doi: 10.1109/JIOT.2023.3311103.

7. Kahmann, F., Honecker, F., Dreyer, J., Fischer, M., & Tönjes, R. (2023). Performance Comparison of Directed Acyclic Graph-Based Distributed Ledgers and Blockchain Platforms. Computers, 12(12), 257. https://doi.org/10.3390/computers12120257
8. S. Müller, A. Penzkofer, N. Polyanskii, J. Theis, W. Sanders and H. Moog, "Tangle 2.0 Leaderless Nakamoto Consensus on the Heaviest DAG," in IEEE Access, vol. 10, pp. 105807-105842, 2022, doi: 10.1109/ACCESS.2022.3211422.
9. Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com.
10. Obyte Foundation. (2024). Obyte platform for IoT. https://obyte.org/platform/iot
11. Zheng X, Sun S, Mukkamala RR, Vatrapu R, Ordieres-Meré J. Accelerating Health Data Sharing: A Solution Based on the Internet of Things and Distributed Ledger Technologies. J Med Internet Res. 2019 Jun 6;21(6):e13583. doi: 10.2196/13583. PMID: 31172963; PMCID: PMC6592507.
12. Popov, S.Y. (2015). The Tangle. https://www.semanticscholar.org/paper/The-Tangle-Popov/43586b34b054b48891d478407d4e7435702653e0
13. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
14. Saare, M. A. ., Jawad, M. N. ., Al-Shareeda, M. A. ., Almaiah, M. A. ., & Obeidat, M. . (2025). Evaluating elliptic curve cryptography in constrained environments: A Raspberry Pi-based approach. International Journal of Innovative Research and Scientific Studies, 8(2), 3966–3976. https://doi.org/10.53894/ijirss.v8i2.6195
15. Li, Y., Cao, B., Peng, M., Zhang, L., Zhang, L., Feng, D., & Yu, J. (2019). Direct Acyclic Graph based Blockchain for Internet of Things: Performance and Security Analysis. ArXiv, abs/1905.10925.