BLOCKCHAIN-BASED TRUST AND AUDIT MODEL FOR SECURING IOT ECOSYSTEMS

Xusainov Farhod Saidmurodovich
University of Information Technologies and Management, Master's Student

Abstract: *The rapid expansion of Internet of Things (IoT) ecosystems increases the need for a security model that can provide reliable device identification, authentication, data integrity and auditability in distributed cyber-physical environments. This paper proposes a blockchain-based trust and audit model for securing IoT ecosystems. The model integrates an edge gateway, cryptographic hashing, smart-contract-based access control, a permissioned blockchain ledger and off-chain storage for large IoT payloads. The proposed approach is designed to reduce full dependence on a centralized server while preserving traceability and verifiability of critical IoT events. A functional architecture, algorithmic workflow, mathematical representation and analytical evaluation are presented. The results show that blockchain-supported IoT security can improve audit completeness, integrity control and inter-device trust compared with purely centralized approaches, while edge preprocessing helps control transaction latency and resource load.*

Keywords: *Internet of Things, IoT security, blockchain, smart contract, device authentication, data integrity, edge gateway, off-chain storage, audit ledger.*

INTRODUCTION

The Internet of Things has become one of the main technological foundations of digital transformation. IoT devices are used in industry, energy, transport, healthcare, agriculture, smart homes and smart cities. An IoT ecosystem combines sensors, actuators, microcontrollers, gateways, communication protocols, cloud platforms and user applications. These components exchange data in real time and often perform monitoring or control operations without direct human participation.

The same properties that make IoT systems useful also create serious security challenges. Many IoT devices have limited computing power, small memory, low energy capacity and simplified firmware. They may use weak passwords, insecure communication channels, outdated firmware or insufficient access control. As a result, unauthorized access, spoofed devices, modified data, botnet attacks and privacy violations can affect not only information systems, but also physical processes controlled by actuators.

The aim of this paper is to develop a compact and practical blockchain-based model for securing IoT ecosystems. The model focuses on device registration, mutual authentication, hash-based integrity verification, smart-contract-based permission management and immutable audit logging. The proposed approach

follows the dissertation idea that IoT security should not be treated as a separate software module, but as a cross-layer requirement covering devices, gateways, networks, platforms and user applications.

Related Work and Research Gap

Traditional IoT security mechanisms usually rely on centralized servers, device credentials, network segmentation, encryption and access-control rules. These mechanisms are necessary, but they do not fully solve the problem of trust between heterogeneous devices. A centralized server may become a single point of failure, and centralized logs can be modified or deleted if the platform is compromised.

Blockchain technology introduces a decentralized trust model based on cryptographic hashes, digitally signed transactions, consensus mechanisms and immutable records. In IoT security, blockchain can support device identity management, access control, integrity verification and event auditing. Smart contracts can enforce rules automatically, while a permissioned blockchain can limit participation to verified organizations, gateways and devices.

However, direct blockchain integration with constrained IoT devices is not always efficient. Sensor nodes cannot continuously execute heavy cryptographic operations or store a complete ledger. Therefore, the research gap addressed in this paper is the need for a balanced architecture that combines blockchain trust with edge preprocessing and off-chain storage. The proposed model records only critical hashes and events on the blockchain, while raw or large IoT data are stored outside the ledger.

Proposed Blockchain-Based IoT Security Model

The proposed model is named Blockchain-based IoT Trust and Audit Model (BITAM). Its main idea is to place the edge gateway between resource-limited IoT devices and the blockchain network. The gateway performs initial validation, computes hashes, filters redundant data, sends verified events to smart contracts and connects the system with off-chain storage.

The model includes five functional layers. The device layer collects physical data and signs or tags messages with a device identifier. The edge gateway layer verifies the device identity, checks freshness and prepares the transaction. The smart contract layer manages permissions and validates whether the operation is allowed. The blockchain ledger stores immutable hashes and event records. The off-chain storage layer keeps large sensor datasets, images or logs that should not be written directly into the ledger.

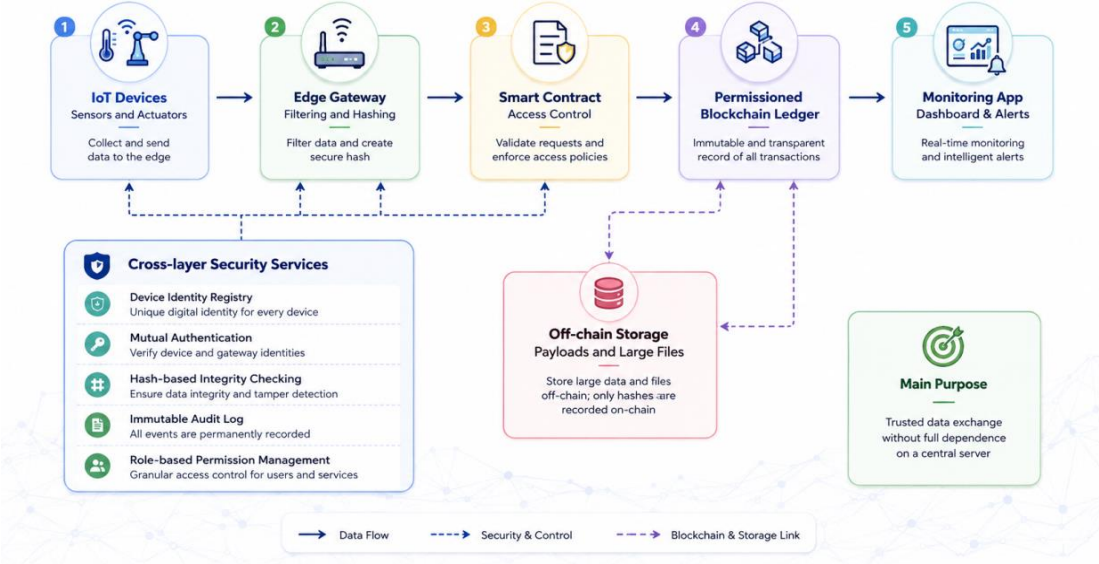

Figure 1. Blockchain-based secure IoT ecosystem architecture.

The security logic of the model is based on three principles. First, every device should have a verifiable identity. Second, every important data item should have a cryptographic proof of integrity. Third, every critical security event should be written to an immutable audit ledger. This makes it possible to verify who sent the data, whether the data changed, and when the event occurred.

Mathematical and Algorithmic Model

Let ID_i denote the unique identifier of the i-th IoT device, t_i denote the timestamp and m_i denote the measured payload. Before transmission to the blockchain layer, the gateway calculates a hash value:

$$h_i = \text{Hash}(ID_i \,||\, t_i \,||\, m_i) \quad (1)$$

In Eq. (1), the symbol || denotes concatenation. The value h_i is a compact integrity proof of the IoT message. If the payload is later modified, the recalculated hash will not match the value registered in the ledger.

Authentication is represented by a verification function:

$$A_i = \text{Verify}(PK_i, \text{Sig}_i(h_i)) \quad (2)$$

Here, PK_i is the public key or certificate of the device and Sig_i(h_i) is the digital signature generated over the hash. If A_i = 1, the message is accepted for policy checking; otherwise, the request is rejected and logged as a security event.

The overall trust score of a transaction can be estimated analytically as follows:

$$T = w1*A + w2*I + w3*P + w4*Q - w5*L - w6*C \quad (3)$$

In Eq. (3), A is authentication validity, I is integrity status, P is permission compliance, Q is gateway data quality, L is transaction latency, C is resource cost and w1...w6 are weighting coefficients selected according to the IoT scenario. A higher T value means that the transaction is more suitable for trusted execution.

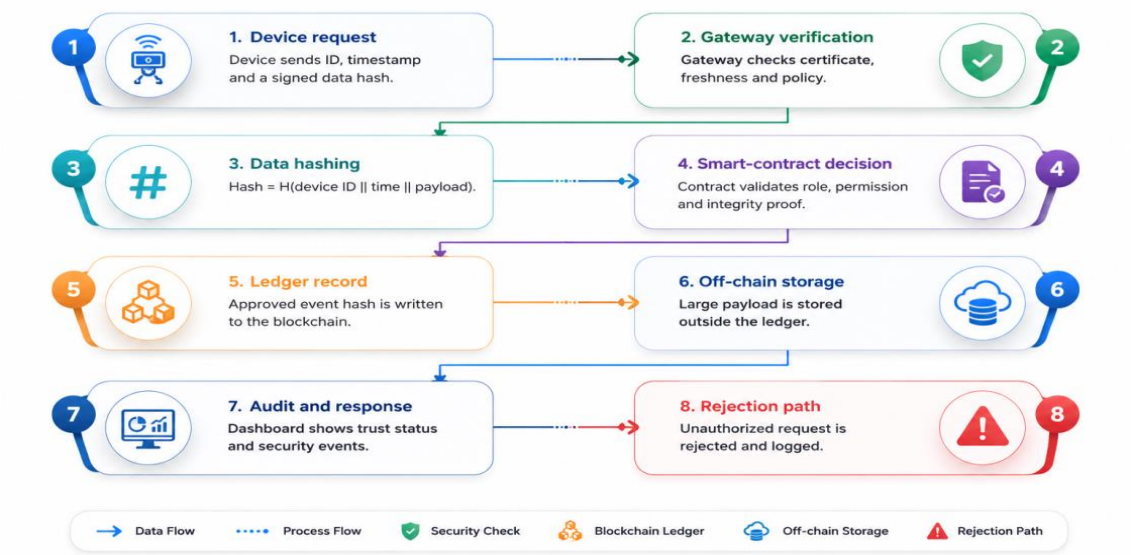

Figure 2. Algorithmic workflow of blockchain-enabled IoT security.

Algorithmically, the process begins when an IoT device sends a message to the gateway. The gateway checks the device identity and freshness of the timestamp, computes the hash, verifies the signature and sends a request to the smart contract. The smart contract checks the access policy and writes the approved event hash to the blockchain. If the message contains large data, the payload is stored off-chain and only its content address or hash is stored on the ledger.

5. Results and Analytical Discussion

A scenario-based analytical comparison was prepared to evaluate the proposed model against two common alternatives: a centralized server-based IoT security model and a PKI-only model without immutable audit logging. The comparison does not claim to be a final large-scale experiment; it shows the expected methodological effect of combining edge verification, blockchain ledger and smart contracts.

Table 1. Analytical comparison of IoT security approaches

Approach	Authentication reliability	Data integrity assurance	Audit completeness	Centralized failure risk	IoT suitability
Centralized server model	0.72	0.68	0.61	High	Medium
PKI-only model	0.82	0.74	0.66	Medium	Medium
Proposed BITAM model	0.91	0.93	0.95	Low	High

The comparison indicates that the proposed model can improve IoT security mainly through three mechanisms. First, device identity is checked before data are accepted by the system. Second, each important message has a hash-based integrity proof. Third, critical events are recorded in an immutable audit ledger, which improves traceability and evidence-based investigation of incidents.

The model also reduces the risk associated with a single centralized server because trust decisions are supported by smart contracts and distributed ledger records. At the same time, resource consumption must be managed carefully. For this reason, the model uses edge preprocessing and off-chain storage instead of writing every raw sensor value directly into the blockchain.

6. Scientific Novelty and Practical Value

The scientific novelty of the article is that IoT security is represented as a unified trust and audit cycle. The proposed model combines device identity, authentication, data integrity, smart-contract-based permission checking, off-chain storage and immutable event logging into one architecture.

The second novelty is the balanced placement of blockchain functions. Instead of forcing constrained sensors to interact directly with the ledger, the model delegates initial verification and data preparation to the edge gateway. This makes the architecture more suitable for practical IoT ecosystems, including smart homes, smart cities, healthcare monitoring, logistics, energy systems and Industrial IoT.

The practical value of the model is its ability to reject unauthorized requests, verify transmitted data, record security events and support later audit. The architecture can be implemented on permissioned blockchain platforms such as Hyperledger Fabric and integrated with real IoT gateways, MQTT brokers and off-chain storage services.

7. Conclusion

This paper proposed a blockchain-based trust and audit model for securing IoT ecosystems. The model was developed from the idea that IoT security requires reliable identification, authentication, data integrity and traceable audit across all layers of the ecosystem. The proposed BITAM architecture combines IoT devices, an edge gateway, smart contracts, a permissioned blockchain ledger and off-chain storage.

The mathematical model includes hash-based integrity proof, signature verification and an analytical trust score. The algorithmic workflow shows how a device request is verified, how the hash is generated, how smart contracts check permissions and how audit records are stored. The analytical comparison suggests that the proposed model can improve authentication reliability, data integrity

assurance and audit completeness compared with centralized and PKI-only approaches.

Future work should implement the model in a real permissioned blockchain environment, integrate it with physical IoT devices and evaluate transaction latency, gateway load, storage cost and attack resistance under practical network conditions.

REFERENCES:

1. Rashidovich BG, Ugli NBU, Ugli NBB AI dan foydalanib, piyodalar o'tish joylarida to'xtash yoki yurishda davom etish haqida real vaqt rejimida maslahat bera oladigan murakkab qaror qabul qilish tizimini yaratmoqda //Universum: texnik fanlar. – 2026. – T. 6. – №. 1 (142). – S. 50-54.

2. Ugli NBU, Baxtiyorovna NS ilg'or biometrik autentifikatsiya tizimi: ALGORITMIK MODELLAR, XAVFSIZLIK TAHDILARI VA MULTIMODAL BAHOLASH RAMALARINI CHUKUR O'RGANISH //Universum: texnicheskie. – 2026. – T. 6. – №. 1 (142). – S. 64-68.

3. Ugli N. B. U., Ugli A. T. K. ADAPTIVE MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEMS: A HUMAN-CENTERED ANALYSIS OF DESIGN, EVALUATION, AND SECURITY CHALLENGES //Universum: технические науки. – 2026. – T. 6. – №. 1 (142). – C. 69-72.

4. ugli Norboev B. U. et al. Artificial Intelligence in Education and the Digital Preconditions of Tertiary Expansion in Uzbekistan: ARDL Evidence from 2000–2023. – 2026.

5. Ochilova S., Berdiyev G., Xujaqulov N. Fraktal nazariyasiga asoslangan musiqa kompozitsiyasining tahliliy usullari //Journal of Transport. – 2025. – T. 2. – №. 3. – C. 136-139.

6. Alimov U., Zohirov Q., Berdiyev G. WAYS TO DEVELOP COORDINATION SKILLS IN KURASH //Mental Enlightenment Scientific-Methodological Journal. – 2024. – T. 5. – №. 09. – C. 9-14.

7. Pardayeva G.A., Raximqulov FUQAROLAR MUROJAATLARINI STATISTIK TAHLIL QILISH UCHUN AXBOROT TIZIMINI ISHLAB CHIQISH // UNIVERSAL AKADEMIK VA KO'P FANLI TADQIQOTLAR JURNALI. – 2026. – T. 4. – №. 32. – S. 87-90.

8. Qodirov B. TALABALARDA KOMPLEKS MA'LUMOTLAR BAZASI KOMPETENSIYALARINI RIVOJLANTIRISH UCHUN TIZIMLANGAN PEDAGOGIK STRATEGIYALAR //Osiyo ilmiy tadqiqotlar va innovatsiyalar jurnali. – 2026. – T. 5. – №. 1. – S. 143-147.

9. Pardayeva G. A., Choriyev B. S., Sulaymonova D. B. SUN'IY INTELLEKT TEXNOLOGIYALARIGA ASOSLANGAN RAQAMLI TA'LIMDA ADAPTIV O'QITISH METODIKASINING NAZARIY MODELI VA AMALIY ASOSLARI //Inter education & global study. – 2025. – T. 3. – №. 10 (1). – C. 256-265.