**Introduction**

Moving towards decentralized architectures, blockchain technology has gained tremendous attention in terms of addressing security, anonymity, traceability, and centralization [92]. The security of this technology stems from the use of hash functions to chain blocks to ensure immutability, as well as the use of encryption and digital signatures to secure data. The distributed nature of the blockchain ensures its availability [18]. Enabling blockchain technology in IoT can help to achieve a properly distributed consensus-based IoT system that overcomes security issues.

IoT system based on blockchain technology had a higher level of security than the IoT system that did not use blockchain technology.

To provide an IoT network with a scalable and dynamic communication architecture, a dynamic blockchain-based trust system was proposed in. The proposed architecture practically labeled all IoT devices and mapped them as full nodes and lightweight nodes. The authors assessed whether this design could improve security by managing the IDs of IoT devices while making it more difficult for attackers to impersonate IoT nodes. For example, if an attacker wants to join an IoT network by impersonating an ID, the label must first be assigned. If the attacker pretends to be a full node, high-level security verification will either catch him or make the attack extremely costly. It is also difficult if the attacker just wants to pretend to be a lightweight node because all history is recorded and the attacker must fake everything all over again each time they try to attack. However, IoT with blockchain topology should not only manage the ID but also protect the information exchanged in the IoT network. Chakraborty et al. [102] proposed a two-layered architecture for dealing with security in resource-constrained IoT nodes. The goal of the model is to provide a more feasi ble framework by considering a large number of real-time factors. The selection of efficient cryptography algorithms, in addition to blockchain, plays a significant role in further strengthening the network.

Alphand et al. [103] proposed IoTChain, an IoT secu rity management platform. IoTChain combined OSCAR architecture elements with the Internet Engineering Task Force (IETF) ACE authorization framework to provide an end-to-end (E2E) solution for secure authorized access to IoT resources. IoTChain is made up of two parts: an authorization blockchain based on the ACE framework and the OSCAR object security model, which has been enhanced with a group key scheme. While OSCAR uses the public ledger to set up multicast groups for authorized clients, the blockchain provides a flexible and trustless way to handle authorization.

CIoTA, a lightweight framework that uses the concept of blockchain to perform distributed and collaborative anomaly detection for devices with limited resources, was proposed by Golomb et al. [104]. Through self-attestation and consensus among IoT devices, CIoTA uses blockchain to incrementally update a trusted anomaly detection model. CIoTA continu ously trained an anomaly detection model while remaining resistant to adversarial attacks. CIoTA also distinguished between rare benign events and malicious activities by lever aging collective wisdom.

Rathee et al. [105] proposed a secure hybrid industrial IoT framework based on blockchain. The authors employed a hybrid industrial architecture in which various branches of a company were located in more than one country. They used a blockchain mechanism to extract information from IoT devices and store the extracted records in the blockchain to maintain transparency among multiple users in various loca tions. Furthermore, the proposed framework has been tested against the internal communication of blockchain, where IoT devices have been compromised by multiple intruders. The results were analyzed against the conventional approach and validated with improved simulated results that offer an 89% success rate over user request time, falsification attack, black hole attack, and probabilistic authentication scenarios.

Liu et al. [98] introduced a blockchain platform called VChain, which can be used in IoT. VChain is a novel blockchain scheme suitable for IoT, and it is more concrete, secure, and practical than Chainspace. VChain proposed a two-layer BFT-based consensus protocol with the HoneyBadger BFT protocol and a collective sig nature scheme as building blocks. VChain supported faulty shard-tolerance and asynchronous network models, which were not possible in Chainspace.

Huang et al. [107] proposed B-IoT, a general, scalable, and secure blockchain system for IoT. The proposed blockchain is a low-cost credit-based PoW for power-constrained IoT devices that improves both security and transaction effi ciency. To protect the confidentiality of sensitive IoT data, the authors devised a data authority management method for regulating sensor data access. Furthermore, their system was built based on a DAG-structured blockchain rather than a chain-structured blockchain, which allows high throughput. The proposed credit-based PoW mechanism, which reduces power consumption for honest nodes while increasing com puting complexity for malicious nodes, contributed to the suitability of DAG-structured for IoT systems. Furthermore, the data authority management method can protect data pri vacy without impairing system performance, which is useful in IoT systems.

Uddin et al. [108] proposed a decentralized architec ture for storing IoT data generated by smart homes/cities using blockchain. The architecture includes a secure communication protocol between power-constrained IoT devices and a gateway that employs a sign-encryption tech nique, which is a lightweight cryptography for IoT devices to ensure the privacy and security of IoT devices. The authors improved Gateway’s functionality as a Miner Selector to bridge the gap between power and memory-constraints IoT devices and blockchain. A software agent running on the gate way was proposed to select a miner node based on the miner performance parameters. The gateway chose a small group of efficient miners to speed up block processing. As a semi trusted center, the network manager increases the dependabil ity and robustness of the proposed blockchain-based smart cities/home monitoring applications.

Manzoor et al. [109] presented a blockchain-based proxy re-encryption scheme to address both scalability and trust issues, as well as to automate payments. After encryption, IoT data are stored in a cloud distributed by the system. The system created runtime dynamic smart contracts between the sensor and the data user to share the collected IoT data, eliminating the need for a trusted third party. An efficient proxy re-encryption scheme was employed to restrict access to the data to the owner and the person presented in the smart contract. The sensor encrypts the data before uploading it to the cloud storage, and then re-encrypts it before sharing.

Mohanty et al. [110] developed an efficient lightweight integrated blockchain (ELIB) model to meet IoT require ments. The presented model was divided into two major levels: smart home and overlay. It generates an overlay net work in which highly equipped resources can merge into a public blockchain, ensuring dedicated security and privacy.