Abstract: Blockchain technology is increasingly being used in the internet of things (BCoT: Blockchain for IoT) to ensure the security and reliability of data exchanged between connected devices. There are several generic blockchain architectures for IoT that differ in their network and consensus characteristics. Blockchain architectures for IoT can be compared based on various criteria such as the type of storage used, consensus, and security. They should be selected based on the specific needs of each use case, and the resource constraints of connected devices and security and resilience requirements. In this article, we present a review of blockchain architectures for the internet of things that have been studied and applied in some well-known contemporary applications.

Keywords: blockchain; internet of things; consensus; BCoT (Blockchain for IoT)

1. Introduction

The IoT is a system of connected devices that are equipped with sensors that detect environmental data and store them in a centralized cloud for analysis [1]. However, these data are vulnerable to attacks. The objective of utilizing a blockchain, which operates on a decentralized system, to link internet of things (IoT) devices, is to eradicate the need for a third-party intermediary and guarantee the protection of instantaneous data [2]. Decentralization has advantages in terms of cost, security, privacy, and eliminating third parties. By leveraging cryptography, the blockchain can establish trust without relying on a central authority. As a result, it can offer mobility, accessibility, simultaneity, lightness, scalability, and transparency in access control for the internet of things (IoT) [3].

Nonetheless, there remains uncertainty regarding how these characteristics can be implemented within the IoT framework, given the constraints of limited resources and the expanding quantity of devices in use. Furthermore, to ensure the integrity of collected data and related interactions, trust mechanisms are imperative for IoT applications [4]. Transparency, auditability, and energy efficiency requirements necessitate the integration of blockchain technology into the IoT.

To address these problems, several architectures have been proposed. The remainder of this document is organized as follows: in Section 2, we present a comparative study of the various existing BCoT architectures. In Section 3, we present a proposed blockchain architecture for the IoT, and Section 4 concludes the document.

2. Comparison of Existing BCoT Architectures

2.1. A Generic BCoT Architecture

A generic BCoT architecture is a design model that uses blockchain technology to create a distributed ledger system for devices in an IoT system. This architecture is designed to enable secure and transparent communication between different IoT devices. Data generated by the device are stored and shared using blockchain technology.
This architecture has become the basis for many other blockchain architectures, as it provides a framework for structuring and organizing the different components of a decentralized and distributed ledger system.

A generic BCoT architecture, as depicted in Figure 1, can be used with diverse IoT devices and infrastructures. Incorporating IoT devices involves a combination of cloud systems, edge computing, gateways, and a variety of IoT devices, covering a range from basic sensors that can only communicate through nearby gateways to more advanced devices with computing and processing capabilities [5].

![Figure 1. A generic BCoT architecture [2].](image)

In the literature, there are two types of architectures, device-based and gateway-based. To measure the performance between the two architectures, most researchers compare the average communication time between nodes of the blockchain for each of these architectures. The results have shown that the transmission speed is reduced when using the second architecture [2].

### 2.2. Comparison of BCoT Architectures

BCoT architectures can be compared based on different criteria, namely:

- **The type of storage used**: Blockchain enables decentralized, distributed, and secure data storage. For IoT, there are several methods of storage in the blockchain, such as storing raw data, data hashes, data proofs, or smart contracts.

- **The consensus used**: In a literal sense, consensus refers to a state of agreement. According to Seibold and Samman [6], a consensus mechanism refers to a technique used for verifying or validating a transaction or value on a blockchain or distributed ledger without having to depend on or trust a central authority.

- **Security**: In BCoT, the encryption layer is a critical component that guarantees the security, confidentiality, and integrity of both the data exchanged between connected objects and the blockchain, and the transactions executed on the blockchain. It can be used at different levels including encryption of data in transit, encryption of stored data, and transaction protection.

Table 1 presents a comparison of various architectures found in the literature based on the criteria mentioned above.
Table 1. Comparison of BCoT architectures.

<table>
<thead>
<tr>
<th>Name</th>
<th>Architecture Type</th>
<th>Consensus Used</th>
<th>Storage Used</th>
<th>Encryption Layer</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoTchain</td>
<td>Three layers architecture</td>
<td>Any lightweight consensus</td>
<td>Distributed storage</td>
<td>No</td>
<td>[7]</td>
</tr>
<tr>
<td>Hybrid IoT</td>
<td>A sub-blockchain utilizing proof of work and connected through BFT consensus</td>
<td>Proof of work and BFT</td>
<td>Each sub blockchain has its own transaction pool</td>
<td>No</td>
<td>[8]</td>
</tr>
<tr>
<td>Fogbus</td>
<td>A cost-effective interface that can be scaled and is not limited to any particular platform</td>
<td>Proof of work</td>
<td>Distributed repository nodes and backing up data to cloud infrastructure at a later time</td>
<td>Yes</td>
<td>[9]</td>
</tr>
<tr>
<td>Proxy re-encryption scheme</td>
<td>In the absence of a trusted third party, IoT data are encrypted and saved in the cloud.</td>
<td>Ethereum smart contract</td>
<td>Data are kept in the cloud while the location of that data is recorded on the blockchain</td>
<td>Yes</td>
<td>[10]</td>
</tr>
<tr>
<td>Multichain and Arduino</td>
<td>Two layers: FOG et IoT</td>
<td>Round robin</td>
<td>Data processed in FOG</td>
<td>No</td>
<td>[11]</td>
</tr>
<tr>
<td>Decentralized access control system</td>
<td>Management hub node requests blockchain access information on behalf of IoT devices</td>
<td>One and only smart contract and private Ethereum [12]</td>
<td>Distributed storage in miner nodes</td>
<td>Yes</td>
<td>[3]</td>
</tr>
<tr>
<td>Trust Architecture</td>
<td>Three layers architecture</td>
<td>Distributed consensus based on reputation, private blockchain</td>
<td>Off-chain storage for data, and on-chain storage for transactions</td>
<td>Yes</td>
<td>[4]</td>
</tr>
</tbody>
</table>

IoTchain [7] is a security architecture designed for the internet of things (IoT) that operates on a three-layer blockchain system. This architecture offers a range of features, including identity verification, access control, privacy protection, and resistance to denial of service (DoS) attacks, all while remaining lightweight and fault-tolerant. To ensure the integrity of the system, the architecture employs the use of hardware security models (HSM) to create and store key pairs, and stores hashes using Merkle trees. Nodes are registered via a certification layer, and their key pairs are added to the HSM to prevent fraudulent activity.

Hybrid IoT [8] merges proof of work and Byzantine fault tolerance (BFT) mechanisms by establishing a sub-blockchain based on proof-of-work, which is subsequently interconnected using BFT. Each sub-blockchain is supported by an independent centralized storage system.

FogBus [9] has been introduced as a solution that facilitates computing near IoT devices by bringing cloud and network computing resources closer to the edge. FogBus is designed to integrate various IoT systems into a fog and cloud infrastructure and operates under a platform-as-a-service (PaaS) model, which allows developers to create various types of IoT applications, tailor services, and oversee resources. To ensure data protection, FogBus provides authentication and encryption techniques.

Manzoor et al. [10] suggested an architecture involving IoT devices, miners, a cloud server, and a data requester, which are all linked via the internet. IoT sensors send data to the cloud, where they are encrypted and subsequently saved. After registering the sensor on the blockchain, the sensor owner can execute smart contracts on the sensor transactions and obtain the necessary key to encrypt the data. Although, instead of being
saved on the blockchain, the data are kept in a centralized cloud. Another paper discusses a blockchain system designed for IoT that is implemented with numerous nodes, including an Arduino [11].

Novo [3] puts forward a decentralized access management system architecture that utilizes blockchain technology to save and distribute access control information. However, the architecture does not incorporate IoT devices directly into the blockchain. Instead, a novel node, referred to as a management hub, is introduced, which functions as a mediator between IoT devices and the blockchain, to request access control information. The system also employs managers, who engage with the one smart contract to create the system’s access control protocol [13].

A trust architecture [4] is composed of three primary layers: the data layer, the blockchain layer, and the application layer. Data are accumulated off-chain, while transactions are registered on the blockchain. The blockchain layer collaborates with the application layer to handle the data and adapt the block validation mechanism. To manage trust, two crucial modules are proposed [14]: the data trust module and the gateway reputation module [15]. These modules empower the blockchain layer to flexibly adjust validation demands by utilizing updated reputation scores. Furthermore, the application layer can incentivize nodes with high reputation scores by offering economic incentives [16].

3. Discussion

We compared several architectures for integrating blockchain into IoT. In BCoT, it is essential to give meticulous attention to the design of data storage and confidentiality, as they are critical components. The majority of the architectures we examined employ centralized cloud storage, which is in opposition to the primary goal of the blockchain and could potentially result in a single point of failure. Nevertheless, a few have utilized distributed storage, which provides no safeguards for data. Safeguarding the confidentiality of distributed storage is a challenging task. As a result, we have concluded that a viable architecture for BCoT is currently unavailable. Considering the extensive benefits that blockchain can provide to IoT, we are convinced that it has the potential to revolutionize cloud computing systems.

In the end, the choice of blockchain architecture is reliant on the specific needs of the IoT application in question [17]. Some applications may require a more censorship-resistant architecture, while others may require a more secure architecture. Additionally, economic and energy aspects must also be taken into account when choosing the appropriate blockchain architecture.

4. Proposed Architecture

Figure 2 shows a potential architecture for integrating blockchain into the IoT. It consists of six layers, namely:

![Figure 2. Potential architecture for integrating blockchain into IoT.](image-url)
• Perception layer: IoT devices collect data and send them to a blockchain network via management nodes.
• Management layer: they are special nodes that connect constrained IoT networks to the blockchain network.
• Blockchain layer: The blockchain network stores data and transactions using decentralized consensus. APIs allow developers to create applications to collect and use IoT data stored on the blockchain network.
• Application layer: an application can be developed to facilitate the management and visualization of IoT data stored on the blockchain network.
• Security layer: this layer is transverse to all previous layers.

This architecture shows how IoT devices collect data, transmit them to a blockchain network through management nodes, and how these data are stored and validated on the blockchain network. APIs allow developers to create applications to interact with the IoT data stored on the blockchain network.

5. Conclusions
All in all, our survey highlighted various architectures for a blockchain-based IoT. The analysis of these architectures showed that the design of data storage and confidentiality of data are important. BCoT architectures have several similarities and differences depending on their design, functionality, and ability to solve specific IoT problems. To implement blockchain-based IoT, it is necessary to design a solution that is energy-efficient, secure, and scalable. It is necessary to equip IoT devices with adaptive storage capabilities and ample computing power, to facilitate transaction management and digital signature verification.

Author Contributions: Conceptualization, Y.E., A.B., M.O. and H.S.; methodology, Y.E. and A.B.; software, Y.E. and A.B.; validation, M.O. and H.S.; formal analysis, Y.E., A.B., M.O. and H.S.; investigation, Y.E. and A.B.; resources, Y.E. and A.B.; data curation, Y.E. and A.B.; writing—original draft preparation, Y.E. and A.B.; writing—review and editing, M.O. and H.S.; visualization, Y.E., A.B., M.O. and H.S.; supervision, M.O. and H.S.; project administration, M.O. and H.S.; funding acquisition, Y.E., A.B., M.O. and H.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References


**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.