Robertas DAMAŠEVIČIUS, Sanjay MISRA, Rytis MASKELIŪNAS, Anand NAYYAR, 2024. Convergence of blockchain and Internet of Things: integration, security, and use cases. *Frontiers of Information Technology & Electronic Engineering*. 25(10):1295-1321. https://doi.org/10.1631/FITEE.2300215

Convergence of blockchain and Internet of Things: integration, security, and use cases

Key words: Blockchain; Internet of Things (IoT); Blockchain-based IoT (B-IoT); Security; Scalability; Privacy

Corresponding author: Anand NAYYAR
E-mail: anandnayyar@duytan.edu.vn
ORCID: https://orcid.org/0000-0002-9821-6146

Motivation

1. The purpose of this work is to provide a comprehensive review of the integration of blockchain and IoT technologies, their security solutions, and their applications in various fields.
2. This study aims to highlight the potential benefits and challenges of B-IoT. The significance of this work lies in its contribution to the understanding of how blockchain and IoT can be combined to create secure, decentralized, and tamper-proof systems for data management and communication.
3. This research provides insights into the potential impact of B-IoT in industries such as healthcare, supply chain management, energy, transportation, and smart cities. By identifying the challenges and future research directions, this study serves as a guide for researchers, practitioners, and policymakers in exploring the possibilities and implications of B-IoT technology.

Main idea

- This research addresses the major puzzle and controversy around the integration of blockchain and IoT technologies. Although the potential benefits of this integration are widely recognized, there are significant challenges and unresolved issues that need to be addressed. The puzzle lies in finding effective solutions to ensure the seamless integration, scalability, security, and privacy of B-IoT systems.
- The controversy arises from the divergent opinions and approaches in tackling these challenges, as well as the ongoing debate on the feasibility and practicality of implementing blockchain in IoT applications. By addressing these puzzles and controversies, this research aims to provide valuable insights and recommendations to bridge the gap between theory and practice in B-IoT systems.

Overview of IoT and blockchain

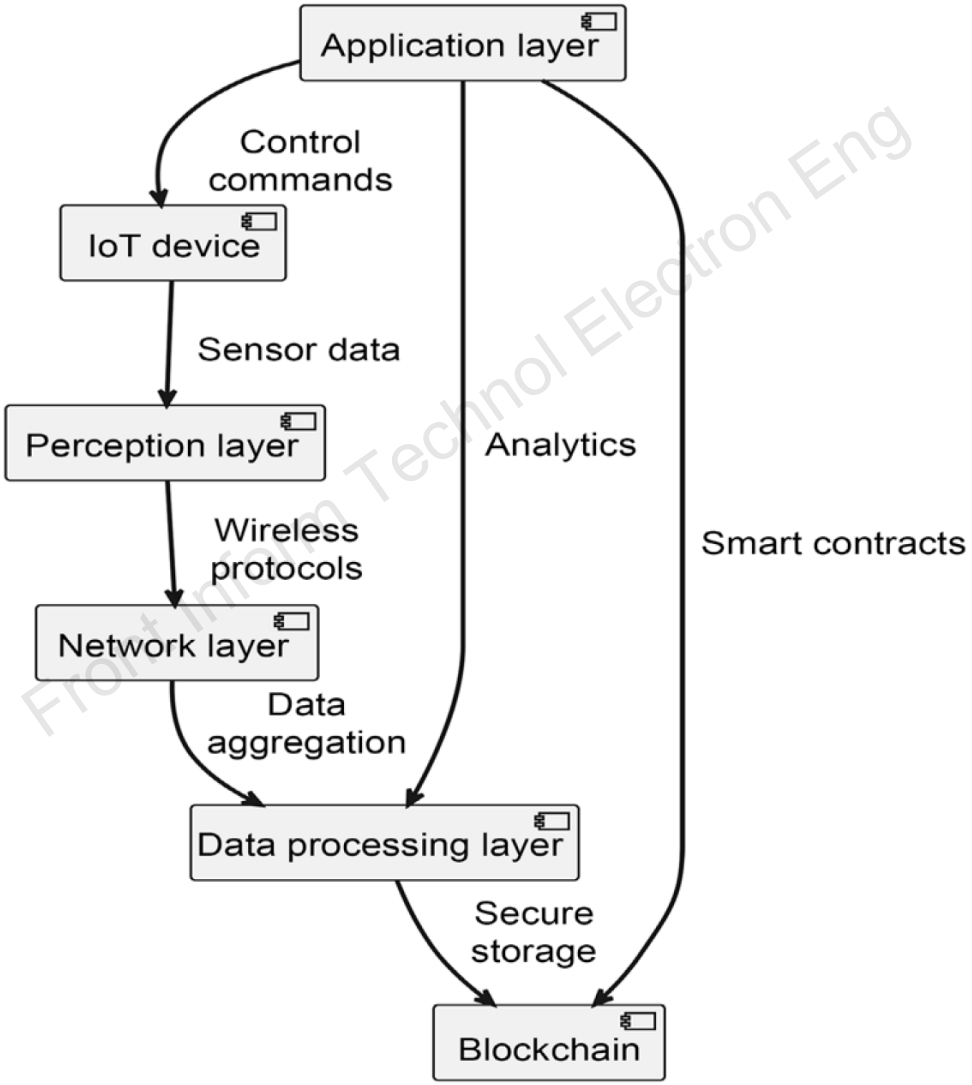
- IoT refers to a network of interconnected physical objects, such as devices, sensors, vehicles, and buildings, which can collect and share data with each other or with other systems over the Internet. An IoT architecture typically includes devices or things, gateways, network infrastructure, cloud platforms, and applications. IoT devices or things are the physical objects such as sensors, actuators, and smart devices that collect and transmit data. Gateways act as intermediaries between devices and the cloud, and perform data aggregation, filtering, and protocol translation.
- Blockchain is a distributed ledger technology that provides a secure and decentralized platform for recording and sharing data. It was first introduced in 2008 as part of a white paper authored by an unknown person or group going by the pseudonym Satoshi Nakamoto, which outlined the concept of a digital currency called Bitcoin. Blockchain was initially used as the underlying technology for Bitcoin to provide secure and transparent transactions between users without the need for a centralized intermediary such as a bank.

Integration of IoT and blockchain

- The integration of IoT and blockchain has become popular as businesses and industries seek to enhance the security, scalability, and transparency of their digital infrastructures.
- Blockchain technology provides an innovative solution to these issues by enabling distributed and decentralized storage and processing of data. By integrating IoT and blockchain, businesses can create a more secure and transparent digital infrastructure that allows for real-time data sharing, tracking, and verification.

- Integration of IoT and blockchain offers a range of benefits for businesses and industries looking to create a more secure, transparent, and efficient digital infrastructure. By leveraging the strengths of both technologies, businesses can create a more trustworthy ecosystem that enables automated transactions, real-time data sharing, and secure product tracking.

B-IoT layers and components



Countermeasures to secure B-IoT systems

- Access control
- Encryption
- Integrity
- Secure communication
- Secure analytics
- Blockchain technology

Blockchain based security solutions in IoT

- Smart contracts and decentralized control
- Immutable data storage
- Identity and access management
- Consensus mechanisms

Use cases and applications of B-IoT

- Supply chain management
- Healthcare and assisted living
- Energy and utilities
- Smart cities and transportation

Conclusions

- This article discusses the integration of blockchain and IoT as a solution to address the security and privacy concerns in IoT systems. It describes the concept and emergence of blockchain, mathematical models, and countermeasures for B-IoT security.
- The article also highlights the multi-layered architecture of B-IoT, along with smart contracts, decentralized control, immutable data storage, IAM, and consensus mechanisms as blockchain-based security solutions.
- It covers scalability issues, security vulnerabilities, convergence challenges, privacy and data protection issues, ownership and control of data issues, trust and transparency issues, and governance and regulation issues in B-IoT.
- Furthermore, the article explores the applications of B-IoT in various fields, such as smart cities and transportation, energy and utilities, healthcare and assisted living, and supply chain management. Finally, the article provides several examples of B-IoT systems specified using unified modeling language (UML), including a traffic management system, smart grid management system, remote patient monitoring system, and inventory management system.