Blockchain Technology and Energy Consumption

Subjects: Telecommunications

Contributor: Kithmini Godewatte Arachchige , Philip Branch , Jason But

Blockchain technology is an information security solution that operates on a distributed ledger system. Blockchain technology has considerable potential for securing Internet of Things (IoT) low-powered devices. Because IoT devices are typically low-powered battery-powered devices, the energy consumption of any blockchain node must be kept low. IoT end nodes are typically low-powered devices expected to survive for extended periods without battery replacement. Energy consumption of blockchain algorithms is an important consideration in any application that combines both technologies, as some blockchain algorithms are infeasible because they consume large amounts of energy, causing the IoT device to reach high temperatures and potentially damaging the hardware; they are also a possible fire hazard.

blockchain Internet of Things energy temperature security low-powered

1. Introduction

Blockchain technology and the Internet of Things (IoT) are innovative technologies that are proving useful in industries as diverse as healthcare, automotives, finance, and supply chain logistics [1]. Security features including the decentralised nature of blockchain technology may address many cybersecurity issues in those respective industries. Aged care is one area that has recently started using IoT technology [2]. Aged care is primarily concerned with the health and wellbeing of elderly people. Lack of information transparency and data leakage in aged care could be life-threatening. The IoT industry uses low-powered microcontroller devices to develop ambient assisted living systems for the aged care industry, and potential data corruption or miscalculation can put lives at risk [3].

The combination of blockchain and IoT technologies creates intrinsic benefits. Securing IoT end devices, which has been a challenge, is one of the key benefits. Blockchain technology has also benefited from microcontroller developments in the emergence of energy-efficient IoT devices and blockchain algorithms [4]. As low-powered microcontroller devices are portable and cost-effective, the IoT industry uses these microcontroller devices to develop and manufacture sensor-based IoT devices. Connected IoT end devices may process a large amount of sensitive sensor data, and it may be difficult to locate the source of a data leak in an event of a cyber threat [4].

Blockchain technology may help ease the potential security and scalability issues of sensor networks. Blockchain technology adds another layer of security to data transmission, and makes it more difficult for cyber attackers to gain access. Additionally, it brings transparency to network access [5]. Alongside increasing the trust between

parties involved, the blockchain can have other benefits, including the elimination of specialist gateways solely intended to secure IoT sensor networks [6].

However, the integration of blockchain technology and microcontroller technologies can be a challenge due to energy consumption requirements [7]. Blockchains require significant computational resources, and thus consume additional energy in energy-constrained sensor devices, leading to higher temperatures. These higher temperatures may damage hardware devices and cause possible fire hazards. Fire hazards can put lives at risk. Understanding potential device temperature levels will contribute to preventing possible fire hazards. Additionally, the size and complexity of the blockchain network can also play a role in the energy consumption and temperature variations of hardware devices. A larger network with more nodes and transactions requires more energy to maintain and process [7].

2. Blockchain Technology and Energy Consumption

Blockchain technology gained public recognition with the first blockchain algorithm, Bitcoin, which was established in 2008. In the last decade, blockchain technology has developed considerably, with a wide range of applications including Ethereum, Monero, Hydrachain, Duino Coin and Hyperledger Fabric [8]. Blockchain technology was invented as an information security solution for cryptocurrency, operating as a digital ledger system. However, researchers have realised that blockchain technology holds the potential to address many cybersecurity issues beyond cryptocurrency [9].

A blockchain forms a shared network among end devices which are called as blockchain nodes. There are three main different blockchain networks.

2.1. Public Blockchain Networks

Public blockchain networks provide unrestricted user access for all blockchain users to the blockchain network and security features. These public blockchain networks are called permissionless blockchain networks [9]. Users can read, write or alter transactions as per their requirements. These types of blockchain networks are self-governed networks that allow users to use security features such as encryption, time stamps, anonymity, and hashes. **Figure 1** shows the architecture of a public blockchain network [9]. The green-coloured dots indicate the users who have access to the blockchain network and services. As per **Figure 1**, all users have access to the blockchain network and its services in public blockchain networks.

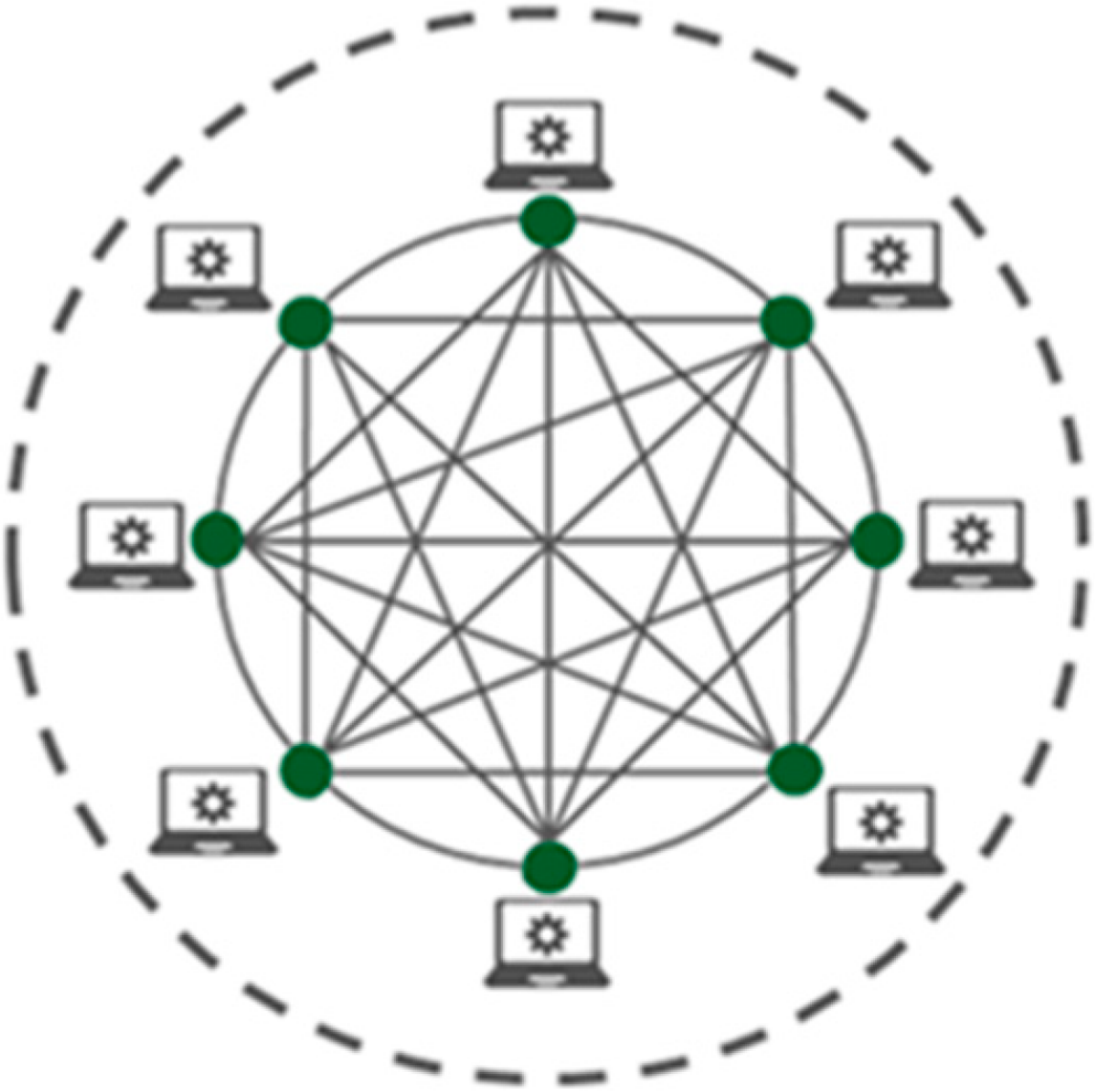

Figure 1. Public blockchain network.

2.2. Private Blockchain Networks

Private blockchain networks provide restricted access wherein only authorised users can have access. Participants can only join these private blockchain networks through an invitation, and are required to verify their identification [10]. User validations are controlled by automated smart contracts [9]. Private blockchain networks are called permissioned blockchain networks. Additionally, only selected or authenticated users can access the shared ledger. **Figure 2** shows the architecture of a private blockchain network [9]. The green-coloured dots in **Figure 2** indicate the users who have access to the blockchain network and services, and the red-coloured dots indicate the users who do not have access to the blockchain network and services. As **Figure 2** shows, only authorised users have access to the blockchain network and its services in private blockchain networks.

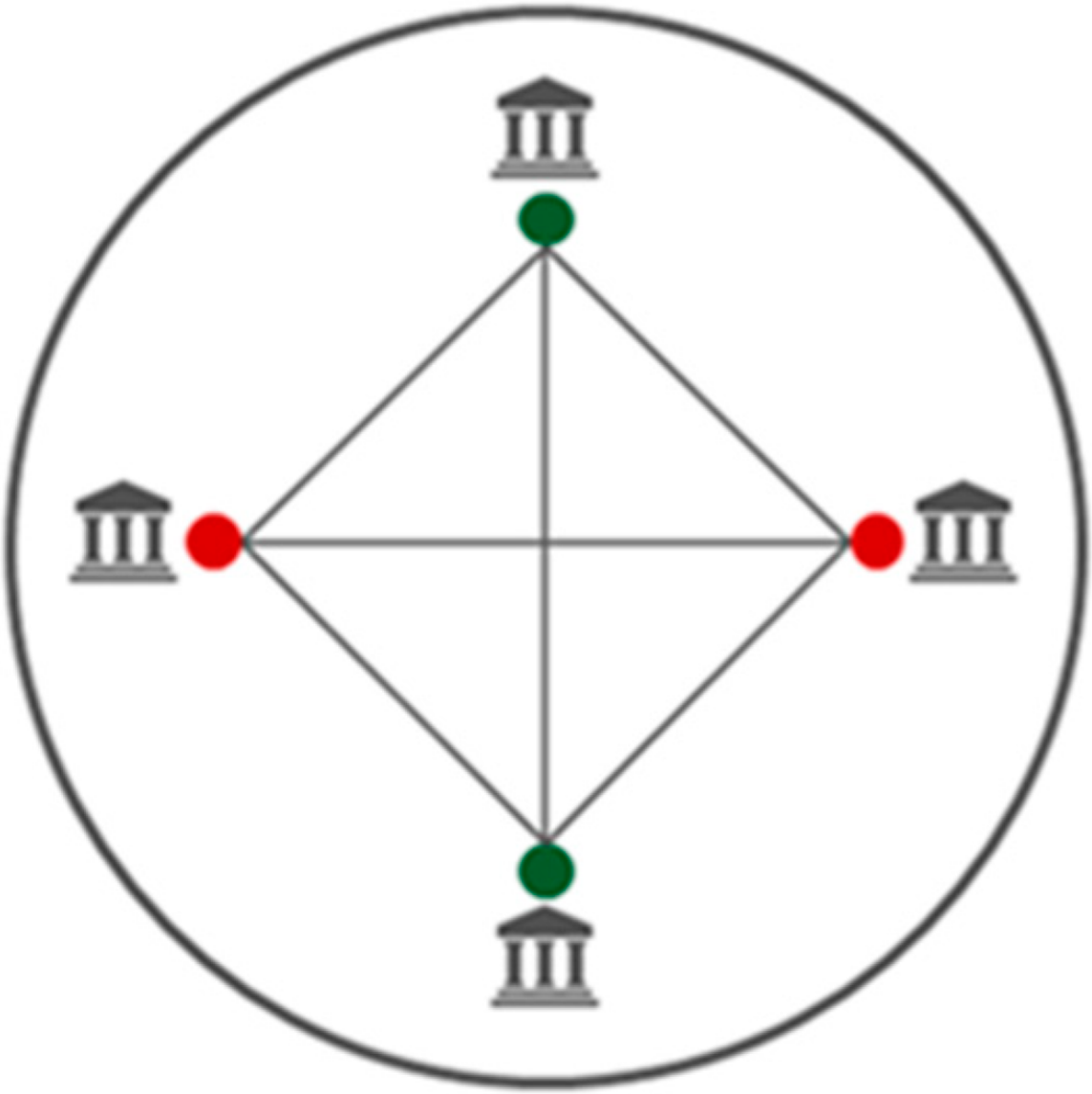

Figure 2. Private blockchain network.

2.3. Hybrid Blockchain Networks

Hybrid blockchain networks are a combination of private blockchain networks and public blockchain networks. They blend essential blockchain components and protocols of both private and public blockchain networks. Any blockchain user can access the blockchain network, but only certain users can access all security features and services [11]. Hybrid blockchains are owned by a private user who can grant access to the public via smart contracts. The structures of hybrid blockchain networks are highly customisable, and users can choose their desired type of transactions. **Figure 3** shows the architecture of a hybrid blockchain network [12]. As **Figure 3** indicates, the green-coloured dots indicate users who have access to the blockchain network and services. The red-coloured dots show the users who do not have access to the blockchain network and its services. **Figure 3** shows that every user has access to the blockchain network, but only certain users have access to blockchain network services.

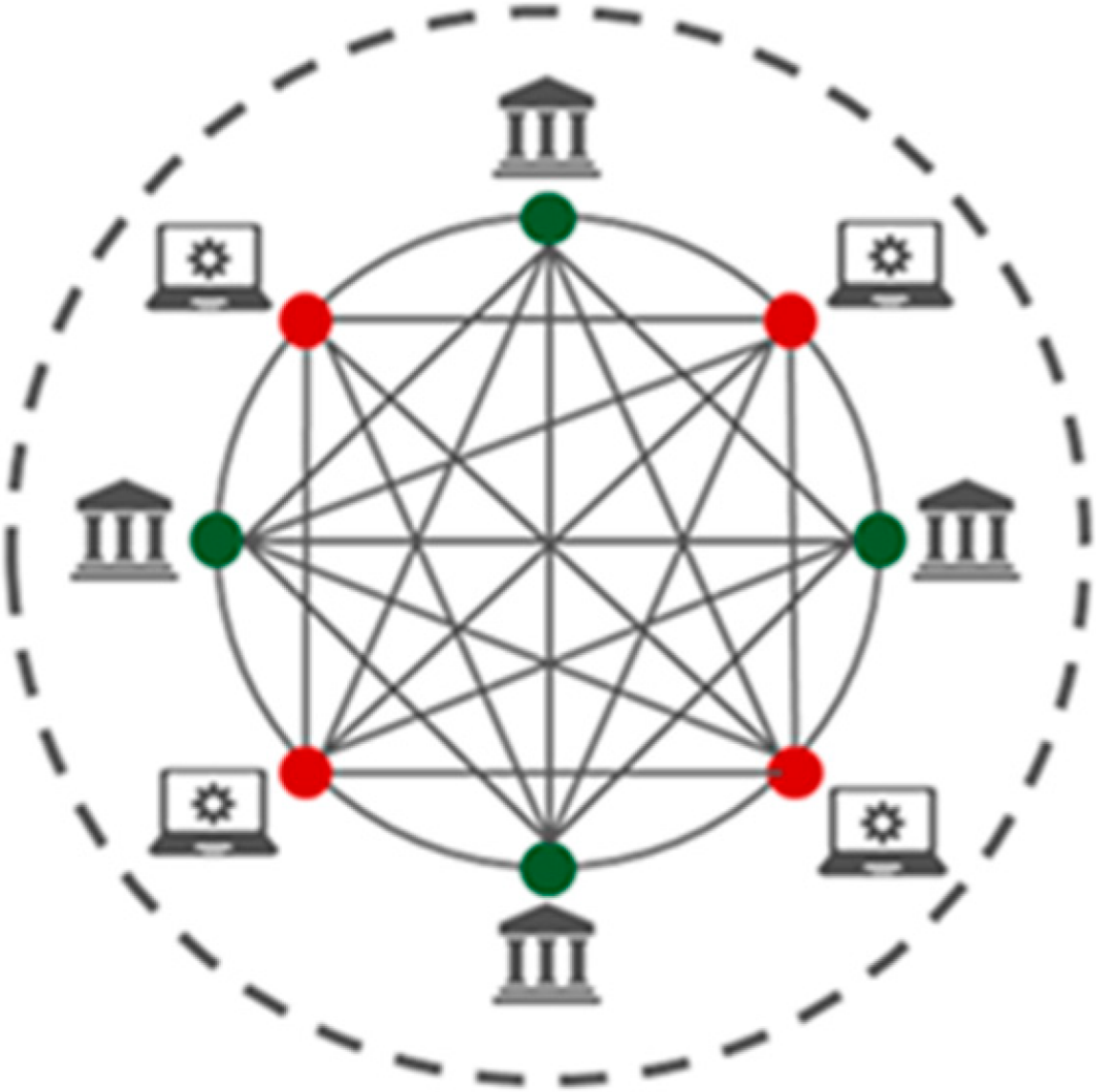

Figure 3. Hybrid blockchain network.

Blockchain technology has primarily been designed for computers with high processing power. However, with the development of the IoT industry, some researchers have begun to focus on energy-efficient blockchain solutions for low-powered IoT devices [13]. In particular, the aged care sector has started using IoT sensor-based devices to develop ambient assisted living systems [14]. As the aged care sector uses low-powered microcontroller devices to implement ambient assisted living systems and health sensor networks, blockchain algorithms must be energy-efficient [14]. The development of blockchain algorithms for IoT low-powered devices is an increasingly active research area [15].

However, very little research has been conducted to identify blockchain energy consumption variations in low-powered microcontroller devices. Blockchain energy consumption in microcontroller devices is a significant factor that needs to be evaluated, as IoT end nodes are expected to run for long periods without battery replacement.

Modern, IoT solutions also focus on renewable energy solutions. As a result of this, low-power IoT devices and energy solutions have been significantly improved by researchers [16]. Understanding the energy requirements of blockchain technologies will contribute to the use of suitable renewable energy sources for low-powered sensor networks. Different blockchain algorithms may consume different amounts of energy, and energy consumption is an important consideration when choosing which blockchain algorithm to use on low-powered microcontroller devices. Low-powered IoT device performance and energy consumption may also be correlated. If the energy consumption of a particular blockchain algorithm is high, the performance of the microcontroller device may be negatively affected [17].

To establish maximum blockchain functionality in a microcontroller device, the utilisation of energy may be necessary. Understanding the energy consumption of low-powered microcontrollers and different blockchain algorithms is important, because it affects battery life and microcontroller performance.

References

1. Anagnostakis, A.G.; Giannakeas, N.; Tsipouras, M.G.; Glavas, E.; Tzallas, A.T. IoT Micro-Blockchain Fundamentals. Sensors 2021, 21, 2784.
2. Cernian, A.; Tiganoaia, B.; Sacala, I.; Pavel, A.; Iftemi, A. PatientDataChain: A Blockchain-Based Approach to Integrate Personal Health Records. Sensors 2020, 20, 6538.
3. Fang, W.; Zhang, W.; Chen, W.; Pan, T.; Ni, Y.; Yang, Y. Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey. Wirel. Commun. Mob. Comput. 2020, 2020, 2643546.
4. Fu, J.; Wang, N.; Cai, Y. Privacy-Preserving in Healthcare Blockchain Systems Based on Lightweight Message Sharing. Sensors 2020, 20, 1898.
5. König, L.; Korobeinikova, Y.; Tjoa, S.; Kieseberg, P. Comparing Blockchain Standards and Recommendations. Future Internet 2020, 12, 222.
6. Forkan, A.R.M.; Branch, P.; Jayaraman, P.P.; Ferretto, A. An Internet-of-Things Solution to Assist Independent Living and Social Connectedness in Elderly. Trans. Soc. Comput. 2019, 2, 14.
7. Dib, O. Consortium Blockchains: Overview, Applications and Challenges. Res. Gate 2018, 11, 51–64.
8. Belotti, M.; Bozic, N.; Pujolle, G.; Secci, S. A Vademecum on Blockchain Technologies: When, Which, and How. IEEE Commun. Surv. Tutor. 2019, 21, 3796–3838.
9. Deep, S.; Zheng, X.; Karmakar, C.; Yu, D.; Hamey, L.G.C.; Jin, J. A Survey on Anomalous Behavior Detection for Elderly Care Using Dense-Sensing Networks. IEEE Commun. Surv. Tutor. 2020, 22, 352–370.

10. Coin-a Simple, Eco-Friendly, Centralized Coin. Available online: https://duinocoin.com/ (accessed on 10 April 2023).
11. Feng, H.; Wang, W.; Chen, B.; Zhang, X. Evaluation on Frozen Shellfish Quality by Blockchain Based Multi-Sensors Monitoring and SVM Algorithm During Cold Storage. IEEE Access 2020, 8, 54361–54370.
12. Kazım Rıfat Ozyılmaz, A.Y. Designing a blockchain-based IoT infrastructure with Ethereum, Swarm and LoRa. IEEE Consum. Electron. Mag. 2018, 8, 28–34.
13. Guo, Q.; Yang, F.; Wei, J. Experimental Evaluation of the Packet Reception Performance of LoRa. Sensors 2021, 21, 1071.
14. Bigini, G.; Freschi, V.; Lattanzi, E. A Review on Blockchain for the Internet of Medical Things: Definitions, Challenges, Applications, and Vision. Future Internet 2020, 12, 208.
15. Alam, S.; De, D. Analysis of Security Threats in Wireless Sensor Network. Int. J. Wirel. Mob. Netw. 2014, 6, 35–46.
16. Sedlmeir, J.; Buhl, H.U.; Fridgen, G.; Keller, R. Recent Developments in Blockchain Technology and their Impact on Energy Consumption; Springer: Berlin/Heidelberg, Germany, 2021.
17. Bada, A.O.; Damianou, A.; Angelopoulos, C.M.; Katos, V. Towards a Green Blockchain: A Review of Consensus Mechanisms and their Energy Consumption. In Proceedings of the 2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS), Pafos, Cyprus, 14–16 July 2021; pp. 503–511.