A Proposal to Research the Viability of Using Blockchain Technology to Secure IoT Wireless Sensor Networks

Summary

As the IoT industry continues to expand into data-sensitive areas such as healthcare, military, and supply-chains, the need for security increases. The information stored in centralized databases, the current standard, can be compromised from a single vulnerability. Blockchain technology offers a decentralized, anonymous, immutable, and cryptographically secure storage system that can be configured for the low processing power of IoT devices. Moreover, the additional use of non-fungible tokens (NFTs) provides a means for better authenticating nodes in a network. Although these qualities are desirable, large block sizes in the chain can slow the rate of data transmission in networks that require real-time updates. The proposed research will evaluate blockchain's ability to securely transfer data, maintain transfer efficiency, and store collected data across devices in an IoT network.

Project Significance

The Internet of things (IoT), the collection of devices that are connected through the Internet to users and other devices, is one of the fastest-growing areas of technology today (Zhang et al., 2014). Currently, there are approximately 12 billion connected IoT devices around the world. That number is projected to grow to about 30 billion devices by 2025, amounting to 4 devices for every human on earth (Leuth). These devices have the capability of forming wireless sensor networks (WSNs) which consist of sensor-equipped IoT devices that monitor and report environmental conditions. Because the IoT networks are low-cost and low-power information collectors and transmitters, they are used to increase manufacturing output and improve healthcare services. John Deer and UPS use IoT tracking in their fleet to make their supply chain more efficient. GE uses IoT devices to measure data about their jet engines, turbines, and wind farms, and use that data for preventative maintenance (Lee et al., 2015). IoT devices are even used by vaccine manufacturers such as Pfizer to gather temperature data inside of frozen, packaged DNA during shipment for quality assurance (Cott et al., 2021). These systems are also used in healthcare to remotely monitor patients' conditions and offload that work from staff, improving the efficiency and effectiveness of treatment (Chou, 2019).

Because often sensitive data is being collected by IoT devices about people and systems, security has become an increasing focus. Unfortunately, most devices have limited processing power and storage, so their encryption algorithms are not as extensive as other, more powerful systems (Arcenegui et al., 2021). In many cases, encryption and antivirus protocols are not deployed at all (Zhang et al., 2014). A 2014 Hewlett Packard study found that 70% of common IoT devices contained serious security vulnerabilities with an average of 25 vulnerabilities per device (Lee et al., 2015). Moreover, a 2014 study found that of the 700 IoT devices they studied, 123 of them had at least one critical vulnerability (Costin et al., 2014). Since most networks are currently using a centralized database, a single point of security failure in the system can give an attacker access to all data. Alarmingly, it was found that 70% of healthcare providers had a data breach on their patient data between 2018 and 2019 (Srivastava et al., 2019). With these

vulnerabilities, the current IoT system with centralized authority and unsecured networks is unsatisfactory.

To remedy these issues and securely store and transfer data, researchers have been turning to blockchain technology. Blockchain was first invented by Satoshi Nakamoto in 2009 with their release of Bitcoin, the first cryptocurrency. Although the monetary value of cryptocurrencies has skyrocketed in recent years, the underlying technology has a value of its own. At its core, blockchain is a decentralized collection of records, meaning it is distributed across all nodes in the network. Records are compiled into blocks that use the unique identifier of the previous block and the contents of the current block to generate a new unique identifier (Omar et al., 2020). Because each block is linked to the last and the validity of each block is determined by the consensus of a majority of nodes, the data is virtually immutable (Sultana et al., 2019). Furthermore, the data being transferred between nodes is secured using asymmetric cryptography. This encryption system ensures that data being transferred can only be decrypted with a private key held by the recipient. Blockchain also maintains anonymity between those involved in the transaction by randomly generating usernames for each user (Zheng et al., 2017). Because of these qualities, blockchain has become an attractive alternative to the traditional centralized database.

Migrating to blockchain seems like the natural choice for securing a network of IoT devices. Many articles published in the past five years with proposed blockchain networks back the idea that this technology has benefits in securing IoT networks. One such model by Manogaran (et al., 2021) distributes collected data across all devices in the network using blockchain. Each block of data is cryptographically chained to the previous block, ensuring that data is immutable. Access control is also managed through blockchain, where encrypted data is sent as a transaction from one device to another. Because the information sent between nodes is encrypted, adversaries must alter permissions stored on the blockchain to gain access. However, consensus algorithms ensure that permissions cannot be changed. Not only did the authors achieve heightened security, but also faster data transfer using distributed data. With this design, the researchers reduced information request delay by 11.91% when compared to Amazon's S3 centralized cloud storage.

Non-fungible tokens have also been studied to better authenticate nodes in a network, preventing an adversary from impersonating a device. NFTs represent uniquely identifiable certificates of ownership located on the blockchain. They ensure that a digital asset can be traced back to a single source (Arcenegui et al., 2021). While traditional requests to databases require proper authentication to be attached to each request for information, NFTs require a single exchange of an immutable token of authenticity. Therefore, it reduces overall transfer size and increases efficient data transmission (Omar et al., 2020). Once a device has received an NFT from another device, it is authorized to access information from the sender (Arcenegui et al., 2021). Omar (et al., 2020) found that although latency is high for token generation, only a single token is needed to establish a link, and subsequent requests can occur much faster. NFTs can be used to complement wireless sensor networks that use asymmetric cryptography in their blockchain data storage. Arcenegui (et al., 2021) introduce a physically unique hardware

component to each device that generates a decryption key. The NFT encapsulates encryption and decryption keys. When the recipient receives the token, a secure line of communication can exist. In summary, this heightened level of security guarantees that no adversary can impersonate a node in the network as all authenticated nodes are linked immutably in the blockchain.

Though blockchain has desirable qualities for security, it is not without flaws. For one, total anonymity cannot be guaranteed. A recent study done on Bitcoin revealed that transactions can still be linked to a user's real identity through studying patterns in their transactions (Zheng, et al., 2017). This sort of tracking could potentially be applied to IoT healthcare networks to learn the identity of patients whether or not the actual data has been decrypted. Furthermore, efficient data transfer can be compromised when the number of devices in a network grows significantly large. Manogaran (et al., 2017) found that once their network grew to 1000 nodes, their request rate was slower than using Amazon's cloud services by a factor of 2. The efficiency of a network is also dependent on the size of blocks in the chain. Larger blocks take longer to propagate across the network and can stall the fulfillment of information requests from devices and users on the network. For devices that require real-time updates like jet engine data recorders or remote patient monitoring devices, slowing computational rates is not a viable option (Srivastava et al., 2019). However, larger block sizes take longer to fill with information, and the hashing required to generate a unique identifier for the block occurs less frequently. Therefore, data can be added to the blockchain at a greater overall rate. A balance must be achieved between collection and transmission rates, a decision that is dependent on the network requirements and limitations.

Objectives

I propose to research the viability of using blockchain technology for the secure transfer of data between nodes in an IoT wireless sensor network. Below is a list of the main objectives that I would like to achieve through this research project.

1. Provide necessary technical background on the characteristics of blockchain technology pertinent to IoT network security: decentralized storage, secure data collection, and node authentication.
2. Evaluate blockchain-based IoT networks on their vulnerability to data interception, ability to store data across all nodes in the network, and efficiency in transmitting data between nodes.
3. Make a recommendation for the best overall IoT network based on the criteria listed in objective 2. This recommendation may come from a single source or be a combination of design features from multiple sources.

Limitations:

Although IoT networks have uses across many different fields and industries, the core technology remains the same. IoT devices gather data through their sensors and transmit that data through a public or private network to intermediary devices and end-users. Therefore, I will not be limiting the scope of this study to one particular field or industry. However, the criteria

used to evaluate IoT networks of interest will be limited to the network's vulnerability to data interception, storage capability, and transmission efficiency. I am imposing this limitation to evaluate IoT networks on their security and their ability to maintain the attractive qualities of IoT: real-time data collection and fast data transfer. Furthermore, studying all potential criteria and metrics for IoT networks would be too much to cover in 9,000 words. Though I will ultimately make a recommendation for the best overall IoT network, I understand that there are many different IoT devices and networks, each with its limitations. Therefore, not only will I make a recommendation for the best overall IoT network, but will make recommendations based on the size of the network, the need for fast data transfer, and the need for secure data storage.

Research Plan

The first objective, to provide necessary background on blockchain, can be achieved through articles dedicated to blockchain's architecture. Zheng (et al., 2017) provide a comprehensive overview of blockchain technology. This peer-reviewed article discusses the qualities of blockchain - decentralization, persistency, anonymity, and auditability - and the design features that lead to them. Information on NFT's ability to authenticate nodes can be found through two sources: Omar (et al., 2020) and Arcenegui (et al., 2021). Both sets of authors detail the necessary technological background of blockchain and NFTs to understand its relevance for IoT networks. To gain further understanding of NFT technology, Chohan (2021) discusses the current use of NFTs and their security limitations. Chohan is the Research Director at the Critical Blockchain Research Initiative and provides sufficient information on how NFTs can securely authenticate a single node in a network.

I have already found articles relevant to the second objective, which is to evaluate proposed systems on three criteria: vulnerability to data interception, ability to store data across all nodes in the network, and efficiency in transmitting data between nodes. Omar (et al., 2020) and Arcenegui (et al., 2021) both have mock systems for using NFTs to authenticate nodes and secure data transfers. They give relevant statistics on their network's data transfer efficiency and thorough explanations of their system's defense against attack. Furthermore, Burkhalter (et al., 2017) give a unique system for using blockchain for controlling access management of stored data. The authors provide a means for distributing data across devices in a network and give metrics on their request fulfillment efficiency. Lastly, Zhaofeng (et al., 2020) presents the role of blockchain in networks that require large amounts of data. The authors of this article present a hybrid approach to data storage with blockchain used for data transfer from a centralized database to the user. It explains in detail its security methods and gives transaction latency relative to the number of samples requested.

Making a recommendation on the best IoT will largely depend on the articles used to support objective two. Unfortunately, sources found for objective two do not have a standardized set of metrics for evaluating their systems. There are unique variables in each design not limited to devices used, size of the network, control systems used for comparison, and latency measurements. Measuring efficiency will require generalized comparisons backed by the statistics that are given for each. For security, I will be using a peer-reviewed article by Alaba (et al., 2017) which discusses the current security threats facing IoT devices in conjunction with

articles on proposed systems. I can then assess the security features of blockchain-based IoT network designs against a list of current IoT security issues. From there, the most useful security features can be selected and included in the overall recommendation. Efficiency metrics from the designs will aid in tailoring recommendations to specific network requirements.

References

Alaba, F. A., Othman, M., Hashem, I. A., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88*, 10-28. doi:10.1016/j.jnca.2017.04.002

Arcenegui, J., Arjona, R., Román, R., & Baturone, I. (2021). Secure Combination of IoT and Blockchain by Physically Binding IoT Devices to Smart Non-Fungible Tokens Using PUFs. *Sensors, 21*(9), 3119. doi:10.3390/s21093119

Chohan, U. W. (2021). Non-Fungible Tokens: Blockchains, Scarcity, and Value. *SSRN Electronic Journal*. doi:10.2139/ssrn.3822743

Chou, S. (2018). THE FOURTH INDUSTRIAL REVOLUTION: DIGITAL FUSION WITH INTERNET OF THINGS. Journal of International Affairs, 72(1), 107-120. Retrieved June 25, 2021, from https://www.jstor.org/stable/26588346

Cott, E., DeBruyn, E., & Corum, J. (2021, April 28). How Pfizer Makes Its Covid-19 Vaccine. *The New York Times*. Retrieved June 24, 2021, from https://www.nytimes.com/interactive/2021/health/pfizer-coronavirus-vaccine.html?searchResultPosition=1

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431-440. doi:10.1016/j.bushor.2015.03.008

Manogaran, G., Alazab, M., Shakeel, P. M., & Hsu, C. (2021). Blockchain Assisted Secure Data Sharing Model for Internet of Things Based Smart Industries. *IEEE Transactions on Reliability,* 1-11. doi:10.1109/tr.2020.3047833

Manzoor, A., Liyanage, M., Braeke, A., Kanhere, S. S., & Ylianttila, M. (2019). Blockchain based Proxy Re-Encryption Scheme for Secure IoT Data Sharing. *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. doi:10.1109/bloc.2019.8751336

Omar, A. S., & Basir, O. (2020). Capability-Based Non-fungible Tokens Approach for a Decentralized AAA Framework in IoT. *Advances in Information Security Blockchain Cybersecurity, Trust and Privacy,* 7-31. doi:10.1007/978-3-030-38181-3_2

State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time. (2021, March 21). Retrieved from https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

Sultana, T., Almogren, A., Akbar, M., Zuair, M., Ullah, I., & Javaid, N. (2020). Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices. *Applied Sciences, 10*(2), 488. doi:10.3390/app10020488

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks, 6*(2), 147-156. doi:10.1016/j.dcan.2019.01.005

Yuvaraju, M., & Mansingh, P. B. (2021). A Secure Data Sharing Scheme Based on Blockchain for Industrial Internet of Things Using Consensus Algorithm. *Industry 4.0 Interoperability, Analytics, Security, and Case Studies,* 119-132. doi:10.1201/9781003048855-8

Zaddach, J., Bruno, L., Francillon, A., & Balzarotti, D. (2014). Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares. *Proceedings 2014 Network and Distributed System Security Symposium*. doi:10.14722/ndss.2014.23229

Zhang, Z., Cho, M. C., Wang, C., Hsu, C., Chen, C., & Shieh, S. (2014). IoT Security: Ongoing Challenges and Research Opportunities. *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*. doi:10.1109/soca.2014.58

Zhaofeng, M., Lingyun, W., Xiaochang, W., Zhen, W., & Weizhe, Z. (2020). Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data. *IEEE Internet of Things Journal, 7*(5), 4000-4015. doi:10.1109/jiot.2019.2960526

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*. doi:10.1109/bigdatacongress.2017.85