Blockchains and Embedded Systems

Tracking the Flow of Assets on Low-Powered Hardware

Isaac Callison, Graduate Student, Computer Science
Dr. Suk Seo (Faculty Sponsor) Computer Science

ABSTRACT

Blockchain technology is a burgeoning technology with massive potential to disrupt entrenched technological modes in a variety of industries. Current blockchain implementations manifest across desktop and cloud computing. Little research has been invested into low-powered devices, devices often colloquially referred to as IoT or Internet of Things and whether a small private blockchain could be run on such devices to track assets. Several types of low-level and low-powered devices of various architectures were investigated. A Wemos D1 Mini esp8266 microcontroller was chosen for its balance of limitations, varying capabilities, and low-cost. Several of these microcontrollers were run in a peer-to-peer network with an RFID sensor to track asset tags. Experimentation led to varying levels of success and such hardware may be too limited to effectuate a reliable private blockchain.

Introduction

Blockchain technology is in its infancy. Most of the relevant literature seems to recognize the newness of this technology; almost every article reviewed includes at least a brief description of how a basic blockchain works. Some articles devote nearly half of their ink to basic concepts[3]. As a high-level overview, a blockchain is an append-only data structure consisting of hashed blocks of similar types of data. This can be likened to a one-way linked list with all the attendent properties of such a data structure[4]. A general differentiation of a blockchain from a linked list would be the fact that each data block is hashed with relation to the data it contains, and each block references the hashes of the blocks before it and after it. This structure is broadcast to member nodes and replicated many times, creating a copy of transactions[3]. In an attempt to discern all of the potential of blockchain technology, it seems that researchers in the field have been striking out in varied directions. Attempts have been made to use blockchain to track trees from forest to end user[6], using blockchain to reduce the cost of Industrial Internet of Things(IIoT)[10], using blockchain for secure firmware updates[9], and using blockchain to guarantee the integrity of sensor data[7]. There is even a paper proposing the use of smart contracts to regulate the charge of Electric Vechicles at condominiums[12]. It seems that a great many of the papers use exisiting blockchain APIs created by large companies, like Microsoft Azure Blockchain Workbench[6].

Background

All blockchains are either public or private [10] databases replicated across several nodes in a peer-to-peer network[3]. These databases can be thought of as an immutable ledger. Businesses have been investigating various aspects of private blockchains like hyperledger; these have the same characteristics of public ledgers, but with restricted members[15]. Members who transact on the blockchain do so with cryptographic keys. Each data block of cryptographically signed transactions and the hash of the previous block is hashed to create a final hash that the next block will reference [3]. Changing data invalidates the chain[11]. Data is updated across nodes using various forms of ”consensus” algorithms[5]. Consensus algorithms verify the integrity of data blocks[5]. Some of these, like Bitcoin’s ”Proof-of-Work” (POW) algorithm require a great deal of compute power. Others are based on different rules and use fewer resources[5]. The goal is to validate new blocks of data appended to the ledger absent third-party intermediaries[14]. Further, the use of ”smart contracts” allow the execution of payment - absent any central authority - upon the completion of pre-programmed conditions[4][2]. What is not addressed in the literature is the implementation of a private blockchain on a low-level or low-powered device such as an Arduino microcontroller. There are a few articles that reference Raspberry PIs as data collection units or sensors[6][7] however.

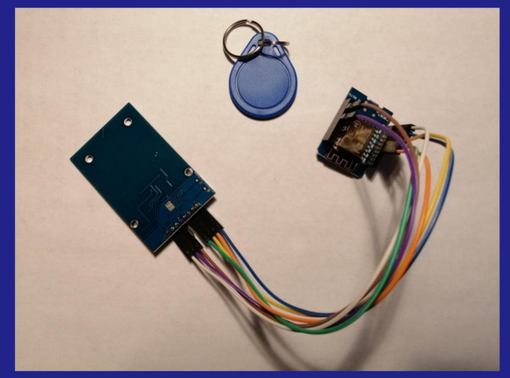
Specific Aims

- Aim 1: To determine feasibility of a blockchain on a limited system such as a microcontroller or ARM based system.

- Aim 2: To create a swarm of several low-level hardware nodes that can track an asset within an organization by creating an immutable ledger of that asset’s movement.

Methods/Results

- Several microcontroller devices (Wemos D1) were obtained and paired with RFID sensors.
- Blockchain code written in C++ and compiled for embeded systems.
- Nodes can connect a peer-to-peer mesh network.
- Scanning fob/card records asset data, records growing blockchain in data structure, and transmits data to other nodes.
- Blockchain also stored to flash memory on microcontroller that survives power cycling.
- Some issues with SRAM and network connectivity.



Pictured above:
RFID sensor on left, Wemos microcontroller on right,
13.56 MHz contactless smart key fob on top.

References

[1] Arora, A. and Arora, M. Digital-information tracking framework using blockchain. Journal of Supply Chain Management Systems, 7(2):1, 2018.

[2] Cong, L. W. and He, Z. Blockchain disruption and smart contracts. The Review of Financial Studies, 32(5):1754–1797, 2019.

[3] Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., and others,. Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10):71, 2016.

[4] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., and Wang, J. Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering, 30(7):1366–1385, 2018.

[5] Elrom, E. The Blockchain Developer: A Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchain-based Projects. Apress, 2019.

[6] Figorilli, S., Antonucci, F., Costa, C., Pallottino, F., Raso, L., Castiglione, M., Pinci, E., Del Vecchio, D., Colle, G., Proto, A. R., and others,. A blockchain implementation prototype for the electronic open source traceability of wood along the whole supply chain. Sensors, 18(9):3133, 2018.

[7] Hang, L. and Kim, D.-H. Design and implementation of an integrated iot blockchain platform for sensing data integrity. Sensors, 19(10):2228, 2019.

[8] Hasan, H. R. and Salah, K. Blockchain-based proof of delivery of physical assets with single and multiple transporters. IEEE Access, 6:46781–46793, 2018.

[9] Lee, B. and Lee, J.-H. Blockchain-based secure firmware update for embedded devices in an internet of things environment. The Journal of Supercomputing, 73(3):1152–1167, 2017.

[10] Leng, J., Yan, D., Liu, Q., Xu, K., Zhao, J. L., Shi, R., Wei, L., Zhang, D., and Chen, X. Manuchain: Combining permissioned blockchain with a holistic optimization model as bi-level intelligence for smart manufacturing. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 50(1):182–192, 2019.

[11] Lin, I.-C. and Liao, T.-C. A survey of blockchain security issues and challenges. IJ Network Security, 19(5):653–659, 2017.

[12] Martins, J. P., Ferreira, J. C., Monteiro, V., Afonso, J. A., and Afonso, J. L. Iot and blockchain paradigms for ev charging system. Energies, 12(15):2987, 2019.

[13] Nakamoto, S. and others,. Bitcoin: A peer-to-peer electronic cash system.(2008), 2008.

[14] Xu, R., Chen, Y., Blasch, E., and Chen, G. Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness. Optical Engineering, 58(4):041609, 2019.

[15] Zheng, W., Zheng, Z., Chen, X., Dai, K., Li, P., and Chen, R. Nutbaas: A blockchain-as-a-service platform. IEEE Access, 7:134422–134433, 2019. 7

[16] Zheng, Z., Xie, S., Dai, H.-N., Chen, X., and Wang, H. Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4):352–375, 2018.

Contact

Isaac G. Callison
ic2d@mtmail.mtsu.edu
https://github.com/cthulhu1988/Projects