**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 attendant 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(IoT)[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 Vehicles at condominiums[12]. It seems that a great many of the papers use existing 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.

**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 effectively utilize a reliable private blockchain.

**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 embedded systems.
- Nodes can connect a peer-to-peer mesh network.
- Node to node track 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.

**References**


**Contact**

Isaac G. Callison
ic2d@mtsu.edu
https://github.com/cithlu1988/Projects

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