Blockchain Based Raspberry Pi Mesh Network

Atharv Chandratre
Student, Dept. of Computer Science
BITS, Pilani - K.K. Birla Goa Campus
Goa, India
f20170009@goa.bits-pilani.ac.in

Yash Chaturvedi
Student, Dept. of Computer Science
BITS, Pilani - K.K. Birla Goa Campus
Goa, India
f20170078@goa.bits-pilani.ac.in

***Abstract*—We want to mainly answer two questions. Firstly, what kind of correlation does increasing distance between IOT nodes on a private blockchain mesh network have with the network latencies involved in block mining and transacting on the network? Secondly, what kind of effect does increasing the number of IOT nodes on the mesh network have on the network latencies in the network? This paper addresses the way blockchain technologies can provide better security and information management on IOT systems, before delving into how the specific problems associated with IOT systems, such as lower computational power and heterogeneity among devices, could be solved. We then run some tests to procure quantitative data which would educate us about the feasibility of our model on larger mesh networks.**

I. Introduction

A. What is Blockchain?

The Blockchain is a protocol that provides a high level of integrity using cryptographic operations in a distributed network to make sure that every node holds the correct data. Blockchain is considered a data structure that forms an append-only database, where the records of this database are shared between all nodes. This protocol forces the validation of the data stored on every node using a consensus mechanism. The most popular consensus mechanism is the Proof of Work (PoW) that requires every node to calculate the hash value of all transactions.

The real innovation which blockchain provides is its ability to perform functions without the requirement of a central authority governing it at all times. This is done by crowdsourcing the governance of the system to change any states in the distributed ledger. In simpler terms, all the transactions performed are confirmed to be valid by all the computers which are a part of the network. For this reason, it is often referred to as the world computer and deemed unhackable, because if a person wanted to hack it, he would have to change a copy of some data item in every single computer on the network. This being such a difficult task computationally, acts as a deterrent for hackers.

Since blockchain technology creates a trackable time-stamped record of all of the changes which have happened to a particular piece of information, it is already finding uses in the field of fin-tech, supply chain management, and marketing. New use cases seem to be emerging every day. Some very interesting use cases have also emerged in the field of diamond mining, where the authenticity of a diamond can be confirmed based on its trackability which the firm that mined the diamond can ensure using a blockchain. Even in gaming, where it is possible to trade purchasable add-ons in games (like skins or modifications to in-game artifacts), these trades can confirm the legitimacy of traded items by recording all of these transactions using the blockchain.

It will be interesting to see further use cases which develop for this technology. As it is relatively new, the first-mover advantage in this field is quite significant. One such emerging use case of blockchain is in the field of Internet of Things Devices.

B. Types of Blockchains:

Blockchain can be developed with different permissions to perform read, write, and validate operations on the records that are shared between nodes. Below are the different types of networks that can be created using the Blockchain protocol:

- **Public Permissionless Blockchains:** any node can join the network, and every node is able to read and insert new transactions. In addition to that, all nodes have to participate in the consensus mechanism. Public Blockchains need to offer an incentive for the nodes that perform the validation. In cryptocurrencies, the network offers an amount of its currency depending on the amount of data that has been validated.

- **Private Blockchains:** recording new transactions is restricted to a centralized organization and the validation of records is done by the predefined nodes while reading permission can be public or private depending on the network design. Usually, no incentive is awarded to nodes that participate in the consensus mechanism.

- **Consortium Blockchain:** sending transactions is restricted to a predefined set of nodes, such that not all nodes have to validate the transactions since only the majority of the network is doing the validation. The right to read processed records can be permissioned or public based on the design. Consortium Blockchains allow the usage of different consensus mechanisms which makes validating the transactions more efficient than public Blockchains and relatively more scalable.

C. Existing Blockchain Platforms:

There exist many Blockchain platforms that enable the creation of decentralized applications. Following are the three most popular platforms -

- **Ethereum:** often defined as the “World Computer” is one of the Blockchain platforms that provide the ability to create Smart Contracts, using Solidity. Ethereum provides the ability to customize different consensus mechanisms other than Proof of Work.

- **Hyperledger:** is a project developed by the Linux Foundation, it provides APIs that facilitate creating private Blockchains. Hyperledger supports the development of Smart Contracts using different programming languages, such as Go and Node.js.

- **Corda R3:** is an open-source project that provides the ability to create financial services on top of a Blockchain. In Corda, records are shared only between parties that are interested in using or validating the transactions to ensure the privacy of data. This makes this platform more scalable than any other Blockchain.

D. Current IOT Implementations:

There are two key problems with current IoT security implementations: inefficiency regarding centralised systems' ability to provide security for large network sizes, and the lack of scalability with size of the network. When these networks need to be updated, there needs to exist a seamless and secure method of transferring the change to all concerned nodes. Moreover, decentralisation is essential to prevent malfunctions in a few devices from affecting communication throughout the network. Lastly, modern IoT networks often involve heterogeneous devices with varying computational power and little standardisation, hence a different approach to security should be taken.

Blockchain solves some of these problems immediately. Decentralisation reduces dependency on managerial systems and increases fault tolerance. The other reason blockchain systems are more reliable is the presence of an immutable ledger that means sensitive data captured by low-power devices is at less risk of loss due to the mechanism of information update across nodes. However, we cannot directly use some blockchain implementations due to problems of latency, resource consumption and bandwidth utilisation. Therefore, one solution to this is to use distributed trust models, involving trust ratings records about other nodes, that eliminate the computational burden of Proof-of-Work consensus mechanisms. These differentiated trust mechanisms also allow for different expectations from lightweight IoT devices, such that not all devices require mining capabilities - a wallet and routing capabilities are enough.

In terms of security features, blockchain-based IoT implementations offer the following:

- **Transaction validation:** In order to prevent malicious updates or attacks, all transactions are validated by a set of delegates that control permissions.

- **Anonymity:** Although blockchain is prima facie a transparency solution, several blockchain implementations, such as Monero, look to conceal user identity. Moreover, transaction mixing services or tumblers can increase anonymity.

- **Soft and Hard Forks:** To account for the vulnerabilities of some blockchain systems to cryptographic attacks (Man in the Middle, quantum key computation), DDoS and double spending attacks, periodic updates can either be brought in through a protocol change (soft fork), or drastic upheavals of existing software (hard forks) to arrest system vulnerability.

E. Mechanism of Information Update in Blockchain Nodes:

Blockchain involves a consensus-based model of information update, without any necessary hierarchy existing between nodes. The shared ledger maintained in common by all nodes is only updated after the new information is verified either by all nodes, or by a majority of nodes, depending on the mechanism employed by each particular blockchain implementation. Every update must be accompanied by a timestamp which determines when it was added to the shared ledger. However, node identity information is not collected during the process of information update.

The types of consensus mechanisms employed are:

- **Proof-of-Work(PoW):** This consensus mechanism compares nodes on the basis of their ability to solve some computationally intensive problem - thus, greater voting rights are accorded to nodes with more computing power. This is also known as mining.

- **Proof-of-Stake(PoS):** An energy-saving alternative to PoW, this mechanism requires nodes to show lower vulnerability and greater importance in order to be accorded more voting rights. Validators lock an amount of cryptocurrency as a deposit. Then one validator is selected randomly to validate the next block, validators with the highest deposit are more likely to be chosen. (Also known as “Casper implementation”). Only the node that is selected is allowed to validate the transaction and if any manipulation happens, the validator loses his deposit and the transaction will be revoked.

- **Delegated Proof-of-Stake(DPoS):** In this consensus mechanism, the ”stakeholder” nodes chosen via PoS select ”delegate” nodes to control permissions for accounting and verification to other nodes.

- **Practical Byzantine Fault Tolerance(PBFT):** is a consensus mechanism used in private Blockchains. In PBFT nodes keeps replying incoming messages as in a gossip network, it begins with one of the validators initiating the communication by proposing a new block into the Blockchain and publishes it to all other nodes, the nodes can accept, edit or deny this block by preparing a message, then send it to all nodes. When 2/3 of the received prepared messages are the same, the agreed action will be taken on this new block.

Some blockchains include nodes that are tasked with verifying new updates, after which all nodes can peruse the update. Acknowledgement transactions are sent by nodes that install these updates - these transactions could be positive or negative to indicate success or failure.

II. Proposed Framework for experimentation

A. Design Choices:

Different choices have to be made with respect to what technologies should be used before implementing the experiment of using the distributed technology with the Blockchain-based Raspberry Pi Mesh Network we are proposing. In order for the feedback values to be shared and validated on a Blockchained network, the following design questions have to be answered:

- **What is the reason for choosing a mesh network?**
  The reason for choosing a mesh topology over other topolgies is that it is more robust and fault tolerant than the only other choices of topology we had, which is the ring and star topology. In the case of the star topology, the node in the middle of the network would inevitably be the single point of failure, which we wanted to avoid. Ring topology has a similar disadvantage, where any one node failing would result in the collapse of the whole network. Also, if a miner and a transacting light node are at diametrically opposite points on the ring network, the latencies involved in transferring information would be unnecessarily high. Hence, the mesh topology was the best one to go with, even though it would be significantly harder to set up in the configuration we wanted (as a hybrid of computer and IOT devices).

- **What will the mesh network design be like?**
  The mesh network will be designed in such a way that there will be one computer and multiple IOT devices. The computer will be the only mining node in the private blockchain and all the other IOT devices will be light nodes. That means they will be able to perform all the transactions and execute smart contracts, but they will not be able to mine blocks and add the new blocks to the blockchain. Only the computer in the network will be able to do that.

- **Why are we going for a computer + IOT Device setup?**
  We are going for this Computer + IOT device hybrid setup over a purely IOT device setup because IOT devices are inherently less powerful than computers. And in our case, we need to have a miner in the system. So to ensure that no particular IOT device gets overwhelmed by having to perform both mining operations and whatever task it may be doing (like temperature sensing), we wanted a dedicated miner in the network.

- **What is the hardware implementation we are using?**
  The hardware implementation we have chosen are as follows:
  - **Desktop Computer:**
    - Quantity: 1
    - OS: Ubuntu 18.04+
    - Processor: Desktop Grade i7, 4th Generation and above. The reason for that is, since the Processor will be the sole miner in the mesh network, it will have to pick up the brunt of the computation.
    - RAM: Minimum 4 GB
  - **IOT Device:**
    - Quantity: Minimum 2
    - Device: Raspberry Pi 3B or above. We need an inbuilt WiFi card in the Raspi, which was available since the 3B model.
    - OS: Raspbian 4.15+
    - Processor: Quad Core 1.2GHz Broadcom BCM2837 64bit CPU
    - RAM: 1 GB

- **What software stack are we planning to use?**
  The software we will be using are:
  - **Docker:** Docker will allow us to use containerization in the Raspberry Pis we use. Since we will be running our code in Docker containers, it will be easy to set-up or bring down or network, and the whole set-up will be relatively lightweight in terms of computational requirements. This is an important consideration as the ARM based processors in the Raspberry Pis do not have a lot of surplus processing power, so using it efficiently is of utmost importance.
  - **Solidity:** Solidity is a object-oriented programming language. It is mainly used to write smart contracts on the Ethereum Blockchain. Solidity enables programmers to write the business logic of their smart contracts in an easy to understand form, which runs efficiently on the Ethereum Virtual Machine. We will be writing a smart contract in this language and deploying it on the nodes of the network to run. This

way we will be able to measure the latencies within the network.

  - **Remix:** Remix is a powerful, open source tool that helps users write Solidity contracts straight from the browser. Remix supports both usage in the browser and locally. Remix also supports testing, debugging and deploying of smart contracts. We will be using it to write any smart contracts we plan to push to the private network we create.
  - **Wireshark:** Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. We will mainly be using it as a packet recording tool to run analysis on the packets sent over the mesh network. This way we will be able to calculate the latencies in the network. We will be using its Command Line Version, tshark, as well.

- **Why are we choosing Ethereum?**
  Among the various blockchain platforms explained above, we have chosen to go with Ethereum for this project as it provides a suitable development environment for our purpose, which is to create a private mesh network. Apart from that, Ethereum has solid support for creating private networks using geth, which allows anyone to run an Ethereum node on almost any device. Finally, Ethereum has been around for around 5 years now, so it has good developer support. We have chosen not to use Hyperledger because it is relatively new and has not been tried and tested to work on ARM based IOT devices yet. And, we are not considering Corda r3 because Corda development team considers any non-financial project "out-of-scope".

- **Which consensus algorithm are we using?**
  Considering our case where we will have a mesh of relatively lower powered Raspberry Pis as the light nodes in the network and one main computer to handle all of the mining of all of the transactions the Raspberry Pis do, we will need to choose a consensus algorithm which will give us control over which blocks are mined but at the same time not overwhelm the mining computer. Hence, we have chosen to go with Proof of Authority as the choice of consensus algorithm. This way, the computer only has to seal the transactions without too much overhead of mining like in Proof of Work. At the same time, the IOT devices, being light nodes, will just initiate transactions on the chain. We have also not gone with Proof of Stake consensus because we do not plan to use ether as a means of transacting value in the mesh network. Therefore, having the ability to sign blocks based on the amount of ether you have will be meaningless as the computer will be the sole miner anyway.

III. Testing Methodology and Implementation:

Our aim is to create a blockchain mesh network using the computer and IOT devices network as stated above, and then formulate a way to test the time latencies within the network. We also document the methodologies used before performing the tests.

A. Hardware and Software Set Up:

First, we will install Wireshark on the main computer and then install tshark on all of the Raspberry Pis. Then we will connect all of them to the same network. After that is done, we will use docker to start the network. Each IOT device will run one docker container. That docker container will essentially make it a light node on the network. The computer on the other hand, will run two docker containers. The first will be to start a miner node on the computer. The second one will run a blockchain explorer, a software which tracks the blocks which have been mined and explore the various transactions which have been conducted within each block. It also records the timestamps with which the transaction was added to the block, which we will use later. We will set the block mining time to a reasonably large amount (5 seconds), which is more than enough to allow that message of a block mined to propagate through a network.

Once that is done, we start the network. After confirming that all of the Raspberry Pis are online and are transmitting data properly, we will start collecting the packets it sends on the network. These packets will then be recorded and sent to us later. This can be done using SSH, for which we will have to enable SSH on the Raspberry Pis. We will also be pre-funding all of the nodes with a large amount of ether. This will prevent any light node from leaving the network because of a lack of funds to execute a transaction.

B. Measurement Methodology

We are aiming to measure the latencies which a transaction initiated by one light node takes to propagate to all nodes on the network.

After connection of the network and letting the block propagation stabilize, we will then use the data we are getting from wireshark to pinpoint which packets are being sent from which IOT device to the miner, and the latency in the network between the execution of a particular transaction and the time it takes for the miner to receive it. We will also measure the time latency between the miner adding a block to the private blockchain and the IOT device receiving the signal that a new block is added.

So to measure it we will vary the following parameters:

- **Distance between nodes:** We will start in a scenario where we have a very small distance between all of the nodes. Then we will repeat the testing procedure multiple times, while increasing this distance and keeping all other parameters constant. Here distance refers to the radial distance of the IOT devices from the miner node. The diagram below explains it.

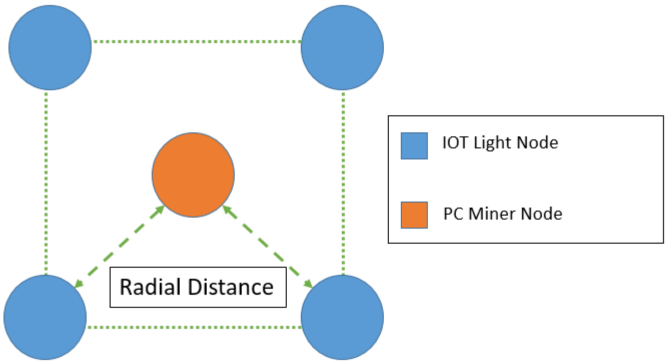

Figure 1. Spacial Setup of Nodes

- **Number of light nodes on the network:** We will start off with One miner PC and one Raspberry Pi. We will then capture the data on that setup, and then progressively keep increasing then number of Raspberry Pis in the network. The diagram below explains it.

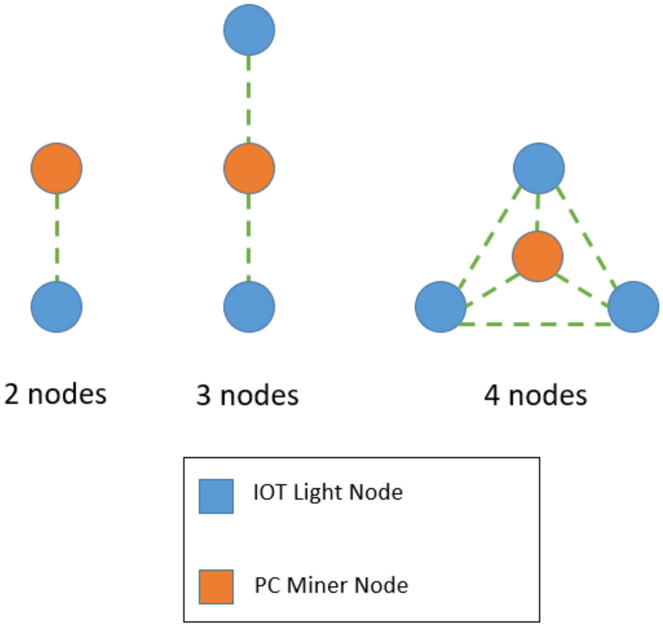

Figure 2. Increasing number of nodes and their setup

We will take the following assumptions into account during this experiment:

- We will assume that they are all connected to a network which has sufficient bandwidth to handle all of the network traffic.
- We will assume that the packet sizes are remaining constant throughout the experiment. This means that the transactions made will all be of the same size. We want to be able to find the impact of varying packet sizes on these latencies in the future though. But for the scope of this project, we will keep them constant. We will be able to ensure that by having the light nodes to no actions at all other than the acknowledgement of new blocks. Or we can push a smart contract onto the private chain and have all of the light nodes execute the same function in that contract independently, with a reasonable time delay between successive function calls.

We will gather data for the time-frame it takes for 10 blocks to be mined in our network. And since we have assumed the block time to be 5 seconds, we will record all the packets coming into and going out of each node. Then we will compare the data for all of the nodes to draw correlations between them. Once we gather our data, we should be able to plot a graph to visualize the relationship between the latency and the distance between the nodes in the mesh. We will also plot a graph between the number of nodes in the network and the latency between the propagation of information within the network.

Our prediction is that there will be a positive linear correlation between the distances between the nodes and the transmission latencies. We also expect a similar positive linear correlation between the number of nodes and the said latency.

IV. Scope for Future Research

-

V. Acknowledgment

The success and final outcome of this project required a lot of guidance and assistance from many people and we are extremely privileged to have got this all along during the progression of my project. All that we have done is only due to their supervision and assistance.

We are extremely grateful to Prof. Neena Goveas, Professor, Department of Computer Science, BITS - Pilani, K.K. Birla Goa Campus, for her guidance as our project mentor. We thank her for providing us amazing support and the hardware resources for this project while taking time out of her busy schedule at regular intervals. Our appreciation also goes to our friends and colleagues who have helped us develop the project, and to all those people who have lent a helping hand with their abilities and skills.

We would also like to take a moment to thank all the organizations and individuals currently working in this field of Blockchain-based Internet of Things Devices. Without their prior breakthroughs, we would not have been able to bring this project to fruition.

References

[1] What is Blockchain Technology?

[2] Permissioned vs Permissionless Blockchains: Understanding the Differences

[3] What Are Private Blockchains and How Are They Different From Public Blockchains?

[4] Consortium Blockchain Explained

[5] Ethereum Whitepaper

[6] About Hyperledger

[7] The Corda Platform

[8] What are smart contracts?

[9] Bitcoin Whitepaper

[10] Solidity Documentation

[11] Remix IDE Documentation

[12] Wireshark User's Guide

[13] Tshark Packet Analyzer

[14] Docker Curriculum

[15] Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT

[16] Internet of Things Architecture: Current Challenges and Future Direction of Research

[17] Towards an Optimized BlockChain for IoT

[18] On blockchain and its integration with IoT. Challenges and opportunities

[19] Blockchain for the Internet of Things: a Systematic Literature Review

[20] Towards Better Availability and Accountability for IoT Updates by means of a Blockchain

[21] Blockchain and the related issues: a review of current research topics