Blockchain for Power Grids

Cadet Velez, Banks, Kim, Neposchlan

(invited paper)

Abstract --- (Challenge (non repudiation of the data being shared) (distributed across the us), what our contribution will be, the motivation)

Our contribution: security (prevent man in middle attack for sharing distributed data) (measure and account for latency) If not timely, it will be useless.

Hyperledger fabric is something that we address first because it is something that will keep us from meeting out time constraint., We don’t want the overhead for blockchain to be the time constraint in our project.

Sharing information is an important part of regulating and maintaining efficient and safe power grids. The main challenge that we face in this project is to develop a more secure method of sharing information across long distances. By implementing technology that creates non-repudiation

This project’s goal is to develop a way of using blockchain technology to share transaction information among different power grids in a secure, controlled, monitored, and efficient manner. Hyperledger Fabric will be implemented in order to create a permissioned network in which power grids will act as nodes that maintain ledger information. By using a distributed ledger as a way to validate transactions though the process of consensus, the system will be able to share information in a manner that is more secure and transparent than traditional information sharing systems. The larger impact of such a system would allow for the further development of automated smart grids that can freely and securely share information. These additional layers of security and speed would help to prevent issues, such as power grid failures, that could stem from the latency involved with traditional methods of validating, processing, and reacting to shared data.

Index Terms - Blockchain, hyperledger fabric.

1. INTRODUCTION

Sharing information across large networks poses many issues and potential risks involving security and usability. For the purpose of sharing information between microgrids, security and confidentiality are paramount. Blockchain architectures provide a variety of solutions to sharing information. Of the many different blockchain solutions currently available, hyperledger provides superior scalability, modularity, and security [1]. For this project, we will implement a hyperledger fabric newtork to facilitate the sharing of information among various microgrids in a way that will potentially be scalable to much larger industry grids.

1. BACKGROUND

a. *Blockchain.* Blockchain is a group of transactions that are linked to their previous modification on a specific channel.[2] The chain is a log that contains the transactions of all previous ‘blocks’ for that particular chain. When a new block is appended unto the chain, the transaction from that previous block is also appended.[2]

A large feature of a blockchain is the use of a distributed ledger.[2] Blockchain ledgers are often decentralized because each person on the network is working with their own replication of the block.[2] Utilizing a decentralized ledger helps add security to the network as all information is not funneling into one node. The ledger contains two characteristics, a world state and a blockchain.[3] A blockchain was explained in the previous paragraph, however, a world state is a database that keeps the values of a ledger state at the current time.[3] This allows anyone or program to pull the current state at any amount of time without having to sweep a log.[3]

b. *Hyperledger fabric.* Hyperledger fabric is a type of blockchain that involves a collaborative approach to community sharing, property rights and the development of standards over time.[5] Just like other blockchain projects, Hyperledger has a ledger and utilizes smart contracts.[5]

1. DESIGN

a. *Powergrid Network.* The endstate for this project is a network with connectivity across six peer nodes including: the United States Military Academy (USMA), the United States Naval Academy (USNA), the United States Air Force Academy (USAFA), Army Research Labs (ARL), Iowa State University (ISU), and Idaho national labs (INL). In essence, all of these nodes will represent microgrids that can communicate with each other and share data in a secure way on the network using Hyperledger. The validating entities inside of the network are USMA, USAFA and ISU. The validating entities will validate transactions, maintain the ledger while ensuring consensus has been achieved on all transactions. Appendix A, Figure 1 is an example of the final network design in which all six peer nodes will reside.

b*. Internal Network.* How we will be retrieving data from the node network is explained in our internal network diagram which is found on Appendix A, Figure 2.

One of the hosts located at USMA will read mySQL data from the USMA MicroGrid, and our OPVN client (Node) will read the data from that PC database. We will obtain that data by running a database query algorithm which is explained in the next paragraph. Then from the OPVN client, data will be sent out the VPN concentrator with a update request to the rest of the nodes on the network, and the nodes will be able to confirm the request to update the ledger. The other nodes will be able to connect to the VPN concentrator in order to send confirmation requests back to our client. Once the request is sent back to our client node validating the update, the ledger state is updated with the appropriate information. Each node on the network will be running a similar instance of OPVN client node as seen on Appendix A, Figure 2.

c. *Database Query Algorithm.*The python script first establishes a connection to the MicroGrid SQL database using proper authentication. After successfully connecting, the script reads from a constraints file provided to us by the Real-Time Smart Grid Capstone team, which contains the IDs of all the PMUs and applicable variables necessary for queries. It then loops through each PMU and queries it for the latest readings that fall within the established minimums and maximums. It writes these queries to a file in readable format, prints each query to console (for verification the script is working) and finally closes all files and connections. We are planning to expand the script to accommodate JSON formatting to more easily create historic data for our network.

d. *Scalability*. Once a successful proof of concept can be run, our framework can be adapted on a larger scale to allow peer nodes to communicate over large distances. The main impact that this would have is an increase in latency. However, as the algorithm improves and is optimized, these effects can be mitigated. Appendix A, Figure 5 shows the 6 microgrids that will be part of the blockchain. As observed on the figure, latency will be an issue as there is a large distance between the microgrids in Idaho, Colorado, and Iowa and the microgrids on the east coast. With larger amounts of latency, the potential for the control system to become unstable rises, which is something that our team took into account for when it comes to scalability.

1. Motivation behind doing the project
2. A 3
3. B 3
4. C 3
5. D 3
6. Example 1
7. A 4
8. B 4
9. C 4
10. D 4
11. Example 2
12. A 5
13. B 5
14. C 5
15. D 5
16. Example 3
17. A 6
18. B 6
19. C 6
20. D 6
21. Example 4
22. A 7
23. B 7
24. C 7
25. D 7
26. Example 5
27. A 8
28. B 8
29. C 8
30. D 8
31. Example 6
32. A 9
33. B 9
34. C 9
35. D 9
36. Conclusion
37. By implementing our design we can create a system that allows microgrids to communicate relevant data across many peer nodes. This can help to solve issues that stem from the current information sharing systems.
38. B 10
39. C 10
40. D 10

Appendix A

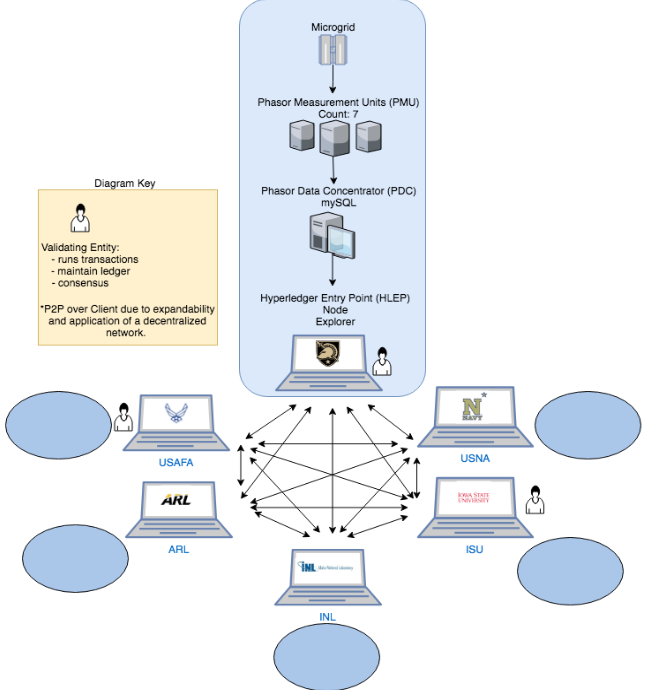


Fig. 1

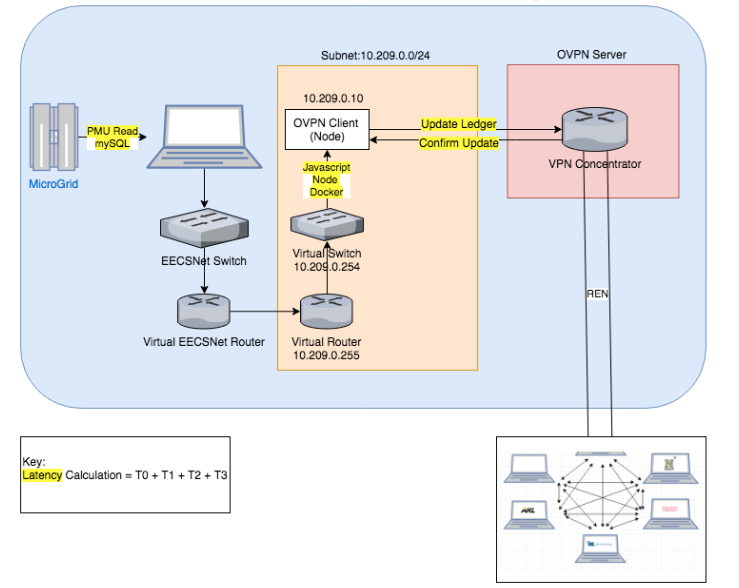


Fig. 2

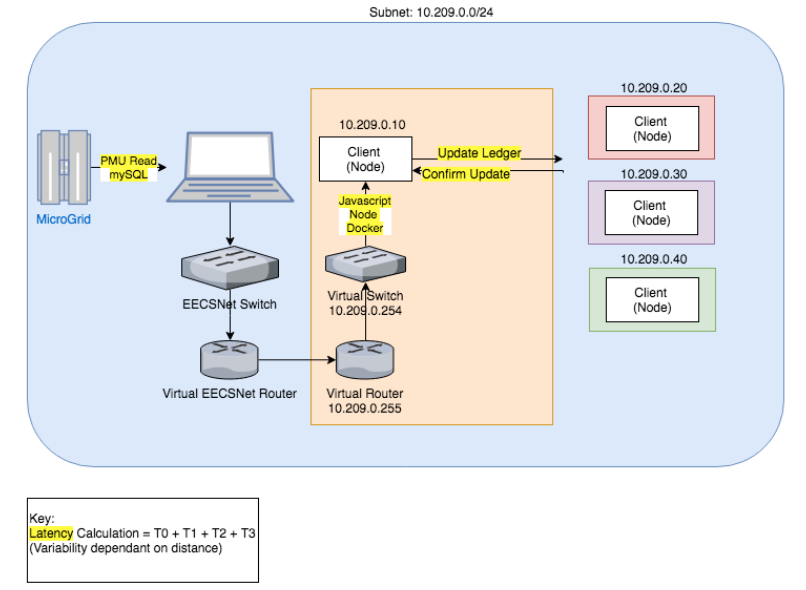


Fig. 3

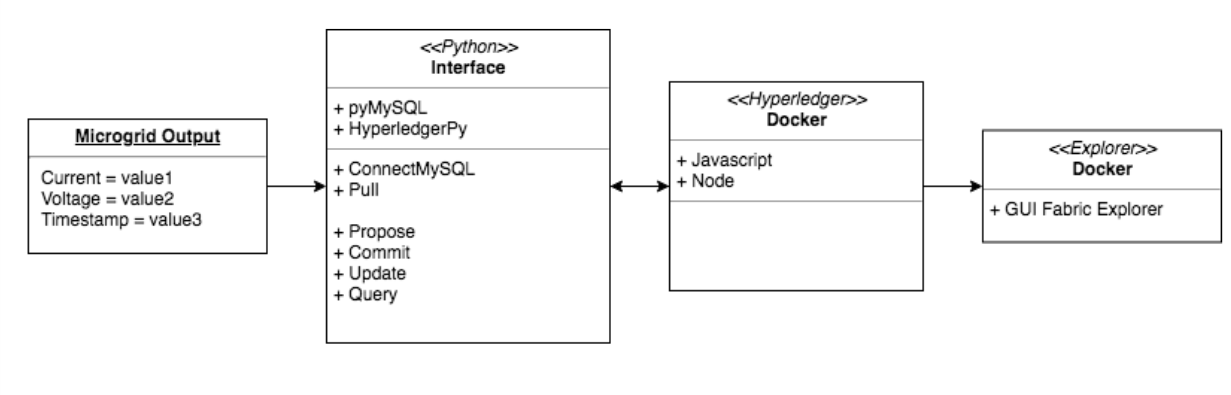


Fig. 4



Fig. 5

Appendix B

Appendix C

Appendix D

Appendix E

Appendix F

Acknowledgment

References

1. <https://www.hyperledger.org/projects/fabric>
2. https://hyperledger-fabric.readthedocs.io/en/release-1.2/glossary.html
3. https://hyperledger-fabric.readthedocs.io/en/release-1.2/ledger/ledger.html
4. <https://trustindigitallife.eu/wp-content/uploads/2016/07/marko_vukolic.pdf>
5. <https://hyperledger-fabric.readthedocs.io/en/release-1.2/blockchain.html>