Gursharan Singh, Rishik Kolli, and Sharmila Nimbkar

Dr. Trowbridge

Grand Challenges for Engineers

5 March 2021

Technology Development Milestones

Overview of Solution:

The US energy grid is unsecured, susceptible to interference, hacking, and interruption from external actors. This problem will only intensify with the internet of things, when all devices and metering systems in homes may be digitally connected to the grid in order to allow for dynamic energy allocation and better energy conservation. It is important now, but also imperative for the technologies of the future, to be able to ensure the safety and cybersecurity of energy networks across America. The proposed solution is the use of blockchain technology to record and verify all activities, data transfers, and records within the electric grid.

Blockchain is a specific type of decentralized database that is different from our traditional databases because data is chained and linked together in Blockchain. Blockchain is usually used in transactions and helps protect a user's information and identity. Blockchain is mainly used for transaction and monetary purposes [1]. There are three highlights or key principles of blockchain: immutability meaning that blockchain prevents outside users from changing or altering information, decentralized systems meaning that the information is not stored in a specific storage area rather the data is copied and spread across a large network of computers, and transparency meaning that users can access all data and history of information [2]. This might be dangerous or a potential pitfall but the information or data is encrypted meaning that an everyday user could not understand the information being presented.

Since blockchain is decentralized, heavily encrypted, and data is recorded in thousands of locations, it is basically unhackable. By storing information and communicating through the blockchain, energy companies will be able to monitor activities across even the largest networks in order to detect suspicious activities, malicious actors, or system malfunctions. A secondary positive impact of blockchain implementation is that when the smart grid is inevitably implemented in the future, it will have a safe and secure mechanism to shuttle data between smart-meters and smart-devices and the power stations/companies that serve them.
Overall, the proposed solution is to sell energy companies (large corporations such as APS and SRP, as well as municipal and federal power stations) a service in which their information is recorded to a specially encrypted piece of the blockchain and monitored and flagged for suspicious activity.

The networks the blockchain will be part of is the preexisting digital infrastructure of devices already in place at energy facilities. Every energy facility has laptops, servers and integrated devices in generators, and sensors that are communicating data back and forth. This communication is the true area which can be infiltrated by threat actors. To prevent this blockchain software will be installed on devices; if the device is not large enough to sustain enough data, the blockchain software will be stored on the next biggest system that is integrated with that device and it has the capability to run the program. What the blockchain is doing is encrypting all the data that is being sent between these devices, data can be anything that is an attempt to alter something. Sensor sending information gathered which is verified and then accepted. This prevents an attacker from getting into a system and excelating through the network and increasing their privileges. Only way to do harm for an attacker is to gain higher privileges but this will prevent this because an attacker can’t enter the system through doors that

it has no permission to enter. All these communications are verified by every device in the system to verify its authenticity. Because blockchain is a decentralized system, every communication is gathered as a ledger by every device, which is then verified by all parties in the system. This program is extremely versatile because it can be extended to ask many devices as wanted, creating a huge network of communication occurring in an encrypted, secure and fast manner.

The network connections include the communications within the power plant, which monitor how much energy is being produced and how it is being distributed, but going forward will increasingly include communications between the energy stations, energy redistribution centers, power consumers such as homes and businesses as smart devices, such as smart meters, are integrated into the power grid.

Functional Requirements and Technical Specifications:

-Record history and data from power plant into the network of computers

- Store around 2920 Tb per hour [3]
- Store all digital transactions into all computers at the facility
- Store data about electric and energy outputs from power plant
- Store data relevant to the different components such as generator, boiler, purification system into the computers
- Store data instantaneously into the network of devices already existing in the energy facility
- Store data from external sources that affect plant operations, such as smart meters and distribution station feedback

- Record data as soon as the machines in the factory can produce reliable information about the logistics of the power plant

-Flag potential threats or suspicious data that is inputted into the systems

- Cross check old data
- Flag data that seems extreme or not relevant to the machine's usual input within a hour
- Record where or why a threat is flagged
- Provide power plant team with updates for why something is flagged in system
- Must flag threats based on data coming from energy ledger

-Remove or block foreign users from entering the interconnected network

- Identify and block users which have already been confirmed as threats
- Maintain a constantly updated database of blocked and flagged users

-Allow any user in power plant to see data produced

- Enable power plant users to access decryption key
- Verify users correctly as employees or administrators of the plant

-Make classified data inaccessible to public

-Must be able to verify threats within a hour in order to protect customers from shutdowns and grid interference

Enabling Technologies for Solution:

Hewlett Packard Enterprise (HPE) sells products that store data into a multi cloud storage and focuses on data protection through highly sophisticated encryption. HPE relies on cloud storage which is an online platform and does not rely on a centralized system for data storage.

HPE's storage solutions are very similar to some concepts of Blockchain relies on such as encryption and a centralized system [6].

Blockchain is gaining implementation wildly around the world, to secure data. Blockchain has been used as a system to create cryptocurrencies. Many nations have started to use blockchain to create safer platforms, to use for national identifications [7]. Nations like Ethiopia have transformed their healthcare system onto a blockchain, by doing so they have created a system that is secure and that can't be tampered with. Saudi Arab transformed government regulators of land ownerships and registry into a blockchain system, making the system hard to be cheated. Land registry blockchain technology has started to become adopted by the Republic of Georgia, Ukraine, Brazil, the Republic of Honduras. DARPA is also creating a blockchain cybersecurity shield, a platform to transmit secure messages and transactions that can be traced. This will be used to facilitate the communications between units and headquarters transmission between intelligence officers and the pentagon. This is effective because every change to the blockchain is being verified and known by all creates an unchangeable history.

The mainstreaming and ubiquitination of blockchain is a prerequisite for enabling widespread data monitoring and security. Currently, it costs $2 to upload 1KB to the blockchain [3]. As blockchain gains popularity, more devices will be added to the blockchain network and storage space will become more greatly available and the cost of blockchain should fall. This solution will require storage capacity on the thousands of terabytes scale: "The requirements for real-time exchange of data is increasing. With a sampling rate of 4 times per hour, 1 million smart meters installed in the smart grid would result in 35.04 billion records, equivalent to 2920 Tb data in quantification" [3]. This number may seem large, but more realistically, a little bit of data will be stored on each device on the network (smart meters, laptops, energy station servers,

energy distribution centers, phones, and other smart devices or IoT enabled technology), so this data requirement is not as overwhelming as it seems.

SHA-256 Hashing Encryption is a technology that is currently in use that is the basis for all encryption on Data on the blockchain is usually encrypted with SHA-256 hashing encryption, which is high in the blockchain and what gives it hackability. It involves 3 different complex mathematical manipulations (hashing, shuffling, rehashing) that are basically impossible to deconstruct without the key [4]. It is very secure and most likely the type of encryption that will be implemented for this solution.

Key Technologies Milestones:

Our solution is an aggregate of existing technologies already in play in the modern world, the only issue that has forecome is to put all together for this purpose. A future milestone that would be further beneficial would be an increase in high level encryption then already in place. This enhanced level of encryption of devices will make the data stored on these devices even more secure than ever before. People willing to buy this software and trust it with national security.

The smart grid, or a system of devices within the energy network that would allow communication and data transmission that allows for dynamic energy allocation, is a system that is currently being looked into for mass implementation. Once it is in place and the US energy infrastructure has transitioned to implementing IoT devices into the grid, our blockchain technology will have enough devices to be a fully integrated network with terabytes of storage capacity. However, it is not really necessary for the initial implementation.

To have a lower cost of blockchain implementation as a service, every device using this encryption will have to allocate certain storage space and computation resources for the blockchain program. This way we will not need a centralized system such as a huge warehouse to store this data that will be gathered but use parts of data through multiple devices through using their allocated resources to compute the computation required to run the program, which ensures security.

List of references;

1. **L Conway, "Blockchain Explained", Investopedia, November 17, 2020. https://www.investopedia.com/terms/b/blockchain.asp**
2. **Omaar, Jamila, "Forever Isn't Free: The Cost of Storage on a Blockchain Database", The Medium. July 19, 2017. https://medium.com/ipdb-blog/forever-isnt-free-the-cost-of-storage-on-a-blockchain-database-59003f63e01**
3. **Y Zhang, T Huang & E.F. Bompard "Big data analytics in smart grids: a review", August 13, 2018. https://energyinformatics.springeropen.com/articles/10.1186/s42162-018-0007-5#:~:text=The%20requirements%20for%20real%2Dtime,et%20al.%2C%202016).**
4. **C Bellet, "Part 5: Hashing with SHA-256", The Medium. Jan 3, 2018. https://medium.com/biffures/part-5-hashing-with-sha-256-4c2afc191c40**
5. **Neo Capacita, "The Logical Components of Blockchain", The Medium, February 18, 2017. https://medium.com/@neocapita/the-logical-components-of-blockchain-870d781a4a3a**
6. **HP Enterprise, "Hewlett Packard Enterprise home", 2020. https://www.hpe.com/us/en/home.html**
7. **A Arnold, "4 Promising Use Cases Of Blockchain In Cybersecurity", Forbes, Jan 30, 2019. https://www.forbes.com/sites/andrewarnold/2019/01/30/4-promising-use-cases-of-blockchain-in-cybersecurity/?sh=3222b8a83ac3**