Blockchain for Nuclear Facilities

Author: John E. Morales García, Polytechnic University of Puerto Rico
Advisor: Jeffrey Duffany, Ph.D., Polytechnic University of Puerto Rico
Advisor: David Mascareñas, Ph.D., Los Alamos National Laboratory
Electrical & Computer Engineering and Computer Science Department (ECE&CS)

Abstract

Nuclear facilities are some of the most highly protected structures in the world. But rapid technological advances, terrorism and the cyberwarfare, has increased the threat of cybernetic attacks on nuclear facilities. Many of these attacks are aimed at altering the operation of the machines within the facility to obtain confidential information about the supply chain. This work focuses on integrating the blockchain technology as a transparent, monitoring mechanism for material movement inside nuclear facilities. With this technology materials movements can be tracked from their point-of-origin, while in transit, and arrival to its final destination. With the use of the Ethereum smart contracts, an example of real-time auditing in material movement was demonstrated. In addition, the principles of vulnerability centric security was utilize to categorize the blockchain as potential security tool for nuclear facilities.

Introduction

The arrival of the blockchain has caused that several companies adopt this technology thanks to its way of maintaining an imputable record of transactions. The department of defense is well inform about this technology and has invest in the monitoring and research of this technology [1]. The use cases for this technology are imaginable, but the nuclear sector has been threaten numerous time through cyberattack and cyber espionage. With the diversity of systems and mission specific hardware the data in diversify and can be hard to keep track of a point of origin if a threat is found. With the blockchain, the heterogeneous data can be fingerprint through the implementation of hash functions. Even though the data is decentralized and anonymize in such system, the cryptographic algorithm is the same for all the data. This allow the utilization of the technology to keep record of the provenance of any valuable asset that flows through the network. Figure 1 shows an overview of the nuclear materials handling to which this work develops a blockchain accountability solution.

Background

In 2009 Satoshi Nakamoto propose a trustless and decentralize technology for achieving transactions without depending on a trusted third party (banks) and solving the problem of the double spend in earlier crypto currencies [2]. After six years later, a new blockchain was develop with a Turing Complete Programing Language, that allow developers to create rules that execute when certain condition were met [3], the era of smart contracts started. In 2016, the reentrancy bug in smart contract was first exploit acquiring the name, “TheDAO bug”, that same year Luu et al. [4] created a symbolic execution tool to identify bugs in smart contracts giving developers a new way to debug smart contracts. A year later Atzei et al. [5] did a survey of the vulnerabilities in smart contracts in Ethereum and created a taxonomical table for help developers identify the vulnerabilities. Three months later Li et al. [6] Conducted a systematic survey on the present risk of smart contract. Recently, Mghna Bal [7] Suggested the blockchain with RFID tags as a way to prevent further proliferation of nuclear material and secure the supply chain of uranium, with highly concern toward countries in developing, due to the vulnerability of the raw material when in transit. Finally the principles of Chamales [8] mention in the Nuclear Threat Initiative, are base in vulnerability centric security and can be used for answering if a technology is suited for a nuclear facility.

Problem

Most people are skeptical to new changes or to quickly accept new technologies. The blockchain is not mature enough to be put on test in various scenarios do to the various vulnerabilities link to crypto wallets and bugs in third party applications. To put aside any doubt, we conduct an experiment to see if the blockchain could be use in the material movement of a nuclear facility. In addition, we utilize the principles of vulnerability centric security mention by Chamales [8] - decrease vulnerability, increase determinism and enhance operations, to see if the blockchain could be consider as a security tool for nuclear facilities and a stepping stone for a solution for nuclear supply chain problem..

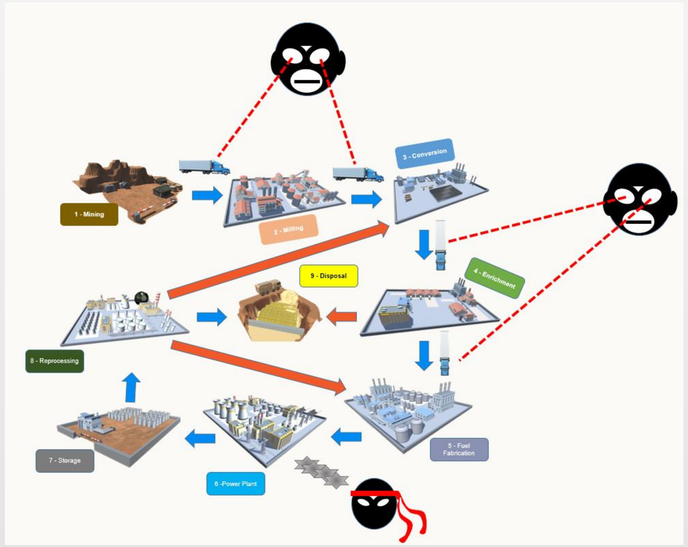

Figure 1
A summary of problems found in the Nuclear Supply Chain according to literature. Cyber Attacks have risen the past year toward power plants and the movement of raw material Is vulnerable to theft, specially in developing countries.

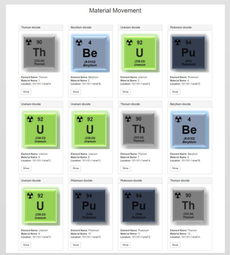

Figure 2
Simulation of a material nuclear facility worker doing a material movement using the blockchain. To the right the web page created with Solidity and JavaScript. Facility Simulation was done in Unity 3D.

Methodology

We analyzing how the blockchain can be incorporated into the material movement system of nuclear facilities with the focus of keeping track of all the transactions that occur when moving the materials. Nuclear facilities operate under strict security protocols. Some of these rules demand adhering to a two-man rule for accepting material. Another important task in these facilities is to provide techniques for monitoring and auditing data, in general. For this work we utilize the Truffle and Ganache testing framework for the Ethereum public blockchain platform. In addition, we utilize the Meta Mask browser plugin to access and interact with the Ethereum decentralized application (Dapps). Our code is based on a boilerplate example provided by the Truffle website. We have extended and modified it, in order to suit ours needs. The web page created shows various materials that can be moved to another area – see figure 2. Our main goal with this simple test is to show how material movement transactions can be recorded in the blockchain and see how they can be customized to fit the needs of an ordinary material movement application. For example, can a transaction be accepted or rejected in compliance with the two-man rule or audits?

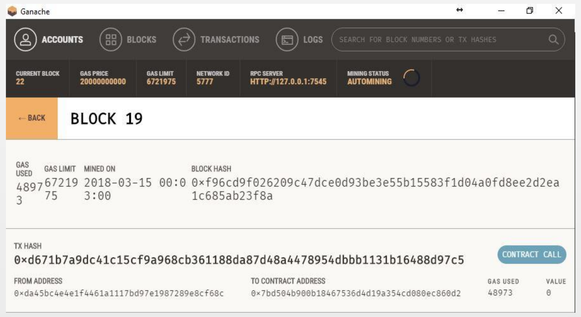

Figure 3
Transaction after pressing he the accept button. No name of any person can be seen in the transaction, just the public keys that represents addresses in Ethereum.

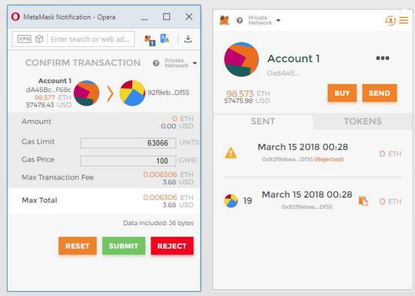

Figure 4
To the left, message asking if the transaction should be submitted. To the right, the transaction in two states: first rejected, wont appear on blockchain and the second, accepted.

Results and Discussion

According to figure 3 and 4, the address of the accounts involved in the transaction appears in a hashed fashion without revealing information about the sender or user. Anyone that has access to the MetaMask or Ganache could only see the hashes of the accounts and not the information or name of the persons involve in the transaction (if any). With the web3.js API, applications similar to MetaMask can be created to manage more robust systems that could feed data contained in the Ethereum platform. An example would be, a system in which a material is moved by one person and then another person accepts or rejects the transaction it in compliance to the two-man rule – see figure 4 and 5. With regards to the gas and ether required for the transactions- see figure 3 block header, there is no way of having an infinite ether system due to complications with Turing complete machine and the halting problem. One approach to addressing this issue is to create another currency or token. From a security perspective, the best way to maintain the integrity of the system is to follow the solidity common development pattern as mentioned before [4][5][6]. In the context of the experiment discussed in this work we can determine that the blockchain is useful for recording and keeping track of items of interest at real time. To contribute with the principles [8], the blockchain can enhance the operations around the facility by providing a quicker way of audition and monitoring without revealing much information to the network about the item in movement inside the facility, by this undesired behavior like stealing or misplace of material can be also decrease. The only troublesome part could be the vulnerability toward the smart contracts, but this can be correct by enforcing good programming patterns in the creation of the contracts and using tools [3] to check for vulnerabilities before deployment. Because once they are deployed they can’t be change, but also in a good manner if they are bug free, they can’t tamper or change, which decrease the vulnerability of the system. With all this we have answer all the question of the Nuclear Facility section and we can also add the blockchain to table 1 and conclude that is one of the technologies

Figure 5
Model of an auditor using the MetaMask web plugin for auditing a transaction as an example of figure 3. Model was created sing Unity 3D.

Conclusions

In this work, we focus on the traceability and security aspect of the blockchain for material management in nuclear facilities. We study the two more famous blockchain (Bitcoin and Ethereum), we determine the security level of the blockchain toward by trying to answer if it comply with the three principles of vulnerability-centric security suggested for technologies that safeguard nuclear facilities. We created a website that simulate a nuclear material movement system to see if the blockchain could keep track of the items in movement and see if the two-man rule of auditing could be implemented. Finally, we mention how the blockchain enhance operations, decrease vulnerabilities and increase deterministic behavior by completing the experiment.

Future Work

Based on the result obtain, we can now move to test the suggestion made by Bal on implementing RFID and other tracking sensors. This way we could incorporate the Ethereum blockchain into an embedded device with a RFID or NFC technologies to gather data and add data as a nuclear facilities inventory monitoring along the supply chain. Another interesting topic to study is how the different consensus algorithm work with more participant in the blockchain and how this impact the monitoring of material if one of the participant consider cheat the system. 8

Acknowledgements

This material is based upon work supported by, or in part by the National Science Foundation Scholarship for Service (NSF-SFS) award under contract/ award # 1563978.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”.
[2] J. I. Wong and J. I. Wong, “Even the US military is looking at blockchain technology—to secure nuclear weapons,” *Quartz*. .
[3] V. Buterin, “A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM,” p. 36.
[4] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making Smart Contracts Smarter,” 633, 2016.
[5] N. Atzei, M. Bartoletti, and T. Cimoli, “A survey of attacks on Ethereum smart contracts,” 1007, 2016.
[6] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A Survey on the Security of Blockchain Systems,” *arXiv:1802.06993 [cs]*, Feb. 2018.
[7] M. BAL, “Preventing Proliferation: Tracking Uranium on the Blockchain,” no. 235, p. 16, 2018.
[8] G. Chamales, “A New Approach to Nuclear Computer Security,” p. 12