Blockchain for Nuclear facilities

J. E. MORALES1, J. DUFFANY2, D. L. MASCAREÑAS3
1 Polytechnic University of Puerto Rico, morales_3400@students.pupr.edu.com
2Turabo University of Puerto Rico, jeff.duffany@gmail.com,
3Los Alamos National Laboratory, dmascarenas@lanl.gov

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 article 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 pointof-origin, while in transit, and arrival to its final destination. In addition, with the use of smart contracts, automated rules can be triggered when certain conditions are met, such as notifying when a material is running out or has been dispatched. Finally, this work seeks to answer questions such: is the blockchain secure for mission-critical systems like nuclear facilities.

Introduction

A Blockchain is a combination of mature technologies (e.g. Merkle trees, timestamps, hashes) that were integrated by a person or group known as Satoshi Nakamoto (Satoshi, 2008). With the recent boom of blockchains, numerous platforms that implement the blockchain have surfaced. One of the most notable among them is Ethereum. This platform is easy to implement and is considered as a blank canvas for building blockchain applications (Web 3). Other sectors have also benefited from the blockchain. Companies such IBM and Hejia have united to provide blockchain capabilities for pharmaceutical supply chains (Stanley, 2017). BHP Billton has created an application to trace geological samples from around the world (Rizzo, 2016). Another sector that seems to be getting interested in blockchains is the UK Nuclear sector with the company Guardtime. They are implementing a Keyless Signature Infrastructure (KSI) technology to secure the Nuclear Power Plants (Guardtime n.d.). This paper is focused on the nuclear sector. In this paper the Ethereum public blockchain will be implemented to create a basic web page for simulating the transit of material inside a nuclear facility.

Methodology

We are analysing 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.

Preparation and pre-processing

For the purpose of 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). As a base for our test, we have extended and modified one of the tutorials available for the Ethereum platform (Truffle Suite n.d.). The web page created shows various materials that can be moved to another area. 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?

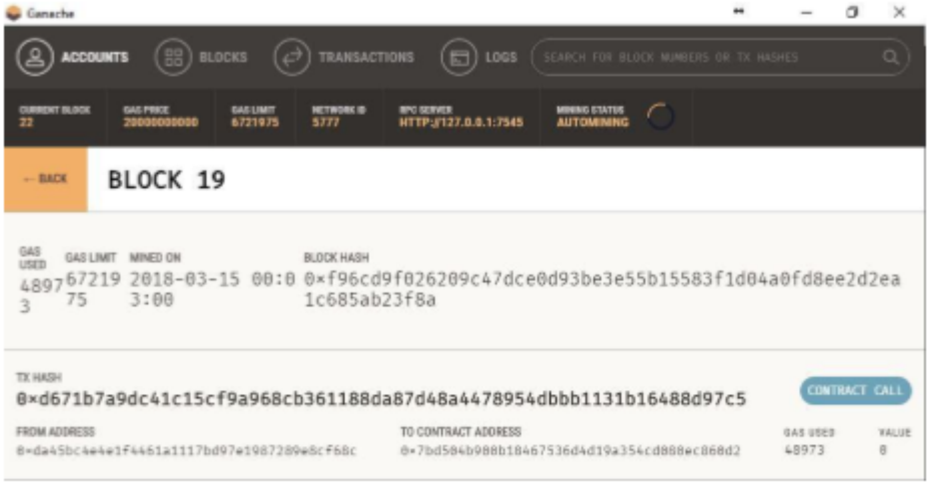
Experimental results

The Ethereum Blockchain

The blocks in any blockchain contain one or more transactions that are hashed together in pairs until only one hash is left. This last hash is known as the root hash and the data structure utilized for hashing data in such way is known as the Merkle tree. However, in Ethereum it is known as a Merkle Patricia tree, because it also stores the state of the accounts. The root hash is then added into the block and then the block is simultaneously hashed into the chain (Wood, 2018). Each block also contains other parameters, these include a gas limit, a gas price, the gas used, and the block number see Fig.1. The gas limit is the total gas that a block contains to allow the execution of contracts and transactions inside that block. The gas price is the amount of gas that each operation costs when the block is executed. The gas used is the total gas consumed in the transaction. Since an Ethereum block contains internal machine states, the whole blockchain can be seen as a virtual machine or Ethereum Virtual Machine (EVM). This behaviour allows the execution of computer code also known as smart contracts inside Ethereum. In the EVM framework, gas acts as the fuel that EVM needs to be able to carry out transactions. From a cryptocurrency perspective cryptocurrency, gas is the fee that a sender must pay in ether in order to send a transaction. Without gas, an EVM cannot execute any transaction, causing it to fail.

Material Movement

Truffle was used to compile and execute solidity code, a JavaScript base programming language that its used for writing code in Ethereum. The test blockchain was generated by Ganache. A material management web page was also generated. The communication between MetaMask and Ethereum is made possible by the web3.js libraries that allow interfacing through an IPC and HTTP connection (web3.js n.d.). For simplicity's sake we consider four materials (uranium, plutonium, beryllium and thorium.) that are commonly utilize in different nuclear facilities see Fig.2. Each material is associated with labels that represent the state, the element name, the material name – a number that represents that item and the location that ends with the shelf where the material is located within the room. When the Move button see Fig.2, is pressed the MetaMask plugin prompt a window Fig.3a that asks the user to submit or reject the transaction. Once the transaction is accepted or rejected, it gets recorded into the MetaMask history see Fig.3b.



CURRENT BLOCK 22
GAS PRICE 20000000000
GAS LIMIT 6721975
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING

BLOCK 19

GAS USED 48973
GAS LIMIT 6721975
MINED ON 2018-03-15 00:03:00
BLOCK HASH 0×f96cd9f026209c47dce0d93be3e55b15583f1d04a0fd8ee2d2ea1c685ab23f8a

TX HASH 0×d671b7a9dc41c15cf9a968cb361188da87d48a4478954dbbb1131b16488d97c5
FROM ADDRESS 0×da45bc4e4e1f4461a1117bd97e1987289e8cf68c
TO CONTRACT ADDRESS 0×7bd584b988b18467536d4d19a354cd888ec868d2
GAS USED 48973
VALUE 0

Fig. 1 Accepted Transaction in Block 19

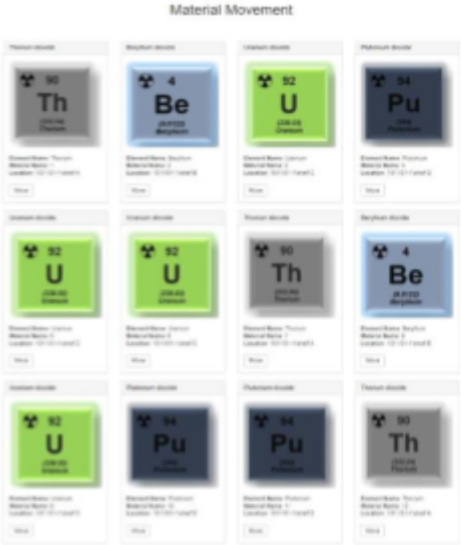
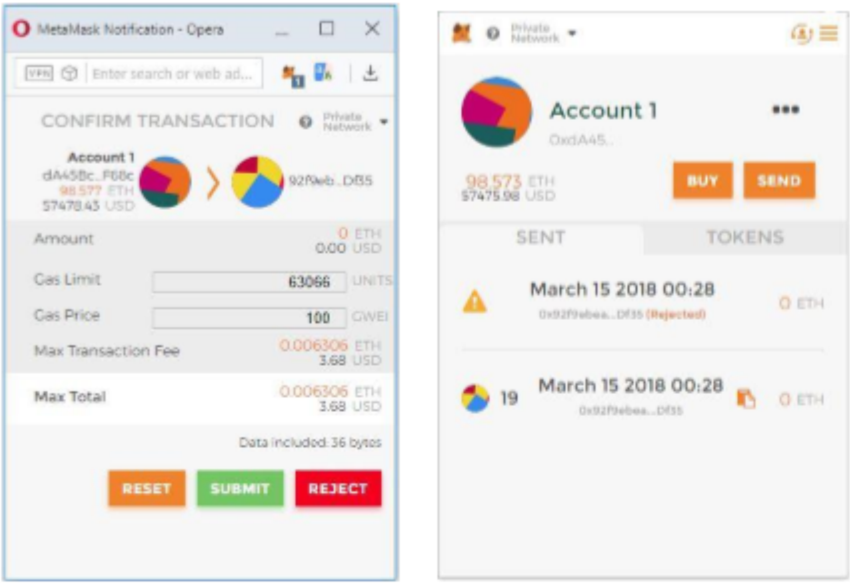


Fig. 2 Material Movement Web Page



MetaMask Notification - Opera

CONFIRM TRANSACTION Private Network

Account 1
dA45Bc...F68c
98.577 ETH
$7478.43 USD
92f9eb...Df35

Amount 0 ETH 0.00 USD
Gas Limit 63066 UNITS
Gas Price 100 GWEI
Max Transaction Fee 0.006306 ETH 3.68 USD
Max Total 0.006306 ETH 3.68 USD
Data included: 36 bytes

Account 1
0xdA45...
98.573 ETH
$7475.98 USD

March 15 2018 00:28 0x92f9ebea...Df35 (Rejected) 0 ETH
19 March 15 2018 00:28 0x92f9ebea...Df35 0 ETH

(a) Submit or Reject material in transit.

(b) Transaction History – (upper) Rejected, (lower) Accepted

Fig. 3 MetaMask browser plugin connected to Ethereum

Discussion

According to Fig.3, 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. With regards to the gas and ether required for the transactions, there is no way of having an infinite ether system due to complications that can lock the nodes permanently (HTRGSFE n.d.). One approach to addressing this issue is to create another currency or token (Triantafyllidis, 2015). From a security perspective, the best way to maintain the integrity of the system is to follow the solidity common development pattern (Solidity doc n.d.). In the context of the experiment discussed in this work we currently can't determine if the blockchain is sufficiently secure for managing nuclear material, but it demonstrates its usefulness useful for recording and keeping track of items of interest. Perhaps with the incorporation of additional technologies, one could achieve results such as those obtained by Guardtime in the development of the KSI, for industrial blockchains. This technology provides security for UK nuclear power plants, flood defense systems and electricity distribution grids. The technology enables data signing across a system and independent verification of time, location and authenticity at any moment in history (Guardtime n.d., Holmes, 2017, Superadmin n.d.)

Acknowledgement

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. Los Alamos National Laboratory is operated by Los Alamos National Security LLC, for the National Nuclear Security Administration of the U.S. Department of Energy, under DOE Contract DE-AC52-06NA25396.

References

Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.

Web 3: A platform for decentralized apps — Ethereum Homestead 0.1 documentation. Retrieved from http://ethdocs.org/en/latest/introduction/web3.html

Stanley, A. (2017, April 11). IBM Ramps Up China Blockchain Work With Supply Chain Trial. Retrieved from https://www.coindesk.com/ibm-amps-china-blockchain-new-supply-chain/

Rizzo, P. (2016, September 23). World's Largest Mining Company to Use Blockchain for Supply Chain. Retrieved from https://www.coindesk.com/bhp-billiton-blockchain-mining-company-supplychain/

KSI Technology | Industrial Scale Blockchain | Guardtime. (n.d.). Retrieved from https://guardtime.com/technology

Ethereum Pet Shop -- Your First Dapp | Truffle Suite. (n.d.). Retrieved from http://truffleframework.com/tutorials/pet-shop

Wood, G. (2018) Ethereum: A secure decentralized generalized transaction ledger Byzantium version. Ethereum Project Yellow Paper. Retrieved from https://ethereum.github.io/yellowpaper/paper.pdf

web3.js - Ethereum JavaScript API — web3.js 1.0.0 documentation. (n.d.). Retrieved from https://web3js.readthedocs.io/en/1.0/

How to remove gas system from ethereum. (n.d.). Retrieved from https://ethereum.stackexchange.com/questions/1953/how-to-remove-gas-system-from-ethereum

Triantafyllidis N, P. (2015) Developing an Ethereum Blockchain Application. Master Research Project, University of Amsterdam, Amsterdam, The Netherlands. Retrieved from http://www.delaat.net/rp/2015-2016/p53/report.pdf

Common Patterns — Solidity 0.4.22 documentation. (n.d.). Retrieved from https://solidity.readthedocs.io/en/latest/common-patterns.html

Holmes, J. (2017, December 1). Blockchain Key to Cybersecurity Protection. Retrieved from https://btcmanager.com/blockchain-for-cyber-security-protecting-infrastructure-datatelecommunications/

Superadmin. (n.d.). Guardtime: Blockchain to guard nuclear power plants. Retrieved from http://www.coinfox.info/news/4316-guardtime-using-blockchain-to-guard-industries