Blockchain for Nuclear Facilities

John E. Morales García
Master in Computer Science
Advisor: Dr. Jeffrey Duffany
Department of Engineering and Electrical Engineering
David Mascareñas
Los Alamos National Laboratory
Polytechnic University of Puerto Rico

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 point-of-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.*

Key Terms *— Blockchain, Ethereum, Nuclear Facilities, Supply chain.*

INTRODUCTION

A Blockchain is a combination of pre-existing technologies (e.g. Merkle trees, timestamps, hashes) that were integrated by a person or group known as Satoshi Nakamoto [1]. 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 [2, p. 3].

Companies have united to provide blockchain capabilities to benefit certain sectors such like pharmaceuticals [3] and mining industry [4]. 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 [5]. The last-mentioned sector is just a scale of a big fish. The nuclear sector is composed of other facilities that process elements extracted from the ground for the development of fuel to supply energy to reactors, for research and the production of electricity. Any attempt to break any of the process of the nuclear fuel cycle could lead to trouble to the stakeholders of this sectors. The blockchain has been useful for maintaining a trustless and transparent ledger of records among the mentioned sectors.

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 to verify the traceability and security of this technology.

RELATED WORK

Although blockchain technology is recently receiving a lot of attention, the idea for the use of this technology for supply tracking is not new. For example, Kim and Lakowski [6], propose the use of traceability ontologies to design intelligent contracts that execute a trace of origin. Francisco and Swanson use Unified Theory of Acceptance and Use of Technology to explain the acceptance of this technology in supply chains. Many are interested in knowing how reliable the use of blockchain is [7]. Kristoffer Just shows with his work that many people trust on control mechanisms and certificates, it also shows a conceptual model of how this trusted platform is applied to the management and use of the supply chain [8].

On the other hand, there has been interest in using Radio-Frequency Identification (RFID) technology to track supplies, as discussed by Chircu et al. He mentions that this technology can improve supply management and validate the quality of drugs [9]. Similarly, Bendavid et al, proposes the use of RFID to monitor important supplies to hospitals [10]. The possibility of implementing the RFID system along with the blockchain in the supply chains [11] as a mechanism for monitoring and transparency of the products has also been explored.

The companies of supply and goods have not been the only ones that have shown their interest in this technology. DARPA for its acronym in English have also invested millions of dollars to test this technology, to ensure sensitive data and maintain the integrity of data in critical systems. With the blockchain, entities such as DARPA can take adversaries to a specific plane within all the heterogeneity of data produced by supply chains [12], in order to use advanced audit and investigation techniques. Meghna Bal, explains how a blockchain based in the consortium algorithm can help in the monitoring of radioactive materials with the use of Near Field Communication (NFC) and RFID since the material is removed from the mines until it reaches its destination [13].

NUCLEAR FACILITIES

There are 447 operable Nuclear Power Plants (NPP) around the world and 61 under construction – by the time this work was done – with United State, France, Japan, China and Russia being the mayor owner of this reactors[14], but not all facilities that exist can be categorize as NPP. Including the nuclear power plants, the facilities that interact with nuclear material - in any of its states – can be cataloged as [15]:

- **Nuclear Power Plants** – The main purpose of this facilities is the generation of cleaner energy (supply electricity for home and industries).
- **Nuclear Material Facility** – In this category can be found enrichment facilities (e.g. Fuel fabrication, Enrichment, Conversion), deconversion facilities (e.g. storage yards, waste disposal) and recovery facilities (e.g. material extraction).
- **Nonpower Production and Utilization Facility –** This category can be subdivided into research and test reactors (e.g. University research), and Medical Radioisotope Irradiation and Processing Facilities (e.g. Medical research).

All the above-mentioned facilities are part of the nuclear fuel cycle or nuclear material supply chain; therefore, the term nuclear facility is used in this work to refer to these facilities. The inaccessibility to any of the nuclear facilities services can be critical to countries that are more dependent on this source of energy. This could cause mission critical failures or blackouts in a bigger scale. For example, in the fuel cycle, if the enrichment is affected, then the nuclear reactors that supply energy to cities and industries will also be affected, just as if at some point the material transportation is affected, the entire cycle also is affected.

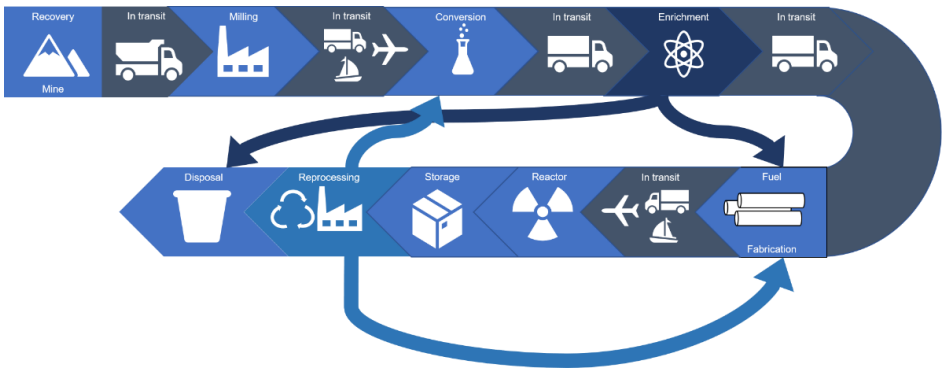

Figure 1
Nuclear Fuel Cycle

In 2017, the top five countries that rely more on nuclear energy were: France with 78% dependence, Slovakia with a 58.9% dependence, Hungary with a 53.4% dependence, Belgium with 47.2% dependence and Ukraine with 43.0% of dependence [16]. More than half these countries energy come from nuclear energy. The importance of these facilities makes them targets for cybernetic attacks orchestrated by groups of hackers with economic reasons, political views, ideals (state a point), espionage and nation-state support. In Ukraine on 2016, for example a group of hackers manage to deploy a malware that contained a timed attack that collapse the energy service by disrupting a substation from the power grid on the city of Kiev [17] - [18]. The reproduction of such an attack on a NPP could be catastrophic for the countries that depend the most on nuclear energy. The Ukraine incident is not the only attack done to a mission critical system of this importance. In Iran [19], for instance, a Uranium enrichment plant got infected - through a USB drive - with a malware worm, that replicate itself through the systems until reaching any device that contains a centrifuge and then make them spin fast enough to degrade the life span of the machinery and in worst case break it. Recently, in 2017, there was a rumor that NPPs were target for cyberattacks [20].

To deal with these problems, Chamales propose the use of technologies base on vulnerability centric security principles, as can be seen in Table 1. These technologies allow the improvement of operations, decrease existing vulnerabilities and those to come, and demonstrates constant behavior [21].

But the problems that nuclear facilities face go far beyond the facility itself. According to a report IAEA Illicit Trafficking Database, from 1993 to 2006 a total of 275 incidents were reported for unauthorized possession and other criminal activities [22]. The 2014 report showed that 55% of the material loss occurred while the material was in transit [23]. Due to the proliferation of radioactive material, errors in packaging, smuggling and uranium black market, and extremist terrorist groups, the supply chain is also affected. In studies related to this topic, Maghna Bal proposed the use of the blockchain as a mechanism to monitor the flow of uranium through the entire supply chain. With a similar approach, this work is mainly focused on nuclear material handling in nuclear facilities. As objective this work:

- Use the vulnerability centric security principles to verify if the blockchain can be suggest as a tool for enhancing security in nuclear facilities.
- Check if the blockchain can be used for monitoring material movement in nuclear facilities and audit or authorize this movements.

BLOCKCHAIN 1.0 AND 2.0

A formal definition of what the blockchain has been given by Seebacher & Schüritz [24], “A

Table 1
Available Vulnerability-Check Security Technologies

Technology	Decrease Vulnerabilities by	Enforce Determinism by	Enhance Operations by
Hardware Virtualization	Removing legacy vulnerabilities in firmware and hardware.	Eliminating unexpected hardware behavior.	Monitoring lowering cost, maintainability, testability, easy deployment.
Application sandboxing	Isolation and containerization.	Preventing unexpected crashes.	Configuration of access level, restrictions mechanism, easy auditing, enforcing policies.
Software Scanning	Feed back and notifications that allow user to act.	Feedbacks to act on unexpected behaviors.	Action base mechanism, alerting, monitoring.
Security Instrumentation	Detecting and patching vulnerabilities	Preventing crashes and unexpected behavior.	Providing less interaction with system. System monitoring.
Deterministic Hardware	Remove unnecessary components.	Performing a specific task.	Removing legacy systems and unnecessary components. Lowering cost.
Cryptography	Tested mathematical proof.	Mathematical proofs.	Providing authentication mechanism base on roles.
Blockchain	?	?	?

blockchain is a distributed database, which is shared among and agreed upon a peer-to-peer network. It consists of a linked sequence of blocks, holding timestamped transactions that are secured by public-key cryptography and verified by the network community. Once an element is appended to the blockchain, it cannot be altered, turning a blockchain into an immutable record of past activity."

The original idea behind the systems was to have a way to make financial transaction without the intervention of a third party and to solve the problem of double spending in peer-to-peer (P2P) networks that past cryptocurrency could not solve. With the release of the Ethereum platform or blockchain 2.0 [25] the blockchain paradigm changed. Ethereum integrated a Turing Complete Programming Language that allows developers to create scripts – known as smart contracts – that are executed when certain conditions are met in the network. This new characteristic extends the blockchain beyond crypto currency system and promote the creation of systems based on: Reputation, Tokens and Decentralize Organizations among other applications known as Dapps.

Accounts

Participants in the blockchain are known as nodes. Exchange of assets is possible in the blockchain by asymmetric key cryptography. Each node participating in the network need to possess an address. The address is created by asymmetric cryptography in where key pairs (private/public keys) are created. The algorithm behind the creation of the keys is based on Elliptic Cyclic Curve and the implementation to handle the signature of the accounts is known as Elliptic Curve Digital Signature Algorithm (ECDSA) [26] - [27].

The generated public key represents the participant's address; therefore, this address is broadcast as a message to the rest of the network without revealing the name of the owner. On the contrary, the private key must be secured, otherwise someone could steal asset from the expose account. The address creation process does not stop with the creation of the public key, there are other steps that are required to create an address.

- The public key is pass through a one-way function – cryptographic algorithm – known as SHA-256
- Then the result is pass through a RIPEMD-160 hash, transforming the address from 32 bits into 20 bits.
- The resulting string gets the 00-prefix added to it and 4-byte checksum (obtained by applying double SHA-256 to this second step) added as a suffix.
- Finally, the result gets encoded into Base58.

The above accounts creation explanation can be attributed to the way that bitcoin and other cryptocurrency (some use other prefixes and checksum) manage they're account addresses [28] [29].

For Ethereum the standards are different. There are two types of accounts: external accounts – controlled by private keys and contract accounts – bytecode executed by the Ethereum Virtual Machine (EVM). For external accounts [29], [30], [31]:

- A private/public key are also generated with the ECDSA algorithm.
- Then the public key is hash with Keccak-256 algorithm – an early version of SHA 3 standard.
- Finally, the address is created by taking the rightmost 20 bytes out of the hash and appending 0x-prefix to the result.

Other characteristics that make differ accounts in Ethereum from bitcoin is the integration fields that allow them to store data and states. Table 2 shows the four types of fields available in each of the accounts.

Table 2
Ethereum Account Fields

Fields	External	Contract
Nonce	# of transactions sent	# of transactions sent
Balance	Amount of ether	current ether
Storage root	Null	Storage pointer
Code hash	Null	Code pointer

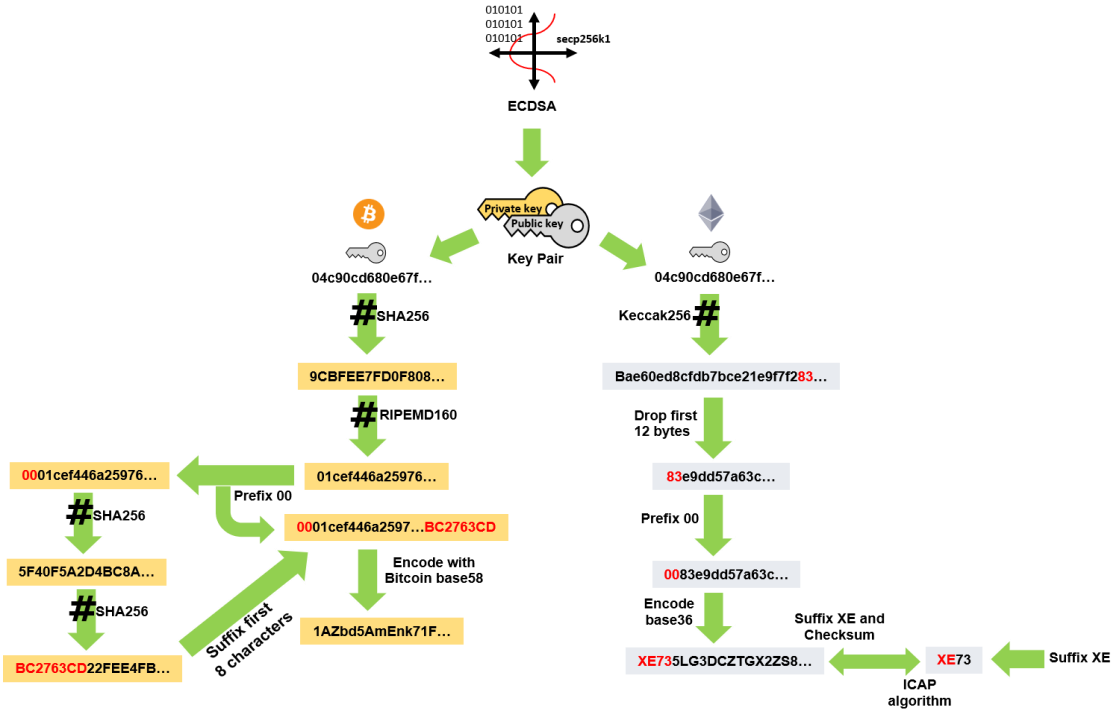

Figure 1

Account Creation Process in Bitcoin and Ethereum

Transactions

Now that the account concept has been define, we can talk about transactions. The concept of a transaction in the blockchain 1.0 can be compare to the transfer of a coin from one owner to the other. In for example, owner B hash his address along with the previous transaction between himself and owner A, and then sign it with his private key and pass it to the new owner C. In reality, no one is storing any currency, instead the system keep track of who has a certain amount of un-spent currency. In Ethereum, instead of just transferring values, the transactions also transfer data. The data is pass by a message that can be created by a contract or by another an external account. Another aspect of the transactions in Ethereum is the number of additional fields: recipient message, sender signature, amount of ether, the data to be sent, gas limit (also known as start gas) and gas price. In both platform there are three types of nodes, light nodes, full nodes and miners. Light nodes only download the header of the transaction to validate them instead of the whole. Mostly light nodes are small device (tablet, cellphones, among others) and depend on full nodes to connect to the blockchain network [32]. Whilst full nodes download the entire blockchain to provide verification and validations in the entire blockchain, this way blockchain rules can be enforce and suspicious transactions can be eliminated out of the chain [33]. Miners role is to add transactions into a block, to then be validated by the rest of the network and accepted in the chain. They don't need to download the entire blockchain, just only the part that are necessary to perform their work, mining. Another characteristic of the miners is that, they get rewarded when their block gets accepted by the rest of the network.

Gas

In Ethereum, to ensure that a miner get rewarded when a transaction is added into a block, the network contains a special fee unit known as gas. Each operation inside the EVM has a predetermined cost in this unit and can't be change by any user. Wood et al. has provided a table of EVM operations with their respective gas cost [34]. Complex operations require more gas, thus is important that the provided

gas limit is enough to run the entire transaction in the EVM. The fee pay to the miner can be calculated by: (gas limit – Sum of Operations cost) x gas price. Where the gas price is in Gwei units (1 ETH x 10-9). If no enough gas was provided for the transaction, an out of gas exception will occur and the transaction will rollback, but the fee will still go to the miner as a payment for his work and finally the transaction is added to the blockchain as a failed transaction. There certain scenarios in where ether is refunded at the end of transactions, but only if the Out of gas exception is avoid. In each scenario at most half the gas is refund and the miner still gets the fee. The first scenario is when the provider assigns more funds than needed in the gas limit. In this case the excess gets refunded. The other two scenarios are similar and occur when a contract is self-destruct and when the storage is clear (set to zero). When a contract gets self-destruct a refund counter is set to 24,000 and for clearing the storage the counter is set to 15,000. There is also a minimum gas limit of 21,000, taking this in account and the fact that excess gas limit is refunded, one can think that setting a high gas limit is a precaution. Well yes and no. Higher gas limit will only discourage the miners from mining the transaction, since they get pay by the amount of gas consume in the transaction. The ideal gas limit is one that is reasonable enough for the miners make some profit, this could help the transaction be the next in line – if the amount is reasonable or just be forgotten – if the amount is high.

Another reason why Ethereum utilize gas is to afront the halting problem of Turing Complete Machines, which *"states that no algorithm can exists which determines whether or not a given algorithm will terminate given some input."* [35] Gas act as the halting condition to stop an infinite loop and since there's no unlimited amount of gas in the network, then the EVM can stop depending on the amount of gas or ether specify in the transaction and the complexity behind it.

Table 3

Blockchain 1.0 and 2.0 Risks according to Li et al

Blockchain version	Risk	Cause
1.0,2.0	51% vulnerability	Consensus mechanism
	Private key security	Public-key encryption scheme
	Criminal activity	Cryptocurrency application
	Double spending	Transaction varication mechanism
	Transaction privacy leakage	Transaction design flaw
2.0	Criminal smart contracts	Smart contract application
	Vulnerabilities in smart contract	Program design flaw
	Under-optimized smart contract	Program writing flaw
	Under-priced operations	EVM design flaw

Table 4

Smart Contracts Vulnerabilities that Oyente can Detect

Oyente Detectable	Vulnerability	Cause	Level
	Call to the unknown	The called function does not exist	Contract Programming Language
	Out-of-gas send	Fallback of the callee is executed	
O	Exception disorder	Irregularity in exception handling	
	Type casts	Type-check error in contract execution	
O	Reentrancy vulnerability	Function is re-entered before termination	
	Field disclosure	Private value is published by the miner	EVM
	Immutable bug	Alter a contract after deployment	
	Ether lost	Send Ether to an orphan address	
	Stack overflow	The number of values in stack exceeds 1024	
	Unpredictable state	State of the contract is changed before invoking	
O	Randomness bug	Seed is biased by malicious miner	Blockchain
	Timestamp dependence	Timestamp of block is changed by malicious miner	
O	Call to the unknown	The called function does not exist	

SMART CONTRACTS

Given the incorporation of a Turing-Complete Programming Language in the Ethereum protocol, the use of a technology first mentioned by Szabo [36] in 1997, can now be used in the blockchain to create a special external account - as mentioned earlier - that allows the coding of agreements in form of rules which are automatically executed when certain events take place in the [37, p. 1], this technology is known as Smart contracts. Their unique address can be invoked by transactions addressed to them. This transaction must be call from other external or by other contracts that interact or define using clients applications - written in various programming languages - that facilitate the interaction between them, but the official programming language is solidity – JavaScript like language. At a code level, contracts resemble a common programming class that can be used as a library to extend other contracts by interchanging messages through function calls. This also allow contract to behave like triggers, since a contract can execute another contract when certain events take inside or outside the network.

The Freedom of generating code in the blockchain expand its use case and new technologies had appear, like for example, the creation of autonomous Decentralize Applications (Dapps) that are govern by the community that sustain it [38] Some other use cases that smart contracts allow are [39, Sec. 3], [40], [41]:

- Creation of legal agreements (e.g. escrow, supply chain governance, Token sales).
- Organizations that exist in the blockchain (e.g. The DAO).
- Healthcare (e.g. EHR in compliance with HIPAA).

The Blockchain is a deterministic network, which mean that for any input into the chain, all the nodes participating on it should obtain the same result by the consensus algorithm. Smart contracts should behave the same manner, but the use of non-deterministic functions can lead to bugs inside the smart contract that could end in a none deterministic behavior. An example of this can be the use of the Solidity function *now***,** which is used to send the current datetime. If such function is added into a smart contract when the replication occurs in the network, the rest of the nodes will end with different timestamps [42] - [43]. Mostly all vulnerabilities are due to the creation of insecure smart contracts, to attend to this problem Luu et al. propose Oyente, a tool that identified 4 types of bugs through symbolic execution, which identify 8,833 out of 19,366 bugs in existing Ethereum contracts [44] Nicola et al. group 12 Ethereum smart contracts vulnerabilities using a systematic approach and generated a taxonomy of vulnerability as a reference for smart contract developers [45]. Li et al. conduct a systematic examination of the security risks in the blockchain and provided suggestion on security enhancement of existing tools [46]. As can be seen in Table 3 and Table 4 de majority of risk and vulnerability are introduce by using bad practices in smart contracts. Even though there are tools that try to detect bugs in the contracts, they don't manage to detect them all. Which leave the smart contract creators to follow good patterns and standards in creating smart contracts [47] and learn by the mistakes of others.

PROOF-OF-WORK

One of the reasons why the blockchain got famous was because the mechanism behind it consensus. By proof of work (PoW) the miners participating on the network can be rewarded by solving a hard – but capable – mathematical problem that determines which block of transactions is going to be the next to the blockchain. Participants only trust in the rules behind the network and not each other. To validate the mathematical problem, each miner has to provide enough computational power to beat other miners in computing and finding the solution to the math problem. The math problem in bitcoin is done by considering following fields from a block, the previous block version, hash, root hash, timestamp, bits and nonce. Then the following

algorithm – in pseudo code, is applied to this fields [48]:

(1) littleEndian(version)
(2) SwapOrder(previousBlockHash)
(3) SwapOrder(rootHash)
(4) littleEndian(timestamp), timestamp most be in in Unix epoch time
(5) littleEndian(bits)
(6) littleEndian(nonce)
(7) Concatenate the previous steps together in order.
(8) Change step 7 from hexadecimal to binary
(9) SHA256(step 8)
(10) SHA256(step 9)
(11) SwapOrder(setp 10)
(12) Compare the result from step 11 to the difficulty level of the block
(13) if result > difficulty, then increment the nonce from step 6 and do all again, otherwise the new block hash has been found.

The mathematical problem must be solved by trial and error and cannot be predicted. At the block is broadcast and the network validates if all the transactions are correct and not tampered. Then the miners compete once more to see who is the next one to solve the new hash. Ethereum also utilize PoW, but in a near future they are planning of moving to another consensus algorithm known as Proof-of-Stake (PoS), which allow users with to participate in the network as validators. For a user to participate it must lock a certain amount of currency and depending of this amount, then the new block validator is selected. PoS can be compare to the lottery, in where the person with more lottery tickets has a higher chance of winning.

The problem with the PoW is the highly consumption of energy that miners (validating nodes) need to spend due to mining. The energy consumption of the bitcoin network in comparison to Ethereum network, according digiconomist [49] - [50] is:

- Bitcon 70.2 TWh
- Ethereum 19.8 TWh

Following the same source, Bitcoin could power 104.4% of Czech Republic and ranking 40 in the countries energy consumption rank. Other statistics, the whole bitcoin network generate more energy than an average power plant or more than the largest coal mine in China [51]. The reason for the high energy consumption is due to the release time that both network have been around. This has led users to find new ways of mining blocks quicker by investing in sophisticated and expensive equipment. For both bitcoin and ether, miners utilize computers with many GPUs - also known as GPU Rigs - to perform the calculation of the block hashes. As a way of saving money in long term, another hardware solution was the use of specialized Application specific integrated circuits (ASIC) designed to calculate the specific hash algorithm utilize in the mathematical puzzle. The later hardware solution does not apply to Ethereum due to the algorithm behind its PoW, which was created to consume great amount of memory access bandwidth to eliminate the use of ASIC equipment [52] – by the time of making this paper this was the case - and give a better competitive edge to miners.

METHODOLOGY

As mentioned before, we are 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.

RESULT AND DISCUSSION

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 [53] in order to suit ours needs and to answer the questions raised in the Nuclear Facility section of this work. 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?

Material Movement Results

Truffle was used to compile and execute solidity code, to interact with Ethereum. The test blockchain was generated by Ganache inside a personal computer. A material management web page was also generated, see figure 3. The communication between MetaMask and Ethereum is made possible by the web3.js libraries that allow interfacing through an IPC and HTTP connection [54, p. 3]. For simplicity's sake we consider four materials (uranium, plutonium, beryllium and thorium.) that are commonly utilize in different nuclear facilities see figure 3. 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, under the element, is pressed the MetaMask plugin prompt a window (see figure 4) 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 figure 5.

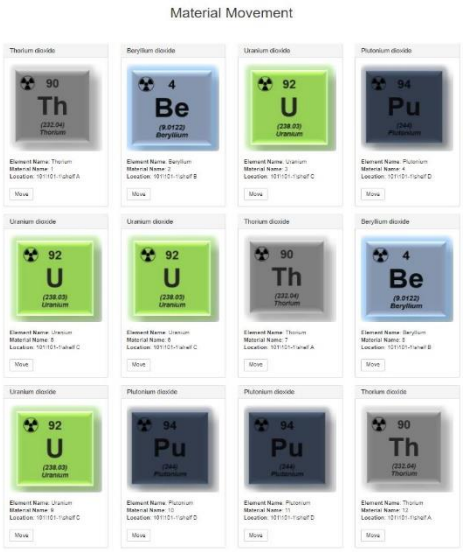

Figure 3
Material Movement Web Page

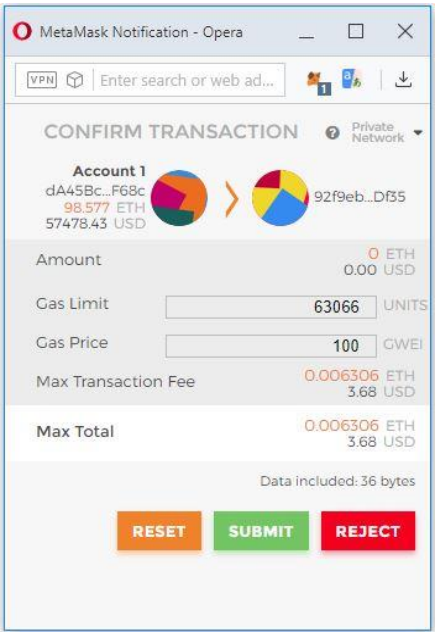

Figure 2
Submit or Reject Material in Transit

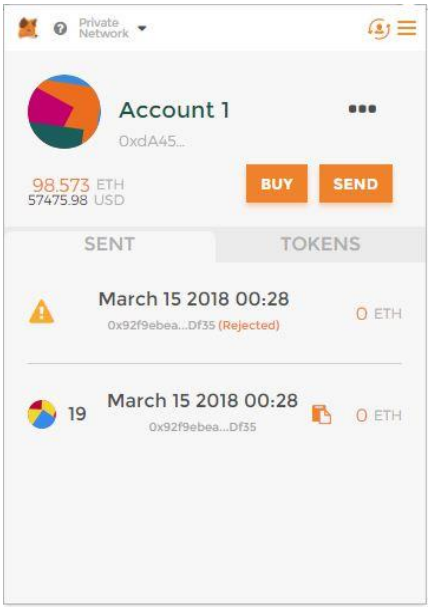

Figure 3
Transaction History-(upper) Rejected, (lower) Accepted

Discussion

According to figure 6, 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. 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 – as already mention, the solidity common development pattern. 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. This 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 like Oyente 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 can now answer all the question of the Nuclear Facility section and we can also add the blockchain to table 1 and conclude that this technology can be evaluated and tested to secure nuclear facilities.

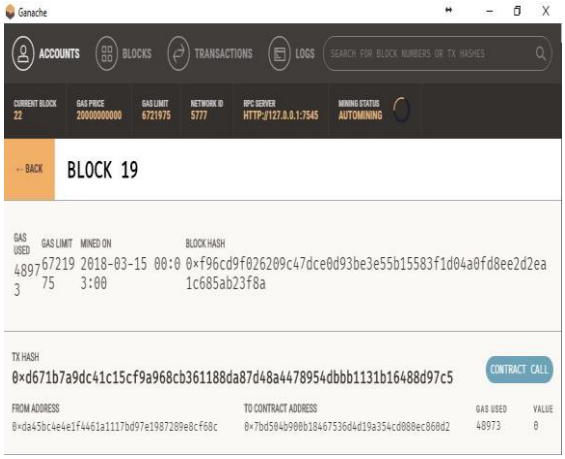

Figure 6
Accepted Transaction in Block 19

FUTURE WORK

Based on the result obtain and the amount of use cases using RFID and other tracking devices, a possible direction for this work to integrate the Ethereum blockchain into an embedded device with a RFID or NFC technologies to gather data and add it to the blockchain. This could also be implemented into the nuclear facilities to monitor inventory. Another interesting topic to study is how the different consensus algorithm could be used to stablish consensus between all the nuclear energy entities and regulators like the NRC and IAEA for auditing purpose only. In the later example the idea that comes into my mind is a distributed consensus that the power of decision is selected by certain conditions or reputation. The problem with that, like always is the trust, but blockchain is a trustless system and to help with that, certain sanctions could be implemented in the system to revoke privilege or degrade the reputation of a participating entity.

CONCLUSION

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 performing a traceability experiment and auditing experiment.

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.

REFERENCES

[1] S. Nakamoto. (2008, October 31). *Bitcoin: A peer-to-peer electronic cash system* [Online]. Available: http://www.bitcoin.org/bitcoin.pdf.

[2] Ethdocs. (n. d.). *Web 3: A platform for decentralized apps — Ethereum Homestead 0.1 documentation* [Online]. Available: http://ethdocs.org/en/latest/introduction/web3.html.

[3] Coindesk. (2017, April 11). *IBM Ramps up China Blockchain Work with Supply Chain Trial* [Online]. Available: https://www.coindesk.com/ibm-amps-china-blockchain-new-supply-chain/.

[4] W. J. Sutherland, *et al.*, "A 2017 Horizon Scan of Emerging Issues for Global Conservation and Biological Diversity," in *Trends in Ecology & Evolution*, vol. 32, no. 1, pp. 31–40, Jan. 2017.

[5] Guardtime. (n. d.). *KSI Technology | Industrial Scale Blockchain | Guardtime* [Online]. Available: https://guardtime.com/technology.

[6] H. M. Kim and M. Laskowski, "Towards an Ontology-Driven Blockchain Design for Supply Chain Provenance," in *SSRN Electronic Journal*, 2016.

[7] K. Francisco and D. Swanson, "The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency," in *Logistics*, vol. 2, no. 1, pp. 2, Jan. 2018.

[8] K. Just, "Blockchain in supply chain," in *Research Gate*, Jun. 2017.

[9] A. Chircu, E. Sultanow, and S. Prakash Saraswat, "Healthcare RFID In Germany: An Integrated Pharmaceutical Supply Chain Perspective," in *Journal of Applied Business Research*, vol. 30, pp. 737–752, Apr. 2014.

[10] Y. Bendavid and H. Boeck, "Using RFID to Improve Hospital Supply Chain Management for High Value and Consignment Items," *Procedia Computer Science*, vol. 5, pp. 849–856, 2011.

[11] K. Clauson, E. Breeden, C. Davidson, and T. Mackey. (2018, March 23). "Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare," in *Blockchain in Healthcare Today* [Online]. Available: https://doi.org/10.30953/bhty.v1.20

[12] J. I. Wong and J. I. Wong. (2016, October 10). "Even the US military is looking at blockchain technology—to secure nuclear weapons," in *Quartz* [Online]. Available: https://qz.com/801640.

[13] M. BAL, "Preventing Proliferation: Tracking Uranium on the Blockchain," no. 235, p. 16, 2018.

[14] World-Nuclear. (n. d.). *Number of nuclear reactors - World Nuclear Association* [Online]. Available: http://www.world-nuclear.org/nuclear-basics/global-number-of-nuclear-reactors.aspx. [Accessed: 02-Jun-2018].

[15] NRC. (2017, September 13). *NRC: Nuclear Materials* [Online]. Available: https://www.nrc.gov/materials.html#responsibilities.

[16] Worldatlas. (2017, April 25). "20 Countries Most Dependent On Nuclear Energy," [Online]. Available: https://www.worldatlas.com/articles/20-countries-most-dependent-on-nuclear-energy.html.

[17] A. Greenberg. (2017, June 12). *Crash Override Malware Took down Ukraine's Power Grid Last December | WIRED* [Online]. Available: https://www.wired.com/story/crash-override-malware/.

[18] C. Osborne. (2018, April 30). "Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout," in *ZDNet*. [Online]. Available: https://www.zdnet.com/article/industroyer-an-in-depth-look-at-the-culprit-behind-ukrain es-power-grid-blackout/.

[19] D. Kushner. (2013, February 26). "The Real Story of Stuxnet," in *IEEE Spectrum: Technology, Engineering, and Science News* [Online]. Available: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[20] N. Perlroth. (2017, December 22). "Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say," *The New York Times*.

[21] G. Chamales, "A New Approach to Nuclear Computer Security," [Online]. Available: http://www.nti.org/

media/pdfs/A_New_Approach_to_Nuclear_Computer_Security_xBVv4RR.pdf.

[22] IAEA. (2017, July 27). IAEA Illicit Trafficking Database Releases Latest Aggregate Statistics [Online]. Available: https://www.iaea.org/newscenter/news/iaea-illicit-trafficking-database-releases-latest-aggregate-statistics.

[23] B. Pack and B. Lee. "CNS Global Incidents and Trafficking Database: Tracking publicly reported incidents involving nuclear and other radioactive materials," NTI, Washington, DC, Annual Rep., 2014 [Online]. Available: http://www.nti.org/media/documents/global_incidents_and_trafficking_2014.pdf.

[24] S. Seebacher and R. Schüritz, "Blockchain technology as an enabler of service systems: A structured literature review", International Conference on Exploring Services Science, Springer, pp. 12-23, 2017.

[25] A. K. Bheemaiah, G. E. de M. K. Bheemaiah, and G. E. de Management, "Block Chain 2.0: The Renaissance of Money," *WIRED*. [Online]. Available: https://www.wired.com/insights/2015/01/block-chain-2-0/.

[26] Bitcoin-Wiki. (2017, December 23). "Elliptic Curve Digital Signature Algorithm" [Online]. Available: https://en.bitcoin.it/wiki/Elliptic_Curve_Digital_Signature_Algorithm.

[27] J. Song and P. B. Architect, "Blockchain 101 - Elliptic Curve Cryptography." [Online]. Available: https://eng.paxos.com/blockchain-101-elliptic-curve-cryptography.

[28] Bitcoin-Wiki. (2017, November 27). "Base58Check encoding" [Online]. Available: https://en.bitcoin.it/wiki/Base58Check_encoding.

[29] Blockgeeks. (n. d.). "What Are Addresses on Blockchains? Blockchain Address 101," [Online]. Available: https://blockgeeks.com/guides/blockchain-address-101/.

[30] J. Ray. (2018, March 25), Ed. "*ICAP: Inter exchange Client Address Protocol," in* ethereum-wiki [Online]. Available: https://github.com/ethereum/wiki/wiki/ICAP:-Inter-exchange-Client-Address-Protocol.

[31] Ethereum Stack Exchange. (2017, February 9). *Ethereumj - Checksum calculation for icap address* [Online]. Available: https://ethereum.stackexchange.com/a/12027.

[32] V. Buterin. (2015, January 10). "Light Clients and Proof of Stake," in *Ethereum Blog* [Blog]. Available: https://blog.ethereum.org/2015/01/10/light-clients-proof-stake/.

[33] Bitcoin. (n. d.). *Running a Full Node* [Online]. Available: https://bitcoin.org/en/full-node#what-is-a-full-node.

[34] D. G. Wood. (2018, May 28). *Ethereum: A Secure Decentralised Generalised Transaction Ledger* [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf.

[35] edward_monahan. (2017, August). "Ethereum Proof of Stake FAQ," in *Hacker News* [Forum]. Available: https://news.ycombinator.com/item?id=15056399.

[36] N. Szabo, "Formalizing and Securing Relationships on Public Networks," in *First Monday*, vol. 2, no. 9, Sep. 1997.

[37] nikhilNikoin. (2018, June 13) *Ed. A Next Generation Smart Contract & Decentralized Application Platform* [Online]. Available: https://github.com/ethereum/wiki/wiki /White-Paper#introduction-to-bitcoin-and-existing-concepts.

[38] Blockgeeks. (2017, May 08). "What Are Dapps? The New Decentralized Future," [Online]. Available: https://blockgeeks.com/guides/dapps/

[39] J. D. Hansen, L. Rosini, and C. L. Reyes, "More Legal Aspects of Smart Contract Applications," Perkins Coie LLP, p. 28, 2018 [White Paper]. Available: https://www.virtualcurrencyreport.com/wp-content/uploads/sites/13/2018/03/Perkins-Coie-LLP-More-Legal-Aspects-of-Smart-Contract-Applications-White-Paper.pdf.

[40] E. Kinoti. (2017, September 27). "Difference between DAO and Dapps on Ethereum network," *coinweez* [Online]. Available: https://coinweez.com/difference-dao-decentralised-application-ethereum-network/.

[41] N. Bauerle (2017, March 09). "What Are the Applications and Use Cases of Blockchains?" in *CoinDesk* [Online]. Available: https://www.coindesk.com/information/applications-use-cases-blockchains/.

[42] K. Minton. (2018, June 15). "VPNFilter Continues to Target More Devices," in *DZone Security* [Online]. Available: https://dzone.com/articles/vpnfilter-continues-to-target-more-devices.

[43] Solidity 0.4.24 documentation. (n. d.). *Units and Globally Available Variables* [Online]. Available: http://solidity.readthedocs.io/en/v0.4.24/units-and-global-variables.html.

[44] L. Luu, D. H. Chu, H. Olickel, P. Saxena and A. Hobor, "Making smart contracts smarter," in *The ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 254-269.

[45] N. Atzei, M. Bartoletti and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," in *International Conference on Principles of Security and Trust*, 2017, pp. 164-186.

[46] 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.

[47] Solidity 0.4.25 documentation. (n. d.). *Common Patterns* [Online]. Available: https://solidity.readthedocs.io/en/latest/common-patterns.html.

[48] Bitcoin Wiki. (2015, December 12). *Block hashing algorithm* [Online]. Available: https://en.bitcoin.it/wiki/Block_hashing_algorithm.

[49] Digiconomist. (n. d.). *Bitcoin Energy Consumption Index* [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption.

[50] Digiconomist. (n. d.). *Ethereum Energy Consumption Index (beta)* [Online]. Available: https://digiconomist.net/ethereum-energy-consumption.

[51] F. Rayal. (2018, February 15). *Power Consumption: Bitcoin Mining vs. Mobile Base Stations* [Online]. Available: http://frankrayal.com/2018/02/15/bitcoin-power-consumption/.

[52] J. Ray. (2018, March 25). "Ethash Design Rationale," in *ethereum-wiki* [Online]. Available: https://github.com/ethereum/wiki/wiki/Ethash-Design Rationale#fnv.

[53] ConsenSys (n. d.). “Ethereum Pet Shop -- Your First Dapp,” in *Truffle Suite* [Online]. Available: http://truffleframework.com/tutorials/pet-shop.

[54] web3.js 1.0.0 documentation. (n. d.). web3.js - Ethereum JavaScript API [Online]. Available: https://web3js.readthedocs.io/en/1.0/.