IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 23, Issue 2, Ser. II (Mar. – Apr. 2021), PP 10-22
www.iosrjournals.org

On-Blockchain Validation Smart Contract Model on Ethereum Distributed Ledger System for Pharmaceutical Products Distribution

Ahubele, B.[1], Eke, B. O.[2], Onuodu, F. E.[3]
[1,2,3] *Department of Computer Science, University of Port-Harcourt, Nigeria*

Abstract
Smart contracts are programs that run on a blockchain computational infrastructure via transaction-based state transitions. Business process and contracts have been difficult or impossible to carry out without third party due to lack of trust, challenge of repudiation and mutability of contract documents. In this work, a smart contract model with an improved verification and validation system was developed and deployed for a Pharmaceutical products distribution chain. The scripting model was used in implementing a smart contract and deploying it in Ethereum Blockchain. The system was designed using Object-Oriented analysis and design methodology (OOADM), and implemented using Solidity programming language, MetaMask and Remix IDE. The executed transactions were successfully deployed on Ethereum Virtual Machine (EVM). The result showed great accuracy, especially in its ability to tackle the problem of counterfeiting of Pharmaceutical products.

Date of Submission: 08-03-2021 Date of Acceptance: 22-03-2021

I. Introduction

An On-Blockchain is a regionalized and circulated digital ledger which record transactions across various PCs with the goal that any included record of transaction cannot be changed retroactively, without the change of the entire subsequent blocks. According to (Carlos et al, 2019) "an On-blockchain allows members to confirm and review exchanges independently and relatively inexpensively. Bitcoin was the first blockchain which was proposed by an individual or group of persons, named Satoshi Nakamoto (Nakamoto, 2008). Centralized systems are mainly trust-based and requires the involvement of a middle-man for the establishment of trust. These trust-based systems have created numerous issues such as single point of failure such as high transaction cost, lack of transparency, misconstrued information and etc. Ethereum blockchain was conceived and launched in 2013 by Vitalik Buterin. It became operational in 2015.

Despite, the opportunities identified by researchers on blockchain-based transactions, there are some inherent vulnerability with existing blockchain contracts, (Juels e tal., 2016) identified the use of smart contracts for criminal activities such as money laundering, market places for illicit goods, ransomware etc. The most famous DAO attack was a known vulnerability that occurred in 2016, in which over $50M was lost. The attacker identified a flaw in the contract code and quickly launched an attack.

In February, 2020, the United Arab Emirates-Ministry of Health and Prevention (UAE-MoHAP), as a team with the United Arab Emirates-Ministry of Presidential Affairs (UAE-MoPA), Health Sector and other important specialists propelled a blockchain-controlled platform that can store information for wellbeing, pharmaceutical government, private offices, wellbeing professionals and medication information as well. The blockchain-based medical platform tends to develop the effectiveness of MoHAP, health authorities, and smart health services by incorporating 100% Artificial Intelligence with health care services in UAE (United Arabs Emirates).

Any risk affecting the supply chain of pharmaceuticals could affect the efficiency of healthcare system and disrupt the supply of medicines. It is necessary to examine the vulnerabilities and risks that plague the industry by helping to ensure best practices for quality ingredient drug and flexibility in business. Over 10-30% of estimated death in Asia and African countries like Nigeria, Gabon etc. are due to distribution of counterfeit drug along the supply chain progression. Often sad to note that the adversative effects of such substandard, spurious, falsely labelled, falsified and counterfeit drugs are health impairment and infant mortality.

A satisfactory comprehension of hazard can assist pharmaceutical enterprises with minimizing cost and obligation, dodge waste and upgrade proficiency of the production network (Kwak and Dixon, 2008). With an estimated global loss of $200 billion, counterfeit drug prevention becomes a major use-case for blockchain in healthcare sector. Potential implementations for blockchain provides a network of solution in the drug

distribution supply chain for a contract-based relationship among the parties in order to facilitate transparency and traceability of drugs.

With smart contract on Blockchain implemented for pharmaceutical distribution, the issue of authenticity or originality of drugs can be verified. By storing information such as date, description, location and quality of products on the blockchain, the origin of a product can be easily traced and verified for any anomaly. For example, in the supply chain, the manufacturers can be assured that their raw materials are coming from reliable sources and consumers will also have more confidence that they are purchasing a legitimate product and from the right manufacturer.

Hull et.al (2016) recognized that shared blockchain technology enables business collaborations which require high reliability, trust worthiness, privacy-preserving and immutable data repositories. Smart contracts and blockchain technology give extraordinary potential for the robotization of business exchanges by lessening the requirement for administrative work, costs, association of legal advisors and court administrations to encourage trust between parties.

In all, a Blockchain based smart contract model can take care of such issues as Lack of trust, absence of verification, challenge of repudiation, need of middle men (witnesses) and lack of transparency and traceability.

II. Blockchain Technology

Blockchain is an innovative distributed ledger technology, that has restructured the way business processes in organizations are managed. It has made it possible to carry out implementation without a central party serving as trust (and failure) factor. It could also be described as a consensus-based, secure decentralised public/private database which stores information as transactions immutably over a peer-to-peer (P2P) network. Alharby and Van-Moorsel (2017) also defined a blockchain as a shared ledger that records all transactions that have ever occurred or exchanged since its creation. Blockchain has no single copy; rather, copies are distributed globally across the network nodes to be updated simultaneously (Chen, 2017). This ensures that the ledger cannot be manipulated by any single party without the consensus of the majority of participants in the network. Each block consist of data of transaction records and the corresponding information contained with each transaction. Every transaction (block) has a timestamp associated with when it was recorded to the blockchain. Subsequent blocks require the identifier (hash) of the preceeding block and this chain all the blocks together. In order to create a new block and add the corresponding block to the blockchain, they must be mined. The most common way to do this is through Proof-of-Work (PoW) mechanism where diggers perform computationally exorbitant undertakings to take an interest in what basically comprises a lottery for the option to add the following square to the chain" (Grech et al., 2016). Miners participate to solve the 'puzzle', and the successful miner broadcasts its PoW to the other miners for verification. Consensus is achieved once there is a slight majority (51%), after which the fresh block is added. Once a block is successfully added, it is disseminated to all the participating nodes to ensure that they are all updated with the latest blockchain. In addition, a reward is allocated to the miner for the work performed. This is usually a cryptotoken tied to the blockchain (e.g. Bitcoin or Ether).

2.1 Features of Blockchain Technology

Zheng et al (2016), listed the blockchain characteristics to include the following:

i. Decentralization
ii. Persistency
iii. Anonymity
iv. Auditability
v. Confidentiality
vi. Robustness
vii. Disintermediation
viii. Availability

2.2 Smart Contract

A Smart contract is a PC protocol that run on demand for Ethereum Virtual Machine (EVM) to carefully encourage, confirm and enforce the arrangement or a transaction performance or an agreement. Smart contracts are self-executing, self-enforcing computer codes that contain rules enforced by contractual parties. Once these agreed rules are realised, the contract is automatically enforced. The EVM on the other hand provides the operating system in which decentralized applications are built, deployed and executed on ethereum blockchain platform.

Smart contract has the following advantages:

i. **Direct customer's relationship**

Smart contracts eliminates trusted third party intermediaries and consents to transparent and direct relationships with customers.

ii. **Resistance to failure.**

Once any participating node within the blockchain network flops, the network will continue to function with no loss of data or integrity. Moreso, in executing applications using blockchain platform, businesses aren't dependent on a third party i.e no single person or entity is in control of data or money.

iii. Trust.

Trust enable business agreements to be automatically enforced and executed. Unlike traditional business process that requires a third party control for trust enforcement.

iv. Fraud reduction.

Since smart contracts remain put away to a distributed blockchain arrange, their result is approved by everybody in that organize. Therefore, nobody can force control toward discharging others' assets or information, as all other blockchain members would detect this and imprint such an endeavor as invalid.

v. Cost efficiency.

Eliminating trusted third party intermediary eliminates extra fees, permitting businesses and their customers not just to interact and transact directly on the other hand to do so without any transaction fee.

vi. Record keeping.

All contract exchanges are put away in sequential request in the blockchain and be able to be gotten to alongside the total review trail.

vii. Security

Smart contracts provides adequate security by employing the maximum level of available data encryption mechanism. However, this level of protection provided by smart contract is among the finest and the most secure on the world-wide-web (WWW).

viii. Speed

Smart contracts are transactions that run on blockchain platform, which executes faster than traditional programs. This speed saves countless hours when likened to traditional business processes implementation off-blockchain.

2.4 Supply chain

Supply chain management focuses on managing the whole supply chain from the raw material producer to the end-customer in order to foster improvements on performance and operational process. Several works exist in literature that attempted to reduce the complications along the supply chain distribution process in order to facilitate business relations for increasing the visibility of the supply network structures. Mahmud et al. (2018) proposed a calculated information model for production network among the executives with the mix of store network individuals and core interests on the business flow between the members. Grishhenko et al. (2018) presented a modern research in supply chain ontology by identifying research-created gaps and six supply chain ontology models. Despite the existing contributions to supply chain management, blockchain has been seen to have great impact in the industry. Furthermore, smart contracts can help to improve supply chain visibility by coupling them with loT devices that can track the location of goods, the inventory and the chain of custody.

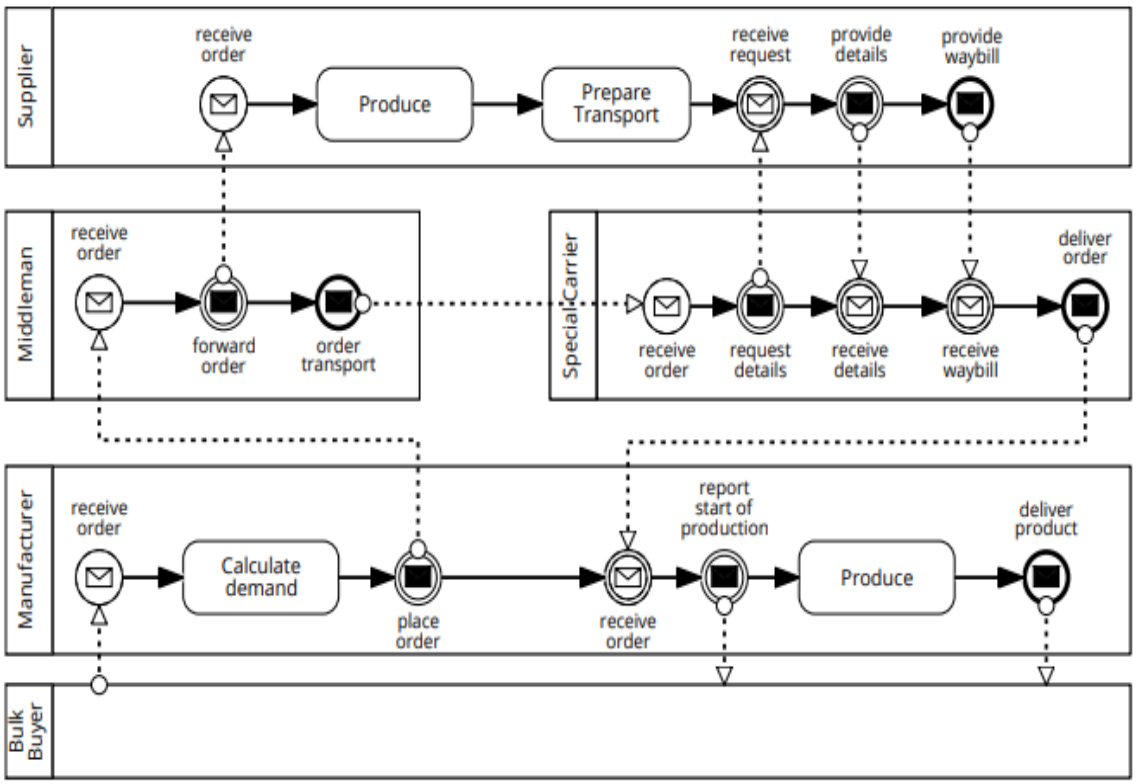

Figure 1: Supply Chain Scenario (Source: Weber et. al, 2016).

2.5 Pharmaceutical Product distribution Supply chain

Blockchain-based smart contract provides transparency across every network participants in order to enable them have access to the same data, providing a single-point of truth (Tsankov et al., 2018). The pharmaceutical production network straightforwardness is very vital but difficult to accomplish due to coordination and inventory network of the board complexity (Alexandre et al., 2018). Some supply chain logistics expert consider blockchain to offer enormous potential to be a much-needed stand for economic renewal (Ciccio et al., 2018) and capable of transforming the supply chain of pharmaceuticals by changing the way drugs are produced and distributed from the manufacturing point to the final consumer (patients).

III. New System Design

In the new system, Ethereum smart contracts provide diverse methods of facilitating contracts to work together with other contracts. The improved model generates correct-by-design ethereum-based transaction system. Verification tool ensures creating secure multiple smart contracts. The system comprises three main stages which include the design time stage, the On Blockchain Run time and the Off Blockchain Run time. In the design stage, the verification of DApps (smart contract) is carried out before the translation and implementation. This is done to ensure that certain error is not introduced in the design stage. A secured and trusted network is created , where only the trusted parties are given permission to join the network. On the backend, the Ethereum permissionless blockchain stores all the necessary exchanges, and once the information is entered to it can never be changed. When an item is produced, it is enrolled in the distributed ledger (blockchain), and hereafter, the drugs will be monitored, trailed and validated at each phase of their distribution. As the drugs proprietorship change truly, its possession will be moved simultaneously on the blockchain network. Drugs manufacturers will be able to see the journey of their products at anytime, from manufacturing to the patient. If the producer produces an extra item, they will generate a remarkable hash that will be attached to the said item. The item will be enlisted on the blockchain utilizing its hash (irreplaceable ID). The item will be considered as a computerized resource on the blockchain system, and its hash will be utilized to follow it wherever on the system. Any extra information of the item can be put away off-chain or on-chain relies upon manufacturer's choice. Off-chain data is merged with on-chain data by means of some kind of identifier. The following figure shows the basic structure of a blockchain based pharmaceutical chain management. The following types of information interaction and participants can be seen in the system:

1. NAFDAC - this is the government body with the responsibility of approving and disapproving drug use in the country. The developer or manufacturer of drugs needs to submit the drug for approval and activities are transacted on smart contract. The issuance of nafdac number for the verification of registered drugs are also handled by the Nafdac.

2. Manufacturer - Produces drugs and takes orders from the drug Distributors. The drug from the manufacturer needs to be verified by Nafdac and confirmed on the Blockchain. The manufacturer's account has the ability to register units of medicines in the system based on a unique identifier (uid), as well as to create transactions on the transfer of ownership of a unit of medicine to the Distributor.

3. Pharmacy - Retails drugs. Pharmacy account has the ability to create a transaction for the transfer of ownership of drugs to the patient allowing drugs to be validated as to be originating from the actual approved manufacturer.

4. Patient - This is the customer tht purchases the drugs on retail from the pharmacy. Purchased drugs can easily be verified on the Blockchain.

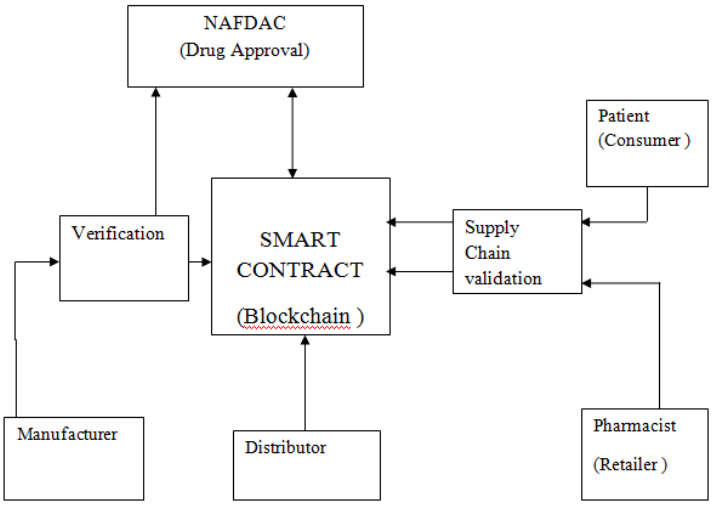

Figure 2: Blockchain Validation Smart Contract Model for Pharmaceutical Drugs Distribution.

3.1 New System Modeling

The system was designed using the Unified Modelling Language (UML). The use case design illustrated the flow of the various actions exhibited by the major components of the system. The use case design shows five main actors- Manufacturar, Nafdac, Distributor, Pharmacist and the Patient (Customer). The Manufacturer is the current contract main stakeholder in the system responsible for the production of the drug. Newly produced drug will get to the Nafdac for approval before it will be package for the distributors who have ordered for the product. Drugs that are not approved leads to termination of contract.

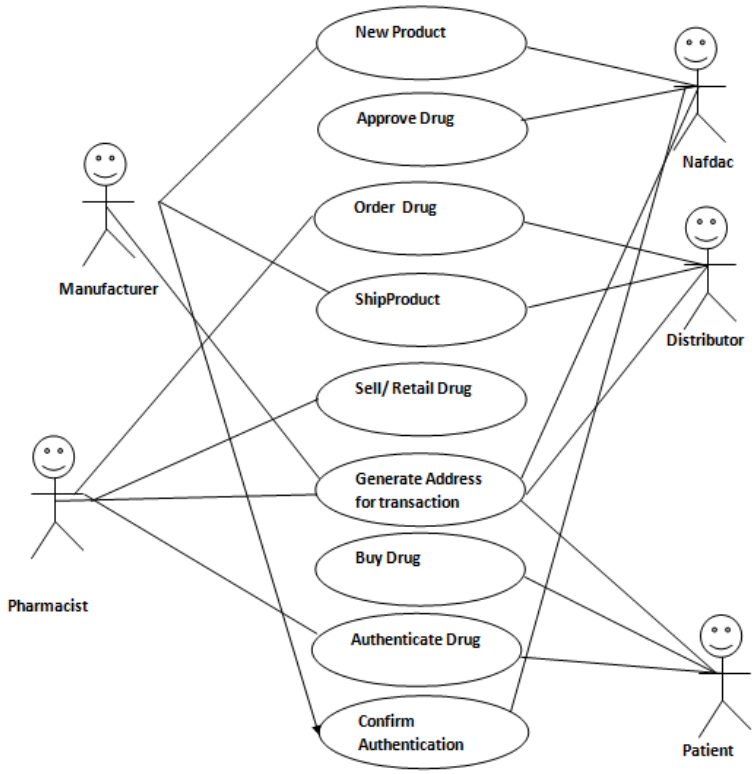

Figure 3: The Use Case diagram of the Proposed model

In the system the executor indicates interest when the asset is placed for bid by the Manufacturer. The Owner still uses his private key peer to trigger the smart contract for execution, the authorization is done to prevent initiation of transaction where the Manufacturer is not actually the one who places the contract for execution. Once the Manufacturer authorizes the transaction key peers are created by the blockchain and the exchange approves the contract. The Nafdac checks to know if the drug is already approved if not the contract submits it for approval if it gets approved then it goes to the next process. If the process proceeds then the exchange approval involves acknowledgement that the Distributor have enough fiat (money) or enough coin to pay for the contract of packaging and shipment execution. When the Distributor sends coins to the executor via the blockchain and the exchange or wallet. The blockchain in return confirms the transfer of the escrow as published in the Ledger of the blockchain. The drug is shipped on confirmation. The same process is carried out by the Pharmacy and the Distributor ships its own consignment to it. The Patients can both validate the drugs on the Blockchain before buying or after purchasing the product since the contract covers pre-purchase and post purchase block verification and validation.

In modeling the Class diagram for the smart contract, the contract was defined using classes; public and private functions, and can inherit from other contracts. We also introduced some new concepts in these diagrams to enhance the model. These concepts are simply introduced as UML stereotypes, which describes tags that can be used in UML diagrams wherever applicable.

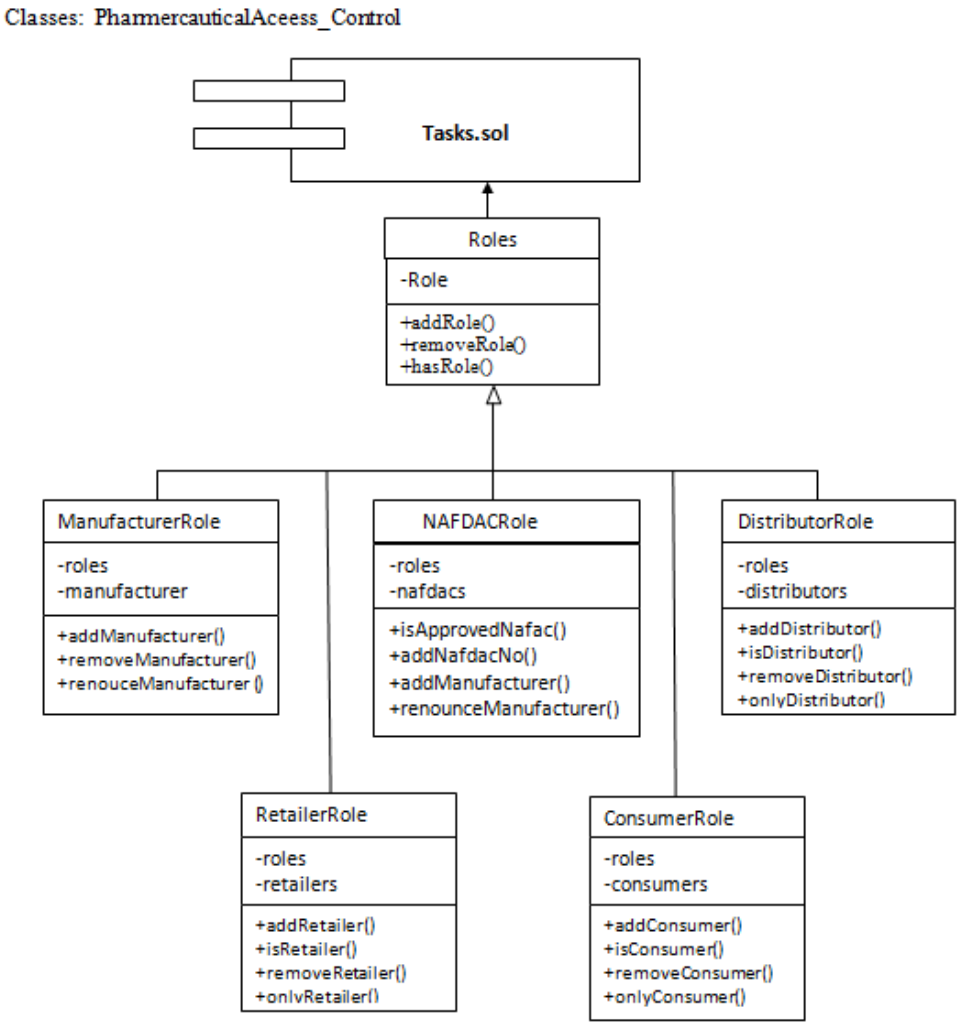

Fig 4 : Pharmaceutical_Aceess_Control UML Class Diagram

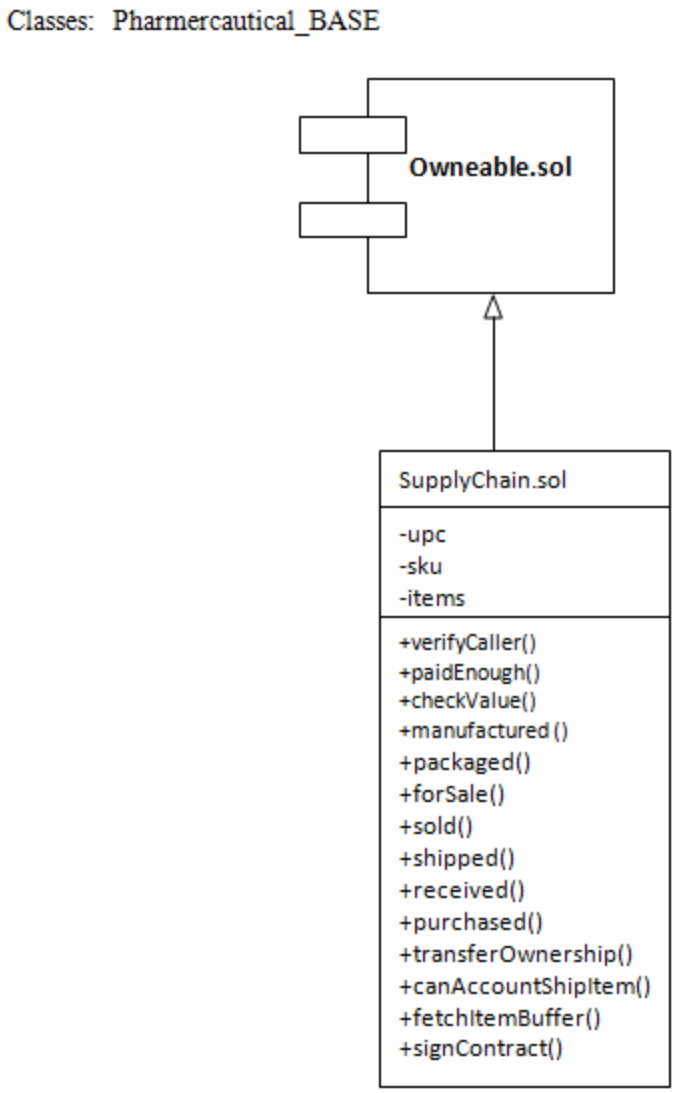

Fig 5: Pharmarceutical_SupplyChain UML Class Diagram

The class diagrams are shown in figure 4 and figure 5. In figure 4, the UML class diagrams show the Roles class, the ManufacturerRole, NafdacRole, DistributorRole, RetailerRole, ConsumerRole. The Roles is a class that handles the assignment of task along the supply chain, the activation of the Contract and handling of the key tasks usable by all the other classes. It depends on the Roles package of the ERC20 code in Solidity library. The ManufacturerRole class inherits from the Roles class and it handles the adding of manufacturer activity address on the Blockchain using addManufacturer(), it can also remove and renounce activity on the Blockchain using removeManufacturer() and renouceManufacturer() methods respectively. NafdacRole class handles the contract part involving the approval of new products and adding same on the Blockchain. DistributorRole class assigning of a Contract for the packaging and shipping of the product to the pharmacy (retailer). The RetailerRole on the other hand is the class that processes the contract for processing order and getting supplied product to the pharmacy and also communicating with the consumer buy requests. ConsumerRole Class allows the customers to interact with the supply chain contract. It adds, removes, allow consumer to check and validate a product from information on the Blockchain. In figure 5 the SupplyChain class uses the activities of the various methods in the classes in figure 4 to coordinate the core activities going on on the supply chain. Some of its methods include +verifyCaller(), +paidEnough(), +checkValue(), +manufactured(), +packaged(), +forSale(), +sold(), +shipped(), +received(), +purchased(), +transferOwnership(), +canAccountShipItem(), +fetchItemBuffer(), +signContract(). It uses some functionality from the ERC20 class which is extended to carry out its internal functionality.
Figure 6 shows the activity diagram of the design, while figure 7 shows the Sequence diagram.

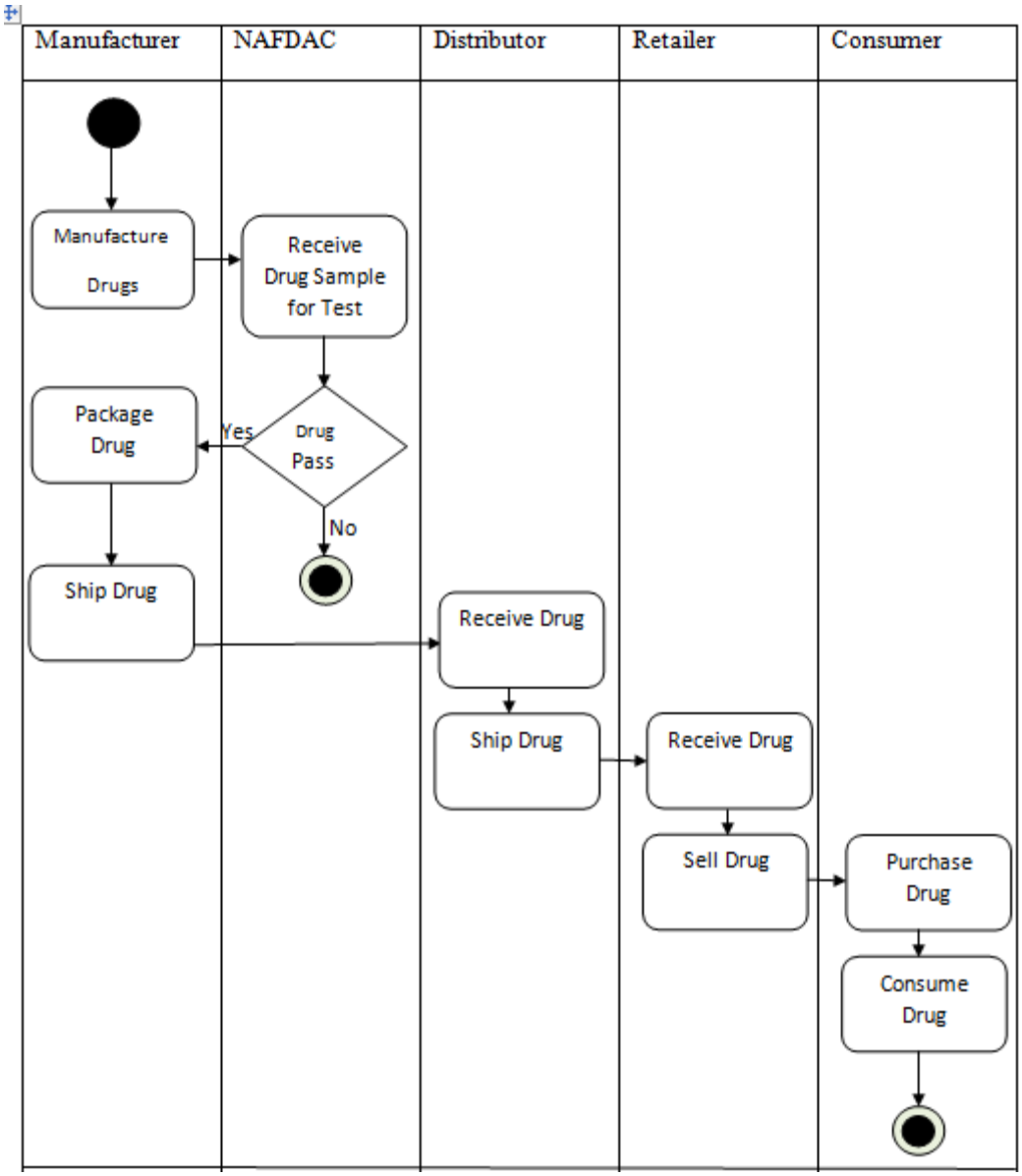

Fig 6 : Pharmaceutical Supply Chain Activity Diagram

The Sequence diagram illustrates the sequence of events, external interactions for approved product in the supply chain. A proof-of-concept which provides a trust-based method for facilitating deals between partners was developed to run on Ethereum, which is an open blockchain platform for building and using decentralized applications. The parties consists mainly of manufacturer, distributor, retailers, courier (shipment) and the consumers. The manufacturer deploy the contract exclusively for the **Retailer's** account. The *Retailer* enters a contractual relationship with the manufacturer and place an order for the quantity of product required. The *Manufacturer* in return confirm the order sent by the retailer and process same by validating his contractual relationship with the retailer. Consequently, the payment made by the *Retailer* for the product order goes to the smart contract account, until the *Manufacturer* ships the requested product to the *retailer*, his payment will not be released. The *Manufacture* equally enters a contractual agreement with the *Courier or shipment* agent for shipping the drugs to the Distributor who actually makes it available to the pharmacy (retailer) as requested.

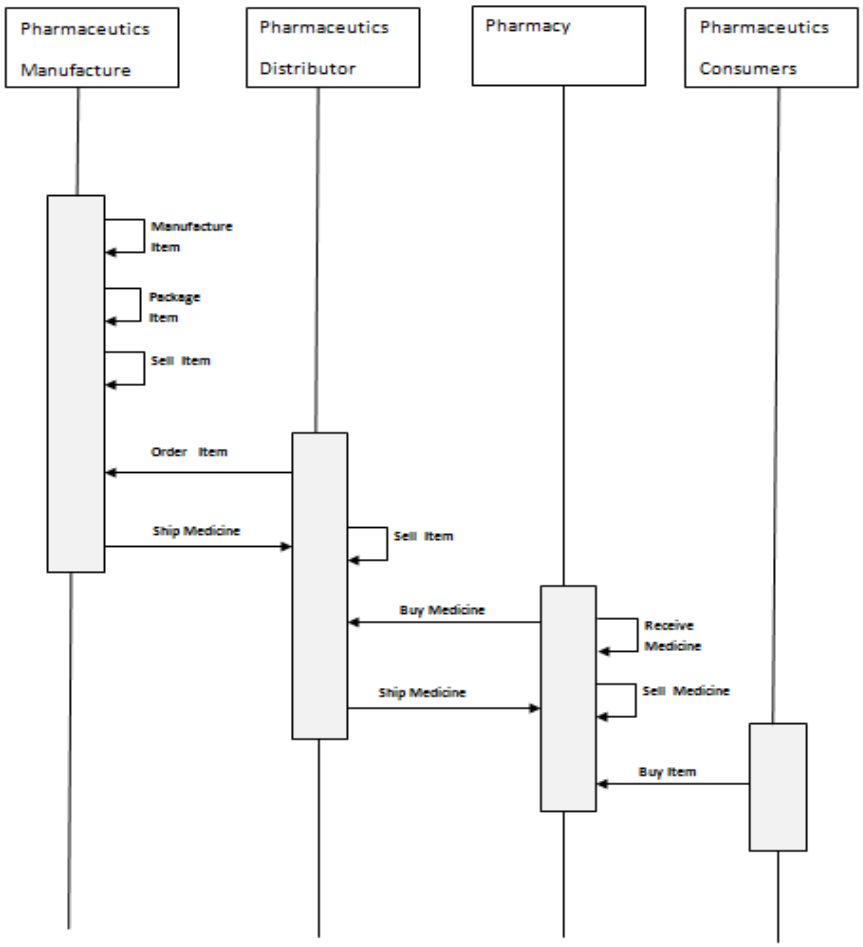

Figure 7: The Sequence diagram of the proposed system

IV. System Output and Result

The Smart Contract was implemented on Ethereum blockchain, where Remix IDE tool was used to develop smart contracts in Solidity programming language. Figure 9 shows how the smart contracts was written and compiled in the Remix IDE. In Remix, a new file was created by selecting the "+" icon in the upper left-hand corner. It was named :MyToken**.sol**. The user enters the smart contracts source codes.

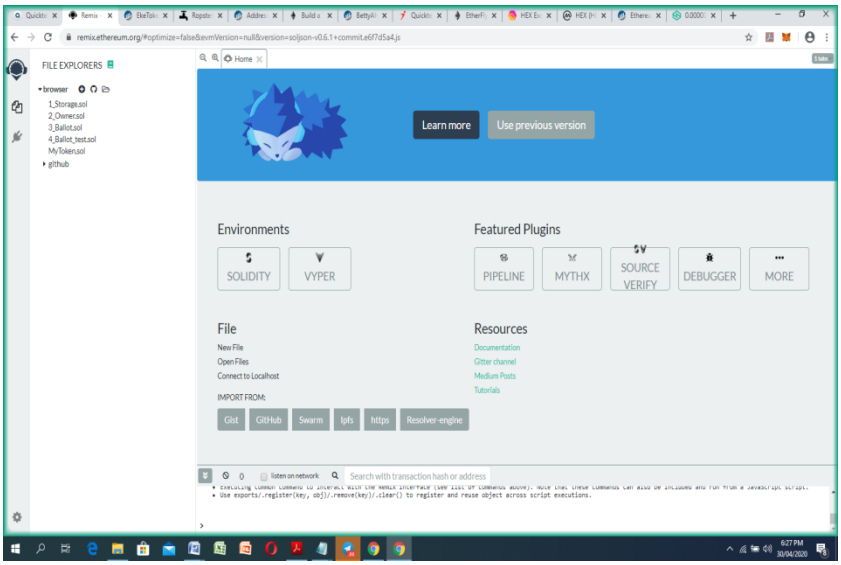

Figure 8: The Remix IDE Environment.

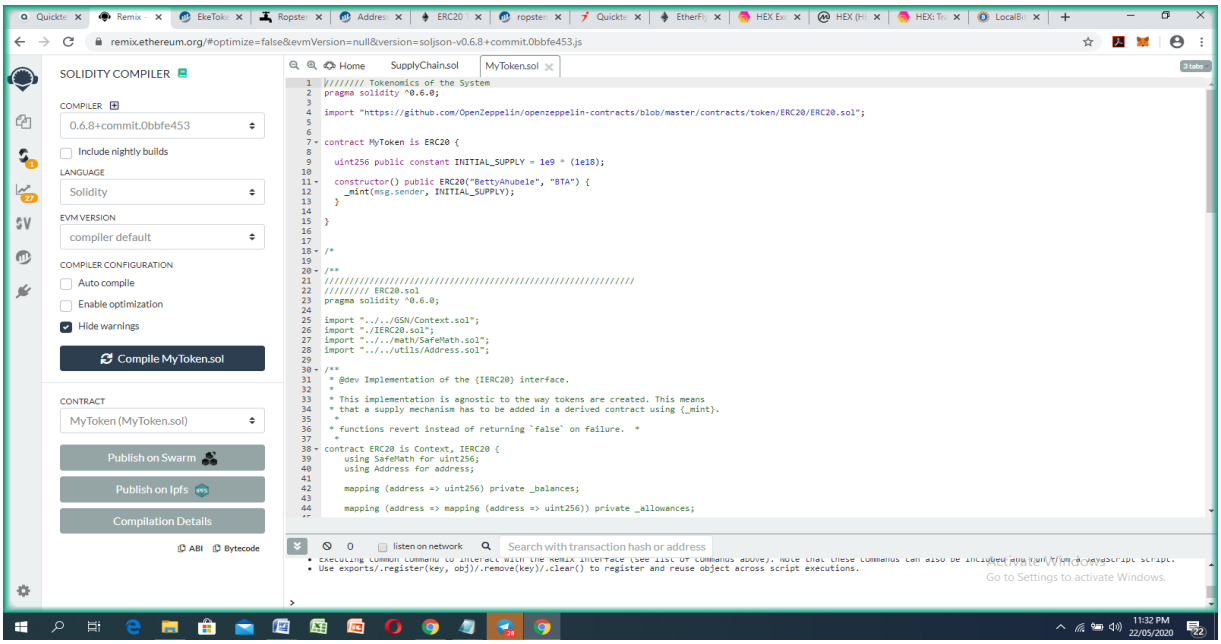

Figure 9: Remix IDE Showing the Code Compilation for the Pharmaceutical Supply Chain.

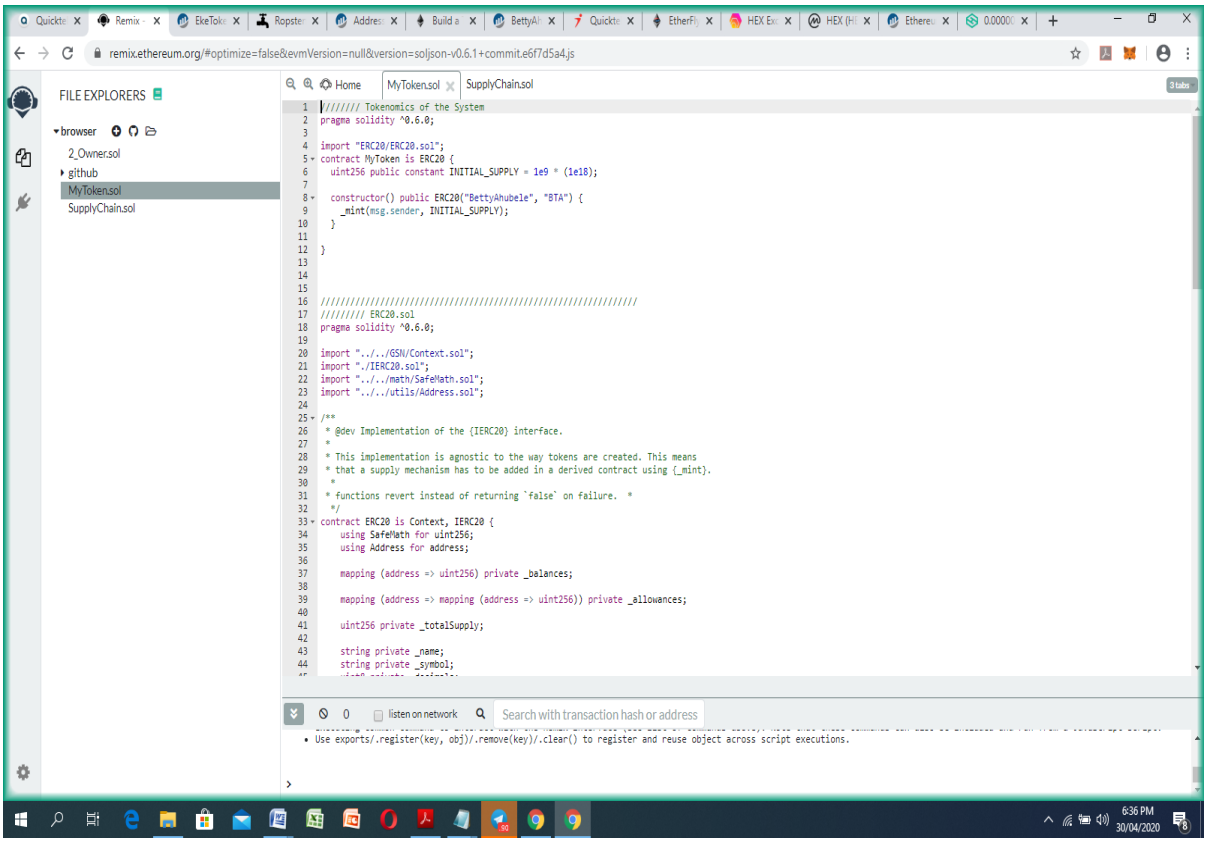

Figure 10: Remix IDE Showing the Code for the Drug Supply Chain.

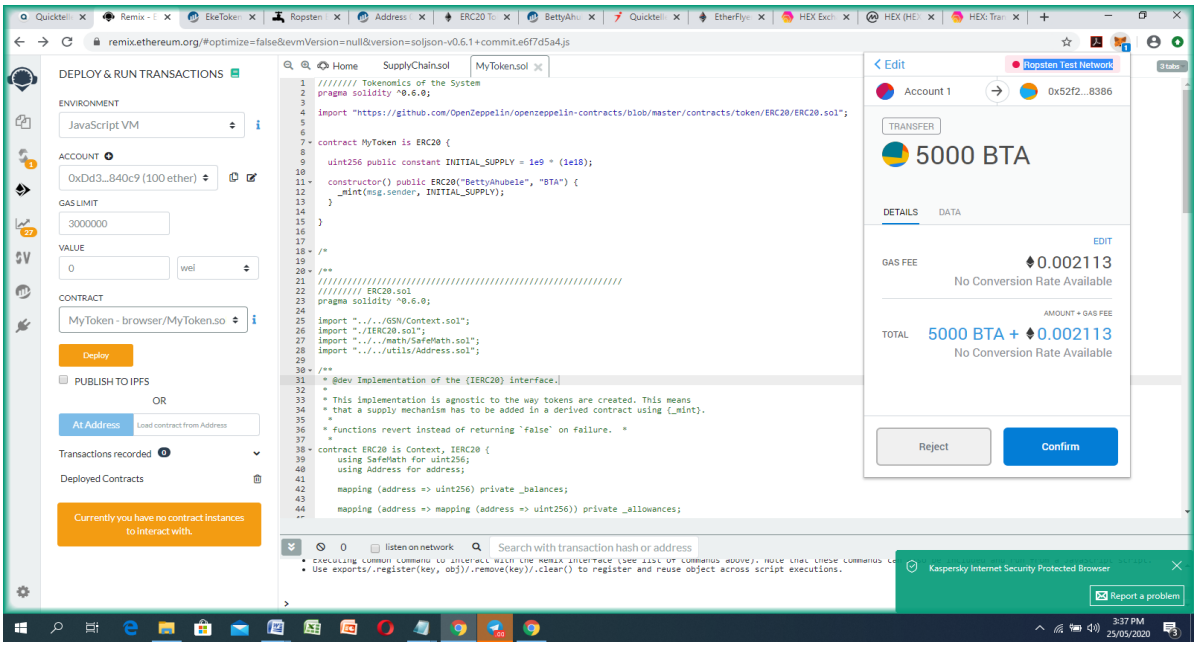

Figure 11: SSCDLS:Smart Contract Scripting and Deployment on Remix IDE

Figure 11 shows the confirmation and transfer of token generated from the deployed contract token. The Token name is BetTyAhubelle (BTA) the transfer of the token required an Ether gas and need to be confirmed. On confirmation the token on the transaction is executed and the details of the transaction published on the etherScan. Once a user initiates deployment of the transaction, a confirmation page will be displayed where the user confirms the transaction before it can be deployed on the Ethereum blockchain. Upon a successful deployment, the user contract is permanently recorded on the blockchain. The user also has a choice to reject a transaction in order to allow any correction. In most cases the testchains are designed to allow programmers to deploy, check and edit the source code. When the test are done, deployment on the Ethereum Mainnet can be effected allowing realife use of the contract.

Figure 12 shows how to verify and publish a transaction on etherscan. It is very pertinent to verify smart contracts in order to show that the contract code is exactly what is being deployed onto the blockchain and also allows the public to audit and read the contract. Etherscan ensures that all token contracts must be verified before they can be updated with information submitted by the contract owner.

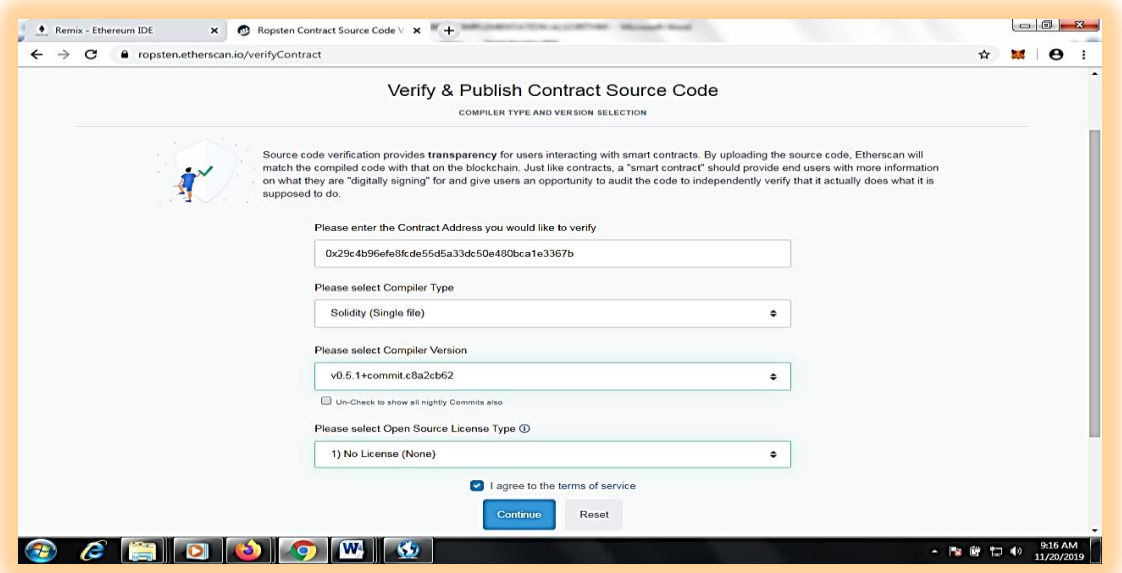

Figure 12: SSCDLS:Smart Contract Verification and Publishing Procedures

V. Conclusion

Smart contracts are self-executing, self-enforcing business logics that run on Ethereum blockchain. In addition, smart contract is an expression used to depict a PC code that can encourage the trading of cash, content, property, offers, or anything of significant worth. When running on the blockchain, a smart contract becomes like a self-working PC program that naturally executes when explicit conditions are met. Blockchain and decentralized applications opens manifold opportunities to redesign collaborative business transactions such as pharmaceutical drug supply chain, food supply chain,travel and tourism industries booking reservation, decentralized global market for computing power, logistics processes and a few others.

The study explored the use of Ethereum blockchain platform to execute smart contracts for Pharmaceutical products supply chain and distribution. The application of Smart Contract in Pharmaceutical distribution will go a long way in eliminating the problem of counterfeit and unverified drugs.

References

[1]. Alexandre, B., R. Brown, R. Julio and B. Antonio (2018).An Exploration of Blockchain Technology in Supplychain Management. 22nd Cambridge International Manufacturing Symposium. University of Cambridge.1-12.

[2]. Alharby, M., and A.Van-Moorsel (2017). Blockchain-based Smart Contracts: A Systematic Mapping Study, International Conference in Programming Languages with Applications to Biology and Security. Springer.142-161. https://doi.org/10.5121/csit.2017.71011. Retrieved 22/09/2018.

[3]. Carlos, M.E., I. Solaima, I. Sfyrakis, J. Ng-Crowcroft (2018). Implementation of Smart Contracts Using Hybrid Architectures with On- and Off-Blockchain Components.23-29. https://arxiv.org/pdf/1808.00093.pdf. Retrieved09/10/2018.

[4]. Chen, T., X. Li, X. Luo and X. Zhang (2017). Under-optimized smart contracts devour your money. IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER). 442-446.

[5]. Ciccio, C.D., A. Cecconi, M. Dumas, L. Garcia-Banuelos, O. Lopez-Pintado, Q. Lu, J. Mendling, A. Ponomarev, A.B. Tran, and I. Weber (2018). Blockchain Support for Collaborative Business.Processes. Informatik Spektrum. 42(3).182-190.

[6]. David, N., R. Riya. and P. Blessy(2019).Conveying Blockchain and Internet of Things. International Journal of Innovative Technology and Exploring Engineering (IJITEE).8(7).662-667.

[7]. Grech, N., M. Kong, A. Jurisevic, L. Brent, B. Scholz and Y. Smaragdakis (2018). Madmax: Surviving Out-of-Gas conditions in ethereum smart contracts. Proceedings ACM Programming Language 2.

[8]. Grishhenko, I., M. Maffei and C. Schneidewind (2018). A semantic framework for the Security Analysis of Ethereum Smart Contracts. 243-269

[9]. Hull, R., V.S. Batra, Y.M. Chen, A. Deutsch, F.F.T. Heath III and V. Vianu (2016). Towards a Shared Ledger Business Collaboration Language Based on Data-Aware Processes. Springer International Publishing, Cham.18-36.

[10]. Juels, A., A.K osba and E. Shi (2016). The ring of gyges: investigating the future of criminal contracts. ACM SIGSAC Conference Proceedings on Computer and Communictions Security.283-295.

[11]. Mahmud, H., J. Lu, and Q. Xu (2018). A blockchain-based service provider validation and verification for Health care Virtual Organization. UHD Journal of Science & Technology. Huddersfield. UK. 2(2). 24-31.

[12]. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. 100-121. https://www.blockchain.org

[13]. Tsankov, P., A. Dan, D.D. Cohen, A. Gervais, F. Buenzli and M. Vechev (2018). Securify: Practical security analysis of smart contracts. https://arxiv.org/abs/1806.01143. Accessed 10/06/2019.

Ahubele, B, et. al. "On-Blockchain Validation Smart Contract Model on Ethereum Distributed Ledger System for Pharmaceutical Products Distribution." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 23(2), 2021, pp. 10-22.