A Triplicate Smart Contract Model using Blockchain Technology

Article · June 2017

DOI: 10.22632/ccs-2017-cps-01

3 authors, including:

Peter U. Eze
University of Melbourne
12 PUBLICATIONS **2** CITATIONS
SEE PROFILE

Chinedu Reginald Okpara
Federal University of Technology Owerri
3 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Special Issue Article

Circulation in Computer Science – *Special Issue*
Disruptive Computing, Cyber-Physical Systems (CPS), and Internet of Everything (IoE), pp:1-10, 2017
https://doi.org/10.22632/ccs-2017-cps-01

A Triplicate Smart Contract Model using Blockchain Technology

Peter Eze
Department of Computing and Information Systems
University of Melbourne
VIC, Australia

Tochukwu Eziokwu
Department of Computer Software Engineering, Afrihub
ICT institute, Central Area,
Abuja, Nigeria

Chinedu Okpara
Department of Electrical &Electronic Engineering,
Federal University of Technology
Owerri, Nigeria.

ABSTRACT
An emergent use of the blockchain technology is to enable the transfer of digital assets between two parties. An extension to this is the Smart Property in which physical assets could be transferred too. Another extension is the exchange of services of all kinds in form of digitally executed contracts. In this paper, the problems with existing attempts to implement an all-inclusive smart contract platform were identified and a new framework proposed. In this framework, the technical and legal terms of any contract could be executed digitally if prepared with appropriate legal prose and required parameters for each of the terms of the contract. The cores of the framework are the technical, business and legal models, which are connected to each other. The technical model adapts block chain technology while ensuring granularity in implementing the terms of the contract as presented by the legal model using legal prose and necessary parameters. Using the proposed framework, some questions that have persisted with current implementation of Smart contracts that involves the blockchain were answered. The framework improves the efficiency and practicability of using smart contract for physical assets and non-financial services with emphasis. The contribution is mainly on ensuring an adoptable and practicable smart contract platform.

Keywords
Smart Contract, Blockchain, 3SmartContract, Cryptocurrency, Framework, Legal Prose

1. INTRODUCTION
Some technologies are disruptive and the blockchain technology is one of them. Blockchain can be seen as a combination of existing technologies and new ways to look at existing phenomenon. The ideas of cryptography, hashing, digital signature, open-source systems and distributed systems, which form the core of the blockchain (as used in bitcoin cryptocurrency) are not new. However, the idea of how they could be used to achieve decentralization of control and proof of ownership of both physical and intangible assets has made it a disruptive technology for various applications.

What is a blockchain? It is a distributed database of verified and irreversible grouped transactions in the form of public ledger, held in such a way that each group of transactions is linked with the next and the previous group [1]. The major idea that makes blockchain technology disruptive is that of ***distributed consensus*** among the participants before a transaction can be committed into the block chain. Any transaction that has been verified by the (majority) nodes in the distributed computing system will be committed into the blockchain and the evidence of such a transaction having occurred will never be erased. Cryptography and digital signature helps to maintain security, authenticity and anonymity of users. A diagrammatic illustration of the blockchain technology is shown in figure 1 below.

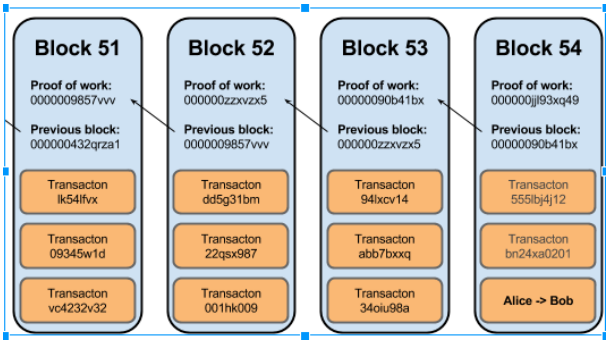

Figure 1 - Sample block chain [2]

In the blockchain, some transactions are grouped together and hashed. The hash of each block contains a hash of the previous block. This reference of a block to the previous block creates a chain back to the first or root block. Hence, the name, block-chain. The linking of the block forms a security feature. Tampering with any of the information in any block would make the hash not to match throughout the block tree. Hence, once a block is verified and committed, it cannot be tampered with in anyway without being detected.

Applications using the blockchain technology and its concepts have been described as largely disruptive as it would change the way the world would conduct business and even think about business in the first place - everyone is expected to look after the created assets so that they will not to be stolen.

In this paper, we enhanced this technology for application in executing smart contracts, especially those that lead to the transfer of ownership or creation of physical properties in the blockchain. Corruption and fraudulent activities often originate from illegal sale or transfer of properties. The motivation for this work comes from the following statement in [2]:

"But a corrupt government can sometimes erase their ledger and demand that you give them back the land that you rightfully own. Other assets such as your laptop, jewelry or phone has proof of your ownership in terms of a sales receipt, once you lose it, it's hard to prove ownership. Physical assets can have the same unique ID the same way people do and can

Guest Editor: Dr. Kennedy Chinedu Okafor
kennedy@ccsarchive.org

be accounted for in a Blockchain. Instead of representing money, the blocks represent tokens of physical assets." [2].

Hence, in order to safeguard one's properties and ensure traceable transactions, one needs to think of a new way of registering and transferring properties in order to ensure irrefutability without involving a third-party human trustee.

This paper is organized thus: Section 2 reviews the blockchain technology and its underlying concepts while section 3 introduces the smart contract concept and its possible applications. Section 4 reviews current works in the smart contract domain and identified nine questions that needs to be answered. Section 5 is our main work and it proposes the ***3SmartContract*** model for answering the questions raised. Section 6 discusses the framework in the light of the raised questions while section 7 concludes the work and identifies areas for further research.

2. THE BLOCKCHAIN TECHNOLOGY

As defined by **[1]**blockchain can be referred to as a distributed database of records or public ledger of all executed transactions (or digital events) which are shared among participating nodes. Nonetheless, the scholarly definition of it had been contentious. While **[30]** is of the opinion that cryptocurrency is an integral part of the block chain since it would always serve as incentive for miners, writer in **[6]** adopted VitalikButerin definition -"*A magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong crypto economically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies.*"- On the grounds that he acknowledged cryptocurrency as a rudimentary characteristic of blockchain when financial applications are being considered rather than a definitional term. However, regardless of which block chain definition is being considered, the reporter in [**5]** identified ***immutability***, ***transparency*** and ***decentralization*** as "key" defining terms of a blockchain. Immutability ensures data integrity using hashing algorithm whereas transparency means the data in the blockchain can be accessed randomly by the public. Finally, it is considered a decentralized system because it is a distributed database of records.

There exists myriads of blockchain technology applications ranging from financial applications to non-financial applications. The works reported in **[1]** and **[6]** elaborated on these applications. However, bitcoin standsas the most prevalent and prominent blockchain application **[1]**. The blockchain under bitcoin protocol operates as follows: a bitcoin seller (S) requires acryptographic proof to send a bitcoin to a buyer (B). With cryptographicproof, each transaction issent tothe "public key" of the buyer digitally signed using the "private key" of the seller. In return, the buyer confirms the seller's digital signature i.e. private key of the transaction using the seller's "public key." Each transaction is broadcasted to every node in the bitcoin network and then it is recorded in the public ledger after the miners have verified the transactions through a process called **Consensus**. Figure 2 shows a pictorial summary of how the blockchain technology works. Four key underlying concepts of blockchain as itemized by **[4]** are: Decentralized consensus, smart contract, trusted computing and consensus protocol such as proof of work/stake, byzantine fault tolerant (BFT), among others.

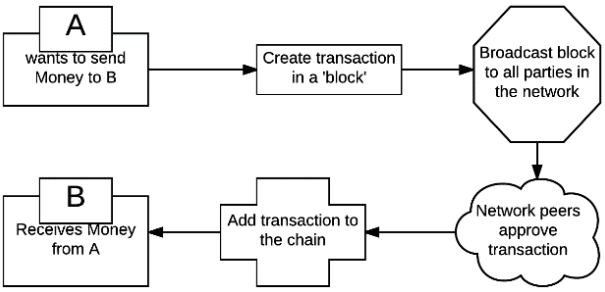

Figure 2- How a block chain works

Having a common agreement among the participating nodes on what information should be included in the blockchain network establishes a decentralized consensus scheme **[5]**. These participating nodes are referred to as ***miners***. Bitcoin (First cryptocurrency to use blockchain**[7]**) developers unveiled the concept of miners. In bitcoin protocol, miners are set of people who have dedicated their computers/nodes to solve complex mathematical problem called **proof of work** in order to ensure no double spending of the bitcoin occurs. However, to ensure that no adversary miner exists in the network, it is expected that more than 50% are trusted miners **[3] [8] [9]**. Otherwise, the adversary miners can come in and maneuver the blockchain, putting illegitimate transaction in block and subsequently including the block in the chain. Every transaction in blockchain occurs in trusted computing environment **[31]**, because all transaction occurs in a peer-peer manner and the nodes involved have to trust each other for such transaction to be successful.

3. CONCEPT OF SMART CONTRACTS

Smart contract is a digitalized way of executing contracts. Clack et al in [14] defined it as user application with inbuilt rules to govern transaction which are enforced by the network miners. With it, two anonymous individuals can buy and sell asset by simply using a node comprising of a computer system with smart contract application. Smart contract had found important applications in the financial industry as mentioned in **[11]**, **[16]** and **[17]**. Aside non-physical assets such as bond, stock, etc., obtainable in financial industry, smart contract is finding applications on physical assets such as land, car, houses, voting system etc**[1]**. Smart contract operates on consensus/blockchain networks such as ethereum, corda, ripple, hyper ledger, bitcoin, among others **[13] [14]**. According to **[1]** many companies that operate blockchain technologies, support smart contract.

To explain the importance of smart contract, report in **[10]**analysed the difference between traditional security market based contract and its smart contract counterpart. As shown in figure 3, the traditional means of executing security market contract such as sell or buy of a stock involves many intermediaries. The seller and the buyer first contacts their stockbroker-usually a pundit in stock exchange. The two stockbrokers charge a commission and introduces them to the second middle man called the Central Counterparty Clearing House (CCP) whose job is to ensure that none of the contracting parties defaults. CCP afteraccepting their own commission, takes the asset from the seller's broker through the seller's custodian and receives money from the buyer's broker through the buyer's custodian. The CCP then instruct the Central Security Depository (CSD) to credit the buyer's custodian with the asset and the seller's custodian, the money.

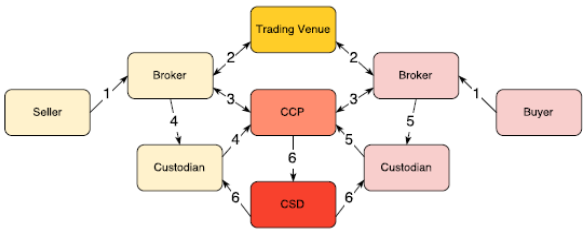

Figure 3- Traditional security market contract [10]

However, in the use of smart contract to execute the contract of asset delivery, as shown in figure 4, the process requires no intermediaries. Rather, smart contract code is run simultaneously on Alice and Bob computers and after some cryptographic verification, the transactions are recorded on the ledgers. According to **[10]**, smart contract whose underpinning technology is blockchain will make the process of contract execution faster since intermediaries which instigates the bottleneck of the traditional system as seen in our stock market today will be eliminated. Also, the cost of transaction is most likely to reduce.

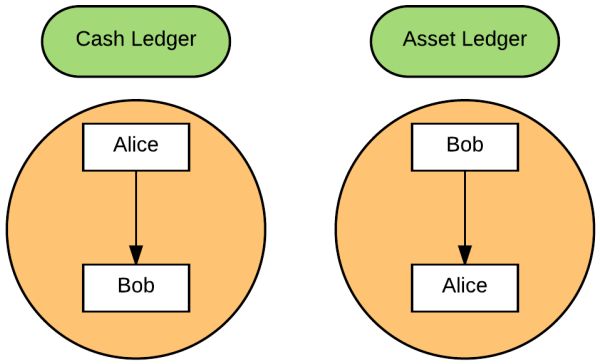

Figure 4- Security market smart contract

Smart contract has two semantics: operational and denotational semantics**[14]**. Operational semantic covers the executable part of the contract and denotational, the legal aspect which is non-operational. Legal framework and an identity-based permissionlessblockchain for smart contract was proposed by **[10]** and **[14]** buttressed it by creating legal template for a smart contract as shown in figure 5. The legal prose and parameter values are developed during the negotiation phase, hence portrays the denotational semantic of the contract. An agreement is reached when all the parameters listed have values **[14]**.

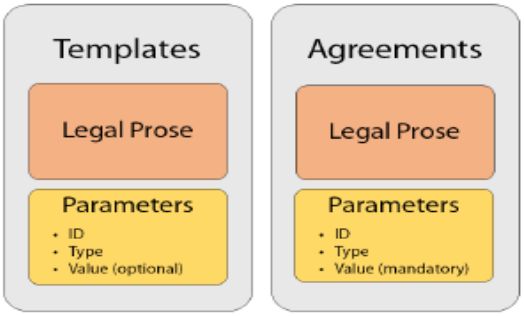

Figure 5: Smart contract template [14]

Similar to traditional contract, contracting parties exist also in smart contract. The party comprises of all the people who agree to use smart contract platform to carry out an agreement **[13]**. The users who wants to engage in a contract, creates the contract and pay a transaction fee to the anonymous miners as shown in figure 6. When the conditions stated by the users are reached, the miners execute the contract code and register it on the ledger. If the contract is breached, the contract code will not be executed. Thomas and Schwartz in **[13]** underscored conversion of terms of contract to code, agreement on the code to be executed once the contract is established and execution of the agreed code in a trusted way, as the three key steps involved in creating a contract.

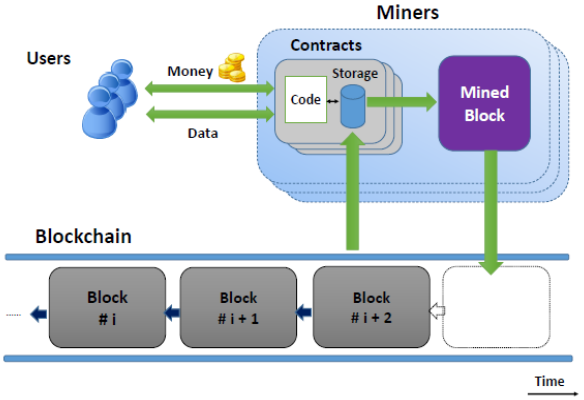

Figure 6: How a smart contract works [15]

Smart contract is a promising technology, however, as an evolving technology, it has faced serious challenges. Researchers have made tangible efforts in solving some of the problems. These problems range from verification of external data for non-deterministic smart contract systems to division and delivery of physical asset. The development of smart oracle has aided in external data verification over smart contract platform **[13] [15]**. However, later part of section 4 adumbrates smart contract issues that are yet to be solved.

4. RELATED WORKS

At the time of this writing not a lot of practical projects have been carried out on implementing smart contracts for practical uses. However, a few prototypes and pilot projects are in existence. In this section, we review some of the existing prototype and pilot implementations in existence, and identify the problems that they may have.

Smart contracts are generally implemented presently as what is called '*colored coin*'. It is an extension of bitcoin that allows assets to be stored on the bitcoin block chain. Coinprism**[20]** is one of the practical implementations of smart contracts using colored coin. Charlon, the CEO of Coinprism, gave a brief description of the implementation concepts in **[21].**Coinprism uses the Open Asset Protocol (OAP) to store and exchange assets (physical and electronic) between buyers and sellers. The position of OAP in the transaction layers is shown in figure 7 below. However, because colored coin is based on bitcoin blockchain, it inherits the problems of transaction delay due to time needed to form and confirm the transactions that would constitute a block. Also the need for a permissioned blockchain with protected identity of users (not complete anonymity) is required for most legal contracts.

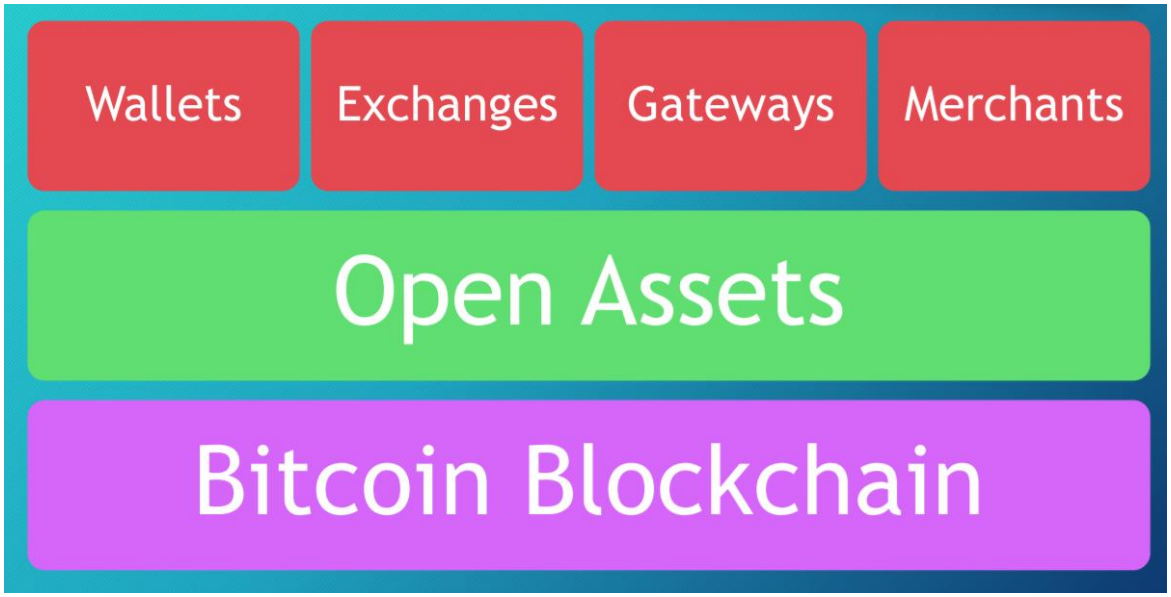

Figure 7 – OAP for implementing Smart Property [21].

OAP can be used to transfer any asset across the world at low transaction fee in a transparent but anonymous way. Coinprism provides services such as sales of stocks, currency exchange and property exchange around the world.

The next popular Smart contract implementation is Ethereum**[22]**. It is based on blockchain technology but does not use bitcoin as the cryptocurrency for executing contracts. It uses Ether, another cryptocurrency. Unlike, bitcoin blockchain, Ethereumblockchain is believed to have been designed from scratch to support Smart contracts. Hence, it has the smart property exchange protocol built right into its blockchain. There is no need for intermediate protocol layer to implement and execute smart contracts. The publication in **[22]** claims that Ethereum runs smart contracts without any downtime, censorship, fraud or third-party interference. It is also a transparent and decentralised system. The contract rules are auto-executed on the platform.

Ripples Codius from Ripple Labs in San-Francisco is another Smart contract platform in existence. It is based on the use of a ***smart oracle***, which can sign a cryptographic key whenever a condition in a contract is met **[23]**. This concept is believed to enable interoperability among the existing smart contract platforms. They also proposed an API-based programming language that will enable programming language-independent development for smart contract applications. However, it will still leverage the blockchain technology from Ripple or other blockchains but would use a cryptocurrency or fiat currency depending on the oracle. The credibility and reliability of the oracle at all times has remained an issue with this implementation

Various research projects in Universities for higher degree have produced smart contract prototypes. Hillbom and Tillstrom in **[24]** designed and implemented a simple smart contract protocol called Smart Property Ownership Exchange Protocol (SPOEP). They used a hybrid database between their local system and that of the bitcoin blockchain. The generation of smart property asset IDs and the payment for the contract was done on the bitcoin block chain. The use of bit messages was utilised for communication between Bob and Alice in executing the smart contract. However, due to limited resources, the project was not tested on real computers but android phone clients and computer server. Their local computer server was used to write and implement the rules of the contract. The problem with this project remains the huge resources in terms of computing power required to implement proof of work as is obtainable with Bitcoin and Ethereum networks.

Another proof of concept implementation of smart contract on Ethereum network is presented in Czepluch et al in **[25]**. With their coffee shop prototype, they were able to identify the strengths and weaknesses of implementing smart contracts on blockchain. The strengths include high security, low maintenance cost, trust-freeness and low cost of transactions. The weaknesses include delay for transaction confirmations, currency conversions, non-scalability and lack of regulations. However, it is believed that as the technology matures the weaknesses will fizzle out.

Though this work is about block chain technology, the concerns raised by **[25]** has called for the consideration and proposal for Transaction chain technology known as ***Openchain***. Openchain has come to increase speed and add scalability as well as closed-loop ledger where participants must first be approved by the administrator**[26]**. Those in closed-loop ledger will have more privileges. This new concept will likely solve the technical issues with blockchain however, the double deposit escrow (where monetary value equal to item offered for sale is also deposited in the escrow to reduce chance of breaching the contract), legal framework for contract breach and the problem of transfer of physical asset to new owner will still need to be solved.

Despite the solutions currently offered by both Blockchain and Openchain technologies for implementing smart contracts, lots of problems still impede the wide adoption of smart contract technologies. The following are some of these problems:

1. How would the identity of a physical asset be reliably issued and verified over the smart contract network?
2. The bitcoin blockchain is not scalable and takes long time for transaction confirmation but it has remained the largest blockchain network.
3. For physical assets, digital ownership may be easily transferred but the delivery of the physical asset

(such as car) may not be reliably transferred electronically.

4. The legal framework for arbitrations and litigations has not been clearly designed and built into most of the smart contract platform.
5. The double deposit escrow for enforcing contracts is a costly method of executing contracts and may not be possible in many cases.
6. How to verify the authenticity and integrity of the information used by smart oracles to enforce the terms of some contracts are still unknown.
7. The concept of proof-of-work is computationally expensive and may not provide much incentive for miners in the smart contract network.
8. The case of double spending in physical asset such as selling a piece of land and then a house built on the same land separately are yet to be considered.
9. There is very low level of integration between smart contracts and fiat currencies. This will hamper the adoption of smart contract platforms for some longer period of time.

Hence, in this research we propose a more realistic framework that will lead to increased adoption of smart contract platforms while solving the above problems.

5. PROPOSED FRAMEWORK

The proposed framework contains mechanisms that are intended to define, integrate and automate the set of rules that have to be met before values (monetary, services or physical assets) can be transferred from one person to another. The '***miners***' in the smart contract implementation will need to perform certain computations to prove that these set of rules and obligations have been fulfilled by the participants in the contract.

5.1 Basic Terms and Concepts

The first thing to decide about smart properties (especially for physical assets) is the issuance and divisibility of the assets. Let's assume that a piece of land of 8 plots was initially issued as a single asset. What happens when the owner wants to sell it per plot? What happens when 5-flat house is built on 5 plots and the owner wants to sell each flat and then the remaining 3 plots of land?

We propose that all divisible assets (such as Land and other divisible properties) must be of type ***root***, ***subroot***or ***leaf*** as shown in figure 8. Only leaf properties can actually be sold.

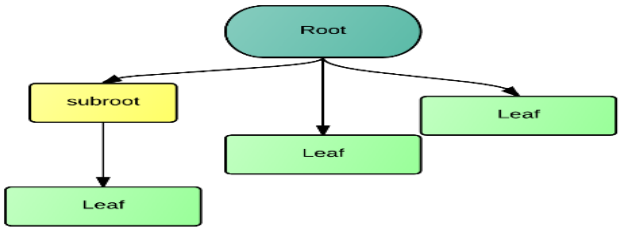

Figure 8 - Divisibility of Assets

To divide a property such as the 8-plot land into 8 plots of different identities, the original 8-plot land would be converted into a root asset, while the resulting 8 plots would get new IDs and become leaf assets. When 3-storey building is erected on say plot 1 and the owner wants to be issued with an Asset ID for the 3-story building, the plot 1 will be converted to a subroot asset and the building becomes a leaf asset with a new asset ID. If in the future the owner wants to sell the ground floor, he converts the entire house to another subroot asset and gets new asset IDs for each of the floors in the building. Hence, each asset can be infinitely divisible and only the smallest unit at a point in time (the leaf asset) can be listed to be part of a smart contract. This idea will be used to solve *'double-spending'* where a landowner lists the land separate from the house built on it as separate asset.

Every asset shall have *birthdate*, *asset ID*, *size/value* (depending on asset type) and GPS-based location (if it is a physical). The location of a physical asset should NEVER be tracked unless it enters the performance phase of a contract. The tracking shall also end when a contract is deemed completed or discharged. The ***proposed*** platform shall continue to track a physical asset if the contract it is into is deemed breached. The GPS tracking system will become an input to a Smart Oracle that will execute a certain clause/legal prose in a contract using the template defined in section figure 11 for physical assets.

Who becomes the asset ***issuing authority***? In our framework, the asset owner cannot be the issuing Authority. The issuing authority would be a government agency or the manufacturer of the item being traded on the smart contract platform. This is necessary in order to establish the authenticity of the asset which will form part of the smart contract.

5.2 3-SmartContract Model

The framework consists of three complementary but separable frameworks: Technical, Business/Economic and Legal Frameworks. These will be known as the ***Triplicate Smart Contract (3SmartContract)*** Model. The high-level design of the proposed framework is shown in figure 9. The core functionality of the framework is implemented through the Technical model. A contract can be either public (permissionless) or private (permissioned) depending on the choice of the users and the value of the transaction to be carried out. The nature of goods and services which can be made to be part of the contract is shown in figure 10. We believe that exchange of goods and services of any kind is just a contract involving the transfer of values between the client and the contractor depending on who is initiating the transaction process. Hence, the nature of the asset being transacted upon determines the procedure or the template for automating the transaction process.

While the legal framework helps to manage both statutory and platform-induced discipline for the participants, the economic/business model tries to explain how the system could be monetized and used for other economic advantages.

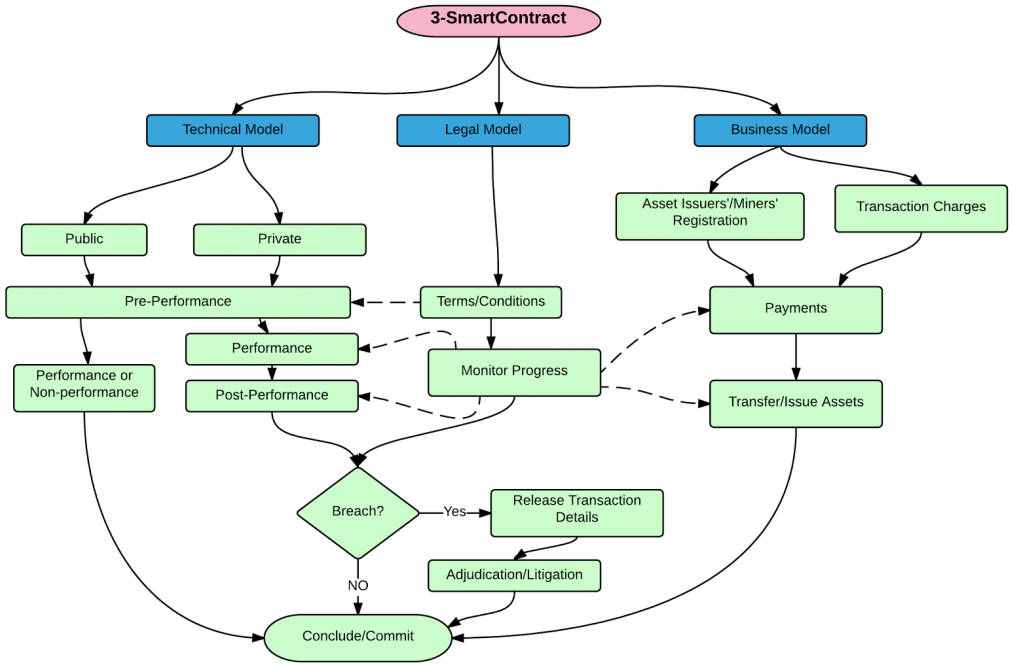

Figure 9 – High-Level Model of 3SmartContract Design

The public aspect is the same as the anonymous blockchain transactions being carried out with bitcoin transactions.

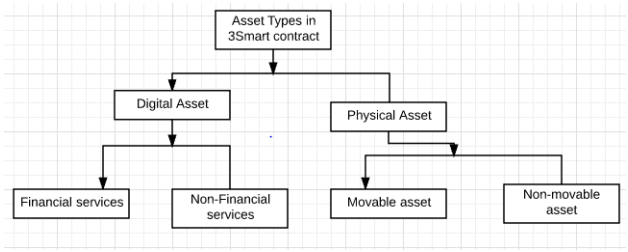

Figure 10- Asset types in 3SmartContract Design

The contract types in ***3SmartContract*** design refers to the type of assets that could take part in a contract on the platform. As shown in figure 10, the design is to handle digital and physical assets. The former is further broken down into financial services such as sales of bonds, shares etc., and non-financial services which encompass all forms of official agreed services to be rendered which has legal backing, such as an employee who opts to work for an employer for an agreed period and pay. In the physical asset design, the movable aspect handles all tangible assets which are to be conveyed from one point to another such as cars, mobile phones etc, whereas the non-movable aspect covers the tangible assets which cannot be relocated such as land and house.

5.3 Technical Model

The technical model consists of the processes that handle the preparation for, execution of and winding up of a contract. We formally divided this model into *Pre-performance*, *Performance* and *Post-performance* stages.

5.3.1 Pre-performance Stage

The pre-performance stage of the ***3SmartContract*** describes the stage of the contract where negotiation and subsequently, agreement is instantiated. It is the non-executable part of the contract which directly precedes and defines the executable part. As shown in figure 11, this stage comprises of two major part, namely: legal prose and parameters.

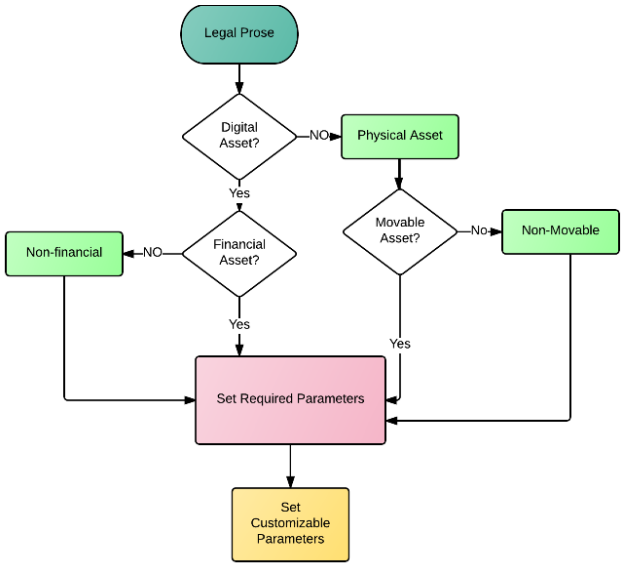

Figure 11- Pre-performance template for a 3SmartContract

The legal prose and corresponding parameters helps one to define a standard template for encoding the terms and conditions of a contract including the selling and buying of items and services. With this concept, the execution or performance stage of the contract can be more accurately carried out automatically. In general, all parameters are designed to have **key**,**value** and **threshold**. The key is the unique identifier for the parameter. The value(s) is/are the set of possible value for the parameter in that contract while the threshold helps to provide a tolerance or critical value for the given parameter. These will help the ***3SmartConttract*** engine

to make better decisions during automated smart contract execution.

5.3.1.1 Legal prose and parameters for financial assets

Legal prose: The seller and buyer should agree on the price for the asset. Thereafter, the seller and buyer is to transfer the asset and money respectively to the escrow within agreed set of time. When the escrow becomes in possession of the asset and money, it is to dispatch the money to the seller and asset to the buyer at agreed time. If one party defaults, the contract is breached and penalty abounds.

Parameters

- Asset ID(assetID,'xxx385','256 bit length')
- Asset type(assetType,'root',' existing assetID before')
- Time period for deposition of asset to the escrow ('TA', 'dd/mm/yyhh/mm/ss'', '140bit length')
- Time period for deposition of money to the escrow ('TM', 'dd/mm/yyhh/mm/ss', '140 bit length')
- Time period for the dispatch of asset and money in the escrow ('TD', 'dd/mm/yyhh/mm/ss,' '140-bit length')

Note: parameter Key, Values and Threshold are shown in the brackets above. Similar expression is applicable to the parameters of other asset types.

5.3.1.2. Legal prose and parameters for non-financial service assets.

Legal prose: The contractor and the client is to agree on specified period of time thecontractor services should last and what amount of money the client is to pay the contractor per defined time throughout the contract period. The escrow is to bein possession of the contractor ownership ID during the contract period. As long as the contractor ID remains in the escrow, the client is meant to pay an agreed amount per time to the contractor. If any party defaults, the contract is breached and legal actions can be undertaken.

Parameters

(Asset ID, Asset type, Contract start date, Contract end date, Total amount to be paid by the client, Total amount to be payed the client per defined period of time, Total amount to be paid per contract stage, Deliverables)

5.3.1.3 Legal prose and parameters for movable assets.

Legal prose: After the seller and buyer have come to a consensus on what the price should be, the buyer deposits the agreed amount to the escrow within an agreed time. Similarly, the seller is to deposit the asset ownership ID into the escrow during the agreed time. Once the escrow confirms the receipt of the asset ID, the seller releases the asset to the buyer. When the escrow confirms that the buyer is in possession of the asset, it shifts the asset ID to the buyer and the money deposited in the escrow by the buyer to the seller. Any deviation from any party is considered a breach.

Parameters

(Asset ID, Type of asset, Time period to deposit money to the escrow, Time period to deposit asset ID to the escrow, Expected time for the buyer to obtain the asset (GPS tracker time), Time period for the escrow to move ownership to buyer and money to seller).

5.3.1.4. Legal prose and parameters for non-movable assets

Legal prose: The buyer deposits money within an agreed time. After that, the seller transfers ownership ID to the escrow at the agreed time. When the escrow have confirmed the receipt of asset ID and money, it dispatches the asset ID to the buyer and money to the seller within an agreed time. If any party defaults in the agreement, it is considered a breach.

Parameters

(Asset ID, Asset type, Time period to deposit money to the escrow, Time period to deposit asset ID to the escrow, Time period for the escrow to transfer ownership to the buyer and money to the seller)

5.3.1.5. Customizable parameter

This parameter refers to both ***necessary*** and ***additional*** parameters. Necessary parameters are used for all private trusted smart contracts whereas additional parameters are optional parameters that are specific to all contract instances whether private or public in the ***3SmartContract*** system. Examples of necessary parameters includes: Name of the participant, Location of the participant, Photo of the participant, Financial history of the participant, Short biography of the participant whereas the examples of additional parameter may include: A car engine type, International Standard Organisation(ISO) certification etc.

5.3.2 Performance stage

The performance stage handles the executable part of the contract. Figure 12, shows the algorithm employed in executing various aspect of the contract. In this high level algorithm design, the financial and non-movable have similar algorithm, hence the pairing. The process for execution of the algorithm below has been defined in the legal prose above.

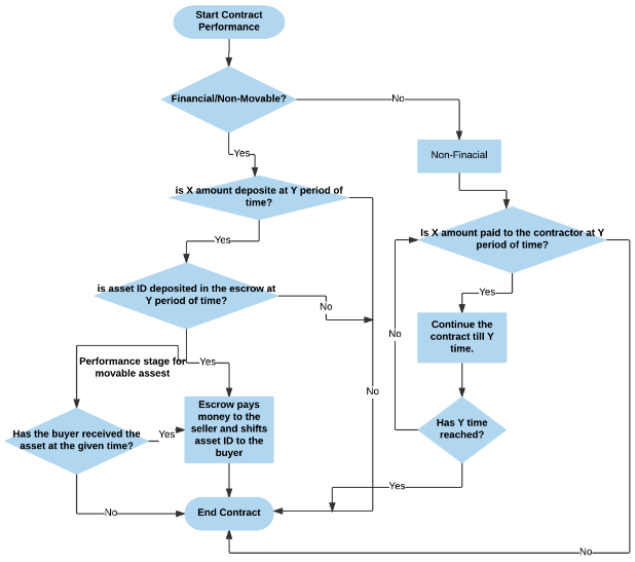

Figure-12 performance stage for 3Smart contract

Celerity in recording transactions in a blockchain is one of the present challenges confronting cryptocurrency and even smart contracts running on the blockchain platform. It is no longer news in the bitcoin world that the transaction takes far beyond 10minutes to get confirmed. This is against the theorized 10minutes which was stated in many blockchain literature. Beigel in **[27]** posits that current increase in bitcoin value had resulted to high demand of bitcoin leading to avalanche of bitcoin transactions. Thus, bitcoin participants have to wait a

little longer (usually beyond 10minutes). The ***3SmartContract*** will solve this problem by integrating the concept of fast payment in **[28]** and open chain in **[26]**.

The security for the ***3SmartContract*** will employ existing blockchain concepts such as Encryption algorithm and prevention of double spending attack. The improvement required in Smart contract is reducing the complexity of proof-of-work and using less complex but highly random generators for the Elliptic Curve Digital Signature Algorithm (ECDSA) used in blockchain transactions **[32]**.

5.4 Business/Economic Model

The continued existence of any technological solution is based on its economic viability and sustainability. Hence, it was a realist approach to integrate economic concepts into the **3SmartContract** model. The revenue from this platform will come from the following ways: Registration of **asset manufacturers**ie producers or owners of assets such as car manufacturer's, lands owners, companies selling shares etc, transaction fee for asset sales over the platform, transaction fee for asset originality verification by the **asset declarers (**miners authorized to verify second hand assets that needs to be registered to take part in a smart contract but not initially registered by its manufacturer**)**, registration of landed properties that could be traced and verified for future transactions and advertisement of trusted agents, asset issuers and manufacturers.

5.5 Legal Model

The legal model is necessary in order to build trust into the system. The statutory aspect of the legal framework is to ensure that all asset (service or physical) issuers or creators must be legal entities registered with the government or recognised bodies. Hence, traceability to issuing authority is a necessity for all assets to be traded on this platform. There are two major components of the Legal Model: ***Statutory*** and ***System-based***. The statutory aspect assumes that any transaction on the **3SmartContract** platform is a legal contract among the asset owner, the platform itself and the asset buyer. Hence, all existing national and international laws relating to execution of such contracts and trades apply. However, the pursuance of such legal entitlements must be within the legal prose and parameters explicitly defined by the transacting individuals or their legal agents within the **3SmartContract** platform. Hence, all are expected to act as law abiding citizens and with fairness.

In order to avoid litigations and prevent legal battles the system algorithm and that of the blockchain itself will help to ensure that all parties are treated fairly and that the critical items being exchanged are held in escrow until all parties are satisfied to the final exchange of ownership to take place. However, some people are bound to misbehave. This is why we introduced the system-based legal system where the **3SmartContract** can increase the credibility of a participant in the system who acts honestly and fairly by executing or providing his part of the terms in legal prose forming the contract, while reducing the credibility of defaulters. This will help customers to evaluate the history of an individual they would like to transact business with and select alternatives if necessary. The terms and conditions as mentioned in figure 8 were further broken down into legal prose and parameters for actual execution on the platform. The provision of inputs to this prose and its output will determine who needs to be rewarded or penalised. It will also provide the necessary evidence for legal actions when required.

6. DISCUSSION

We have thought out a theoretical design of a framework for reliable smart contract framework. We listed some questions in section 4 that militates against the use of existing smart contract frameworks for most existing physical and nonphysical assets. In this section, we highlight how our framework would solve the problems mentioned in Section 4.

*How would the identity of a physical asset be reliably issued and verified over the **3SmartContract** network?*

With the provision of asset manufacturers and asset declarers, assets at any point is verified and reliably issued. Asset manufacturers ensure that assets produced are registered on the ***3SmartContract***, thereby facilitating verification. Similarly, subsequent verification of any asset which had been sold previously by the asset manufacturers will be handled by the asset declarers acting as miners.

The bitcoin blockchain is not scalable and takes long time for transaction confirmation but it has remained the largest blockchain network.

This would be solved using open chain which confirms each transaction and not a block. Also the proof that double spending in block chain is increasingly becoming impossibleand zero confirmation is a reliable transaction would help as well. Also there are less difficult Elliptical curve key with less computational complexity but high randomness than those used in current blockchain digital signature [32].

F*or physical assets, digital ownership may be easily transferred but the delivery of the physical asset (such as car) cannot be handled electronically.*

GPS tracking will be incorporated into the platform. Part of the prose and parameters will include the source and destination GPS locations. A delivery agent will be part of the network. at the end of the contract, the deliverer, the receiver and the sender has to confirm on the network that the goods have been delivered successfully.

The legal framework for arbitrations and litigations has not been clearly designed and built into most of the smart contract platform

Our platform tries to prevent litigations in the first place by utilizing verified assets and also using escrow for transactions. In our platform we have a means of disciplining potential defaulters while the legal prose is meant to provide a means of gathering evidence for statutory litigations outside of the platform. (See section 5.3). The integration of the principles guiding the International Court of Arbitration (ICA) will be interesting to be explored for Smart contract Platforms.

The double deposit escrow for enforcing contracts is a costly method of executing contracts and may not be possible in many cases

Traditional double deposit escrow expects participants in a contract or transaction to deposit cryptocurrencies that are worth more than the goods or services they are using for the transaction. This means one has to have twice the value of what one wants to sell beforehand. In this framework. What is deposited to escrow is actually the cash and the asset involved. Though the challenge of non-reversible bitcoin payment is popularly known, the use of Multi-signature escrow helps to provide a 'third-party' that determines a transfer or a refund. Hence, for physical assets, both asset ID ownership and the actual amount paid to purchase the asset

will be held in escrow until the transaction is completed. This will be part of the legal prose for transaction with smart assets.

How to verify the authenticity and integrity of the information used by oracles to enforce the terms of some contracts are still unknown

Every smart oracle is as correct as its information source. In our framework, the smart decisions will mainly come from the legal prose defined by the parties in the contract and the platform-based legal prose which will be intrinsic but known to every participant. For external oracle of GPS tracking, the technology is reliable through trackers and through the trust of the shipping agents who will be made 'miners' in their own right.

The concept of proof-of-work is computationally expensive and may not provide much incentive for miners in the smart contract network.

There is yet to be a developed means of proofing the correctness of the transaction tailored specifically for the **3SmartContract** platform. While research is still on in this aspect, proof-of-stake appears to be the most effective approach but it has the problem of not being sure to solve the 51% attack.

The case of double spending in physical asset such as selling a piece of land and then a house built on the same land separately are yet to be considered.

This has been handled in our platform using the concept of root, sub-root and leaf assets. With Asset IDs generated from keys of length 128, any length of sub-classification of an asset can be achieved. However, each issued leaf asset will have to be registered in a verifiable manner on the platform.

There is very low level of integration between smart contracts and fiat currencies. This will hamper the adoption of smart contract platforms for some longer period of time.

Though this was not specifically considered in this framework, there are existing ways of using prevailing exchange rate to convert from one cryptocurrency to a fiat currency. This has become established is few advanced countries. In the United State, there are about 666bitcoin ATM/ tellers **[29]** at the time of writing. Hence, cryptocurrency Debit/Credit cards would be used for such transactions. Such APIs are evolving.

In summary, granularity of contract terms should be taken into consideration for any smart contract design. The implication of this is that more technical legal experts are needed. The technical, legal and economic aspects of a smart contract platform should be intrinsic in its implementation. For physical assets, a reliable (tracking) method of making the asset part of the execution process is necessary.

7. CONCLUSION

The **3SmartContract** was proposed in this work. The fundamental approach is to integrate physical and nonphysical assets into a contract platform that automates the technical, business and legal aspects of a contract from initiation to completion. The realities and constraints existing in traditional contracts was put into consideration and solved using a top-down design approach.

For better operation of the proposed **3SmartContract**, some existing smart contract concepts such as open chain, proof of double spending attack and bitcoin ATM were integrated into the platform making it more efficient. More concise definition of the terms of contract using legal prose, parameters and parameter thresholds were introduced to ensure granularity and preciseness of contract terms in order to ensure it can be coded and executed by a computer program.

Our future work will focus more on development of a standardized, more effective and less expensive means of computing the correctness of each transaction in **3SmartContract**. Also, most of the theoretical concept developed in this white paper would be implemented so as to prove its validity. In addition, the scope of our future work will encapsulate further research in smart oracle alongside with investigation, development and implementation of fiat-currency payment system in a smart contract platform.

8. REFERENCES

[1] M. Crosby, Nachiappan, P. Pattanayak, S. Verma and V. Kalyanaraman. Block Chain Technology: Beyond Bitcoin. Sutardja Center for Entrepreneurship & Technology, University of California Berkeley, October 16, 2015.

[2] How the 'Blockchain' might disrupt the banking & financial industries. By Matthew Lim on September 28, 2016. http://fifthperson.com/how-the-blockchain-might-disrupt-the-banking-financial-industries/ retrieved 15th December, 2016

[3] S. Apte, N.petrovsky. "Will blockchain technology revolutionize excipient supply chain management?" Journal of Excipient and Food chemicals," Vol. 7, pp. 1-3, sept.2016.

[4] M. Chinaka., "Blockchain technology-applications in improving financial inclusion in developing economies. Case study for small scale agriculture in Africa". June 2016. https://dspace.mit.edu/bitstream/handle/1721.1/104542/958426765-MIT.pdf?sequence=1 [Retrieved Dec 24, 2016].

[5] J. Czepluch, N. lollike, S. Malone. "The use of blockchain technology in different application domains". May 2015. http://www.lollike.org/bachelor.pdf [Retrieved Dec 22, 2016].

[6] M. Pilkington. "Blockchain Technology: Principle and applications", Research handbook on digital transformational. September, 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660 [Retrieved Dec 27,2016]

[7] K. Heires. "The risk and rewards of blockchain technology." Forefront (March, 2016), pp.1-3.

[8] LearnCryptography.com. "51% Attack". https://learncryptography.com/cryptocurrency/51-attack [Retrieve Dec 31,2016]

[9] J. Garay, A. Kiayias, N. Leonardos. "The bitcoin backbone Protocol:Analysis and applications." April 2015. Vol 9057, pp.4-6. http://courses.cs.washington.edu/courses/cse454/15wi/papers/bitcoin-765.pdf [Retrieved Dec 27, 2016]

[10] E. Wall, G. Malm. "Using blockchain technology as smart contract to create a distributed securities depository" M.SC thesis, Lund University, Sweden, 2016

[11] U.S. Securities and Exchange Commission. "SEC Approves Overstock.com S-3 filing to issue shares using bitcoin blockchain." December, 2015.

https://www.sec.gov/Archives/edgar/data/1130713/000110465915084240/a15-9206_9fwp.htm [Retrieved Dec 28, 2016]

[12] R. Brown, J. Carlyle, I. Grigg, M. Heam. "Corda: An introduction." Sept 2015. https://www.researchgate.net/publication/308636477_Corda_An_Introduction [Retrieved Dec 25, 2016]

[13] S.Thomas and E.Schwartz. (2014, July). "Smart Oracle: A simple, powerful approach to smart contracts" July 2014. https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts [Retrieved Jan 1, 2017]

[14] C. Clack, V. Bakshi, L.Braine, "Smart contract template: foundations, design landscape and research directions." Aug 2016. https://arxiv.org/pdf/1608.00771.pdf [Jan 1, 2017]

[15] G. Green, "Why many smart contract use cases are simply impossible." Apr 2016. http://www.coindesk.com/three-smart-contract-misconceptions/ [Retrieved Jan 10, 2017]

[16] R. Wells, E. Ditmite. "Nasdaq and chain to partner on blockchain technology initiative" June 2015 http://ir.nasdaq.com/releasedetail.cfm?releaseid=919287 [Retrieved Jan 7, 2017]

[17] M. long, "Santander becomes the first U.K bank to use ripple for cross-border payment" May 2016. https://ripple.com/insights/santander-becomes-first-uk-bank-use-ripple-cross-border-payments/ [Retrieved Jan 4, 2017]

[18] K. Delmolino, M. Arnett, A. Kosba, A. Miller, E. Shi. "Step by step towards creating a safe smart contract: insight from crypto currency lab" Nov 2015. http://eprint.iacr.org/2015/460.pdf [Retrieved Jan 2, 2017].

[19] Adriano, Andreas, and Hunter Monroe. "The internet of trust: created to avoid banks, bitcoin's blockchain technology may end up helping them." Finance & Development, June 2016, p. 44+. Academic OneFile, elibraryusa.state.gov/primo?url=http://go.galegroup.com/ps/i.do?p=AONE&sw=w&u=wash89460&v=2.1&id=GALE%7CA454943110&it=r&asid=a31bb7c8af2fcb8eb35fb9adb8ffd8de. Accessed 21 Dec. 2016.

[20] Coinprism https://www.coinprism.com/

[21] F. Charlon. Colored coins in Practice.CoinPrism, 2014. https://le-coin-coin.fr/wp-content/uploads/2014/11/Day2_0945_Charlon.pdf [Retrieved Jan 12, 2017].

[22] Ethereum Foundation https://www.ethereum.org/

[23] D. Cawrey. "Ripple Labs Unveils Proposal for New Smart Contract System" In CoinDesk, July 21, 2014.

[24] E. Hillbom and T. Tillstrom. Applications of Smart-contracts and smart property utilizing blockchains. Masters of Science Thesis in Computer Science, Chalmers University of Technology and University of Gothenburg, Sweden. Febuary, 2016.

[25] J.C Czepluch, Z. Lollike and S.O Malone. The Use of Block Chain Technology in Different Application Domains. Bachelor Project in Software Development, the IT University of Copenhagen. 20th May, 2015.

[26] F. Charlon. OpenChain Documentation: Release 0.7.0. December 18, 2016.

[27] O. Beigel. (2016, June), "Why is my bitcoin trasaction pending for so long?- Bitcoin fees for dummies."https://99bitcoins.com/why-bitcoin-transaction-pending-bitcoin-fees/ [Feb 6, 2017]

[28] Tobias Bamert et al. Have a Snack, Pay with Bitcoins http://www.tik.ee.ethz.ch/file/848064fa2e80f88a57aef43d7d5956c6/P2P2013_093.pdf

[29] Bitcoin ATMs in United States https://coinatmradar.com/country/226/bitcoin-atm-united-states/ .Retrieved 4th March, 2017

[30] Swanson, T., Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems. Working paper. 6 April 2015. Retrieved from http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributedledgers.pdf

[31] Understanding the blockchain By William Mougayar January 16, 2015 https://www.oreilly.com/ideas/understanding-the-blockchain [Retrieved 20th march 2017]

[32] H. Mayer. "ECDSA Security in Bitcoin and Ethereum: A Research Survey". CoinFaabrik, June 28, 2016.