Periodicals of Engineering and Natural Sciences ISSN 2303-4521
Vol. 7, No. 3, September 2019, pp.1021-1029
Available online at: http://pen.ius.edu.ba

Implementation of national cryptocurrency using ethereum development platform

Hussain Ali Mutar[1], Muayed S. AL-Huseiny[2]
[1,2]Electrical Department, College of Engineering, Wasit University, Iraq

Article Info

Received Feb 09, 2019

Keyword:

Implementation
National Cryptocurrency
Ethereum
Development Platform

ABSTRACT

While Ethereum run in public networks which make the blockchain size large and transaction run time longer than time for private or national network, that led to continuous worries over the expanding size of Ethereum Blockchain, which certainly reduce Cryptocurrency's effectiveness. The estimations were on increase and believed it would cross the node limit of 1 TB terribly shortly. If new consumer a full node enters to that blockchain and cryptocurrency world, a node is a computer software cum database of the blockchain, which a full node client must download on their personal computers to become a full node in the blockchain. in this way, the client can be verifying transaction on the network with the help of other nodes on the system. We proposed to implement national cryptocurrency which developed using Ethereum as a development platform that could serve national or regional people that has limited or slow internet connections like Iraq, in addition payments in countries with unstable fiat currencies, although cryptocurrencies are suffering from unstable exchange rates against fiat currencies, the use of national cryptocurrency instead of the native fiat cash could even be a far better alternative for individuals in certain countries like Iraq, Iran and Syria, with high rate of inflation. The reminder of this paper is arranging as following: an introduction, the advantages and drawbacks of cryptocurrencies, Background on Blockchain and Ethereum, implementation, results and conclusion.

Corresponding Author:

Hussain Ali Mutar
Electrical Department, College of Engineering, Wasit University, Iraq
Email: hmutar@uowasit.edu.iq

1. Introduction

By the arrival of Bitcoin by Satoshi Nakamoto' in 2009 [1] a different scoops of blockchain platform has developed. The blockchain developers seek after a shared objective, to be in charge of specific asset of specific decentralizing application. They accomplish this by replacement of confidence in centric structure by a great network of untrusted elements who endeavor to achieve consensus of the right history of the transactions. The trust is gotten by means of the assumption by most of these hubs demonstration loyally and regard the blockchain protocol, so as to verify the task of the blockchain all in all. The asset of Bitcoin's is its cryptocurrency, with trust in decentralized structure to supplant of classical banks. Present day blockchains, for instance, Ethereum go above and beyond. The last plans to decentralize the computer all in all by using of Ethereum Virtual Machine (EVM) [2],which engages the disseminated process of projects, as purported smart contracts, conveyed on the Ethereum platform. The EVMs are stack-based virtual machines which underpins a guidance group of 134 operation codes (opcodes) so as to have the capacity to implement the Turing-complete projects. Smart contract capacities are conjured through exchanges. Every activity on EVM take fees as specific amount of gas. At the point when the aggregate sum of gas doled out to an exchange is surpassed, program rendering is ended, and its belongings returned. the gas amount is determined by ether, designers are propelled to compose effective projects to retain exchange fees low and to maintain a strategic distance from unbounded circles on the EVM. Engineers for the most part compose the cod of the smart contract in a state language which aggregates into EVM bytecode. Albeit different exploratory variant of abnormal state dialects existing, at the time of the comparison, Solidity [3] is the widely pervasive programming language to create smart contracts. By the first impression, the JavaScript/C-like sentence structure of Solidity appearance comfortable to designers with involvement in C or JavaScript and supports quick improvement of the smart contracts. However, the manner of smart contracts processed, just as their security properties, are generally different from traditional programs and might prompt to unforeseen behavior during execution. In addition, the lack of strain static consent and shortage of support of development kit, developers are urged to change the code of smart contract till it "just works". although this would be a workable methodology for prototype, its potential outcomes in deadly errors when deploying the smart contracts as real decentralized applications (DApps), on the open Ethereum blockchain. As opposed to classical programs, when writing to a blockchain, they can’t be modified longer. The unexpected transactions by the developer are unchangeable.

In Sept 2018 the market evaluation of the well observable virtual assets (“tokens”) of the Ethereum platform amounts to US$ 35 billion, not count the US$ 17.5 billion of ether, the platform’s hardwired cryptocurrency[4].

Cryptocurrencies are a kind of digital currencies that are counting on cryptographically verifications of transactions. Cryptocurrencies possess three features ensuring limited anonymity, no central authority need (independence) and protection from double spending attack. As stated by Jan Lansky, the system of the cryptocurrency satisfy 6 terms [5]:

- A system that doesn’t need a centric controller; its status is preserved by distributed ledger.
- The system holds a summary of digital money units and their possession.
- The system set where or not to create new units of the cryptocurrency. within the event that new units of cryptocurrency created, the system circumstances the conditions of their source and the way to decide their possession.
- possession for units will be well-tried only by cryptography.
- The system permits exchanges to be completed within responsibility for units of cryptocurrency is modified. A transaction statement should be release by an element demonstrating the present possession for units.
- If two distinct instructions try to change the possession of the same units of cryptocurrency are concurrently entered, the framework performs at the most one among them.

Advantages

- Open source code for process of mining cryptocurrency – Ethereum used similar calculations that are utilized in web based bank services.
- No inflation –Most extreme digit of coins is carefully constrained by 100 million in Ethereum. .
- Peer to peer cryptocurrency system – this system has no central controller, that is chargeable for each function.
- Unlimited potentialities of transaction – every wallet holder can pay to anyone, anyplace and any amount.
- No confines. Payments created during Ethereum are not possible to withdraw. The cryptocurrency units can’t be forged, copied or spend doubly.
- Low cost Ethereum operation. The Ethereum cryptocurrency acts as classical money, in addition to the features of e-trading.
- Decentralization. the system has no centric management controller within the system, it possesses distributed network to entire entrants, every pc mining Ethereum is a part of this network.
- Simple to use. With taking into consideration that the steps of creating an account, the corporate in Iraq banks is complicated and may be rejected while not clarification, implementing Ethereum is convenient for corporations. The corporate take about five minutes to make a Ethereum wallet and instantly starting use it with no more inquiries and taxes.

- Anonymity. It’s totally anonymous and absolutely transparent.
- Transaction speed. the flexibility to transfer money anyplace and anyone within a short time when the Ethereum system perform the transaction.

Drawbacks of cryptocurrencies

According to [6] the disadvantages are as follows [7]:

- robust volatility – unsteady of the Ethereum price rely directly on the announced report from different country’s authorities.
- massive hazards of investment in cryptocurrencies that ought to thought-about at present time and future.

The disadvantages of cryptocurrencies are significantly more, and are linked with money laundry, terrorist and other illicit action financing, absence of centric controller, implies that there is no legitimate formal agent to assurance in the event of bankruptcy, and corresponding. However, though it’s very hard to anticipate, many studies about this topic claiming that the future of cryptocurrencies is shining because it will take off trade barriers and intermediaries, it would reduce the fees of transactions, and thus raise the economy and the trading. and so on, though, it must be think about pessimistic sounds in the academic filed as well, proposing that the high hazards of volatility, hacking hazards, and limited of institutional support led to some suspicions for the future of cryptocurrencies [8]

2. Background on blockchain and ethereum

Blockchain are often as an open (to the public) decentralized databases in which replication distribute cross many nodes at the same time [9]. In Blockchain there's no authority responsible of overseeing and keeping up the record of transactions. The ledger’s version validity is determined by a consensus method among the collateral nodes. the utilization of blockchain technology permits a secure validation of transaction’s information integrity. Bitcoin, for instance, that is that the first application developed over blockchain by Satoshi Nakamoto [1]. On another side Ethereum blockchain is open source, decentralized and distributed computing infrastructure which process programs called smart contracts [10]. it's developed to empower decentralization application programs and just not for a cryptocurrency, which is made by using a virtual machine (Ethereum Virtual Machine, EVM) to process a scripting language. in contrast to Bitcoin during which that alone Boolean analysis of paying conditions are in concerning, EVM is by some means is the same as a general pc that simulates what an informatics system will process. Modifying the contract status in the blockchain wants transaction fees that are estimated in Ether. Ether is taken into thought because the fuel for operative the decentralized application. for that, Ethereum is presently the second worthiest cryptocurrency that features a market capability around 68 billion dollars till May 2018, and numerous cryptocurrencies are merge smart contracts. Ethereum accounts can be classified into two types:

1. Externally owned Accounts (EOA): this account known by the wallet address and managed by a personal key. The owner of this personal key can exchange cryptocurrency and make signature of transaction from this account. EAO is consider user kind account and it is joined to special cryptographical keys pair, created according to account generation. the public one is utilized to point to the account, additionally referred to as EOA address while the personal key on the opposite side uses to sign transaction prior to any execution of transactions on the system to evidence legitimacy. EOA possesses balance that store cryptocurrency [11].
2. Smart Contract: the smart contract is an account that's managed by itself [12]. it's considered like an independent client processed using EVM and is the core basis and also the main structure of any DApp [13].as the code deploy to the blockchain, the EVM can ensure that it will continue working, because of the terms enforce. It is necessary to notice as the smart contracts deploy to the blockchain system, they will be publicly visited and seen using associated addresses, transactions (timestamp, to_address, from_address, etc..). calling functions from a smart contract is available to any account whenever the following conditions are obtaining:
    a. known address of each smart contract.
    b. The caller function possesses enough balance to trigger. Additional value gives by the smart contracts, the code governing the business logic is presently in public (easily verifiable) and not mysterious as in typical server.

3. Proposed system and implementation

To implement national cryptocurrency, the following development tools are used:

1- Solidity, which is a novel programing language native to Ethereum, the second largest cryptocurrency by market capitalisation, released free in 2015. Ethereum isn't solely a cryptocurrency capable of storing price or creating payments, however a completely fully development platform for making what’s referred to as a smart contract.

For all intents and functions, a smart contract is a programmable written agreement of kinds, an independent middleman or a good decide capable of managing a financial transaction between varied parties and autonomously arbitrating a dispute.

2- Truffle is developing environs, framework test and asset pipelines for Ethereum, target to turn out the Ethereum developing process easy. Truffle has the following features:

- Compiling smart contracts, link up, binary management and deployment.
- Fast development by automated contracts testing.
- Scriptable, extensible and deployment.
- Migrations framework, extensible deployment and scriptable.
- Managing network to deploy any number of private and public networks.
- software management with Ethereum package manager (EthPM) and Node Package Manager(NPM), using the ERC190 standard.
- interacting console for straight contract communication.
- Build conformation pipeline with support for tight integral.
- Capable to run external script which executes scripts among Truffle environment.

3- Ganache is a personal blockchain that allows developers to create smart contracts, decentralized application (DApps), and test software that is available as a desktop application and command-line tool for Windows, Mac, and Linux[14].

4- MetaMask is an internet browser extension which permits you to access distribute web in internet browser. It permits user to execute Ethereum distributed application within internet browser while not operating an Ethereum full node[15]. MetaMask implies a secure identity vault, came up with an interface to handle user identification on diverse sites and sign transactions before sent it to blockchain. MetaMask additionally allows users produce and administer their identification (through private key, local consumer wallet and hardware wallets, therefore once a distributed platform application needs to execute a transaction and transfer it to the blockchain, the consumer got a safe interface to check the transaction, before approved or rejected it.

5- Geth: The go-Ethereum client is usually named as geth, that is the instruction line interface for operating an Ethereum full node carry out by Go. By installing and running geth, you'll be able to participate within the Ethereum frontier live network and:

- mine ether
- exchange funds among addresses
- make contracts and send exchanges
- investigate block history

The overall implementation of the system is shown in figure 2.

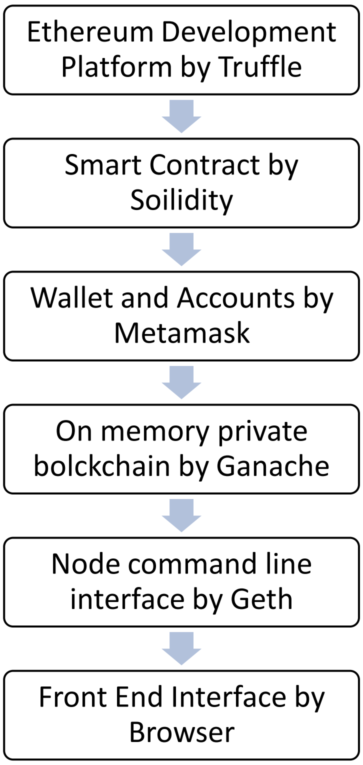

Ethereum Development Platform by Truffle
Smart Contract by Soilidity
Wallet and Accounts by Metamask
On memory private bolckchain by Ganache
Node command line interface by Geth
Front End Interface by Browser

Figure 1.Block diagram for the system during the development process

Smart Contract: is simply a line of code that is running on Ethereum. It's referred to as a "contract" as a result of code that runs on Ethereum will control valuable things like ETH or other digital assets.
The project consist of the following drectories and files as shown in fig.3

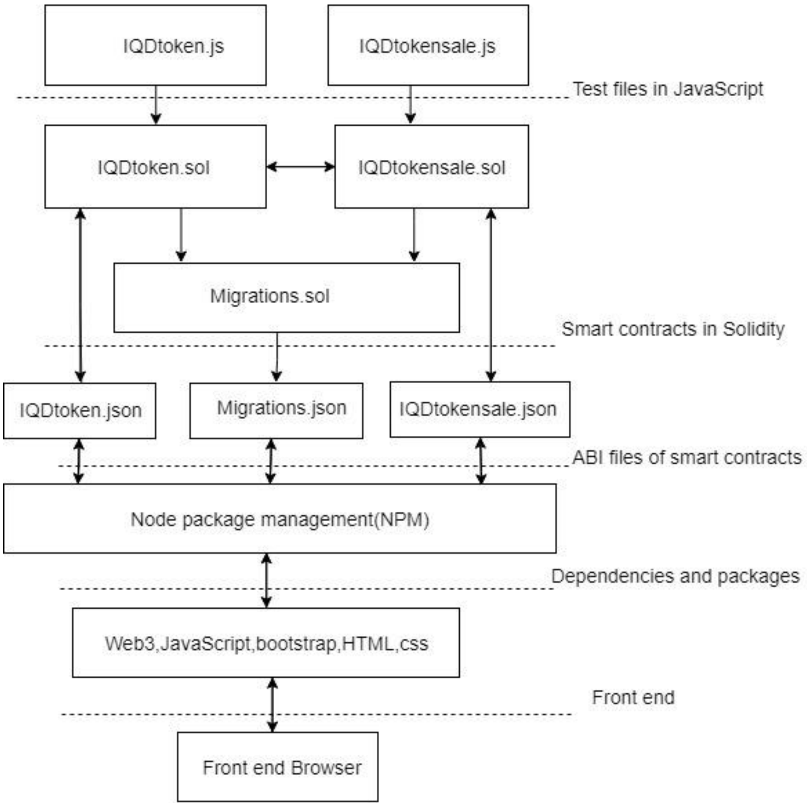


Figure 2.Directories and files of the proposed system

1- Contract directory: it's include tow smart contracts of the project that perform the core operation of the system and the contracts are:
   a. IQDtoken.sol: this is the basic and the most important contract which include the genisis parameters for the cryptocurrency and it inchage of write to and form the blockchain.this file determind the behavious of the cryptocurrency and most be implemented according to ERC-20 standerd,so it include:
      i. Name of the cryptocurrency which is "IQDtoken".
      ii. Symble of the cryptocurrency which is "IQD".
      iii. Standerd of the version of the system which is "v1.0"
      iv. TotalSupply of the system which is "1,000,000".
      v. It must be allow for transfer token from address to another.
      vi. It most be allow for transferFrom fuctionality in case of transfer on pehave of another account according to approval and within allowence.
   b. IQDtokensale.sol: this contract govern the IQD token during initial coin offering (ICO),and it possess the following functionality:
      i. Provision token to token sale contract.
      ii. Set the price of token in Wei.
      iii. Make sure that the contract has enugh tokens.
      iv. Assign an admin whom control the ICO.
      v. Keep track of token sold during ICO.
      vi. Transfer remining IQDtoken to admin befor ending ICO.
      vii. End the sale of ICO.

   c. Migrations.sol :Solidity file that helps in the deployment process.

2- Migrations directory :it include migration fileswritin in java script that handle the migration whenever deploying smart contract to the blockchain,that will change the state of blockchain and transaction is created,those file possess the following functionality:
   a. Migrates smart contract to blockchain whenever deploying the smart contracts.
   b. Initialized the system with one milion money.
   c. Set token price in wei.

3- Test directory: this is essential part of the project that include the test files. since the smart contract are immutable whenever it deploy to blockchain it cant't be modifyed,so it vital to write testing file and execute them during the development process to make sure there is no inexcpected behavious of smart contracts.the system has two test files :
   a. IQDtoken.js: this is jave script file perfome testing operatoin on IQDtoken.sol smart contract file according to ERC-20 standerd and check its functionality as bellow :
      i. Initialized the contract with the correcte values:
         1. Has the correcte Name.
         2. Has the correcte symble.
         3. Has the correcte standerd.
      ii. Allocalte the total supply upon deployment:
         1. Set the totalSupply to 1,000,000.
         2. It allocate the initial supply to admin accounts.
      iii. Transfers token wonership:
         1. Chack the balance.
         2. Log the account that the token tranfer from.
         3. Log the account that the token transfer to.
         4. Log the transfer amount.
         5. Add the amount to the reciving account.
         6. Deducts the ammount from the sending account.
      iv. Approve token from delegate transfer:

1. Shuold be approved.
2. Log the account that the token tranfer from.
3. Log the account that the token transfer to.
4. Log the transfer amount.
5. Store the allowance for Delegate transfer.

v. Handles delegated token transfers:
1. Check balance
2. Ckeck the approval
3. Check the allowance.
4. Log the account that the token tranfer from.
5. Log the account that the token transfer to.
6. Log the transfer amount.
7. Add the amount to the reciving account.
8. Deducts the ammount from the sending account.

b. IQDtokensale.js: A java script file that test the IQDtokensale smart contract functionality as bellow:

i. Initialized the contract with the correcte values:
1. Has contract address.
2. Has token contract address.
3. Token price is correcte.

ii. facilitates tokens buying:
1. Should be the "Sell" event.
2. Log the account that purchased the token.
3. Log the number of tokens purchased.
4. Increment the number of token sold.
5. Check the contract has enugh tokens.

iii. Ends token sale:
1. Must be admin to end the Sale.
2. Returns all unsold IQD tokens to admin.
3. Reset token price.

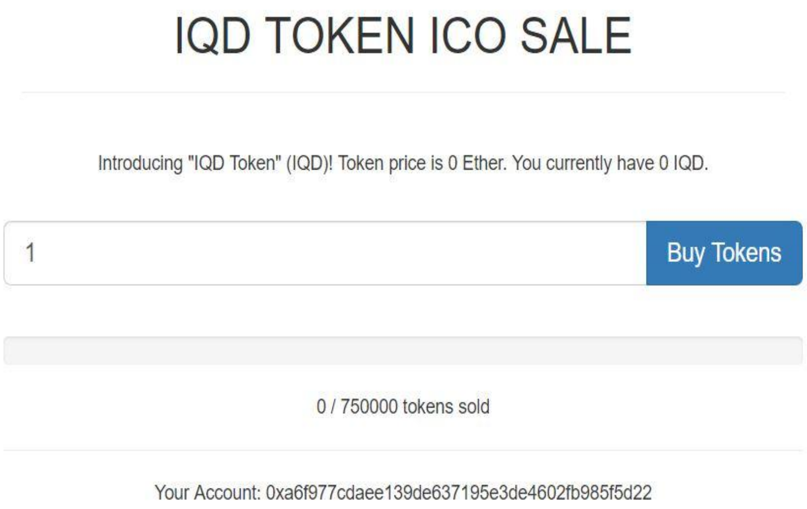
c. Build directory : The standered output directory for compiling smart contract which include contracts sub-directory that include the json files of the smart contracts in abi bytecode. These artifacts are fundamental to the internal activities of Truffle, and has an significant role in the fruitful deployment of the system.

d. truffle-config.js: configration file that configure the project. It's seeded with settings for different networks and indicates the accessible network for deployment throughout migration, additionally as certain transaction factors once interactive with every network (like gas cost, from _address, and so forth). once compile and run migration on a selected network, contract artifacts are store and record for later use. once the contract abstraction find the specific Ethereum consumer is connect to the network, they will use the contract artifacts related with this network to facilitate system deployments.

4. Results

The result of our proposed system is the successful implementation of the project. The experiment is based on an Intel Core i7 2.80 GHz processor with 16 GB of RAM, the smart contracts implemented by Solidity programing language. and all the functionality of the system was test by two methods:

1. Using in on memory local blockchain development tool” Ganache” with MetaMask google chrome extinction and successfully buy and selling tokens among different address with successful transactions with custom gas fees as showing in images bellow:
2. Using GoEthereum (geth) with Rinkeby testing network [16] and successfully work on that testing network using the front end of the project.



IQD TOKEN ICO SALE

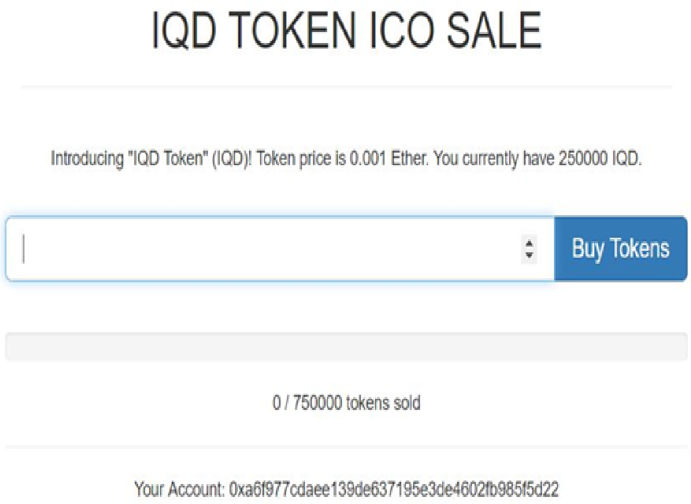
Introducing "IQD Token" (IQD)! Token price is 0 Ether. You currently have 0 IQD.

1

0 / 750000 tokens sold

Your Account: 0xa6f977cdaee139de637195e3de4602fb985f5d22

Figure 3. Initialized Admin account with zero balance



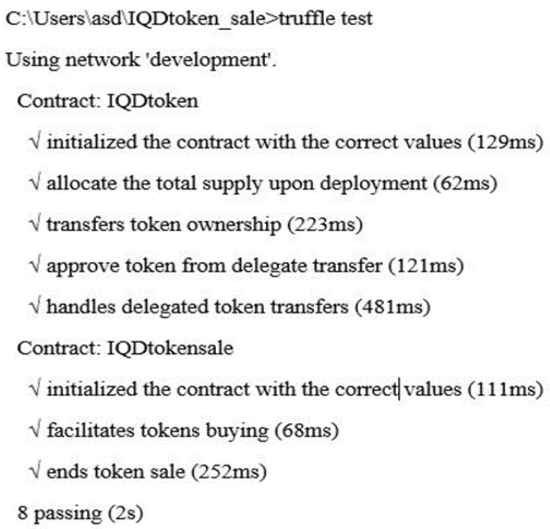
IQD TOKEN ICO SALE

Introducing "IQD Token" (IQD)! Token price is 0.001 Ether. You currently have 250000 IQD.

0 / 750000 tokens sold

Your Account: 0xa6f977cdaee139de637195e3de4602fb985f5d22

Figure 4. Add total supply of one million to admin account



```
C:\Users\asd\IQDtoken_sale>truffle test
Using network 'development'.
  Contract: IQDtoken
    √ initialized the contract with the correct values (129ms)
    √ allocate the total supply upon deployment (62ms)
    √ transfers token ownership (223ms)
    √ approve token from delegate transfer (121ms)
    √ handles delegated token transfers (481ms)
  Contract: IQDtokensale
    √ initialized the contract with the correct values (111ms)
    √ facilitates tokens buying (68ms)
    √ ends token sale (252ms)
  8 passing (2s)
```

Figure 5.Transfer 750,000 token to IQDtokensale for ICO in order to sell the balance

5. Conclusion

implementing national cryptocurrency using Ethereum as a development platform that has smaller blockchain size and smaller transaction time than the original Ethereum public cryptocurrency in addition to the ability to customized the geneses file parameter which cannot be done in public Ethereum Network, by this implementation we have full control over the cryptocurrency during the development process and before the initial coin offer(ICO), Compatible with IRC-20 standard cryptocurrency could have a name, version, initial coin balance, gas limit and gas fess.

References:

[1] Nakamoto, S., Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Wood, G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014. 151.

[3] Solidity. Solidity 0.4.24 documentation. Retrieved June 9, 2018 from. 2018; Available from: http://solidity.readthedocs.io/en/v0.4.24/.

[4] ERC-20 Token Standard. 5 Sept 2018]; Available from: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md.

[5] Lansky, J., Possible State Approaches to Cryptocurrencies. JOURNAL OF SYSTEMS INTEGRATION, 2018.

[6] Ivaschenko, A.I., Using Cryptocurrency in the Activities of Ukrainian Small and Medium Enterprises in order to Improve their Investment Attractiveness. Problems of economy, 2016.

[7] Tymoigne, Do Cryptocurrencies Such as Bitcoin Have a Future? No: As a Currency, Bitcoin Violates All The Rules of Finance. Wall street journal 2015. Eastern edition, 265(49), p. 1-2.

[8] Vora, G., Cryptocurrencies: Are Disruptive Financial Innovations Here? Modern Economy, 2015, 6, 816-832, 2015.

[9] J. Yli-Huumo, D.K., S. Choi, S. Park, and K. Smolander, is current research on blockchain technology? a systematic review. PloS one, 2016. 11(10): p. e0163477.

[10] al., V.B.e., A next-generation smart contract and decentralized application platform. 2014(white paper).

[11] Wood, G., Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, 2014. vol. 151: p. 1–32.

[12] K. Delmolino, M.A., A. Kosba, A. Miller, and E. Shi, Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab. in International Conference on Financial Cryptography and Data Security.Springer, 2016: p. 79–94.

[13] Pilkington, M., 11 blockchain technology: principles and applications,”. Research handbook on digital transformations, 2016: p. 225.

[14] Truffle. Ganache. 2019; Available from: https://truffleframework.com/.

[15] MetaMask. MetaMask 2019; Available from: https://metamask.io/.

[16] rinkeby. rinkeby:Ethereum Testnet. 2019; Available from: https://www.rinkeby.io/#stats.

[17] Barazanchi, I. Al, Shibghatullah, A.S., and Selamat, S.R., 2017. A New Routing Protocols for Reducing Path Loss in Wireless Body Area Network (WBAN). Journal of Telecommunication, Electronic and Computer Engineering model, 9 (1), pp.1–5.

[18] Abdulshaheed, H.R., Binti, S.A., and Sadiq, I.I., 2018. A Review on Smart Solutions Based-On Cloud Computing and Wireless Sensing. International Journal of Pure and Applied Mathematics, 119 (18), pp.461–486.

[19] B. Durakovic, "Design of Experiments Application, Concepts, Examples: State of the Art," Periodicals of Engineering and Natural Scinces, vol. 5, no. 3, p. 421–439, 2017.