International Journal of Advanced Trends in Computer Science and Engineering

Blockchain Technology for Managing land Titles in Nigeria

Obamehinti Adeolu Seun[1], Touraj Khodadadi[2], Sellappan Palaniappan[3]

[1,2,3]Department of Information Technology, School of Science and Engineering, Malaysia University of Science and Technology, Selangor, Malaysia,

[1]lebiobamehinti@gmail.com, [2]touraj@must.edu.my, [3]sell@must.edu.my

ABSTRACT

Blockchain is a trending technology that has paved way to solving various challenges in different sectors. It has received much interest from researchers over the years, as it is known to be a transparent, secured, no third party and tamper-proof public records repository system for documents, contracts, properties and assets. land title as being a major challenge in Nigeria due to the fact the existing traditional system, used to manage the sector is not effective, thus brought about issues such as, double spending, tamper, third party interference, it is not transparent. Hence the need for blockchain technology. The methodology considered for this research is ethereum blockchain with smart contract which is written in solidity programming language. The research clearly shows the result of using ethereum blockchain to manage land title and how the challenges of land title has been solved. This paper examines Blockchain Smart Contract for managing land titles in Nigeria. Specifically, it presents a detailed smart contract for land title and transfer between owner (government) and buyer.

Key words: Blockchain, Smart Contract, Ethereum, Solidity, Landtransaction, Land title.

1. INTRODUCTION

Researchers have shown much interest in Blockchain cryptocurrency transaction in the past years. However, ethereum blockchain has not been considered much, it still new in the research stream as it was introduced in 2015. It has therefore proven to be a technology that has a solution to various challenges in our everyday sector management. This research indicates the methodology, result and discussion of a tested ethereum Blockchain technology, where smart contract is the executable rules written in the blockchain to guide every land transaction in the blockchain, in other to avoid double spending, third party interference, tamper and it also provide a decentralized application where every participant is a decision making body in the system.

Blockchain is a novel, disruptive technology. Blockchain technology is a type of technology that is tamperproof, clear, secure, and highly immutable, [3], [10]. With Blockchain, domains and sectors like finance, Education and real estate can perform their business transactions more effectively and efficiently.

In Nigeria, land title management has posed as a major challenge to the economy and wellbeing of the populace, the present system used which is the national archives has not paid off in terms of proper management, [2]. Through this Centralized system, which is controlled by an individual, gave rise to double spending, third party interference, tamper with, it does not provide a secured system for land title, and records are lost over time [14].

Land titles are expected to be overseen by the government, with the proposed ethereum blockchain technology this would solve these challenges as its major characteristics are transparency, secured tamper resistant, anonymous, also serve as a database for keeping public record. Hence to meet the world class standard on how the said sector is properly managed.

This paper indicates the methodology, result and discussion of ethereum Blockchain Smart contract for managing land titles. Section 1 discusses introduction to Blockchain technology. Section 2 discusses related works. Section 3 discusses the methodology adopted. Section 4 indicates result and discussion of the proposed system. Section 5 concludes the paper.

1.1 Research Goal and Questions

The purpose of this research is to show how ethereum blockchain technology with smart contract can be used to manage land title. To perform transaction between two anonymous parties who do not trust each other and also need no third party for the transaction. A proof of work concept mechanism is used for the smart contract land title management application. The research goal is broken down into three research questions:

1. Research question one: what are the challenges of existing technology presently used to manage land title in Nigeria?

   To provide an answer to this question a literature review on existing work and related technology on blockchain technology is carried out and a comparison between the existing technology and the proposed technology is made to indicate the strength of the proposed technology over the existing technology.

2. Research question two: how can blockchain technology, architecture, be used for public database, tamperproof, to

perform a secured transaction between two people who doesn't need to trust one another without the interference of third party?

To answer this question, a proposed methodology, ethereum smart contract is use which serve as executable rule that guide every transaction in the blockchain network, to make it immutable, anonymous, and secured and tamperproof.

3. Research question three: how can the proposed blockchain technology be tested to ascertain that it has provided solutions to the challenges on land title in Nigeria?

To answer this question, a Rospten test network is use to test and confirm that the smart contract written has made provision for anonymity, tamperproof, for record keeping of land transaction, secure network for transaction and a decentralized blockchain network that need the verification of all participant (blocks) in the blockchain to verify transaction, there by kicking out third party interference and avoiding the issue of double spending in land title sector.

2. LITERATURE REVIEW

A review of blockchain related work, to ascertain how it has been effective in related sectors and prove the need to create a blockchain application for managing land title in Nigeria, also a comparison was made between the existing technology use to manage land title in Nigeria and the proposed blockchain technology.

Blockchain technology can be used i, for the purpose of for the purpose of obtaining house rent, [7]. It was clearly discussed in the research on how smart contract is written as executable rule so as to provide solution to the rental challenges and a secured platform for the said transaction.

Blockchain technology Blockchain technology is used to process both currency exchange and transactions that comply with executable programming rules which is smart contract, [12], [17]. All these transactions could be validated between parties who fully trust each other without relying on a trusted middleman.

The Blockchain technology highlights all banks are currently engaged in developing a vision of what this technology means for their business, [4], [8]. In research and practice the main criteria for Blockchain implementations such as security, data privacy, and usability are subject to select the best algorithm to ensure consensus and validity, [9], [13].

Blockchain technology can also be used in the waste management system sector. This research indicate how blockchain could be used as a mechanism for higher authentication security in waste management, [16].

Such alternative approaches require a portion of a trust in some elements of the network, such as actors based on the resources they put at risk during validation (e.g., proof-of stake) or in the manufacturers of devices that are used to validate transactions (e.g., proof-of-elapsed time in Hyper-Ledger Saw-tooth Lake), [7], [8].

The related work has indicated how the blockchain technology is used for currency exchange, for data privacy security and how it can be used in a rental system. However, the purpose of this research is to see how blockchain technology can further, be put to use especially in the aspect of managing land title in Nigeria. Table 1 indicate the weakness of the existing technology used to manage land title and the strength of proposed blockchain technology to manage land title in Nigeria when adopted.

Table 1: Comparison of Existing Technology with the Proposed Blockchain Technology

Strength/weakness	Existing method	Proposed method
Third party	There is need for a third party, this increase the cost of purchasing a land in Nigeria and create bottle at some point	The smart contract is an executable code that ensures all policy are obeyed with this it rules out the need for third party
Tamperproof/ secured	It can be tampered with by the ministry of land, being that it is a centralized system	It is a decentralized system; it can't be tampered with by any participant thus making transaction secured
Durability/ public record keeping	Documents often times get damage due to human interference or natural hazard	Documents are durable and kept intact.
Transparency	The transaction often times are not transparent.	It is transparent, every participant in the blockchain have a public key to very every transaction initiated in the blockchain.

Double spending	Often times land is sold to multiple person.	No double spending is allowed as a unique transaction has id is allocated to every confirmed transaction, hence prevent double spending.
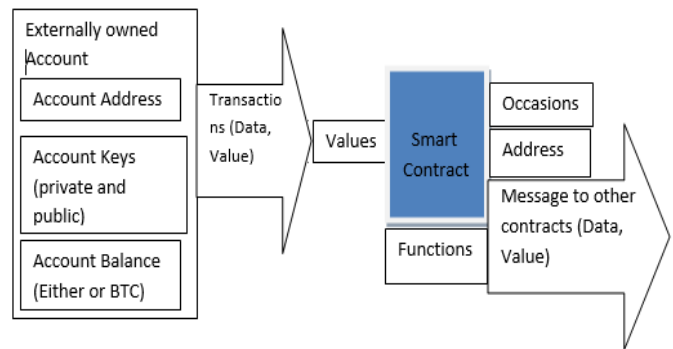
Figure 1: Smart Contract Land Title Conceptual Framework

Proof-of-work approaches require high levels of energy but guarantee relatively high levels of consistency and protection against forgery by any participant in the network (e.g., in Bitcoin) compete against less costly ones, [12], [14].

There is different parameters that are required to be considered while designing and deploying the implemented Blockchain" For the design and deployment of Blockchain implementation, [11]. Blockchain can be used for proper tax system. The research indicate how cryptocurrency can be tax properly which stand at an advantage over the fiat currency taxation where often at times there is no standard tax system, [15]

Blockchain can be used to give sustainability to contractors in the construction industry. Discussion was made on how the issue of how non sustainable materials that is used for construction by contractors, their undeclared work, the hazard incurred, how employee are paid would be addressed with ethereum blockchain where the smart contracts serve as executable rule that ascertain that every contractor meets criteria for every contract issued and employers of the construction industry are paid for their services, [15], [23]

3. RESEARCH METHODOLOGY

For the purpose of this research, the methodology is adopted from Karamitsos, I. [6]. However, the method considered was used by the said researcher which limited is findings to rental system where a landlord can use blockchain to guide its house rentals in Dubai. For the purpose of this research, a smart contract is written to cover the purpose of land rental, land sale and also record keep of land title in Nigeria.

The ethereum blockchain is one technology used where smart contracts are created. The basic actions Performed in the transactions are based on state machine and function, [9]. A high-level programming language which is known as solidity programming language is used to write the smart contract and decentralized applications. The software code is executed on a virtual machine. Ethereum virtual machine. (EVM), [2].

A conceptual framework is drawn to capture the basic framework of the proposed method. Figure 1 indicate the conceptual framework for the ethereum blockchain smart contract suited for managing land title.

3.1 Ethereum set up

Externally Owned Account: the externally owned account is created by the owner of the land in which the smart contract is written based on it to make transaction. Under the externally owned account we have the Account Address, Account public and private key then the Ether.

1. Account Address: once a block is mined by the miners this particular block gets an addressed which is in binary form, with this it can't be traced to anyone with a specific name. This makes the owner and buyer of any land, under the transaction anonymous.

2. Account private and public key: this key is a product of digital encryption of signature. The purpose of the private key which is only owned by the owner of the transaction is to sign a transaction once the smart contract conditions are met. For the public key, this is owned by every participant in the node, this key is used to verify that the said transaction still exists and the acclaimed owner of the transaction is actually the owner.

3. Ether Account: this is the account used in the ethereum blockchain where the commodity/money used to make transaction in the blockchain are kept. Every transaction required a specific amount of gas before the transaction can go through. Once a buyer indicate interest in a transaction, he needs to have an ether account, then purchase some ether after which he can buy the gas needed for the transaction.

4. Transaction: the transaction process accepts the data of the particular block which is about to be transacted is sent to it and process it has a value.

5. Smart Contract: this the executable code, which verifies the value of the transaction and check if it meets all the rules embedded in the contract before it can proceed to send message through individual id addresses to participants in the blockchain network.

3.2 Proof of Work Concept

It requires all nodes on the network to solve a cryptographic puzzle by applying the brute force formula. Take for example if the ethereum blockchain has a new transaction which are tentatively committed and they are based on POW output, a selected block created by the winning node is broadcasted to all the nodes, at specific synchronization interval, [1], [4].

Once the block is transmitted using a peer to peer network to other nodes the same is included in the blockchain and any other tentative transaction are rolled back (by rule of probability the consensus is achieved by 51% if power rather than 51% people count).

The reason for the proof of work concept is because compared to other algorithm it is considered secure as it make it almost impossible for the concept to be attacked unless a miner acquires 51% of computing power which it is made impossible by the blockchain structure, [13].

Mining **is** finding a nonce which contribute to a partially prescribed has. Nonce= an arbitrary meaningless number.

Proof of work with sha 256^2
Ethereum uses {0, 1}2^64 $\longrightarrow$ {0, 1} ^256
X $\longrightarrow$ sha 256 (sha 256(x)) e {0, 1} ^256
Given a 'target' T.E {0, 256}
To 'mine' block – data until hash<t
Nonce=next nonce
Hash= h (block – data/nonce)
There is no better way than guessing probability of success for on nonce t/2^256
T is adjusted every 2016 blocks to keep producing block every 10 minutes

4. IMPLEMENTATION AND RESULTS

The implementation of this project is where the theoretical design is turned into a working system and it give confidence on the new application for the users that it will work efficiently and effectively. Application indicates how the contract is able to control land transaction using the executable code as a medium of policy to actualize the desires aim of this project. The smart contract is written on remix compiler, a user interface is created for the purpose of interaction with the ethereum smart contract and the smart contract is tested on a Roptsten network for the purpose of contract deployment and confirmation. A MetaMask is used as the bridge that connects the ethereum blockchain to the Roptsten network. Figure 2 indicates the landtransaction smart contract executable code written on a remix compiler.

4.1 Smart Contract Landtransaction

The landtransaction smart contract in figure 2 indicates that the contract has been initiated by the landowner and a buyer as indicated interest in the land hence was successfully deployed. It also indicates an environment, Ethereum virtual machine

environment which is can read and execute ethereum blockchain smart contract. The following are the functions of the blockchain smart contract:

The following are some of the features of the smart contract application.

1. Remix ide: the compiler used as indicated in figure 2 is a remix ide.

2. Solidity language: the smart contract as it is indicated in figure 2 is written in solidity high level programming language.

3. Environment: the environment where an ethereum smart contract can be executed is on an ethereum virtual machine environment. For the purposed of this research, an injected web3 environment is used to execute the smart contract code.

4. Account: the account as it is indicated in figure 2 is the ethereum wallet account where the ether which is the money spend in an ethereum blockchain for the purpose of land transaction is saved.

5. Deployed contracts: this is the contract that has been deployed after the smart contract executable code has been compiled, for the purpose of this research, a smart contract titled landtransaction is deployed

```solidity
browser/land1.sol
1  pragma solidity >=0.4.22 <0.6.0;
2  contract landtransaction {
3
4      struct buyer {
5          uint weight;
6          bool bought;
7          uint8 buy;
8          address delegate;
9      }
10     struct Proposal {
11         uint buyCount;
12     }
13 // The Contract managing contract.
14
15     address landowner;
16     mapping(address => buyer) buyers;
17     Proposal[] proposals;
18
19     /// Create a new landtransaction with $(_numProposals) different
20     constructor(uint8 _numProposals) public {
21         landowner = msg.sender;
22         buyers[landowner].weight = 1;
23         proposals.length = _numProposals;
24     }
25
```

Figure 2: Land transaction Smart Contract

4.3 Transaction Confirmation

Using rospten test network where MetaMask is the bridge between the test network and the landtransaction smart contract. This is done to indicate that every participant of the

blockchain has verified the contract deployed by the landowner and can be transacted to the land buyer. Figure 3 and figure 4 indicate the transaction confirmed between two parties and verified by other nodes in the blockchain also in this section a comparison is drawn between two confirmed contracts in the blockchain landtransaction application to indicate the authencity, transparency and avoidance of double spending of land transaction in the landtransaction blockchain network.

4.3.1 Rospten network setup

1. Transaction hash**:** is a unique id that is generated for every transaction that is performed in the blockchain network. For every transaction confirmed, there is a different id and with this it has avoided the problem of double spending in the land title management and transaction. The status shows it was succesful, this indicate that the transaction is genuine and the nodes have used their public key to verify the genuineness of the transaction.

2. Block: there is a unique block number for every node(participant) in the ethereum blockchain, the blockc number indicates a block was successfully mined by the miner also it indicates that the transaction was confirmed by nodes with their public key, in the blockchain, this in a way has created a transparent system of transaction where it is decentralized and cant be tampered with by anyone. This has defeated the use of third party.

3. From and To: the from is the owner of the transactionand to is the buyer of the land. A unique id is also given to the owner and buyer for the purpose of anonymity when do ing a transaction. This as also fulfilled another purpose for which ethereum blockchain was propsed to manage land title and transactions

4. Transaction fee: this is the ether consumed i.e the amount of monet spent to perform the transaction.

5. Nonce: the nonce for this blockchain application is the arbitrary number that is used just once for the purpose of crytopraphic communication the blockchain network. It a random number that is used for the authentication protocol of this transaction in the block so as to make attack or replay of the same transaction impossible.

6. Time stamp: The server for time stamp works by taking a hash of a block of item to be time stamped and widely publishing the hash. Time stamp prove the data must have existed at a time.

7. Gas limit and Gas price: The Ethereum blockchain requires a certain amount gas, depending on the size and type of each transaction. Gas measures the amount of work miners need to do in order to include transactions in a block. The total cost of the Gas Limit and Gas Price (gas limit x gas price) the gas limit for the above transaction and the gas used is, 505,371 (100%)

The figure 3 and figure 4 initiated by the same owner but for different land transaction, this has clearly solved the challenges Nof double spending in land title and transparency of land transaction. There is a unique transaction hash for every land sold in the blockchain. The figure 3 and 4 inidcates that a owner with who has more than one land sold it out to and the transaction hash of the first is different from the second one. This indicates transparency of transaction. Table 2 Indicate the comparison between the two confrimed contract resul setup
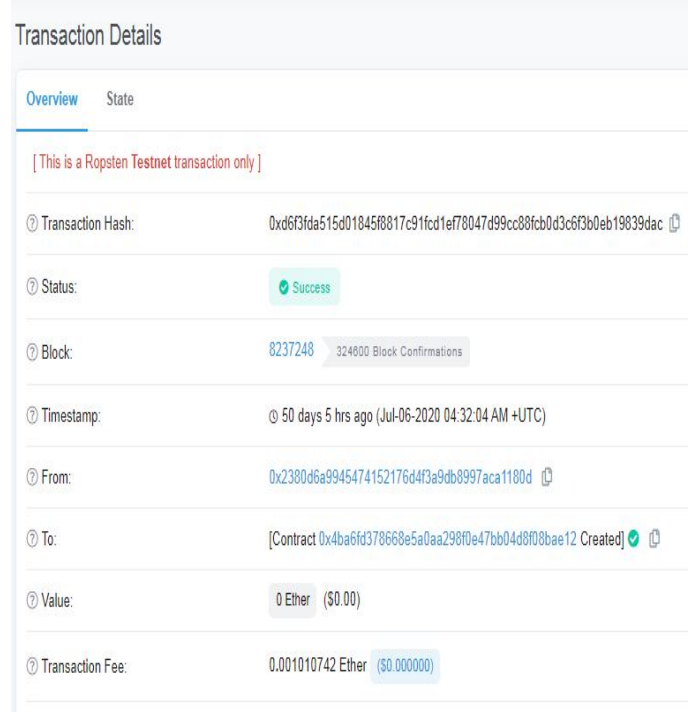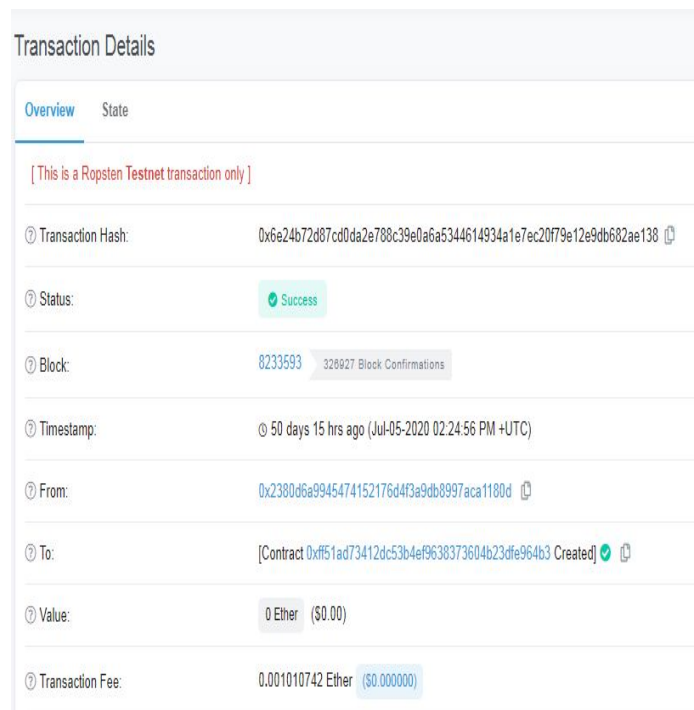

Figure 3: land transaction 1 details

Figure 4: Land transaction 2 details

Table 2: Comparison between two Confirmed Land Transactions

Functions	Land transaction 2	Land transaction 1
Transaction hash	0x6e24b72d87cd0d a2e788c39e0a6a53 44614934a1e7ec20 f79e12e9db682ae1 38	0xd6f3fda515d01845f8 817c91fcd1ef78047d99 cc88fcb0d3c6f3b0eb19 839dac
Block	8233593	8237248
Block confirmation	326927	324600
Time stamp	50 days 15 hrs ago (Jul-05-2020 02:24:56 PM +UTC)	50 days 5 hr. ago (Jul-06-2020 04:32:04 AM +UTC)
From/ landowner	0x2380d6a994547 4152176d4f3a9db8 997aca1180d	0x2380d6a9945474152 176d4f3a9db8997aca11 80d
To/ land buyer	0xff51ad7312dc53 b4ef9638373604b2 3dfe964b3	0x4ba6fd378668e5a0aa 298f0e47bb04d8f08bae 12

4.3.2 Comparison between Landtransaction 1 and Landtransaction 2

1. Transaction hash: the transaction hash is unique and is different for the two transactions this is to confirm the land has not been sold before

2. Block: a block is mined for every transaction initiated in the blockchain. The two transaction block numbers are different this is to show that the transaction is transparent and have not been tampered with.

3. Block confirmation: the number of blocks that confirmed each transaction as of the time the transaction took place are different.

4. Time stamp: this is the time at which the transaction took place which are indicate the two transactions was carried out at different time for each different transaction

5. From/landowner: here the id is the same because the government in this place is referred to have landowner that has land in various places and has the right of ownership.

6. To/land buyer: the buyer at the time of the two transactions are different with their unique address stated. This is to indicate that any citizen can buy from the blockchain since it's a permissionless type of blockchain that was created.

5. CONCLUSION

For this research a proof of concept blockchain application is built to manage land titles and transactions that is carried out within the sector, this application, ethereum smart contract has therefore defeated the challenges faced, using the previous system for managing land title which is the national archives.

The smart contract landtraction written as executable code, landtransaction, has indicated that every transaction performed in the blockchain is secured, tamper proof, anonymous and it keeps every record of the transaction in the network thus providing a secured application for the management of land title in Nigeria. The research questions as been answered with the result obtained in the curse of undergoing this research.

Research question 1 is answered in section 2 with the table therein. Related work to blockchain and existing work was study and a comparison is indicated to show the strength of the proposed blockchain technology over the existing, digital archives used to manage land title in Nigeria.

Research question 2 is answered in section 4 where the result of implementation is stated in figures 3 and 4 it also shows a contract was successfully deployed, hence the smart contract blockchain could effectively control managing of landtransaction.

Research question 3 is answered section 4 where the figure 3 stated how the transaction was successfully tested, with a unique transaction id to prevent the issue of double spending, also a unique id is given to the owner of the transaction and the buyer, to make the transaction anonymous, this in way as solve the problem of third party as they do not necessarily need to trust one another or know one another to transact.

A block number is also generated for the transaction and also clearly shows the number of blocks participants in the blockchain that verified the transaction with their public key digital signature to give transparency in doing transaction. Also, this has solved the problem of tamper with transaction. Also, a feedback of the tested blockchain from stakeholders of ministry of land, Lagos Nigeria.

REFERENCES

1. Atzori, **Blockchain-based architectures for the Internet of Things**: IEEE Communication Survey Tutorial, 18, 2084-2123, 2016.
https://doi.org/10.2139/ssrn.2846810
2. A.G. Awolaja, **Land registration in Nigeria: Issues, challenges** Covenant Journal of Research in the Built Environment, 2(2): 176-194, April, 2016.
3. Buterin, **On Public and private blockchain.** *Ethereum Blog, Crypto Re-naissance Salon*. 7th August 2015.
4. Das, ManikLal, "**Privacy and security challenges in Internet of Things***," Distributed Computing and Internet Technology*.pp. 33-48, 2015.
5. F. Glaser, **Pervasive Decentralization of Digital Infrastructures: A Framework for Blockchain Enabled system and Use Case Analysis**. *50th Hawaii International*

Conference on System Sciences HICSS, Waikoloa, Hawaii, USA, 1-14, 2017.
https://doi.org/10.24251/HICSS.2017.186

6. J. Jonas and N. Christoffer, "**How the blockchain technology can enhance sustainability for contractors within the construction industry",** *Master's Thesis in the Master's Programme Supply Chain Management,* 2018.

7. I. Karamitsos, M. Papadaki and N.B. Barghuthi, **Design of the blockchain smart contract: a use case for real estate.** Journal of In-formation Security, 9, 177-190, 2018.

8. A. Kosba, A. Miller, W. Shi, Z. Wen and C. Papamanthou, 'Hawk**: The blockchain model of cryptography and privacy-preserving smart contracts**', *Proceedings of IEEE Symposium on Security and Privacy (SP),* San Jose, CA, USA, pp.839–858, 2016.
https://doi.org/10.1109/SP.2016.55

9. D. Kraft, '**Difficulty control for blockchain-based consensus systems'**, *Peer-to-Peer Networking and Applications,* Vol. 9, No. 2, pp.397–413, 2016.

10. D. Miorandi, S. Sicari, F.D. Pellegrini, and I. Chlamtac, **'Internet of things: vision, applications and research challenges'**, *Ad Hoc Networks*, Vol. 10, No.7, pp.1497–1516, 2012.
https://doi.org/10.1016/j.adhoc.2012.02.016

11. S. Nakamoto, **Bitcoin: A Peer-to-Peer Electronic Cash System**. *https://bitcoin.org/bitcoin.pdf*, 2008.

12. C. Noyes, Bitav**: Fast Anti-Malware** by *Distributed blockchain consensus and feed forward,* 2016a.

13. S. Omohundro, **'Cryptocurrency, smart contracts, and artificial intelligence'**, *AI Matters*, Vol. 1, No. 2, pp.19–21, 2014.

14. Ojo, "**Evaluation of end-users satisfaction on land title registration Process in Akure, Nigeria".** *Covenant Journal of Research in the Built Environment,* 2(2): 176-194, 2014.

15. R Oleg et al, "**Tax on cryptocurrency as innovative financial instrument in IT sphere".** *Internal journal of advanced trends in computer science and engineering,* vol. 9, No. 1.2, 2020.
https://doi.org/10.30534/ijatcse/2020/4191.22020

16. R Sham et al, **Refuse management system and blockchain: a practical view.** *Internal journal of advanced trends in computer science and engineering,* vol. 10, No. 1.3, 2020
https://doi.org/10.30534/ijatcse/2020/1491.32020

17. F. Tschorsch and B. Scheuermann. **"Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies"**. IEEE *Communication Survey Tutorial*, 18, 2084-2123, 2016.

18. C. Walsh, P.O Reilly, R. Gleasure, J. Feller, and J. Cristoforo. **New Kind on the Block: A Strategic Archetypes Approach to Understanding the Blockchain**. *37th International Conference on Information Systems, Dublin*, 1-12, 2016.

19. B. Nezhad, M. Alizadeh, T. Khodadadi. "**Extending the Network Lifetime by Distributed Selection of Cluster Head in Homogeneous Wireless Sensor Networks**".

International Journal of Advanced Trends in Computer Science and Engineering, 9(3), 2020.
https://doi.org/10.30534/ijatcse/2020/94932020

20. T. Khodadadi, A. M. Islam, S. Baharun, S. Komaki. "**Evaluation of recognition-based graphical password schemes in terms of usability and security attributes"**. *International Journal of Electrical and Computer Engineering*, 6(6), 2939, 2016.

21. T. Khodadadi, A. M. Islam, S. Baharun, S. Komaki. "**Privacy Issues and Protection in Secure Data Outsourcing"**. *Jurnal Teknologi*, 69(6), 2014.

22. Y. Huang, J.S Chen, L.M Wang. "**Performance of Transmission Delay and Energy Consumption of Adaptive Listening Mechanism for Wireless Sensor Networks".** *International Journal of Advanced Trends in Computer Science and Engineering.* 8(6), 2019.
https://doi.org/10.30534/ijatcse/2019/88862019

23. M. Hamza, T. Khodadadi, & S. Palaniappan. "**A Novel automatic voice recognition system based on text-independent in a noisy environment".** *International Journal of Electrical and Computer Engineering*, 10(4), 3643, 2020.
https://doi.org/10.11591/ijece.v10i4.pp3643-3650