A Real Estate and Landed Property Blockchain Distributed Ledger for Elimination of Double Dealing

Nwachukwu C. B.
Department of Computer Science
University of Port Harcourt

Onyejegbu L. N.
Department of Computer Science
University of Port Harcourt

Eke B. O.
Department of Computer Science
University of Port Harcourt

ABSTRACT
In the real estate sector of the national economy land racketeering and property double selling have risen to a higher level due to activities of malicious land agents and those that abetted their dubious activities within the government. In this paper a Blockchain of Real Estate and Landed Property transaction ledger system is developed to record property transactions in a distributed ledger that makes double dealing by the criminal land agents impossible. This will prevent the selling of properties to more than one person by land agents and double dealers and will publish transactions in a public ledger in a transparent way. The system is designed using object-oriented analysis and design methodology and the Blockchain was built directly from the cryptographic system. The result of the system development show that the system was able to produce crypto blocks which can be mined and stored in the chain to both produce the data and the reward system for the real estate industry to use in protecting itself from double dealing and from the criminals. The work is implemented using public key cryptography and Python programming language. The system will bust the real estate sector and bring to minimum the malicious activities of the land agents and their collaborators who commit crime by swindling unsuspecting land buyers and property developers of their fund by double selling and dealing on properties that does not belong to them.

General Terms
Cryptography, Blockchain, Cryptocurrency

Keywords
Blockchain, Distributed Ledger, Real-Estate, Cryptography, model

1. INTRODUCTION
Cryptography is not a new concept, it is the science of using mathematics to hide data on transit from third party (encryption) and also allow the receiver to convert (decrypt) data. It enables users to store or transmit sensitive information from source to destination in a way that it cannot be read by anyone except the intended recipient [1]. The growth of the Internet has made cryptography very important and critical in electronic application systems. When a system is not able to provide some mechanisms to ensure security services, the system will have problems to be accepted. However, with application of cryptography criminals still operate and sign secured system using their digital signature to defraud unsuspecting users. Cryptography is especially useful in the cases of financial and personal data. Hence, information security is a precondition of e-application systems when communicating over untrusted medium like the Internet.

A cryptography system which provides two complementing functions, encryption and decryption is called cryptosystem. Cryptosystems use encryption algorithms to determine the encryption process, the necessary software component, and the key to encrypt and decrypt the data [2]. Cryptography techniques are always employed to protect critical and confidential information against malicious attack from the intruders.

Many modern business transactions rely heavily on cryptographic systems which are the basic foundation for the development of Blockchain (crypto-currencies) that use transaction ledgers to keep record of transactions and signatures of the blockchain network.

Criminals often pervert activities by double dealing to enrich themselves and cause confusion in society. This activity is very common in landed property and Real Estate industry where some legitimate owners of property sale to more than one buyer expecting to use the money collected from the second buyer to offset the first buyer and keep the difference.

This dissertation develops a crypto system for checking Real estate and land double dealing transactions using distributed ledger system.

1.1 Real Estate
Real estate can be referred to as property involving land and the buildings on it, along with its natural resources such as crops, minerals or water. It is immovable property that have a way of handling them and the interest vested in this item of real property, buildings or housing in general. The business of real estate; the profession of buying, selling, or renting land, buildings, or housing [3]. Real estate business isoften carried out by people known as Estate Agents some of them well registered while others are self-appointed. An estate agent is really a person or business that arranges the selling, renting, or management of properties andother buildings. An agent that specializes in renting is often called a letting or management agent. Estate agents are mainly engaged in the marketing of real estate that is for sale, and a solicitor or licensed conveyancer is used to prepare the legal documents. Sometimes the solicitors also act as estate agents.

The estate agent remains the current title for the person responsible for the management of one group of privately owned, all or mostly tenanted properties under one ownership. Alternative titles are Factor, Steward, or Bailiff, depending on the era, region, and extent of the property concerned. Many of these agents are reliable but some are very malicious and dubious in dealing with clients. Some go to the extent of collecting advance fee for non-existing property or sale a single property to a client only to resale it when another client offers a higher fee only to claim to refund the first buyer. There areoccasions where they connive with government agents to sale properties belonging to government illegally causing the buyer some lost when government is out to reclaim the properties. This research develops a Blockchain system to check such criminal activities.

1.2 Crypto currency and fiat e-payments

All currencies need some way to control supply and enforce various security properties to prevent cheating (Satoshi, 2008). In fiat currencies, organizations like central banks control the money supply and anti-counterfeiting features to physical currency. These security features raise the bar for an attacker, but they don't make money impossible to counterfeit. Ultimately, law enforcement is necessary for stopping people from breaking the rules of the system. The fiat currencies are also transacted online via electronic transfers and source to destination information about the fund transfers also require electronic security which can only be provided via cryptography. Cryptocurrencies too, must have security measures that prevent people from tampering with the state of the system, and from equivocating, that is, making mutually inconsistent statements to different people. If Uche convinces Amina that he paid her a digital coin, for example, he should not be able to convince Carol that he paid her that same coin. But unlike fiat currencies, the security rules of cryptocurrencies need to be enforced purely technologically and without relying on a central authority. As the word suggests, cryptocurrencies make heavy use of cryptography. Cryptography provides a mechanism for securely encoding the rules of a cryptocurrency system in the system itself making it to prevent tampering, criminal and equivocation, as well as to encode the rules for creation of new units of the currency into a mathematical protocol [4]. Before we can properly understand cryptocurrencies then, we'll need to delve into the cryptographic foundations that they rely upon.

1.3 Cryptography

Cryptography is a field that uses many advanced mathematical techniques that are notoriously subtle and complex. Fortunately, crypto currencies only relies on a handful of relatively simple and well-known cryptographic constructions. A cryptosystem is composed of two complementing functions, encryption and decryption. Encryption is the conversion of data into a form, called a ciphertext that cannot be easily understood by unauthorized people based on input key. Decryption is the process of converting encrypted data back into its original form, so it can be understood using the decryption key. Encryption and decryption keys are the same for symmetric cryptosystem and different for asymmetric cryptosystem [5]. Cryptosystems are used to achieve several goals such as:

i) Confidentiality: This is the process of keeping information private and secret so that only the intended recipient is able to understand the information.

ii) Authentication, which is the process of providing proof of identity of the sender to the recipient, so that the recipient can be assured that the person sending the information is who and what he or she claims to be.

iii) Data integrity which is a service which addresses the unauthorized alteration of data. To ensure data integrity, the system must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.

iv) Non-repudiation is a mechanism used to prove that the sender really sent this message. This is achieved by using a digital signature mechanism.

A fundamental goal of cryptography is to adequately address these four areas in both theory and practice.

This research studies cryptography and crypto systems used in secured business transactions on the internet. It will develop a distributed ledger system for tracking attempts to sale real estates and landed properties to more than one individual by the same owner. The system publishes each transaction on the blockchain preventing double spending on any single property thereby checking the sale of the property to more than one person.

The use of online payments, crypto currencies and online based business transaction have increased, and the volumes of online transaction have equally increased [6]. Land racketeering and double sale of a single property to more than one client is thriving throughout the cities and communities in Nigeria and many are being defrauded of their hard-earned funds by criminal minded land owners and agents. But the challenge of how to check these land racketing activities has become elusive to both government and communities. How can blockchain technology be applied to check the activities of the land double dealers. Many are in court due to the said problem of land double selling. That is, two or more individuals are in court claiming ownership of a piece of land which has been sold to them by same person who is probably at-large, while other defrauded persons may not want to go to court, others use fetish means to recover their fund and some may go to the extent of killing their offenders. The cause and effect of this property racketeering is everywhere in Africa and particularly in Nigeria. The challenge of land racketeering and double sales is what this project intends to solve via the crypto distributed ledger system (blockchain technology) [7].

The aim of this study is to develop a crypto system for check-mating real estate and land racketeering criminal activities using distributed ledger tracking system. The objectives include:

i) To design a crypto system based distributed ledger tracking system capable of rendering land racketeering useless.

ii) To implement the online transaction crypto system using crypto Application Programming Interface (API) and python programming language.

The distributed ledger tracking system will be the focus area in which the researcher will concentrate on.

2. CRYPTOGRAPHIC SCHEME

There are several factors that limit the extent to which the research could reach. Some of the limiting factors include scarcity of fund as well as time limitations allocated to the research. Other barriers are scarcity of research materials that can be used in the proper examination of alternative findings. In other to have a successful result these barriers need to be examined with the aim of reducing them as low as reasonably practicable.

2.1 Distributed System

Peer-to-Peer (P2P) technology plays a vital role in the Internet. Currently, over 50 per cent of consumer Internet traffic is generated by peer-to-peer networks [8]. The number of users is growing all the time – a report published by the OECD estimates that some 30 per cent of Internet users have downloaded music or files in filesharing systems. File-sharing systems can be used to exchange any kind of computer data, including music, movies, ebooks and software. Historically, file-sharing systems have been used mainly to exchange music, but the exchange of videos is becoming more

and more important [9].

The technology used for file-sharing services is highly sophisticated and enables the exchange of large files in short periods of time. First-generation file-sharing systems depended on a central server, enabling law enforcement agencies to act against illegal file-sharing in the Napster network. Unlike first-generation systems (especially the famous service Napster), second-generation file-sharing systems are no longer based on a central server providing a list of files available between users [10]. The decentralised concept of second generation file-sharing networks as illustrated in figure 1 show clearly that files are no longer stored in a single location but distributed over a geographical area difficult to close down at a single action. If a server in one country is closed, then the servers in other countries or geographical area continues to operate making it more difficult to prevent them from operating.

However, due to direct communications, it is possible to trace users of a network by their IP-address. Law enforcement agencies have had some success investigating copyright violations in file-sharing systems. More recent versions of file-sharing systems enable forms of anonymous communication and will make investigations more difficult. File-sharing technology is not only used by ordinary people and criminals, but also by regular businesses. It is not all files exchanged in file-sharing systems violate copyrights. Examples of its legitimate use include the exchange of authorised copies or artwork within the public domain [11].

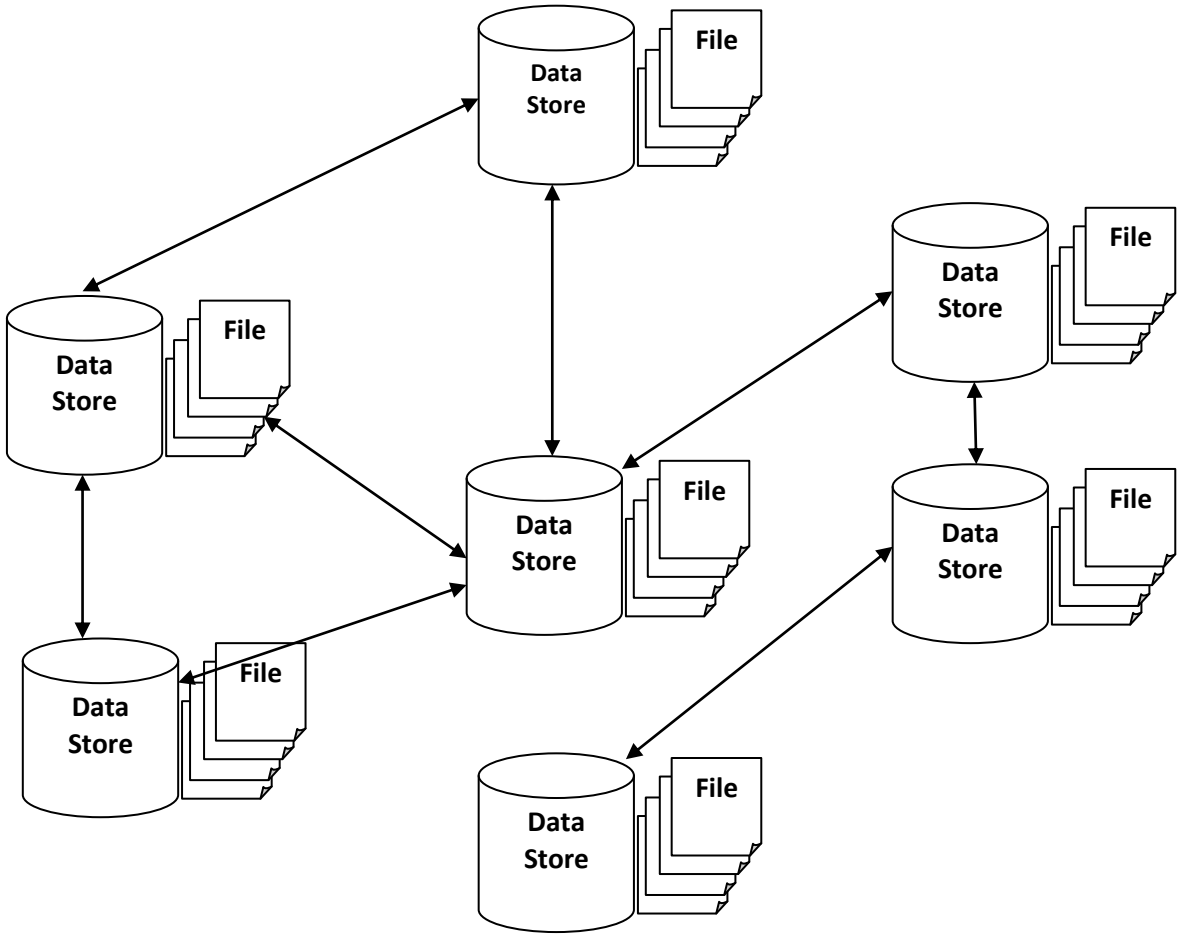

Fig 1: Decentralized second generation file-sharing networks

3. ANALYSIS OF THE PRESENT CRYPTOSYSTEM

In the present cryptosystem it is clear that A prepares a message to B using his *private key* to encrypt then when the message reaches the destination then B can decrypt it using A's *public key* represented as

$Y = E_{KRa}(X)$ ---------- 1

$X = D_{KUa}(Y)$. ---------- 2

During the message preparation A's private key is used indicating that the message could only have originated from A therefore the entire message serves as a **digital signature of A**. This is illustrated in figure 3.1, and clearly the sender must store the message as a **proof of authenticity** to show that he has sent the message since his public key have been made public. Storing the message is very untidy and cumbersome. There must be a way to create a function that is one to one with the message in such a way as to make sure that the original message cannot be changed without changing the function. The cryptographic algorithm used in the present system is also displayed. It shows the process of carrying out the cryptography of the system which at the end produces an encrypted form of transaction M. The M is stored in the ledger as an information that can easily be verified when the public key is used to decrypt it [12].

3.1 Algorithm of the Existing System

Step 1. Let $e_k e_{k-1} \ldots e_1 e_0$, that is, e_i where i= k, k-1, k-2 to 0 be the binary representation of e.
Step 2. Set the variable C to 1.

Step 3. Repeat steps 3a and 3b for i = k; k-1, . . ., 0:

Step 3a. Set C to the remainder of C^2 when divided by n.

Step 3b. If $e_i = 1$ then set C to the remainder of C. M when divided by n.

Step 4. Halt. Now C is the encrypted form of M.

The diagram in figure 2 show the keypair (KRa as the private key of A and KUa as the public key of A) in the message transmission from sender A to the receiver B who acquires and uses the public key of A KUa to decrypt the message sent by A in the crypto process. An algorithm is dedicated for both the encryption and the decryption following the rule of bitstring secure naming arrangement [13].

3.2 Architecture of the Proposed System

In the proposed architecture the Peer-to-Peer network is still connected to the peer discovery system which is responsible for checking and tracking available peers for connection in the cryptographic space. The connected peers are stored in the Peer database from where they can be accessed by the connection manager and the Peer-to-Peer network. The application (app) usually on the browser or mobile user agent is the gateway for users who want to have access to the system or who want to use it. They usually start with invoking a Remote Procedure Call (RPC) that provides access to creation of a user wallet. The wallet also connects with the storage engine which always have direct contact with the coins, the blocks, the header and the holdings (Asset or land information). Once a wallet is needed to be accessed or a remote procedure call (RPC), the connection manager provides the needed connection to the peers to supply their key peers for transaction purposes. The RPC is what the application easily communicates with the connection manager in the process of interacting with the system. The RPC usually checks through the connection manager to know the peers that are communicating for transaction [14].

When an asset buyer intends to transact, the RPC calls the storage engine which in turn links with authorization engine to check if the asset and the owner (Holding) exist in the ledger. The Holding connects with the connect manager to check if the peer exists in the store. The owner-buyer peer is established and connection with the wallet is used to make payment of coins through the storage engine which checks if corresponding coin number actually exists in the storage. Once the asset contract is completed and sealed the coin is transferred and the transaction recorded in the public ledger with information about transferred coin and the new information about the new owner. The transferred coin information is published in the Blocks ledger and through the validation engine and the storage engine the Blocks are stored in the Blocks data storage. Similarly, the information on the Holding ledger is also stored in the Holding storage. The memory pool translates the transaction and assigns it a transaction number (Txs) which is a pointer to the ledger. New buyer of the land (asset) can demand the Txs number and use it to verify the original and new owner of the land.

This makes it impossible for double spending (selling of the land) since the transaction transfers the ownership and cannot do that two times. When the asset is published it call the storage engine which also stores the key peers especially the public keys using the storage engine as the storage processor inside blocks and headers.

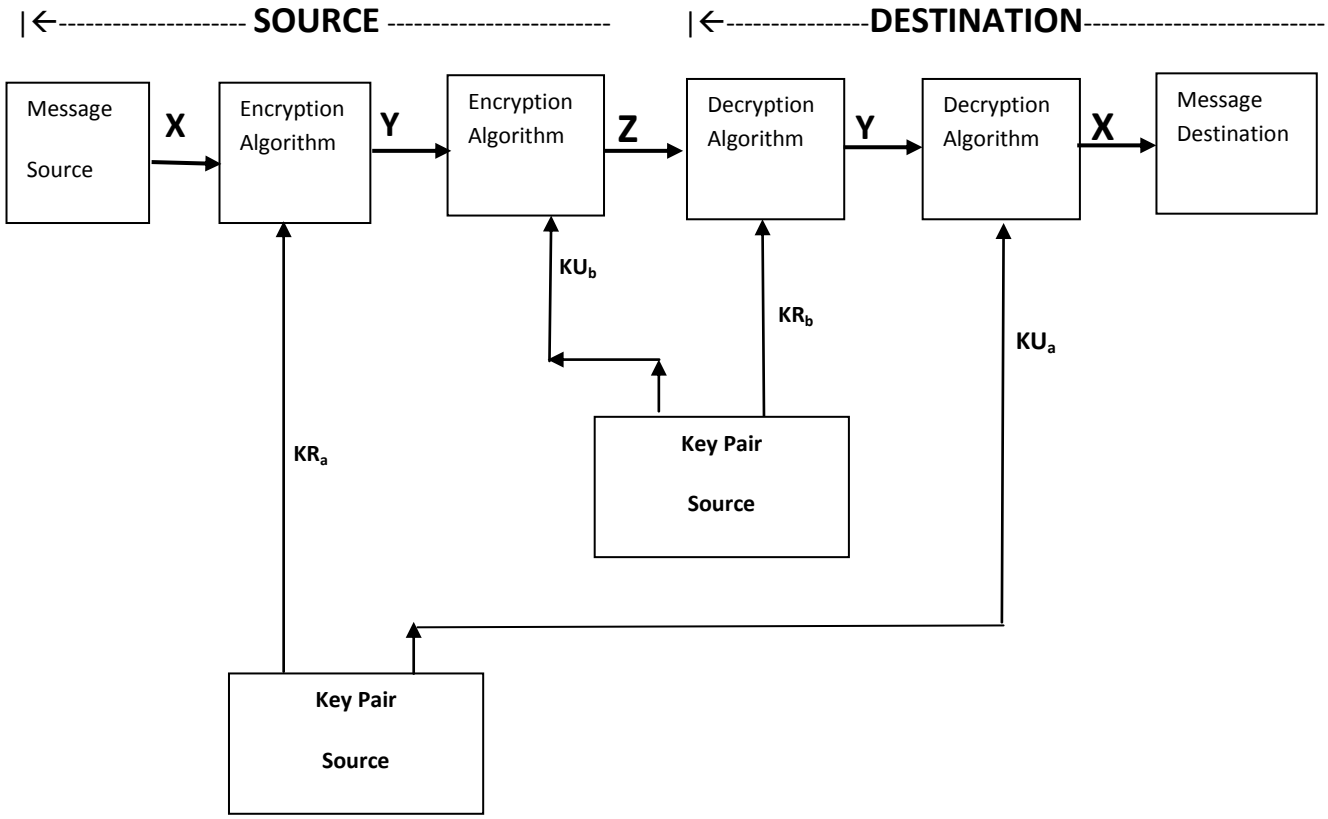

Fig 2.: Cryptographic Process showing the keypair (KRa as the private key of A and KUa as the public key of A)

The Coins are usually called up for the extraction of a specified amount to be used through the remote procedure call (RPC) which uses the storage engine to check the number of coins owned by the buyer before sealing the contract. If the buyer does not have enough coins in the system, the transaction is terminated [15].

In the proposed system the Holding ledger is introduced to publish the land ownership information in ledger. The storage of the Holdings is also introduced in the proposed system to store the land ownership transaction. Authorization engine is introduced to make sure that the asset cannot be transferred without the authorization of the most current owner. So, if the asset is to be sold by the original owner A to a buyer B then the system will demand authorization from A and once it is authorized by A it is ready to be transacted. B can then pay and the system transfers ownership to B and publish it in the Holding Ledger. If A establishes a Sell mode to resell the asset to C assuming that C indicates interest to buy then the system will call for B's authorization and will deny A's authorization then A cannot resell the asset.

3.3 Use Case Design

In the use case design the flow of the various actions carried out by the major components of the system and the actors that carry out the actions are represented in use case diagram [16]. In the diagram in figure 3 the design clearly shows four main actors the Owner of the asset, the Buyer of the asset, the crypto-exchange and the Blockchain. The Owner actor is the current title holder of the land that needed to be sold. The Buyer is the actor representing the person that have indicated interest in acquiring the asset. The Crypto-Exchange is the middle system that links to the Banks for transfer of fiat money between the buyer and the seller [17]. The Blockchain is the cryptocurrency system that handles the transaction internally between the buyer and the seller peers. In the system the buyer indicates interest when the asset is placed for sell by the Owner of the land. The Owner still uses his private key peer to authorize sell, the authorization of sell is done to prevent initiation of transaction where the owner is not actually the one who places asset for sale. Once the Owner authorizes sale the transaction key peers are created by the blockchain and the exchange approves of the transaction. The exchange approval involves acknowledgement that the seller have enough fiat (money) or enough coin to purchase the asset.

Then the buyer sends coins to the seller via the blockchain and the exchange or wallet. The blockchain in return confirms the transfer of the asset as published in the Holding Ledger in the blockchain. Figure 4 show the actors in the use case design and the action that each of the actor is expected to carry out. In real world there may be more than four actors but the actors can still be correctly grouped into the major four presented in the design.

3.3.1 Actors

These actors include :

i) Blockchain: This actor is the ledger itself where the transactions are recorded in the distributed nodes. Each node within the network is expected to have its own ledger whose content must march with the content on the other ledgers in the other nodes before a transaction is confirmed by the system.

ii) Asset Owners: The owner actor is the real estate owner or the land owner that wish to transact on the Blockchain by either renting the asset or out rightly selling it out on the Blockchain. As an actor the owner need to interact with the other actors to successfully carryout the needed operations on the system.

iii) Asset Buyer: This actor represents both the person that intend to purchase a real estate and the people who wants to rent the property. They are provided with the opportunity to interact with the other aspects of the use case both the actors and the actions.

iv) Crypto-exchange: This actor can be in form of a Blockchain cryptocurrency exchange but what is sold and bought will be rents and property against the crypto coin and other fiat currencies. It could also be in form of a block explorer that allow properties to be listed with their hash addresses and others can interact via the explorer. It is a point of convergence of the other actors.

3.3.2 Actions

The actors presented in the use case design include :

i) Place Asset for sale: this action facilitates the placement of asset by asset owners in the block explorer or exchange.

ii) Place demand to acquire asset: the action is used by asset buyers to place a deman on a listed asset.

iii) Authorize Sell: When an offer is made the owner is still given the priviledge to authorize sell before sell is made.

iv) Create key peers: is an action carried out by the Blockchain to be able to transfer asset to the new owner.

v) Approve the placed demand: this action is carried out by the exchange,

vi) Accept Asset value in coins: the asset owner, the asset buyer and the crypto-exchange have to auto accept value in coin by default or by selecting an action.

vii) Confirm transfer of Asset: the action enable the system to transfer asset and create new block information for the asset in favour of the new title holder.

viii) Send Coins: Crypto can be transferred from buyer to seller using this action

ix) Publish transaction in ledger: this action finalizes a deal by publishing it on the ledger for all to see and confirm.

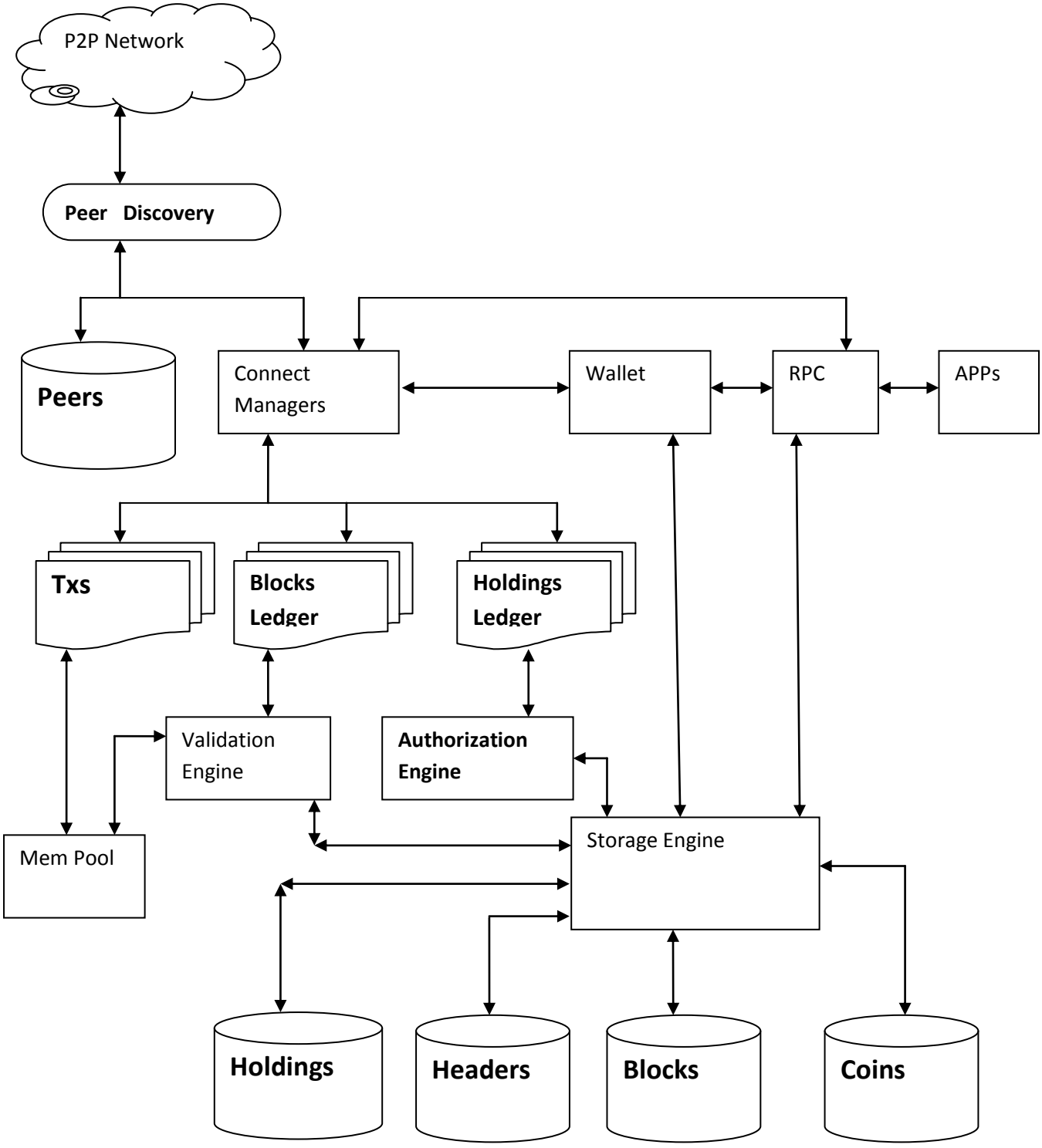

Fig 3: Architecture of the Proposed Distributed Ledger System

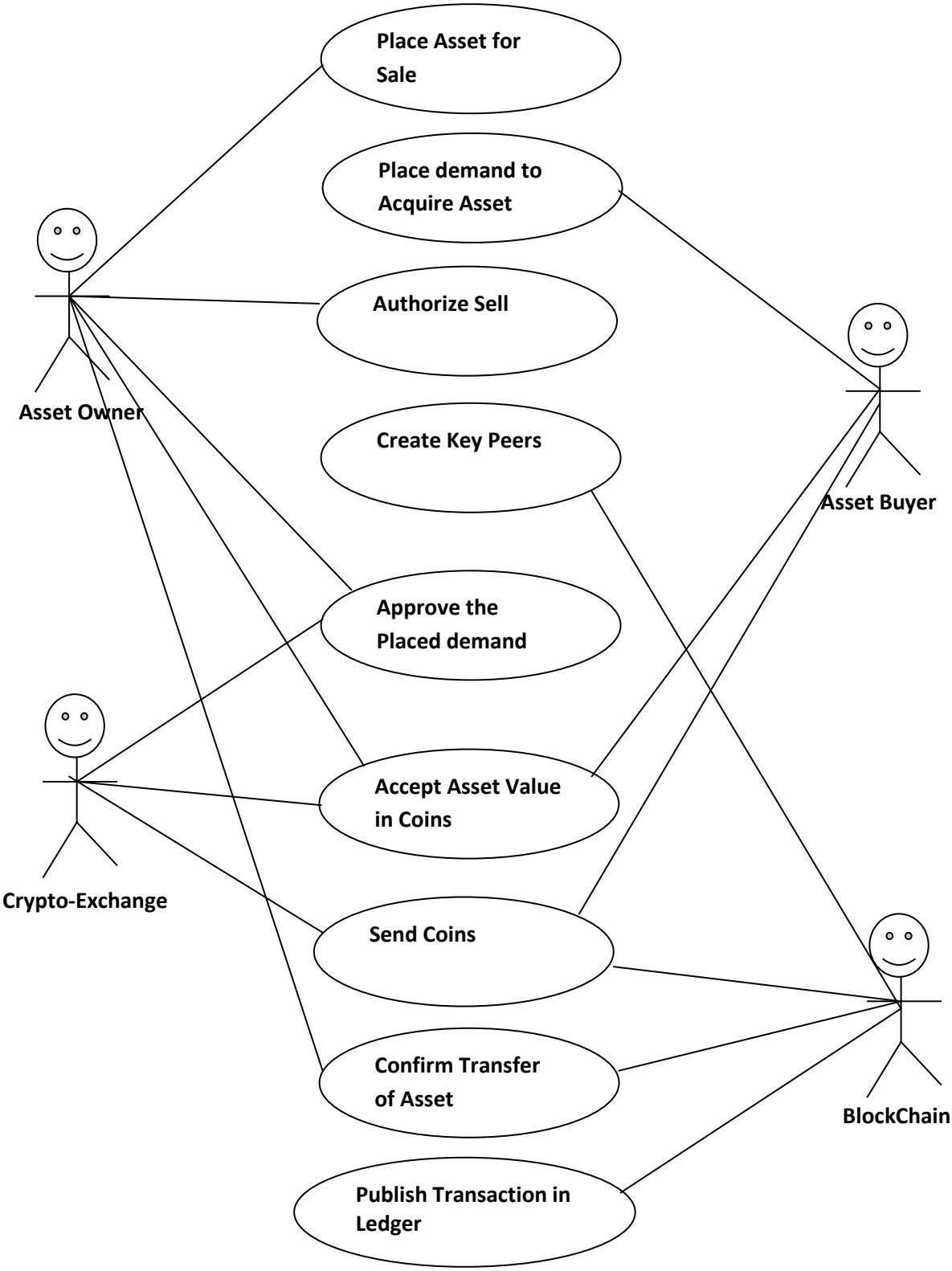

Fig 4.: The Use Case Design of the Proposed Real-Estate Blockchain Asset System

4. DATABASE DESIGN AND RESULT

In most recent time databases seem to be fixed in their design nature. Most of them are relational databases with tables fields and records. Blockchain Ledgers are not relational databases rather they are meta databases that are often generated in an unstructured format[18][19]. They need to be stored in such a way as to allow proper storage and retrieval based on the information required. The data is provided with cryptographic hash, and a timestamp that will be useful in verifying when a block is mined and the hash address of the mined block.[20][21]. The timestamp of a particular digital asset assist the system to actually identify the miner to be rewarded with digital coins[22]. In the listing below a design of the structure show the meta data A which is a Blockchain Ledger itself. Inside the Blockchain are other data values which include B, C and D. It is of particular interest to note that B1 and B2 are the data components that are used in building the B data which in turn combines with C and D to form the A database. The data is arranged in such a way as to use lower data in defining higher data. This increases the speed of data storage and retrieval and allow the data in the system to easily scale to any size provided there are memory space to store the data. The implementation of this data structure is often done using JSON or other variants. The JSON format makes the data very easy to read by both the machine and humans.

The file input into the Blockchain system is where the initial information required by the ledger is stored in a JSON format file.

A real-life representation of the ledger of the first block in JSON is given below:

{"hash"

"000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",

"confirmations" : 308321,

"size" : 285,

"height" : 0,

"version" : 1,

"merkleroot" : "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",

"tx" : [

"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"

],

"time" : 1231006505,

"nonce" : 2083236893,

"bits" : "1d00ffff",

"difficulty" : 1.00000000, “asset”: [

“asset_type”: land”,

“Owner_name” : “IkechukwuMicheal”

“assetblockhash” :

"17b89c00839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048",

“token”: 4500502]

“authorization” : 512

"nextblockhash : "00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048"}

This listing is a JSON version of the proposed ledger showing a single block and how it is referencing the next block by displaying the nextblockhash.

The command typed in the browser is chain to view the chain pre-mining. The window displayed the Genesis Block (First Block before mining starts) which so the first success. The chain can only grow when new blocks are mined and added into it. Genesis is only on ledger but once a new block is mined it will be added into the block to make it two blocks, another mined block will make it three blocks and so on. In the illustration in figure 6, the results of the mining is clearly shown. The index of the block is 2, the hash address of the genesis block is shown and the transaction code is also indicated. The new mined block also indicate the time stamp that the new block was mined. The other information that also accompany the system is the recipient and the sender information. During mining the recipient and sender seem unknown since the mined coin have not being allocated for transaction. During allocation the receiver is known, and the receiver can then enter the wallet address of the to be assigned to the sender section. In real world implementation a HTML form can be easily used to fill in the values of the sender and receiver

The web view is not just a simple HTML, it is a server powered page by flask a Python web server that has good synchronization capability. The server is capable of hosting three or more nodes in the localhost.

Fig 5: Output of the initial Chain

Fig 6: Mine of the Genesis Block

The flask server is used in creating the database, but the client side of the system activated from the web browser shows us the action that goes on in the web server. Once the mine key word is activated by attaching it to the node address it automatically activates the mining operation and show the mined block. A repeat of the mine command will cause the second block to be mined and so on.

In figure 7, the executing program clearly shows the new chain after three mining operation have been carried out in the system. The three consecutive blocks with index 1,2 and 3 showing the hash address of the previous blocks in a well linked chain.

Fig 7: Mining of other Blocks

5. CONCLUSION

In conclusion Blockchain crypto-currency ledger have been studied and presented using a well-articulated design of a system that can handle various activities within the block to make sure that land transaction is transferred once, and that the transaction is recorded in the Block. The Blockchain is usually a public ledger which will be available for even non-Nigerian to view and actually know who owns a land and can easily trace ownership using the blockchain. Investment on land and the use of land in getting collateral can easily be facilitated. Criminals who depend on double dealing on land can then be well busted and put out of business. The system designed in the project was developed and implemented using Python, Flask framework and JSON which is a NoSQL data management technology with capability and ability to handle challenges of criminal land double dealing and can speedy execute blocks and mine within the Blockchain. The logic of the distributed blockchain ledger system was implemented using Python.

5.1 Recommendation

The system developed in this project is recommended to organizations that are managing land and landed property and the ministry that is in charge of land registration and certification. They can deploy the technology and use it in managing the transfer of land ownership. The system is also being recommended to developers of crypto-currency for us in imbedding similar contract into their blockchain and used in executing the contract. Advanced research persons will also need the work done in this project as a stepping stone to improve on quality of blockchain developed and very important contracts that can be embedded into it to make the coin developed around it to be useful in solving societal problems which are multifaceted in our society. Other interested researchers may also need the work for the purpose of profiling, testing and redevelopment of a blockchain system to study some of the features that have been presented in the course of this research work.

5.2 Contribution to Knowledge

A crypto system for check-mating real estate and land racketeering criminal activities is presented by developing a crypto system that is used to hash and assign a code to real estate and land and publish same on a distributed ledger system. This is a new application of blockchain technology and real estate professionals can put it to commercial use.

A crypto-system was designed and a distributed ledger capable of checking double sales/ spending of land transaction which can check land racketeering was developed.
A blockchain crypto system using crypto API and python programming language was also implemented.

6. ACKNOWLEDGMENTS

Our thanks to the Oyol Computer Consult, Inc for typesetting the paper. We also acknowledge the tokens Binance exchange offered in its trading competitions that helped in financing the app development.

7. REFERENCES

[1] Schneier,B.(1996) “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, John Wiley & Sons.

[2] Stalling, W. (2006) "Cryptography and Network Security: Principles and Practices", Prentice Hall.

[3] Malgorzata R. (2018) Incentives for Polish higher education institutions to improve real estate efficiency, Journal of Corporate Real Estate, Vol. 20 Issue: 3, pp.214-227,

[4] Satoshi N. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System,https://www.bitcoin.org/bitcoin.pdf, Accessed, 2017

[5] Andreas M. A. (2017) Mastering Bitcoin: Programming the Open Blockchain, O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.USA.

[6] Arvind N., Bonneau J., Edward F., Andrew M., Steven G. (2015) Bitcoin and Cryptocurrency Technologies, Princeton Pu Ltd, USA.

[7] Wilber, D. Q. (2015). Encrypted Devices Let Criminals Go Dark, U.S. Prosecutor Warns. *Bloomberg*. Retrieved on 10th June 2015 from http://www.bloomberg.com/news/articles/2015-05-06/encrypted-devices-letcriminals-go-dark-u-s-prosecutor-warns.

[8] Kshetri, N. (2010). Global Cybercrime Industry: Economic, institutional and strategic perspectives. Berlin Heidelberg: Springer Science & Business Media.

[9] Tikk, E. (2011). Ten Rules for Cyber Security, Survival: Global Politics and Strategy, 53(3), 119-132.

[10] Wadhwa, V. (2015). Quantum computing is about to overturn cybersecurity’s balance of power. *The Washington Post*. Retrieved on 22nd May 2015

[11] Joe G., Sidney J. H., Michael O. and Jose I. R. (2015) Protecting Intellectual Property and Trade Secrets in the United States and Beyond, FDCC Quarterly/Summer.

[12] Abdelsalam A., andUounis A. (2012) Developing a Cryptosystem for XML Documents, International Journal of Information Science, 2(5): 65-69 DOI: 10.5923/j.ijis.20120205.03

[13] Haber, S and Stornetta W. S (1997) Secure names for bit-strings, In Proceedings of the 4th ACM Conference on Computer and Communications Security, 28-35.

[14] Anderson, R. and Steven J. M. (2014) EMV: why payment systems fail. Communications of the ACM 57.6 : 24-28

[15] Zhigang, Y. (2011). Cyber Variants of Traditional Crimes and Criminal Law Responses. Social Sciences in China, 32(1), 66-79.

[16] Massias, H., Avila, X. S. and Quisquater, J. J (1999) Design of a secure timestamping service with minimal trust requirements, In 20th Symposium on Information Theory in the Benelux,

[17] Eli Dourado and Jerry Brito (2014) cryptocurrency, Palgrave Macmillan The New Palgrave Dictionary of Economics, www.dictionaryofeconomics.com, retrieved 2017

[18] Cameron S. D. B. (2015) Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, International Journal of Cyber Criminology (IJCC) . 9 (1): 55–119. DOI: 10.5281/zenodo.22387

[19] Merkle, R. C. (1980) "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, 122-133, April 1980.

[20] Back, A. (2002) Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf.

[21] Bayer, D., Haber, S and Stornetta, W. S (1993) Improving the efficiency and reliability of digital time-stamping, In Sequences II: Methods in Communication, Security and Computer Science, 329-334.

[22] Haber, S and Stornetta, W. S. (1991) How to time-stamp a digital document," In Journal of Cryptology, 3(2), 99-111.