ABSTRACT

Land issues have always been a major concern faced by people from every background. When one buys a property, he must find a secure title and get it signed by Lawful owner, in order to get a 'Good Title'. This seems to be very easy, but the real devil lives in details. Blockchain technology is already being exploited in various ways for saving cost with high security to create and manage the distributed system as well as to record information about transactions without the verification of the third party. Flawed paperwork, forged signature, defects in foreclosure and mortgage documents have marred proper documentation of property ownership. The ultimate solution to fix these issues is "Blockchain Based Land Registry". That provides immutable history of transaction records, i.e. provides undoubted Authenticity, Records are permanently linked to system, that restricts tampering of records. It provides robust validation. With Blockchain, we provide immense level authentication to records of Land Registry. It would be stored on a distributed ledger, providing genuine and gigantic endorsement. Land registry blockchain can solve the above problem by keeping record in an open distributed ledger, that can record transactions between two parties efficiently in an verifiable and permanent way. One has to upload the document file, and keep the receipt of the transaction. The receipt hash would be further used to search for the property. This would serve as a very reliable proof to enhance the robustness of legal authorities.

INTRODUCTION

In every manner the security of a Document, Land Registry is of immense importance. The paper-pen preservation of land document always had a threat or breach of fraud. We need to have a secure system that would decrease the frodery, fraud land ownership, duplicacy, multiple ownership. From a long time, the traditional pen and paper scheme is being used. Now, digitalisation of this is needed in order-to preserve the legal document along with providing easy search and validation on the property.

Blockchain is a distributed , append-only, inconvertible, public ledger. This new technology works through four main features:-

• The ledger exist in many different location. No single point of failure in maintenance of the distributed ledger.

• Blockchain keeps a record of all data exchange - thus record is reffered to as a ledger and each data exchange is a 'Transaction'. Every transaction is added to ledger as 'Block'.

• It utilises a distributed system to verify each transaction - a peer to peer network of nodes.

• One signed new transaction added to blockchain and could not be altered.

DECENTRALISATION

Decentralisation makes the blockchain impervious to censorship, tempering or corruption. The most important concern while preserving the land registry document is that of proper validation and verification. Now, since decentralisation uses a peer-to-peer network, copies of same data is stored in many different location, and unless one could track every single block, you can not destroy it. As well,

because so many different, independent nodes are keeping track of ledger, modifying the data culpritly could not be taken too far, as all other nodes should be verified , and other blocks won't agree with transaction and won't add it to the ledger. Blocks store info that distinguish them from other blocks. Much like you and I have names to distinguish us from one another, each block stores a unique code called a "hash" that allows us to tell it apart from every other block.

No single point of failure:

Crashes and failures are the single biggest problem with any centralized network. A single failure can cause service disruption and potentially cause millions in losses.

Scalability advantage:

Decentralized networks are made up of independent nodes. When the load on a network increases, the supply can easily increase as well. These nodes can simply be home computers with an internet connection.

Democratic decision making:

Most centralized systems have a single authority that controls all the power and makes all the decisions. There are dozens of examples of how bad decision making by a central authority can be bad for users and make the entire system crumble. For example, a social media company that has total control over its users' data.

PRIVACY

Trust is risk judgement between different parties , and in digital world , determining trust often boil down to proving identities and proving permissions. In case of blockchain technology, private key cryptography provides a powerful ownership tools that fulfill authentication requirement. Possesion of private key is ownership. It also spares a person from having to share more personal information than they would need to for an exchange, leaving them exposed to hackers. We are highly concerned about, and need to protect the information that is stored at a computer , it could be some useful asset or of some indiviual's identity. The data we protect are the "Personal Data" which is any information relating to an identified or identifiable natural person, sometimes called a data subject, and have made protecting privacy and the confidentiality of Personal Data.

INTEGRITY

Merkle Tree is a data structure used by several Blockchains. Every block stores all the transaction data it has in the form of a Merkle tree. In this data structure, hashes of child nodes are combined together into the parent node's header. This technique of combining the child nodes' headers and adding it to the header of the parent node continues iteratively till we reach the final node, right at top, the root node. Thus, the root node will contain information about all of the nodes present in the tree.

First- All the transactions of the block are individually hashed. For example, L1 is hashed to hash 0-0. Then the combination of hash 0-0 and hash 0-1 is hashed and stored into a parent node. Same procedure

is repeated for other nodes. And lastly, combination of hash 0 and hash 1 is hashed and stored in its parent node and this is, so to say, the final node of this Merkle tree. It is called the root node or simply the Merkle root. This Merkle root along with previous block header hash, a time-stamp and a nonce is used to generate the block header.

To summarise, hash of all the transactions in a block is stored in the the Merkle tree. So when a node wants to verify if any transaction is changed, the node will only have to build the Merkle tree using all the transactions of block. This makes it very simple to validate or invalidate a transaction. Thus, Merkle tree helps maintain security in Blockchain.

LAND REGISTRY AND BLOCKCHAIN

We are building a chain of block that would store the Land registry documents. The Record of User would be stored on the block. Every land document would be enter into the Records as file of any format, that would be stored on the blocks. After uploading the document would click on the "Get Receipt", and a receipt would be generated that would have a transaction hash. The user would store the Hash, and this hash would be stored to make further references, of transfer of property, buying or selling of property. BlockChain is Chain of blocks that stores our Information .It was originally described in 1991 but it came in existence after 2008. Once any data is stored in block it cannot be altered. Each block contains data, hash of the block and hash of the previous block. If hash of a block change then all the next blocks would become invalidate. When a purchaser seeks to buy property today, he or she must find and secure the title and have the lawful owner sign it over.This seems simple on the surface, but the devil is in the details. For a large number of residential defects in foreclosure and mortgage documents have marred proper documentation of property ownership. Land registration generally describes systems by which matters concerning ownership, possession or other rights in land can be recorded (usually with a government agency or department) to provide evidence of title, facilitate transactions and to prevent unlawful disposal.

SMART CONTRACT:

The use of blockchain in land registry is primarily being explored for its potential to enable the "almost instant" transfer of property securely. With smart contracts enabling self-execution when certain conditions are met transactions could be completed faster. For example, a rule could be put in place to facilitate the title of a property being automatically transferred to the new owner when they deposit funds to the appropriate account. There is also the potential for the registration gap to be removed. The use of smart contracts would speed up the process by automatically updating the ledger, instead of buyers having to transfer ownership through an application form. The technology can also enhance trust between parties in transactions due to the contracts being automatically executed and enforced, ensuring that outcomes are validated by everyone in the blockchain's network.

A smart contract is a protocol that enforces the performance of a contract with adding the terms of the agreement into the code. Smart contracts are a great way to exclude any third party from the transaction and make transaction prices lower, as they need no validation. Smart contracts are implemented in a lot of cryptocurrencies to control the transfers of digital currency, establish a

governance and a lot of other things. But smart contracts have a wider range of possible implementations. Smart contracts may be used in voting, management, machine-to-machine interactions in the internet-of-things, real estate and in the building of personal data storage with specific access policies, e.g., medical databases.

IPFS(INTERPLANETARY FILE SYSTEM):

The InterPlanetary File System (IPFS) is a distributed file storage protocol that allows computers all over the world to store and serve files as part of a giant, peer-to-peer network. Every single computer that's running IPFS acts as both a client and a server. In other words, each computer running the IPFS software can serve content to any other computer in the network, as well as request content from anyone in the network. So if you run IPFS on your computer and upload a picture to the IPFS network, that image can be viewed and downloaded by anyone else in the world who is also running IPFS.Here the transaction data to be stored in the IPFS. Only the IPFS hash of the transaction is packed in the block to alleviate the blockchain data storage pressure.IPFS is a secure, high-throughput, content addressed block storage model that supports high-capacity storage and high concurrent access. An IPFS hash is only a few tens of bytes. Therefore, consider storing the transaction data in IPFS and storing the returned IPFS hash in the block, thereby achieving a large reduction in storage space.

UPLOADING THE DOCUMENTS:

The Land Registry document are salient legal document that needs to be safeguarded from frauds. Land registration generally describes systems by which matters concerning ownership, possession or other rights in land can be recorded (usually with a department) to provide evidence of title, facilitate transactions and to prevent unlawful disposal. Land registry blockchains seek to fix these problems. The document would consist of Land documentary, that would be stored on the IPFS. Consider the case:

• John wants to upload a PDF file to IPFS but only give Mary access

• He puts his PDF file in his working directory and encrypts it with Mary's public key

• He tells IPFS he wants to add this encrypted file, which generates a hash of the

encrypted file

• His encrypted file is available on the IPFS network

• Mary can retrieve it and decrypt the file since she owns the associated private key of

the public key that was used to encrypt the file

• A malicious party cannot decrypt the file because they lack Mary's private key

This hash would be passed as value to string variable. The reciept would be generated, that would store the hash. This hash will be the unique receipt value that would be used to refer to future transaction. This would be valid receipt that can be used further by the owner to look for his property. Miners would verify the transaction, they checks the received transaction, insert them into the pool. If transaction is

valid, it is stored on IPFS, keeping the IPFS hash in return. Then in the process of calculating the next block, each miner puts the IPFS hash of verified transaction into new block, calculates the merkle root and the block hash. If miner A successfully calculates the block hash that meets the difficulty, the block will be broadcast to miners B,C and D. Then they need to verify the transaction and the block hash. Then the validity of transaction and the block would be confirmed. Afterwards, the new block can be appended to the blockchain ledger.

The smart contract to store the value of ipfs hash, and generate receipt:

```
pragma solidity ^0.4.17;

contract Contract {

string ipfsHash;

function sendHash(string x) public

{

  ipfsHash = x;

}

function getHash() public view returns (string x)

{

  return ipfsHash;

}

}
```

SEARCH FOR THE NEW PROPERTY:

Everyone on the network would be able to access these records as they are not stored centrally. Single server farm could provide massive cost benefits and economies of scale for all sorts of applications, like storage and computing power. However, over time, the inherent flaws of a centralized system have become apparent.

The user could use the receipt vaue to know full detail of the property, and see the documents uploaded. One could buy or sell the property without any loophole, or any risk of fraud. As document would be stored on a decentralised network, if somebody ever tried to create a false property, it has to be verified by all the others on network. The new block should have valid hash of previous block, then only it would serve as a valid block. Since, a false block could not have the previous hash, as not only storing the previous hash would do, but all the preceeding block are related to one another. In order to get a new

block, whole blockchain needs to be generated again. This would take million of years, so there can not be any mistake regarding the security of the record. The user would find valid and verified property, with true ownership and hence Trustworthy.

CONCLUSION

The solution of adapting Blockchain technology for storing our Land registry records, would result in a process that would serve more secure, validating, robust, cheaper, faster and easier. It removes certain fraudsters between the buyers and seller, various property owners. It also gives more solid support to conserving the peace of the legal evidence. In this paper, we introduced a unique, blockchain-based Land Registry system that utilizes smart contracts to enable secure and cost efficient Record maintaining while guaranteeing privacy. We have outlined the systems architecture, the design, and a security analysis of the system. By comparing to present day methods, we have shown that the blockchain technology offers a new possibility for people to advance from the pen and paper, lockers scheme, to a more cost- and time-efficient Land Registry scheme, while increasing the security measures of the todays scheme and offer new level of integrity control.

The merkle root in the block header of the model is calculated based on the IPFS hash of the transaction. The block header hash is calculated based on the merkle root. Therefore, the validity of the blockchain can be verified directly . Once a malicious node wants to change a transaction data in the block, its IPFS hash also has to change. A small change will cause a huge difference in the merkle root, which will cause the block hash to change. Therefore, the invalid block will not be recognized by the blockchain network, which ensures security of the block data.

Using an Ethereum blockchain, it is possible to send hundreds of transactions per second on to the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain. Our Land registry scheme allows government official to upload the Asset and store it on the ipfs, the hash would here work as unique key to access record, and the data would be stored on blocks guranting no tampering or integrity breakdown of the records.