HACETTEPE UNIVERSITY

DEPARTMENT OF COMPUTER ENGINEERING

BBM 443 – FOUNDATIONS OF BLOCKCHAIN

PROJECT REPORT

LAND REGISTRY

Group Members:

Atakan Ayyıldız- 21526681

Göktuğ Candemir- 21627064

Ahmet Kasım Toptaş - 21627667

Mert Emre Öztürk-21986578

1 Introduction

What is Land Registration?

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 prevent unlawful disposal. The information recorded and the protection provided will vary by jurisdiction. In our country, this is done by the land registry cadastre management.

Introducing the Problems

The purchaser has to pay a large amount of money to get the title deed of the real estate he/she bought.

Since it is a centralized management, an attack on the center or an incorrect operation may cause data loss.

Deed transactions can only be processed during business hours. Blockchain, on the contrary, enables transactions to be processed at any time.

Difficulties encountered when purchasing a property from different countries.

Why Blockchain is Useful for Land Registry Works

-Providing a reliable money transfer opportunity.

-Inability to delete or change the transaction by malicious individuals

-Protected against attacks since it is not centralized. (At war etc.)

-Provides a platform for digitizing assets and selling them as shares

Main Characteristics of Our Land Registry System

Database:Instead of using a traditional land registry system (they provide source database and backup databases) our system provides a shared database system. One copy to each manager and they connected to each other (P2P).

Trust: We can not ignore the state so that the state is going to appoint a proxy.

Multiple writers: There are multiple entities which generate transactions that modify the database.

Validation: Blockchain holds all blocks in a sequence. It is immutable.

Scalability:The Blockchain is easily expandable. Everyone who would like to upload a transaction on the blockchain can do so.

Efficient: By force of our system, people don’t need to go to traditional land registry offices.Therefore, buying and selling processes will occur without unnecessary people transactions.

Usability: Our system is very simple for many people and they will perform buying/selling their land easily and they will save all the time whenever they want.

Eco-friendly: Our system will reduce paperwork in the land registry offices.

Timing: In blockchain, we can process a certain time.It provides many operations made at the right time and will preserve the system from duplicate and late operation.

Security: Blockchain holds many transactions block in its scope.Each land registry block holds hashing of previous and next blocks,if malignant people want to change a block,all blocks will be invalid in their scope because previous and next block hold hashing of original block but other people preserve original blockchain, this harmful operation doesn't affect them,therefore it provides reliability for system.

2 State-0f-The-Art

There are problems with traditional land registry progress. A lot of articles shows us many problems.

Land registration is a waste of time and money. Deed registration takes an average of 15 and 39 days in developed countries, the USA and Germany. On the other hand blockchain provides us time efficiency.

The traditional land registry uses central databases for the land registration. So untrusted employees of government could manipulate the records. 20 percent of land service users, confirms the bribe which they paid for land registration according to the International transparency policy. Those could hurt the people's trust in the government.

Actually Blockchain can solve many problems. But in the blockchain users trust each other to provide the security of information. It uses distributed ledger as a shared database.

Blockchain applications in land registration use private, public or a hybrid approach.

Private blockchain uses a small number of nodes and it causes that rules can be adjusted easily. System becomes flexible. Writing procedures are entitled to only one party which could be the government. But there is the same risk as the traditional land registry cause of being hacked. Users can read transactions. It looks like a traditional land registry system. Therefore that approach doesn't provide much value. Total costs could be lower than the traditional land registry system but computational cost is not certain. However, less decentralised blockchain which private blockchain's characteristics supports much faster transaction speed because of the consensus finality.

Public blockchain is the same as a traditional blockchain system. Everyone can make transactions publicly. The system doesn't need the government. Trust is provided by users. As there are many users that in the system, 51 percent of users allow the transaction to be valid. It is totally decentralized. But that approach can't provide reverse transactions. It means we can't fix registration problems which shouldn't be. Likewise Court orders can not be enforced about land registration.

Hybrid blockchain systems mix of private and public systems. It provides public and private characteristics. All users can make transactions but validation is provided by centralised management. There could be managers who are appointed by the government. It can allow us to revert transactions. However information can be seen by everyone.

There are some blockchain projects in the land registry.

In Japan:

In 2018 ,Zweispace , a Japan company that develops applications for the real estate industry, has begun live testing of its patented blockchain-based property registry. On April 2nd the platform officially went to work, recording data from real estate transactions on the Bitcoin Cash (BCH) blockchain.

In 2018 a Japan company Zweispace began live testing of its patented blockchain-based property registry. According to the CEO of Zweispace The company uses that patented blockchain-based property registry as a supplement to the government. They integrate this system into their product which is Ohudokun. Ohudokun's platform registers data such as that necessary to identify the owner of the property; seller data (optional); a timestamp, realtor IDs, and any other required information. The CEO said governments might consider using blockchain for official records. Zweispace wants to use blockchain of their real estate-related products.

In Georgia:

Bitfury created the first-ever blockchain land-registry system in partnership with the Republic of Georgia's National Agency of Public Registry (NAPR) and renowned economist Hernando de Soto.

Bitfury and Republic of Georgia formed to establish a project to strengthen property owners' rights, enhance citizens' trust in government and reinforce data security in 2016. They use a hybrid approach.All the records can be made online.

In Ghana:

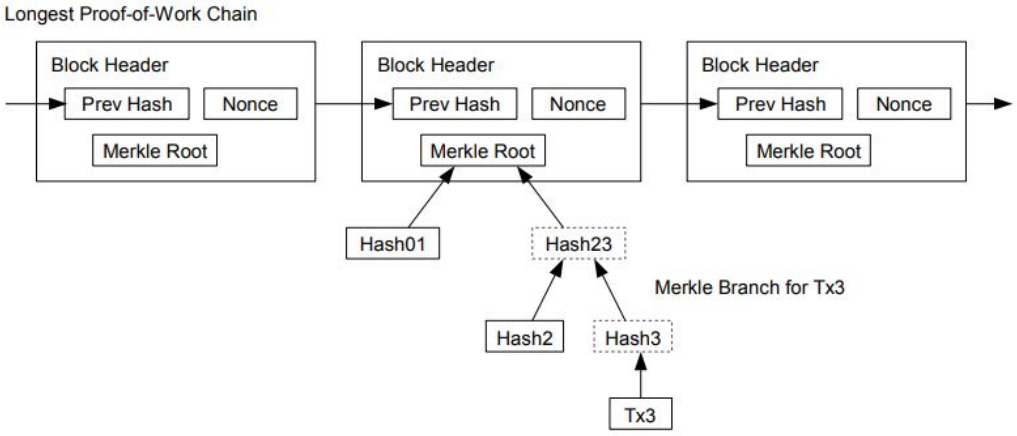
BenBen: is a team of motivated engineers and innovators dedicated to improving government technology in Ghana. BenBen is a digital land database that leverages blockchain technology to provide fast easy access to trusted land content.

3 Analysis

- **Proof of work:**

First of all we need to talk about DMMS. (A Decentralized Blockchain Ledger for the Management of Medication Histories). Although this is a decentralized system we need a clear example for proof of work. Every record on this is encrypted with the receiver user's public key. So only he can open it up with his private key. In our project we consider Simplified Payment Verification Proof (SPV proof).This is a DMMS when an action occurred on Bitcoin-based proof of work blockchain.(Also solution to Byzantine Generals Problem)

SPV will be composed of a list of blockheaders of proof of work and an output was created in one of the blocks in the list.



Therefore the problem is dishonest collusion with greater than 50% of the SPV clients. We can say that “low probability”.

- **Cryptography:**

The whole data (user information, transactions, etc.) must be stored in a confident way. Hashing is a good mechanism that is provided.(SHA-256).

But our blockchain is composed of many cryptographic components, any one of whose failures could cause a total loss of value. (What will happen to manager others).

- **Scalability:**

Larger block size needs larger data centers. Yes we have already said that we need a centralized system. (because we are not authorized to operate the country's land without permission from the state) But our center means that there are some managers; they can be people and also not people. So if our peer centers will grow up too much. This will obviously be a centralized system. Therefore bitcoin supports only a “one size fits all” solution.

- **DAO Hacks:**

It is a fork situation. The failure of the hack spotted a loophole[1] in the DAO’s smart contract and made use of it. 60 million US Dollars were lost[2].(in Ether, the cryptocurrency that is used on Ethereum).

- **Fraudulent transfers:**

This type of problem always happens. If it happens the manager should have considered some cases and decide what it has to do. No reaction or reverse the transaction. In both cases we can't believe it has definitely been resolved in either case.

- **Technical problems:**

---

[1] A description of the DAO-hack can be found here: http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit (Last accessed on October 31., 2016).

[2]See: http://www.forbes.com/sites/francescoppola/2016/06/20/the-dao-hacking-shows-that-coders-are-notinfallible/#33a8791c125d (Last accessed on October 31., 2016).

Transaction malleability is a problem in blockchain which allows arbitrary users to change transaction data in a way that breaks any later transactions which depend on them, even though the actual content of the transaction is unchanged. There is an example of malleability(we can say that flexibility) is probabilistic payments.

4 Proposed Model

4.1 Proposed Model and Purpose

Almost all of us, a family member or someone you know, have gone to the land registry office to buy a house, car, land, etc. If you ask these people about their experience, you will see that they all say that they wait hours for a simple trade and pay a high amount of money even for a small trade. Also, if you decide to buy a property from different countries or cities, this becomes even more difficult and arduous. In addition, since these records are kept in a central system, an error in the system in case of war, earthquake or cyber attack may cause data loss. As an example of this situation, many problems arose because the land registry office was damaged after the earthquake in Haiti. The same situation happened in Iraq as a result of America's attack on Iraq. In addition, the current system has a burden on the state. Many people work at the land registry office and create a salary burden on the state. Also, a lot of paper is wasted for all these processes. Our purpose is to design a model that can be beneficial for both the state and the people to solve these problems. Since making these procedures independent of the state will not be accepted by the state, it is imperative to devise a model that includes the state. The contract on which these transactions will run will belong to the state and the state will charge a certain fee from these transactions. With this model we designed, people will make purchasing and selling transactions much faster and easier. In addition, in this blockchain-based model, records will not be in a single central location, so data loss can be prevented in the event of a cyber attack, natural disaster or a war that I mentioned earlier. In this model, people can do their buying and selling transactions safely. The state takes a certain fee from these transactions as a tax.

4.2 Implementation of Model

First of all, the database that keeps the current title deed status and all the title deed records in the country will be provided by the state. Using the database we can see registered information about the property (address, owner, size etc.). There are two types of users in our model, namely user and manager. Users can view transaction history, balance, property, etc., using an interface. Managers can be compared to miners on a blockchain. It is their responsibility to check and confirm the validity of the transactions made by the users. The user can agree with the owner of the land he wants to buy and make the transactions in a reliable and easy way through the model we designed. The work of evaluation and approval of transactions is done by the managers under the responsibility of the state. Since there will be more than one manager in the system, there is no certain time limitation for the operations to be performed by the users. These operations can be performed at any time of the day and are approved by the managers working in shifts if the transaction is valid. In summary, the user agrees with the owner of the property he wants to buy and signs the purchase using his private key. The property owner signs this transaction with his own private key, indicating that he wants to sell. After both parties sign the transaction, they come to the manager for approval. The sha256 algorithm is used in the manager proof-of-work calculation. If the transaction is valid, they confirm the transaction and the sale transaction is completed. State database is also updated. It is explained in more detail in the Implementation details section.

5 Implementation Details

```
library ECDSA {

  /**
   * @dev Recover signer address from a message by using their signature
   * @param hash bytes32 message, the hash is the signed message. What is recovered is the signer address.
   * @param signature bytes signature, the signature is generated using web3.eth.sign()
   */
  function recover(bytes32 hash, bytes signature)
    internal
    pure
    returns (address)
  {
    bytes32 r;
    bytes32 s;
    uint8 v;

    // Check the signature length
    if (signature.length != 65) {
      return (address(0));
    }

    // Divide the signature in r, s and v variables with inline assembly.
    assembly {
      r := mload(add(signature, 0x20))
      s := mload(add(signature, 0x40))
      v := byte(0, mload(add(signature, 0x60)))
    }

    // Version of signature should be 27 or 28, but 0 and 1 are also possible versions
    if (v < 27) {
      v += 27;
    }

    // If the version is correct return the signer address
    if (v != 27 && v != 28) {
      return (address(0));
    } else {
      // solium-disable-next-line arg-overflow
      return ecrecover(hash, v, r, s);
    }
  }

  /**
   * toEthSignedMessageHash
   * @dev prefix a bytes32 value with "\x19Ethereum Signed Message:"
   * and hash the result
   */
  function toEthSignedMessageHash(bytes32 hash)
    internal
    pure
    returns (bytes32)
  {
    return keccak256(
      abi.encodePacked("\x19Ethereum Signed Message:\n32", hash)
    );
  }
}
```

```
  constructor(string _name, uint _id){
      fee = 10 ether;
      purchasingTime = 10 minutes;
      manager.managerAddress = msg.sender;
      manager.name = _name;
      manager.id = _id;

  }

  function join(string _home,string _telephone,string _name,data _birth, string _ssn, Land[] _ownedLand) public{
      users[msg.sender] = User(msg.sender, msg.value, _home, _telephone, _name, _birth, _ssn, _ownedLand );
      contractBalance += fee;
      users[msg.sender].balance -= fee;
  }

  function selling(uint _id,uint _percentage,uint _price,uint _index) onlyUser public{
      offerTime = now;
      lands.push(Lands(_id, _percentage, _price, users[msg.sender].ownedLand[_index]));
      const messageHash = web3.sha3("approved by seller");
      const signature = await web3.eth.personal.sign(messageHash, web3.eth.defaultAccount);
      sellerHashMessage = signature;
  }

  function buying(uint _id,uint _price) onlyUser public{
      require(users[_addressOfBuyer].balance >= _price);
      for (int i = 0; i < lands.size(); i++){
          if ( lands[i].id == _id){
              const messageHash = web3.sha3("approved by buyer");
              const signature = await web3.eth.personal.sign(messageHash, web3.eth.defaultAccount);
              buyerHashMessage = signature;
          }
      }
  }
```

In the **buying** and **selling** functions: We had used web3.sha3() function to encrypt the transaction. Then we sign the message hash with await web3.eth.personal.sign() function with his private key. Private key is generated by the web3 elements. These functions are called by the users.

```
function verification (address _addressOfSeller,address _addressOfBuyer,uint _index,uint _price, uint _percentage, bytes _signatureOfSeller,
bytes _signatureOfBuyer) onlyManager public{
    require(offerTime <= purchasingTime);
    bytes32 hashSeller = keccak256(abi.encodePacked(uint256(_addressOfSeller)));
    bytes32 messageHash = hash.toEthSignedMessageHash();
    bytes32 hashBuyer = keccak256(abi.encodePacked(uint256(_addressOfBuyer)));

    address signerSeller = messageHash.recover(_signatureOfSeller);
    address signerBuyer = messageHash.recover(_signatureOfBuyer);
    require(signerSeller == _addressOfSeller);
    require(signerBuyer == _signatureOfBuyer);

    users[_addressOfSeller].ownedLand[_index].shareOwned[_addressOfSeller] -= _percentage;
    users[_addressOfBuyer].ownedLand.push(users[_addressOfSeller].ownedLand[_index]);
    users[_addressOfBuyer].ownedLand[_index].shareOwned[_addressOfBuyer] += _percentage;

    users[_addressOfSeller].balance += _price;
    users[_addressOfBuyer].balance -= _price;

}
```

Verification function is done to formalize the operations performed by the government appointed managers.The manager confirms that the transaction was signed by both the owner and the recipient by decoding the message they sent. To decode the message, we used the ECDSA library, which can also be used in solidity. If the transaction is valid, the necessary money transfer takes place and the property sale becomes official.

6 Result

Advantages:

Enables transactions to be processed at any time.
It allows the landowner to sell a certain percentage of his land without selling all of his land. For example, the landowner can put 5% of his land up for sale.
Everyone can see the blocks and if someone wants to change a block, this block will be invalid but other users' blocks will be valid.
Corruption and bid rigging can also be detectable. If you can figure out who is the owner of that key.
The government will manage all processes efficiently.(expenditure of employees, government offices are unnecessary in our system)
Blockchain technology will prevent the insecurity and injustice that are part of these land registries.
This system will be adapted for the new world because everyone uses new technology,new methods for business.
Paperwork will be reduced explicitly,government offices use many papers just for only one work and cause environmental pollution for these reasons.This system will reduce pollution.

Disadvantages

Land registration can not be **decentralized**; States would not let their own land be sold without its permission.
If the government lets the first **clause**:Unemployment will rise.Because many people will be redundant. Also; politically, it will cause loss of votes.

State provides **reliability**. If fraud occurs due to some sickness such as Alzheimer, no one can help.
If anyone will forget their own private key,it will be a critical issue and this will cause complexity for those people.

7 Conclusion

In this project,we struggle to rearrange land registry processes for primarily our country.People can pay less money than previous times and they can save their time.Nowadays they struggle to find suitable time but unfortunately they won’t find the best time for complete their works.In recent years,the world is changing to digital world,for this reason we can catch them using with new technology such as blockchain.Our project provide all of these.

We have designed a solution that can benefit both the state and the public by using blockchain technology to solve all these problems and facilitate people's transactions.We have designed a solution that can benefit both the state and the public by using blockchain technology to solve all these problems and facilitate people's transactions.