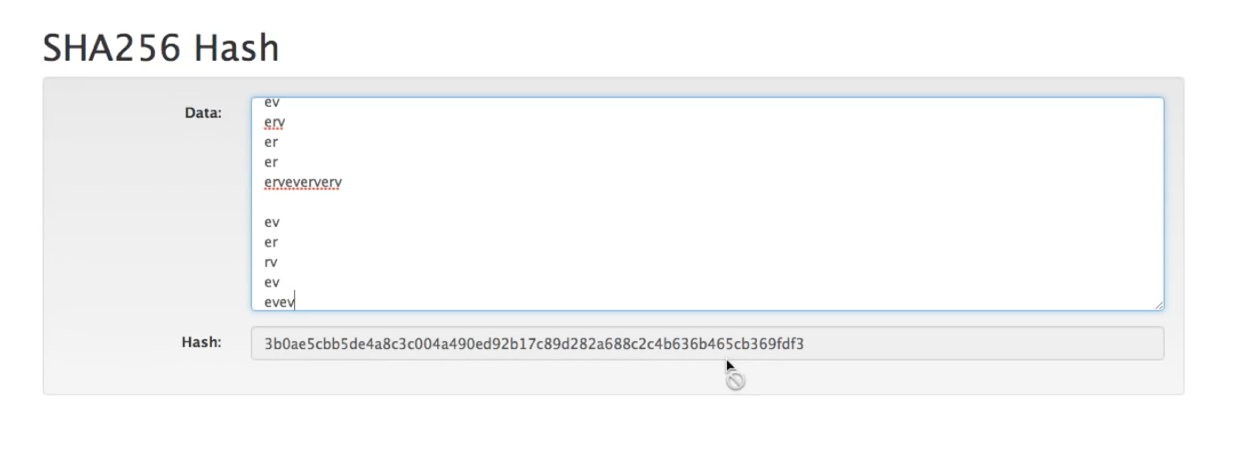
Bitcoin Assignment 2 (Day 3)

1. Experiment with Adners Blockchain

* SHA256 Hash

It is used to encrypt the given data into random letters and numbers. It is a fingerprint to every data. Even with the slight change of the data, the hash would change



* Block

We have to extend this idea into a block. Block looks similar to SHA256 but data is blank and begins with 4 zeros which makes the block assigned or valid. If we put something in data, then the block may not become assigned or valid as the initial 4 zeros may get changed.

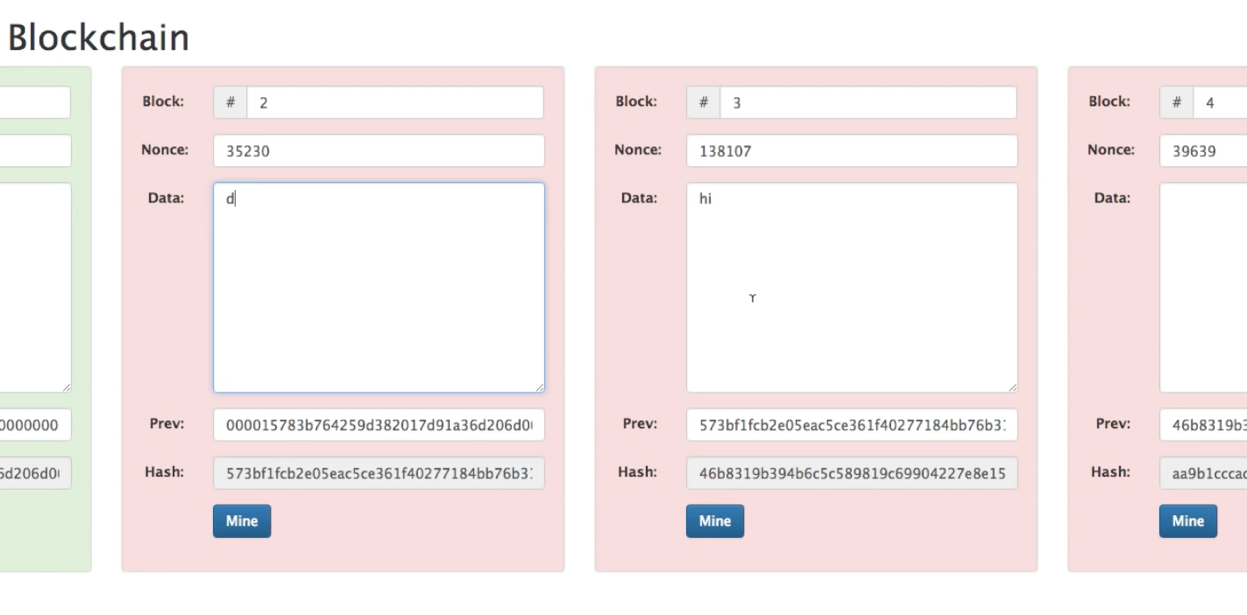


Hence, we need nonce. By changing nonce, we can make the hash start with 4 zeros but manually it will take a long time. Hence, we need to use ‘mine’ and it will give the exact number for the ‘nonce’ for the hash to start with 4 zeros



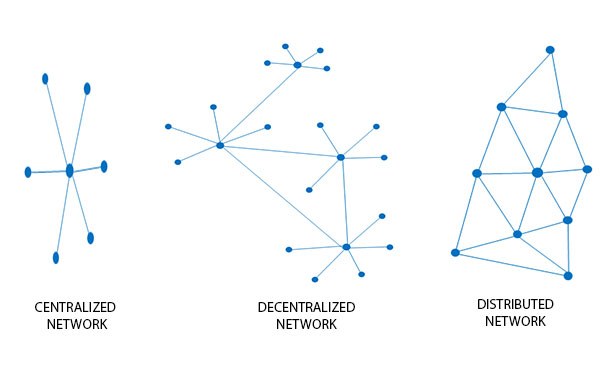
* Blockchain

It contains a series of blocks; the next block will have previous blocks hash as well and other properties remain the same. If we change the any previous block’s data, the next blocks will break. So, we need to mine that block and the next blocks as well.



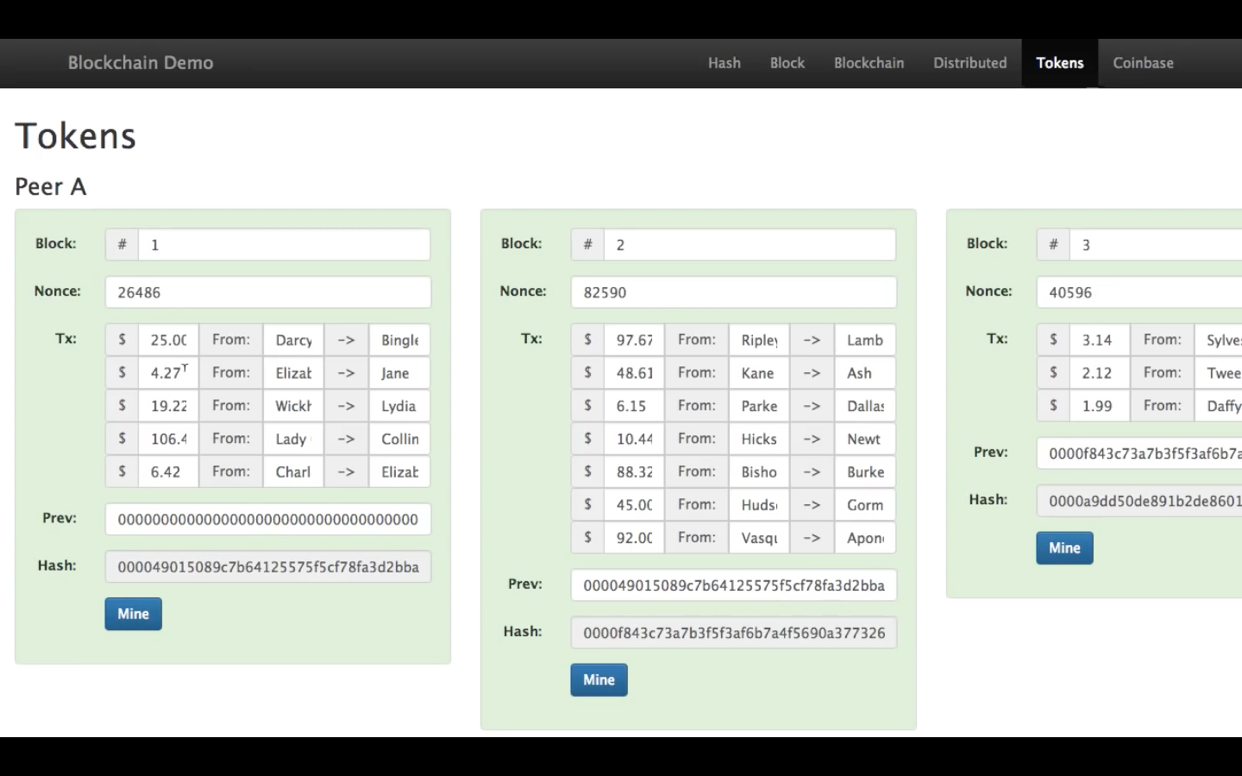
* Distributed Blockchain

They share the same blockchains in various peers or systems. Even after we change the data and mine it a particular blockchain, the hash should also be the same in that chain otherwise they are not identical which could indicate that the blocks have been altered.

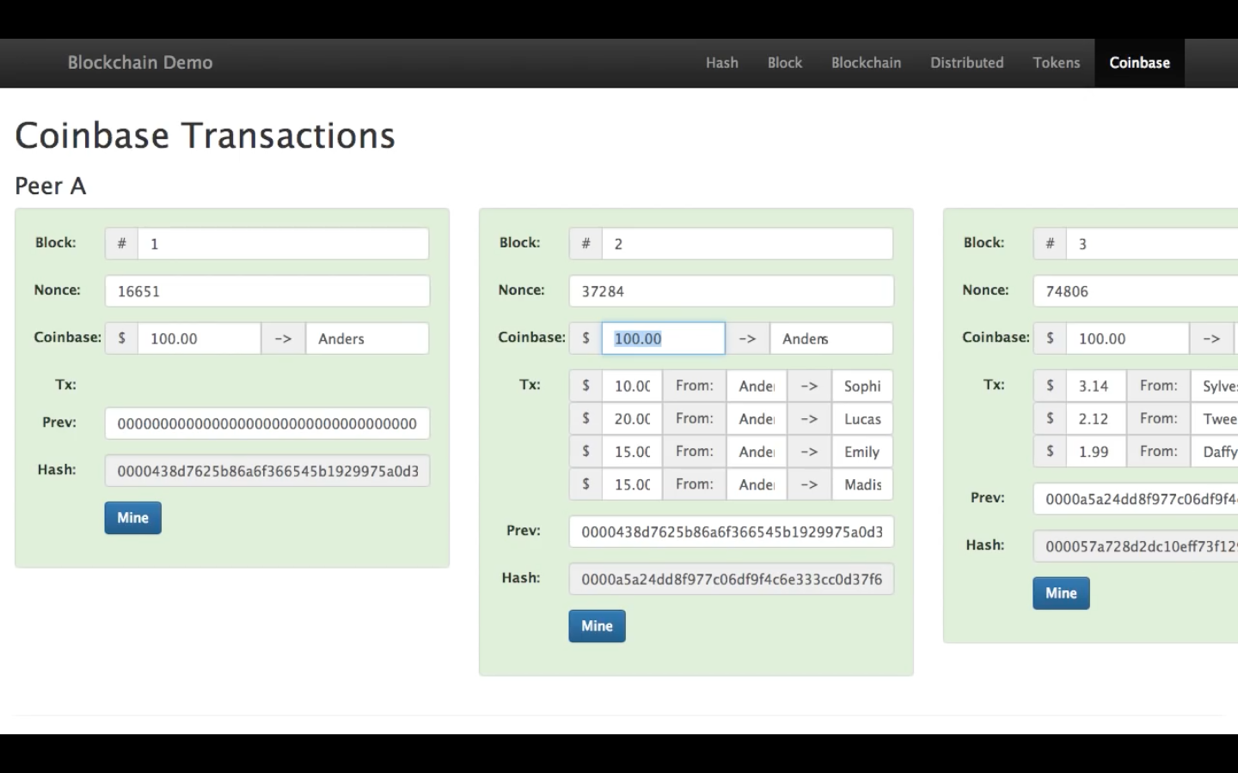


* Token

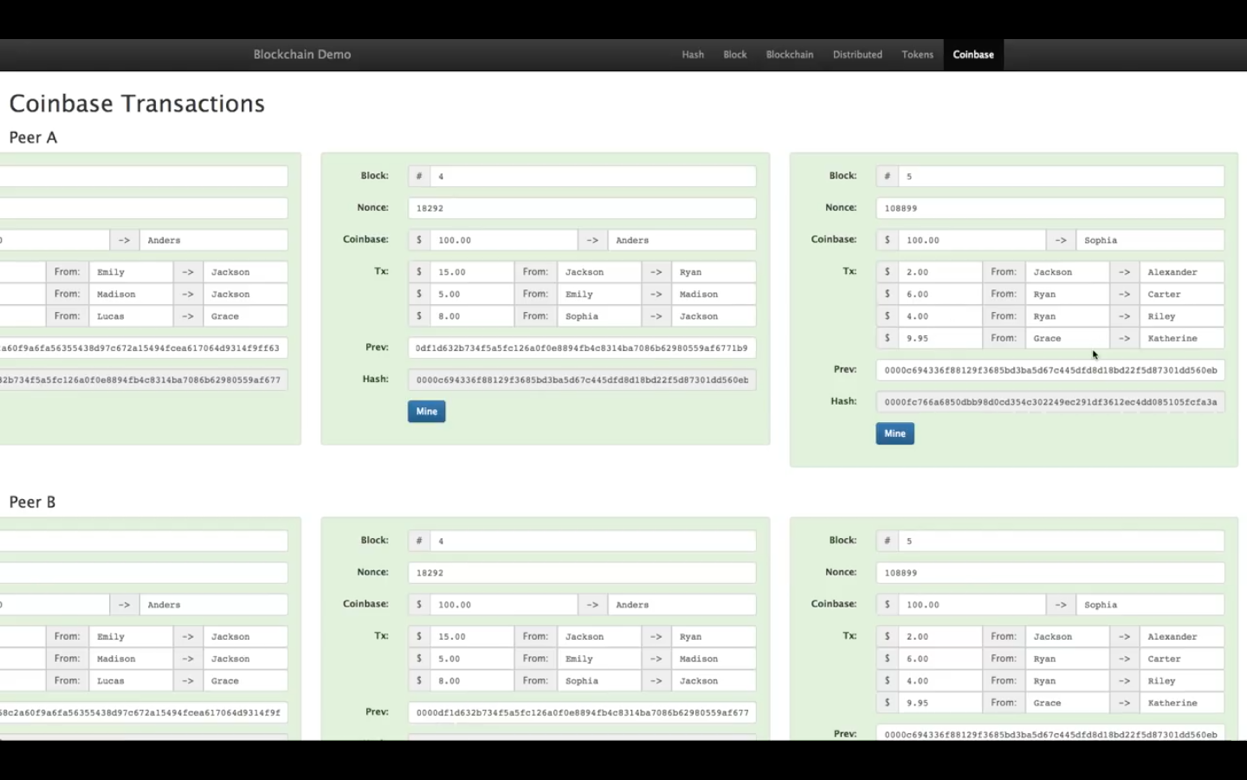
It shows the transaction data in every block of the blockchain instead of data. That’s the real reason why we use blockchain distributed network as the altered data could be easily verified and tracked by the peer network. Only money transfer is recorded and not other details such as the bank records.



* Coinbase Transaction



We aren’t sure if the person doing the transaction has any money. Hence, we put the first block such that only a certain amount is transferred to a person and no other transaction is present. This is called as Coinbase transaction. That’s why we need previous hash to trace the providence of the coin transfer.



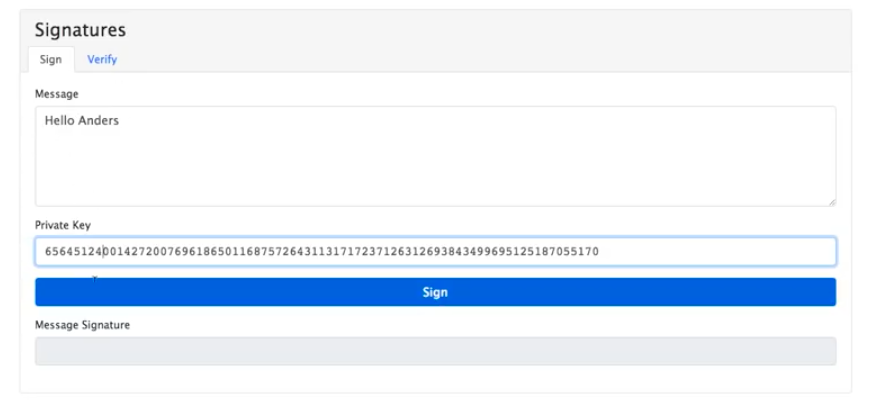
* Public and Private Keys

Public key is available to everyone and this has potentially no risk if anyone knows about it. Private key is available to only specific people.



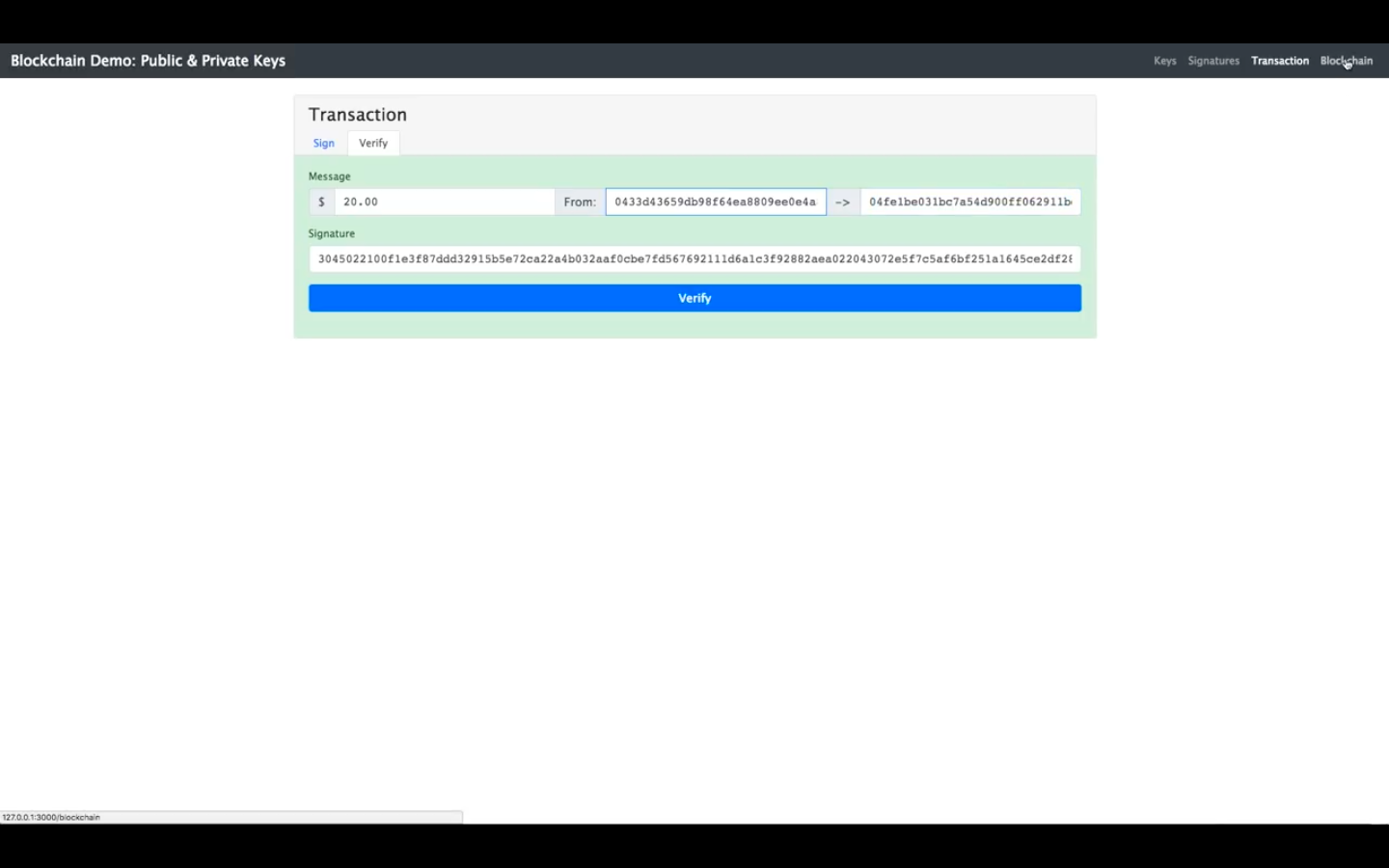
* Signatures

A message is to be revealed. We have the public key. We need to enter a correct signature or private key to access the message.

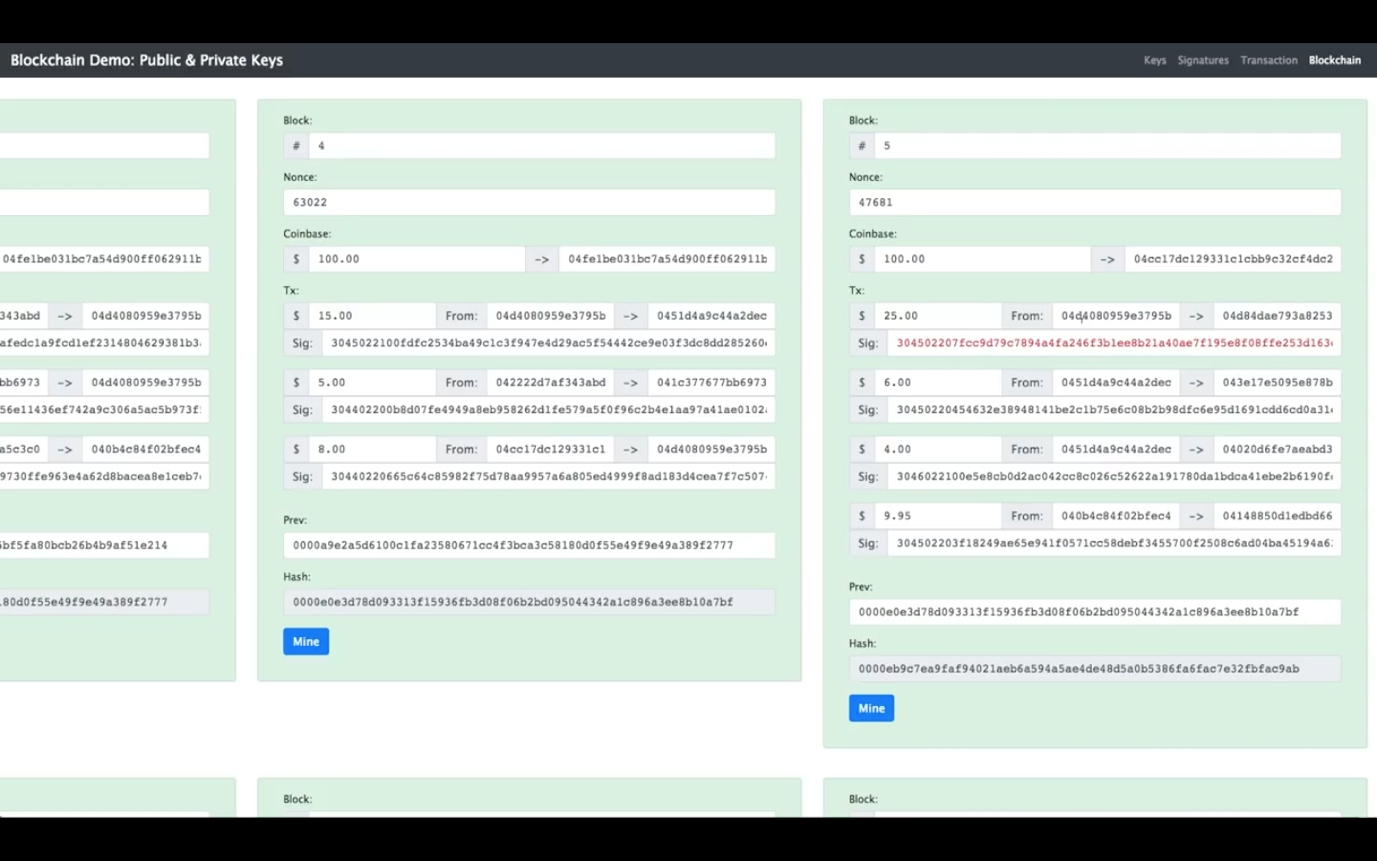


* Transaction

We use signatures to ensure safe transaction of an amount of money. That amount of money is transferred from one public key to another public key. We have the private key as we are signing this transaction. After signing, we get a message signature. This is used to verify the user who is sending the money.



We need to use these concepts in the blockchain. When someone changes the transaction and mines the block, the block may become valid but the signature is still invalid. Only the true user knows the private key



2. Make a sample smart contract on remix.ethereum.org and publish it in your github

pragma solidity >=0.4.17 <0.7.0;

contract Land{

string OwnerOfTheLand;

string addressOfLand;

function Land( string newOwner ) public{

OwnerOfTheLand = newOwner;

}

function setDetails( string newOwner ) public{

OwnerOfTheLand = newOwner;

}

function getDetail() public view returns(string){

return(OwnerOfTheLand);

}

}