Important notes - Blockchain

Ethereum network consists of many nodes. These nodes are any machines. There are many types of networks in Ethereum. Each of the nodes contain the whole copy of blockchain.

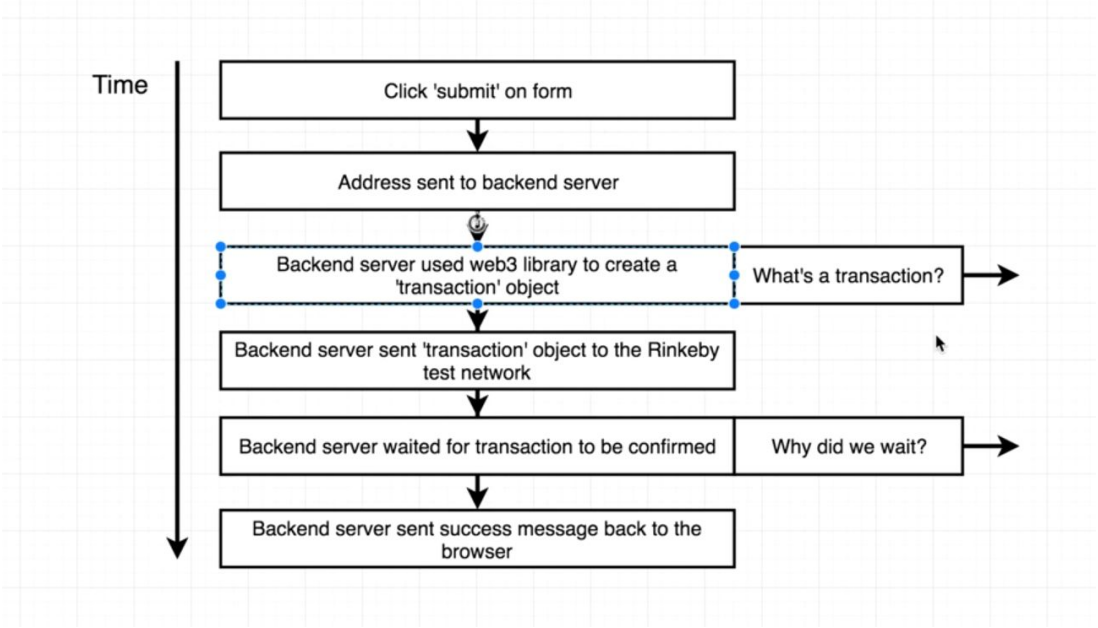
Blockchain - It can be described like a database that consists of all the transactions upto that point of time.

Metamask - A chrome extension to create an account in an ethereum network
Metamask consists of :-

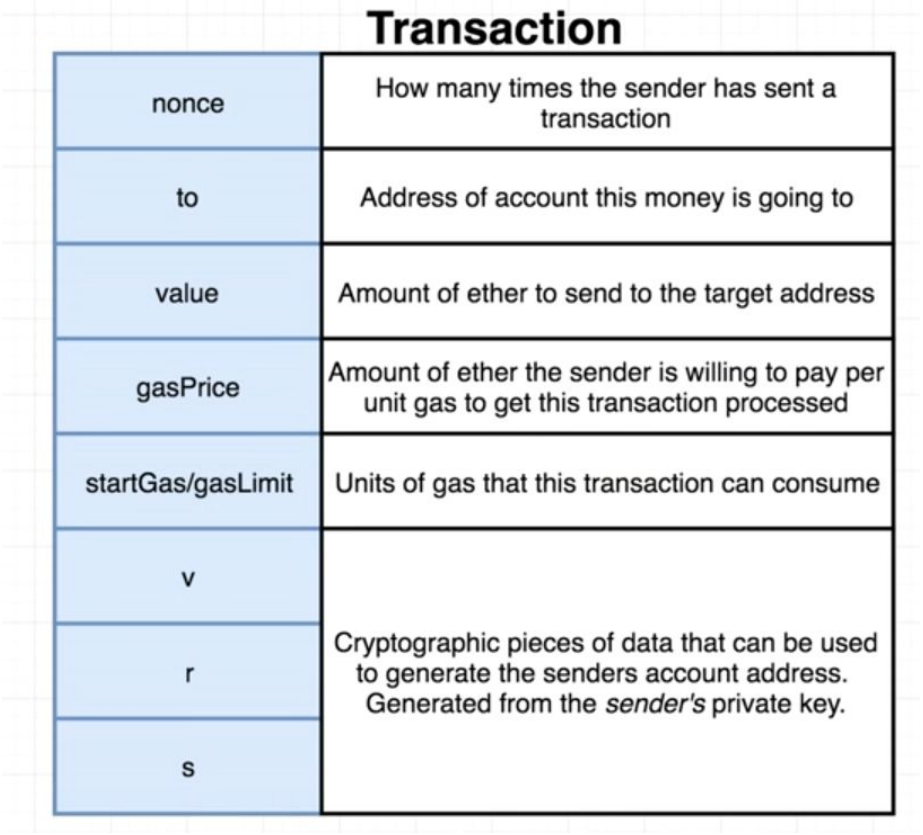
1. **Account address -** It is the address that uniquely Identifies our account in the network.
2. **Public key and Private key -** Combined together to form a password kinda thing.Authorize sending of fund from our account to the other account.**Private key shouldn't be shared.**

The above two are stored as hexadecimal numbers.

- One account is going to connect to all the ethereum networks out there. Like the Main network, Ropsten network, Kovan network, Rinkeby network….
- Secret Backup phrase example : "tray business sadness raven club come badge photo tuition adjust blouse illness"
- Account address : "0x432a101A3DAb074d1EeFA5EF8f6B4BCe10F75f08"
- For testing purpose of transaction to Rinkeby network use http://rinkeby-faucet.com. Here the ether is send only to this network. And none to the other networks.
- The process happening in Rinkeby-faucet.com.



What is a transaction ?



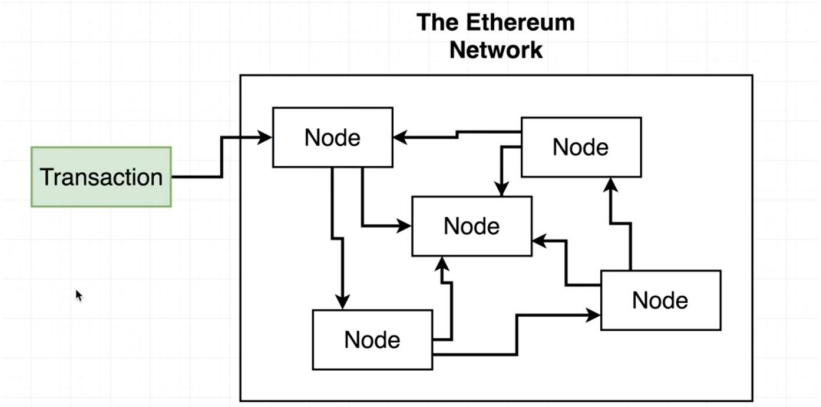
Transaction

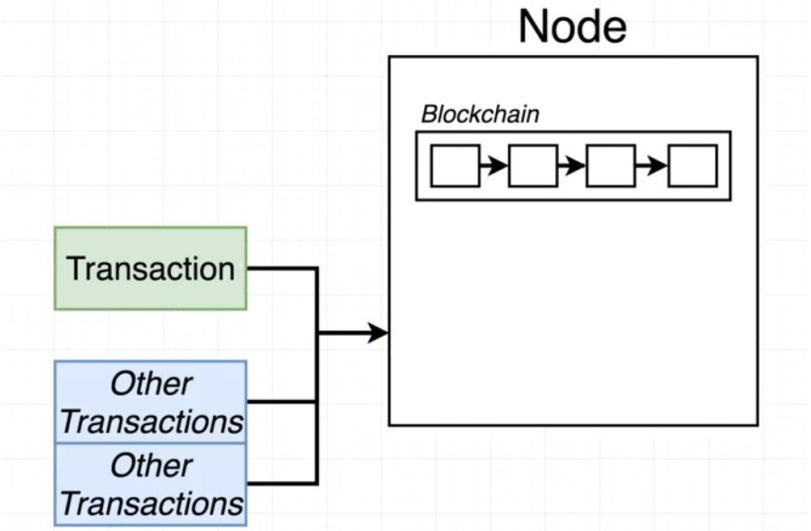
nonce	How many times the sender has sent a transaction
to	Address of account this money is going to
value	Amount of ether to send to the target address
gasPrice	Amount of ether the sender is willing to pay per unit gas to get this transaction processed
startGas/gasLimit	Units of gas that this transaction can consume
v	Cryptographic pieces of data that can be used to generate the senders account address. Generated from the *sender's* private key.
r	
s	

Why do we wait ?

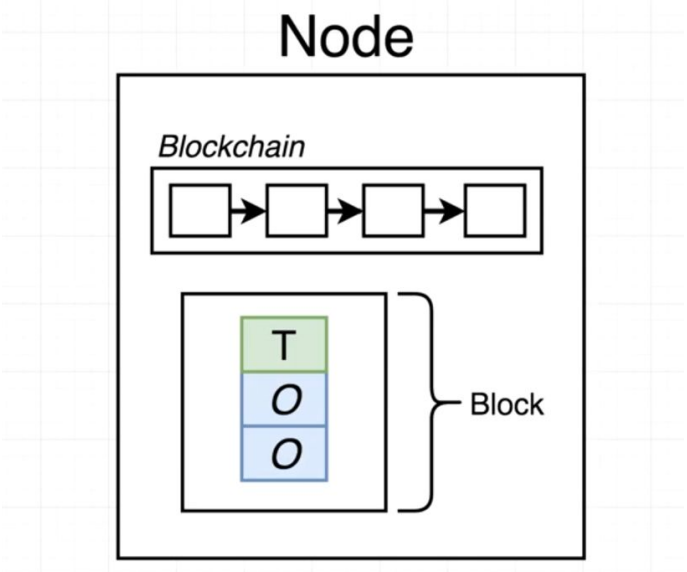
- We send the transaction to one particular node in the ethereum network.
- There can be more than one transaction at the same time.All these transactions are grouped together and made into a list and stored into a block which is stored in the node. The node then runs some validation logic on this block . This running of validation logic is called the **Mining.**

-





-



Doubt : Are all the transactions done on a network going on the same node. And by node do you mean the machine ? So if it's the machine then its our account right ?

- **To Know more about how blockchain works visit :** https://anders.com/blockchain/coinbase.html
- **Block time -** The total time required to find a solution. That is, the total time required to find a output hash such that it's corresponding base 10 number is less than a particular target value specified.

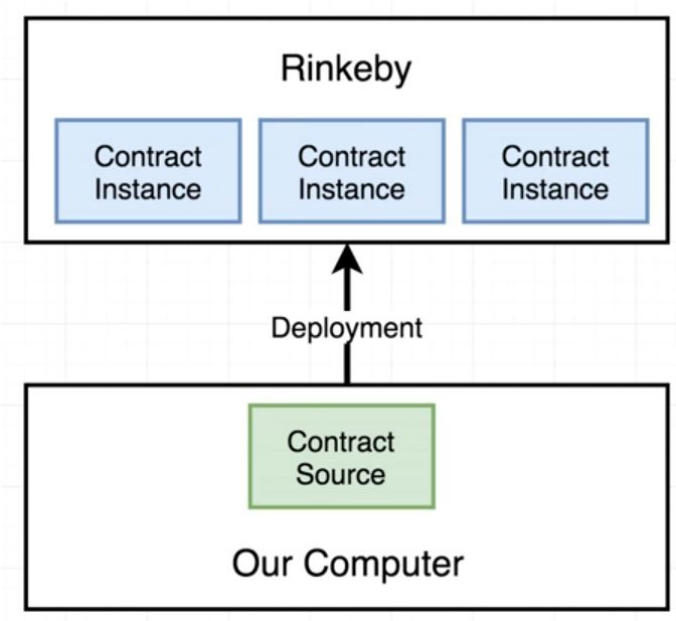
Smart Contract

Account controlled by code.

Contract Account	
Field	Description
balance	Amount of ether this account owns
storage	Data storage for this contract
code	Raw machine code for this contract

Types of accounts:

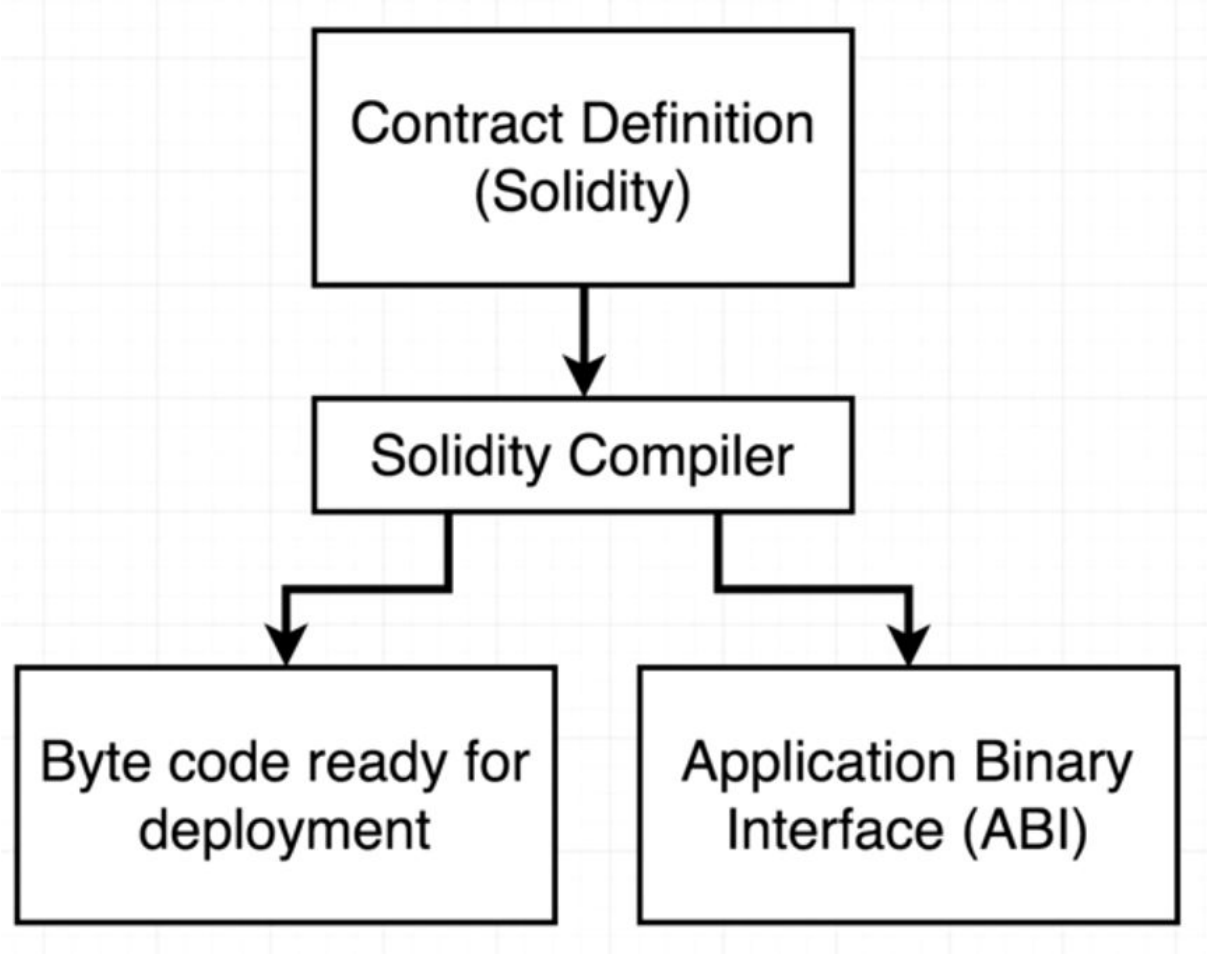
1. External accounts - Owned by Human beings
2. Contract account - Account controlled by code spread across only one network unlike the External accounts.



Solidity Programming Language

- Extension is .sol
- Similar to JS
- Strongly typed language(Unlike JS which is Dynamically Typed)
- Has big **Gotchas**

What we do with solidity :



Sample contract using solidity :

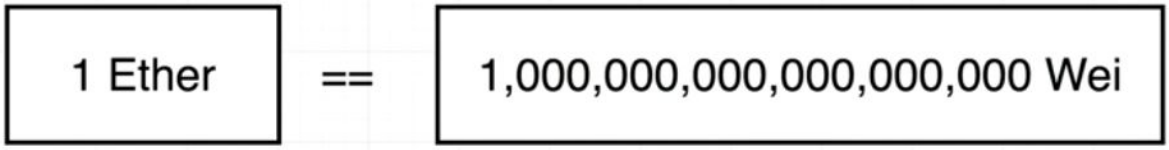
```
pragma solidity ^0.4.17;/* Version of solidity  */

/* Similar to class */

contract Inbox {
    string public message;/* Storage Variable  */
    /* Functions that control the Storage variable  */

    function Inbox(string initialMessage) public {
        message = initialMessage;
    }

    function setMessage(string newMessage) public {
        message = newMessage;
    }

    function getMessage() public view returns (string) {
        return message;
    }
}
```

Now we will deploy an Instance of this contract In-browser fake network using Remix IDE : http://remix.ethereum.org/

Wei vs Ether

- Sending a transaction to a function will **cost some amount of ether.**

So what is WEI ?



This will be useful for conversion and stuff : https://etherconverter.online/

- **So what is GAS ?**
  Gas is something like For each mathematical operation in the contract you make it is going to cost some units of gas to you. Using this gas we can calculate the amount of **Wei** It is going to cost.

gasPrice	Amount of Wei the sender is willing to pay per unit gas to get this transaction processed
startGas/gasLimit	Units of gas that this transaction can consume

gasPrice	300

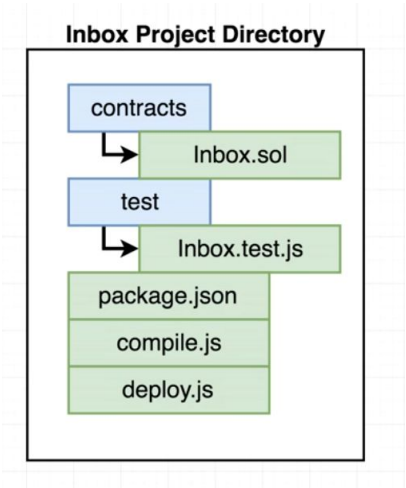
Used 14 gas

$$\text{Total cost} = 300 \frac{\text{wei}}{\text{gas}} \times 14 \text{ gas} = 4{,}200 \text{ wei}$$

- **Mnemonics are those weird words given by metamask when we create a new account. Using those mnemonics we can know the possible address and Public keys possible for that particular mnemonic given by metamask (<u>Basically helps in deriving the address and the public keys).</u>**

TRUFFLE

- So what is truffle ? It is basically a tool which helps us in **deploying smart contracts**.
- And for testing we are going to use **Mocha test library.**
- So the project directory of our first project using solidity will be as follows


Inbox Project Directory
contracts
Inbox.sol
test
Inbox.test.js
package.json
compile.js
deploy.js