Ethereum and Solidity - The Complete Developer's Guide

Section 1. What is Etherium

- **31-Oct-2008 White Paper about Bitcoin**
  - https://bitcoin.org/bitcoin.pdf
  - Jan-2009 Bitcoin was launched

- **Dec-2013 White Paper about Ethereum by Vitalik Buterin**
  - http://web.archive.org/web/20131228111141/http://vbuterin.com/ethereum.html
  - 👍 Introduced the idea of Smart Contract
  - 30-Jul-2015 Ethereum was launched

An Ethereum Network
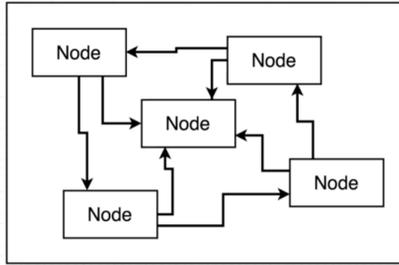
Ethereum networks are used to transfer money and store data
There are many different Ethereum networks.
Networks are formed by one or more nodes.
Each node is a machine running an ethereum client.
Anyone can run a node.
Each node can contain a full copy of the blockchain
The 'blockchain' is a database that stores a record of every transaction that has ever taken place

### Transaction

| Field	Description
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	

Transaction fields

v, r, s identify FROM

- 👍 **Visual demo of blockchain technology** — https://andersbrownworth.com/blockchain/
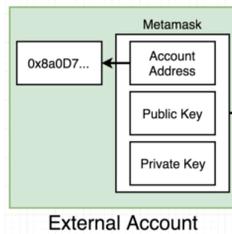
External Account

External Account exists on all networks.
Contract Account exists on one specific network

Contract Account

Field	Description
balance	Amount of ether this account owns
storage	Data storage for this contract
code	Raw machine code for this contract
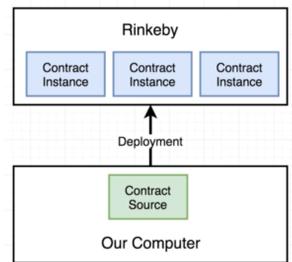
Contract Account should be deployed to the network
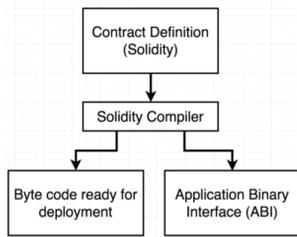
- **IDE for writing Ethereum smart contracts** — https://remix.ethereum.org/

- **Contract creation transaction** — Is a transaction with some extra
  - To = <empty>
  - Data = <compiled code>

Running Contract Functions

'Calling' a Function	Sending a Transaction to a Function
Cannot modify the contract's data	Can modify a contract's data
Can return data	Takes time to execute!
Runs instantly	Returns the transaction hash
Free to do!	Costs money!

Two ways of calling functions on blockchain

- Changing anything = transaction
  - ⚠️ Cannot return value - it returns transaction hash!
  - ⚠️ IT TAKES TIME! (if run on public networks)
- Reading data (no changes to blockchain) is fast and free

Operation costs

- 1 ether = 10^18 wei
- https://docs.google.com/spreadsheets/d/1n6mRqkBz3i-WcOlRem_mO09GtSKEKrAsfO7Frgx18pNU/edit#gid=0
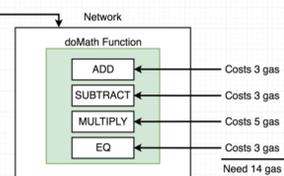
Total cost = 300 $\frac{wei}{gas}$ X 14 gas = 4,200 wei

- **12-word mnemonic phrase**
  - A more convenient way to manage multiple accounts via MetaMask
  - https://iancoleman.io/bip39/

- **How to get Ether on test nets**
  - https://faucets.chain.link/rinkeby
  - https://faucet.rinkeby.io/
  - https://faucet.ropsten.be/