Ethereum Platform

Raza Sikander & Chitresh G
C-DAC Hyderabad

Outline

- Ethereum Overview
- Ethereum History
- Terminology & Tools
- Smart Contract Development

Ethereum Overview

Ethereum Overview

- Public Blockchain
- Permissionless
- Consensus: PoW/PoS
- Cryptocurrency
- First to bring in Smart Contracts on Blockchain

Public vs Private Blockchain

Public	Private
Open - Any one can join the network	Restricted - Only invited member can join the network
Each node has equal transmission power	Only certain node can create new transaction
Low speed of transaction accomplishment	Fast speed of transaction accomplishment
Participants are anonymous	Identities are known
Slow transaction speed	Fast transaction speed
Large energy consumption	Low energy consumption

Permissioned vs Permissionless

Permissioned	Permissionless
Require permission to join and interact with consensus	No permission is required to join and interact
Private membership	Transparent and open
Managed by group of nodes	No one owns the network
Faster	Slower

Cryptocurrency

Cryptocurrency is a digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority.

The word “cryptocurrency” is derived from the encryption techniques which are used to secure the network.

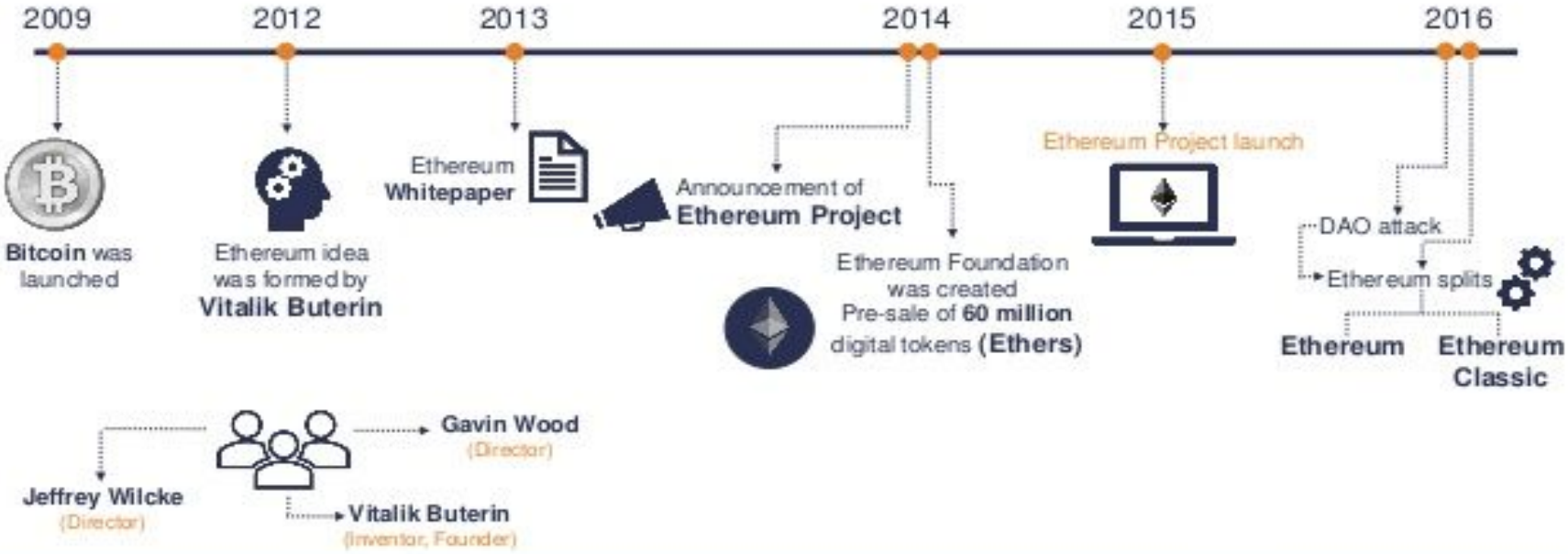
Smart Contract

- A smart contract is a computer program or a transaction protocol which is intended to automatically execute or control legally relevant events and actions according to the terms of a contract or an agreement.

Ethereum and other platforms

- It’s not just a currency, it’s an environment
- Anyone can take advantage of this platform to build
  - projects and DApps(decentralized applications)
  - through smart contracts

The birth of Ethereum



Source : https://www.slideshare.net/cordieliea/binarycom-what-is-ethereum-and-how-does-it-work

DAO

- A decentralized autonomous organization (DAO), sometimes labeled a decentralized autonomous corporation (DAC)
- DAO is an organization represented by rules encoded as a computer program that is transparent, controlled by the organization members and not influenced by a central government.

How a DAO works

- A group of people writes the smart contracts (programs) that will run the organization
- There is an initial funding period, in which people add funds to the DAO by purchasing tokens that represent ownership – this is called a crowdsale, or an initial coin offering (ICO) – to give it the resources it needs.
- When the funding period is over, the DAO begins to operate.
- People then can make proposals to the DAO on how to spend the money, and the members who have bought in can vote to approve these proposals.

DAO Attack

- On June 17, 2016, the DAO was subjected to an attack exploiting a combination of vulnerabilities, including the one concerning recursive calls.
- One hacker spotted a flaw in the DAO's code and managed to drain 3.6 million Ether into a personal account
- Around a third of the 11.5 million Ether that had been committed to The DAO - valued at the time at around $50M.

Hard Fork and Soft Fork

Soft Fork:
With a soft fork, only one blockchain will remain valid as users adopt the update.

Hard Fork:
both the old and new blockchains exist side by side, which means that the software must be updated to work by the new rules.

Ethereum vs Ethereum Classic

- Ethereum Classic (ETC) is the original Ethereum blockchain.
- ETH and ETC share the same blockchain record before the July 2016 hard fork.
- Because of that, the initial design and functionality of these two networks were essentially the same.
- The hard fork in 2016 split the blockchain into Ethereum Classic and Ethereum, dividing the community at the time.
- Most developers chose to upgrade to the new Ethereum protocol, limiting the size of the ETC community and its ability to improve the network.

DApps

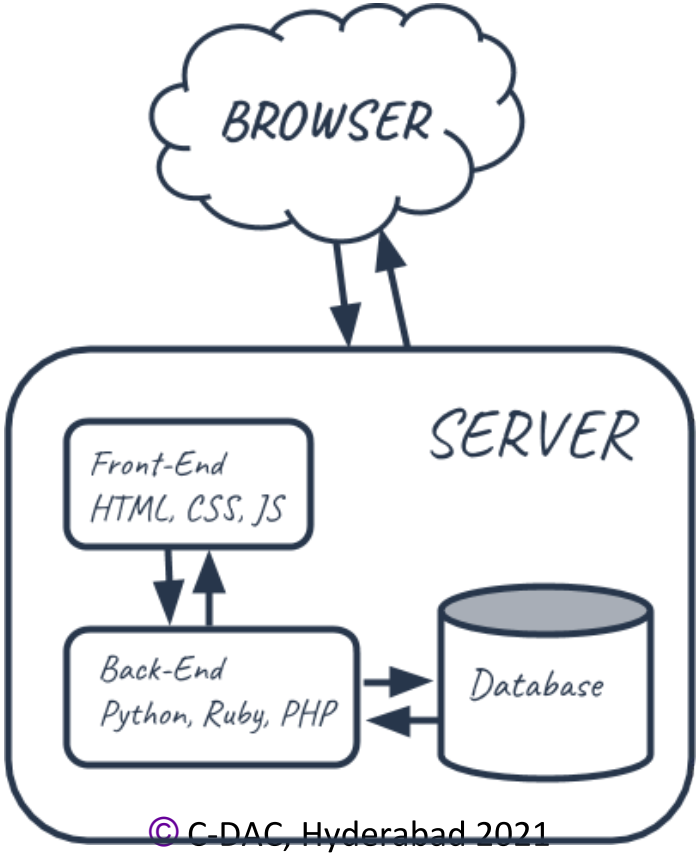
Traditional Web Application

- A web application (or web app) is application software that runs on a web server, unlike computer-based software programs that are run locally on the operating system (OS) of the device.

- Web Applications are centralized software programs that are stored on remote servers controlled by a host, better known as “the cloud”.

- Web applications are accessed by the user through a web browser with an active internet connection.

Traditional Web Application



Issues of Traditional Web Application

- Data can altered
  - Overwrite data
  - Delete data
- Rules can be altered
  - Code logic

Eg. Voting App

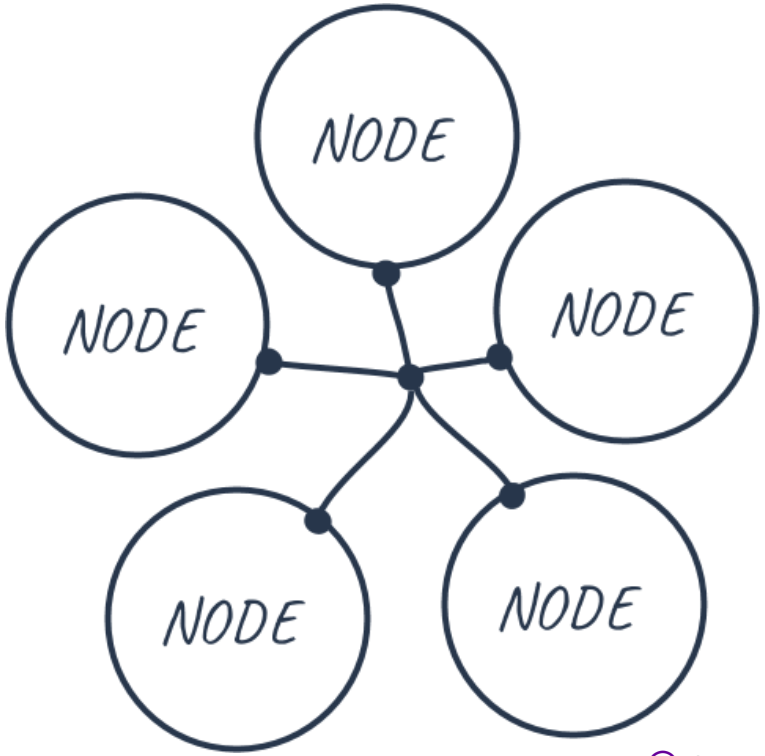
- Data can altered
  - Overwrite data (Votes can be changed)
  - Delete data (Votes can be deleted)
- Rules can be altered
  - Code logic (Change the code to make the candidate with least votes win)

What is DApp?

- DApp is short for 'decentralized app'.
- This means it's stored on thousands of nodes, rather than a single database
- Peer to Peer
- Data is shared
- Code is shared

- It is open source with autonomous features
- Uses an immutable public ledger to store data
- Cannot be deleted and can only be modified through user consensus
- Can connect two users without the need for a ‘middle man’;
- Can allow users to maintain privacy using their private keys.

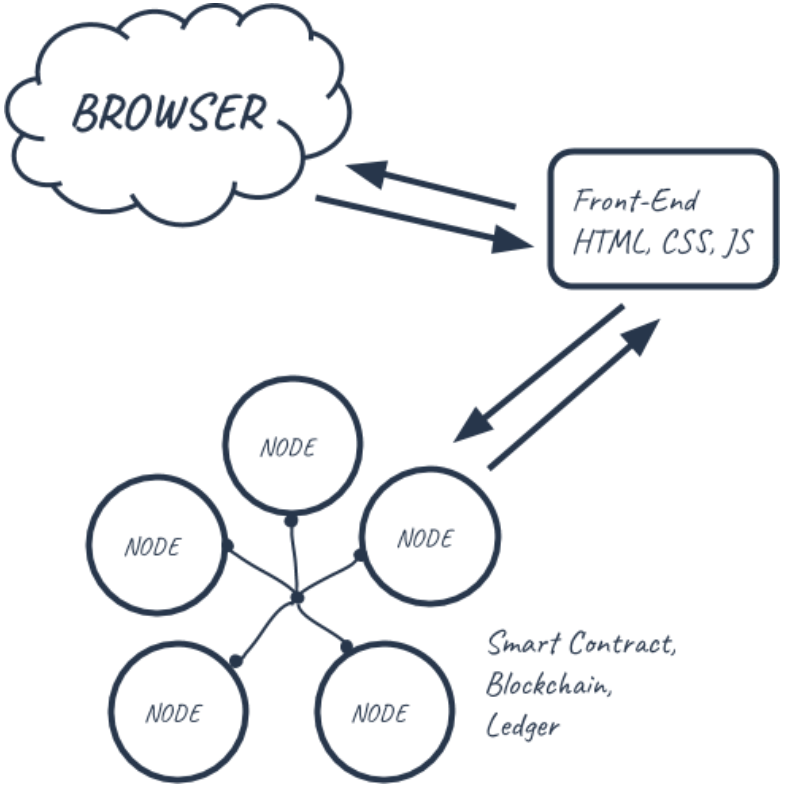
Decentralized Apps (DApps)



. It's a Database
. It's a Network

. Code
. Shared
. Tamperproof

Typical Dapp Structure



Pros

Web Apps	DApps
• User-friendly, even for a non-technical person. • Easy to develop since they work on all browsers. They are also available on every device and easy to access. • They can be designed to the specific requirements that match user needs and objectives. This also allows developers to be creative and offer better products.	• Decentralised, peer-to-peer validation, blockchain-based applications that makes them scalable. • They are open-source applications. Developers can make changes and bring value to the app for everyone's benefit. • They don't crash and cannot completely die from any technical errors. They remain available all the time because of their peer-to-peer network. • Blockchain, Proof-of-Work, and Smart Contracts help make it trustworthy, reliable and impossible to hack. • There is no central authority or a third party that controls the app, making it faster and safer.

Cons

Web Apps	DApps
• Data is stored on servers, hence central points of failure. This means they can be hacked and tampered with. • It only stores value, it does not allow the creation of value, like cryptocurrencies. • Third party involvement is highly time-consuming. Also, information exchanged with outside parties is not encrypted so it can be tampered with.	• DApps are very slow and transactions take a very long time. At the moment, they can only process an estimate of 15 transactions per second. • The compensating system means that DApps charge a small fee each time a user wants to use it. • Blockchain makes it impossible for a DApp be taken down from a network. The only way to that would be to shut down the network completely.

Consensus Basics

Consensus

A consensus mechanism is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies.

Consensus Types

- (PoW) Proof of Work (Bitcoin, Ethereum, ...)
- (PoS) Proof of Stake (Ethereum in Future)
- (PoI) Proof of Importance (used in NEM)
- (PBFT) Practical Byzantine Fault Tolerance (Hyperledger Fabric)
- (FBFT) Federated Byzantine Fault Tolerance (Ripple, Stellar)
- (DPoS) Delegated Proof of Stake
- (PoET) Proof of Elapsed Time (Hyperledger Sawtooth)

Proof of Work

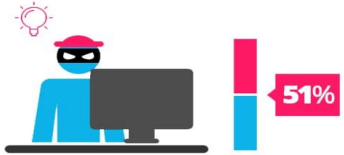
- Proof-of-Work, or PoW, is the original consensus algorithm in a Blockchain network.
- In Blockchain, this algorithm is used to confirm transactions and produce new blocks to the chain.
- With PoW, miners compete against each other to complete transactions on the network and get rewards

Proof of Stake

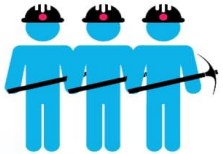
- Proof of stake (PoS) is a type of consensus algorithm
- which a cryptocurrency blockchain network aims to achieve distributed consensus.
- It also states that a person can mine or validate block transactions according to how many coins he or she holds

Proof of Work vs. Proof of Stake

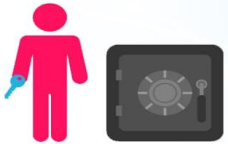
To add each block to the chain, miners must compete to solve a difficult puzzle using their computers processing power.



In order to add a malicious block, you'd have to have a computer more powerful than 51% of the network.



The first miner to solve the puzzle is given a reward for their work.



There is no competition as the block creator is chosen by an algorithm based on the user's stake.

In order to add a malicious block, you'd have to own 51% of all the cryptocurrency on the network.

There is no reward for making a block, so the block creator takes a transaction fee.

Source: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

Terminology

Terminology

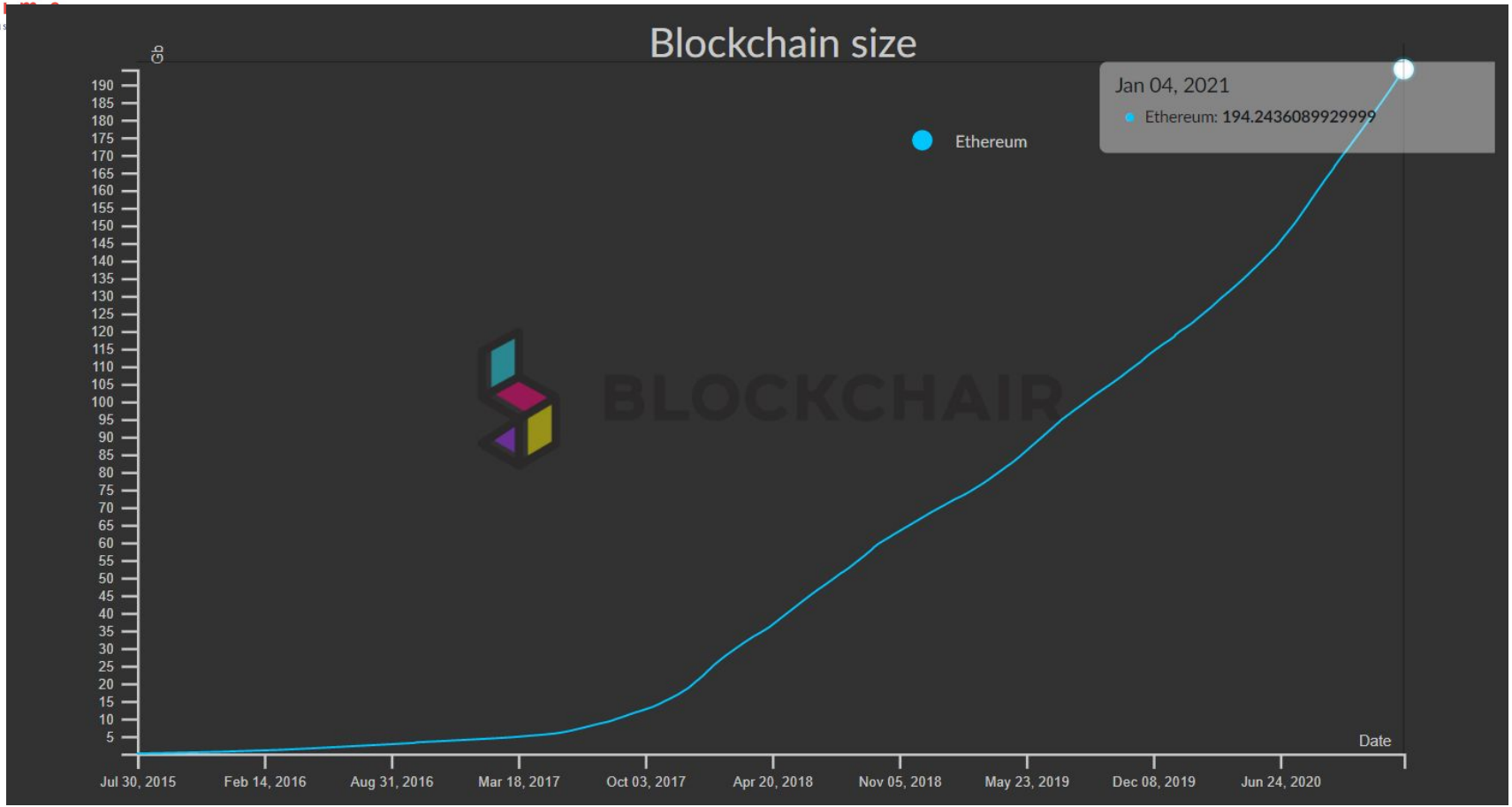
- Ethereum Units
- Nodes
- Wallets
- Ethereum Virtual Machines (EVM)
- Solidity
- Transactions

Ethereum Units

Unit	Wei Value	Wei
wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
milliether (finney)	1e15 wei	1,000,000,000,000,000
ether	1e18 wei	1,000,000,000,000,000,000

Ethereum Nodes

- Full Nodes download the whole chain
  - Very large (195Gb as of Jan 2021)
  - Resource intensive
  - Not possible on low end hardware (mobile, embedded)
- Light Ethereum subprotocol
  - Only headers are fetched (1KB / 2 sec)
  - Only fetch data concerning the client
  - Full functionality in terms of safely accessing the blockchain



Source:
https://blockchair.com/ethereum/charts/blockchain-size

Accounts

- External accounts (wallet)
  - can send transactions to the blockchain
  - transactions can simply transfer ETH
  - or they can call contract functions
  - or they can create contracts
  - controlled by private keys

- Contracts
  - can send messages to other contracts
  - can have functions executed via transactions and messages
  - do not have private keys
- Ethereum Address
  - Derived from Public Key

EVM

- Every node contains a virtual machine (similar to Java)
  - Called the Ethereum Virtual Machine (EVM)
- Executes smart contract code and broadcasts state
- Every full-node on the blockchain processes every transaction and stores the entire state

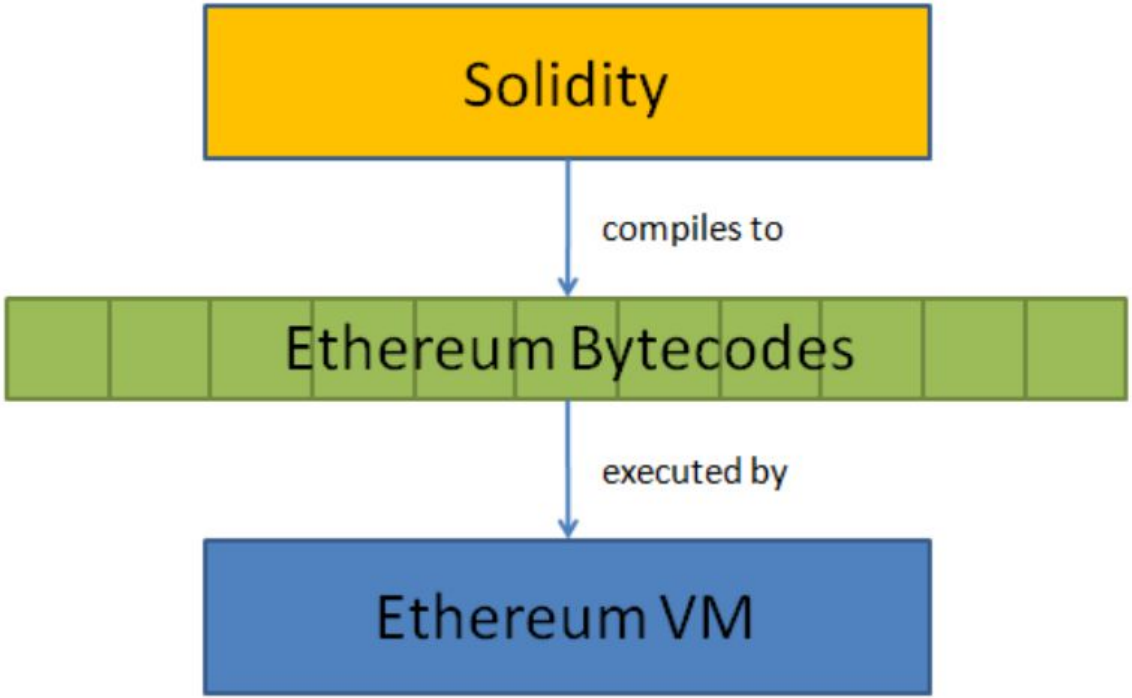
Smart Contract Programming

- Solidity (Javascript based), most popular
  - more mature
- Serpent (Python based)
- LLL (Lisp based)

Most popular tools for Ethereum

- **Geth**: Console to setup the node
- **Mist**: Browser and Wallet
- **Ganache:** Quick Ethereum node for testing
- **Truffle**: Framework for Smart Contract
- **Solidity**
  - Programming Language for Ethereum Smart contract
- **Remix IDE:** IDE for Smart Contract Development & Deployment

Solidity and EVM



Creating Wallet

With:

- **Metamask**
- **Ganache**

Transaction Specifications

Transaction Specifications

- From: Account creating this transaction
- To: Target recipient of the transaction
- Data: Parameters
- gasPrice: How much they are willing to pay (in wei) per one unit of gas
- gasLimit: How much total gas they are willing to pay for
- signature: Proving this transaction

Estimating transaction costs

- The total ether cost of a transaction is based on 2 factors:
  - gasUsed is the total gas that is consumed by the transaction
  - gasPrice price (in ether) of one unit of gas specified in the transaction
- Total cost = gasUsed * gasPrice

Gas

- Halting problem (infinite loop) – reason for Gas
- Problem: Cannot tell whether or not a program will run infinitely from compiled code
- Solution: charge fee per computational step to limit infinite loops and stop flawed code from executing

Gas

- Every transaction needs to specify an estimate of the amount of gas it will spend
- Essentially a measure of how much one is willing to spend on a transaction, even if buggy

Gas Cost

- Gas Price: current market price of a unit of Gas (in Wei)
  - Check gas price here: https://ethgasstation.info/
  - Is always set before a transaction by user
- Gas Limit: maximum amount of Gas user is willing to spend
  - Helps to regulate load on network

Gas Cost

- Gas Cost (used when sending transactions) is calculated by gasLimit*gasPrice.
  - All blocks have a Gas Limit (maximum Gas each block can use)

Remix IDE

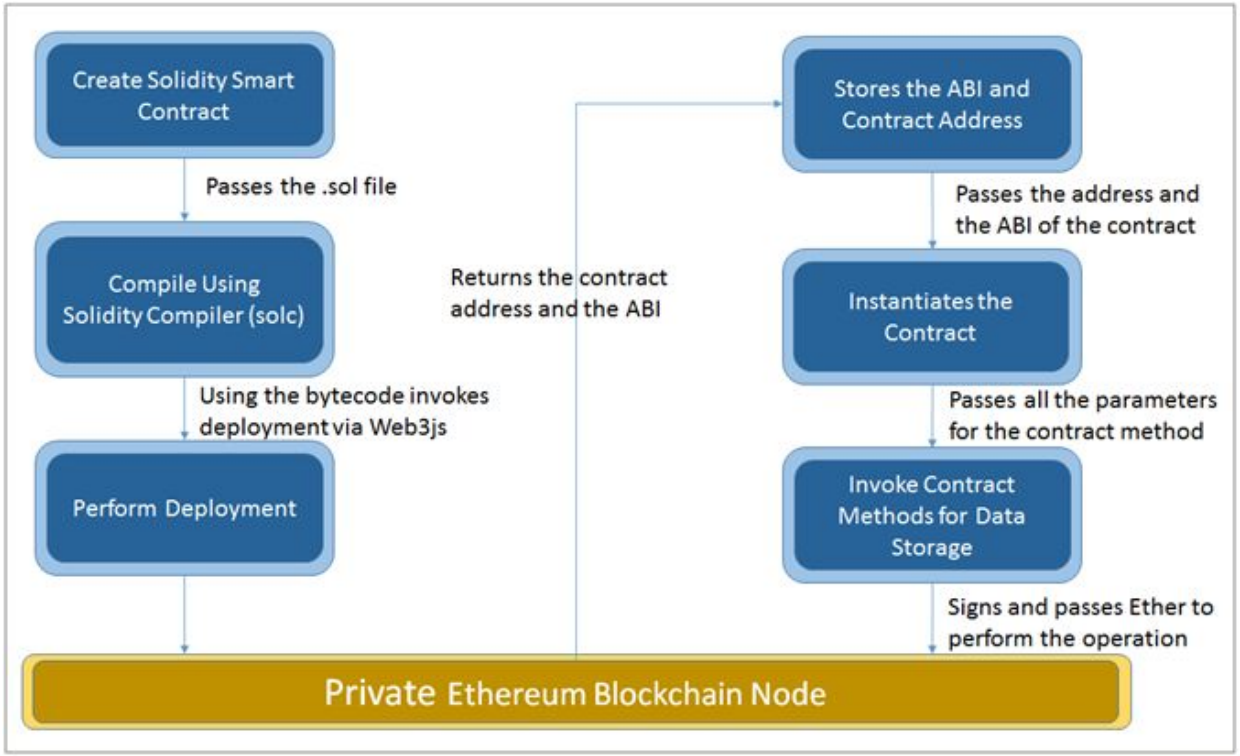
Web url :

https://remix.ethereum.org/

Docker:

- docker pull remixproject/remix-ide:latest
- docker run -p 8080:80 remixproject/remix-ide:latest

Demo Flow



Setup

- Create our own private test network
  - Ganache
  - Metamask
- Accounts
  - Private Keys
  - Address
- Ethers in per Account
- Genesis Block

Thank You