# Blockchain-III

Dr. Maumita Chakraborty

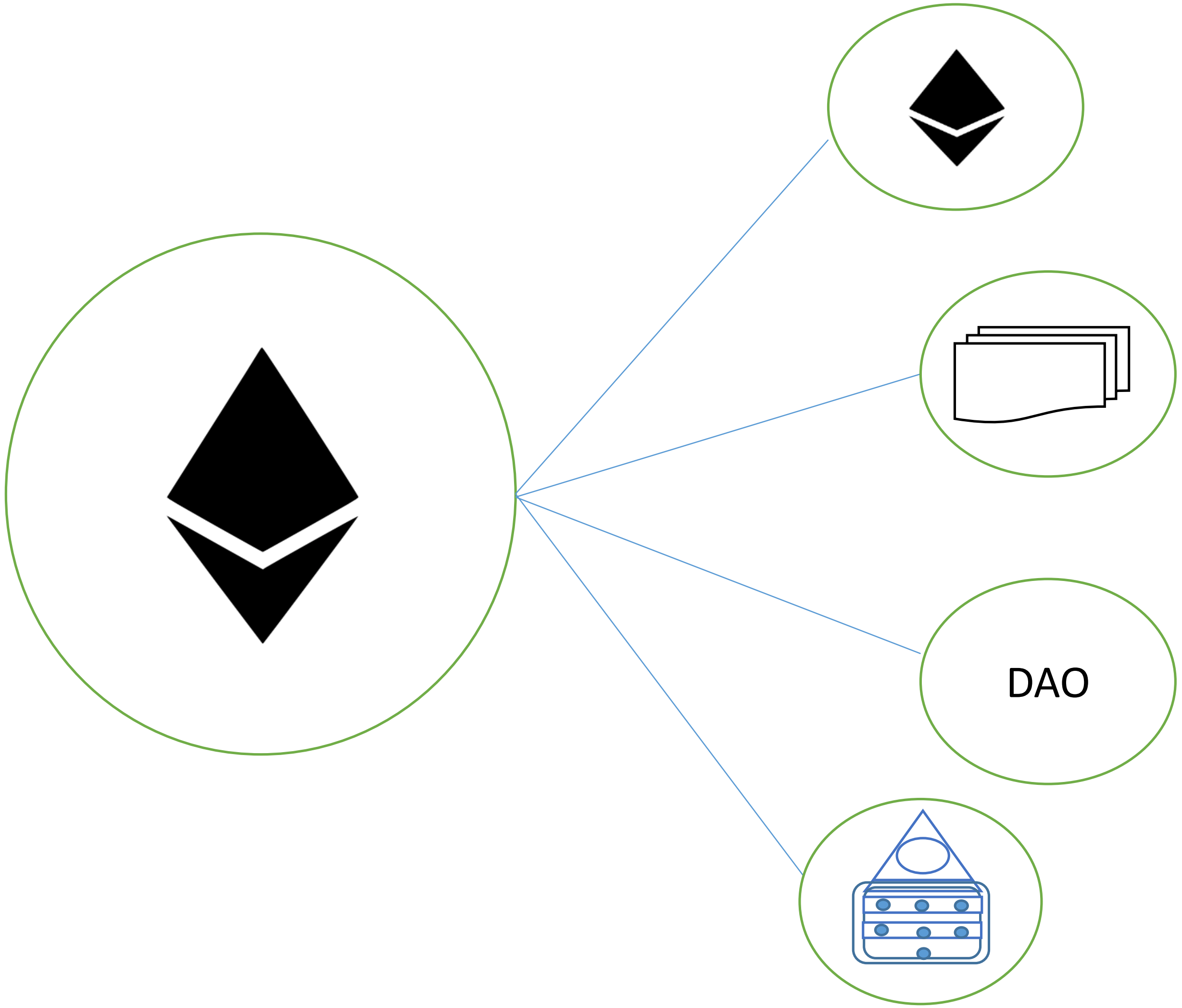
University of Engineering and Management Kolkata

# Ethereum

# Ethereum Blockchain

- Also referred to as DApps – de-centralized applications/programs.
- To produce a brand new application that no person controls – need to learn Ethereum programming language named Solidity.
- It is not just a currency, it is a platform.
- Smart Contracts – logic to execute DApps.

# Ethereum Characteristics



Cryptocurrency

Smart Contracts

DAO

Smart Property

The ownership of smart property is controlled via the Ethereum Wallet that functions as a gateway to DApps on the Ethereum Blockchain.

# Smart Contracts

- Piece of code that lives in the Ethereum Blockchain.
- Can be instructed to do certain things by having a person or another contract send a message to it.
- They are at the absolute core of Ethereum.
- Contract is a collection of conditions and actions.
- Ethereum programmers write the requirements for their applications (DApps) and Ethereum network implements it.
- Why smart? Handle every facet of the contract – authorities, direction, performance and payment.
- Once set on the Ethereum system, it cannot be corrected or edited. (Immutable)

# Decentralized Autonomous Organization (DAO)

- “Code is Law”: Contract on Ethereum is ultimate authority, nobody can overrule the contract.

- Electronic digital organization that works with no hierarchical direction, functions in a decentralized and democratic way.

- Based on a Blockchain system where it is regulated by the protocols inserted inside a smart contract i.e. DAOs count on smart contracts for decision-making.

- DAO Attack occurred: problem found with DAO code and not in Ethereum network. Hackers stole Ether from DAO. Problem in block number 1919999.

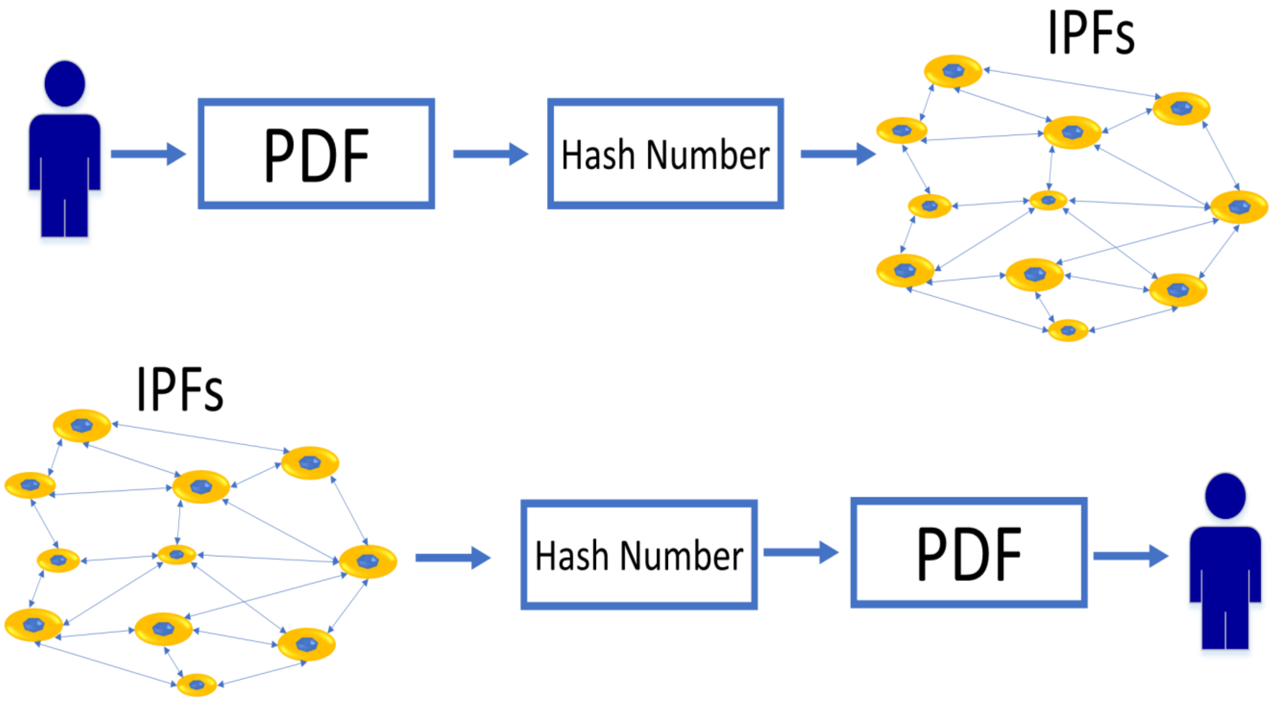
- Ethereum split into ETH (Ethereum) and ETC (Ethereum Classic) after the DAO attack. New rule sets for Ethereum and old rules for Ethereum Classic.

# Ethereum Components

- Miner and mining node
- Ethereum virtual machine
- Ether
- Gas
- Transactions
- Accounts
- Swarm and Whisper
- Ethash

# Miner and Mining Node

- **Miner:** responsible for writing transaction to the Ethereum series.
- Miners get 2 kinds of rewards:
  - Benefit of writing a block into the series
  - Accumulative gas prices from all transaction in the block (unique concept in Ethereum Blockchain, not available in Bitcoin Blockchain)
- Every miner needs to have backup of Blockchain transactions, as data is not stored directly in the Blockchain.
- Data is stored in some distributed hash table, like IPFs (Interplanetary File System).
- IPFs give back a hash or content address for all contents and help to retrieve the file from the data storage system.
- Hash points of the data are stored in Blockchain.



PDF → Hash Number → IPFs

IPFs → Hash Number → PDF

# Miner and Mining Node

- Miners compete and try to write transactions in a Blockchain.
- Miner who solves the given problem can only write the block comprising transactions to the ledger and receives five ether as a reward.
- Two types of nodes in an Ethereum network:
    - Mining nodes
    - Ethereum Virtual machines
- Generally, no devoted EVM nodes in Ethereum, all nodes may function as a miner in addition to EVM node.
- Mining nodes are the nodes that belong to miners.
- Mining nodes are part of the same network where EVM is hosted.
- Each mining node maintains its version of Ethereum ledger and needs to ensure that their ledger is always upgraded with the latest blocks.

# Functions performed by Miners on Mining Nodes

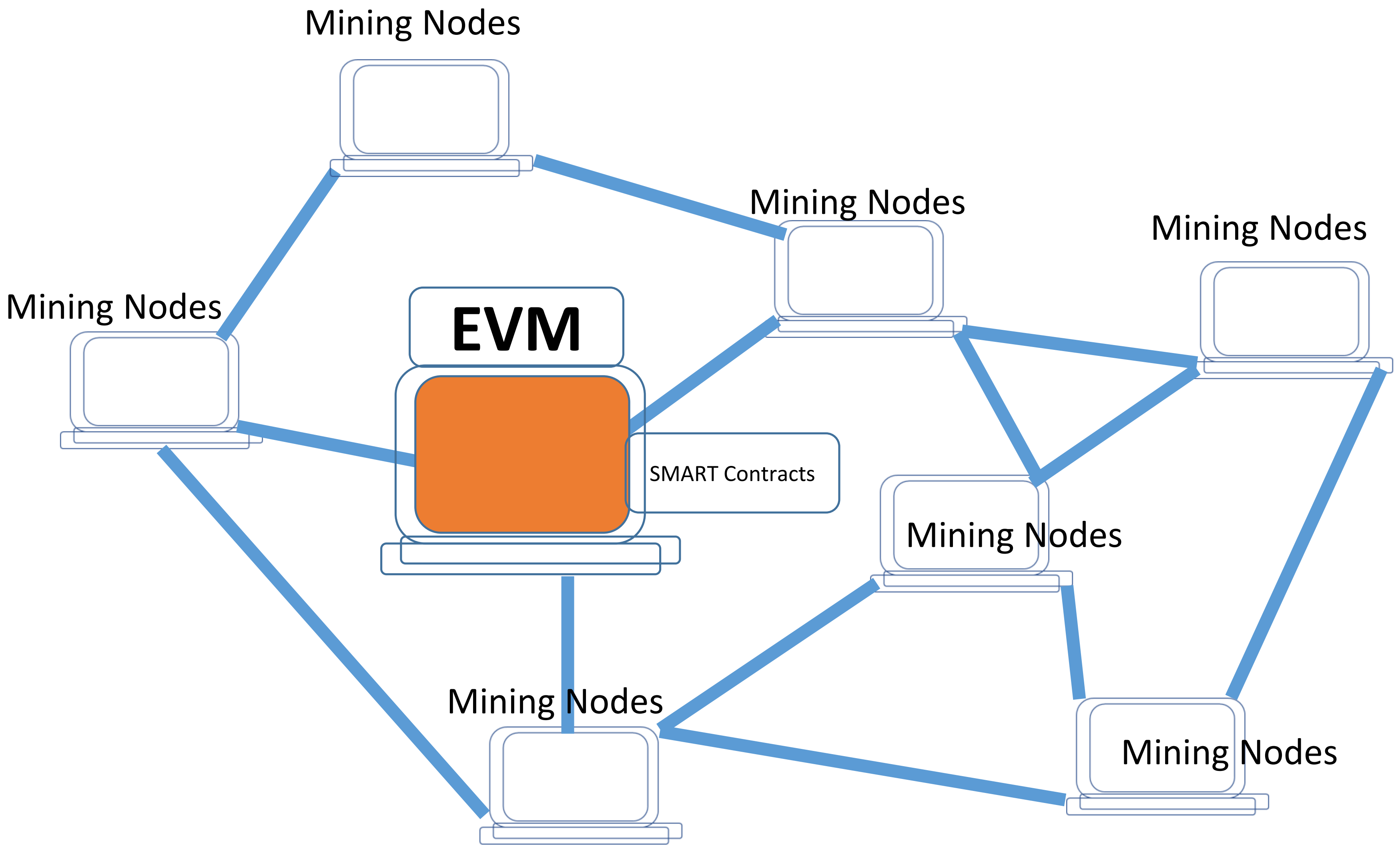
- Three fundamental functions:

- Mining: Make a fresh new block together with the transaction and compose it into Ethereum Ledger.

- Advertise: Promote and send a recently mined block to other miners.

- Accept: Accept new blocks created by other miners and maintain them in the ledger.

# EVM and Smart Contracts



# Ethereum Virtual Machine (EVM)

- Nodes in Blockchain network who do not want to mine, but function as aids for implementing smart contracts.
- Each node connected with different nodes on the network system and uses peer-to-peer protocol to communicate.
- By default, nodes utilize the 30303-port number to communicate with each other.
- EVM hosts smart contracts: supply a runtime where codes from smart contracts can be compiled.
- Smart contracts help in expanding Ethereum by writing business functionality to it and may be implemented as part of the transaction.
- Does not need access to ledger: has limited information regarding current transaction.
- Transaction has to be signed using an account holder’s private key, which helps to confirm the transaction.
- EVM implements a contract together with programming rules that are initially written by the programmer.
- Programmers may write smart contracts using languages like Solidity, Serpent etc.

# Ether

- Cryptocurrency used in Ethereum. Referred to as ETH.
- Money required to get machines, to power them up, save them and cool them whenever required.
- Price of Ethereum is Ether.
- It incentivizes people to follow Ethereum protocol in their PC.
- To set up a smart contract using Ethereum platform, contract author needs to pay in the form of ether.
- People should write optimized codes that do not waste the Ethereum network's computing ability on unnecessary tasks.
- Ether was distributed in Ethereum's authentic Initial Coin Offering (ICO) in 2014.
- 40 cents were charged initially to buy an ether. Now one ether equals hundreds of dollars. One ETH is comparable to USD 269.55.
- Every task onto Ethereum that modifies its state costs Ether.
- Miners are rewarded Ether.
- Ether can be transformed into dollars (or alternative conventional currencies) through crypto-exchanges.
- Second biggest cryptocurrency behind Bitcoin.
- Vitalik Buterin along with others launched Ethereum in 2015 and started its momentum of growth from 2017.

# Ether and Wei

- Ether comes with a metric system of denomination.
- Smallest such denomination (foundation component of ether) is Wei.
- The subdivisions for its token is to make it easier to calculate the computational fees for the miners.
- Other cryptocurrencies have a fixed fee for the mining operation known as mining rewards.
- On the Ethereum network, the amount of ether you pay to the miners for verifying your transaction depends upon the time in which you want your transaction to be confirmed.

| Unit | Wei | Ether |
|---|---|---|
| Wei | 1 Wei | $10^{-18}$ ETH |
| Babbage | 1,000 Wei | $10^{-15}$ ETH |
| Lovelace | 1,000,000 Wei | $10^{-12}$ ETH |
| Shannon | $10^{9}$ Wei | $10^{-9}$ ETH |
| Szabo | $10^{12}$ Wei | $10^{-6}$ ETH |
| Finny | $10^{15}$ Wei | $10^{-3}$ ETH |
| Ether | $10^{18}$ Wei | 1 ETH |

Units of Wei

# GAS

- Gas refers to the unit that measures the amount of computational effort required to process transactions and smart contract on the Ethereum network.
- Each Ethereum transaction requires computational resources to execute, each transaction requires a fee.
- Gas refers to the fee required to conduct a transaction on Ethereum successfully.
- Gas fees are paid in Ethereum's native currency, ether (ETH).
- Gas prices are denoted in gwei, which itself is a denomination of ETH - each gwei is equal to 0.000000001 ETH ($10^{-9}$ ETH).
- For example, instead of saying that your gas costs 0.000000001 ether, you can say your gas costs 1 gwei.
- The word 'gwei' itself means 'giga-wei', and it is equal to 1,000,000,000 wei.
- Wei itself is the smallest unit of ETH.

# GAS

- Concept was introduced to compensate miners for their work done on maintaining and securing the Blockchain.
- Transaction prices based on Gas Limit and Gas Price.
- Gas Limit: Maximum amount of work estimated that a validator will do on a particular transaction. Or, Maximum number of units of gas you are willing to pay for to carry out a transaction (Standard transaction sending ETH normally costs 21000 gas).
- Gas Price: Price per unit of work done.
- Transaction cost = Gas Limit X Gas Price
- Lower estimation of gas limit by a user -> lower the priority in the queue they will be.
- Ethereum validators are awarded this fee for staking their ether and verifying blocks.
- Supply and demand for transactions dictate gas prices.
  - Network congested -> gas prices high.
  - Not much traffic -> gas prices low.

# Transactions in Ethereum

- Ethereum stores transactions within blocks.
- Transaction (Contract) is a set of agreements between parties.
- There may be exchange of assets, products, or services in place of currency, cryptocurrency either in the present or in the future.
- Ethereum helps in executing a transaction.

# Ethereum Accounts

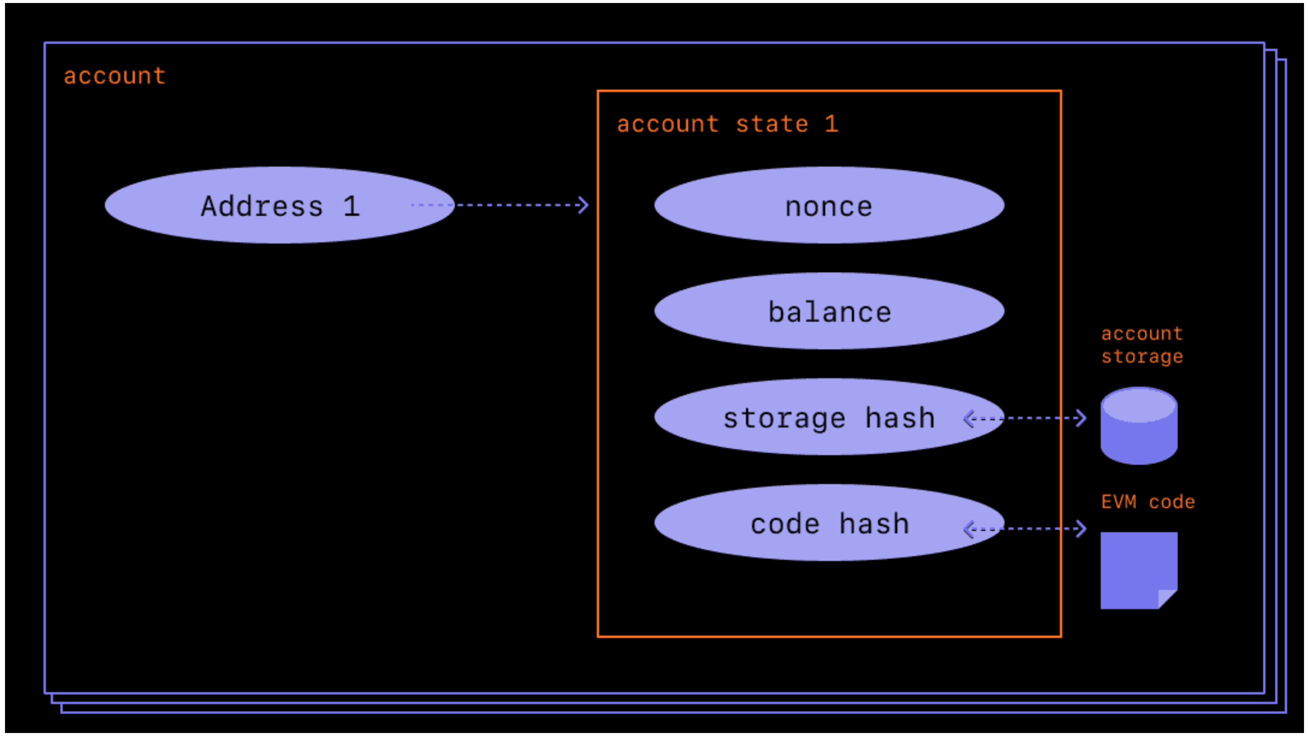
- Accounts: Primary building block for Ethereum ecosystem.
- Every account comes with a balance (present value saved in it).
- Two types of accounts: externally owned account, contract account.
- On creation of externally owned account on Ethereum, a public-private key is produced.
- Public key: ID of the account, consists of 256 characters. First 160 characters represent the identity of an externally owned account.
- Private key: Unique identifier assigned to each node.
- Externally owned account may keep Ether in its balance and not have any code related to it.
- They can transact with other externally owned accounts by invoking functions within smart contracts.
- Normal contract accounts have a programming code for smart contracts comprising of state variables and functions.

# External account vs. Contract account

| External Account | Contract Account |
|---|---|
| Controlled by anyone with private keys | A smart contract deployed to the network, controlled by code |
| Can receive, hold and send ETH and tokens | Can receive, hold and send ETH and tokens |
| Can interact with deployed smart contracts | Can interact with deployed smart contracts |
| Creating an account costs nothing | Creating a contract has a cost, as network storage is being used |
| Can initiate transactions | Can only send transactions in response to receiving a transaction |
| Transactions between externally-owned accounts can only be ETH/token transfers | Transactions from an external account to a contract account can trigger code which can execute many different actions, such as transferring tokens or even creating a new contract |
| Made up of a cryptographic pair of keys: public and private keys that control account activities | Contract accounts don't have private keys. Instead, they are controlled by the logic of the smart contract code |

# Components of Accounts (External and Contract)

- **Nonce:** Only one transaction with a given nonce can be executed for each account.
  - For external accounts: Number of transactions sent from that account.
  - For contract accounts: Number of contracts generated via this account.
- **Balance:** The number of wei owned by this address.
- **Code hash:** Hash code of an account on the EVM.
  - For contract accounts: Code is hashed and stored as the code hash. **
  - For external accounts: Code hash field is not applicable. Code hash has empty string.
- **Storage Root:** Has the main root node of the Merkle Tree. The tree encodes the hash of all the storage contents of the account. Empty by default.



# Swarm and Whisper

- Ethereum must have the capabilities to:
  - Calculate
  - Store
  - Communicate
- Swarm: A peer-to-peer document sharing platform (like Bit Torrent) incentivized with micropayments of ETH.
  - File records divided into small chunks, dispersed, and stored with volunteers.
  - Nodes which save and function on those pieces are paid with ETH from people using the information.
- Whisper: An encrypted messaging protocol used by nodes to send messages directly to each other in a secure way, that hides sender and recipient identity from third-party snoopers.

# Ethash

- Ethereum’s PoW mining algorithm.
- Used to dynamically adjust the mining difficulty of the Blockchain that implements it.
- “Difficulty”: Together with Ethash, outcome in hashing process should result in a hash value below a particular threshold.
- Using Ethash, Ethereum system can increase or decrease the threshold, to control the speed and time at which blocks are mined on Ethereum network.
- Rate of blocks increases -> system automatically boosts difficulty -> diminish system threshold -> reduces number of valid hashes with the capacity to be detected.
- Amount of exposed blocks decline -> system threshold increases -> create a higher number of hash values which are available.
- Typically one block is produced by the system every 12 seconds.
- Miner receives block reward comprising of 3 (variable) ethers.
- All the gas spent on the block are included within the block.
- Gas price credited to miner’s account: additional reward for adding transactions in a block.

- **Ethereum switched on its proof-of-stake mechanism in 2022 because it is more secure, less energy-intensive, and better for implementing new scaling solutions compared to the previous proof-of-work architecture.**

# End-to-End Transaction in Ethereum

- Four different types of transactions to transfer Ether across accounts.
- Accounts can be:
  - Externally owned accounts
  - Smart contract accounts
- Possible cases:
  - Externally owned account can send ether to another externally owned account in a transaction
  - Externally owned account can send ether to a contract account in a transaction
  - Contract-to-contract ether transaction
  - Contract to externally owned account transaction

# End-to-End Transaction in Ethereum: An Example

- Say, Anie wants to send 3 ETH to Paul.
- Anie generates a transaction message containing From and To value fields and sends it across the Ethereum network.
- “From Account”: Account that is originating the transaction and is ready or about to send gas or ether. Can be externally owned or contract account.
- “To Account”: Account that is obtaining ethers. Is an empty string for transactions regarding deployment of the contract.
- Transaction is not written instantly into the ledger. It is set in a transaction pool.
- Mining node puts all transactions from the pool, based on gas limitation standards, and adds them to a brand new block.
- Every block includes an upper gas limit, every transaction desires a specific quantity of gas to become a member of its implementation.
- Accumulative gas from many transactions cannot exceed the block gas limit. Hence, all transactions do not get stored in just one block.
- In an example, if gas used by the transaction is 11500 and gas price is 20 Gwei. Then 20Gwei X 115000 gives the actual transaction fees.

# End-to-End Transaction in Ethereum: An Example

- Miners compete to validate the block with the new set of transactions.
- The winning miner creates a new block and receives a reward.
- Accounts are upgraded using a new balance. Paul receives 3 ETH from Anie.
- Block is duplicated across every node of the network.
- Transactions are hashed and stored in the block.
- Hashes of two transactions are hashed once again to get a new hash.
- Finally one hash results from many transactions stored inside the block, which is known as Transaction Merkle Root Hash and is stored in the block’s header.

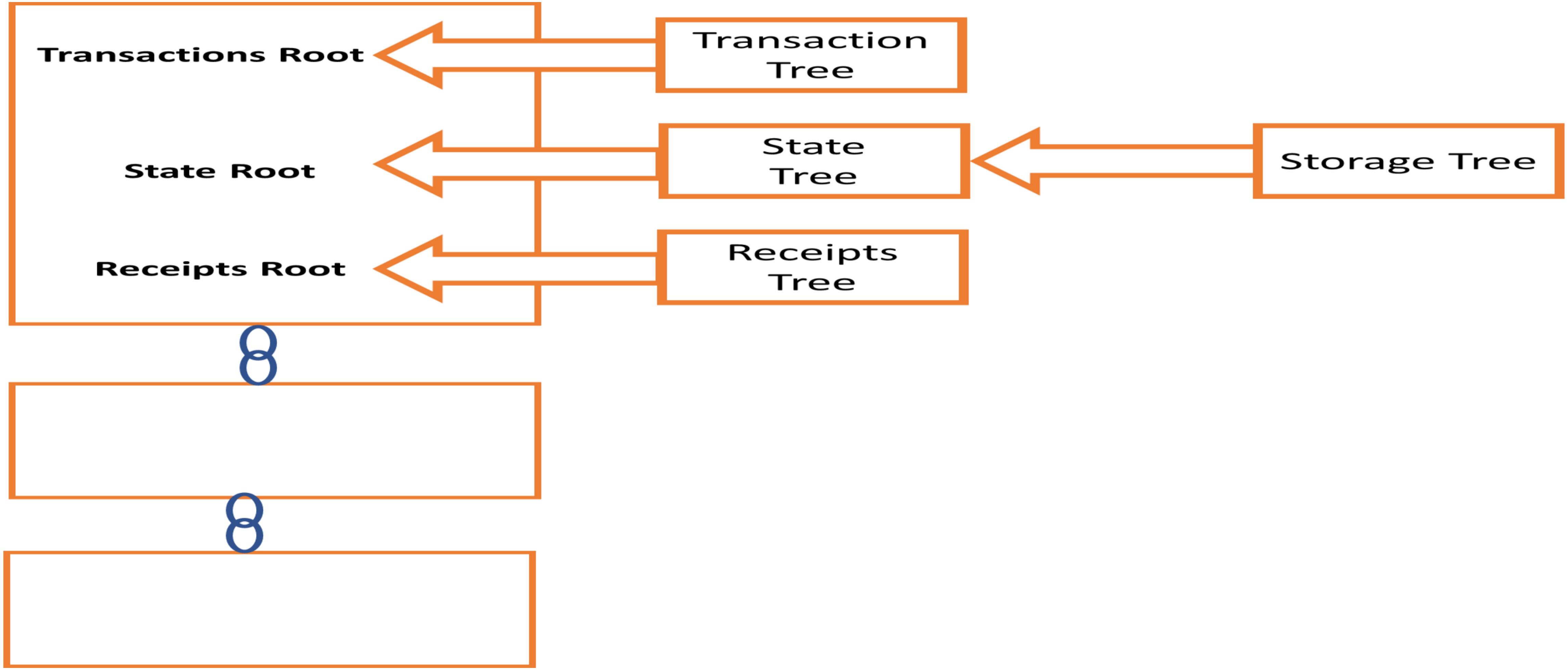
# Mining in Ethereum

- Mining is different from that of bitcoin.
- Miners always look forward to mine new blocks and listen actively to receive new blocks from other miners.
- Miners gather transactions from transaction pool and adds them to a brand new block.
- Before adding, transactions assessed to check if it is not yet written in a block received from other miners. If so, transactions dropped.
- Miner will then add his coin-based transaction to get the reward of mining the block.

# Contents of Block header

- Parent Hash: Hash of previous block.
- LogsBloom: Log information.
- Transaction, state and receipt hash: *Simplifies Merkle tree to get three different forms of items, namely transactions, receipts and states.
- Nonce: Random number that can be used once in a cryptographic communication, to uniquely identify a transaction and reduce chances of duplicate transactions.
- Timestamp: Seconds passed after 1st January 1970, a 10-digit number.
- Ommer Block: A block whose parent corresponds to current block's parent's parent. Also called orphaned blocks.
- MixHash: **A hash which when together with all nonce demonstrates that a block has enough computation. Miners generate a mixhash until the outcome is below the desired target hash.
- Difficulty: Complexity of puzzle/challenge awarded to miners of a particular block. Gas limit of the block decides most gas allowed for the block. Helps in estimating number of transactions that might be part of the block.
- Number: Sequential number of a block on the chain.

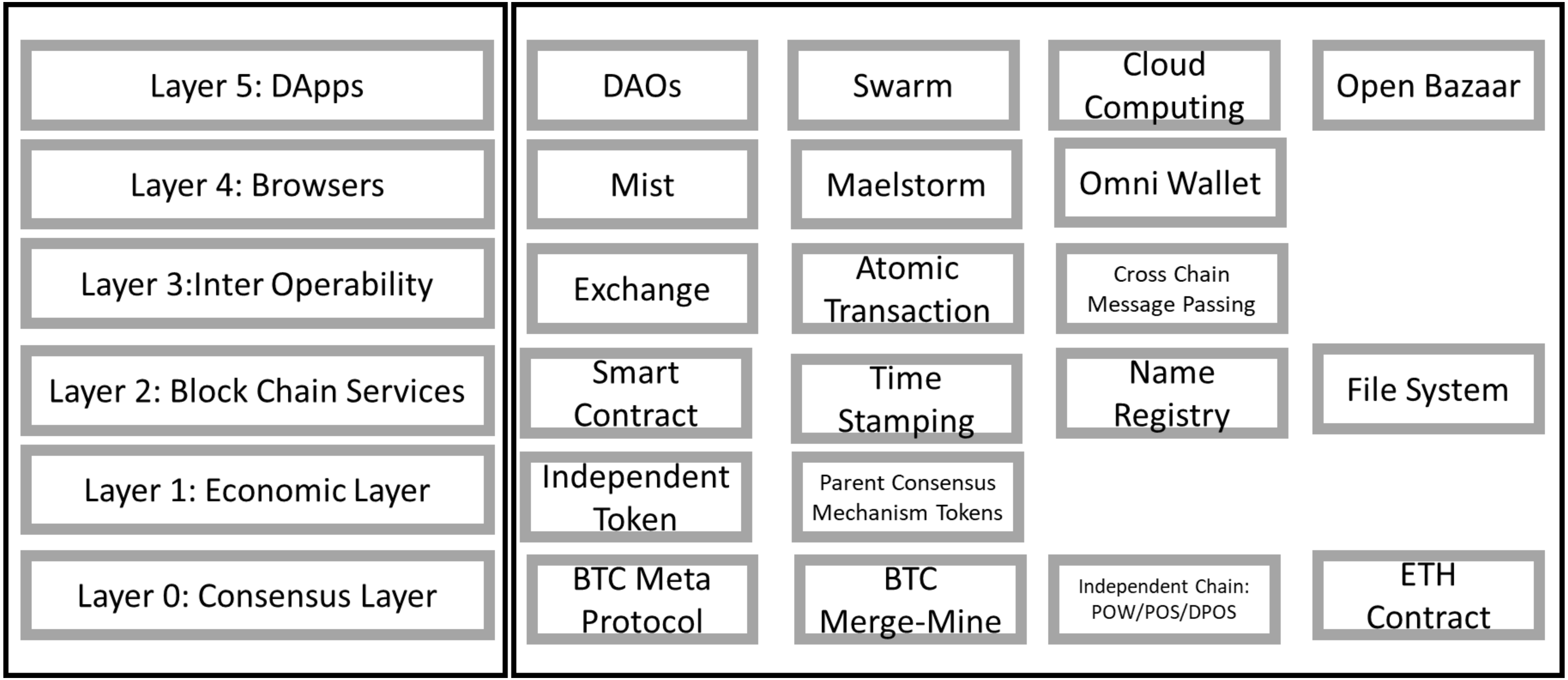
# Merkle Patricia Tree



# Merkle Patricia Tree

- There is a tree called Merkle tree inside each Ethereum block.
- It has a pointer to the previous hash of the last block, has a nonce and a Merkle root.
- Massive scalability problems can be created when we store data as a huge list. Hence, trees.
- A way to hash a large number of chunks of data together, which splits the pieces into buckets, and each bucket only contains few chunks. Thus, it hashes down the chain like a kind of file directory.
- Enables us to get Merkle proof, which comprises the hash root of the tree and also the branch comprising of all hashes moving up across the path.
- Merkle root used in Bitcoin cannot prove anything about the current state of the contract or transaction, i.e. difficult to identify the details of who is currently holding the particular digital asset and the execution status of the financial contract.
- Ethereum blockchain modifies the Merkle tree to store three different types of objects: transactions, receipts and state. A decentralized computer can store a state.

# Ethereum Architecture



| | | | | |
|---|---|---|---|---|
| Layer 5: DApps | DAOs | Swarm | Cloud Computing | Open Bazaar |
| Layer 4: Browsers | Mist | Maelstorm | Omni Wallet | |
| Layer 3:Inter Operability | Exchange | Atomic Transaction | Cross Chain Message Passing | |
| Layer 2: Block Chain Services | Smart Contract | Time Stamping | Name Registry | File System |
| Layer 1: Economic Layer | Independent Token | Parent Consensus Mechanism Tokens | | |
| Layer 0: Consensus Layer | BTC Meta Protocol | BTC Merge-Mine | Independent Chain: POW/POS/DPOS | ETH Contract |

# Ethereum Architecture

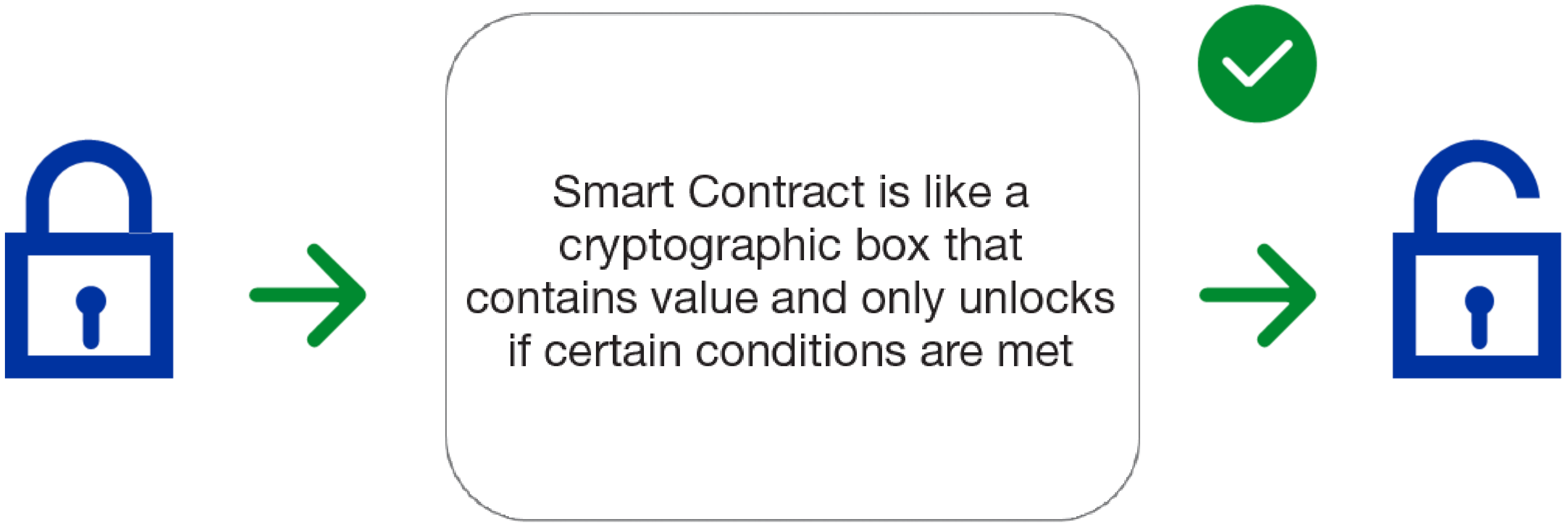
- Layer 0: Consensus: We need some way to agree upon all of the application-level constructs.
- Layer 1: Economic: To incentivize the nodes, either to do the computation or perform the storage operation (Layer 2).
- Layer 2: Blockchain Services: Here crypto tokens get involved.
  - AWS or Google Cloud generally utilized.
  - Desire is to have a brand new form of decentralized storage, which is peer-to-peer reviewed along with IPFs.
  - Smart contracts: code snippets which live on Blockchain, used for decentralized computation.
  - IPFS decentralizes storage and content delivery, smart contracts decentralize computation.
- Layer 3: Interoperability: Universal wrapper around all cryptocurrencies.
  - Exchange protocol transfers amount between different tokens.
  - A stack of decentralized APIs, that all use their tokens. Top API can be paid with any token, and in turn, it pays all the other APIs and the tokens.
- Layer 4: Browser: To access the decentralized applications.
  - Mainstream browsers (like Chrome, Firefox, Opera) accept decentralized protocols natively.
  - Some browsers, like Mist, Omni Wallet, and Maelstrom are made for decentralized applications.
- Layer 5: Dapps: Application-level constructs are added.
  - Does not depend on any specific existing party.
  - More about a network, a community of people, who share the ownership of some piece of software. Everybody profits and everybody contributes in some way.

# Bitcoin vs. Ethereum

| | BITCOIN | ETHEREUM |
|---|---|---|
| Founder | Satoshi Nakamoto(unknown) | Vitalik Buterin and Team |
| Purpose | Crypto Currency | Network Software |
| Release Date | January 2009 | July 2015 |
| Scripting Language | Turing Incomplete | Turing Complete |
| Coin Release Method | Early Mining | Thru ICO |
| Average Block Time | Approx. 10 minutes | Approx. 15 second |
| Transaction Model | UTXO | Account |
| Coin Symbol | BTC | ETH |
| Tokens | Not available | Available |
| Monetary Policy | Hard Coded (max. 21 million bitcoins) | Not Hard Coded (No upper limit, emission rate occasionally reduced) |
| Emission Rate | Halving policy followed | Occasional |
| Backward compatibility | Available | Not Available |
| Block Limitation | 1 MB per block | No limit |

# Smart Contracts

# Smart Contract Concept



Smart Contract is like a cryptographic box that contains value and only unlocks if certain conditions are met

Smart Contracts eliminate the need for trusted third parties

# Benefits

- Simple, faster to execute, availability of updates in real-time.
- No requirement of mediators and centralized entities.
- Lesser cost as there is no need to pay fees to middlemen.
- No delay in delivering outcomes.

# Characteristics

- Can track performance and transactions in real-time.
- Can avail external information by interacting with a web browser.
- Verify itself
- Execute itself
- Be tamper-resistant
- Automate legal transactions in terms of rules
- Provide a high degree of security
- Reduce reliance on trusted intermediaries
- Lower transaction costs

# Types of Smart Contracts

**Smart Legal Contracts**

(Smart contracts with legal contract templates)

**Decentralized Autonomous Organizations (DAO)**

(Multiple smart contracts combined with governance mechanisms)

**Distributed Applications (DApps)**

(Combination of smart contract codes)

**Smart Contracting Devices**

(Combined with IoT)

# Types of Smart Contracts

- Smart Legal Contracts: Just execute the contracts as per the templates used.
- DApps: Run point-to-point network of computers instead of a single computer.
    - Have an unlimited number of participants from market.
    - A ‘blockchain enabled’ website, Smart contract allows it to connect to blockchain.
    - Dapps covers from end to end – both front-end and back-end.
    - In order to create a decentralized application on a smart contract system, several smart contracts must be combined and third-party systems have to be relied upon for the front end.
- DAO: Allows multiple cloud computing users to enter a loosely coupled peer-to-peer Smart Contract collaboration.
- Smart Contracting Devices (combined with IoT): To manage and access data from IoT devices, hacker has to bypass an additional layer of security coded with some robust encryption standards. There is no worry of a single-point failure.

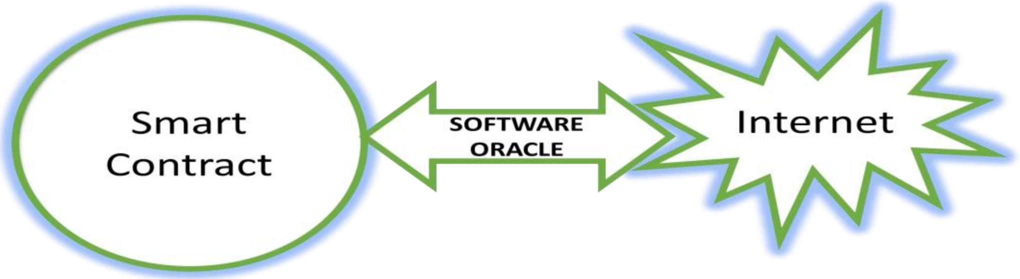
# Oracle

- An agent that verifies real-world occurrences and submits the details to a Blockchain to be used by smart contracts.
- Example: Trustee agrees to release funds only when a particular set of conditions is met. To release any fund, an oracle has to sign the smart contract as well.
- Based on usage, four types of oracles:
  - Software Oracle
  - Hardware Oracle
  - Inbound and Outbound Oracle
  - Consensus based Oracle

# Software and Hardware Oracles

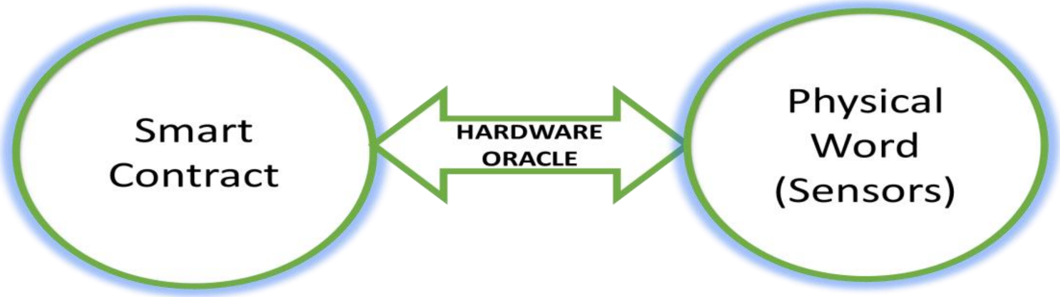
**Software Oracle**

- Handle information generally available over the Internet.
- Eg.- Prices of commodities, details of flight or train delays etc. Data originates from online sources like e-commerce sites, railway reservation sites etc.
- Software oracle pulls out relevant information and sends it to smart contract.



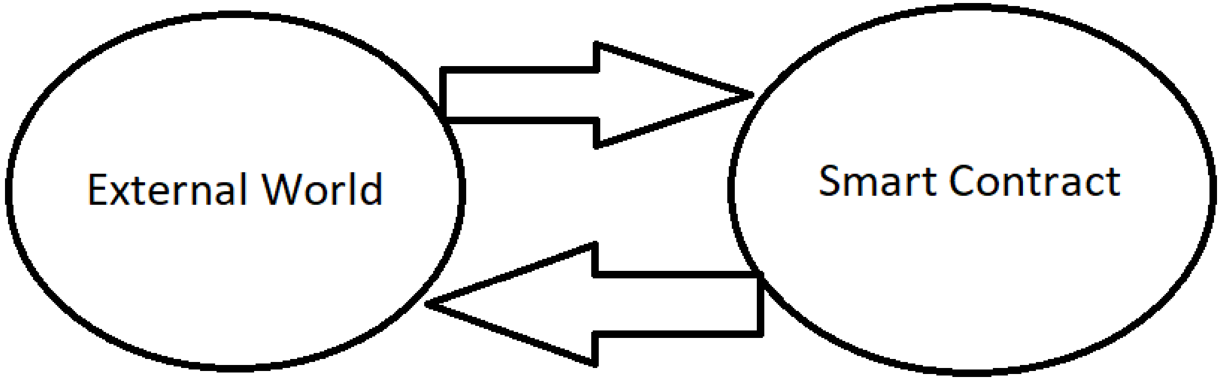
**Hardware Oracle**

- Smart contracts get input directly from physical world.
- Eg.- Used to track details of a car crossing a specific junction (date, time, speed, direction, location).



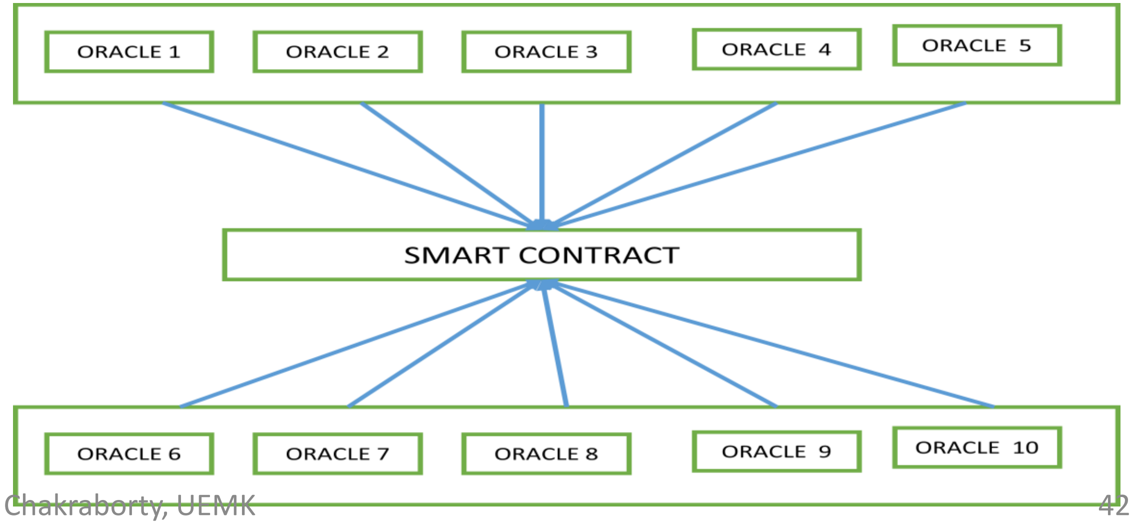
# Inbound and outbound Oracles

- Inbound oracles provide smart contract with data from external world. Eg.- Automatic purchase order for some goods, if the goods stock value hits a certain inventory number.
- Outbound oracles allow smart contracts the capability to send data to the outside world.



# Consensus-based Oracles

- Prediction market rely heavily on oracles.
- It is risky to depend on only one source of information.
- A combination of different oracles is used for enhanced security.
- Eg. – 6 out of 10 oracles (majority) could determine the outcome of an event.
- Connecting a smart contract to external data and existing applications, data feeds, APIs, bank payments etc. is essential for creating smart contracts.



# What is Crowdfunding?

- Use of small amounts of capital from a large number of individuals to finance a new business venture.

- Makes use of the easy accessibility of vast networks of people through social media and crowdfunding websites to bring investors and entrepreneurs together.

- Investors can contribute to any project effectively by creating smart contracts.

- Through smart contracts, the contributors can have a control over the invested money and also both the project creators and investors can effectively make and reserve funding for the project.

# How smart contracts can help in crowdfunding?

- **Automating the process of investment, funds allocation and withdrawal**
- **No middlemen** — there is no need for a third party involvement
- **Increased transparency** — the investors know exactly what happens to their funds when fundraising is successful or if it does not reach its goal
- **Improved safety and credibility** — encryption ensures that all documents are protected from any kind of interference
- **Secure data storage** — all the documents are stored digitally on blockchain, and the distributed ledger technology allows to secure and backup the data and therefore removes the risk of data loss
- **Reliability** — smart contracts are much more foolproof due to the elimination of manual filling of numerous forms typical to traditional contracts
- **Distributed assets** — no physical parties are in control of the allocated funds; the output of your contract is validated by everyone on the network
- **Immutability** — once a smart contract is created it cannot be changed, so investors know exactly what is going to happen to their capital
- **Speed and efficiency** — smart contracts work as automated computer codes, which help to significantly increase the time efficiency and save hours upon hours on drawing up agreements

# Smart Contracts in Various Industries

- Healthcare:
  - Goal is to give patients the authority over the entire medical history and to provide one-stop access to patients and physicians.
  - Allows authorized parties to access, receive and make changes to their records.
- Manufacturing and Supply Chain:
  - Can be monitored securely and transparently.
  - Can review time delays and human mistakes, which are very costly for drug industries.
  - Can monitor costs, labour, or even waste at every point of the supply chain.
  - Can be used to verify the originality of the product, tracking it from origin.
- Banking and Financial Services:
  - Processing becomes faster.
  - Higher security is maintained.
- Other Industries:
  - **Legal:** Can track contract parties, terms, transfer of ownership, and delivery of goods.
  - **Government:** To store personal ID information, criminal backgrounds and e-citizenship authorized by biometrics.
  - **Food:** Can be used to trace product origin, batch, processing, expiration, storage conditions, and shipping.
  - **Insurance:** Overall costs decrease as there is no need for auditing and authenticating data.
  - **Education:** To store grade or credentials data around assessments, degree and transcripts.
  - **Travel and Hospitality:** Hotel customers and airline passengers store their authenticated travel ID on the blockchain. It will help them with travel document identification cards, loyalty program, personal preferences, and payment data.

# Thank You