Public Blockchain

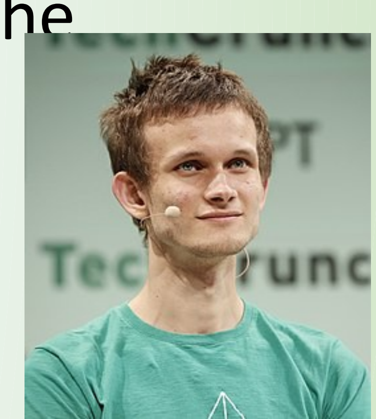
Smita Kulkarni-Pai

Public Blockchain

- A public blockchain is a non-restrictive, permission-less distributed ledger system. A node or user which is a part of the public blockchain is authorized to access current and past records, verify transactions or do proof-of-work for an incoming block, and do mining.
- **Characteristics of Public Blockchain**
  - Every node has access to read and write on the ledger
  - Anyone can download and add nodes to the system
  - The technology is fully decentralized in nature
  - It offers anonymity, which means no one can track your transactions back to you
  - It's a bit slower compared to the private blockchain

Ethereum

- **Ethereum** is a decentralized blockchain with smart contract functionality. **Ether** (Abbreviation: **ETH**; sign: **Ξ**) is the native cryptocurrency of the platform. Among cryptocurrencies, ether is second only to bitcoin in market capitalization. It is open-source software.
- Ethereum was founded in 2013 by programmer Vitalik Buterin. Additional founders of Ethereum included Gavin Wood, Charles Hoskinson, Anthony Di Iorio and Joseph Lubin. In 2014, development work began and was crowdfunded, and the network went live on 30 July 2015



Ethereum

- Ethereum allows anyone to deploy permanent and immutable decentralized applications onto it, with which users can interact. Decentralized finance (DeFi) applications provide financial instruments which do not directly rely on financial intermediaries like, exchanges, or banks.
- This facilitates borrowing against cryptocurrency holdings or lending them out for interest. Ethereum also allows users to create and exchange non-fungible tokens (NFTs), which are tokens that can be tied to unique digital assets, such as images.

Ethereum

- On 15 September 2022, Ethereum transitioned its consensus mechanism from proof-of-work (PoW) to proof-of-stake (PoS) in an upgrade process known as "the Merge". This has cut Ethereum's energy usage by 99%.

Ethereum 2.0

- Ethereum 2.0 (Eth2) was a set of three or more upgrades, also known as "phases", meant to transition the network's consensus mechanism to proof-of-stake, and to scale the network's transaction throughput with execution sharding and an improved EVM architecture.
- The switch from proof-of-work to proof-of-stake on 15 September 2022 has cut Ethereum's energy usage by 99%. However, the impact this has on global energy consumption and climate change may be limited since the computers previously used for mining ether may be used to mine other cryptocurrencies that are energy-intensive.

Ethereum & its components

- Ethereum and its component
  - Blockchain nw: geth
  - Ether
  - Accounts
  - Address
  - Virtual Machines
  - Gas
  - DApp

- **Ethereum Component: Ether**
  - Ether (ETH) is the cryptocurrency generated in accordance with the Ethereum protocol as a reward to validators in a proof-of-stake system for adding blocks to the blockchain.
  - Ether is represented in the state as an unsigned integer associated with each account, this being the account's ETH balance denominated in wei (1018 wei = 1 ether).
  - At the end of each epoch, new ETH is generated by the addition of protocol-specified amounts to the balances of all validators for that epoch, with the block proposers receiving the largest portion.
  - Additionally, ether is the only currency accepted by the protocol as payment for the transaction fee.

- **Ethereum Component: Ether**
  - The transaction fee is composed of two parts: the base fee and the tip.
  - The base fee is "burned" (deleted from existence) and the tip goes to the block proposer.
  - The validator reward together with the tips provide the incentive to validators to keep the blockchain growing (i.e. to keep processing new transactions).
  - Therefore, ETH is fundamental to the operation of the network.
  - Ether may be "sent" from one account to another via a transaction, which simply entails subtracting the *amount to be sent* from the sender's balance and adding the same amount to the recipient's balance.
  - Ether is often erroneously referred to as "Ethereum".

- **Ethereum Component: Accounts**
  - There are two types of accounts on Ethereum: user accounts (also known as externally-owned accounts) and contracts.
  - Both types have an ETH balance, may send ETH to any account, may call any public function of a contract or create a new contract, and are identified on the blockchain and in the state by an account address.
  - Contracts are the only type of account that has associated code (a set of functions and variable declarations) and contract storage (the values of the variables at any given time).
  - A contract function may take arguments and may have return values.

Ethereum Component: Addresses

- Ethereum addresses are composed of the prefix "0x" (a common identifier for hexadecimal) concatenated with the rightmost 20 bytes of the Keccak-256 hash of the ECDSA public.

- In hexadecimal, two digits represent a byte, and so addresses contain 40 hexadecimal digits after the "0x",

e.g. 0xb794f5ea0ba39494ce839613fffba74279579268

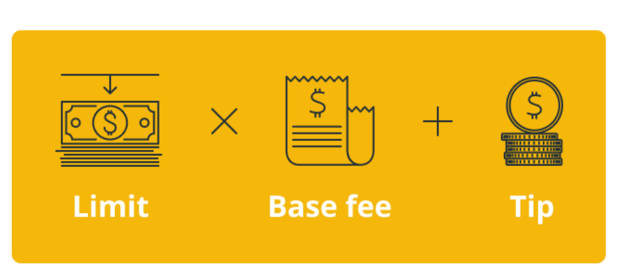
- Contract accounts also have a 42 character hexadecimal address:
- Example:

- 0x06012c8cf97bead5deae237070f9587f8e7a266d

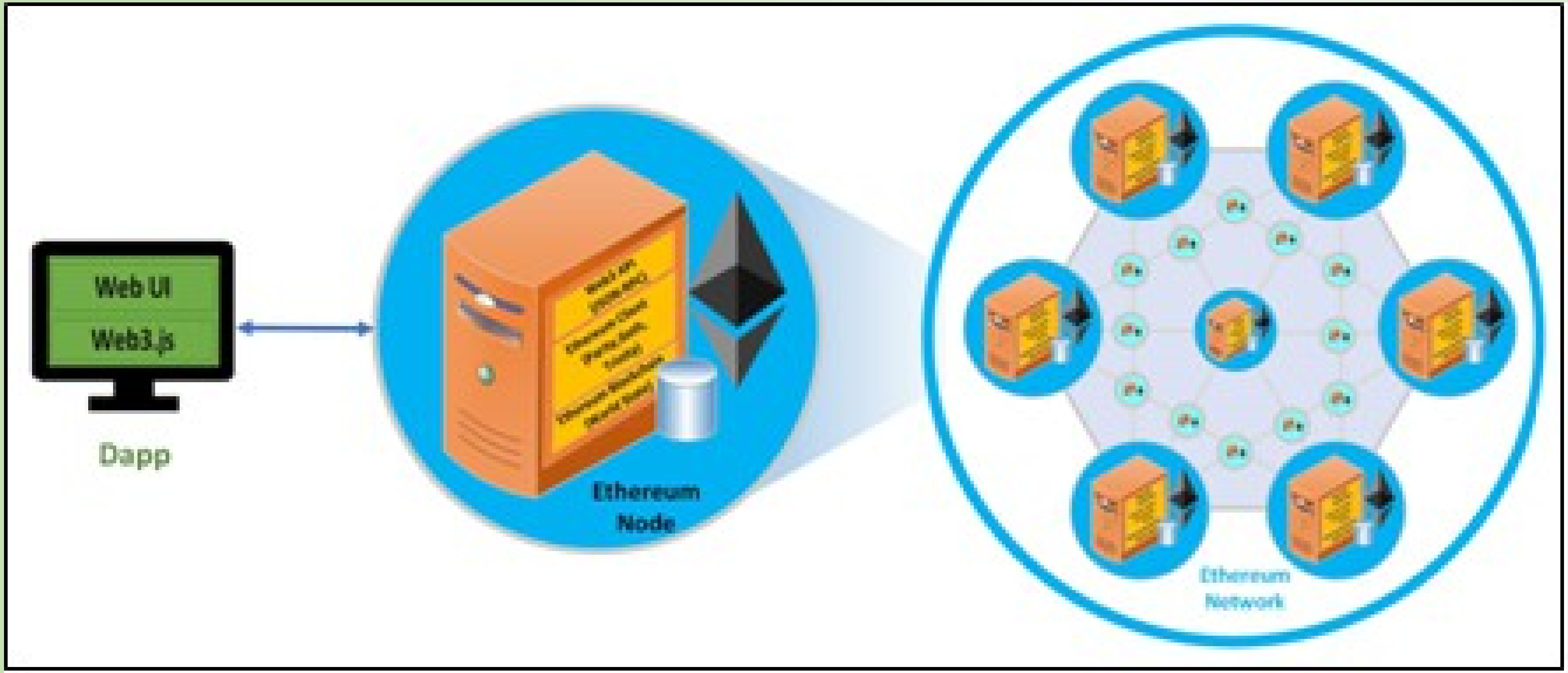
- **Ethereum Component: Addresses**
  - **Key differences**
  - **Externally-owned**
    - Creating an account costs nothing
    - Can initiate transactions
    - Transactions between externally-owned accounts can only be ETH/token transfers
    - Made up of a cryptographic pair of keys: public and private keys that control account activities
  - **Contract**
    - Creating a contract has a cost because you're using network storage
    - Can only send transactions in response to receiving a transaction
    - 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
    - Contract accounts don't have private keys. Instead, they are controlled by the logic of the smart contract code

- **Ethereum Component: Virtual machine**
    - The Ethereum Virtual Machine (EVM) is the runtime environment for transaction execution in Ethereum.
    - It includes, among other things, a stack, memory, gas balance, program counter, and the state (including contract code).
    - The EVM is stack-based, in that most instructions pop operands from the stack and push the result to the stack.
    - The EVM is designed to be deterministic on a wide variety of hardware and operating systems, so that given a pre-transaction state and a transaction, each node produces the same post-transaction state, thereby enabling network consensus.
    - The formal definition of the EVM is specified in the Ethereum Yellow Paper. EVMs have been implemented in C++, C#, Go, Haskell, Java, JavaScript, Python, Ruby, Rust, Elixir, Erlang, and soon WebAssembly

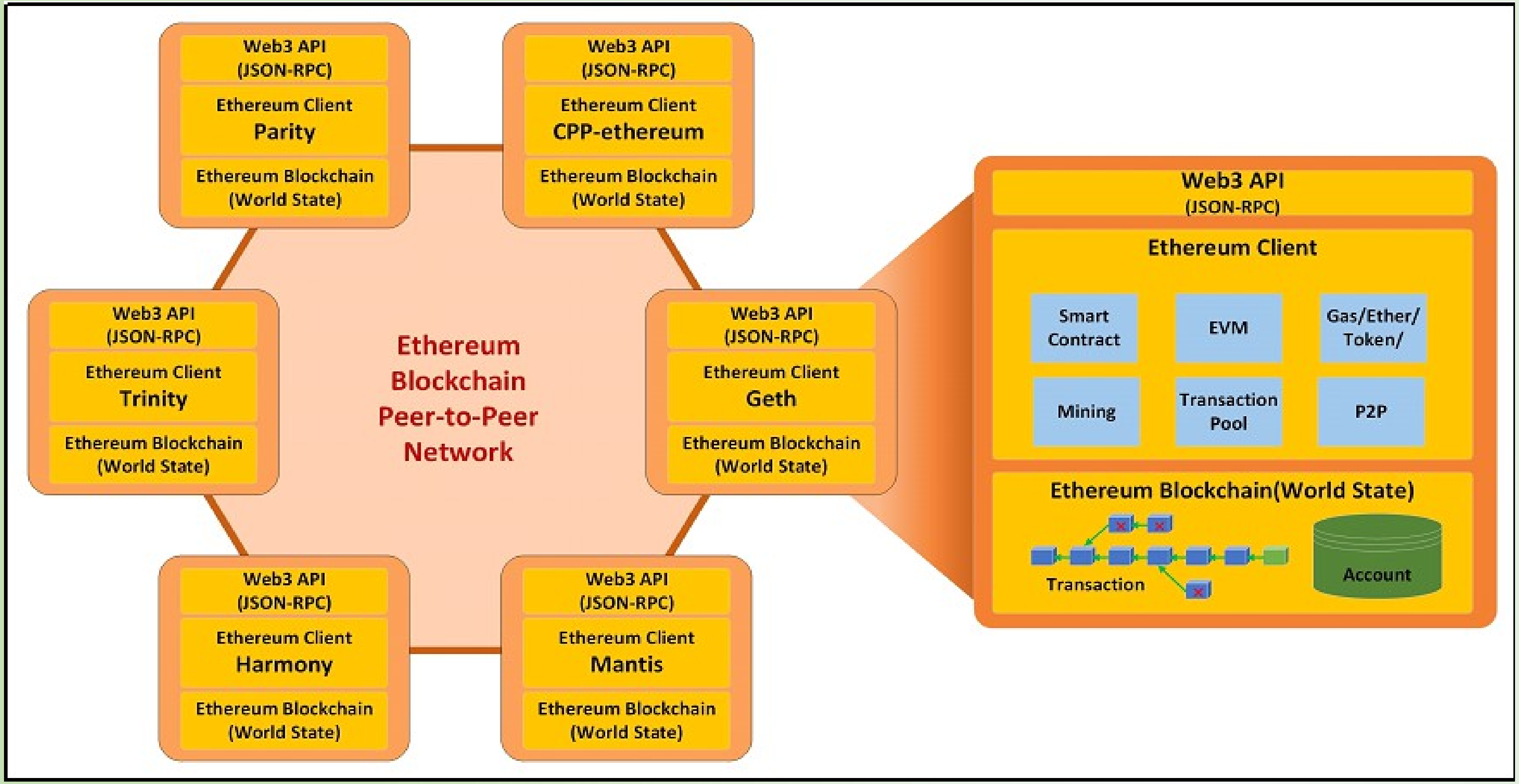
- **Ethereum Component: Gas**
  - Gas is a unit of account within the EVM used in the calculation of the transaction fee, which is the amount of ETH a transaction's sender must pay to the network to have the transaction included in the blockchain.
  - When a sender is creating a transaction, the sender must specify a *gas limit* and *gas price*.
  - The *gas limit* is the maximum amount of gas the sender is willing to use in the transaction, and the *gas price* is the amount of ETH the sender wishes to pay to the network per unit of gas used.
  - A transaction may only be included in the blockchain at a block slot that has a *base gas price* less than or equal to the transaction's *gas price*.
  - The portion of the *gas price* that is in excess of the *base gas price* is known as the tip and goes to the block proposer; the higher the tip, the more incentive a block proposer has to include the transaction in their bloc quicker the transaction will be included in the blockchain.



- **Ethereum Component: Applications(DApps)**
- Blockchain based applications, Distributed Applications.



- **Ethereum Component:**



Ethereum Mining

- Proof-of-work is no longer underlying Ethereum's consensus mechanism, meaning mining has been switched off. Instead, Ethereum is secured by validators who stake ETH.

- Mining is the process of creating a block of transactions to be added to the Ethereum blockchain in Ethereum's now-deprecated proof-of-work architecture.

Mining ether = Securing the Network

Ethereum Mining

- **Cost of mining:**
  - Potential costs of the hardware necessary to build and maintain a mining rig
  - Electrical cost of powering the mining rig
  - If you were mining in a pool, these pools typically charged a flat % fee of each block generated by the pool
  - Potential cost of equipment to support mining rig (ventilation, energy monitoring, electrical wiring, etc.)

Ethereum Mining

- **Working of mining:**
  1. A user writes and signs a transaction request with the private key of some account.
  2. The user broadcasts the transaction request to the entire Ethereum network from some node.
  3. Upon hearing about the new transaction request, each node in the Ethereum network adds the request to their local mempool, a list of all transaction requests they've heard about that have not yet been committed to the blockchain in a block.

Ethereum Mining

- **Working of mining:**

4. At some point, a mining node aggregates several dozen or hundred transaction requests into a potential block, in a way that maximizes the transaction fees they earn while still staying under the block gas limit. The mining node then:

    1. Verifies the validity of each transaction request (i.e. no one is trying to transfer ether out of an account they haven't produced a signature for, the request is not malformed, etc.), and then executes the code of the request, altering the state of their local copy of the EVM. The miner awards the transaction fee for each such transaction request to their own account.

    2. Begins the process of producing the proof-of-work "certificate of legitimacy" for the potential block, once all transaction requests in the block have been verified and executed on the local EVM copy.

Ethereum Mining

- **Working of mining:**

5. Eventually, a miner will finish producing a certificate for a block which includes our specific transaction request. The miner then broadcasts the completed block, which includes the certificate and a checksum of the claimed new EVM state.
6. Other nodes hear about the new block. They verify the certificate, execute all transactions on the block themselves (including the transaction originally broadcasted by our user), and verify that the checksum of their new EVM state after the execution of all transactions matches the checksum of the state claimed by the miner’s block. Only then do these nodes append this block to the tail of their blockchain, and accept the new EVM state as the canonical state.

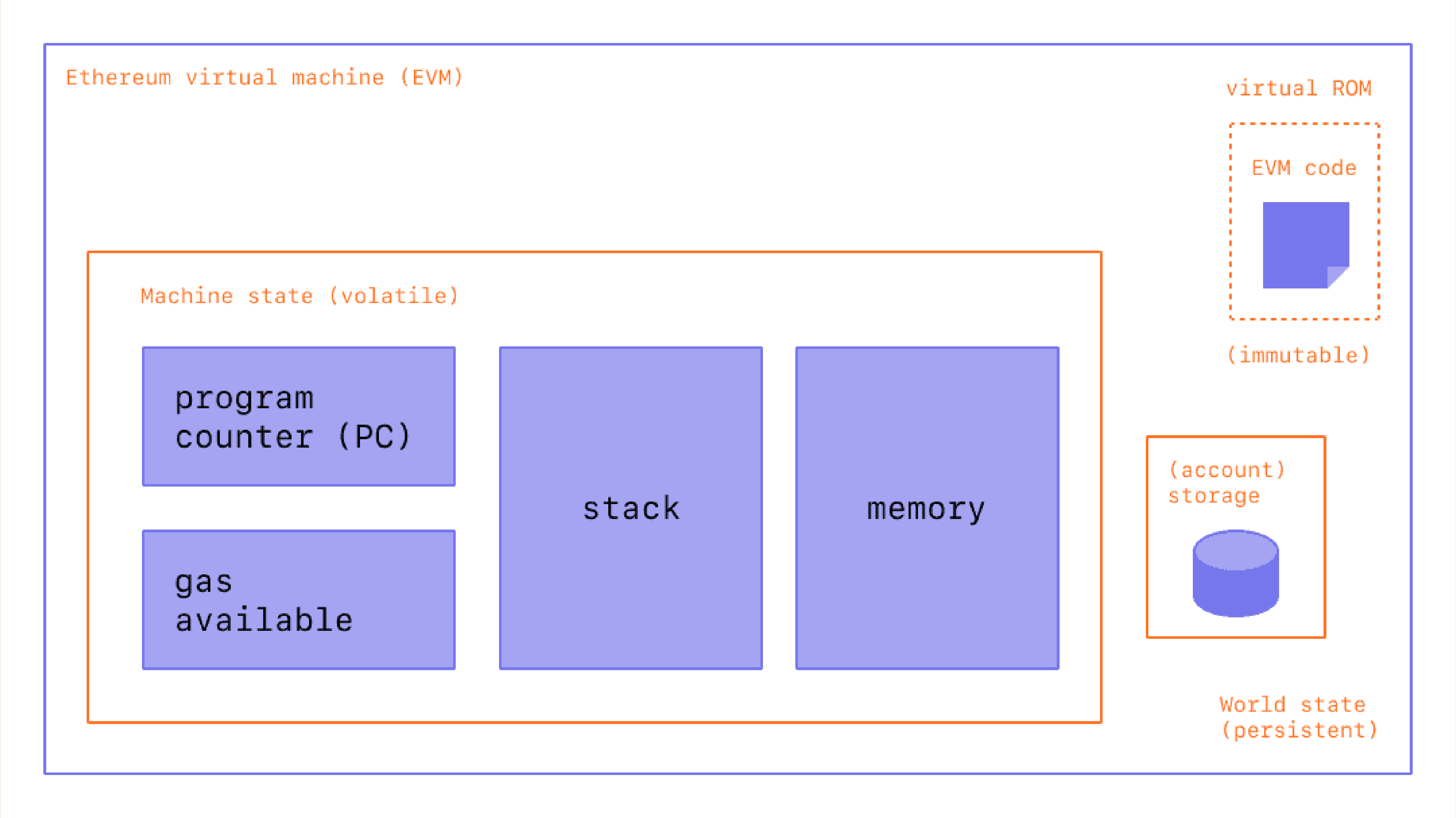
Ethereum Mining

- **Working of mining:**

7. Each node removes all transactions in the new block from their local mempool of unfulfilled transaction requests.

8. New nodes joining the network download all blocks in sequence, including the block containing our transaction of interest. They initialize a local EVM copy (which starts as a blank-state EVM), and then go through the process of executing every transaction in every block on top of their local EVM copy, verifying state checksums at each block along the way.

ETHEREUM VIRTUAL MACHINE (EVM)



ETHEREUM VIRTUAL MACHINE (EVM)

State

In the context of Ethereum, the state is an enormous data structure called a modified Merkle Patricia Trie, which keeps all accounts linked by hashes and reducible to a single root hash stored on the blockchain.

Transactions

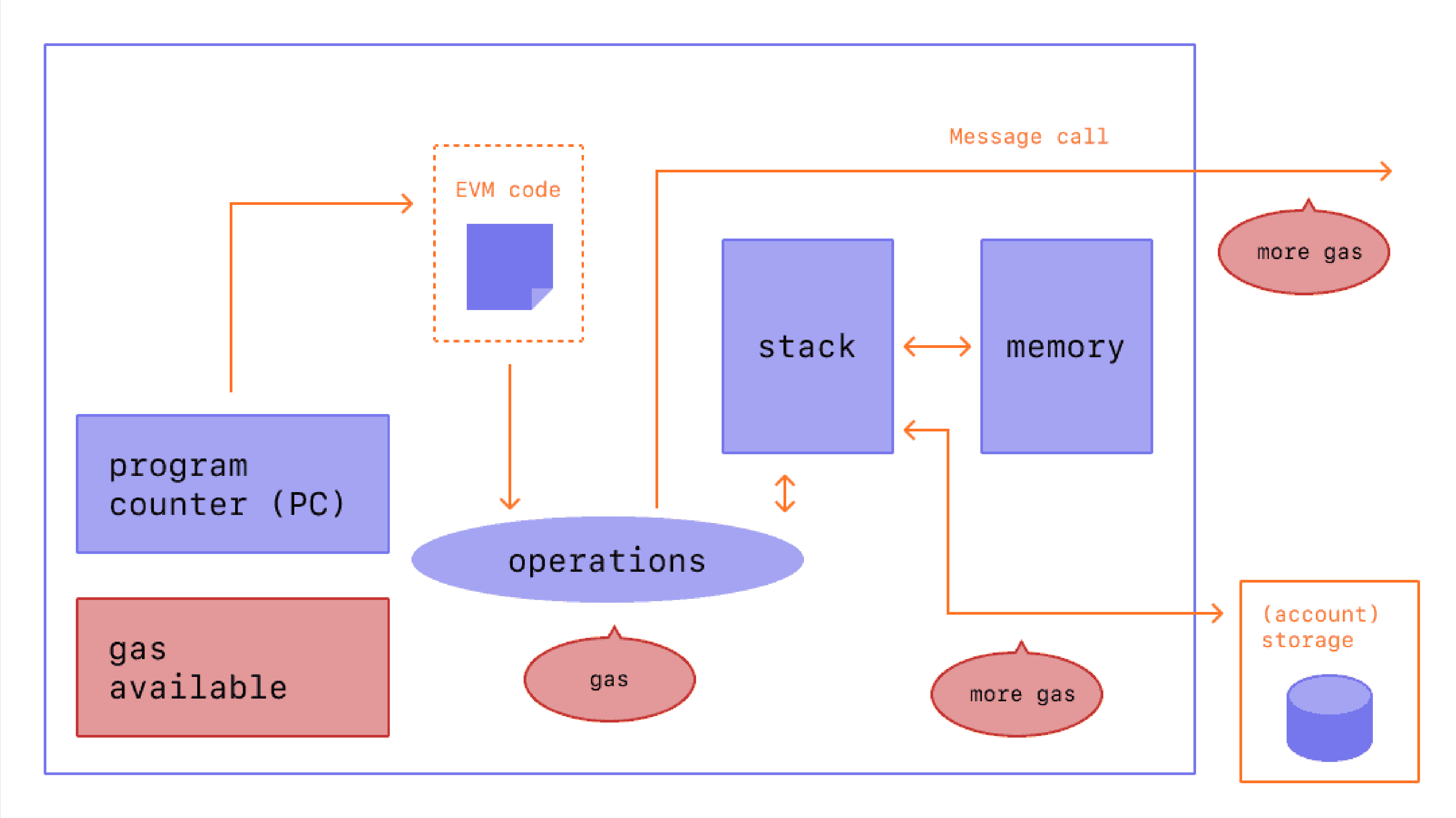
Transactions are cryptographically signed instructions from accounts. There are two types of transactions: those which result in message calls and those which result in contract creation.

EVM INSTRUCTIONS

The EVM executes as a stack machine(opens in a new tab) with a depth of 1024 items. Each item is a 256-bit word, which was chosen for the ease of use with 256-bit cryptography (such as Keccak-256 hashes or secp256k1 signatures).

Compiled smart contract bytecode executes as a number of EVM opcodes, which perform standard stack operations like XOR, AND, ADD, SUB, etc. The EVM also implements a number of blockchain-specific stack operations, such as ADDRESS, BALANCE, BLOCKHASH, etc.

ETHEREUM VIRTUAL MACHINE (EVM)

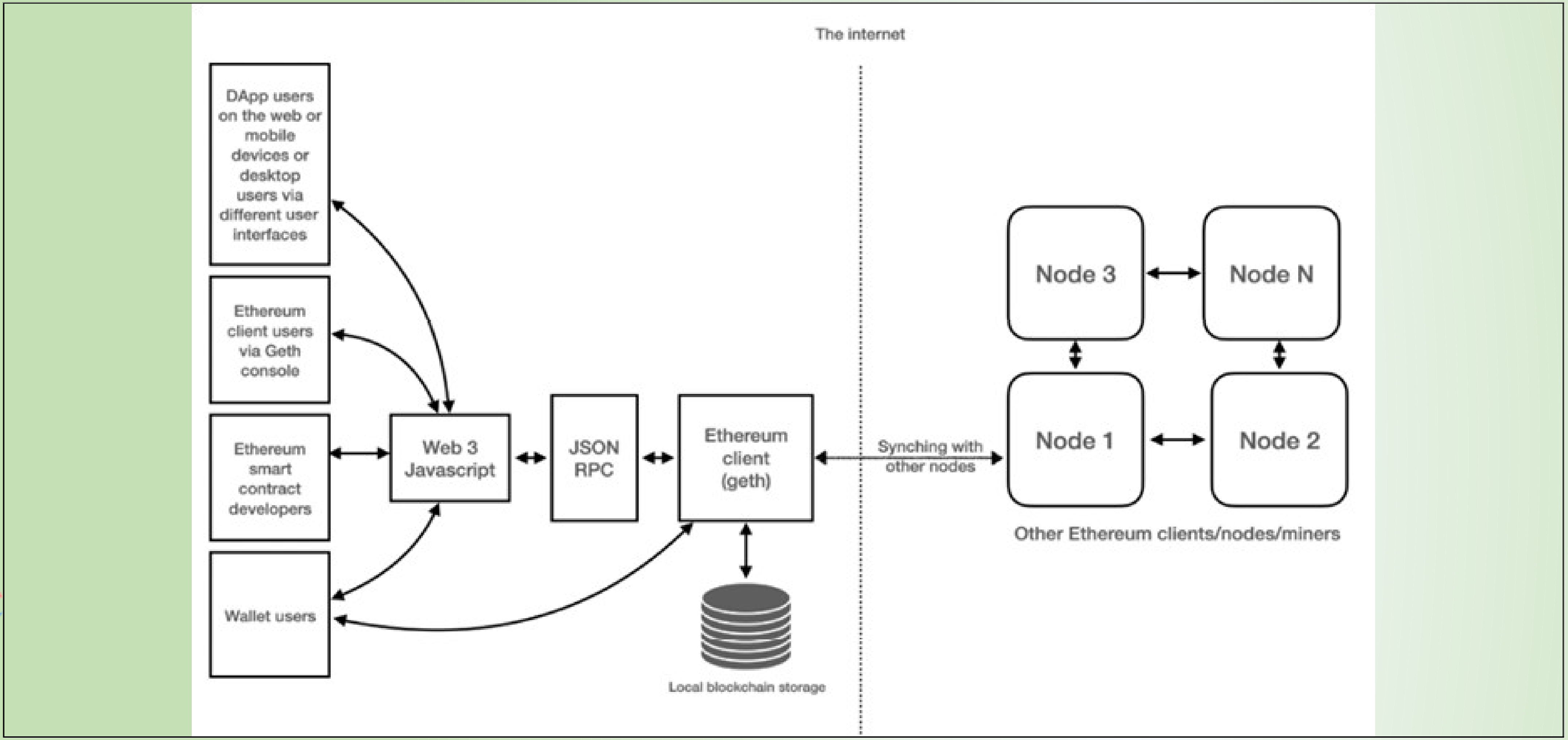


ETHEREUM Architecture

- The Ethereum blockchain stack consists of various components.
- At the core, there is the Ethereum blockchain running on the peer-to-peer Ethereum network.
- Secondly, there's an Ethereum client (usually Geth) that runs on the nodes and connects to the peer-to-peer Ethereum network from where blockchain is downloaded and stored locally.
- It provides various functions, such as mining and account management. The local copy of the blockchain is synchronized regularly with the network.
- Another component is the web3.js library that allows interaction with the geth client via the Remote Procedure Call (RPC) interface.

ETHEREUM Architecture

The overall Ethereum ecosystem architecture is visualized in the following diagram:


The internet
DApp users on the web or mobile devices or desktop users via different user interfaces
Ethereum client users via Geth console
Ethereum smart contract developers
Wallet users
Web 3 Javascript
JSON RPC
Ethereum client (geth)
Local blockchain storage
Synching with other nodes
Node 3
Node N
Node 1
Node 2
Other Ethereum clients/nodes/miners

ETHEREUM Architecture

- **Ethereum clients** provide a set of web3 APIs over JSON-RPC for DApps interacting with an Ethereum blockchain.
- From your web or wallet application, you can use the web3 object provided by the web3.js library to communicate with the Ethereum network.
- It works with any Ethereum client.
- Behind the scenes, it connects to a local or remote Ethereum node and makes RPC calls. In some sense, this is like the old client-server model, where DApps are the client, and the entire Ethereum network as a whole, acts as a server.
- To DApps, the Ethereum network is just like a giant world computer, assembled together with thousands of computing devices throughout the internet.

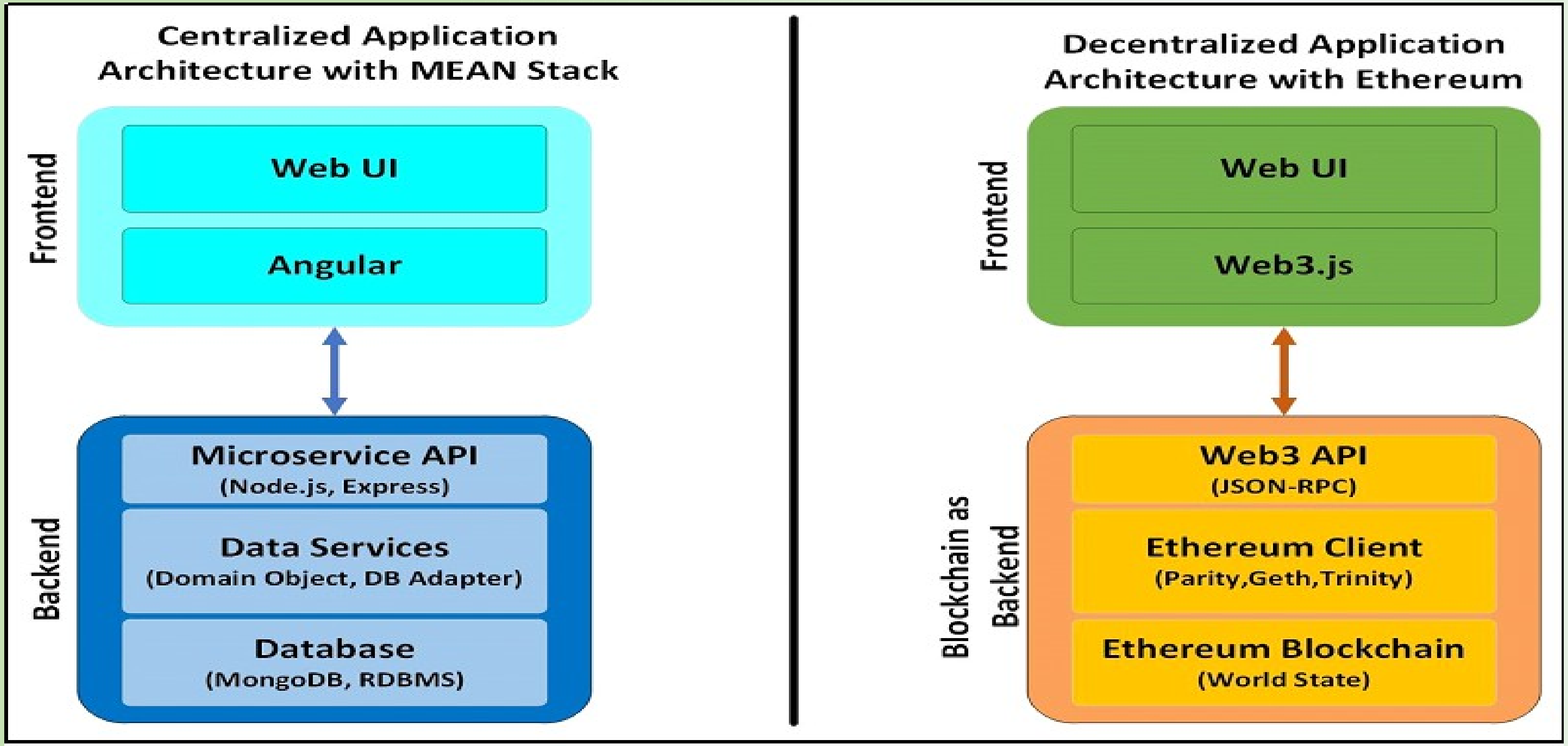
ETHEREUM Architecture

- Beyond smart contracts and the EVM, an Ethereum client provides all blockchain components to maintain world state and state transitions in the blockchain network, including the following:
    - Managing transaction and state transition with the Ethereum blockchain
    - Maintaining world state and account state
    - Managing P2P communication Block finalization with mining
    - Managing transaction pool
    - Managing cryptoassets, gas, ether, and tokens

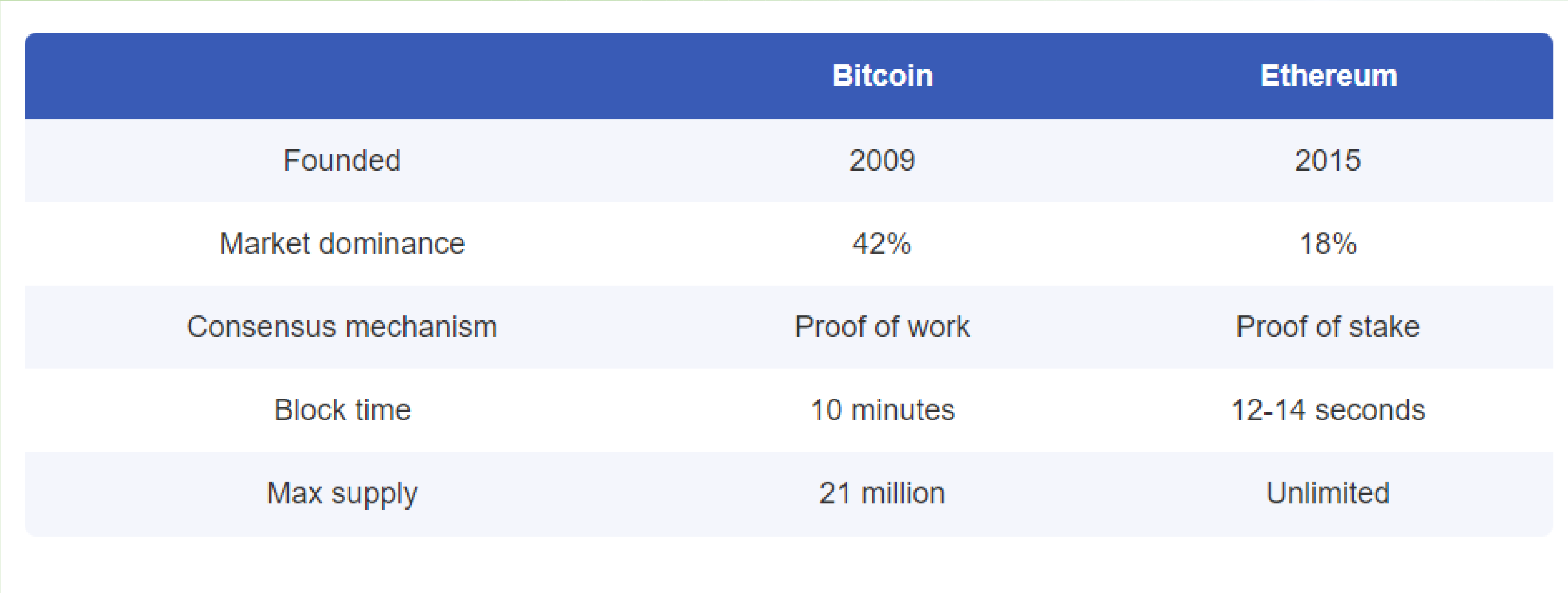
ETHEREUM Architecture

- **A DApp** is an application or service that runs on a blockchain network and enables direct interaction between consumers and providers, for example, connecting buyers and sellers in a decentralized marketplace.
- Similar to the centralized application architecture, a DApp usually involves a decentralized backend that runs on the blockchain network and a centralized frontend that allows end users to access their wallets and make a transaction.
- The below diagram shows the differentiation between centralized and decentralized applications:

ETHEREUM Architecture

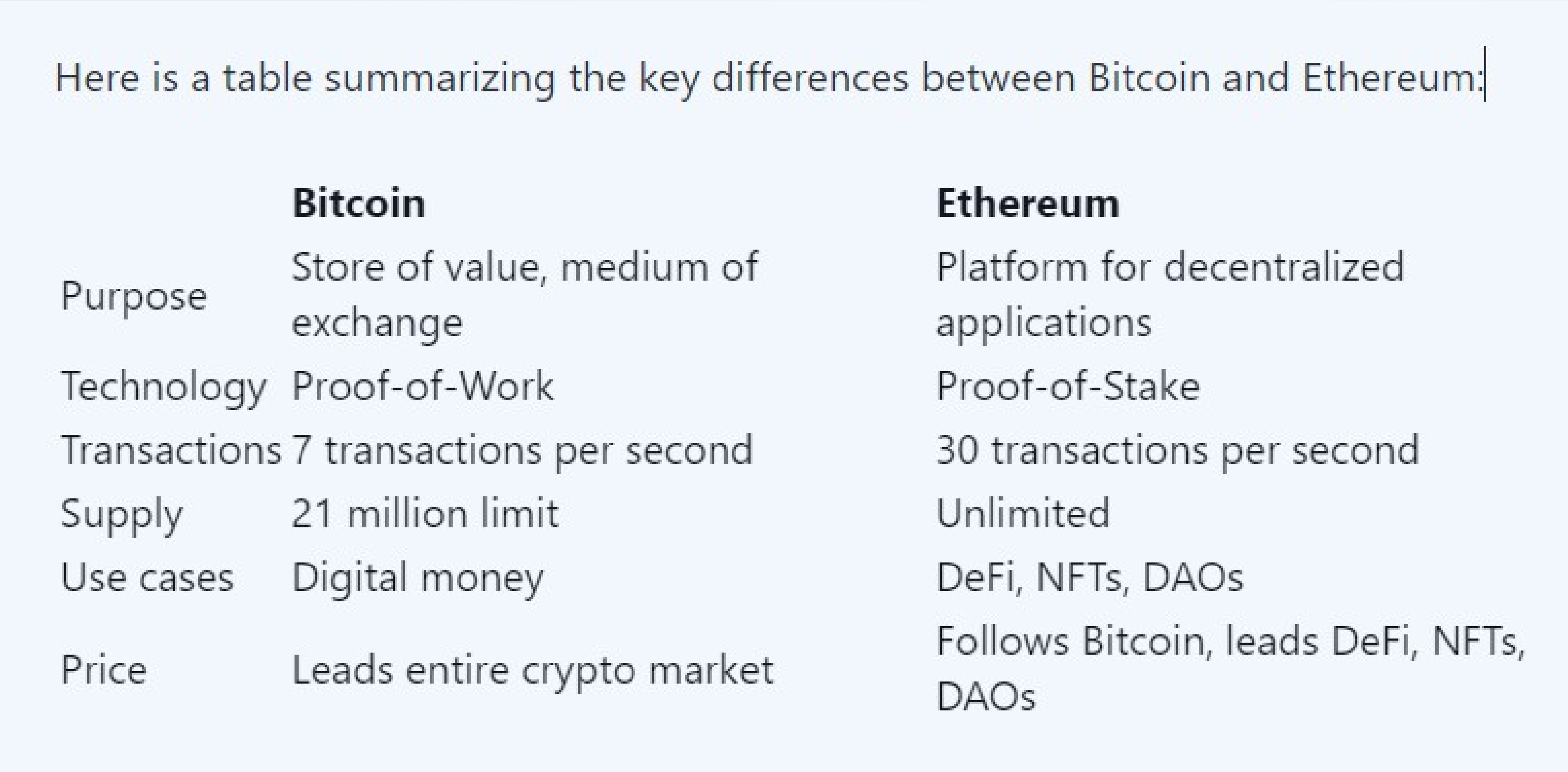


BITCOIN vs ETHEREUM



	Bitcoin	Ethereum
Founded	2009	2015
Market dominance	42%	18%
Consensus mechanism	Proof of work	Proof of stake
Block time	10 minutes	12-14 seconds
Max supply	21 million	Unlimited

BITCOIN vs ETHEREUM



Here is a table summarizing the key differences between Bitcoin and Ethereum:

	Bitcoin	**Ethereum**
Purpose	Store of value, medium of exchange	Platform for decentralized applications
Technology	Proof-of-Work	Proof-of-Stake
Transactions	7 transactions per second	30 transactions per second
Supply	21 million limit	Unlimited
Use cases	Digital money	DeFi, NFTs, DAOs
Price	Leads entire crypto market	Follows Bitcoin, leads DeFi, NFTs, DAOs

- **References:**

  - **https://en.wikipedia.org/wiki/Ethereum**
  - **https://ethereum.org/en/developers/docs/intro-to-ethereum/**
  - **https://www.coding-bootcamps.com/blog/ethereum-architecture-and-components.html**
  - **https://www.bitcoin.com/get-started/difference-between-bitcoin-and-ethereum/**
  - **https://www.forbes.com/advisor/in/investing/cryptocurrency/bitcoin-vs-ethereum/**