

Ethereum

Saravanan Vijayakumaran

Department of Electrical Engineering
Indian Institute of Technology Bombay

February 4, 2026

Ethereum

- A blockchain platform for building decentralized applications
 - Application code and state is stored on a blockchain
 - Transactions cause code execution and update state, emit events, and write logs
 - Frontend web interfaces can respond to events and read logs
- Most popular smart contract platform
 - Initial Coin Offerings (ICOs)
 - Non-Fungible Tokens (NFTs)
 - Decentralized Finance (DeFi)
- Ethereum History
 - Proposed by then 19 y.o. Vitalik Buterin in 2013
 - Vitalik visited the Mastercoin team in Oct 2013
 - Released the Ethereum white paper in Dec 2013
 - Bitcointalk announcement on Jan 24th, 2014
 - A presale in July-Aug 2014 collected 31,591 BTC worth 18 million USD in return for 60,102,216 ETH
 - About 12 million ETH created to pay early contributors and setup non-profit foundation
 - Release 1.0 on July 30, 2015
 - Switched to proof-of-stake on September 15, 2022

Bitcoin vs Ethereum

	Bitcoin	Ethereum
Specification	Bitcoin Core client	Ethereum yellow paper
Consensus	SHA256 PoW	Proof-of-Stake
Contract Language	Script	EVM bytecode
Block interval	10 minutes	≈ 12 seconds ¹
Block size limit	4 MB	141 KB to 272 KB (Jan 2024) ²
Currency supply	Fixed to 21 million	Variable (120 million in Jan 2024) ³
Currency units	1 BTC = 10 ⁸ satoshi	1 ETH = 10 ¹⁸ Wei

¹<https://etherscan.io/chart/blocktime>

²<https://etherscan.io/chart/blocksize>

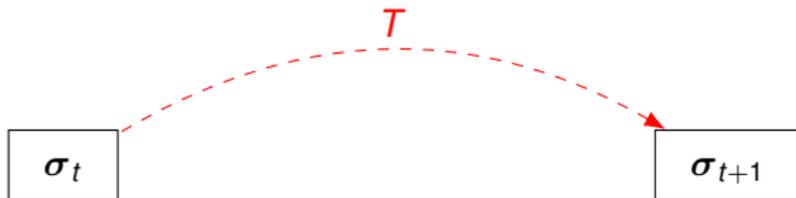
³<https://etherscan.io/chart/ethersupplygrowth>

Ethereum Architecture

- Specified in the Ethereum yellow paper by Gavin Wood
- Implemented in Go, C++, Python, Rust
- Yellow paper models Ethereum as a transaction-based state machine

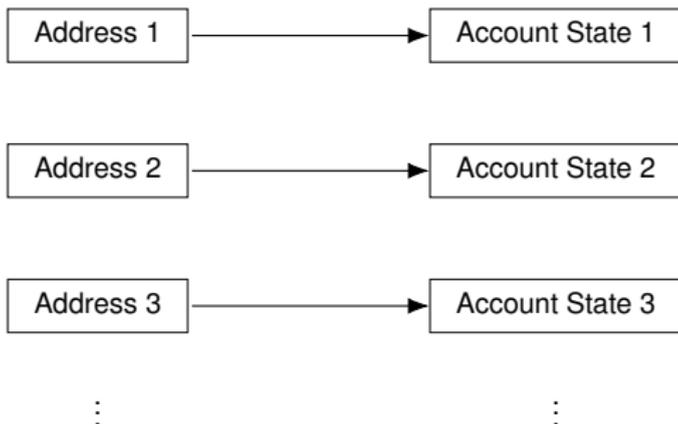
$$\sigma_{t+1} = \Upsilon(\sigma_t, T)$$

- σ_t = State at time t
- T = Transaction
- Υ = Transaction-level state-transition function



Ethereum World State

- World state consists of **accounts**
- Each account has an address and account state



- The world state is maintained in a Merkle Patricia trie
 - Trie = Tree optimized for information **retrieval**
 - Patricia = Practical Algorithm To Retrieve Information Coded in Alphanumeric
 - Merkle: Tree nodes are hashed to generate a root hash

Ethereum Accounts

- Account types
 - **Externally owned accounts (EOAs)**: Controlled by private keys
 - **Contract accounts**: Controlled by contract code



- Account state
 - **nonce**: Number of transactions sent or contract-creations made
 - **balance**: Number of Wei owned by this account
 - **storageRoot**: Root hash of account storage Merkle Patricia trie
 - **codeHash**: Hash of EVM code if contract account
- The storage root and code hash will be empty for EOA accounts
- For contract accounts, the code and storage variables will be stored in a key-value database
- Each account has a 20-byte address
 - EOA address = Right-most 20 bytes of Keccak-256 hash of public key
 - Contract address = Right-most 20 bytes of Keccak-256 hash of [senderAddress, nonce]

Keccak-256

- Cryptographic hash function used by Ethereum
- NIST announced competition for new hash standard in 2006
- Keccak declared winner in 2012
- In August 2015, FIPS 202 “*SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*” was approved
- Ethereum adopted Keccak-256 but NIST changed the padding scheme
- Keccak-256 and SHA3-256 give different outputs for the same message
 - <https://ethereum.stackexchange.com/questions/550/which-cryptographic-hash-function-does-ethereum-use>

Ethereum Smart Contracts

Ethereum Contracts

- “Smart contracts” is a misnomer
 - Not smart or legally binding
- Contract = Collection of functions and state at a specific address
- Contract logic is stored in EVM bytecode
 - EVM Opcodes <https://www.evm.codes/>
- Written in a high level language which compiles to bytecode
 - Solidity <https://solidity.readthedocs.io>
 - Vyper <https://vyper.readthedocs.io>
- Components of a contract
 - State variables
 - Functions
 - Events

SimpleStorage Contract

```
pragma solidity >=0.4.16 <0.9.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

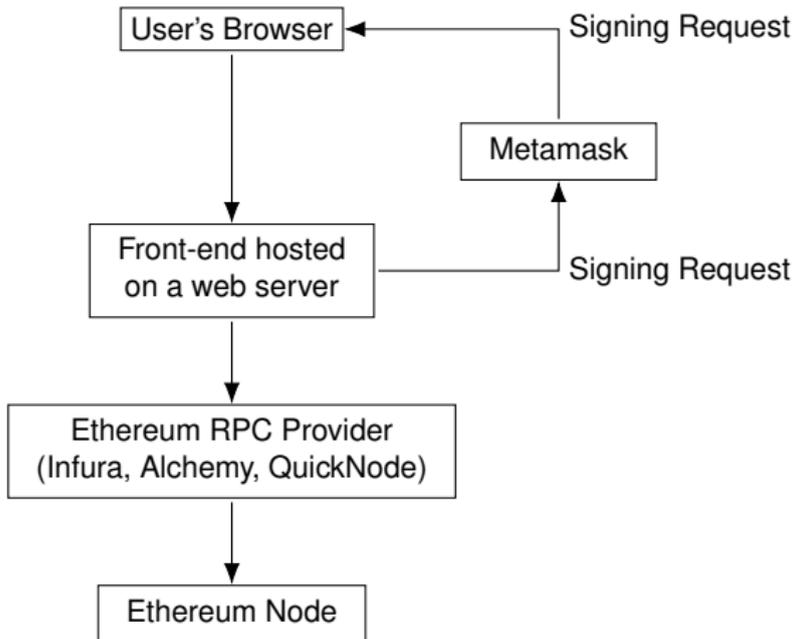
    function get() public view returns (uint) {
        return storedData;
    }
}
```

- `storedData` is a 256-bit unsigned integer
- Once the contract is deployed on Ethereum, anyone can set the value in `storedData`
 - Setting the value involves sending an Ethereum transaction
 - Costs transaction fees
- Anyone with RPC access to a full Ethereum node can read the value in `storedData` (no transaction or fees required)

Deploying a Contract

- Deploying a contract on Ethereum requires a contract creation transaction
 - Contract needs to be first compiled to get EVM bytecode
 - An externally owned account needs to pay the transaction fees for contract creation
- Demo using Remix on Sepolia Testnet
 - Remix is a browser-based IDE for smart contract development
 - Testnets are instances of a blockchain used for testing
 - Testnet coins are available from websites called faucets
 - Metamask browser plugin can be used to generate an Ethereum address to receive the testnet coins
 - Instructions at <https://www.respectedsir.com/ethlab/>

Anatomy of an Ethereum Application



Applications

- **Ethereum Name Service** <https://ens.domains/>
- **OpenSea NFT Marketplace** <https://opensea.io/>
- **Paragraph Publishing Platform** <https://paragraph.com>

References

- **Yellow paper** <https://ethereum.github.io/yellowpaper/paper.pdf>
- **A Prehistory of the Ethereum Protocol**
<https://vitalik.ca/general/2017/09/14/prehistory.html>
- **Ethereum announcement on Bitcointalk**
<https://bitcointalk.org/index.php?topic=428589.0>
- **History of Ethereum** <https://ethereum.org/history>
- **Ethereum App Architecture** <https://www.preethikasireddy.com/post/the-architecture-of-a-web-3-0-application>
- **Testnet Opensea NFT Marketplace** <https://testnets.opensea.io/>
- **Solidity Documentation** <https://solidity.readthedocs.io>
- **Remix IDE** <https://remix.ethereum.org>
- **Metamask** <https://metamask.io/>
- **Solidity by Example** <https://solidity-by-example.org/>