L05: Ethereum & Smart Contracts

BSc Blockchain Course

Digital Finance

2026

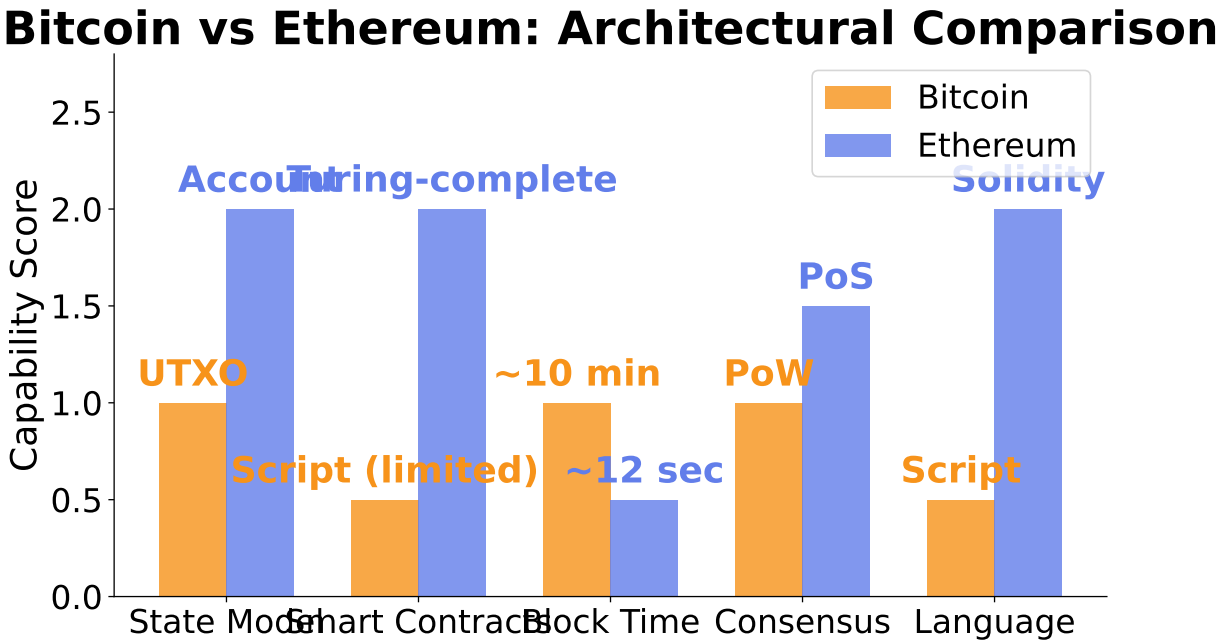
Learning Objectives

By the end of this lesson, you will be able to:

1. Compare Ethereum's account model with Bitcoin's UTXO model
2. Explain the Ethereum Virtual Machine (EVM) architecture
3. Understand gas mechanics and EIP-1559 fee market
4. Describe smart contract lifecycle and storage
5. Analyze Ethereum's state management via tries

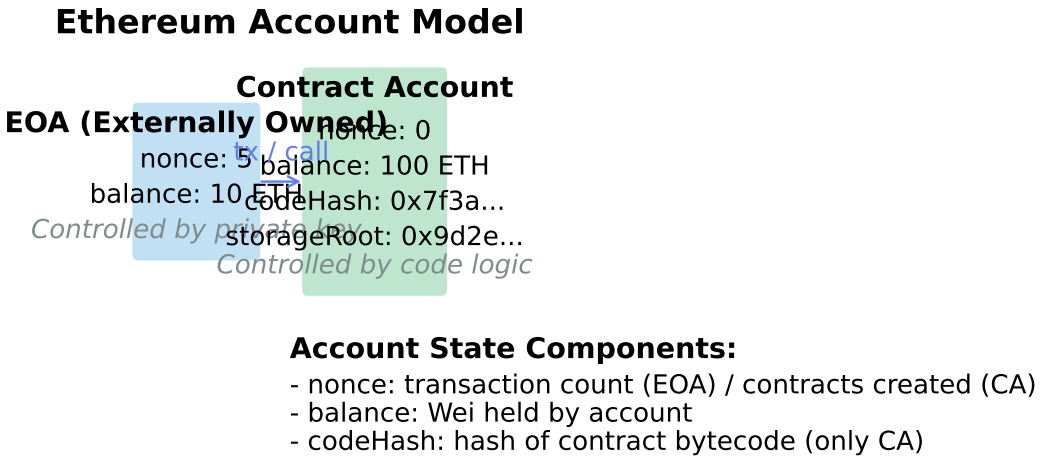
Ethereum extends blockchain from payments to programmable contracts.

Ethereum vs Bitcoin



Bitcoin: digital gold. Ethereum: world computer.

Account Model

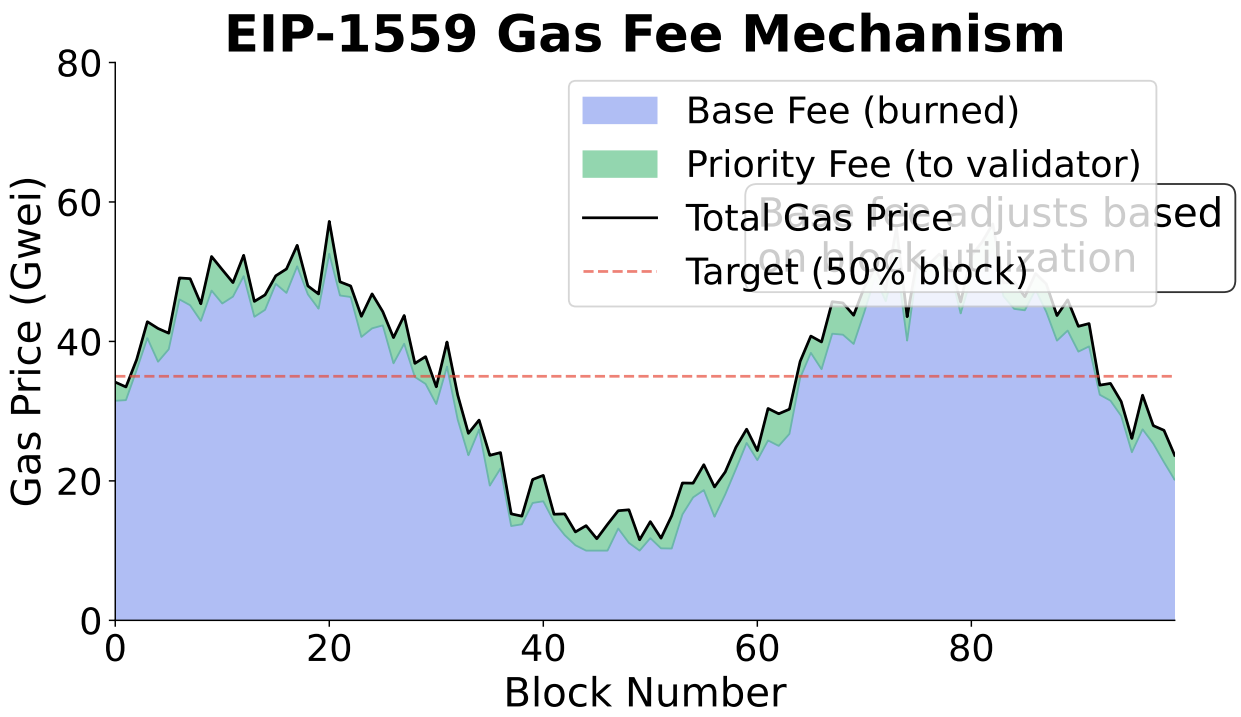


Account State Components:

- nonce: transaction count (EOA) / contracts created (CA)
- balance: Wei held by account
- codeHash: hash of contract bytecode (only CA)

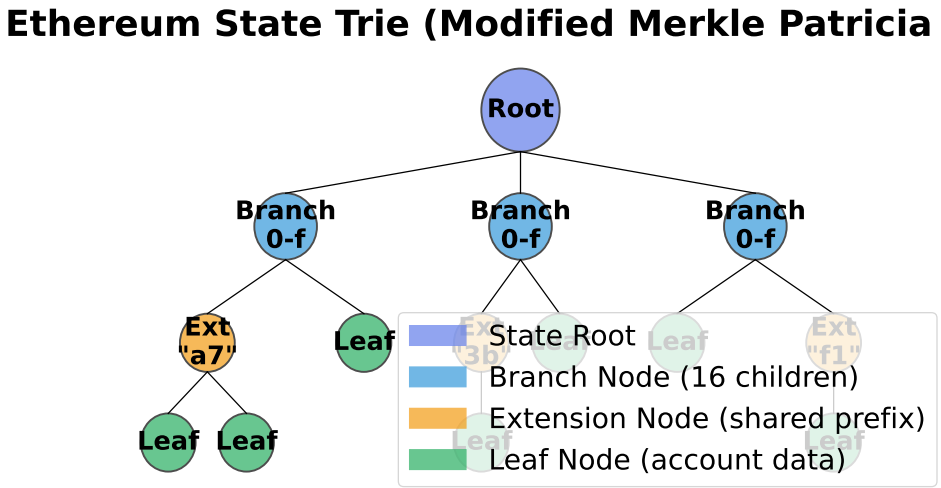
EOAs controlled by keys; contracts controlled by code.

Gas Mechanics



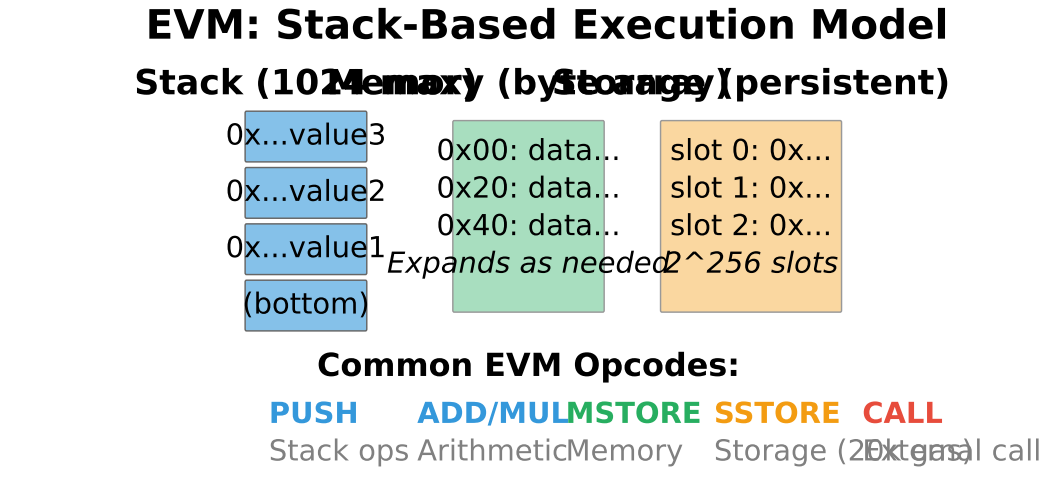
EIP-1559 burns base fee, making ETH deflationary under high usage.

State Trie



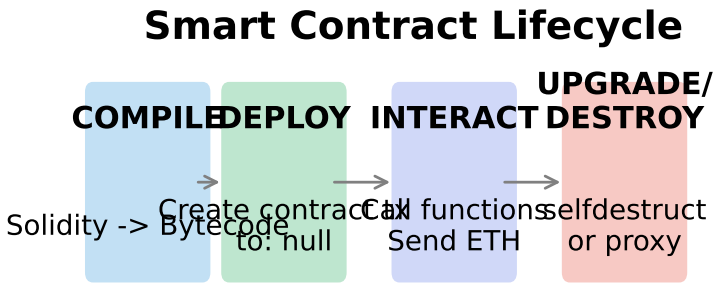
Merkle Patricia Trie enables efficient state proofs.

EVM Execution



Stack-based architecture with deterministic execution.

Contract Lifecycle



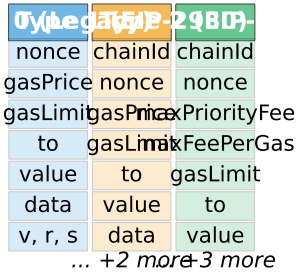
Key Concepts:

- Constructor runs ONCE at deployment (initialization)
- Contract address = keccak256(deployer, nonce)
- Code is immutable after deployment (unless proxy pattern)
- selfdestruct sends remaining ETH to specified address

Code is law – immutable once deployed (without proxy patterns).

Transaction Types

Ethereum Transaction Types

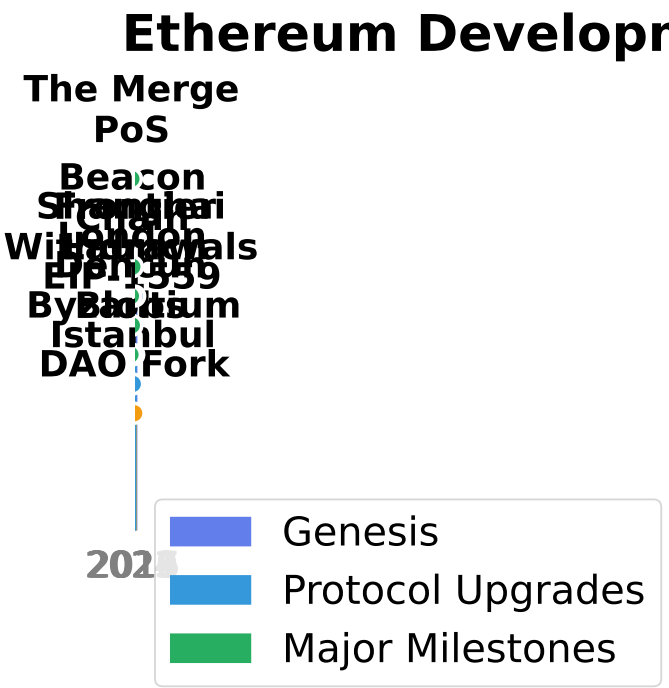


Type 2 (EIP-1559) is now standard - enables predictable fees and ETH burning

accessList pre-declares storage slots for gas savings

EIP-1559 (Type 2) is now the default transaction format.

Ethereum Roadmap



Future

Surge (sharding)

Verge (verkle)

Purge (history)

Splurge (misc)

From PoW to PoS, now scaling via L2 and data availability.

Key Takeaways

Remember These Points

1. Ethereum uses account model (not UTXO)
2. EVM is Turing-complete stack machine
3. Gas prices follow EIP-1559 (base fee + priority fee)
4. State stored in Modified Merkle Patricia Trie
5. Contracts are immutable; use proxies for upgrades

Next Lesson: Solidity Programming – syntax, patterns, security.