Ethereum Virtual Machine

What is Ethereum?

“[A] system such that users can be guaranteed that no matter with which other individuals, systems or organisations they interact, they can do so with absolute confidence in the possible outcomes and how those outcomes might come about.”

ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER, EIP-150 REVISION, DR. GAVIN WOOD FOUNDER, ETHEREUM & ETHCORE
GAVIN@ETHCORE.IO

What is Ethereum?

- Many details with many implementations and choices

Permissioned Burrow Ethereum Chain

Public Ethereum Chain

What is Ethereum?

Impartial, autonomous execution of contracts

What is a (Smart) Contract?

- “A contract is a voluntary arrangement between two or more parties that is enforceable by law as a binding legal agreement.” - Wikipedia
    - The arrangement is described in natural language
    - Enforcement is handled manually by the law
    - The outcome depends on interpretation
- An Ethereum smart contract is a voluntary arrangement between two or more parties that is enforceable by Ethereum.
    - The arrangement is described in Ethereum Virtual Machine byte code
    - Enforcement is handled automatically by the network
    - The outcome is deterministic

What is a Smart Contract?

State transition function

The Ethereum Virtual Machine

- A *quasi*-Turing-complete, specialized instruction set:
  - `0x00 STOP; 0x01 ADD; 0x02 MUL; …; 0x0a EXP; 0x0b SIGNEXTEND`
  - `0x10 LT; 0x11 GT; …; 0x1a BYTE`
  - `0x20 SHA3; 0x30 ADDRESS; …; 0x3a GASPRICE; …; 0x40 BLOCKHASH; …; 0xa0 LOG0`
- A 256-bit, stack-based, big-endian architecture
- Global state is the machine’s persistent storage
- Execution is limited by Gas

The Ethereum Virtual Machine

- A *quasi*-Turing-complete, specialized instruction set:
  - `0x00 STOP; 0x01 ADD; 0x02 MUL; …; 0x0a EXP; 0x0b SIGNEXTEND`
  - `0x10 LT; 0x11 GT; …; 0x1a BYTE`
  - `0x20 SHA3; 0x30 ADDRESS; …; 0x3a GASPRICE; …; 0x40 BLOCKHASH; …; 0xa0 LOG0`
- A 256-bit, stack-based, big-endian architecture
- Global state is the machine's persistent storage
- Execution is limited by Gas

State transition function executor

The Ethereum Virtual Machine

What it doesn’t do:

- Manage accounts and associated storage
- Create new externally owned accounts
- Compile EVM code
- Validate identities or permissions
- Transfer value between accounts
- Communicate with other virtual machines
- Handle exceptions

Batteries not included...

These are provided by Ethereum
(or the platform using the EVM)

State - Accounts and Storage

- Everything in state is associated with an account.
- Each account has a:
  - Contract The contract associated with the account
  - Balance The value (in Ether) associated with the account
  - Storage A set of (256-bit, 256-bit) key-value pairs defined by the contract

The EVM runs on Gas

- “[A]ny given fragment of programmable computation...has a universally agreed cost in terms of gas.”
- Gas is purchased from miners with Ether
- Gas price is set by supply and demand:
  - Transactors specify a gas price for each transaction they want processed
  - Miners choose which transactions to process based on the gas price