Ethereum Virtual Machine

Ethereum Virtual Machine

EVM code

```
.code
  PUSH 60             contract Ballot {\n
    struct...
  PUSH 40             contract Ballot {\n
    struct...
  MSTORE              contract Ballot {\n
    struct...
  CALLVALUE                function Ballot(uint8 _numProp...
  ISZERO              function Ballot(uint8 _numProp...
  PUSH [tag] 1             function Ballot(uint8 _numProp...
  JUMPI               function Ballot(uint8 _numProp...
  PUSH 0              function Ballot(uint8 _numProp...
  DUP1                function Ballot(uint8 _numProp...
  REVERT              function Ballot(uint8 _numProp...
tag 1                 function Ballot(uint8 _numProp...
  JUMPDEST                 function Ballot(uint8 _numProp...
  PUSH 40             function Ballot(uint8 _numProp...
  MLOAD               function Ballot(uint8 _numProp...
  PUSH 20             function Ballot(uint8 _numProp...
  DUP1                function Ballot(uint8 _numProp...
  PUSHSIZE                 function Ballot(uint8 _numProp...
  DUP4                function Ballot(uint8 _numProp...
  CODECOPY                 function Ballot(uint8 _numProp...
  DUP2                function Ballot(uint8 _numProp...
  ADD                 function Ballot(uint8 _numProp...
  PUSH 40             function Ballot(uint8 _numProp...
  MSTORE              function Ballot(uint8 _numProp...
  DUP1                function Ballot(uint8 _numProp...
  DUP1                function Ballot(uint8 _numProp...
```

EVM Features

- Stack of max depth of 1024
- 32-byte words
- Dedicated crypto opcodes
  - SHA-3
- Big num multiply
- GF-256 operators

Ethereum Memory

Storage: $\{0,1\}^{256}$ —> $\{0,1\}^{256}$ map (permanent)

Memory: $\{0,1\}^{256}$ —> $\{0,1\}^{256}$ map (volatile)

- Memory is zero initialized
- Memory is arranged in 256-bit words
- Storage is very **expensive**

Ethereum Memory

Storage: $\{0,1\}^{256}$ —> $\{0,1\}^{256}$ map (permanent)

Memory: $\{0,1\}^{256}$ —> $\{0,1\}^{256}$ map (volatile)

- Memory is zero initialized
- Memory is arranged in 256-bit words
- Storage is very **expensive**

Yellowpaper --> fee of 20k gas to store a 256 bit word
Gas Price = 10 Gwei = 10^10 Wei = 10^(-8) ETH
1 kilobyte --> 640k gas --> 0.0064 ETH = 6.4 USD

The cost of storing 1 kb is currently 6.4 USD

EVM provides an API for programmer

Input

- Transaction information: sender, value, gas limit
- Resource usage: gas remaining, memory used
- Block info: depth, timestamp, miner, hash

Output

- Sent messages
- Write to logs
- Self destruct