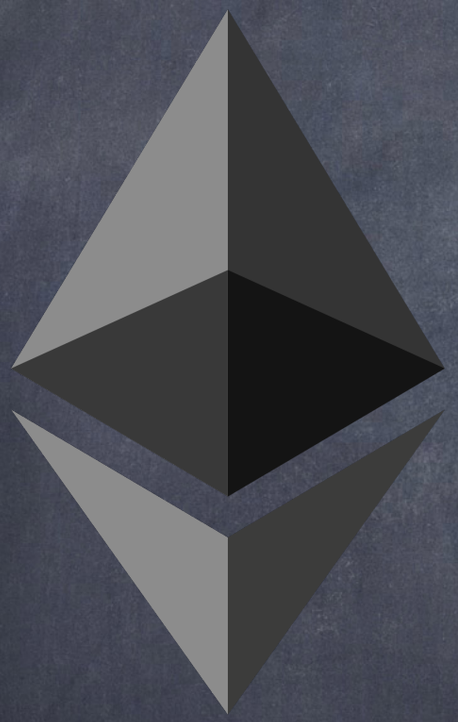
Ethereum 101

Secureum Bootcamp

#1

Ethereum



Blockchain

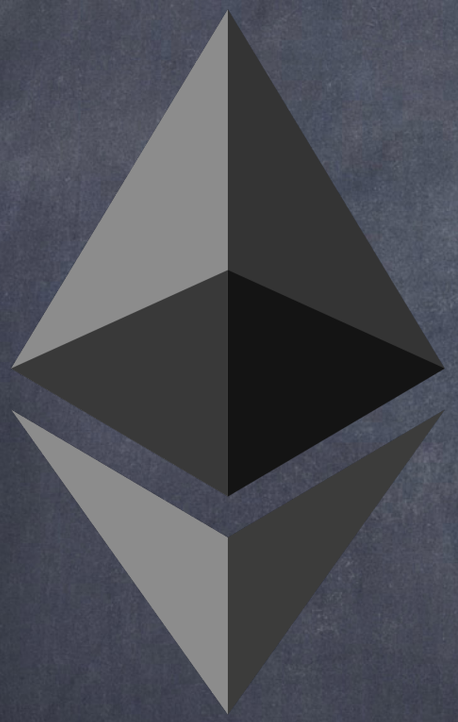
Next-generation

Smart Contracts

Decentralized Application Platform

#2

Turing Complete



Turing-complete Programming Language

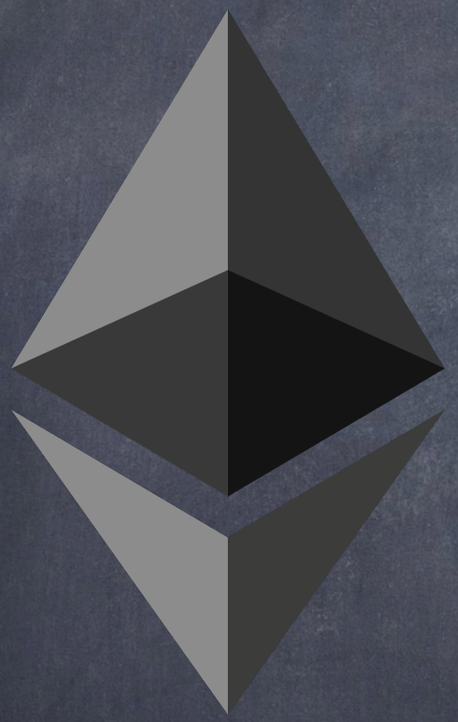
Smart Contracts -> Decentralized Applications

State -> Rule -> State'

Any State/Rule -> Any Application

#3

Infrastructure



Open-source
Protocol & Code

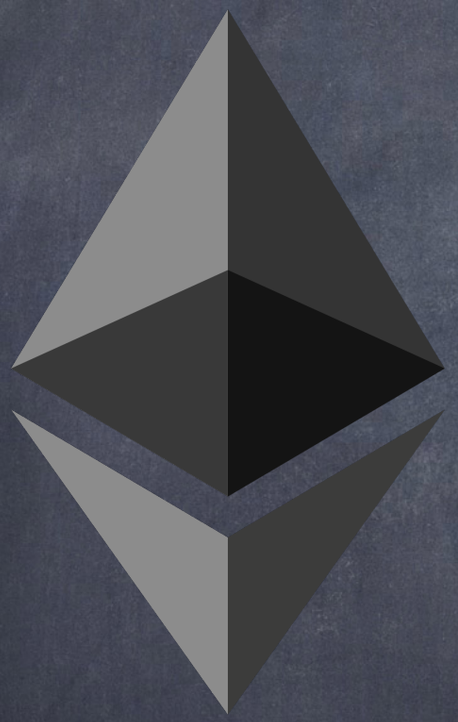
Blockchain -> State
Store & Synchronize

ether -> Native Currency
Meter & Constrain

World Computer

#4

Properties



Permissionless Apps
Built-in Economics

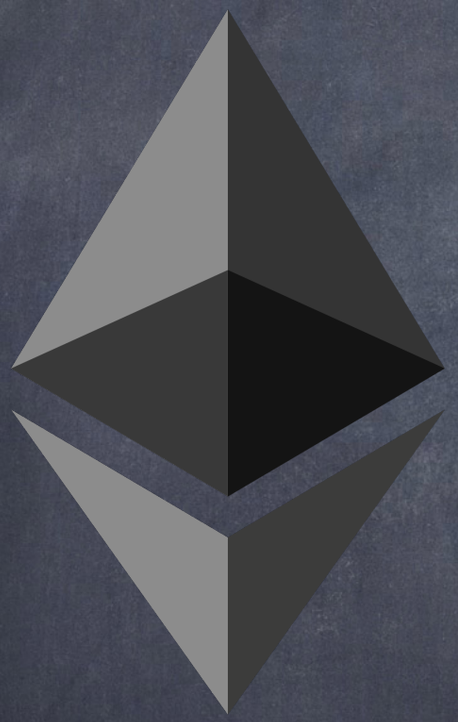
High Availability
High Auditability

High Transparency
Neutrality

Censorship Resistant
Lower Counter-party Risk

#5

Purpose



Not Currency
Not Payment Network

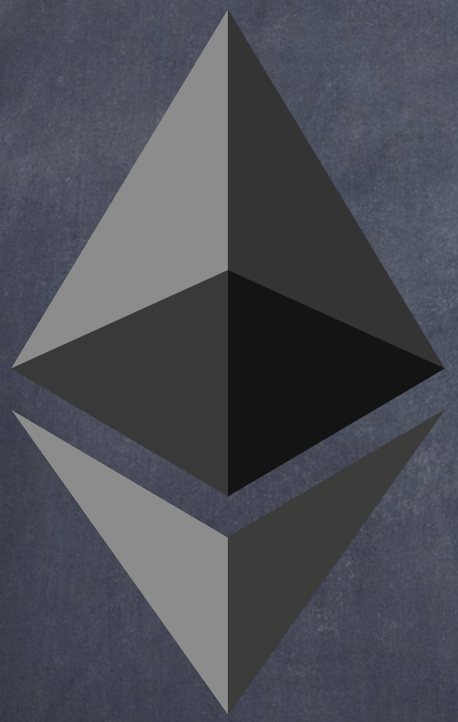
ether -> Operation
Necessary & Integral

Utility Token

Use -> Ethereum
Pay -> ether

#6

Vs Bitcoin Script



Script -> Limited Scripting Language

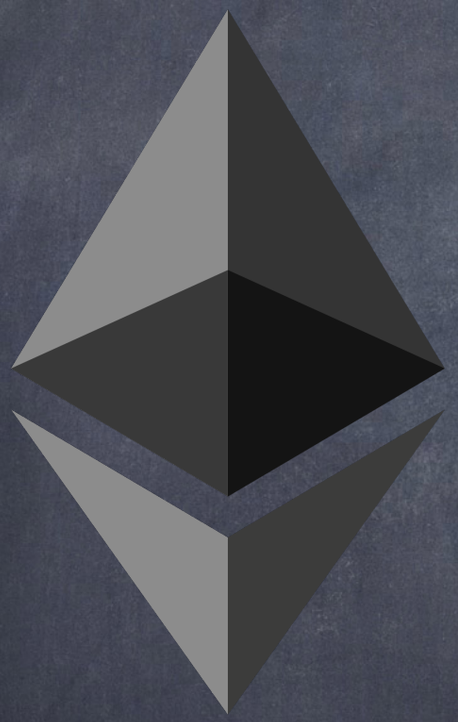
Script -> true/false Spending Conditions

EVM -> General-purpose Programming Language

Turing Complete
Arbitrary Code/Complexity

#7

Vs Bitcoin Blockchain



Bitcoin Blockchain
bitcoin -> Ownership

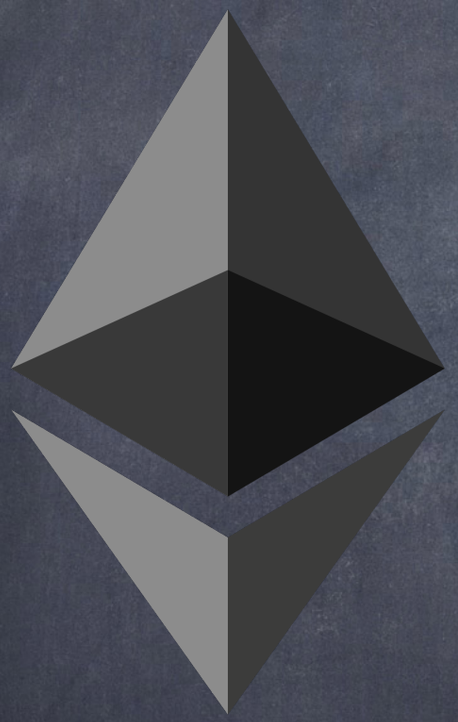
Bitcoin UTXO
Transfer -> Transition

Ethereum Blockchain
General-purpose State

Ethereum Account/Balance
State -> Transition

#8

Core Components



P2P Network
TCP Port 30303: ÐΞVp2p

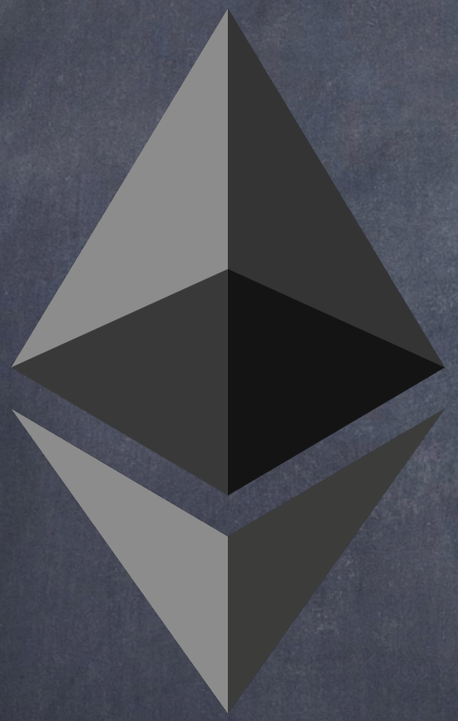
Transaction: sender, recipient, value, data

State Machine -> EVM
HLLs (Solidity) -> bytecode

Data Structures
Merkle Patricia Tree

#9

More Core Components



Consensus Algorithm
Nakamoto -> PoW

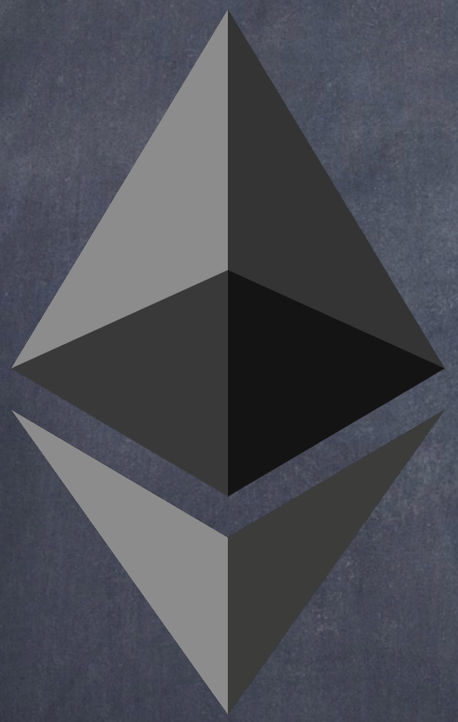
PoW -> PoS
Ethereum 2.0 or Serenity

Economic Security
PoW -> Ethash

Clients: Geth, Erigon,
Nethermind, OpenEthereum

#10

Halting Problem



Turing Complete -> Halting Problem

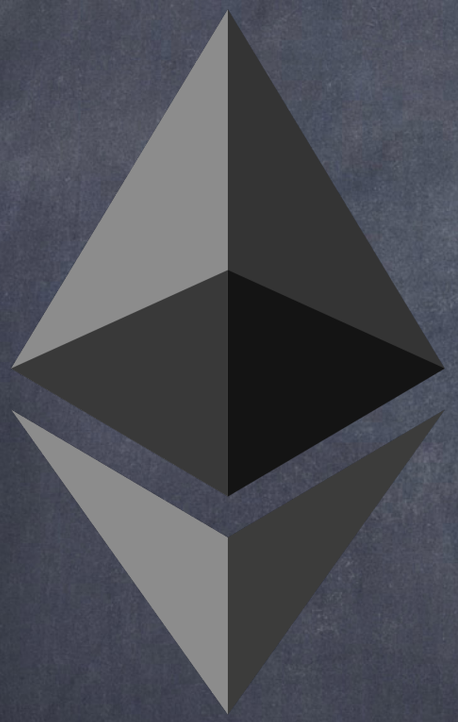
Arbitrary Program/Input
Predict -> Stop?

Smart Contracts
Predict -> How Long? Stop?

Constrain Resources
Metering -> Gas

#11

Gas
Metering



EVM -> Smart Contract
Instruction -> Gas

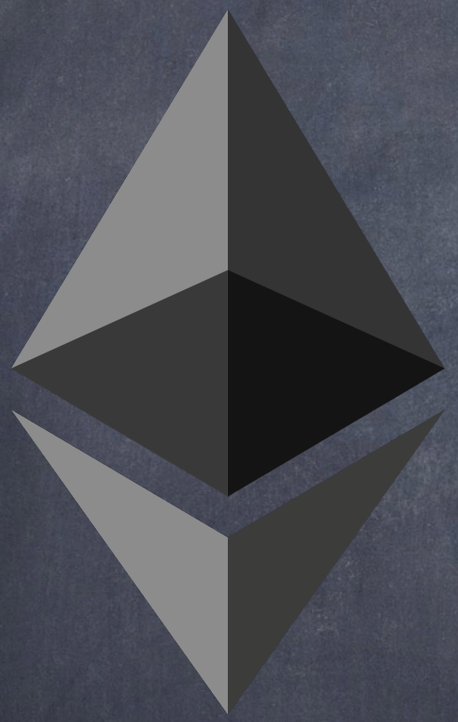
Transaction -> Contract
Gas -> Limit

Gas Exceeds -> Limit?
EVM Terminates -> Exec

Turing Complete
Gas -> Constrain

#12

Gas Mechanism



Transaction -> Gas
Price -> ether

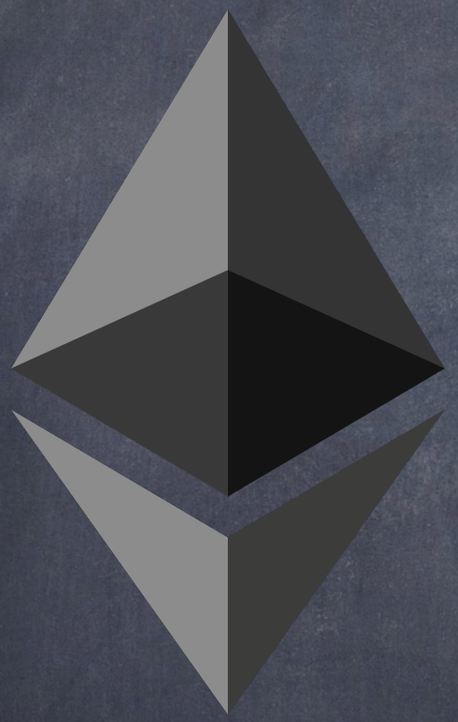
Gas Price -> Not Fixed
Varies -> Demand

Gas -> Purchase
Transaction -> Execute

Gas -> Consumed
Remaining -> Refunded

#13

ĐApp



Decentralized Application

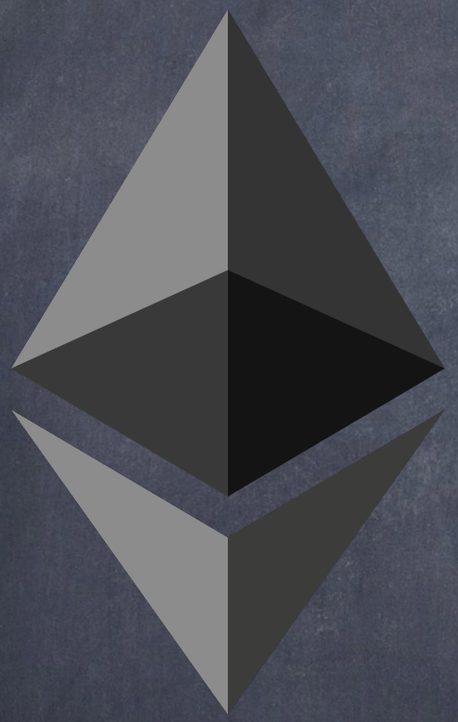
Web App + P2P Infrastructure

P2P -> Compute, Storage or Network

ĐApp -> Web App + Smart Contract

#14

Web 2.0 Vs
Web 3.0



Web 2.0 -> Client-Server
Existing Infrastructure

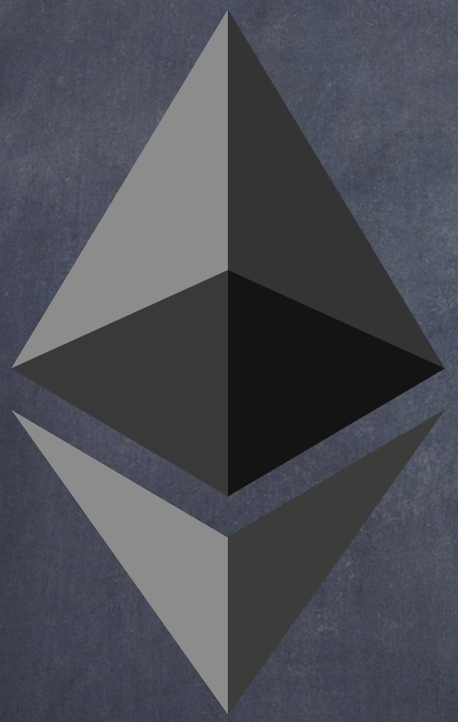
Centrally Managed
Freemium/Ad Biz Models

Web 3.0 -> P2P
Compute/Storage/Network

Decentralized
Incentivized Participation

#15

Ethereum Triad



Ethereum -> Compute

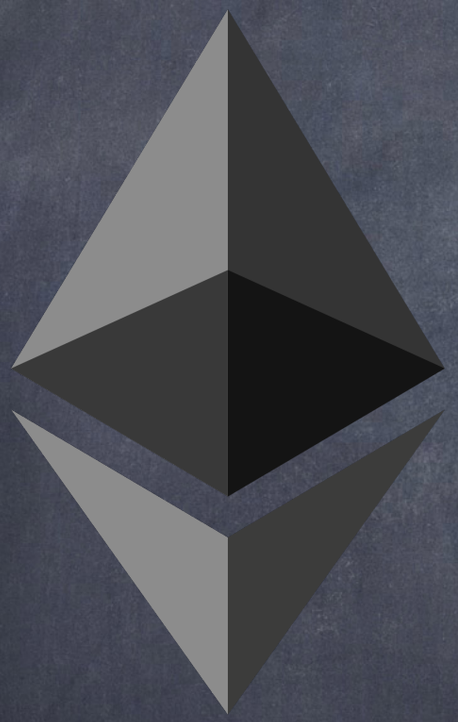
Swarm -> Storage

Whisper/Waku -> Network

Triad -> Ethereum &
Swarm & Whisper/Waku

#16

Decentralization



Three Types

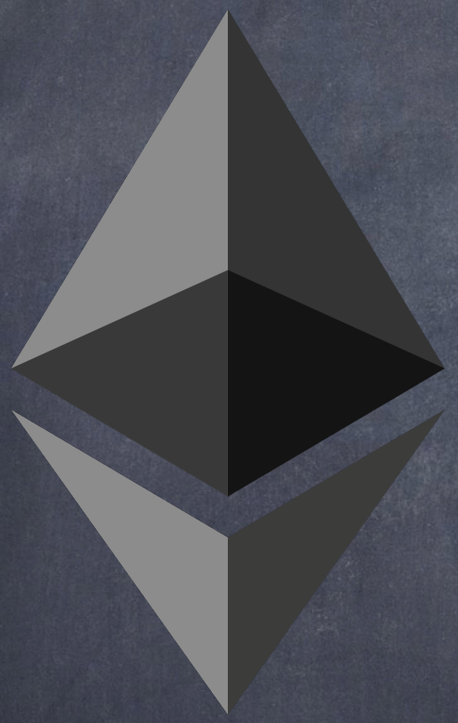
Architectural -> Physical Computers (Hardware)

Political -> Individuals/ Organizations (Wetware)

Logical -> Data Structures (Software)

#17

Native Currency



Ether -> 18 Decimals

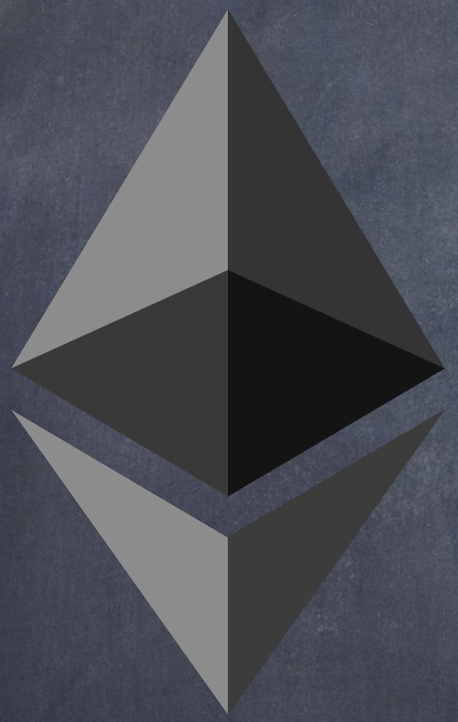
Smallest Unit -> Wei
10**18 Wei -> 1 Ether

10**3 Wei -> 1 Babbage

10**6 Wei -> 1 Lovelace

#18

Cryptography



Public Key Cryptography

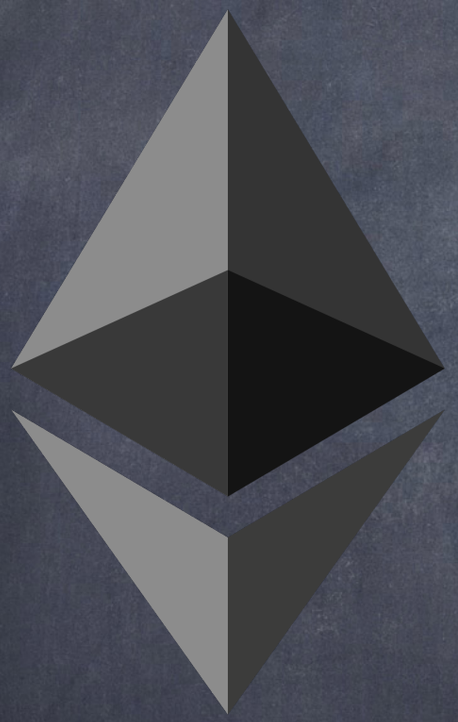
Public-Private Key Pairs

Private Key -> Public Key

Digital Signatures
Not Encryption

#19

ECDSA



Elliptic Curve Digital Signature Algorithm

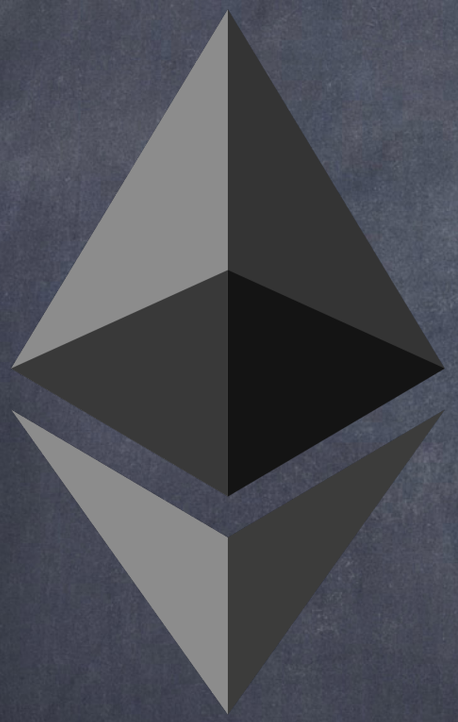
Elliptic-curve Cryptography (ECC)

SECP-256K1 Curve

Elliptic Curves
Finite Fields

#20

Private Key



Secret -> 256-bit

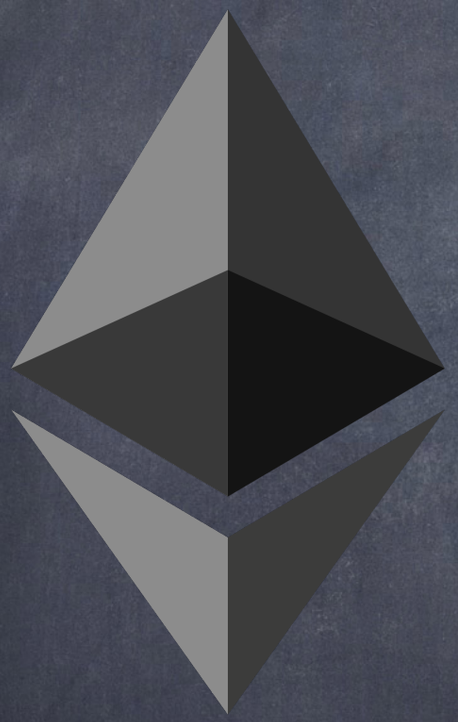
Random Number

Private Key -> Public Key

Public Key -> Address/ Account

#21

Public Key



Not Secret -> Public

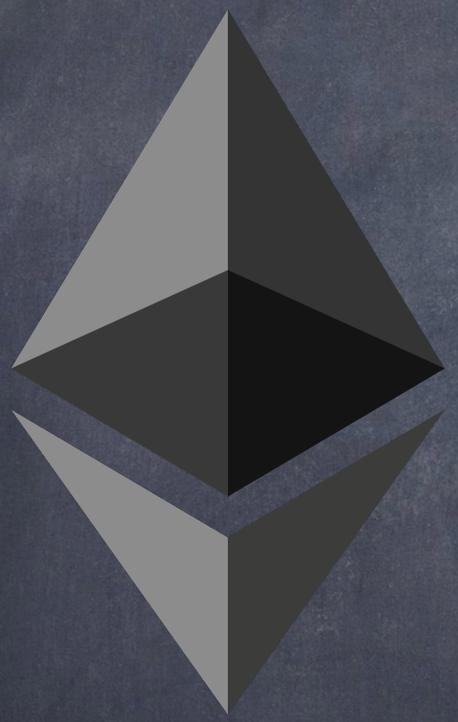
Private Key -> Public Key

Elliptic Curve Point -> Multiplication

Public Key X-> Private Key

#22

Ethereum State



State -> Accounts

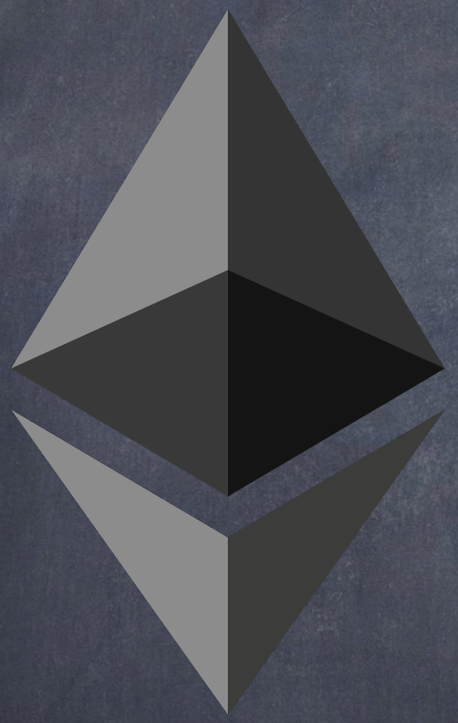
Account -> 20 Byte Address

Account <-> Account

Transfer of Value & Information

#23

Ethereum Account



Four Fields

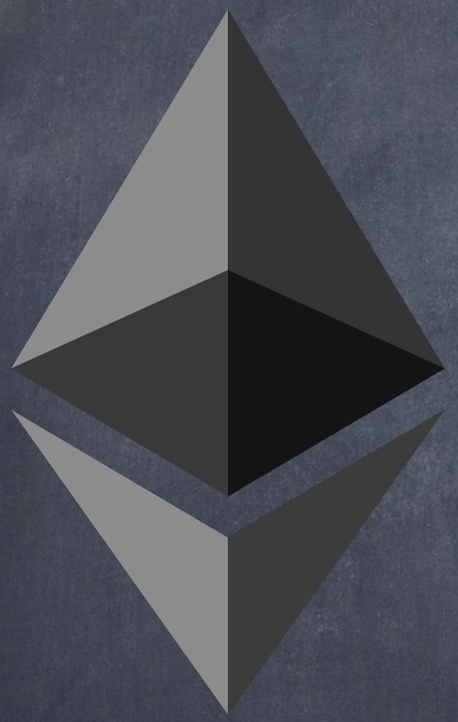
Nonce -> Counter

Balance -> Ether

Contract Code
Contract Storage

#24

Account Types



Two Types: EOA & Contract

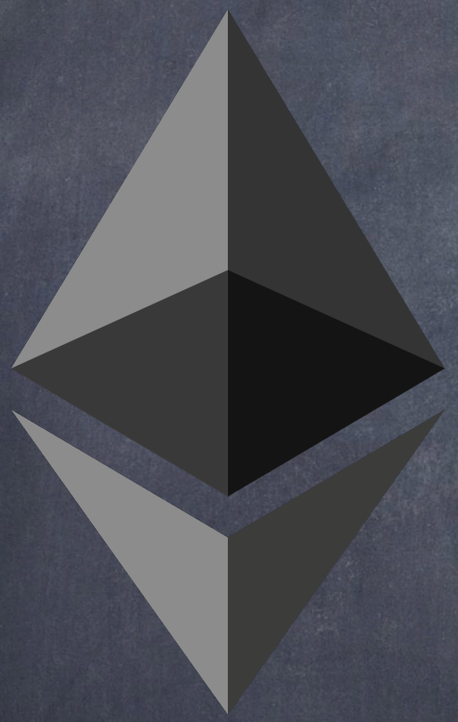
EOA -> Externally Owned Account

EOA -> Private Key

Contract Accounts -> Code

#25

EOA Ownership



EOA -> Externally Owned Account

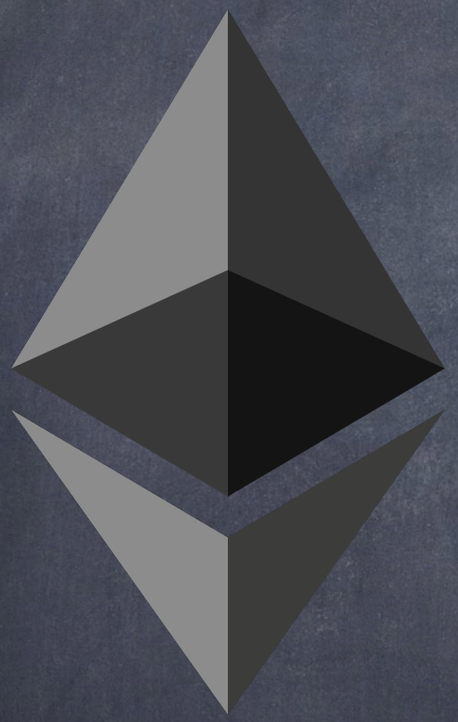
EOA -> Private Key

Private Key -> Digital Signature

Digital Signature -> Account Balance

#26

EOA



Account -> Nonce, Value,
Code, Storage

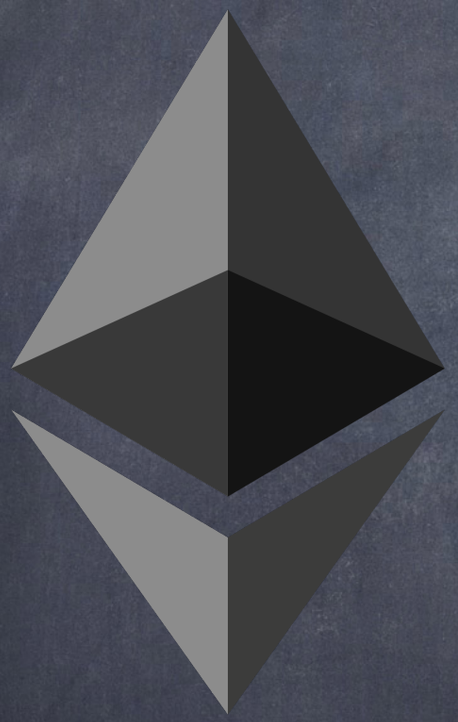
EOA X-> Code
EOA X-> Storage

Digital Signature -> Message
Other Accounts

Transfer Value
Trigger Contract

#27

Contract Account



Account -> Nonce, Value, Code, Storage

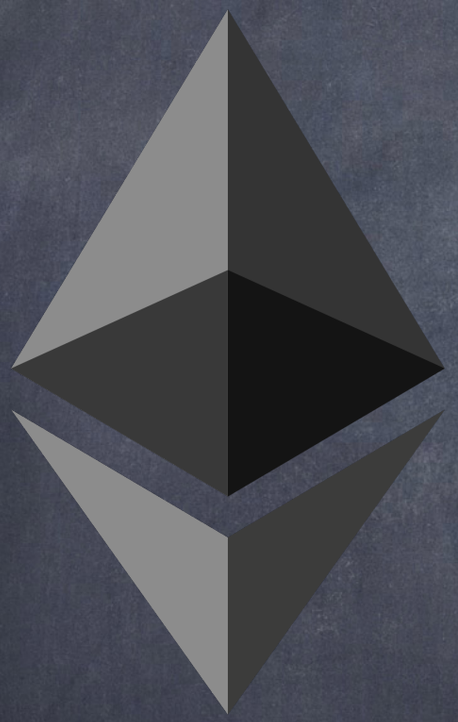
Contract -> Code
Contract -> Storage

Receive Tx/Message -> Run Code & Access Storage

Message Accounts
Create Contracts

#28

Smart Contracts



Autonomous Agents

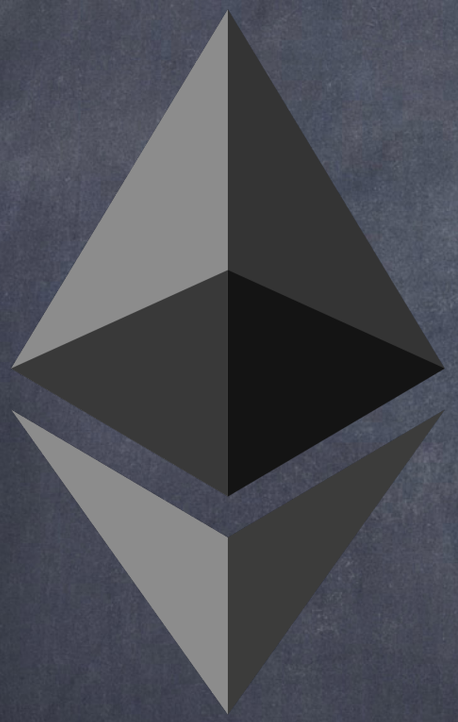
Ethereum Blockchain Execution Environment

Receive Tx/Message -> Execute Code

Ether Balance
Contract Storage

#29

Keccak-256



Cryptographic Hash Function

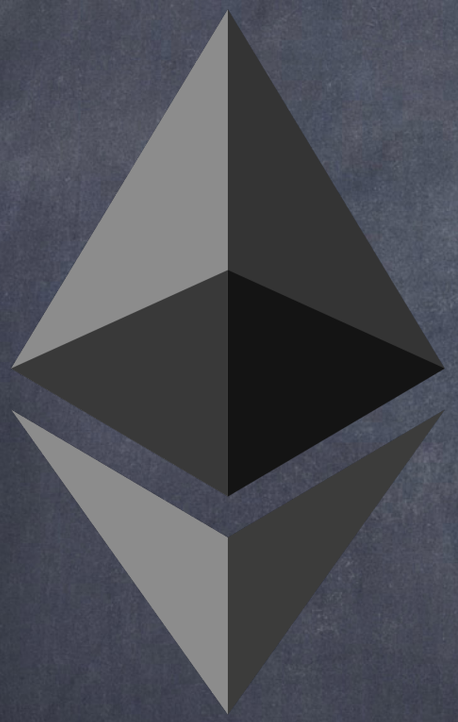
SHA-3 -> Secure Hash Function (NIST, 2015)

Keccak-256 Vs SHA-3

Fundamental Primitive

#30

EOA Address



Private Key -> Public Key

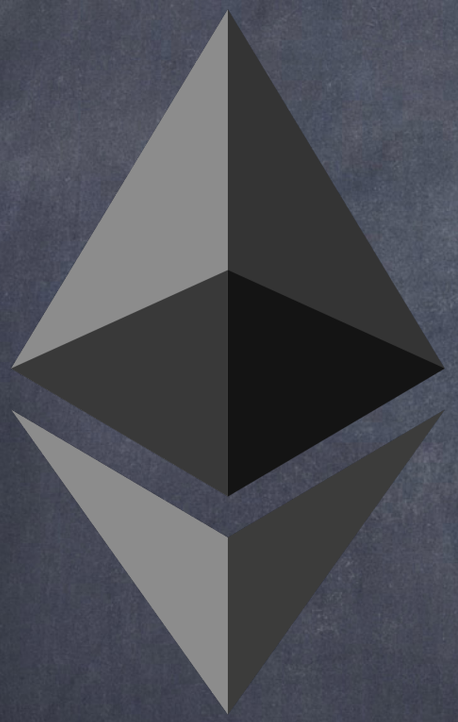
Public Key -> Keccak-256

Last 20 Bytes -> Least Significant Bytes

Address -> 160 Bits or 20 Bytes

#31

Transaction



Signed Message

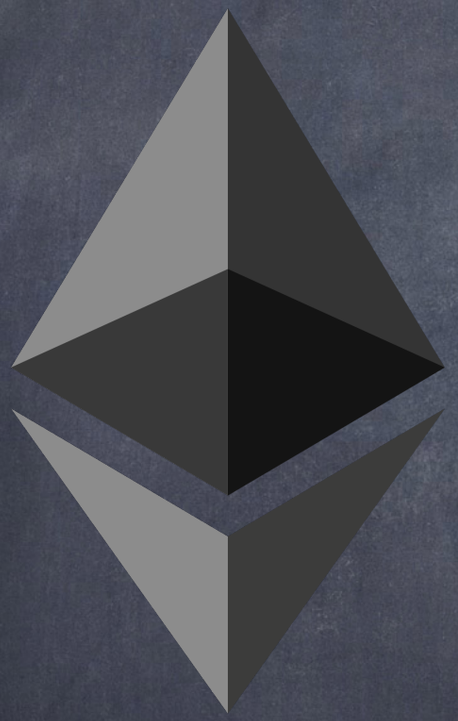
Origin -> EOA

Trigger -> State Change

Transmitted -> Network
Recorded -> Blockchain

#32

Transaction Properties



Atomic -> All or Nothing
Cannot be Divided/Interrupted

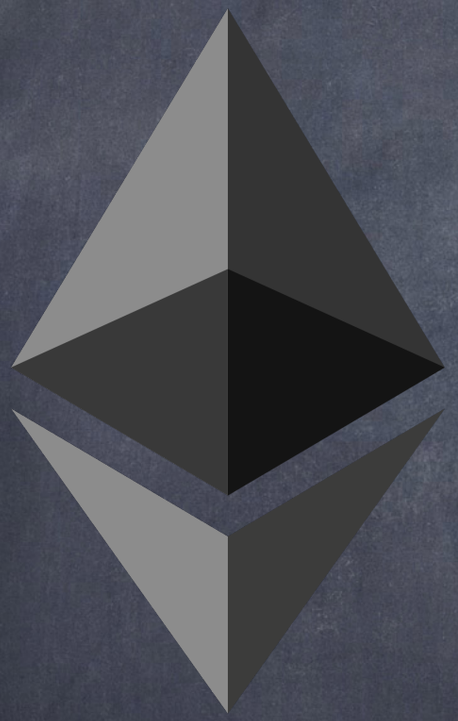
Serial -> One after Another
Sequentially -> No Overlapping

Inclusion -> Miners
Congestion, gasPrice

Order -> Miners
Congestion, gasPrice

#33

Transaction Components



Serialized Binary Message
nonce -> Sequence Number

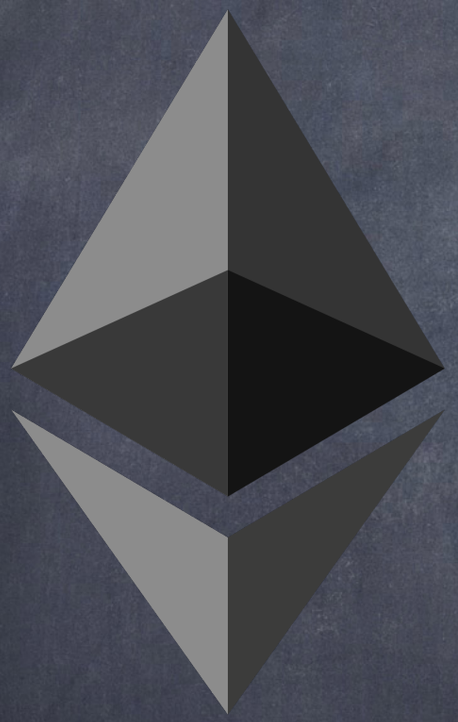
gasPrice -> Wei / Gas Unit
gasLimit -> Max Gas

recipient -> Destination Addr
value -> Wei

data -> Payload
v, r, s -> ECDSA Signature

#34

Nonce



Nonce -> Number used only Once

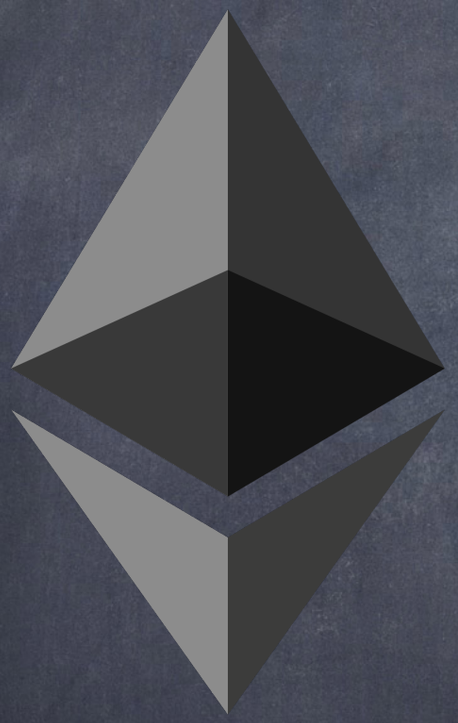
Sequence Number -> Prevent Replay

EOA -> #Txs Sent

Contract -> #Contracts Created

#35

gasPrice



Gas Price -> Originator Willing to Pay

Wei / Gas Unit

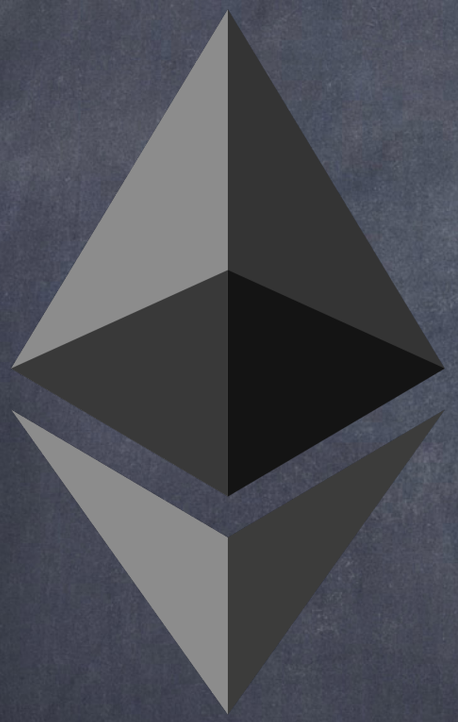
Higher -> Faster Block Inclusion by Miner

Price -> Demand

Block -> Limit

#36

gasLimit



Max Gas Units ->
Originator Willing to Pay

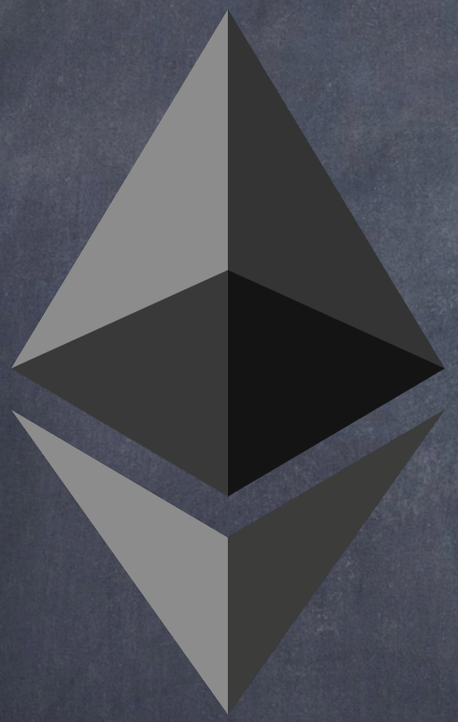
Ether Transfer -> 21000
Gas

Contract Tx -> More Gas
Less Gas -> OOG Error

Estimated Gas -> Tx
Excess Gas -> Sent Back

#37

Recipient



20-Byte Address
Tx Recipient

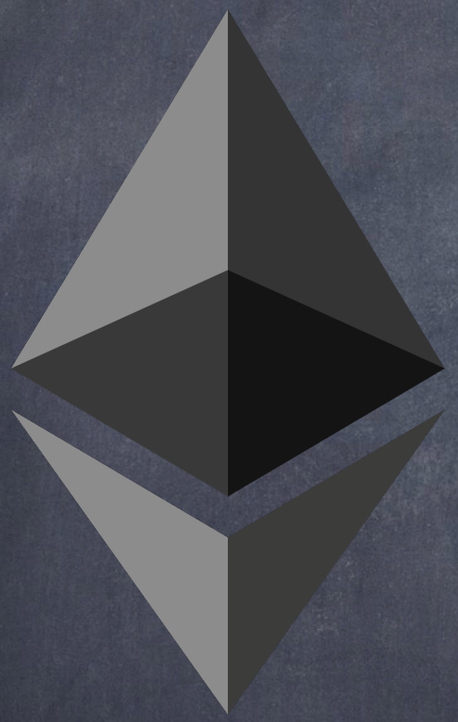
EOA Address
Contract Address

Any Address
No Protocol Validation

No From Address
v, r, s -> Pub Key -> Addr

#38

Value



Value of ether
Sender -> Recipient

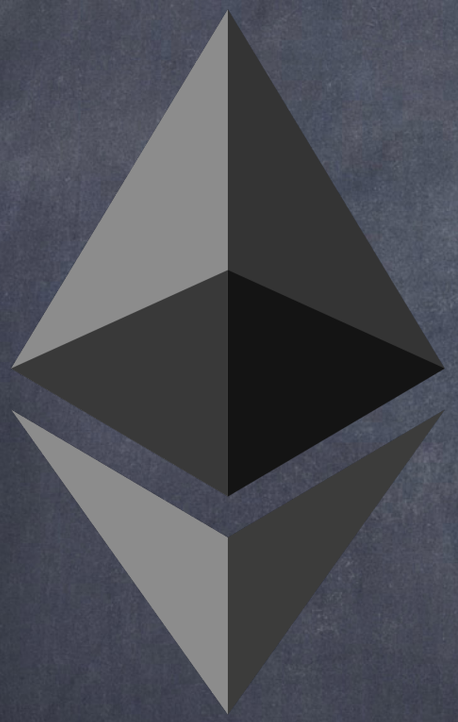
EOA -> Balance Increase
Sender -> Balance Decrease

Contract -> Data?
Data -> Contract Function

No Data -> receive/
fallback/exception

#39

Data



Data
Sender -> Recipient

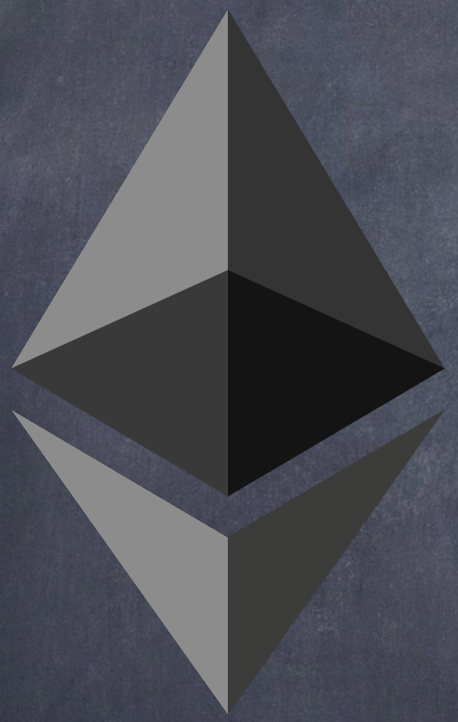
Recipient -> Contract Account

Data -> Contract Function

Data -> Function Args

#40

v, r, s



ECDSA Signature
65 Bytes

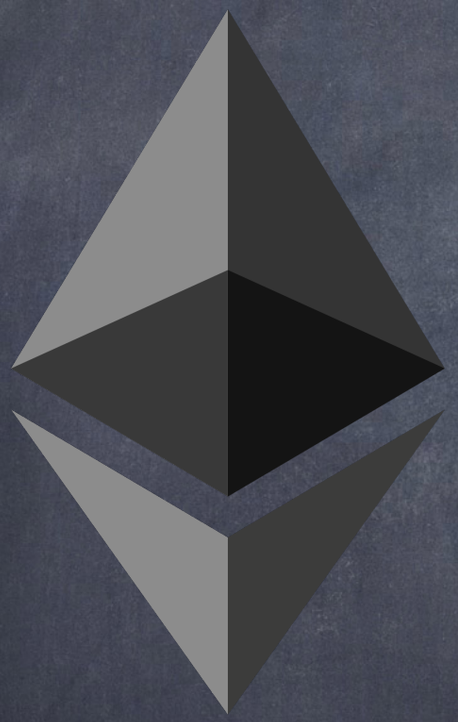
r, s -> Signature
32 Bytes Each

v -> Recovery Identifier
1 Byte

v -> 27/28 or
chainID*2 + 35/36

#41

Signature
Purpose



ECDSA Signature
3 Purposes

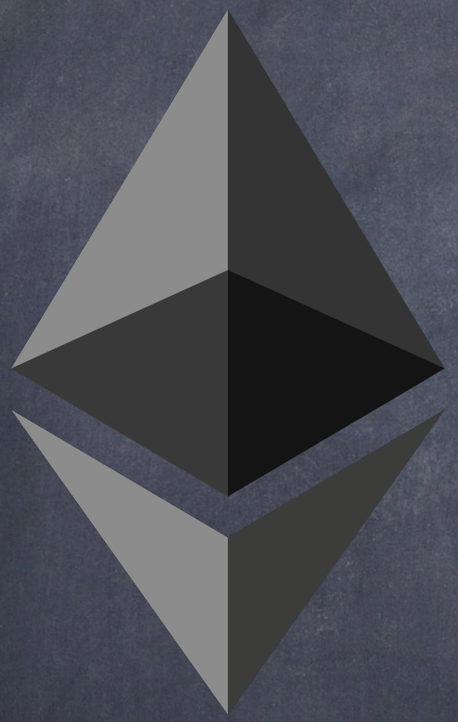
Authorization
Auth -> ether/Contract

Non-repudiation
Auth -> Undeniable

Integrity
Tx Data X-> Modified

#42

Contract Creation



Creation Transaction

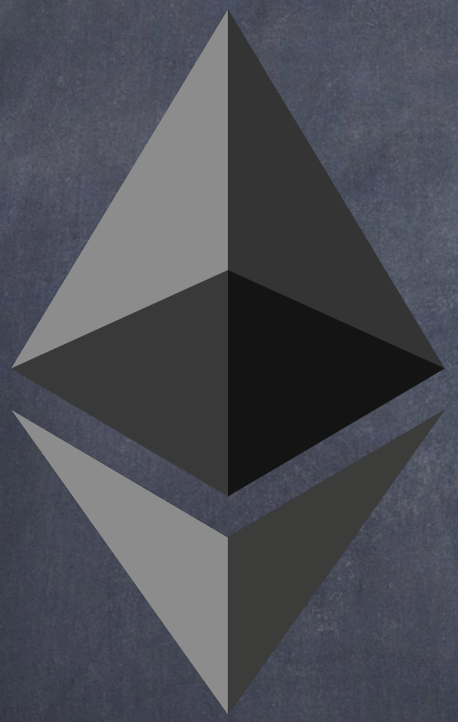
Recipient -> 0x0 Address

Data -> Contract Bytecode

Value -> Contract Balance

#43

Txs Vs Messages



Tx: Offchain -> Onchain
Msg: Onchain -> Onchain

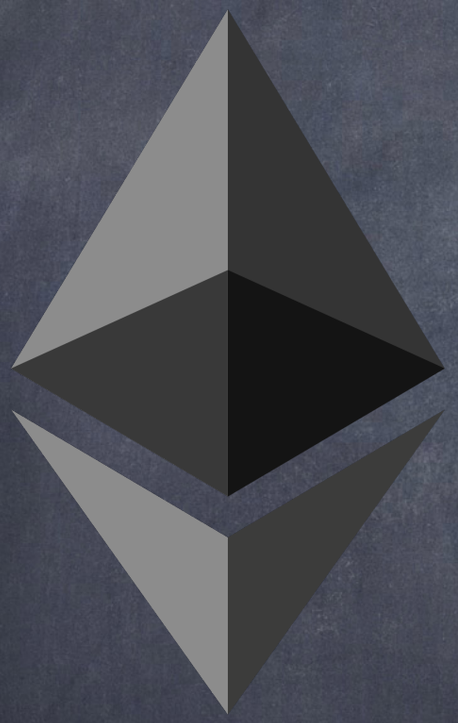
Tx -> Triggers Msg
ETH Transfer or Contract Code

Msg -> Triggered by EOA Tx
EOA -> EOA or Contract

Msg -> Triggered by EVM CALL
Contract -> Contract

#44

Txs & Blockchain



Transactions Grouped Together

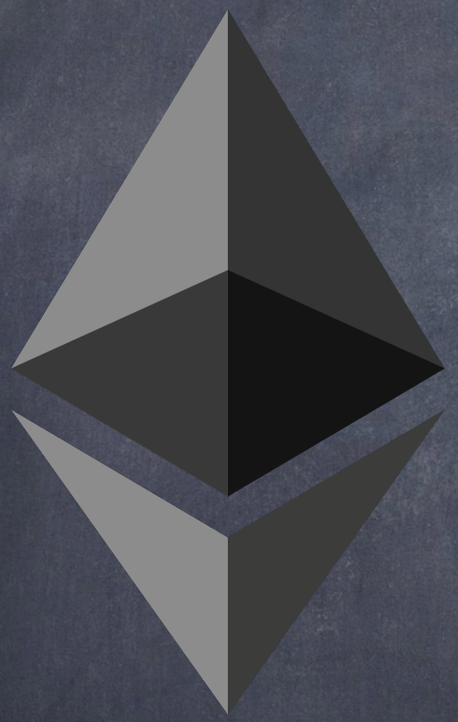
Transactions -> Block

Blocks Linked Together

Blocks -> Blockchain

#45

Block



Block -> Grouped Transactions

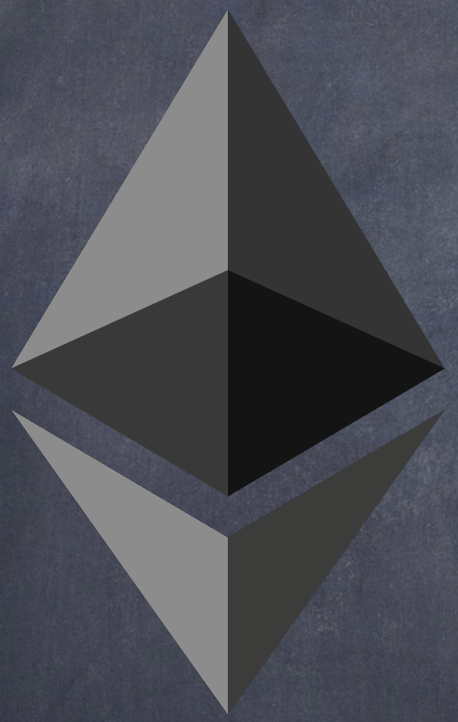
Hash -> Previous Block

Block Change -> Affects All Following Blocks

Integrity X-> Fraud

#46

Ethereum Node/Client



Node -> Protocol Impl
Ethereum Specification

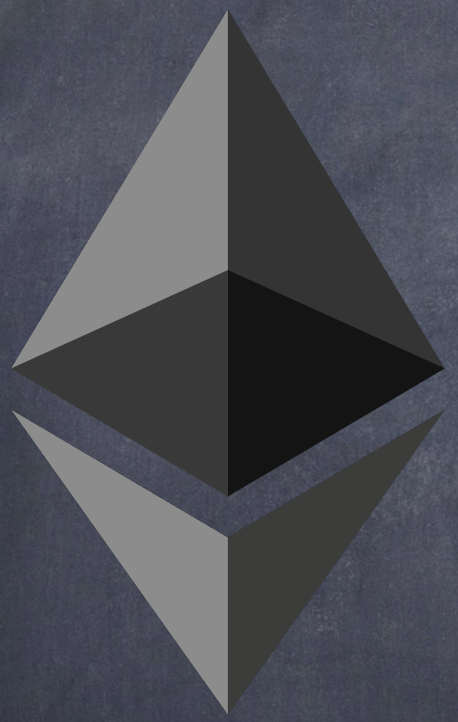
P2P: Node <-> Node

Client -> Specific Implementation

Geth, OpenEthereum, Erigon, Nethermind

#47

Ethereum Miners



Entities Running Ethereum Nodes

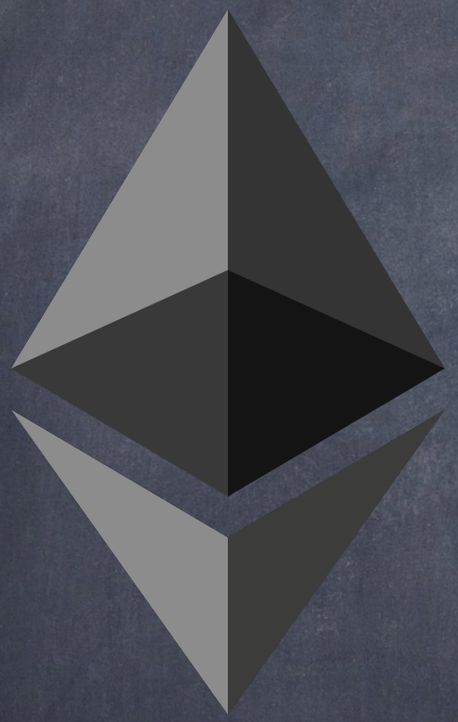
Transactions -> Validate/ Execute/Combine -> Blocks

Block Validation -> Proof of Work (PoW)

Block Reward -> 2 ETH
Tx Fees -> All Block Txs

#48

Block Gas Limit



Total Gas Spent
All Txs in Block

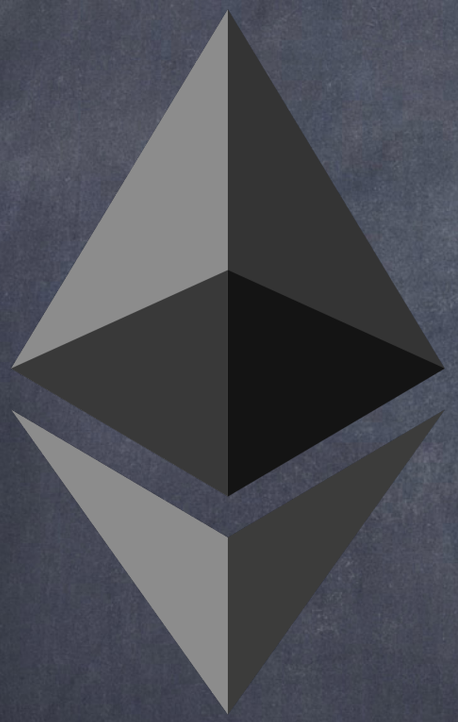
Txs -> Block
Caps -> #Txs in Block

Block Size X-> Fixed #Txs
Gas/Tx -> Gas Limit

Set -> Miners
Current -> 15 Million

#49

GHOST



Miners -> Blocks
Network -> Propagation

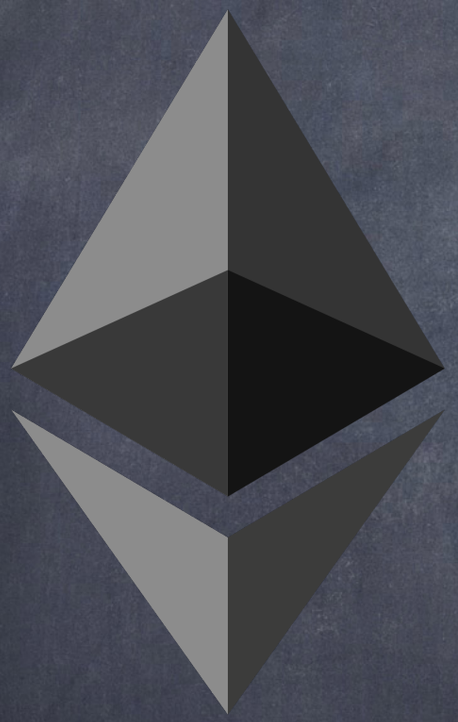
Multiple Valid Blocks
Choose One Block

Greedy Heaviest Observed
Subtree Protocol (GHOST)

Canonical Blockchain
Stale Blocks -> Ommers

#50

Consensus



Nakamoto Consensus

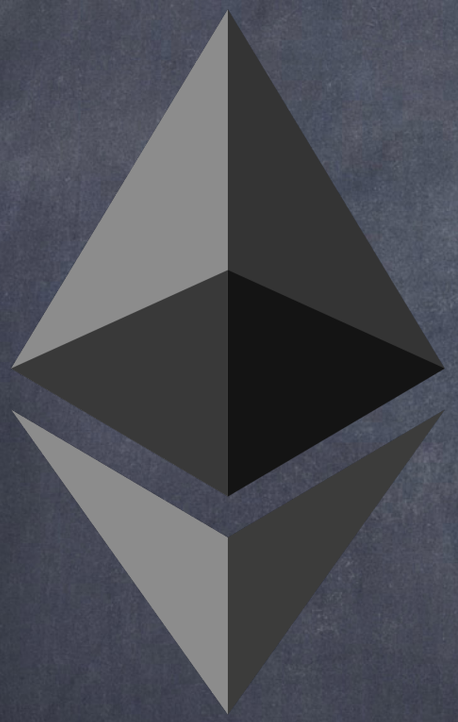
Next Block -> Which Miner?

Proof-of-Work (PoW)

Longest Chain Rule

#51

Ethereum State



Address -> Account State

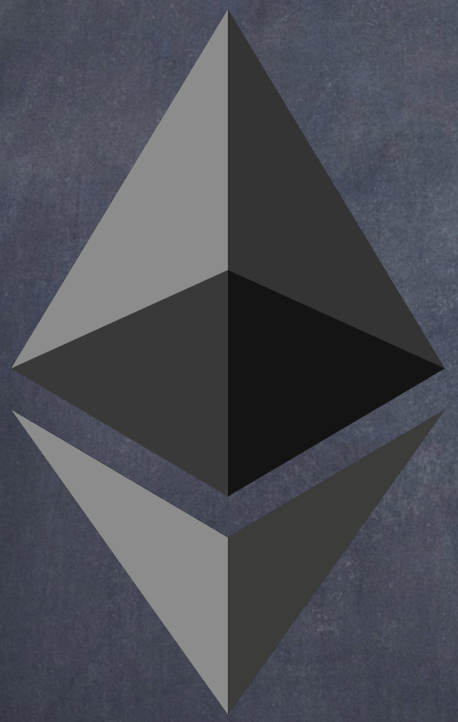
Modified Merkle-Patricia Tree
Binary Tree

Leaf Nodes -> Data
Intermediate Nodes -> Hash
(Two Child Nodes)

Single Root Node -> Root Hash

#52

Ethereum PoW



Ethash

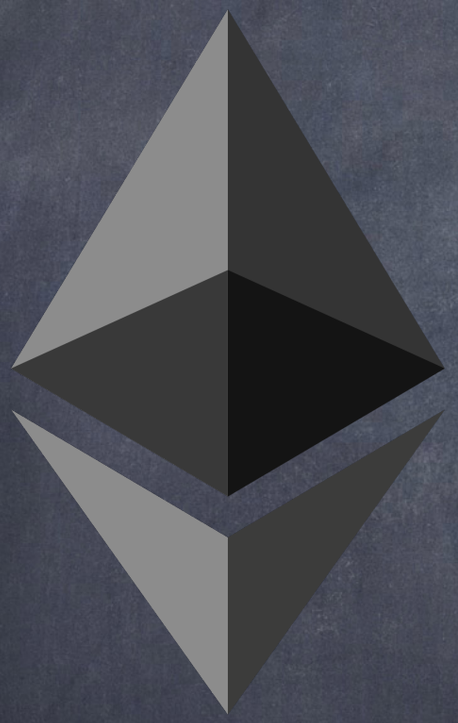
$(m, n) = PoW(H_n, H_n, d)$

$m = H_m \wedge n <= 2**256/H_d$

n: Nonce, H_d - Difficulty
m: Mix Hash, d: Data Set

#53

Block Header



Block -> Header, Txs,
Ommers' Headers

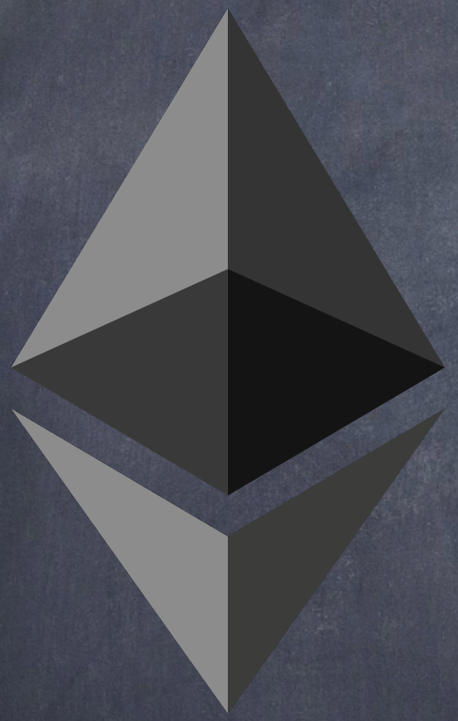
Block Header ->
parentHash, ommersHash,
beneficiary

stateRoot, transactionsRoot,
receiptsRoot, logsBloom,
difficulty, number

gasLimit, gasUsed, extraData,
timestamp, mixHash, nonce

#54

State Root



256-bit Hash
Modified Merkle-Patricia Tree

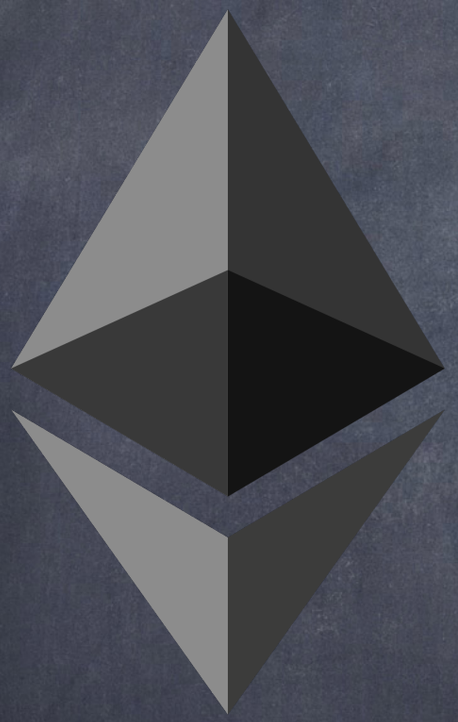
Leaves -> Key-Value Pairs
Address -> Account

Account: Nonce, Balance,
codeHash, storageRoot

codeHash: Hash(Code)
storageRoot: Account Storage

#55

Tx Receipt



Tuple -> Four Items

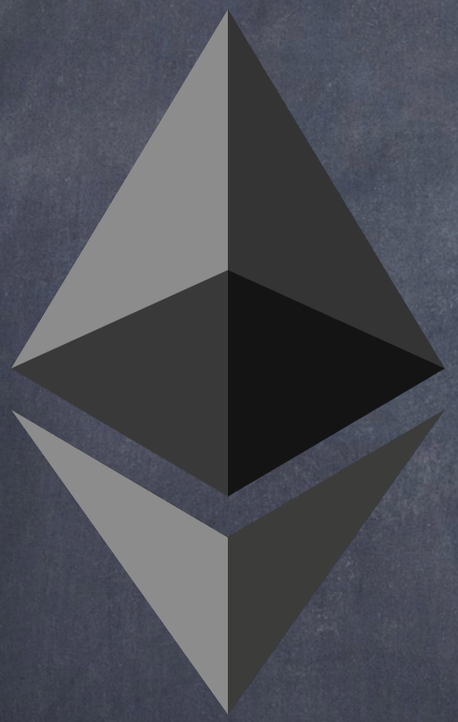
Cumulative Gas Used

Tx -> Set of Logs
Logs -> Bloom Filter

Tx Status Code

#56

Tx Gas



Beneficiary & Refund

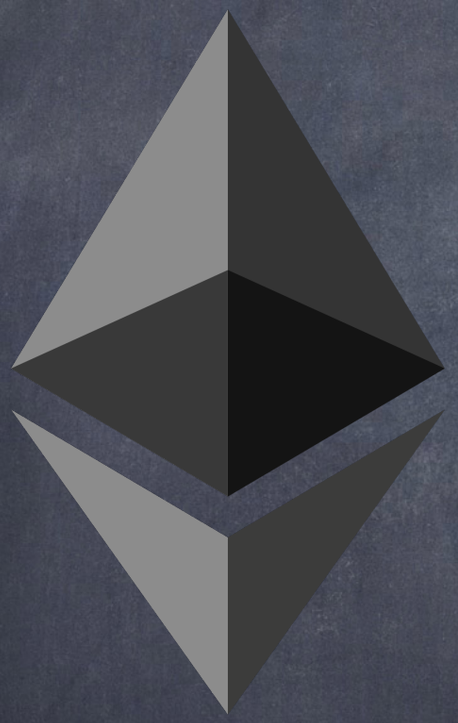
Beneficiary -> Miner
Tx Fees

Gas Refund
Tx gasLimit - Gas Used

Refund -> Sender
Same gasPrice

#57

EVM



Ethereum Virtual Machine

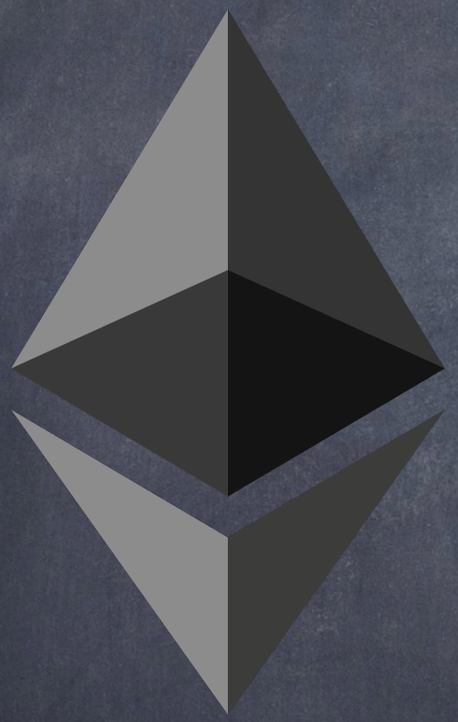
Smart Contracts ->
Runtime Environment

Quasi Turing Complete

Turing Complete -> Gas
Bounded Computation

#58

Ethereum Code



Ethereum Virtual Machine (EVM)

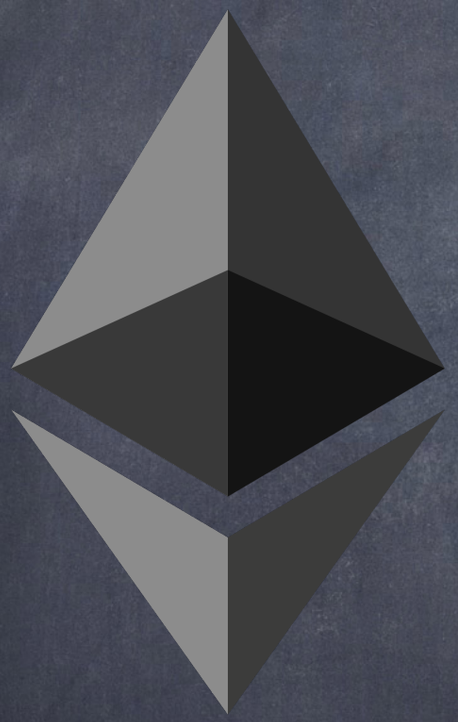
Low-level & Stack-based EVM Machine code

Series of Bytes -> Bytecode

One Byte -> One Operation

#59

EVM
Architecture



Stack-based Architecture

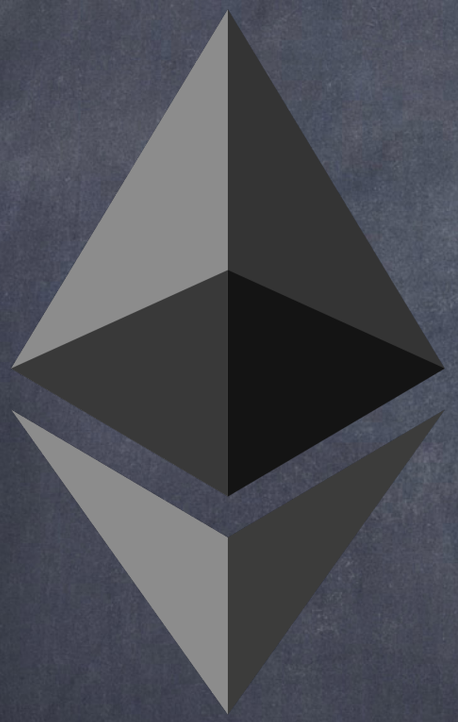
Stack
Volatile Memory

Non-volatile Storage
Calldata

Word Size -> 256-bits
Keccak-256 & ECC

#60

Stack



1024 Elements
256-bits

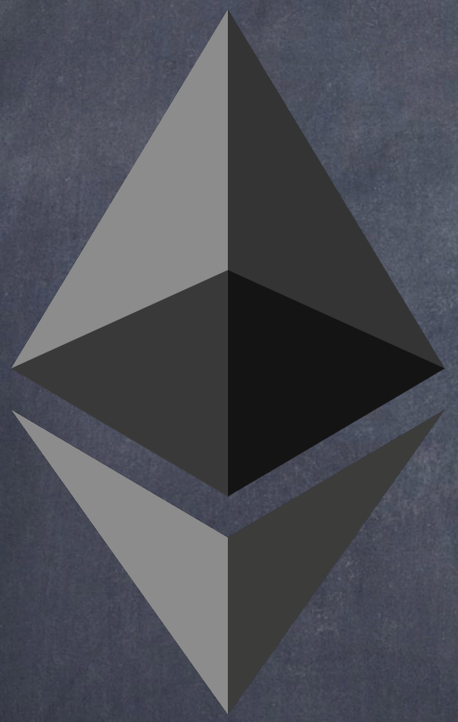
Most EVM Operations ->
Stack Elements

Stack-based Architecture
Top 16 Elements

Stack-specific Operations
PUSH/POP/SWAP/DUP

#61

Memory



Volatile Memory

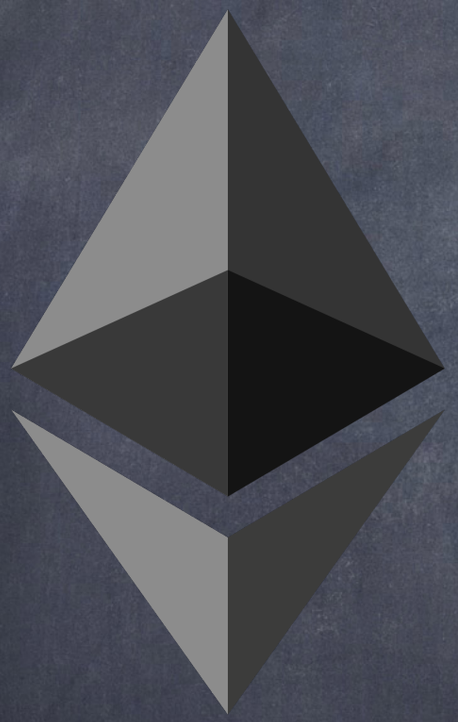
Linear Byte-array
Byte-level Addressable

Zero-initialized

MLOAD/MSTORE/MSTORE8

#62

Storage



Non-volatile Storage

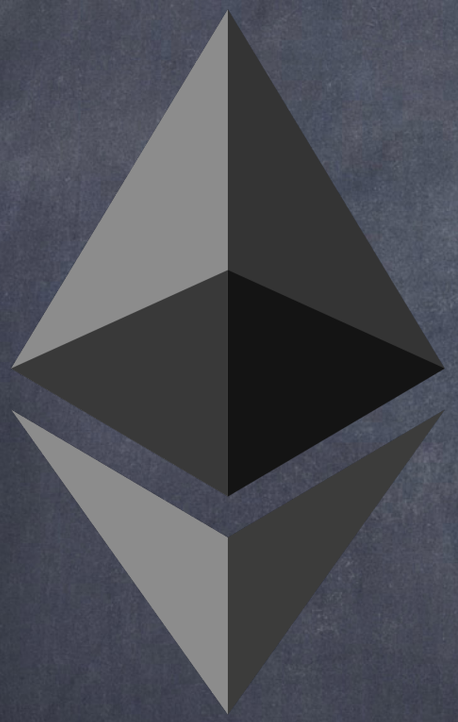
Key-Value Store
256-bit <-> 256-bit

Zero-initialized
storageRoot -> stateRoot

SLOAD/SSTORE

#63

Calldata



Data Parameters
Txs & Message Calls

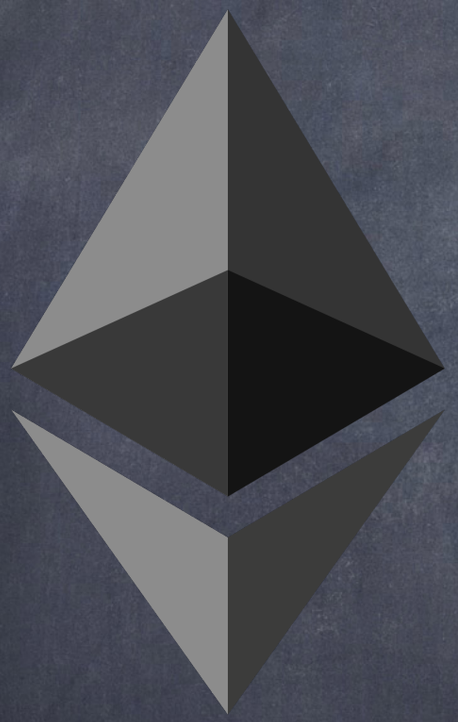
Read-only
Byte-addressable

Three Instructions
CALLDATASIZE

CALLDATALOAD/
CALLDATACOPY

#64

EVM Architecture



von Neumann Vs Harvard

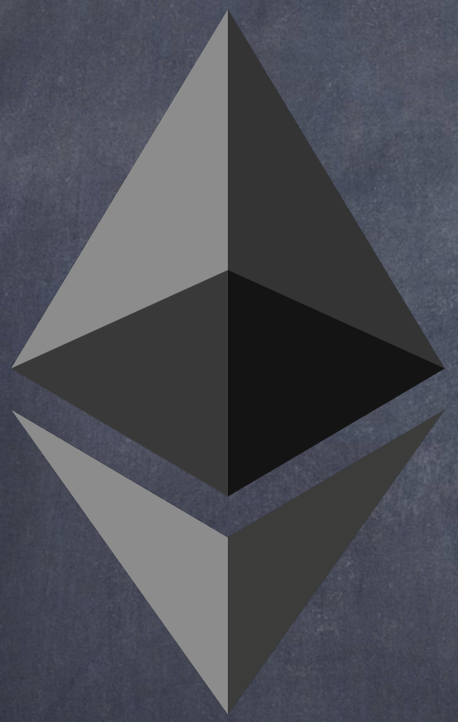
Code & Data

Memory & Pathways
Together or Separately

EVM Code -> Virtual ROM
Special Instructions

#65

EVM Ordering



Big-endian Vs Little-endian

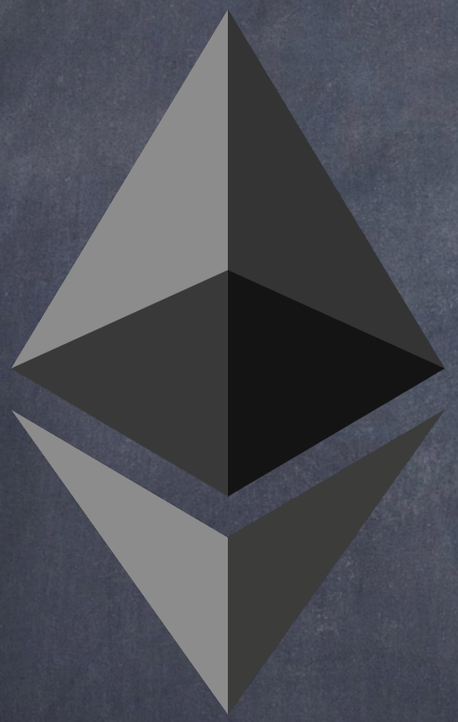
Big-endian

MSB -> Lowest Address

LSB -> Highest Address

#66

Instruction Set



Eleven Categories

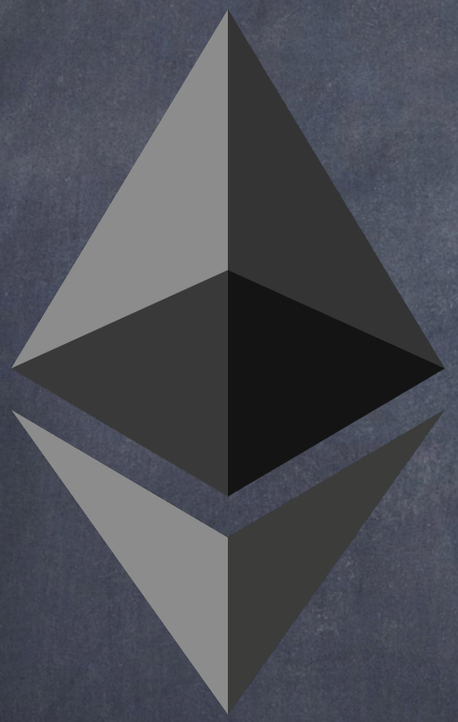
1. Stop and Arithmetic
2. Comparison & Bitwise Logic
3. SHA3

4. Environmental Information
5. Block Information 6. Stack, Memory, Storage and Flow

7. Push 8. Duplication 9. Exchange 10. Logging 11. System

#67

Stop & Arithmetic



0x00 STOP 0 0
0x01 ADD 2 1
0x02 MUL 2 1

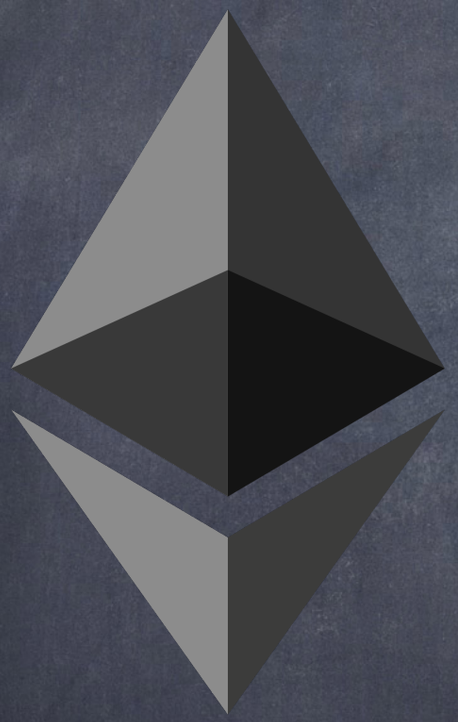
0x03 SUB 2 1
0x04 DIV 2 1
0x05 SDIV 2 1

0x06 MOD 2 1
0x07 SMOD 2 1
0x08 ADDMOD 3 1

0x09 MULMOD 3 1
0x0a EXP 2 1
0x0b SIGNEXTEND 2 1

#68

Comparison & Bitwise Logic



0x10 LT 2 1 | 0x20 GT 2 1
0x12 SLT 2 1 | 0x13 SGT 2 1

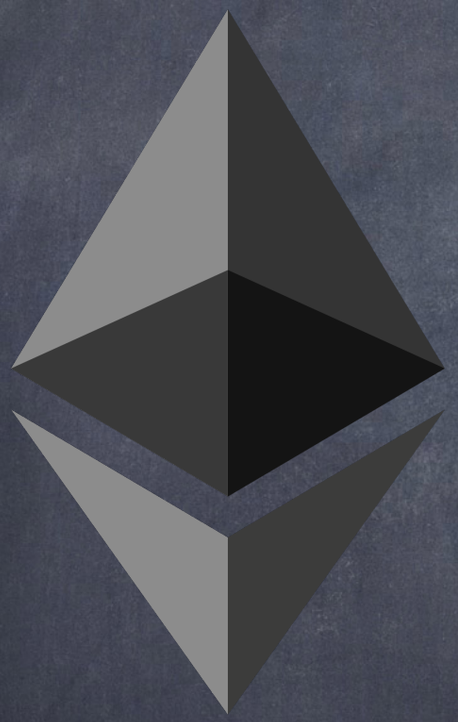
0x14 EQ 2 1 | 0x15 ISZERO 1 1
0x16 AND 2 1 | 0x17 OR 2 1

0x18 XOR 2 1 | 0x19 NOT 1 1
0x1a BYTE 2 1 | 0x1b SHL 2 1

0x1c SHR 2 1 | 0x1d SAR 2 1

#69

SHA3



0x20 SHA3 2 1

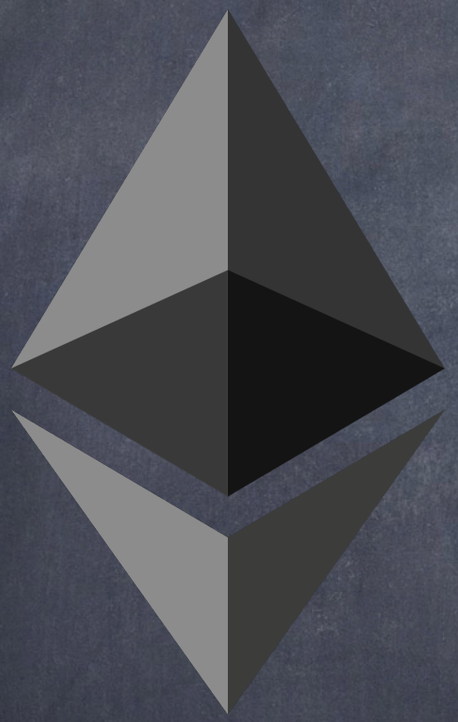
Compute Keccak-256 Hash

$\mu's[0] \equiv KEC(\mu m[\mu s[0]... (\mu s[0] + \mu s[1]-1)])$

$\mu'i \equiv M(\mu i, \mu s[0], \mu s[1])$

#70

Environmental Information



0x30 ADDRESS 0 1
0x31 BALANCE 1 1
0x32 ORIGIN 0 1
0x33 CALLER 0 1

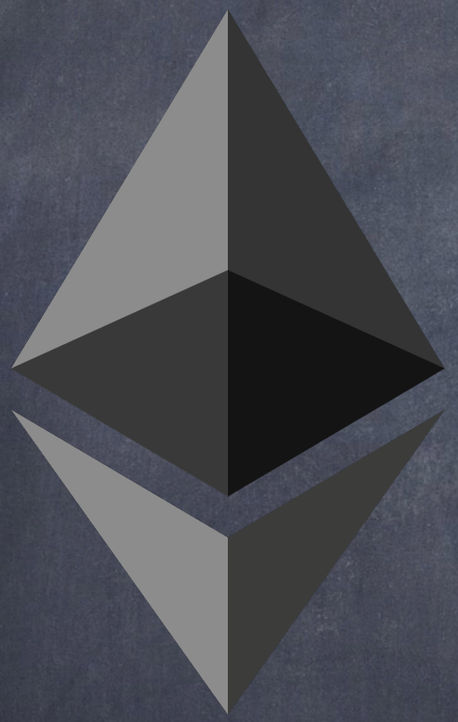
0x34 CALLVALUE 0 1
0x35 CALLDATALOAD 1 1
0x36 CALLDATASIZE 0 1
0x37 CALLDATACOPY 3 0

0x38 CODESIZE 0 1
0x39 CODECOPY 3 0
0x3a GASPRICE 0 1
0x3b EXTCODESIZE 1 1

0x3c EXTCODECOPY 4 0
0x3d RETURNDATASIZE 0 1
0x3e RETURNDATACOPY 3 0
0x3f EXTCODEHASH 1 1

#71

Block Information



Information -> Transaction's Block

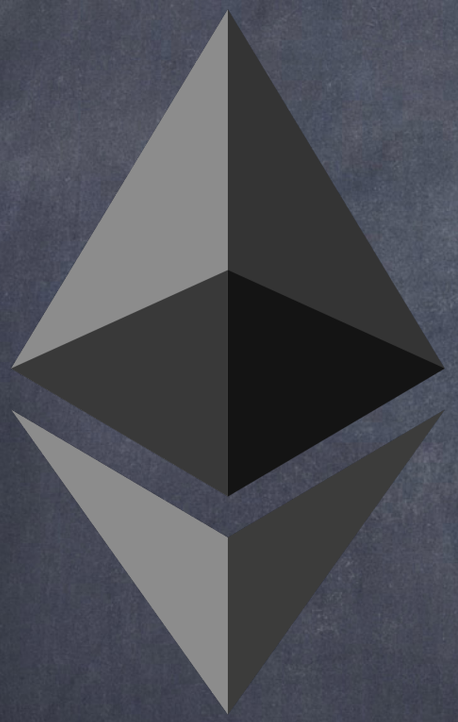
0x40 BLOCKHASH 1 1
0x41 COINBASE 0 1

0x42 TIMESTAMP 0 1
0x43 NUMBER 0 1

0x44 DIFFICULTY 0 1
0x45 GASLIMIT 0 1

#72

Stack, Memory, Storage and Flow



0x50 POP 1 0
0x51 MLOAD 1 1
0x52 MSTORE 2 0

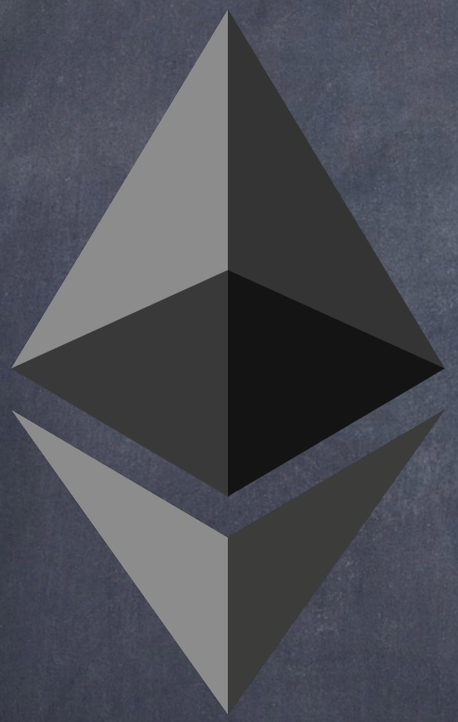
0x53 MSTORE8 2 0
0x54 SLOAD 1 1
0x55 SSTORE 2 0

0x56 JUMP 1 0
0x57 JUMPI 2 0
0x58 PC 0 1

0x59 MSIZE 0 1
0x5a GAS 0 1
0x5b JUMPDEST 0 0

#73

Push Operations



Place Items -> Stack

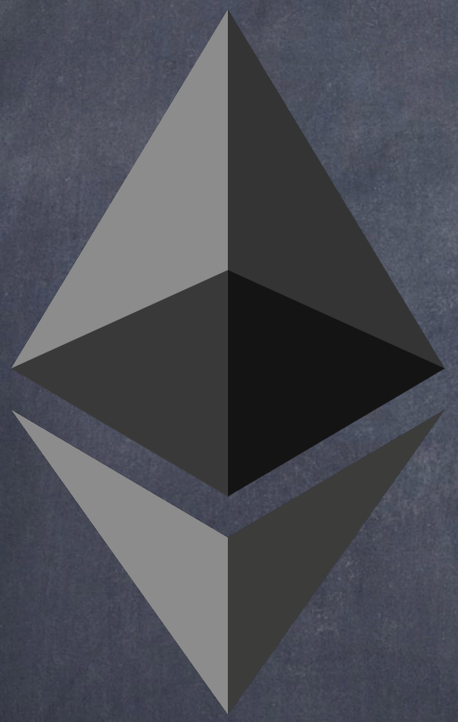
0x60 PUSH1 0 1
0x61 PUSH2 0 1

PUSH3, PUSH4, PUSH5...
PUSH31

0x7f PUSH32 0 1

#74

Duplication Operations



Duplicate Items -> Stack

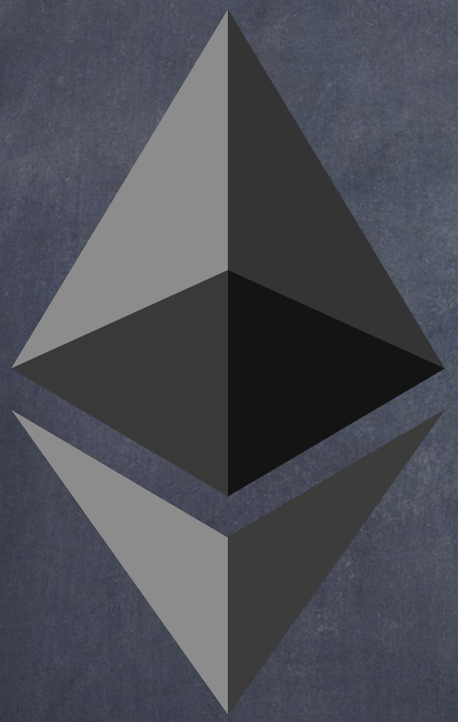
0x80 DUP1 1 2

DUP2, DUP3...DUP15

0x8f DUP16 16 17

#75

Exchange Operations



Exchange Items -> Stack

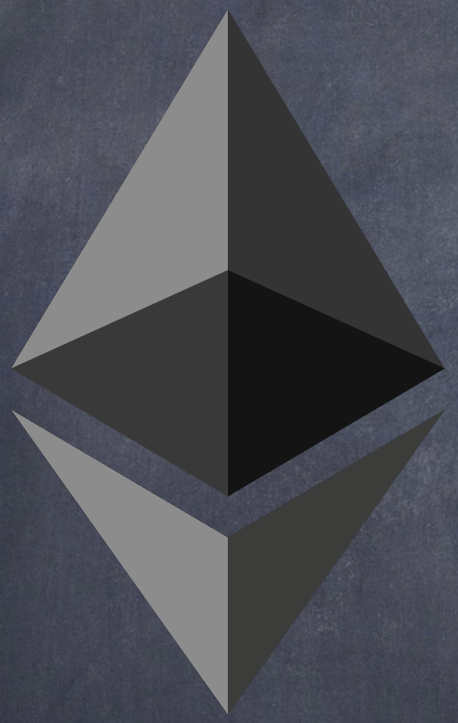
0x90 SWAP1 2 2

SWAP2, SWAP4...SWAP15

0x9f SWAP16 17 17

#76

Logging Operations



Append Log Record -> Topics

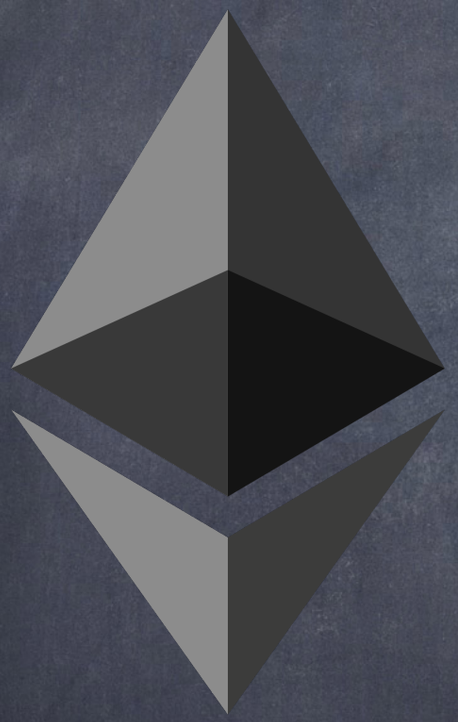
0xa0 LOG0 2 0

0xa1 LOG1 3 0
0xa2 LOG2 4 0

0xa3 LOG3 5 0
0xa4 LOG4 6 0

#77

System Operations



0xf0 CREATE 3 1
0xf1 CALL 7 1
0xf2 CALLCODE 7 1

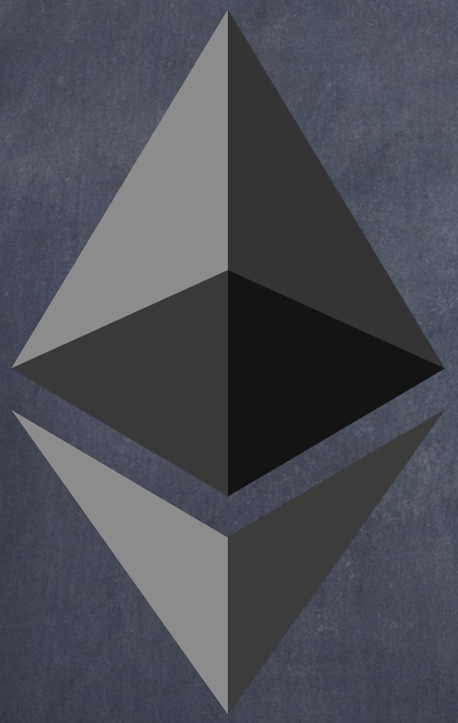
0xf3 RETURN 2 0
0xf4 DELEGATECALL 6 1
0xf5 CREATE2 4 1

0xfa STATICCALL 6 1
0xfd REVERT 2 0
0xfe INVALID ∅ ∅

0xff SELFDESTRUCT 1 0

#78

Gas Costs



Diff Instructions -> Diff Costs
Computational/Storage Load

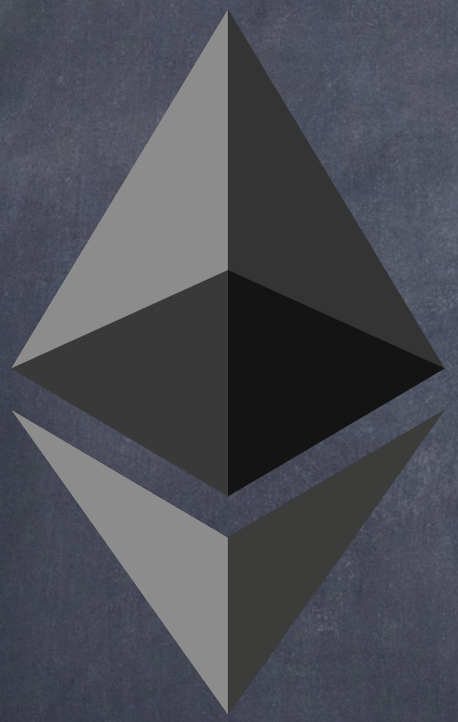
STOP/INVALID/REVERT: 0
Most Arithmetic/Logic/Stack: 3-5

CALL*/BALANCE/EXT*: 2600
MLOAD/MSTORE/MSTORE8: 3

SLOAD: 2100 SSTORE:20000/5000
CREATE: 32000 SELFDESTRUCT: 5000

#79

Transaction Reverts



Different Exceptional Conditions

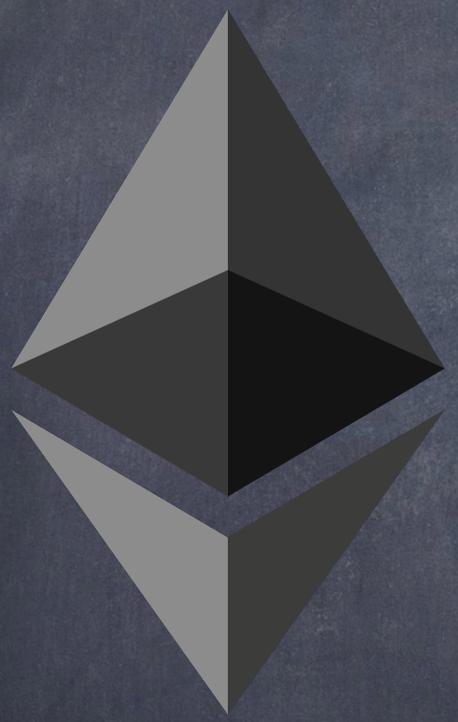
E.g.: Out of Gas, Invalid Instructions

State Changes -> Discarded

Original State -> Restored
As if Tx X-> Executed

#80

Transaction Data



Recipient -> Contract Address

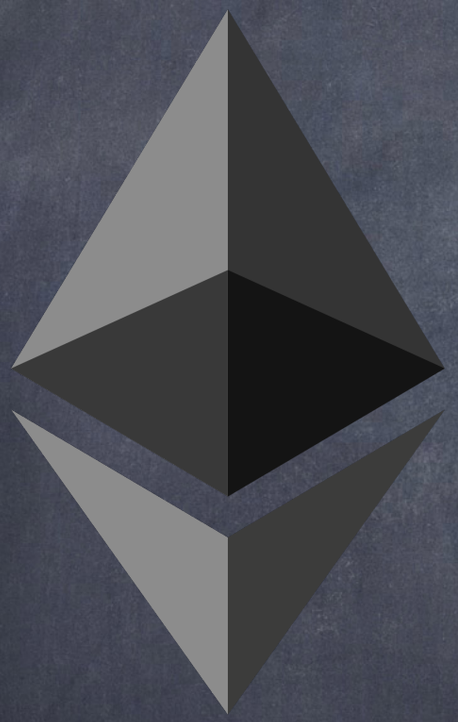
Tx Data -> Target Function & Arguments

Encoded -> ABI

ABI -> Application Binary Interface

#81

ABI



Application Binary Interface

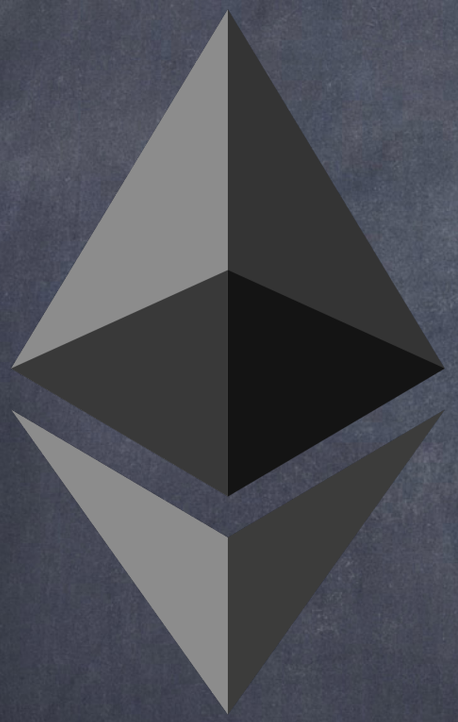
Required -> Interact with Contracts

Interface Fns -> Strongly Typed

Known -> Compile Time & Static

#82

Function Selector



Selector -> Contract Function

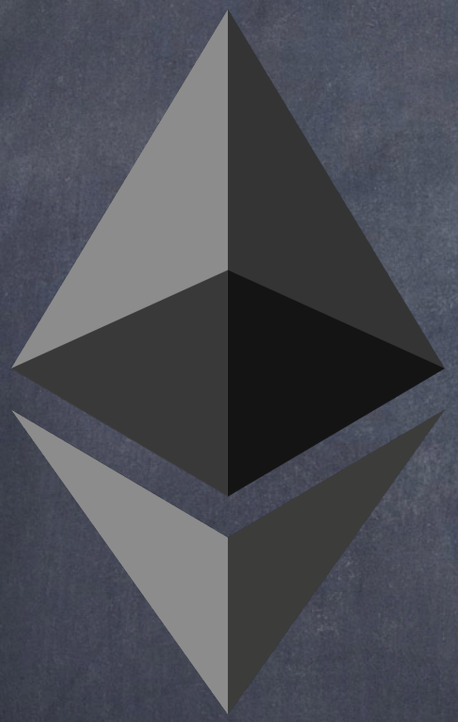
First 4 Bytes -> Keccak256(Fn Sig)

Fn Sig -> Name(Param1$_{type}$,Param2$_{type}$...)

Fn Args -> Encoded & 5th Byte Onwards

#83

Block Explorer



Application -> Web Portal

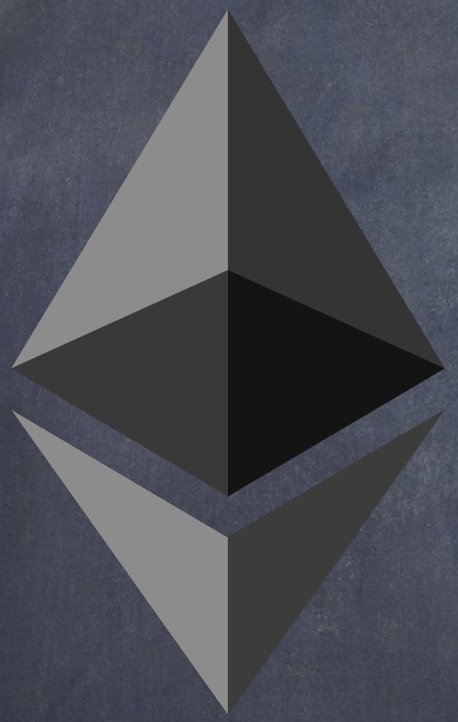
Real-time On-chain Data
Blocks & Transactions

Accounts, Interactions, Gas,
Balances, Calls

Etherscan, Etherchain,
Ethplorer, Blockchair,
Blockscout

#84

Mainnet



Main Ethereum Network

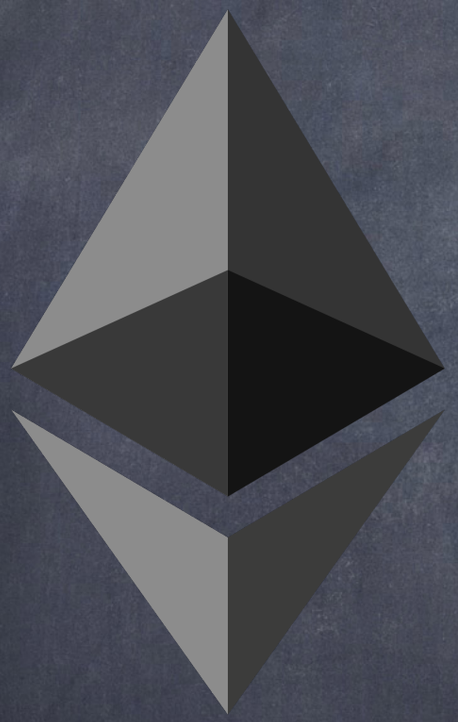
Mainnet Vs Testnets
ETH Vs Faucet Test ETH

Görli: PoA Testnet
Kovan: PoA OpenEthereum

Rinkeby: PoA Geth
Ropsten: PoW

#85

EIP



Ethereum Improvement Proposal (EIP)

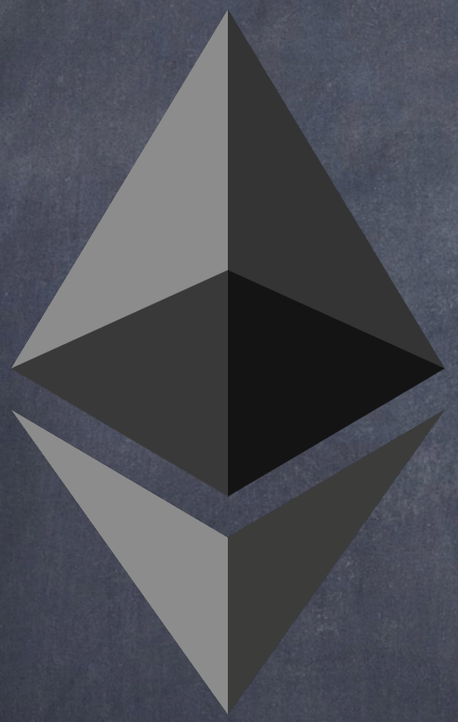
Standards & Specifications

Core, Networking, Interface, ERC (e.g. ERC-20)

Meta & Informational

#86

Eth 2.0



Ethereum ~~2.0~~
Biggest Upgrade

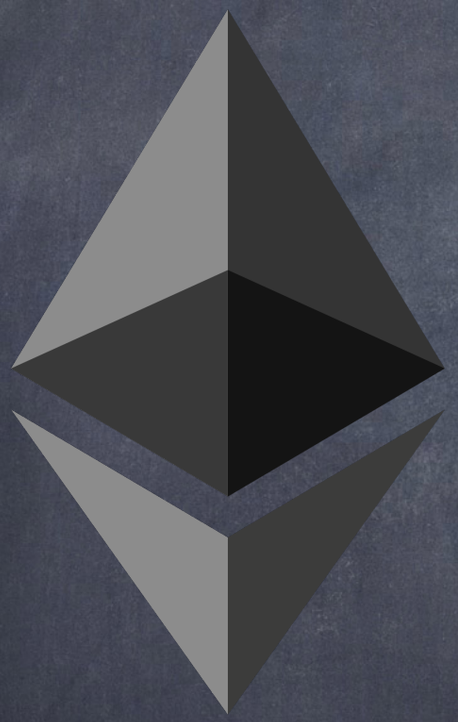
More Scalable
Sharding

More Secure
Proof-of-Stake

More Sustainable
PoW -> PoS

#87

Immutable Code



Immutable Contracts
Bugs X-> Fix

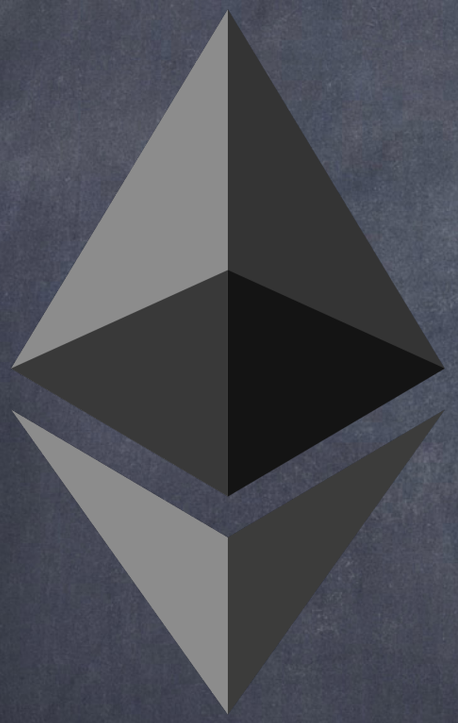
Contract -> Redeployed

Upgradeable Proxy

CREATE2

#88

Web3



Permissionless, Trust-minimized, Censorship-resistant

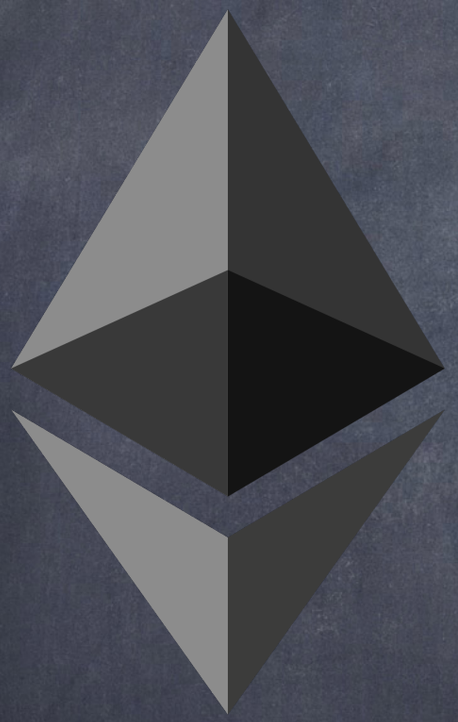
P2P: Compute/Storage/Network -> Ethereum/Swarm/Waku

Privacy & Anonymity

Web2 Principles & Practices Paradigm Security Shift

#89

Languages



Web2 -> JavaScript, Go, Rust, Nim

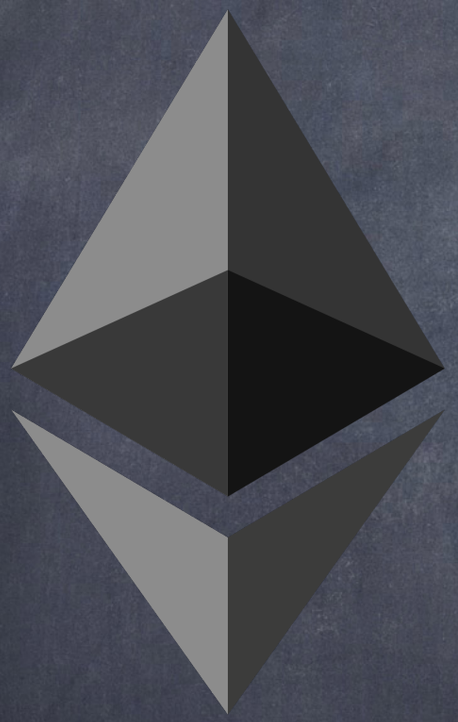
Web3 -> Web + Smart Contracts

Smart Contracts -> Solidity, Vyper, Others WIP

Solidity -> Most Used

#90

Onchain Vs Offchain



Web2 -> Offchain

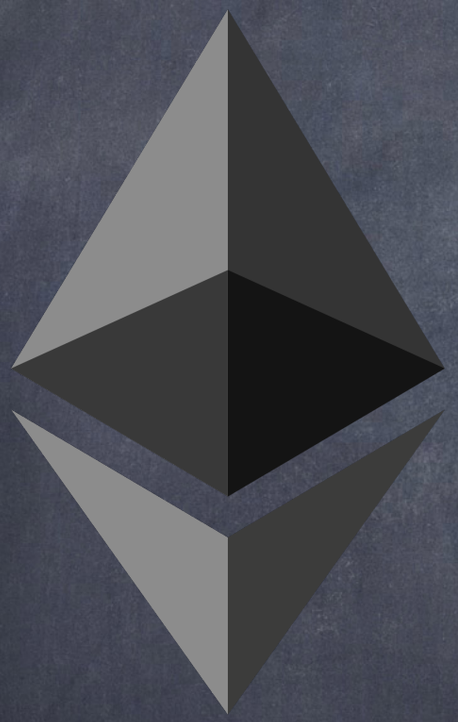
Web3 -> Offchain + Onchain

Security -> Offchain + Onchain

Main Difference
Onchain -> Smart Contracts

#91

Open-source &
Transparent



Open-source by Default
Verified Contract

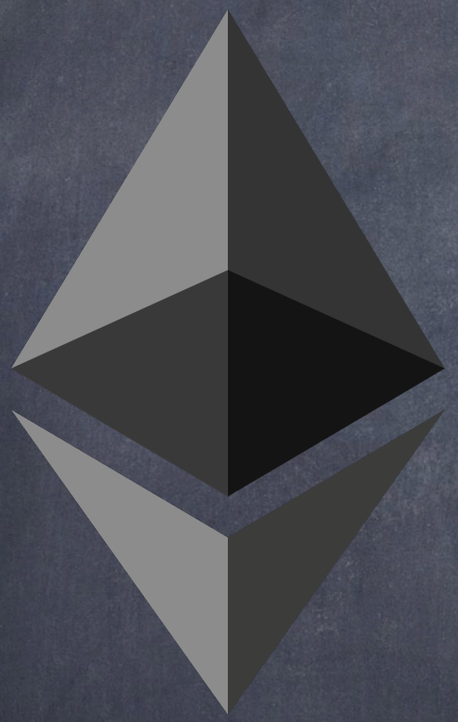
Txs & State -> Public
Real-time & Historical

All Txs -> Blockchain
Pending Txs -> Mempool

No Security by Obscurity

#92

Unstoppable & Immutable



ĐApps -> Decentralized Infrastructure & Gov

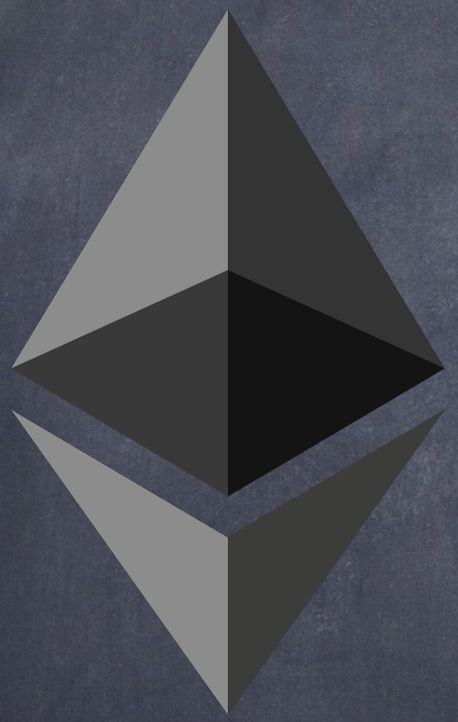
One Entity X-> Stop/ Change ĐApps/Infra/Gov

Contracts X-> Change/Stop Upgrade or Kill Switch

Harder -> Fix Vulnerability or Incident Response

#93

Pseudonymity & DAOs



Regulatory Uncertainty & Legal Implications

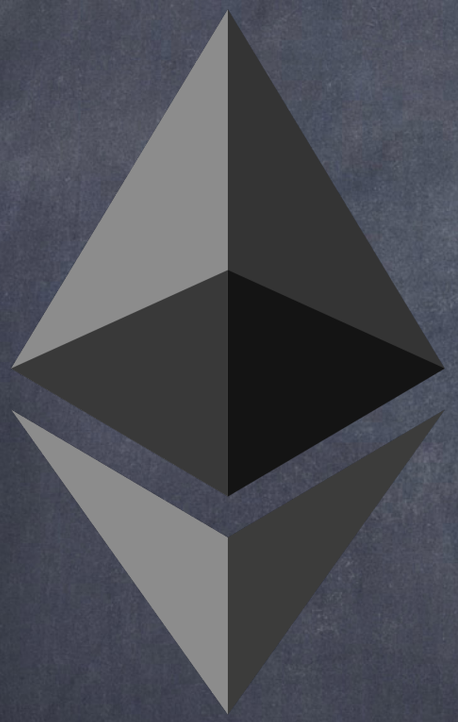
Reputation & Trustworthiness

Legal/Social Accountability
Wetware Vs Software

DAOs -> Decision Making
Security Implications

#94

Arch & Lang & Tools



Ethereum & EVM

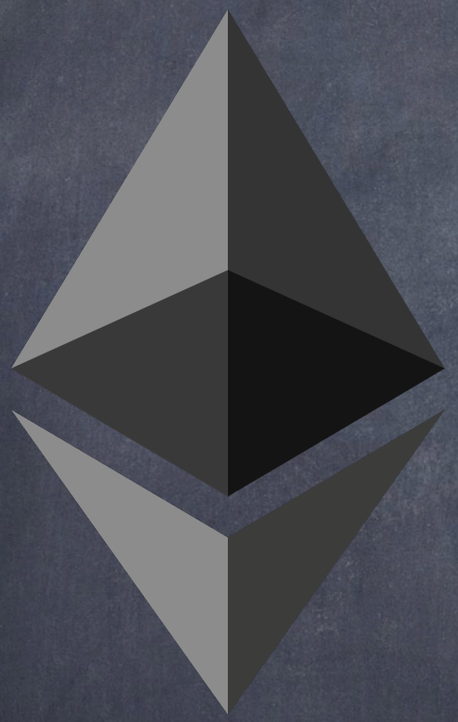
Solidity, Vyper & More

Hardhat, Truffle, Brownie, OpenZeppelin & More

Slither, MythX & More

#95

Byzantine Threat Model



Web2 -> Insiders/Outsiders
Trusted/Untrusted

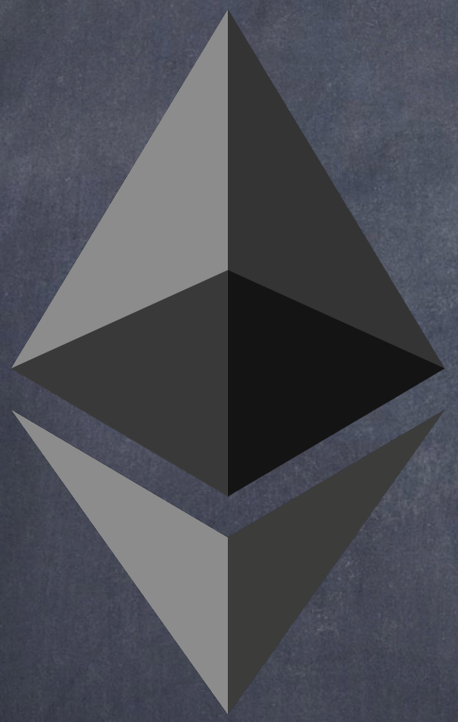
Web3 -> Byzantine Fault Tolerance

Arbitrarily Malicious Mechanism Design

Untrusted by Default
Users <-> Abusers

#96

Keys & Tokens



Passwords Vs Keys

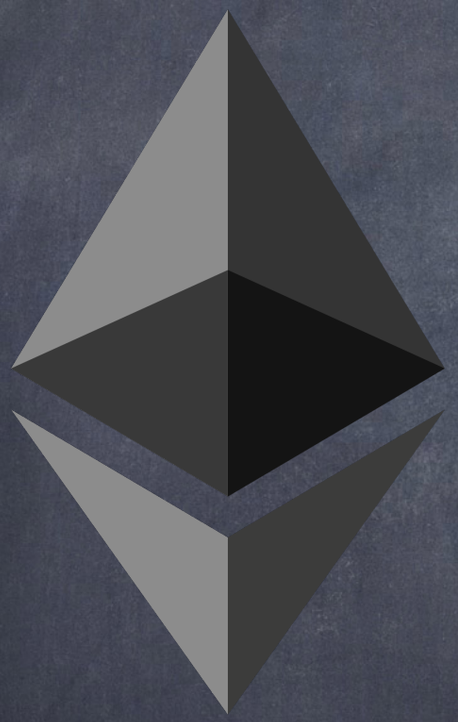
Reset/Restore Vs
Permanent Loss

Data Vs Tokens

Fines/Reg/Reversals Vs
Irreversible/Immutable

#97

Composability



Open/Composable by Design

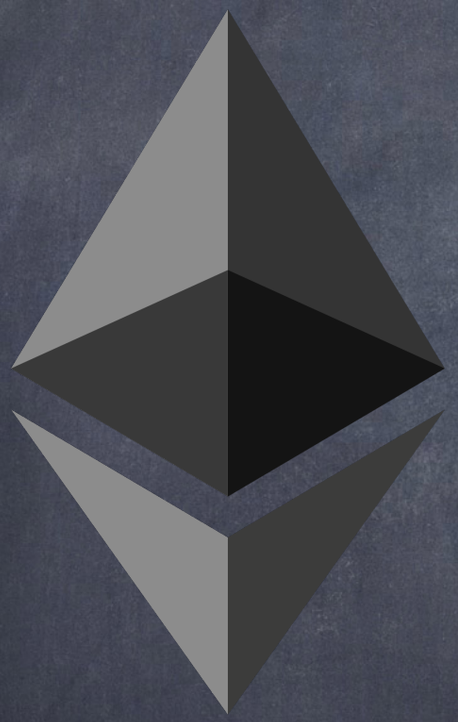
Permissionless Access Users/Contracts

Components, Configs & Dependencies

Vulnerabilities, Exploits & Attack Surface

#98

Timescale



Compressed Timescales

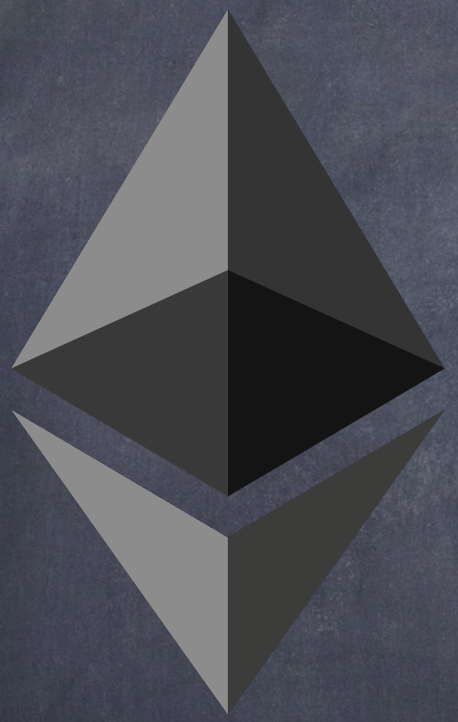
Open-source & Composable
Permissionless & Borderless

Token Incentivized &
Execution Speed

Security X-> Design & Dev
Vulnerabilities & Exploits

#99

Test-in-Prod



Compressed Timescale
Unrestricted Composability

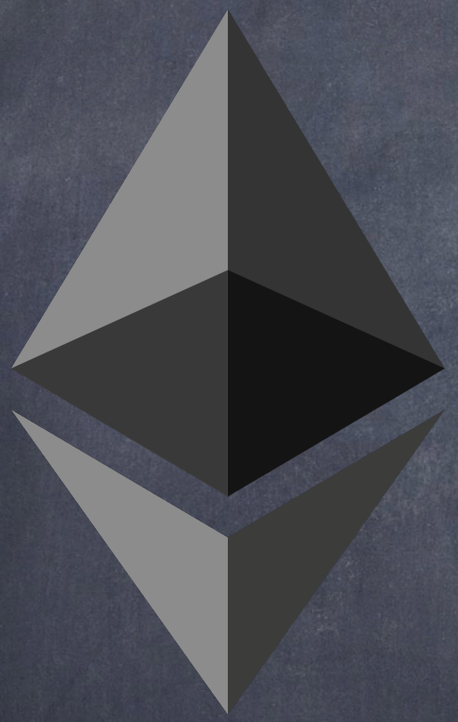
Byzantine Threat Model
Full-state Replication

Experimental Tools
Mechanism Design

Real-world Failure Modes
-> Mainnet

#100

SSDLC -> Audits



Web2 -> SSDLC

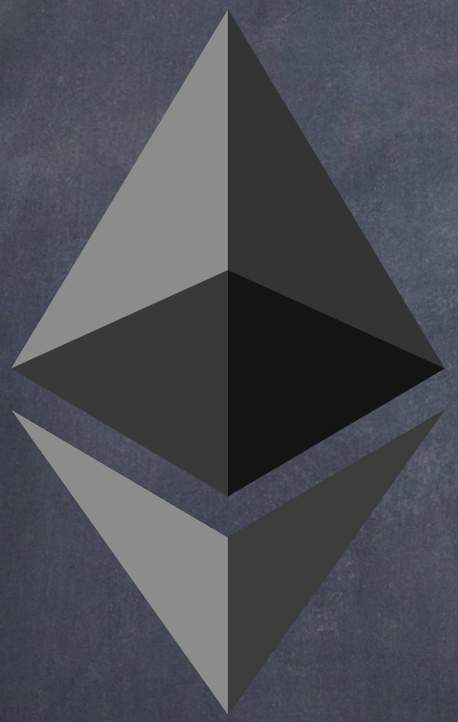
Web3 -> Audits

Build -> Audit -> Launch

Audit-as-a-Silver-Bullet

#101

State of Audits



External Assessment
Security Approval X-> Stamp

In-house X-> Expertise
External Audit Firms

Unreal Expectations
Very Expensive

Demand >> Supply
Increase/Train Auditors