TIBA

Lecture 3
Blockchain 2.0 Ethereum

By Samuel Tang, TIBA

Fall 2020 @ Tsinghua University

TIBA

Goal: How does Ethereum work?

TIBA

Content

- Ethereum
  - Identity: Account
  - Transaction
    - Message
  - Network
    - EVM
  - Blockchain
    - Smart Contract


Ethereum

Ethereum Blockchain

Ethereum: the World Computer

ethereum

Source: https://www.youtube.com/watch?v=j23HnORQXvs

TIBA

Blockchain History – Ethereum

What is Ethereum?

- **Ethereum** is a public blockchain-based distributed computing platform featuring **smart contract**
  - Ethereum VM, decentralized *Turing-complete* virtual machine for executing scripts
  - "ether", cryptocurrency token
  - "gas", a priced resource for computation

ethereum

Source: https://en.bitcoinwiki.org/wiki/Ethereum; https://en.wikipedia.org/wiki/Ethereum;

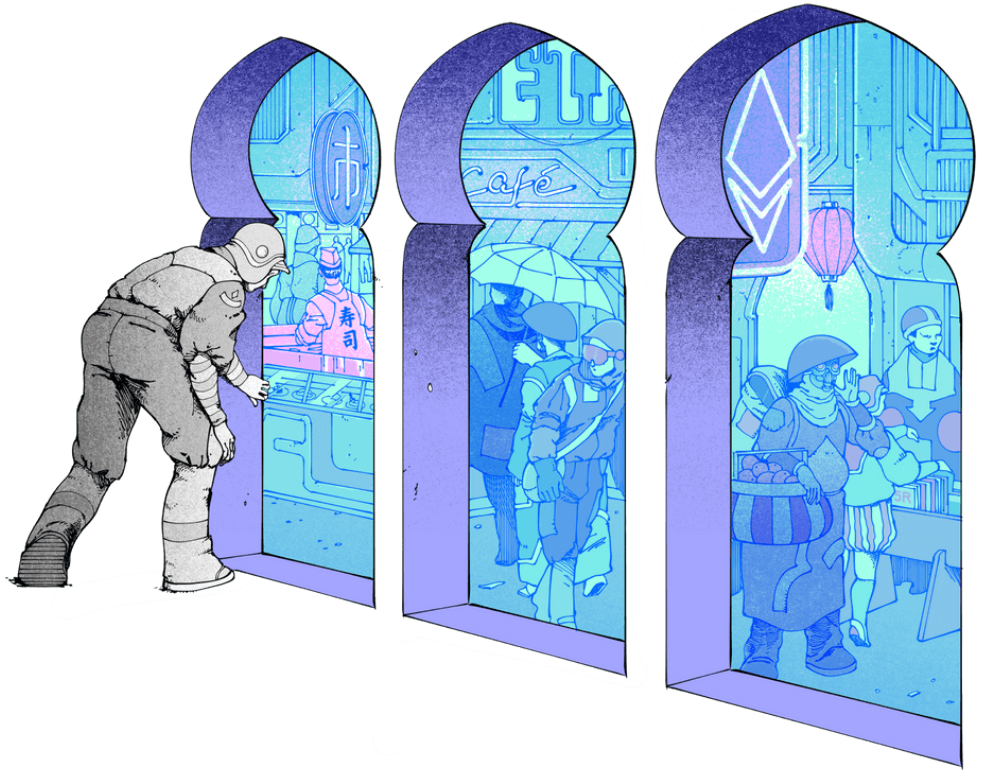
Identity: Account

TIBA

Ethereum Identity - Account

Account-based Blockchain

- **Ethereum State** is made up of objects called "**accounts**"
- each account has a 20-byte address
- an account contains four fields:
  - nonce, a counter used to make sure each transaction can only be processed once
  - current ether balance
  - contract code, if present
  - storage (empty by default)



Source: Ethereum Whitepaper; Img: https://ethereum.org/en/assets#illustrations

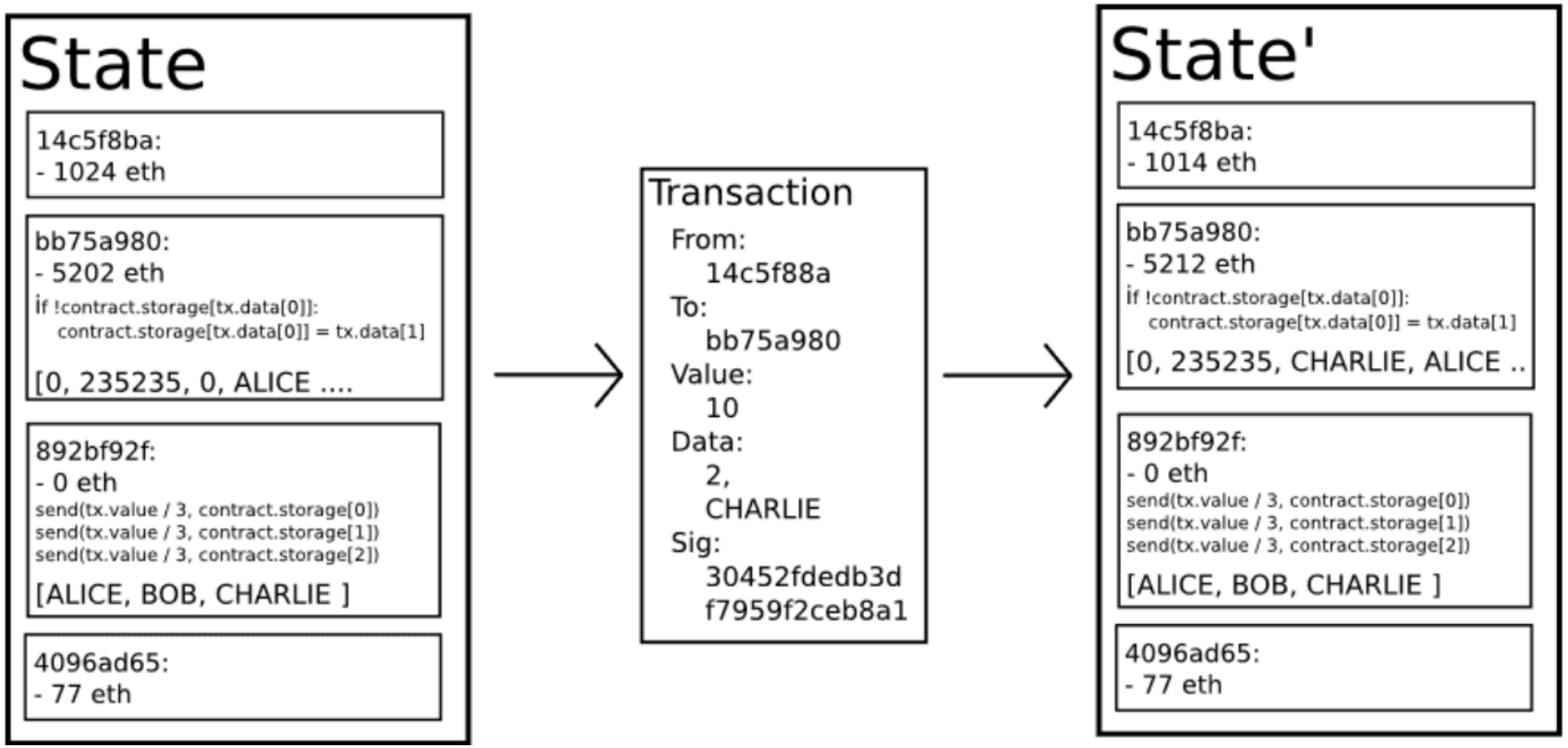
TIBA

Ethereum Fundamental - State

Ethereum State Transition Function

- **Ethereum is a transaction-based state machine**

- **state transitions** = direct transfers of value and/or information between accounts



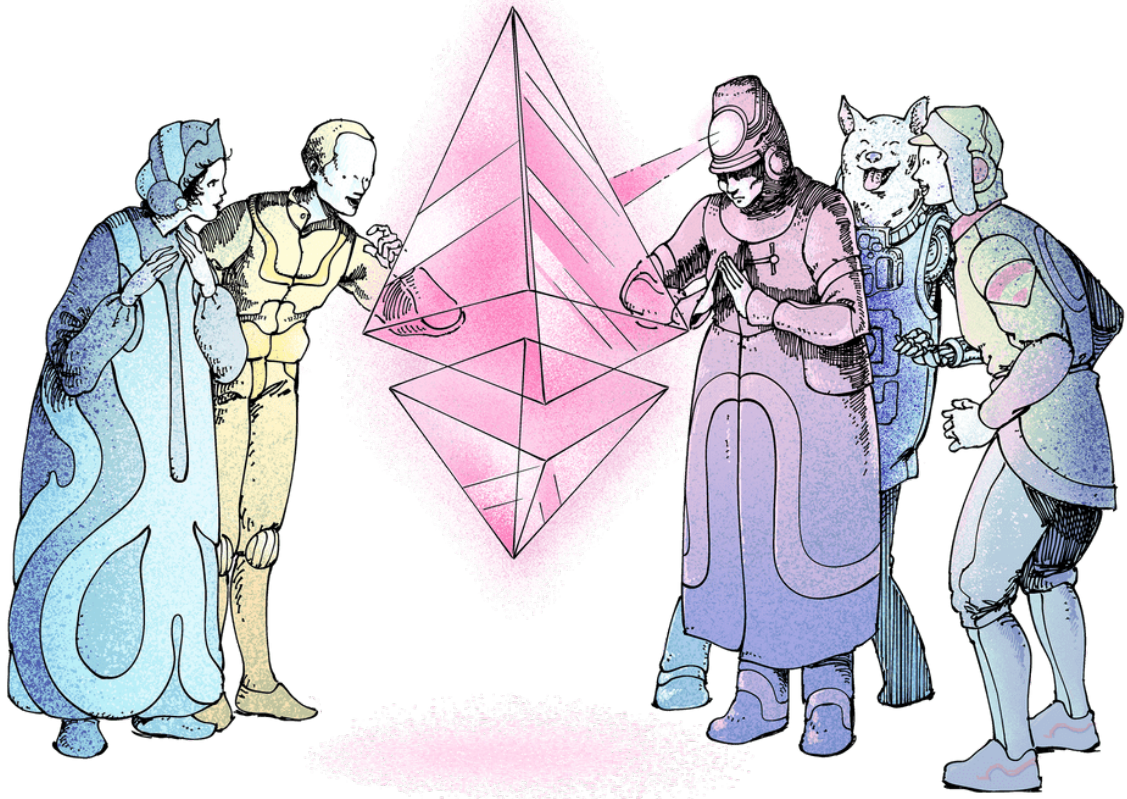
Source: Ethereum Whitepaper

TIBA

Ethereum Identity - Accounts

Two types of Accounts

- **Externally Owned Accounts**
  - controlled by private keys
  - Created by generating a private-public keypair
- **Contract Accounts**
  - controlled by their contract code
  - Created by deployment from either externally owned accounts or other contract accounts



Source: Ethereum Whitepaper; Img: https://ethereum.org/en/assets#illustrations

TIBA

STATE OBJECTS

Externally Owned Accounts **State**: Balance	Contract Accounts **State**: Balance & Storage

Address: 0x9BC11a4Abae1BDfe7d2b05C16B1A15502b5447f7
Balance: 10 ETH
Transaction Count (Nonce): 3

Address: 0xaC76Cad279439b9267FF3a3c36d4134f8d3A314c
Balance: 50 ETH
Account Creation Count (Nonce): 30
Storage (...)
Contract Code:
52341561000f57600080fd5b604051602080...

Source: ConsenSys Academy


Transaction

TIBA

Ethereum Supply & Unit of Measure

Ether the Ethereum Token

- "Unlike Bitcoin, and many other cryptos, there's no limit or cap on Ethereum's cryptocurrency, ETH. Instead, its supply increases every year."

- **Wei** is the base unit of Ether
  - 1 Ether = 1,000,000,000,000,000,000 Wei (10^{18})

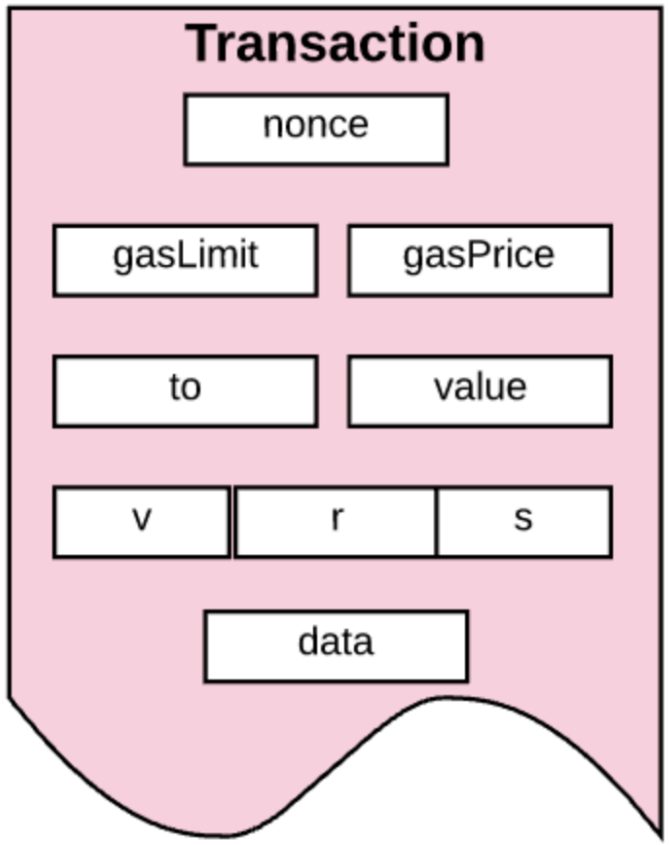
Unit	Wei Value	Wei
wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
microether (szabo)	1e12 wei	1,000,000,000,000
milliether (finney)	1e15 wei	1,000,000,000,000,000
ether	1e18 wei	1,000,000,000,000,000,000

Source: https://decrypt.co/38271/so-what-is-the-ethereum-eth-total-supply ; Img: https://ethdocs.org/en/latest/ether.html

Transactions

Transfer of Value and Information

- Transaction = signed data package that stores a message to be sent from an externally owned account
- two types of transactions:
  - message calls and contract creations
- Transactions contain:
  - Nonce, transaction count from sender
  - The recipient of the message
  - A signature identifying the sender (V, R, S)
  - The amount of wei to transfer from the sender to the recipient
  - An optional data field
  - Gas Limit
  - Gas Price



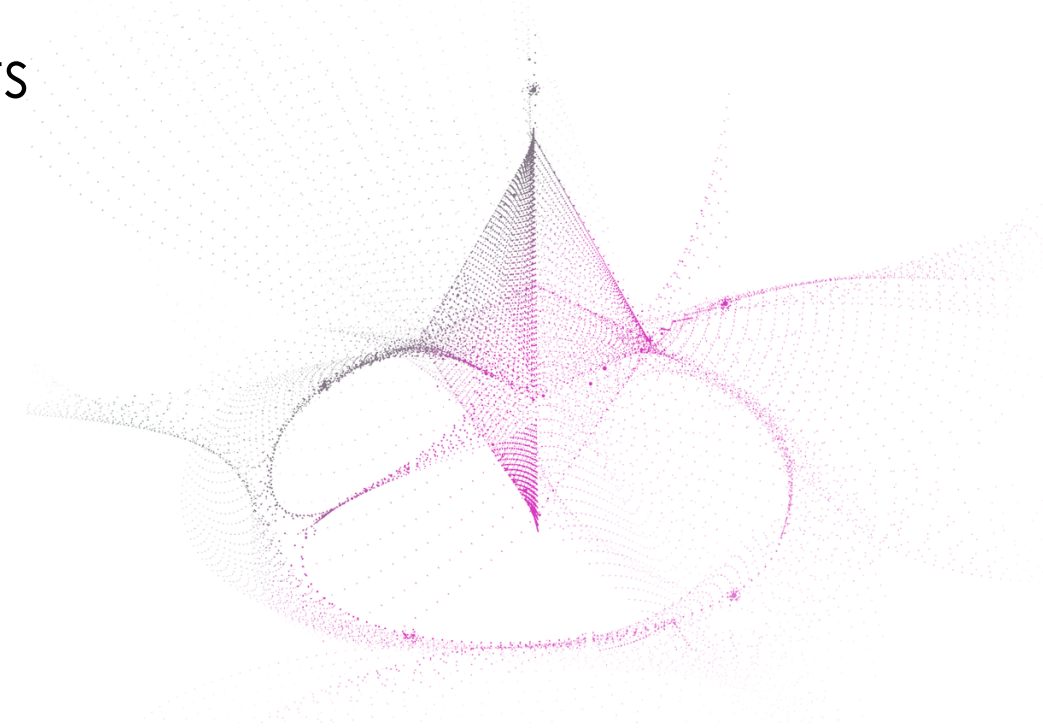
Source: Ethereum Whitepaper; How does Ethereum work, anyway? By Preethi Kasireddy

TIBA

Message/Internal Transaction

Transfer of Value and Information

- Initiated by Externally Owned Accounts message calls, produced by Contract Accounts
- A message contains:
  - The sender of the message (implicit)
  - The recipient of the message
  - The amount of wei to transfer alongside the message
  - An optional data field
  - Gas Limit



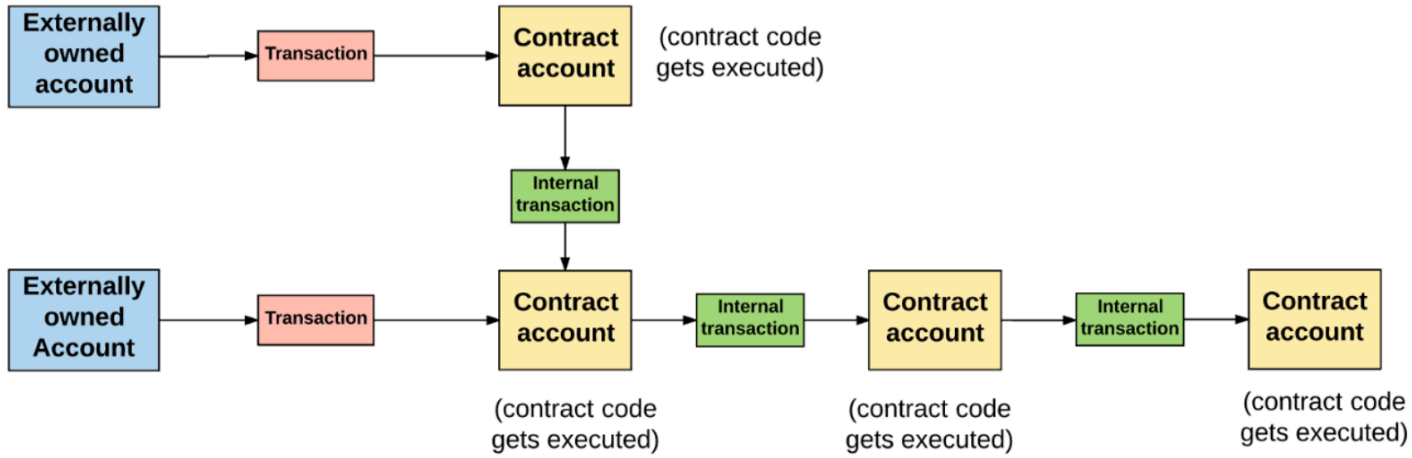
Source: Ethereum Whitepaper; Img: https://ethereum.org/en/assets#illustrations

TIBA

Message/Internal Transaction

Transfer of Value and Information

- a message:
  - from externally owned account to contract account
    - activates the contract account's code, allowing it to perform various actions
  - from one contract to another contract
    - the associated code that exists on the recipient contract account is executed

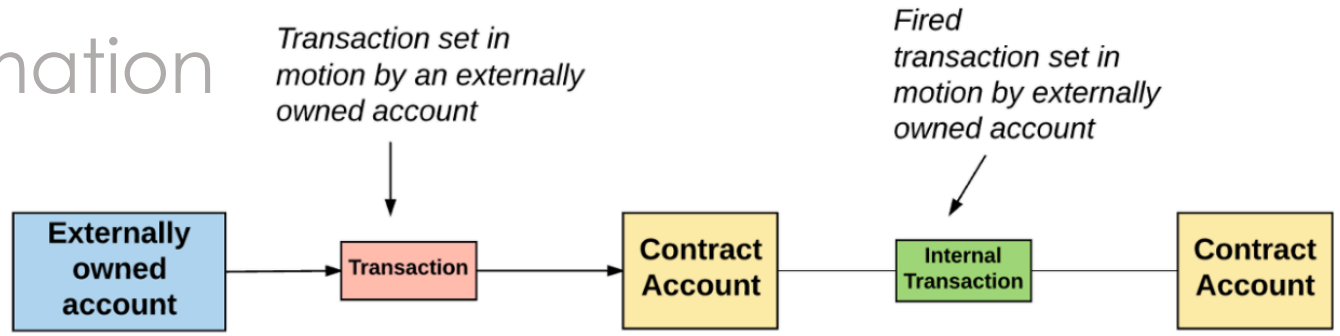


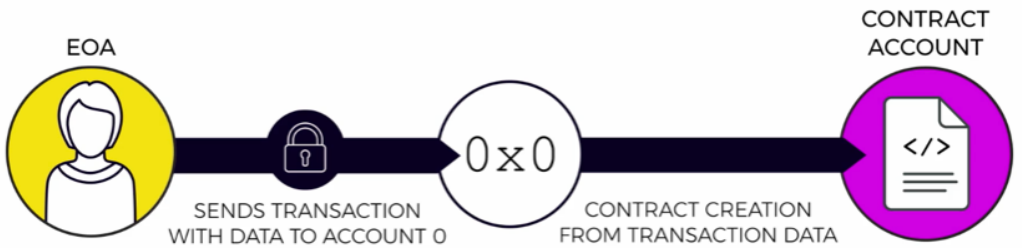
Source: Ethereum Whitepaper; How does Ethereum work, anyway? By Preethi Kasireddy

Transaction Target

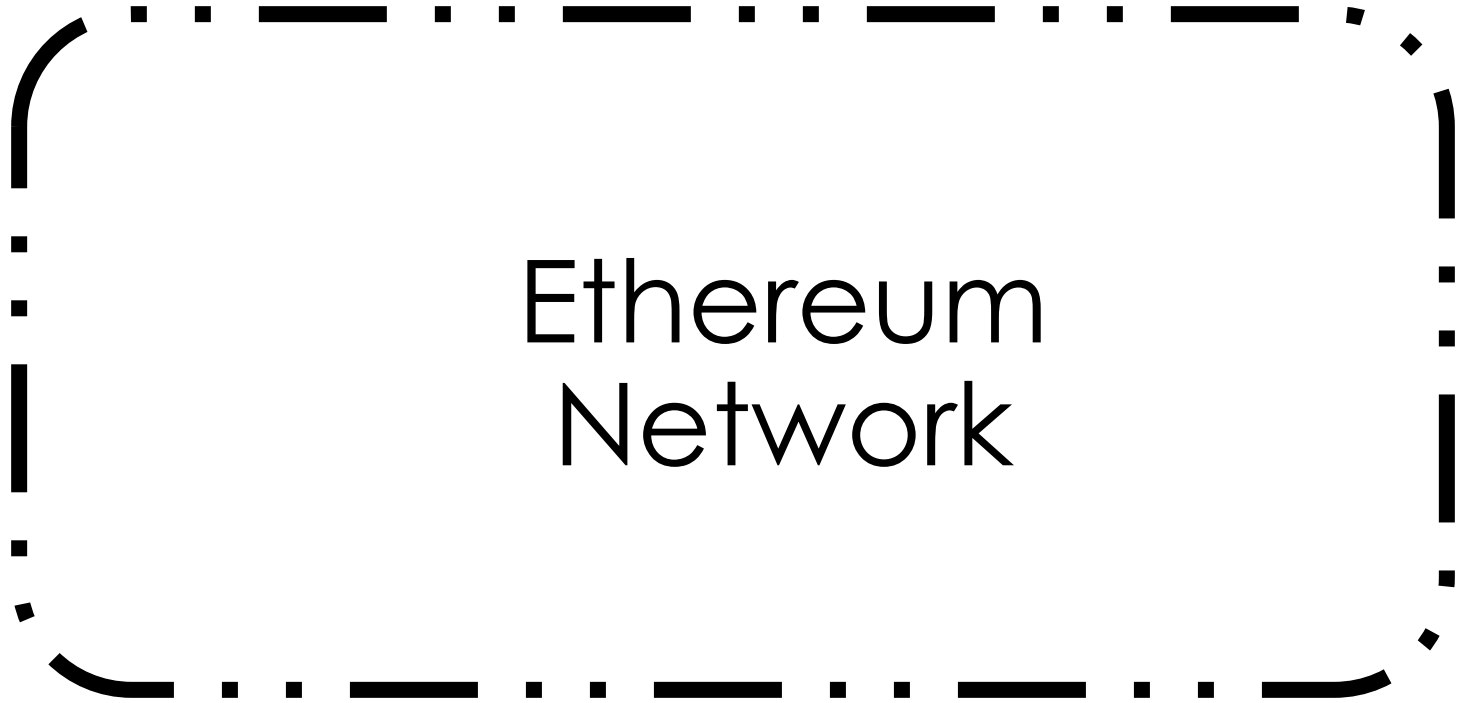
Transfer of Value and Information

- If transaction target is a externally owned account
  - value transfer between two accounts
- If transaction target is a contract
  - Contract code executes with transaction data as input
- If transaction target account is 0
  - Create a new contract from transaction data





Source: Ethereum Whitepaper; How does Ethereum work, anyway? By Preethi Kasireddy; ConsenSys Academy

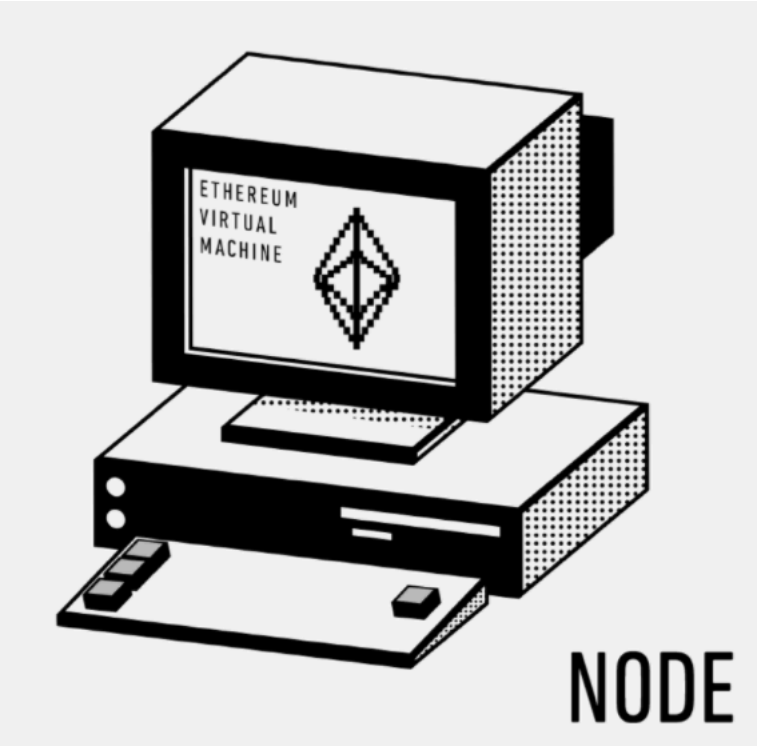

Ethereum
Network

TIBA

Ethereum Virtual Machine

EVM

- Each node runs EVM
  - a “mini” computer that process all transactions and runs contract code
- Turing Complete
  - can perform any computation given enough time and memory
- Operates on bytecode
- Slow (10-20 transactions per second)
  - Every transaction is processed by every node
  - Only as fast as the slowest machine



Source: ConsenSys Academy; Img: https://ethgas.io/it/;

TIBA

Gas

Digital Fuel for EVM

- **Gas** = unit that measures the amount of computational effort required to execute specific operations on EVM

- Every operations on EVM requires some gas in order to execute
  - Process transaction
  - Each step in contract code

Source: Blockchain at Berkeley, Fundamental Decal; https://ethereum.org/en/developers/docs/gas/; Img: https://www.blockchain.us/ether-what-are-gas-gas-limit-and-gas-price; ; https://www.ethos.io/what-is-ethereum-gas/

TIBA

Gas

Digital Fuel for EVM

- **Gas Limit**, (aka Start Gas) the maximum amount of gas that the sender is willing to pay for executing this transaction. This amount is set and paid upfront, before any computation is done.

- **Gas Price**, the fee the sender pays per unit of gas (per computational step)

- Gas Limit * Gas Price = Gas paid when submit transaction (transaction fee)

Source: https://ethereum.org/en/developers/docs/gas/; Img: https://www.blockchain.us/ether-what-are-gas-gas-limit-and-gas-price/; https://www.uptrennd.com/post-detail/looking-for-gas-analysis-on-matic~NzIxNDI3

TIBA

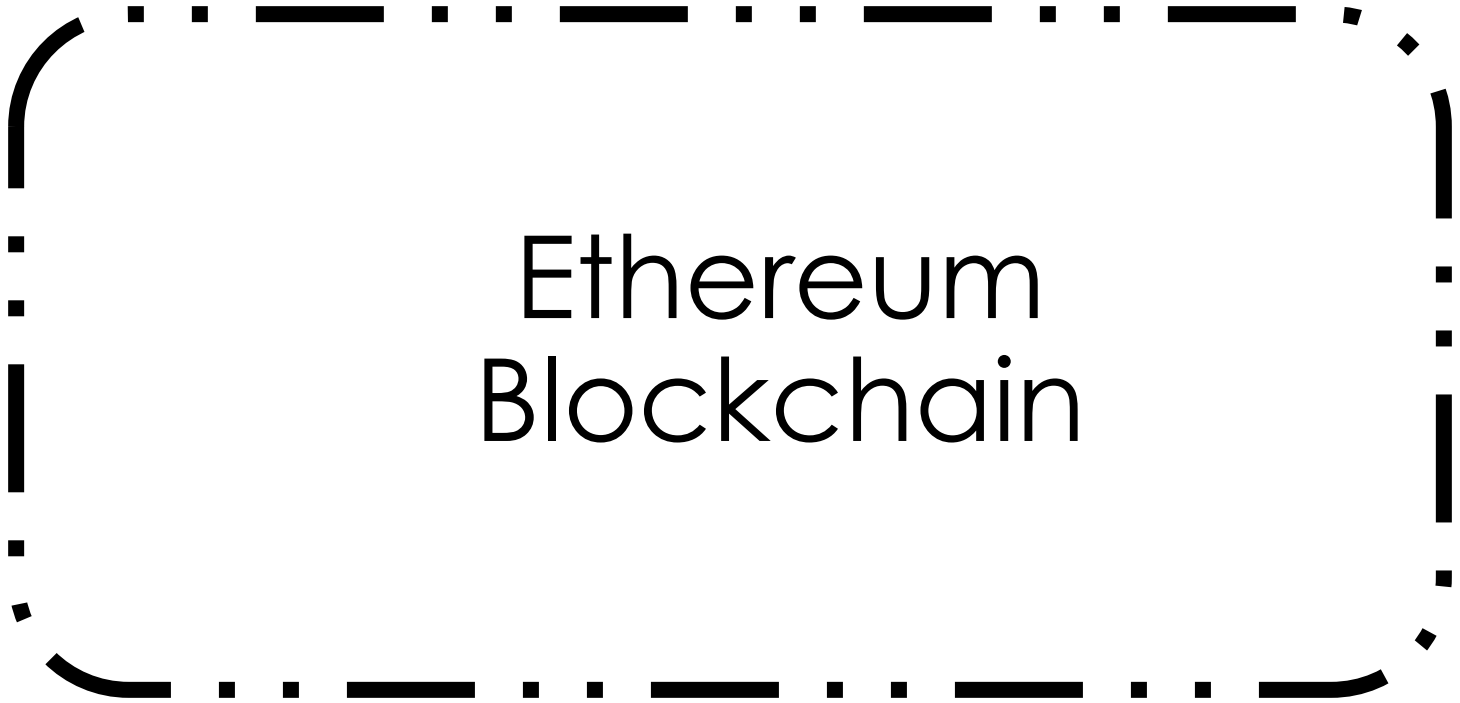
Gas

Digital Fuel for EVM

- If execution successfully
  - Remaining gas is refunded to sender

- If execution runs out of gas
  - Execution reverts back to the state before transaction was made
  - Gas paid is not refunded

Source: Blockchain at Berkeley Fundemental Decal; Img: https://ethereum.org/en/assets#illustrations


Ethereum
Blockchain

TIBA

Proof of Work (PoW)

Ethereum 1.0's Consensus Algorithm

- **Proof of work** – the process of solving a cryptographic puzzle
  - hard to solve, easy to verify
  - the only way to solve is by using brute force method
  - consumes a lot of energy
  - **Ethereum**:
    - Find a nonce (number only used once) such that the hash of the block results in certain amount of leading zeros
    - able to adjust mining difficulty by changing the number of leading zeros

TIBA

Proof of Work (PoW)

Ethereum 1.0's Consensus Algorithm

- Ethereum Mining:
  - Download entire Ethereum blockchain
  - Verify incoming transactions and run Smart Contract code invoked by transactions
  - Create a block
  - Find a valid nonce
  - Broadcast your block
  - Profit!

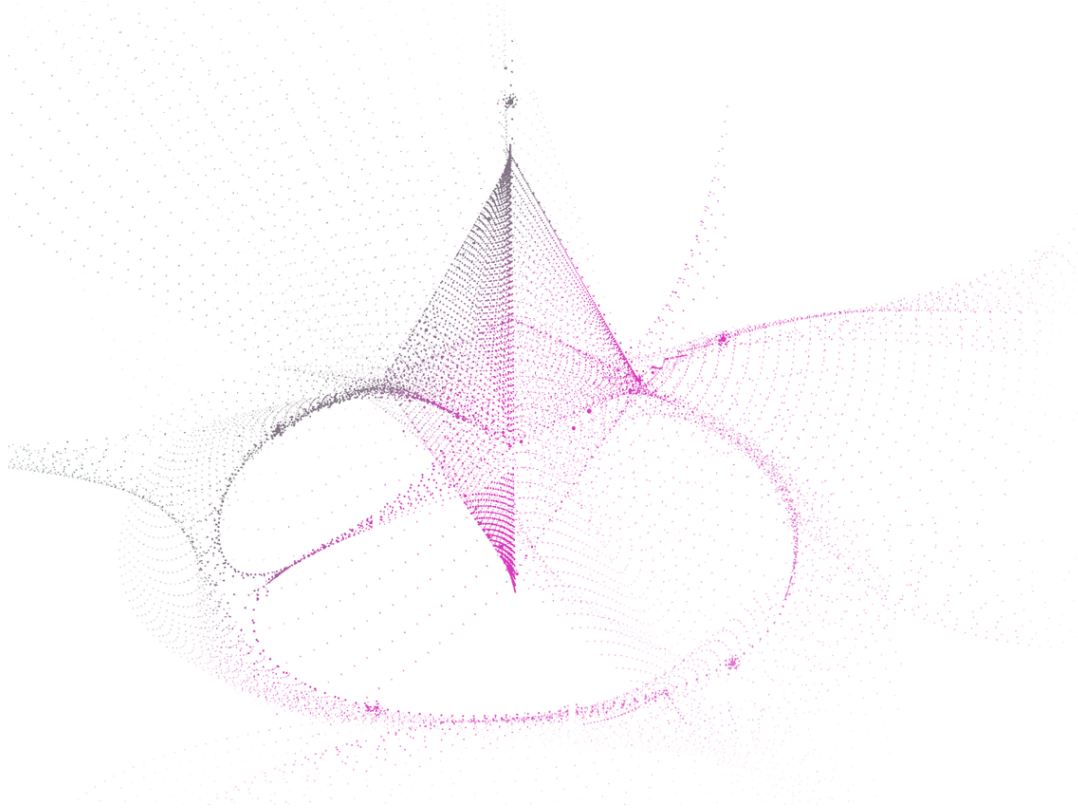
Source: Blockchain at Berkeley Fundamental Decal

TIBA

Ethereum Blockchain

Basics

- A block is found every ~ 15 seconds
- Uncles blocks – a discovered block not included in the main chain (longest chain)
- Discovering uncle blocks is rewarded



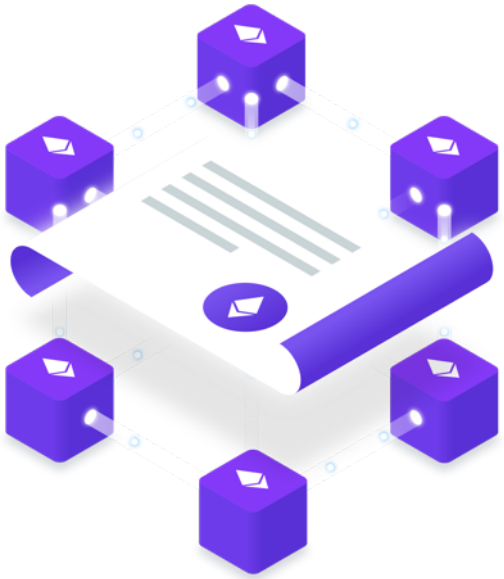
Source: ConsenSys Academy; Img: https://ethereum.org/en/assets#illustrations

TIBA

Smart Contract

Self-executing digital contract

- A **smart contract** is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code
- The code is stored on and exist across a distributed, decentralized blockchain network
- first proposed in 1994 by **Nick Szabo** (invented “Bit Gold" in 1998)

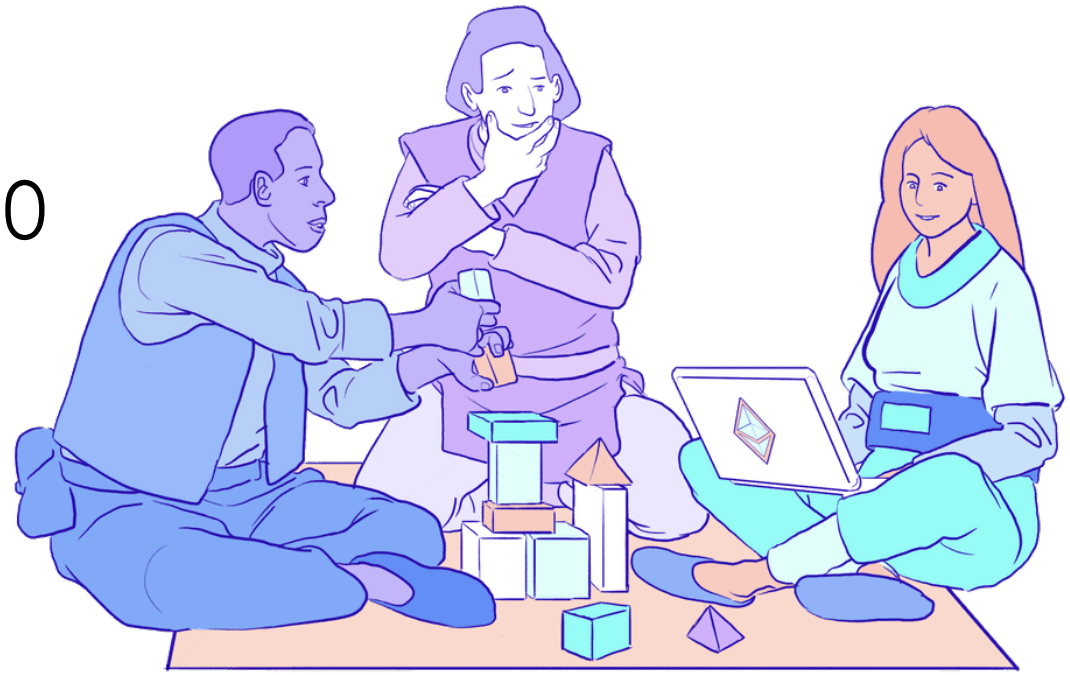


Source: https://www.investopedia.com/terms/s/smart-contracts.asp
https://www.pulsehyip.com/smart-contracts-development; https://www.originprotocol.com/en/product

Ethereum 2.0

Eth2

- upgrade to the current Ethereum network(Ethereum 1.0)
- Phase 0 planned to launch in 2020
- Increase scalability and security
- Proof of Stake (PoS)
  - Locking up “stake” (Ether)
  - Validators instead of miners
  - Replace energy consumption with a financial commitment



Source: https://ethereum.org/en/eth2/

TIBA

Questions?

Homework Assignments

- Medium - How does Ethereum work, anyway? By Preethi Kasireddy
- Ethereum Whitepaper
- Coindesk, Ethereum History in 5 Charts
- WHAT IS ETHEREUM? The foundation for our digital future
- Ethereum Official Website
- Decrypt, So, what is the Ethereum (ETH) total supply?
- GAS AND FEES
- Ethereum 2.0 (Eth2)

TIBA

Blockchain 2.0
Ethereum
by
Samuel Tang

Thank you for listening!
See you next week!