

Ethereum

21CSPH0 Blockchain Technology and Applications

Motivation

Bitcoin scripting language is too restrictive

Not turing complete

No loops

Less functionality

Introduction

Founded by Vitalik Buterin in 2013

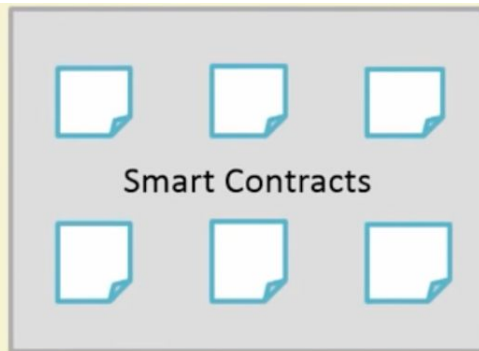
Introduced the notion of smart contract - business logic

Smart contracts are termed as DApps - Decentralized Applications which runs on Ethereum Virtual Machine

Developed by Ethereum Foundation

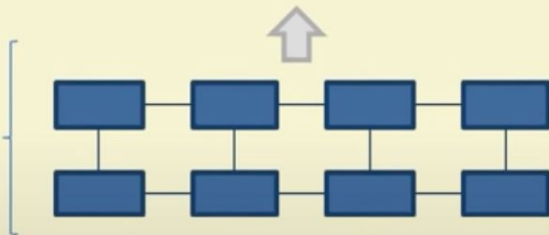
Introduction

Founded by Vitalik Buterin (bitcoin scripting language too restrictive for smart contracts)



The smart contracts are also known as Dapps (Decentralized Applications), and run on the Ethereum Virtual Machine (EVM)

Ethereum is an overloaded term. May refer to public network, a private/permissioned network, or open source software



Public mainnet runs more than 16,000 nodes, average block time is 17s (as of May 2018); Miners currently get 5 ETH + transaction fees

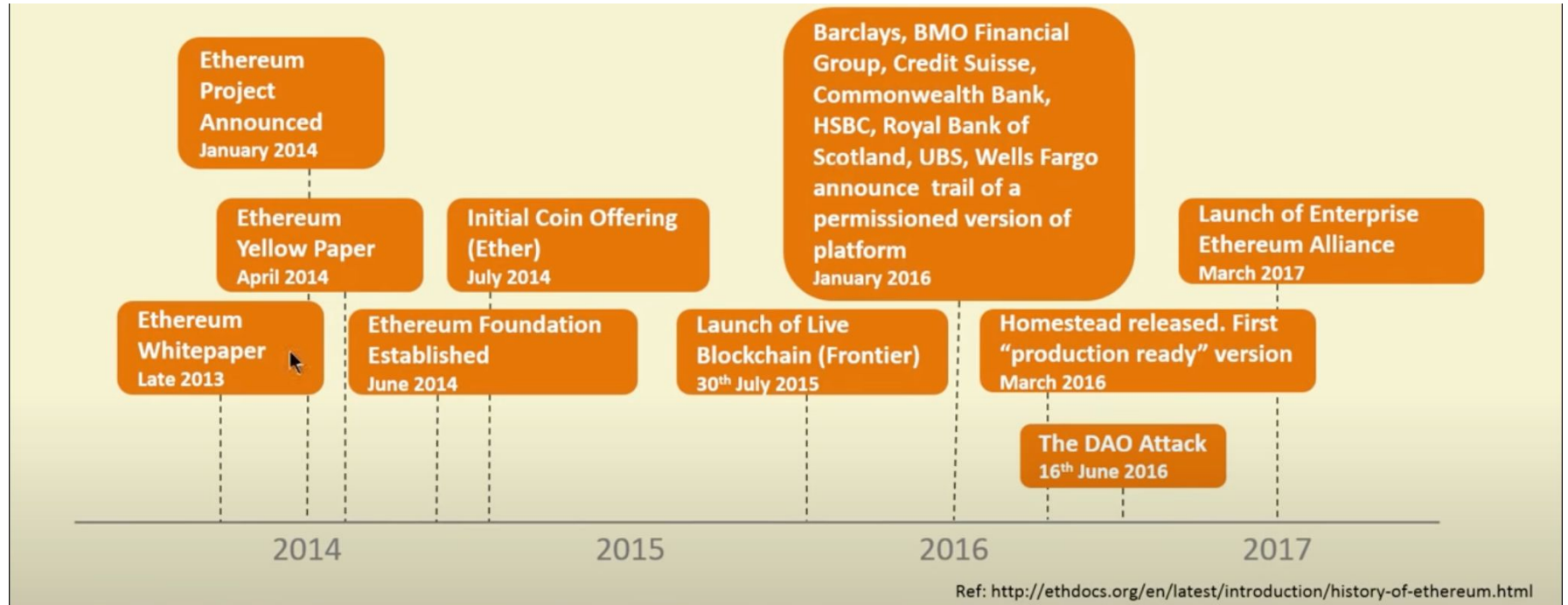
Developed by the *Ethereum Foundation*, a Swiss nonprofit organization with many contributions coming from the broader community.

Reference Links

<https://ethernodes.org/history>

<https://etherscan.io/>

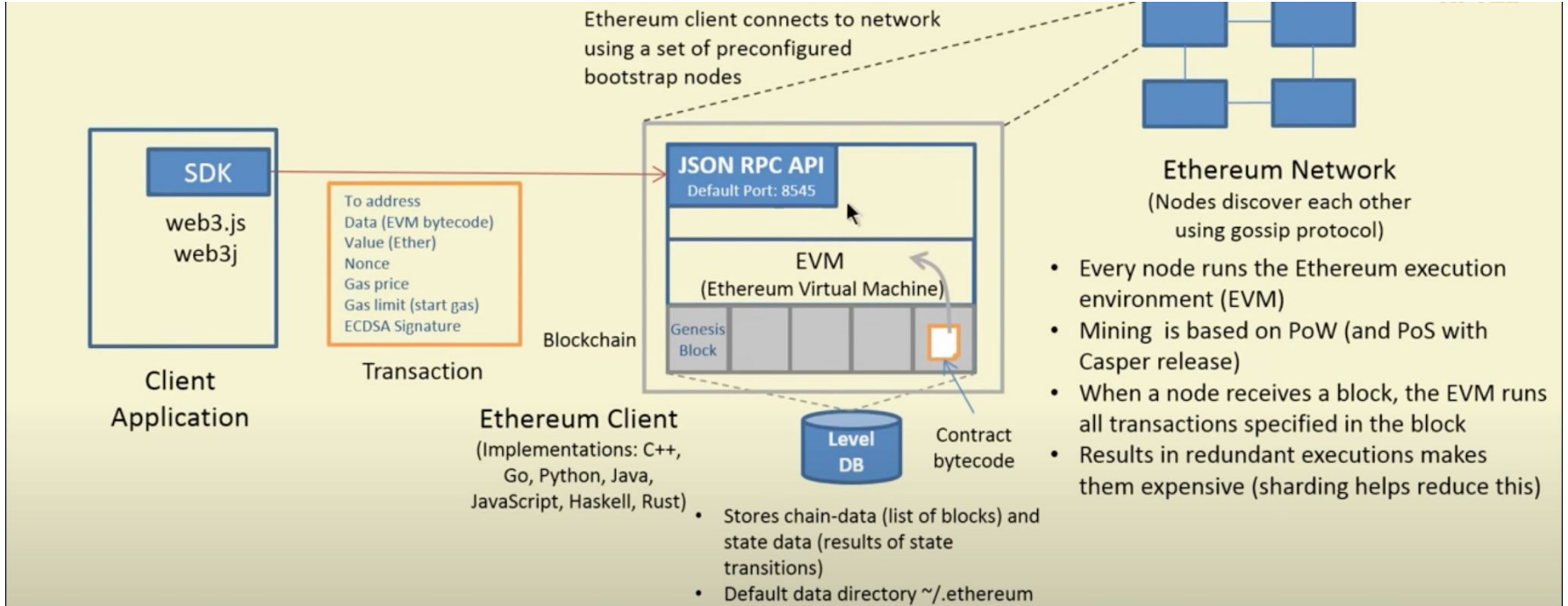
History



Initial Coin Offering

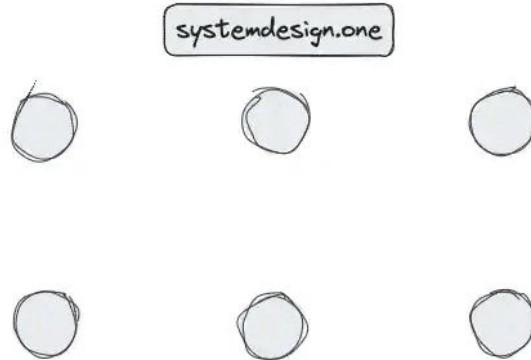
- Funding through cryptocurrencies - crowdfunding
- A quantity of cryptocurrency is sold in the form of 'tokens' ('coins') to investors
- In exchange for existing cryptocurrencies
- The tokens are promoted as future functional units of currency
- An ICO can be a source of capital for startup companies
- Ethereum raised money with a token sale in 2014, raising around 31,000 BTC in July, equal to approximately \$18.3 million at the time.

Ethereum Architecture



Gossip Protocol

- The gossip protocol is a decentralized peer-to-peer communication technique to transmit messages in an enormous distributed system.
- The key concept of gossip protocol is that every node periodically sends out a message to a subset of other random nodes.
- The entire system will receive the particular message eventually with a high probability.



Account Types, Gas and Transactions

