

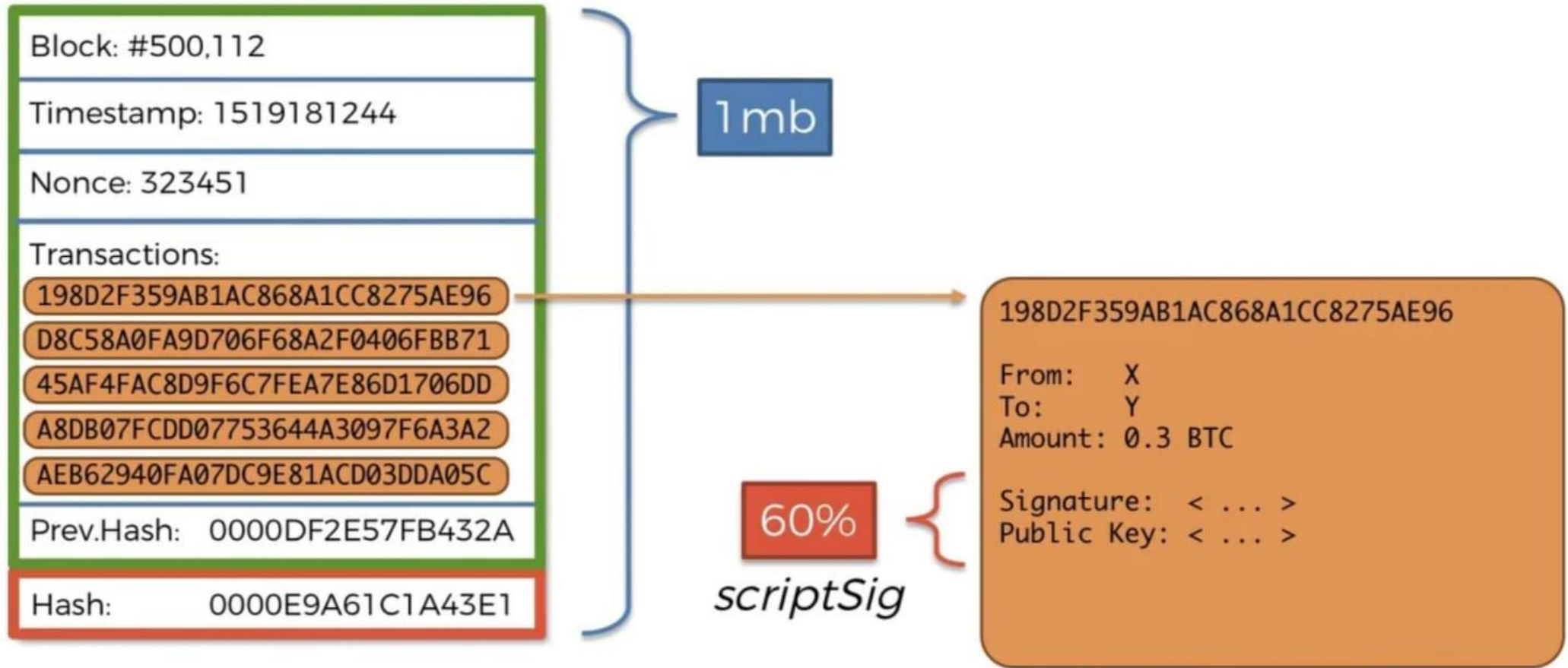


Blockchain and Cryptocurrency

By: Syeda Tayyaba Bukhari

Segregated Witness (SegWit)

49



DAO Attack



2016

On Ethereum

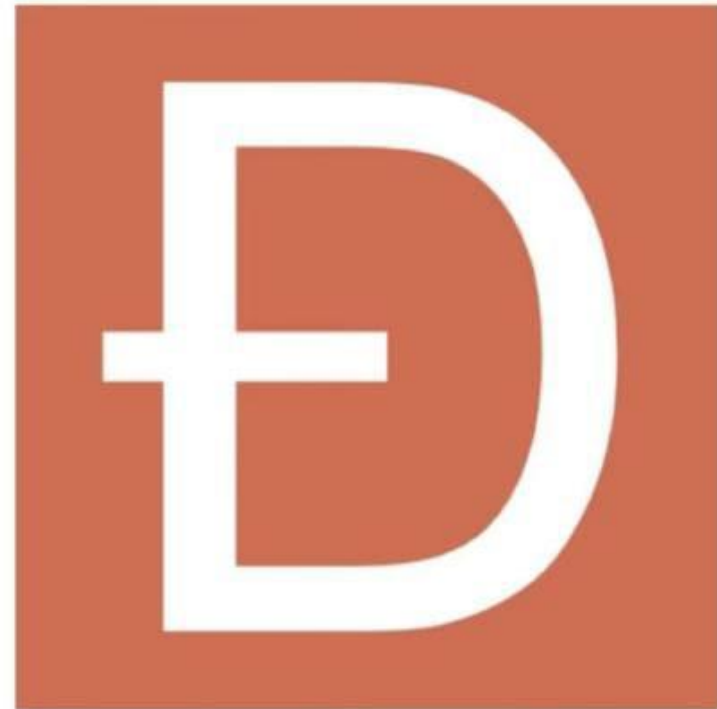
Investor-directed venture capital fund

Stateless

May 2016 Crowdfunded ~\$150,000,000

June 2016 Hacked for ~\$50,000,000

Dilemma: *"Code Is Law?"*



The background of the image is a dense field of 3D black dollar signs (\$). In the center, one dollar sign is highlighted in a bright orange color, standing out from the rest. The text "Solution presented was:" is written in white, sans-serif font across the middle of the image, partially overlapping the orange dollar sign.

Solution presented was:

Solution: Hard Fork




Solution: Hard Fork

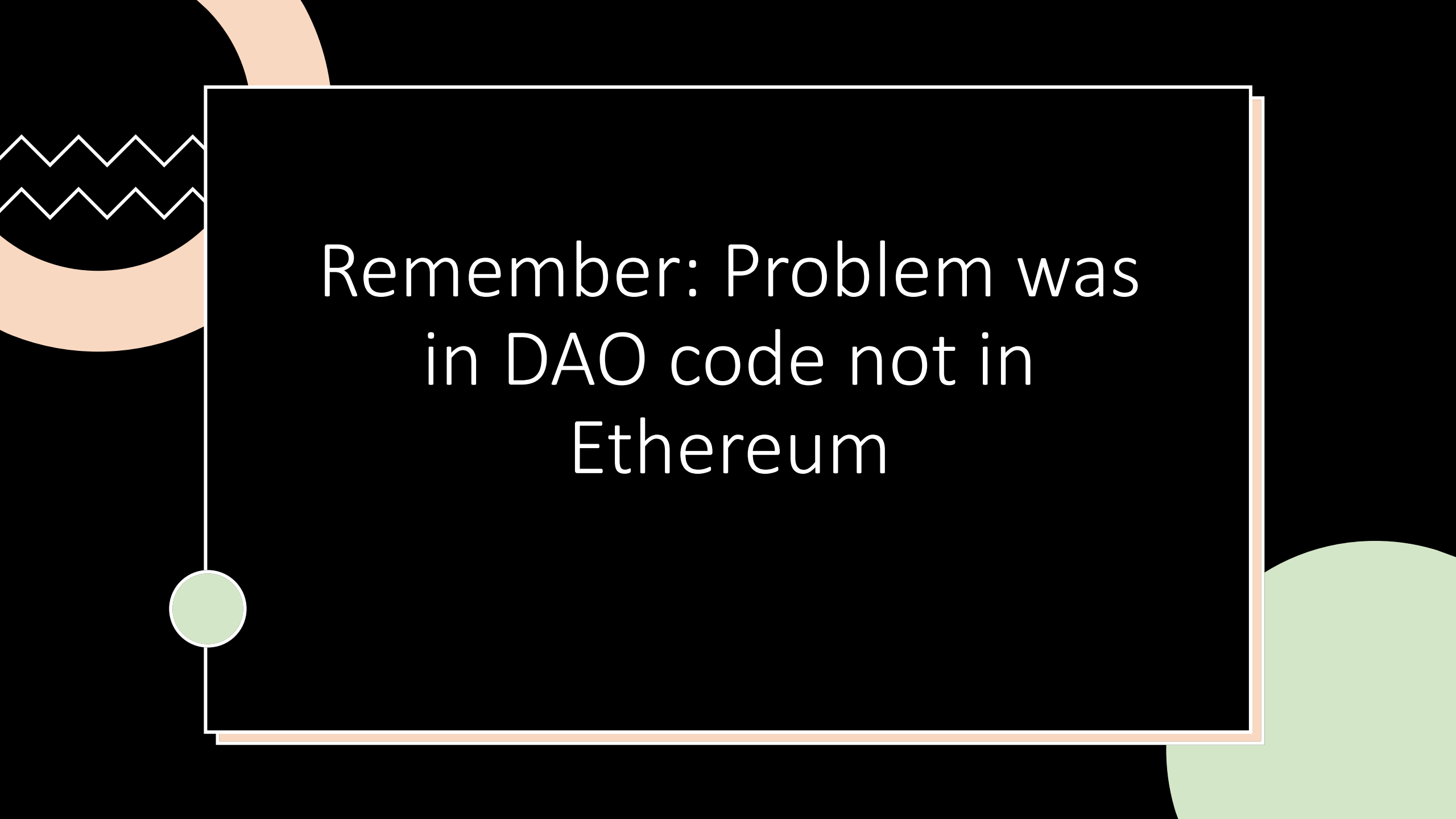
-> Ethereum split into 2 parts

-> ETH and ETC

ETH(Ethereum): Money returned to owner/DAO

ETC(Ethereum Classic): Money remains on child account and will be transferred to hacker's account after decided time limit



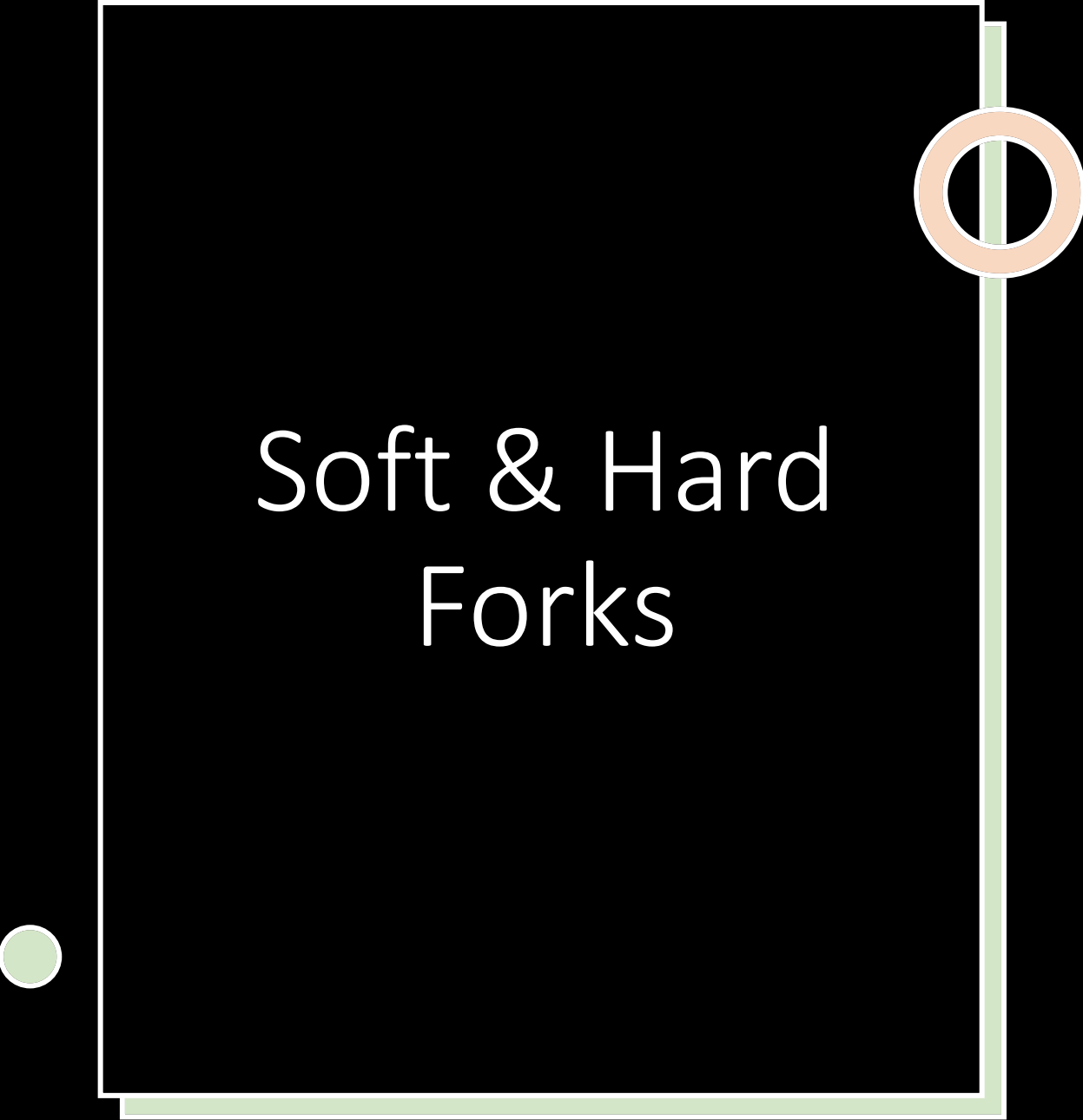


Remember: Problem was
in DAO code not in
Ethereum

Must read Blog:

The Ether Thief

<https://www.bloomberg.com/features/2017-the-ether-thief/>



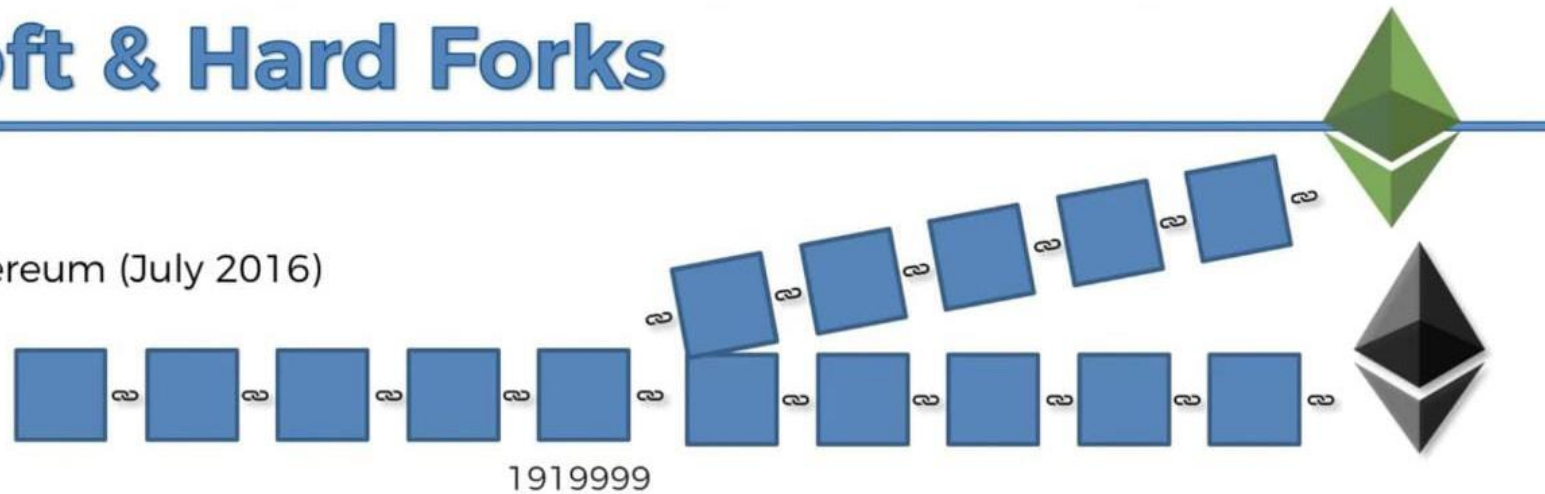
Soft & Hard Forks



Hard Fork produced ETH and ETC

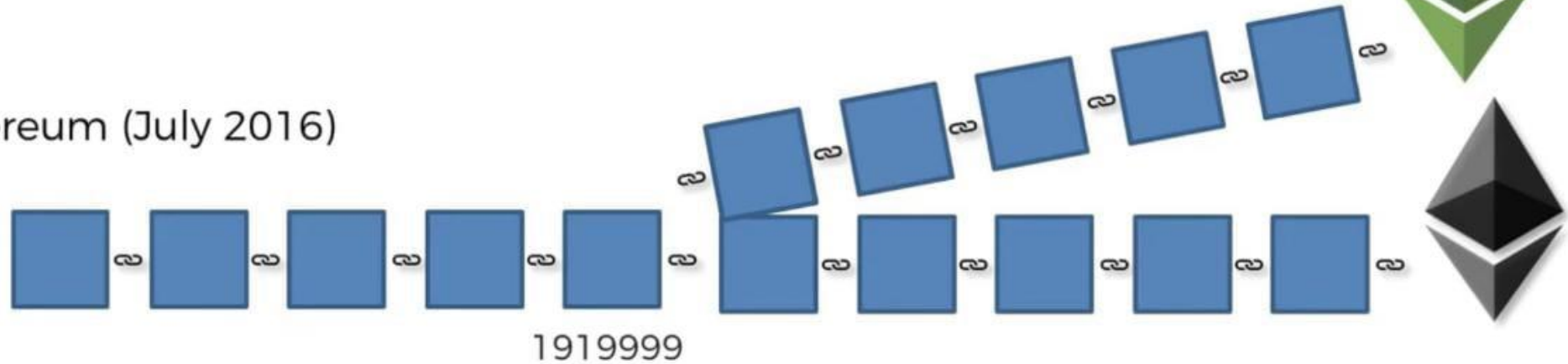
Soft & Hard Forks

Ethereum (July 2016)

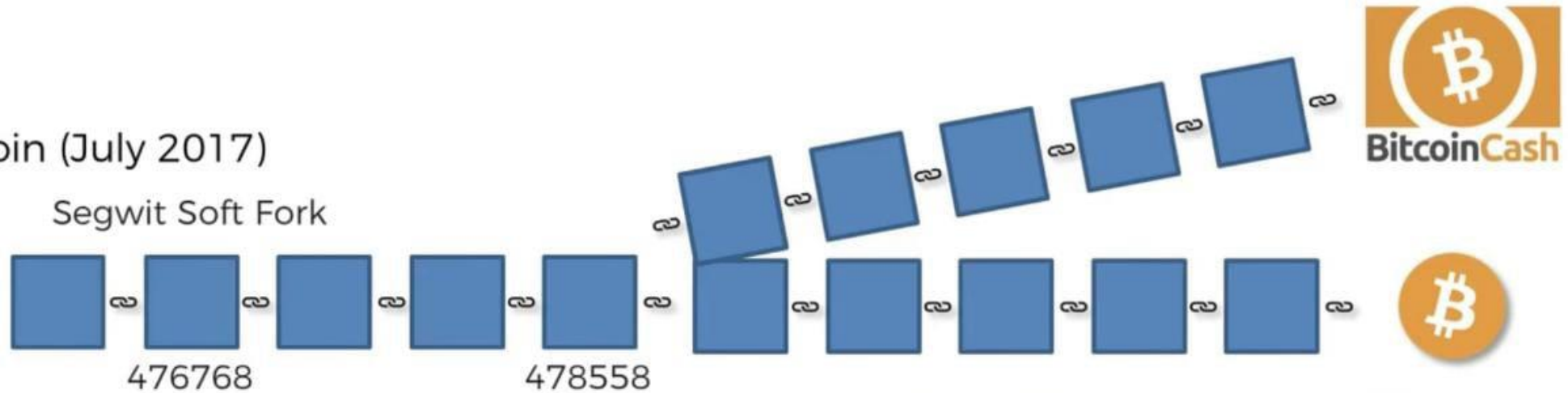


Soft & Hard Forks

Ethereum (July 2016)

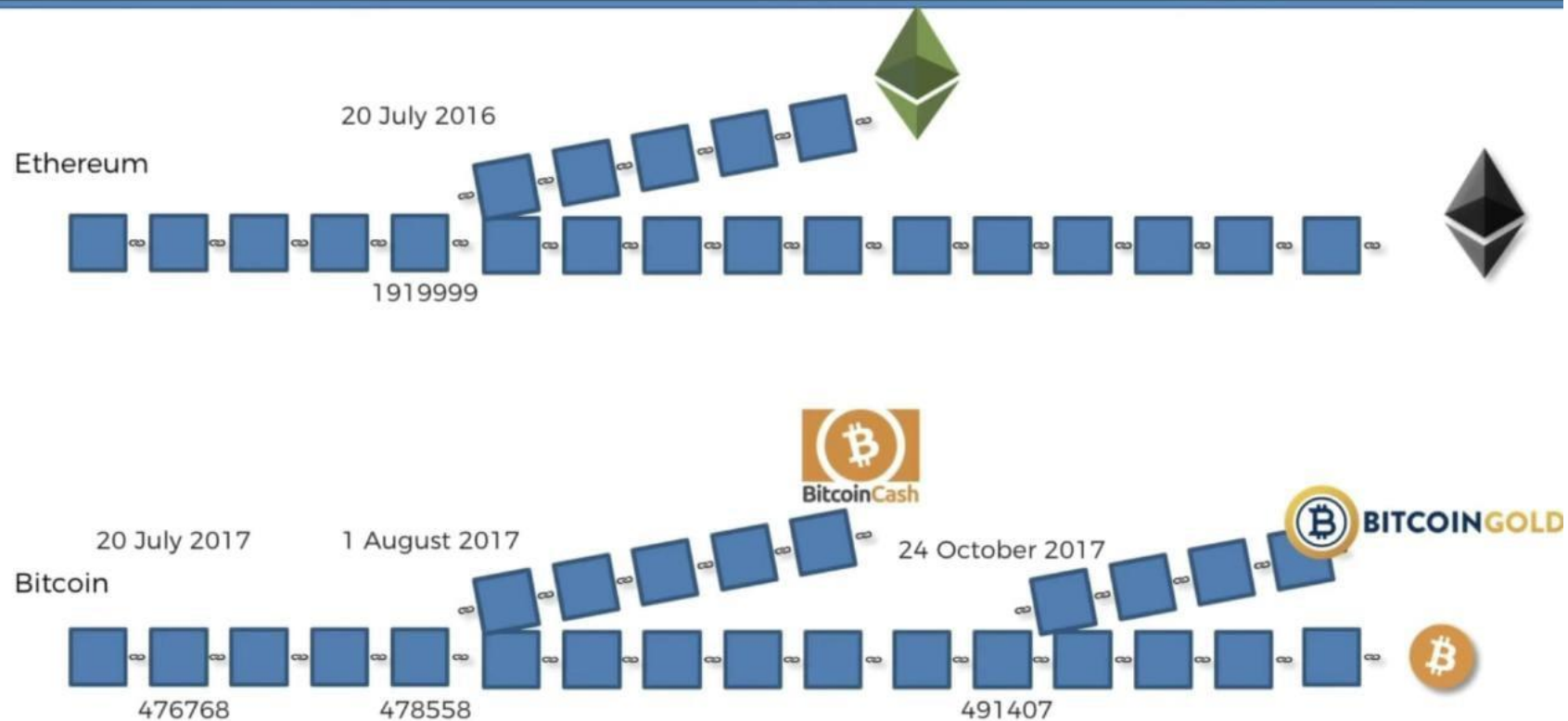


Bitcoin (July 2017)



20 July 2016 --- Hard Fork on Ethereum to change rules of smart contract due to DAO attack
20 July 2017 --- Soft Fork on Bitcoin to upgrade Bitcoin with Segwit Witness feature
1 August 2017 --- Hard Fork on Bitcoin to increase the Block size up-to 8MB from 1 MB
24 October 2017 --- Hard Fork on Bitcoin to make ASIC resistant network.

Soft & Hard Forks



Soft & Hard Forks

Hard Forks = Loosen Rules

Soft Forks = Tighten Rules

Lecture 20

- ASM-002 Evaluations

Acknowledgement and Source:

- <https://www.udemy.com/course/build-your-blockchain-az/>