OST
Eastern Switzerland
University of Applied Sciences

Distributed Systems Advanced & Blockchain

In the News

Thomas Bocek

14 September 2020

In the News

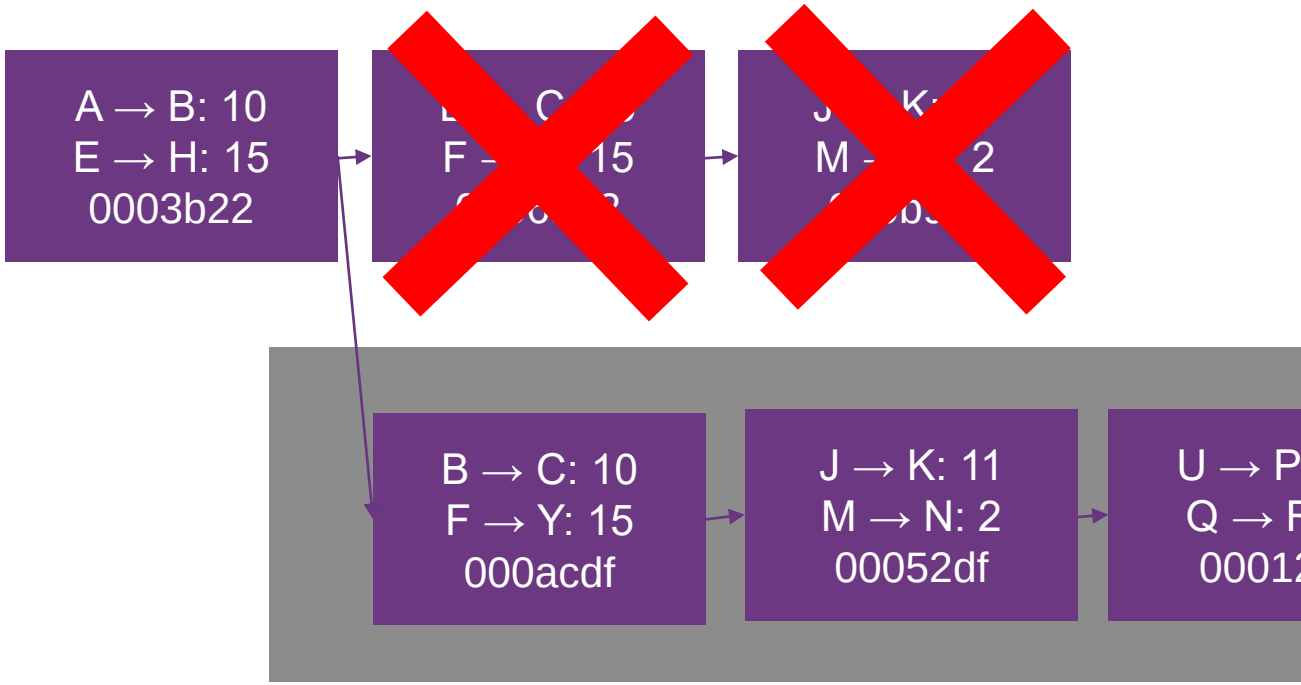
- 51% Attack in Ethereum / Bitcoin
- “If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.”
  - https://bitcoin.org/bitcoin.pdf
- How expensive is a 51% attack?
  - Buy an attack?
  - “Ethereum Classic Labs singled out crypto-mining marketplace NiceHash for allegedly facilitating multiple attacks against the network”

- 01.08.2020: Ethereum Classic suffered a 3,693-blockchain reorganization early Saturday morning, an event first thought to be a possible 51% attack, after a miner used old software after having been offline, according to Terry Culver, CEO of Ethereum Classic Labs.
- 06.08.2020: Ethereum Classic has suffered its second 51% attack in a week after more than 4,000 blocks were reorganized Thursday morning.
- 17.08.2020: OKEx has confirmed a loss of approximately $5.6 million in Ethereum Classic (ETC) from two recent 51% attacks and is considering removing ETC from its exchanges.
- 01.09.2020: Ethereum Classic (ETC) Suffers Yet Another 51% Attack, Major Changes Needed to Improve Blockchain Platform’s Security

OST

In the News

- Longest chain survives (same as Bitcoin)
- Double spend: rollback transactions
  - X is an exchange address
  - Mine secretly, Y is attacker address
  - X arrived – exchange does payout USD (wait 2 block conf.)
  - You mine faster as you have 51%, broadcast secret chain
  - Tx F→X: 15 never happened, goes to Y, but attacker already got the USD
    - Attacker can spend the 15 coins again (double spend)



OST

In the News

- 28.08.2020: Ethereum is a Dark Forest
  - Someone sent tokens to the pair contract, not to the intended recipient
  - If smart contract not designed with that in mind, tokens are locked forever
    - Uniswap was designed that tokens can be recovered
    - … by anyone, tokens worth $12’000
  - Problem: generalized frontrunner
    - Bots monitoring mempool of new transactions, and e.g., checking if they could replace an address in the contract with their address → if they can do it, create new transaction with higher gas
    - Frontrun and profit
- Approach idea
  - Create contract that has a function to do the withdraw
  - Deploy contract (even 2 contracts)
  - Generalized frontrunner not smart enough to get tokens when running the contract
  - Issue transaction that calls the contract
  - Generalized frontrunner cannot do anything with this transaction
- Authors tried to conceal and hide withdraw
  - Failed