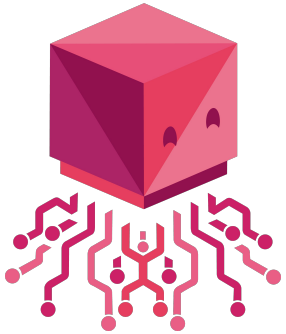
Cloning Attack

On Proof-of-Authority Ethereum Blockchains



BLOCKCHAIN
REALLABOR
RHEINISCHES REVIER

Thanks to the great paper by Ekparinya et al.

P. Ekparinya, V. Gramoli, and G. Jourjon, “The Attack of the Clones Against Proof-of-Authority,” presented at the Network and Distributed System Security Symposium, San Diego, CA, 2020, doi: 10.14722/ndss.2020.24082

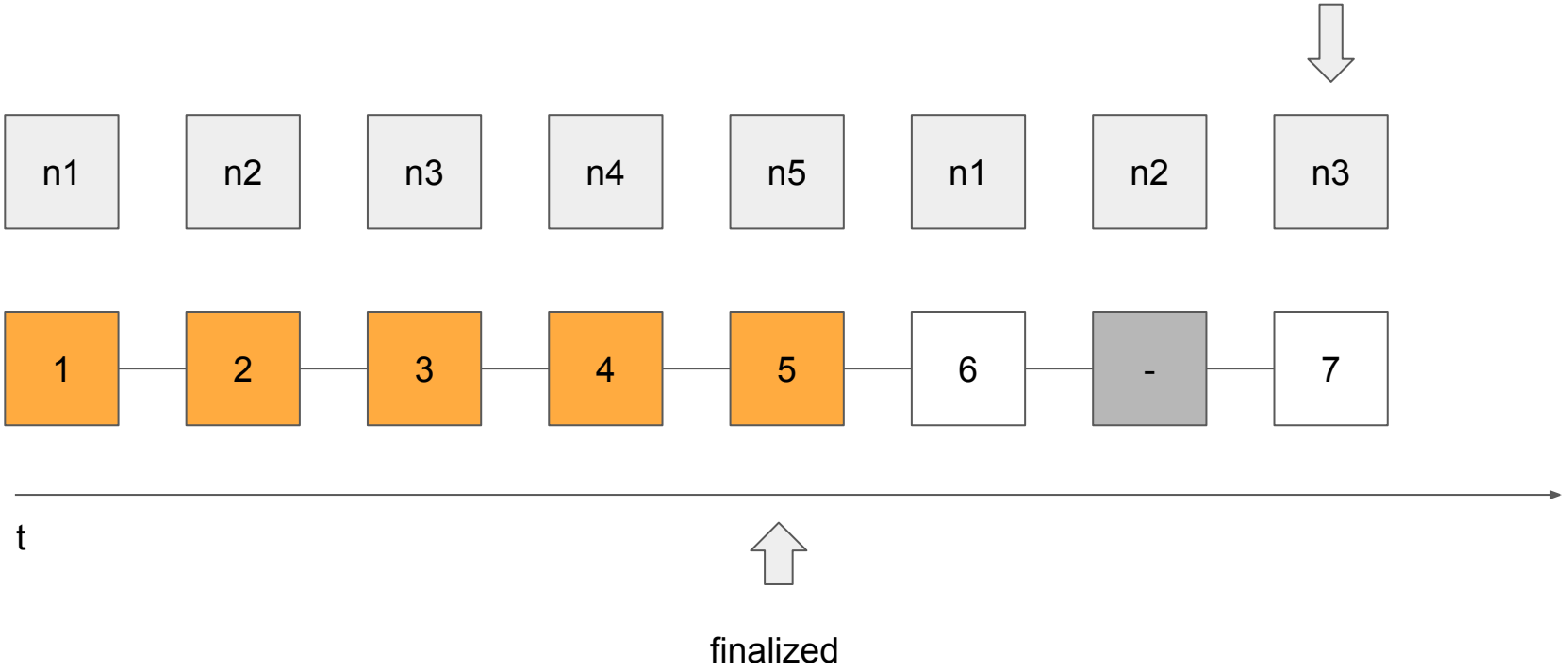
What is Ethereum?

- Second largest cryptocurrency platform
- Turing-Complete “World-Computer”
- “Rich Statefulness”
- Supports development of DApps using Smart Contracts
- Public PoW networks
  - MainNet, Ropsten, Classic
- Public PoA networks
  - Bloxberg (Aura consensus)
- Private PoA networks
  - Cloud offerings, e.g. Azure

Aura - Authority Round (aka majority vote)

- Time is divided into steps of discrete duration t
- Primary for a step s is the node with index: s mod n
- Chain score SCORE(C) for a given chain C can be considered as height of C
- Each node keeps a set of signed blocks:
  - $SIG\_SET(B) = \{a | \exists b \in B : AUTHOR(b) = a\}$
- Finalized valid chain ending with C[K…] if
  - $|SIG\_SET(C[K..])| > \frac{n}{2}$

Aura - Sealing for 5 Validator Nodes



What happens in case of network partition?

- Network partitions might occur during normal operation because of network/internet glitches
- SCORE(C) function in Aura protocol means, longest chain wins after network partition is over and normal mode of operation is resumed

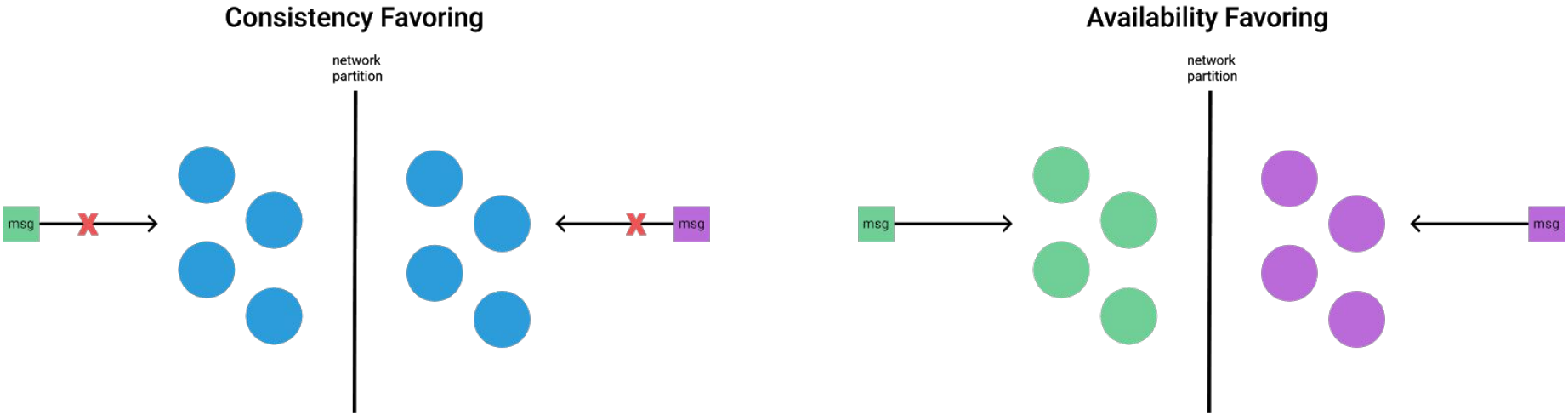
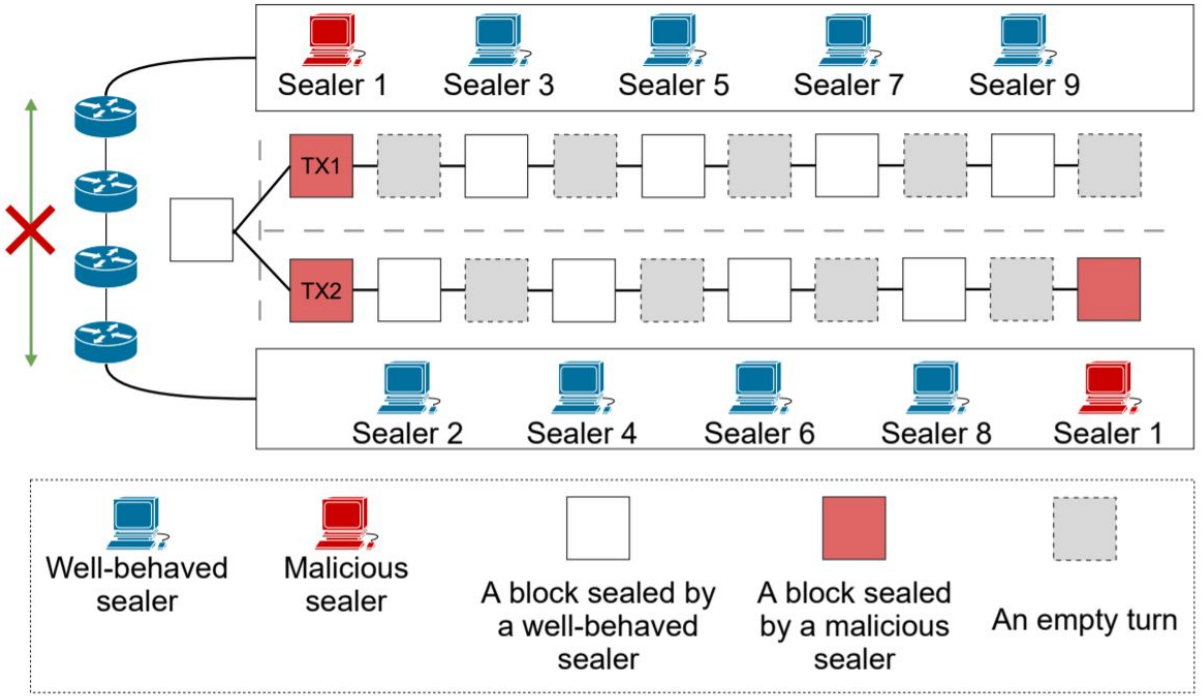


Image source: https://medium.com/mechanism-labs/finality-in-blockchain-consensus-d1f83c120a9a

Network Split & Cloning Attack



P. Ekparinya, V. Gramoli, and G. Jourjon, “The Attack of the Clones Against Proof-of-Authority,” presented at the Network and Distributed System Security Symposium, San Diego, CA, 2020, doi: 10.14722/ndss.2020.24082

Parameters for Attack Success

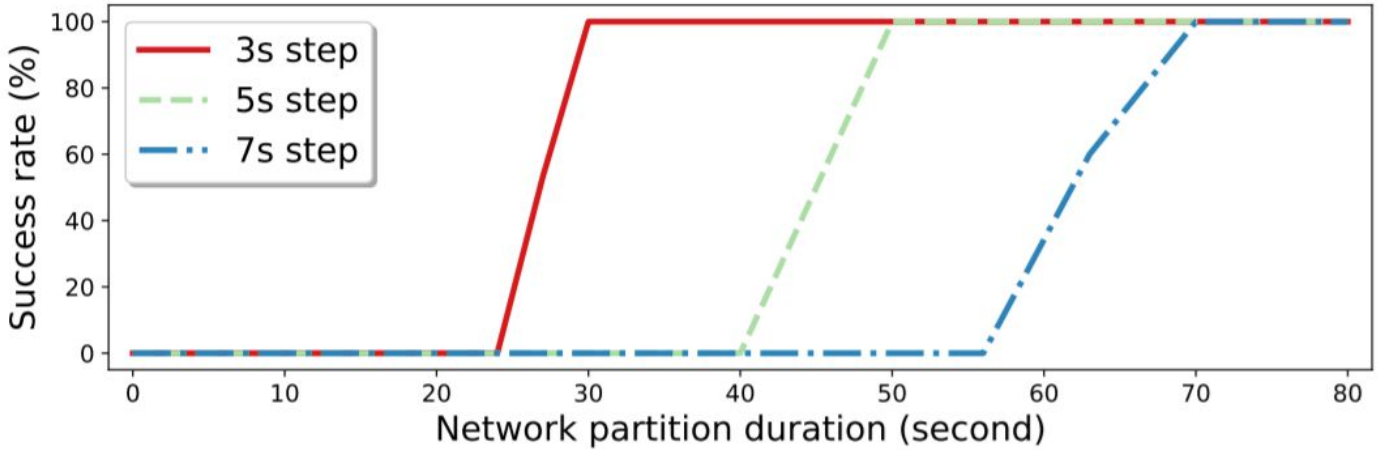
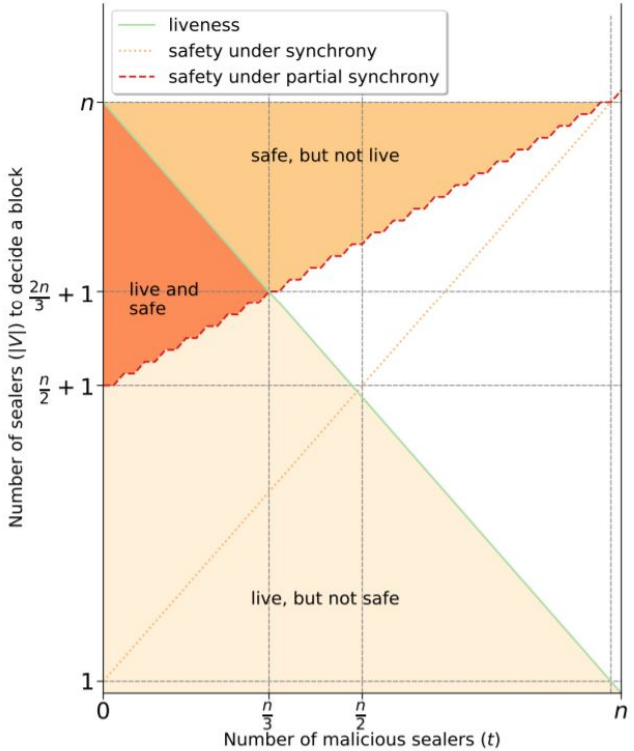


Figure 3. The success rate of double spending with the Cloning Attack in Aura

P. Ekparinya, V. Gramoli, and G. Jourjon, “The Attack of the Clones Against Proof-of-Authority,” presented at the Network and Distributed System Security Symposium, San Diego, CA, 2020, doi: 10.14722/ndss.2020.24082

Mitigations

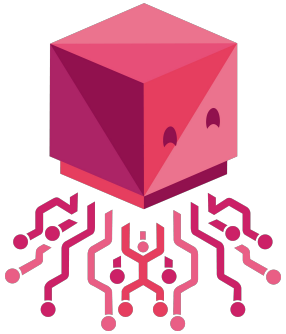


P. Ekparinya, V. Gramoli, and G. Jourjon, “The Attack of the Clones Against Proof-of-Authority,” presented at the Network and Distributed System Security Symposium, San Diego, CA, 2020, doi: 10.14722/ndss.2020.24082


DISTRIBUTED SYSTEMS
HOW HARD CAN IT BE?

Cloning Attack

On Proof-of-Authority Ethereum Blockchains



BLOCKCHAIN
REALLABOR
RHEINISCHES REVIER