Bitcoin-Enhanced Proof-of-Stake Security: Possibilities and Impossibilities

최원재
wonjae@snu.ac.kr
2025. 01. 23

Virtual Machine & Optimization Laboratory
Dept. of Electrical and Computer Engineering
Seoul National University

Two Papers From Babylon

IEEE S&P '23

Bitcoin-Enhanced Proof-of-Stake Security: Possibilities and Impossibilities

Ertem Nusret Tas
Stanford University
nusret@stanford.edu

David Tse
Stanford University
dntse@stanford.edu

Fangyu Gai
BabylonChain
fangyu.gai@babylonchain.io

Sreeram Kannan
University of Washington, Seattle
ksreeram@uw.edu

Mohammad Ali Maddah-Ali
University of Minnesota
maddah.ali.ee@gmail.com

Fisher Yu
BabylonChain
fisher.yu@babylonchain.io

ACM CCS '23

Interchain Timestamping for Mesh Security

Ertem Nusret Tas
Stanford University
nusret@stanford.edu

Runchao Han
BabylonChain
runchao.han@babylonchain.io

David Tse
Stanford University
dntse@stanford.edu

Fisher Yu
BabylonChain
fisher.yu@babylonchain.io

Kamilla Nazirkhanova
Stanford University
nazirk@stanford.edu

Bitcoin-Enhanced Proof-of-Stake Security: Possibilities and Impossibilities

Ertem Nusret Tas
Stanford University
nusret@stanford.edu

David Tse
Stanford University
dntse@stanford.edu

Fangyu Gai
BabylonChain
fangyu.gai@babylonchain.io

Sreeram Kannan
University of Washington, Seattle
ksreeram@uw.edu

Mohammad Ali Maddah-Ali
University of Minnesota
maddah.ali.ee@gmail.com

Fisher Yu
BabylonChain
fisher.yu@babylonchain.io

PoW → PoS

Less Energy

Faster Confirmation

More Accountability

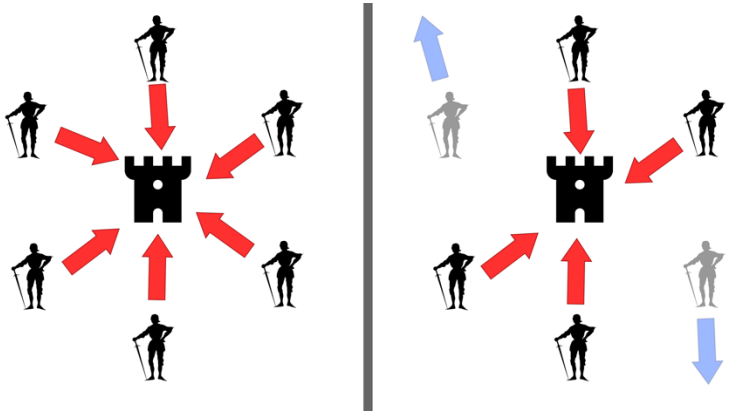
Accountable Safety

Definition

- If there is a safety violation, 1/3 adversarial validators can be *provably* identified as protocol violators.

Byzantine Fault Tolerance (BFT)

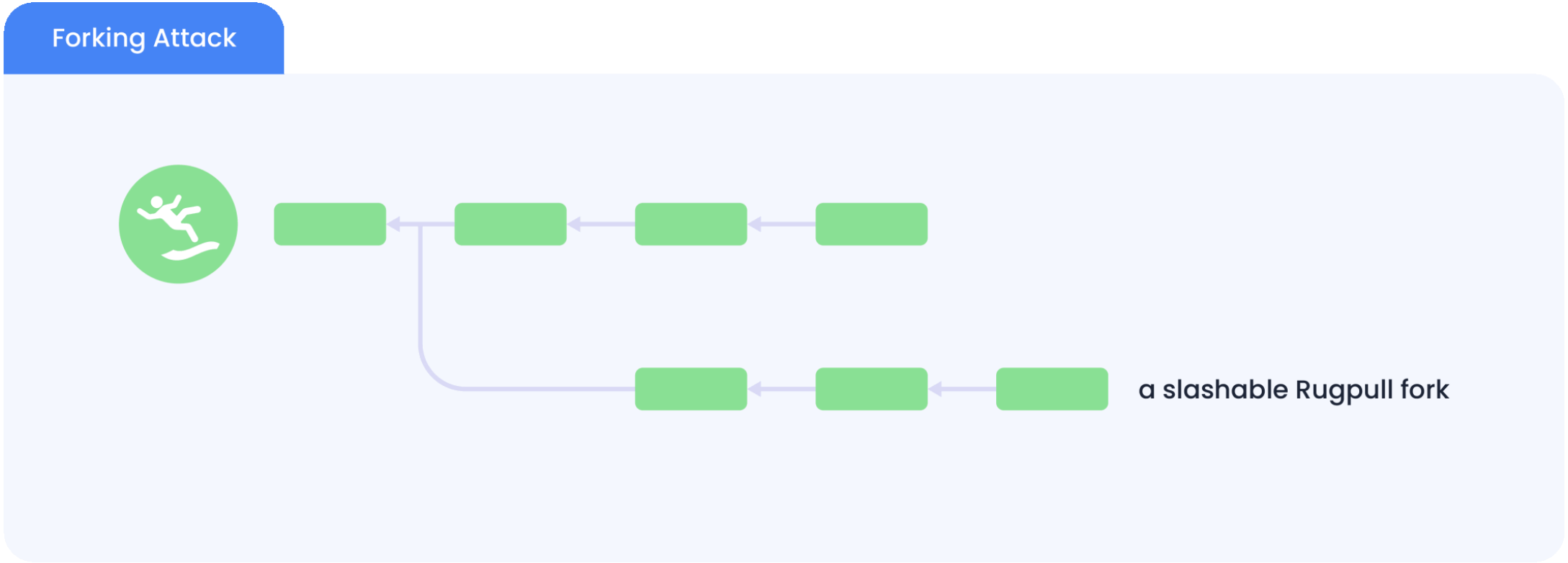
- Protocol is safe unless more than 1/3 of validators are adversary.
- Therefore, Accountable Safety implies BFT. (i.e. stronger safety)



Accountable Safety – How it works?

How to get Accountability

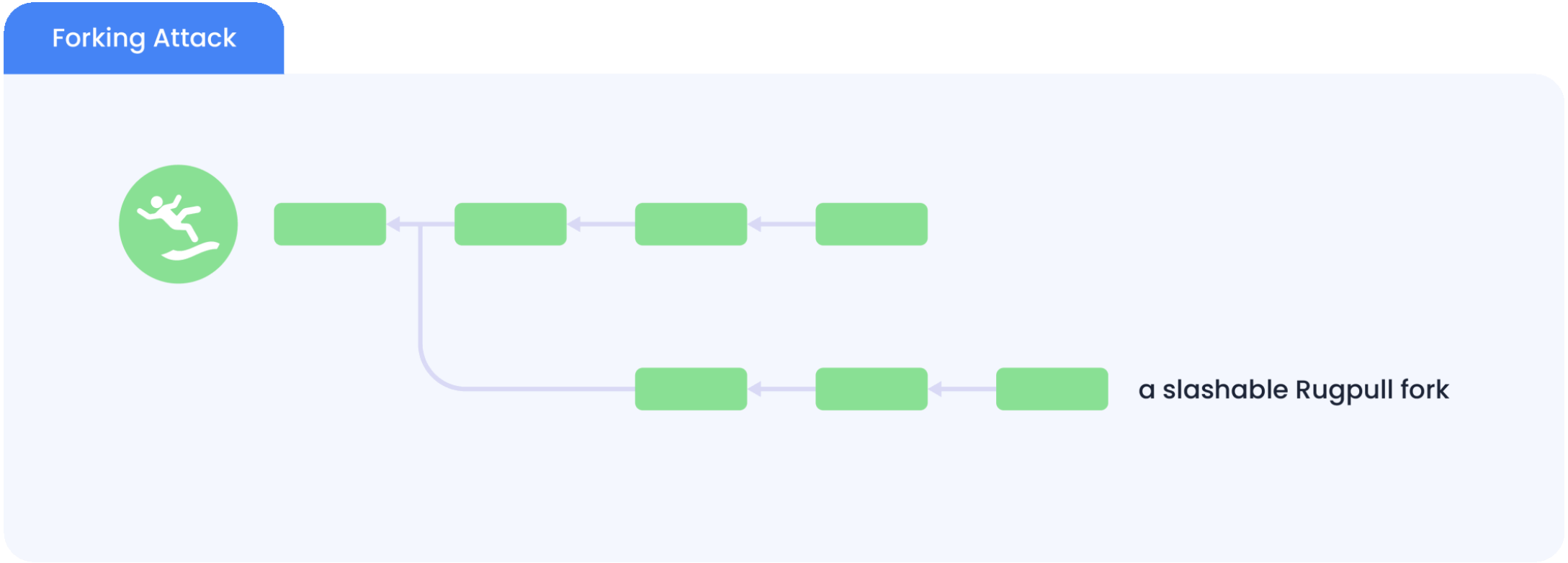
- Normal clients can compare two blocks and inspect the violators.



Accountable Safety – Why it matters?

Goal

- To impose economic punishment to the violators (Slashing)
- To provide Economic Security



Slashable Safety

Accountable Safety is not enough for PoS

- Violators can withdraw their stake before identified by the protocol.

Defintion

- If there is a safety violation, 1/3 adversarial validators can be provably identified as protocol violators before they withdraw their stake (i.e. unbond).
- Provides economic security for PoS blockchains.

Current Blockchains

- Many PoS protocols have accountable safety (e.g. Tendermint, Ethereum PoS)
- But no PoS protocol can have slashable safety without external trust.

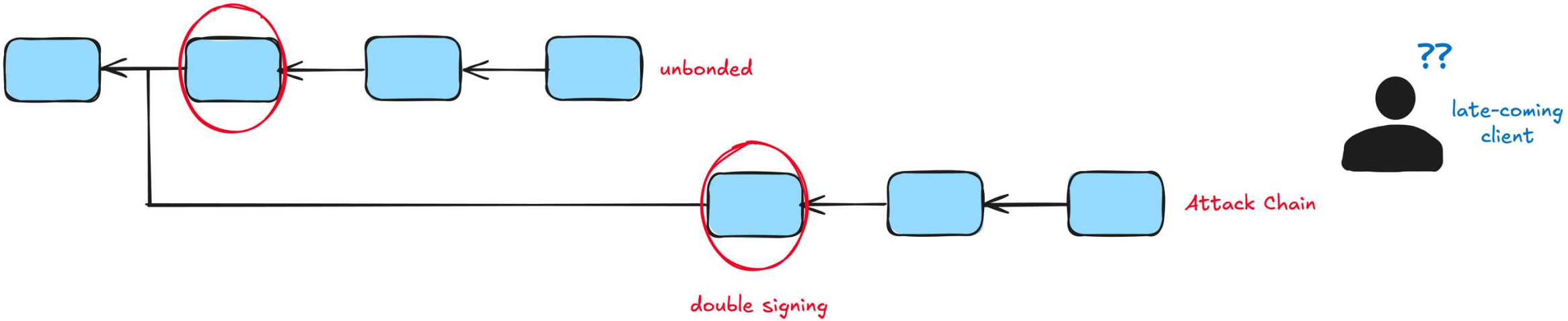
No Slashability: Posterior Corruption Attack

Problem Scenario

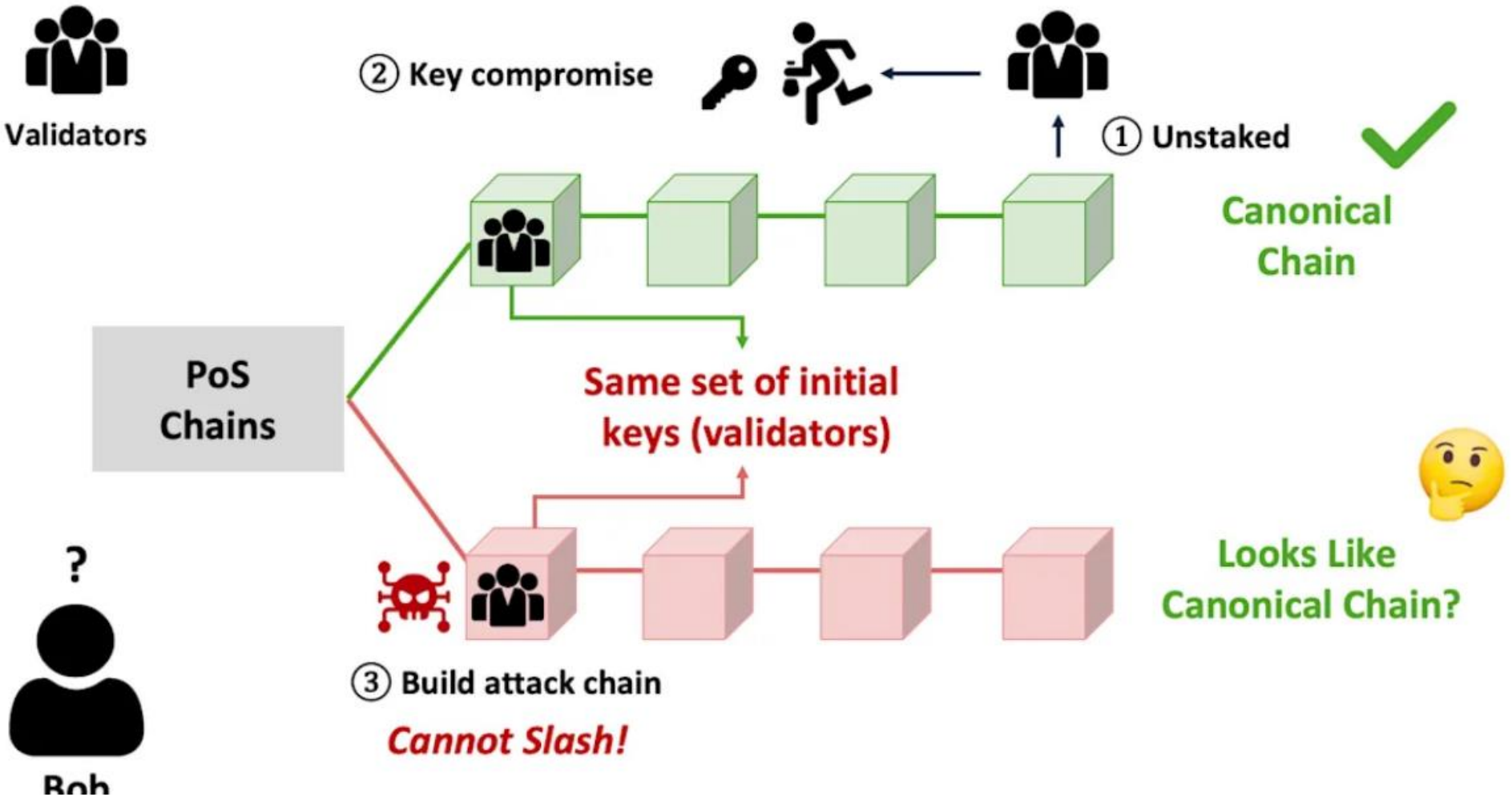
- Attackers wait until they unbond their stakes.
- They publish the attack chain after they unbonded their stakes.

Issues

- Existing clients can reject the late chain.
- But, the late-coming clients cannot distinguish the attack chain.



Example: Long Range Attack



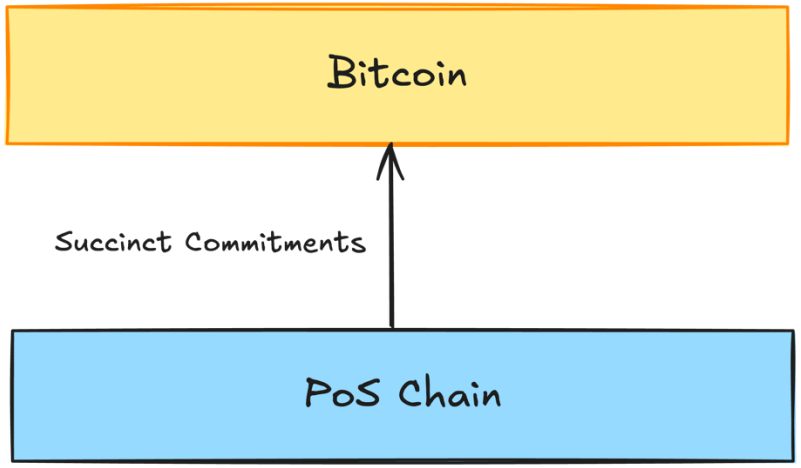
Bitcoin as a Timestamping Server

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

"In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions."

Babylon Protocol

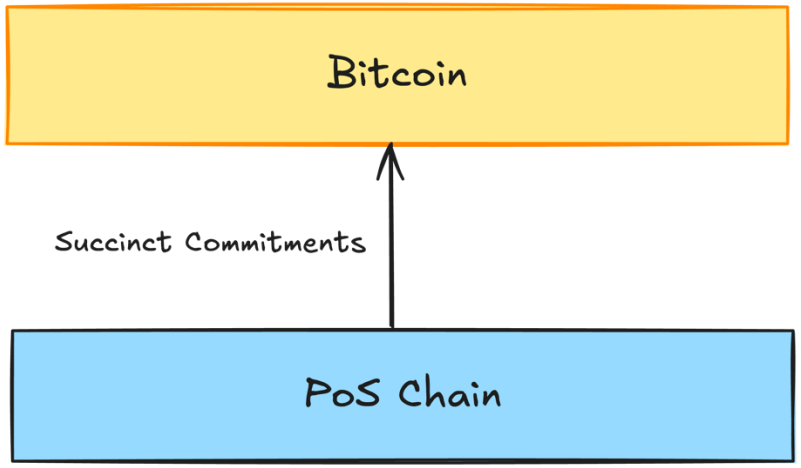


Babylon Protocol provides

- Slashable Safety with resilience of 1/3
- Liveness with resilience of 1/2

Babylon Protocol is optimal for PoS chains given a data-limited timestamping server.

Babylon Protocol



Babylon Protocol provides

- Slashable Safety with resilience of 1/3
- Liveness with resilience of 1/2

Babylon Protocol is optimal for PoS chains given a data-limited timestamping server.

Babylon Protocol vs Stand-alone PoS Chain

Babylon Protocol

- Slashable Safety with resilience of 1/3
- Liveness with resilience of 1/2

An optimal **stand-alone** PoS chain

- Accountable Safety with resilience of 1/3
- Liveness with resilience of 1/3

(Sheng et al. 2021)

How?