# BLUEHAT

IL 2022

# A primer on cross-chain bridges and how to break one

Niv Yehezkel

# Whoami:

- Security researcher
- Pasten CTF team member
- Working on a new web3 security startup

# Once upon a time…

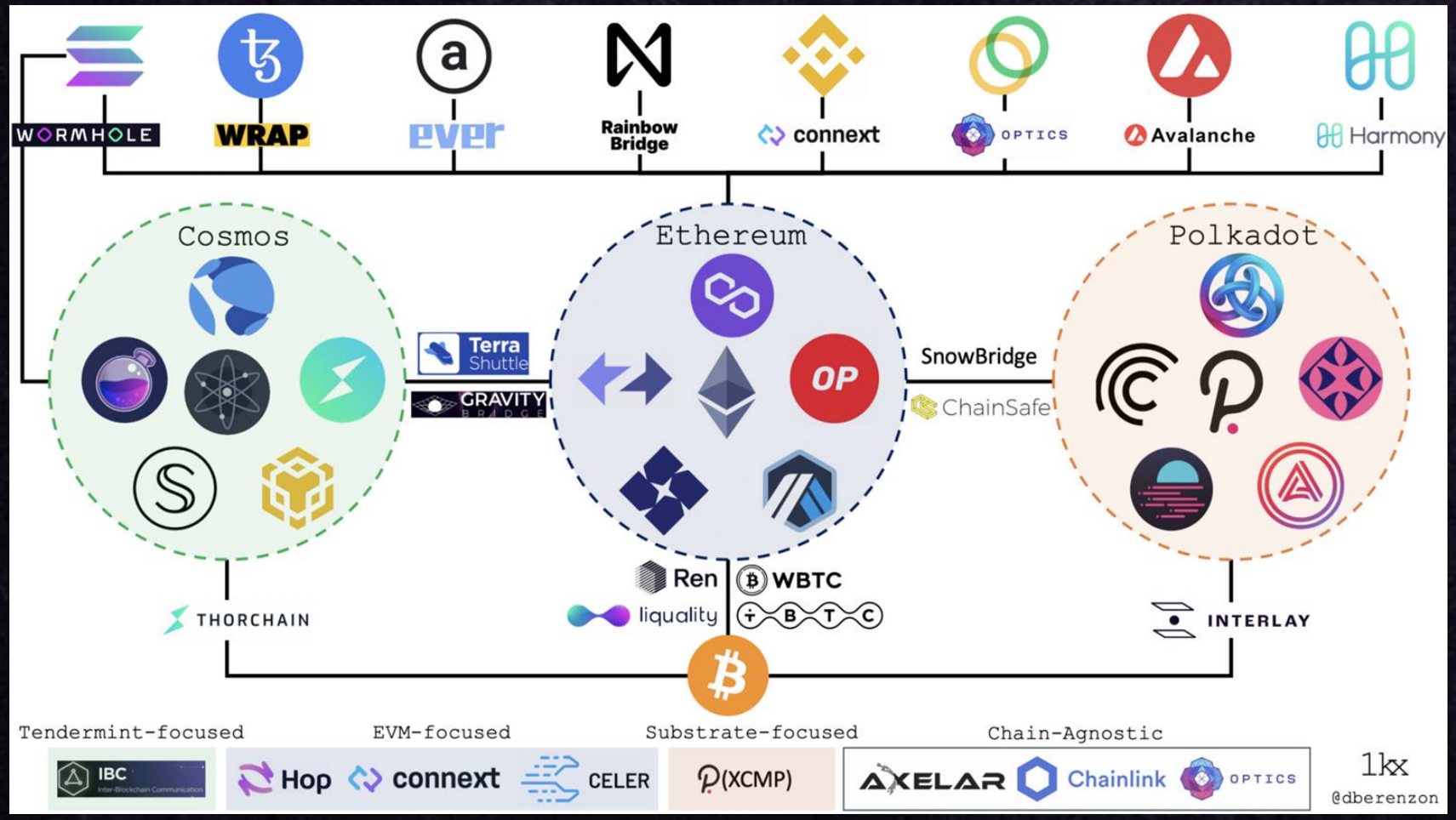
there was a single decentralized blockchain

# 6 years later…

A new general-purpose blockchain called Ethereum came to life

# Fast forward to today -

A multi-chain present and future



# What about cross-chain?

Blockchains are great but cannot trustlessly interact with each other

**vitalik.eth**
@VitalikButerin

My argument for why the future will be *multi-chain*, but it will not be *cross-chain*: there are fundamental

* Recommended reading: https://twitter.com/VitalikButerin/status/1479501366192132099

# Why even bother?

Interoperability

User Experience and Capital Efficiency

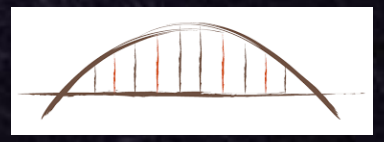
# Bridges to the rescue!

# How it works - lock, mint, burn and release

Chain A → Chain B

Chain A

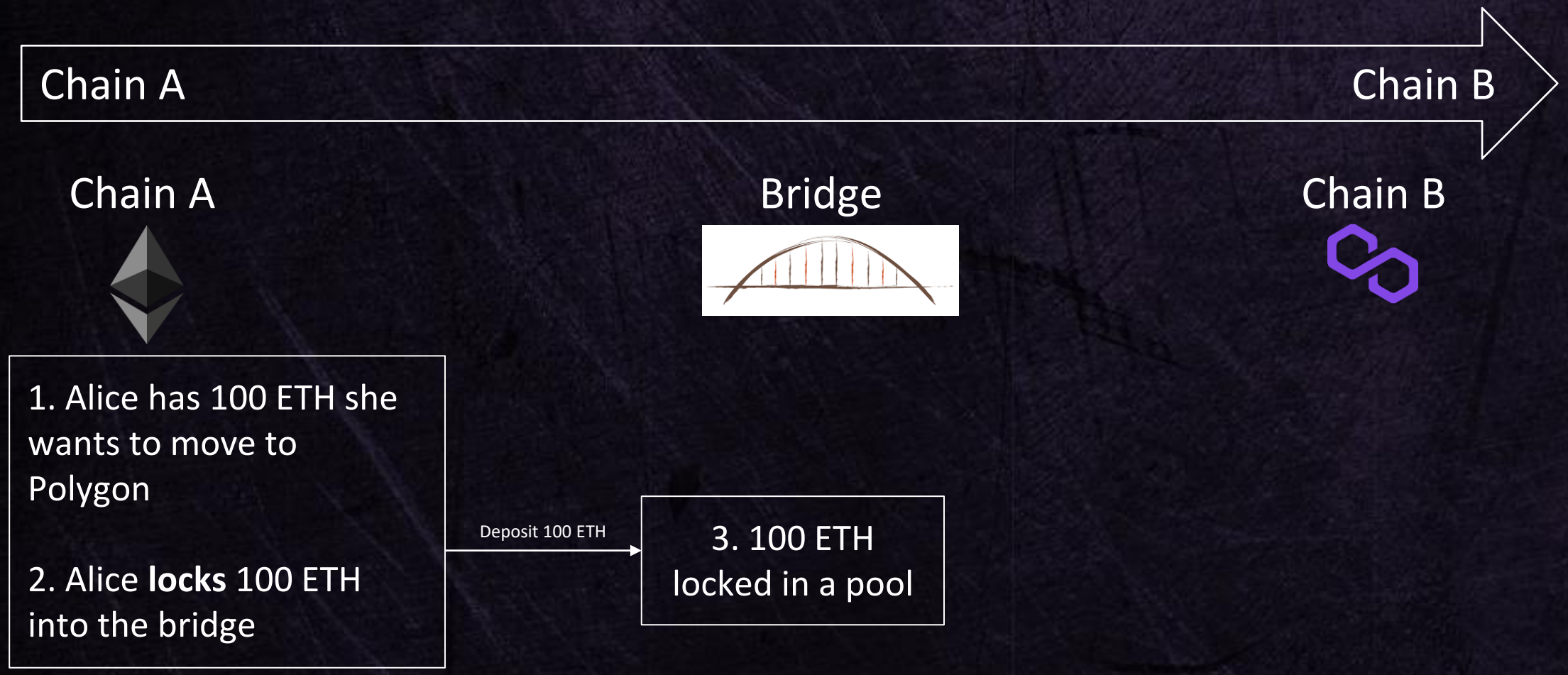
Bridge



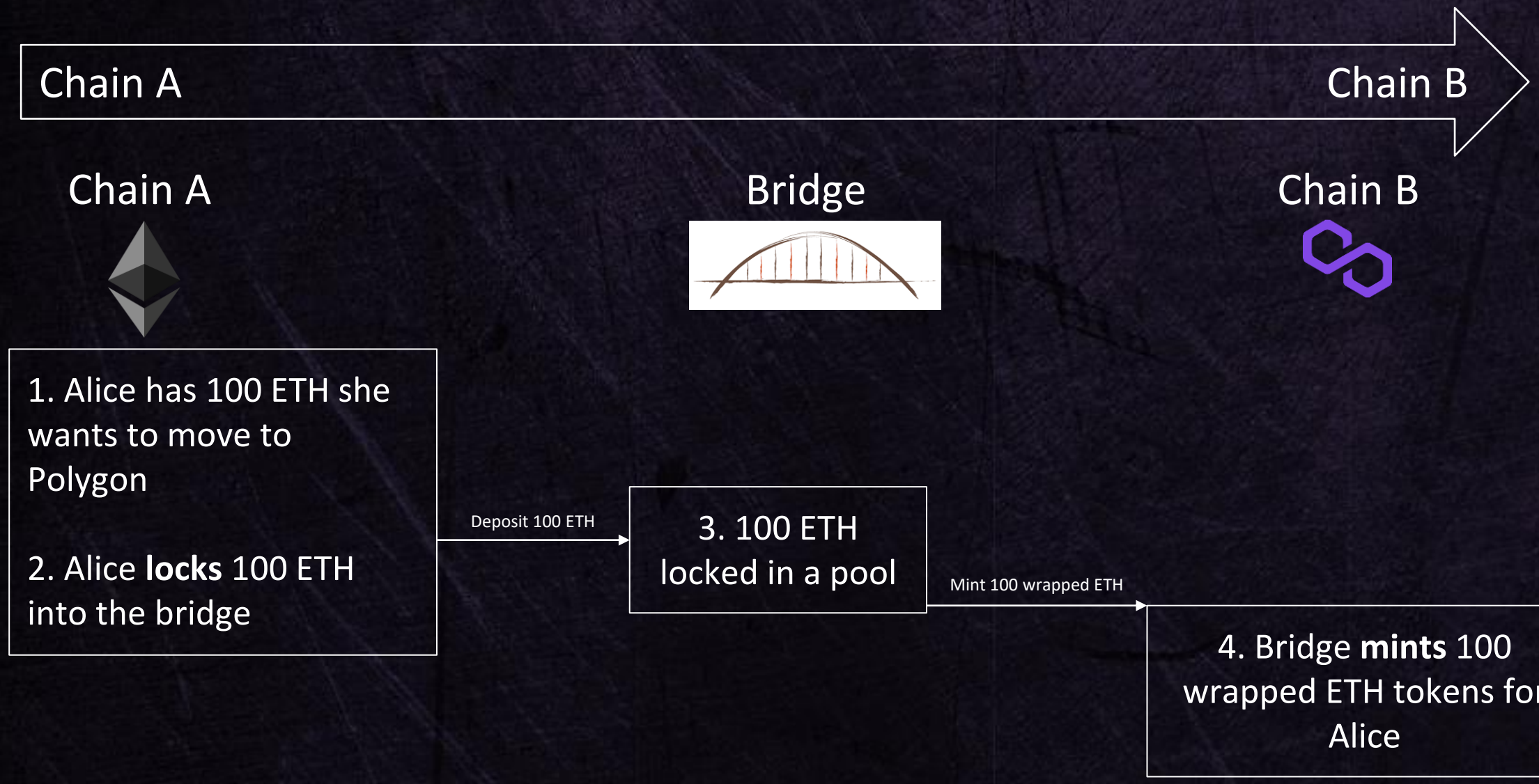
Chain B

1. Alice has 100 ETH she wants to move to Polygon

# How it works - lock, mint, burn and release



# How it works - lock, mint, burn and release



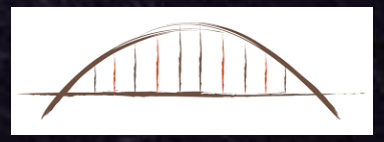
# How it works - lock, mint, burn and release

Chain A

Chain B

Chain A

Bridge



Chain B

1. Alice has 100 wrapped ETH tokens she wants to move back to chain A

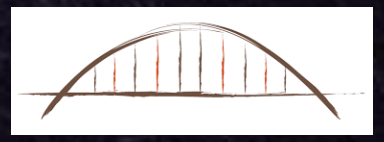
# How it works - lock, mint, burn and release

Chain A

Chain B

Chain A

Bridge



Chain B

1. Alice has 100 wrapped ETH tokens she wants to move back to chain A

2. Alice **burns** her 100 wrapped ETH tokens

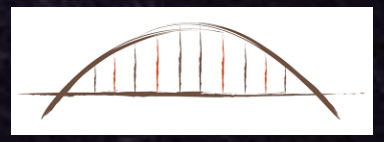
# How it works - lock, mint, burn and release

Chain A

Chain B

Chain A

Bridge



Chain B

1. Alice has 100 wrapped ETH tokens she wants to move back to chain A

2. Alice **burns** her 100 wrapped ETH tokens

3. Bridge sees alice burned her tokens and **releases** ETH from the pool on chain A

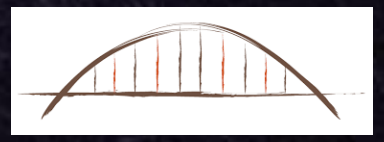
# How it works - lock, mint, burn and release

Chain A

Chain B

Chain A

Bridge



Chain B

1. Alice has 100 wrapped ETH tokens she wants to move back to chain A

2. Alice **burns** her 100 wrapped ETH tokens

3. Bridge sees alice burned her tokens and **releases** ETH from the pool on chain A

Release 100 ETH

4. Alice gets 100 ETH

# Bridges are cool

So how can we break them?
Starting with the Polygon PoS bridge

# The Polygon chain

- Powered by Proof of Stake
- Polygon chain has so-called validator nodes powering it
- Validators stake tokens, mine new blocks in the chain and get rewarded for it

# Polygon PoS bridge

- Bridges tokens to and from Ethereum to Polygon
- The bridge is composed by a set of contracts that are deployed on Ethereum and Polygon

- Moving assets from Ethereum to Polygon
  - **Lock** assets into **Ethereum** PoS bridge contracts
  - Validator nodes monitor Ethereum contracts logs
  - Wrapped assets are **minted** on **Polygon**

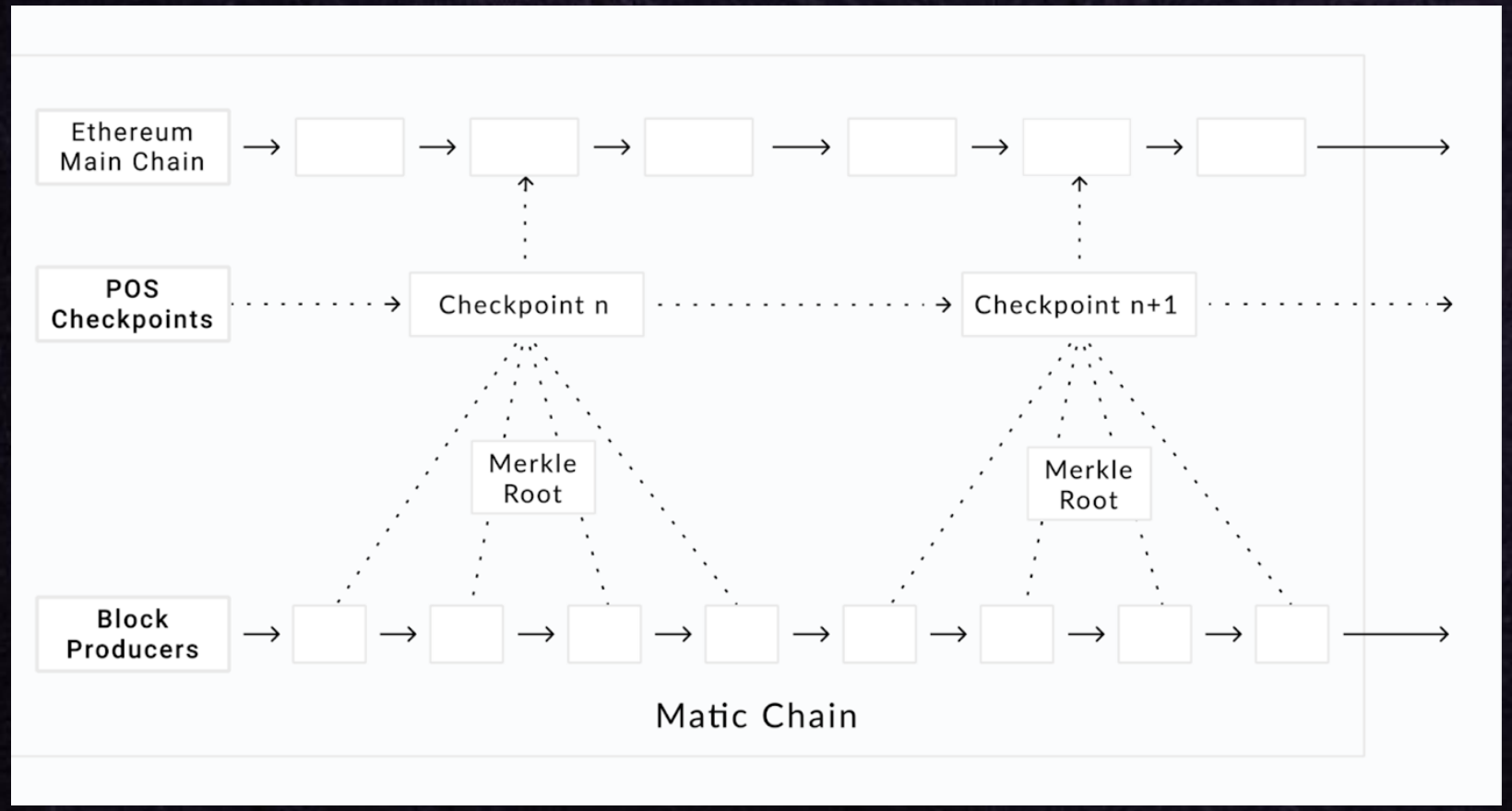
# Polygon PoS bridge - cont.

- Withdrawing wrapped assets from Polygon back to Ethereum
  - **Burn** the asset on **Polygon**
  - Save the tx hash
  - Wait for a *checkpoint* to be sent to Ethereum
  - Submit a proof of the burn on **Ethereum** to **release** the asset

- How can the contracts on Ethereum trust the proof of something that happened on Polygon? What's even a checkpoint?

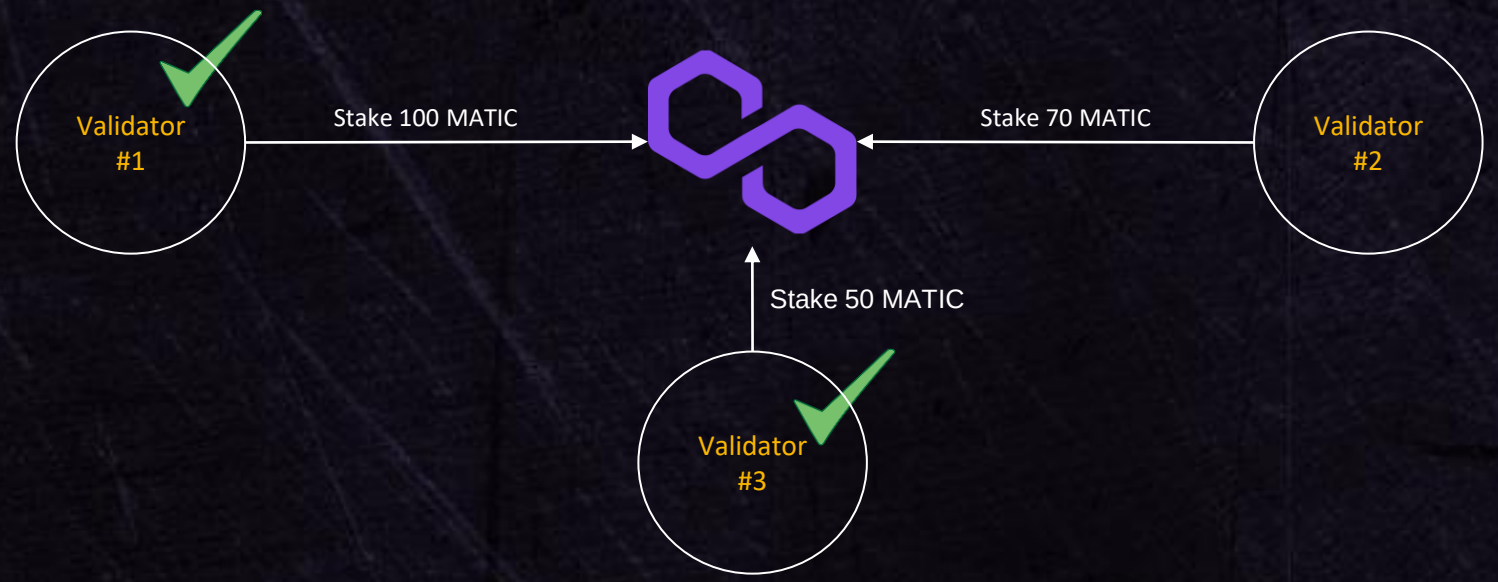
# Checkpointing

Checkpointing is the process of merging the Polygon transactions into the Ethereum blockchain



# Why consensus matters

- Checkpoints are accepted only if ⅔ + 1 of the total staking power of the validators signed the checkpoint
- Checkpoints are then used to verify proofs of burnt tokens in Polygon
- **A malicious checkpoint can drain the pool of the bridge**




Total staking power: 220

⅔ * 220 + 1 = 148 for a checkpoint to be accepted

# How does staking work?

- There are currently 100 validator nodes on Polygon
- Running a validator node is a hassle
- Fortunately anyone can delegate any amount of tokens into any validator node
- Example:

Total staking power: 100

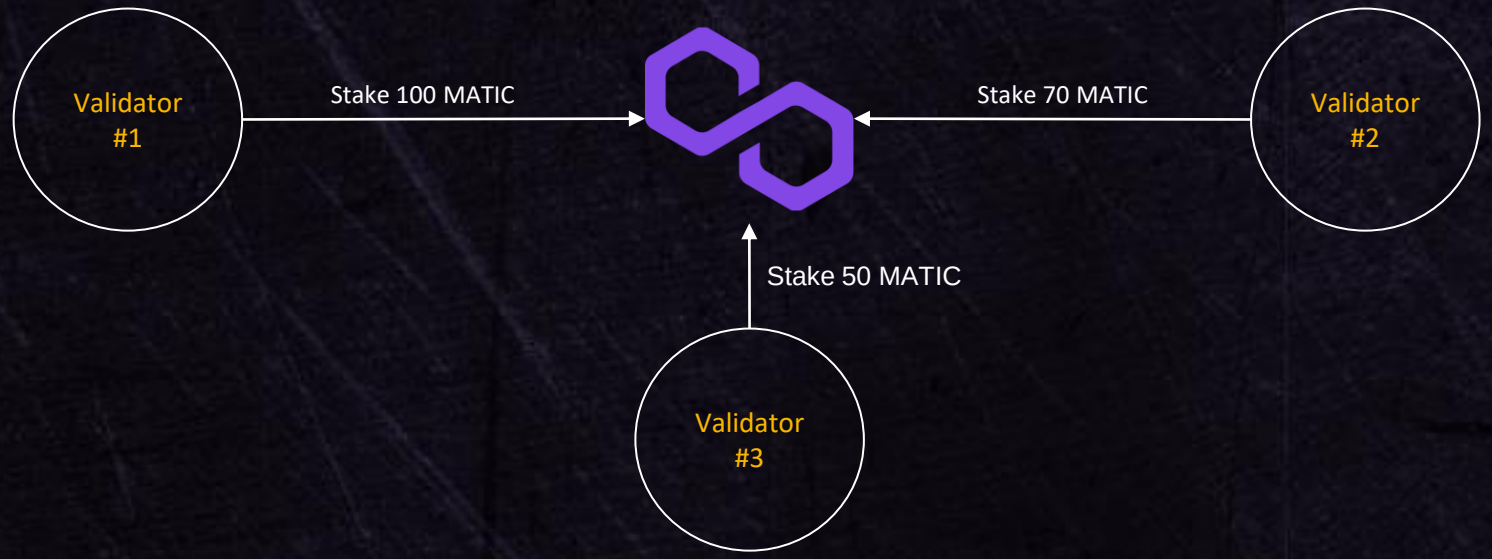
# How does staking work?

- There are currently 100 validator nodes on Polygon
- Running a validator node is a hassle
- Fortunately anyone can delegate any amount of tokens into any validator node
- Example:

Total staking power: 170

# How does staking work?

- There are currently 100 validator nodes on Polygon
- Running a validator node is a hassle
- Fortunately anyone can delegate any amount of tokens into any validator node
- Example:

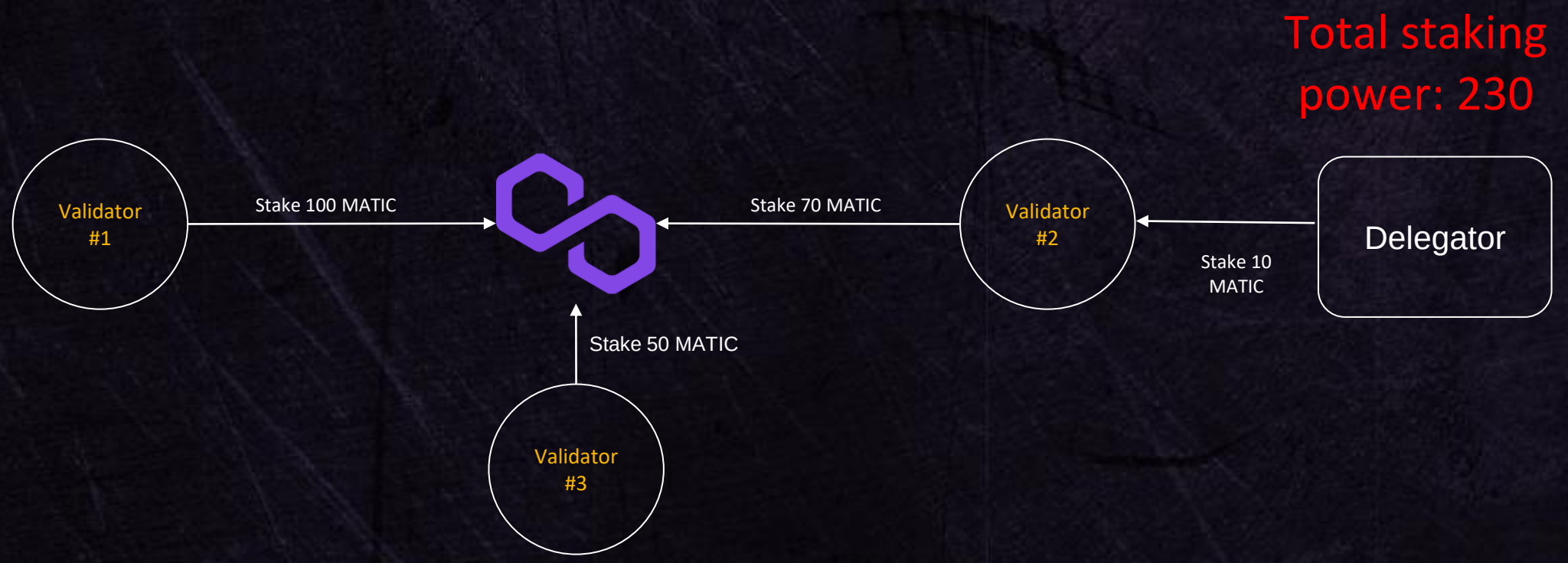



Total staking power: 220

To accept a new checkpoint submission - signed staking power on that submission has to be at least:
⅔*220 + 1 = 148

# How does staking work?

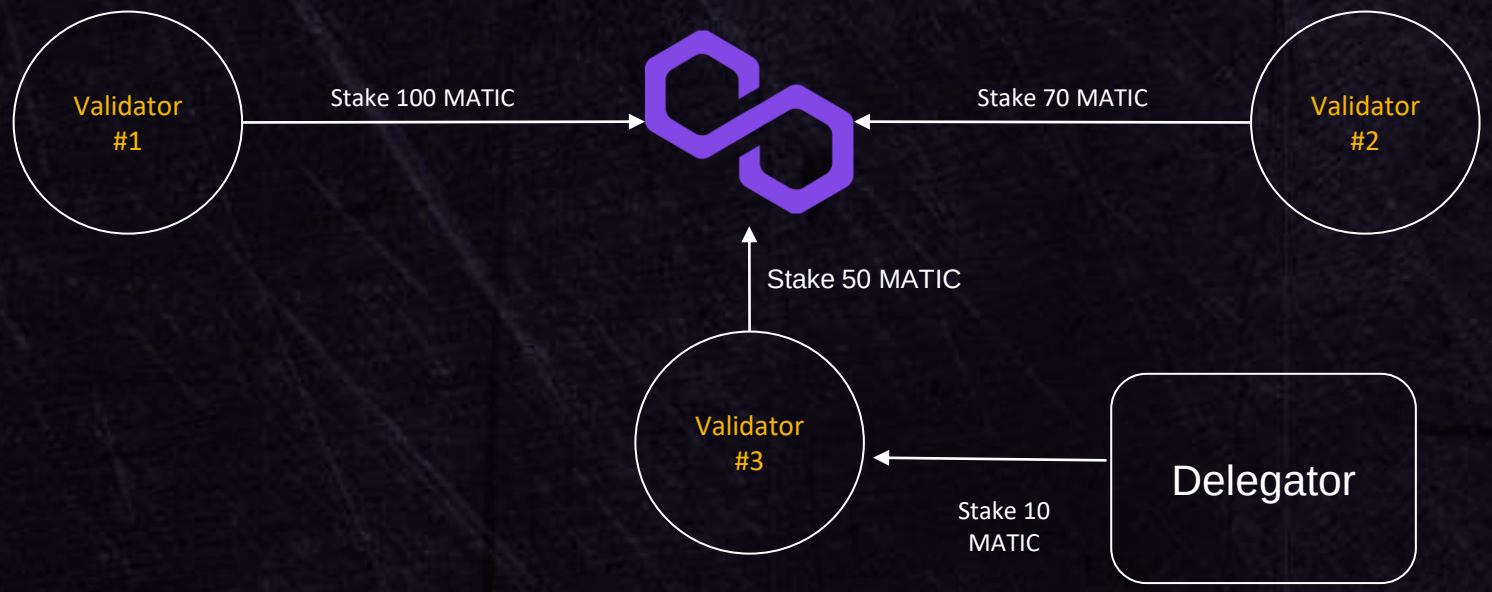
- There are currently 100 validator nodes on Polygon
- Running a validator node is a hassle
- Fortunately anyone can delegate any amount of tokens into any validator node
- Example:



# Migrating delegator tokens

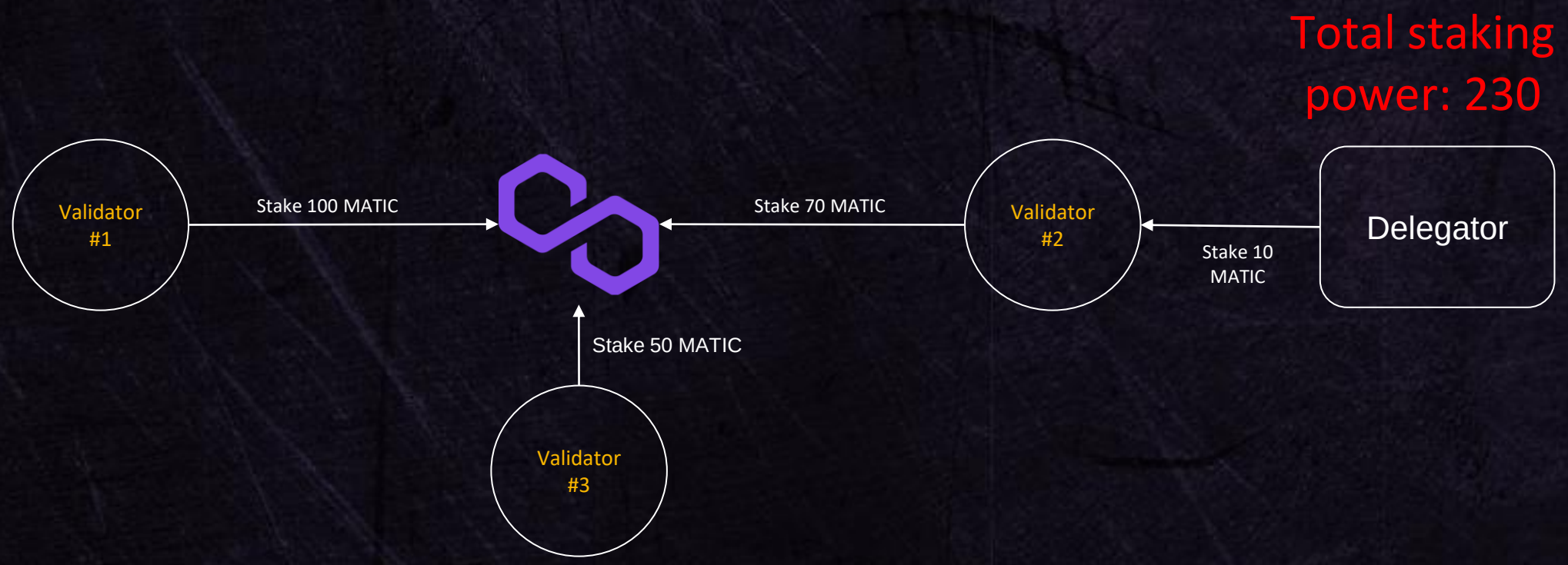
- A delegator can also migrate from one validator to another if he desires without needing to pull his tokens out
- Example:

Total staking power: 230



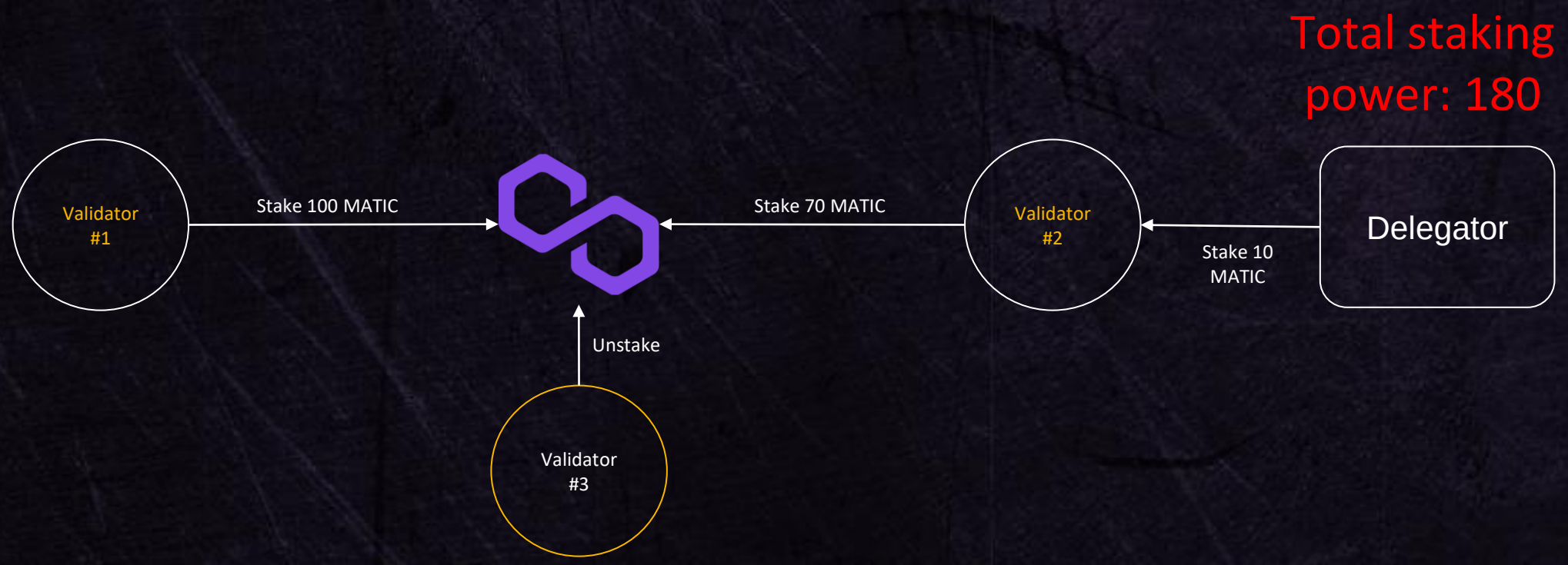
# How does unstaking work?

- Validators can unstake when they want to
- Total staking power counter has to decrease accordingly
- Example:



# How does unstaking work?

- Validators can unstake when they want to
- Total staking power counter has to decrease accordingly
- Example:



# One counter to rule them all

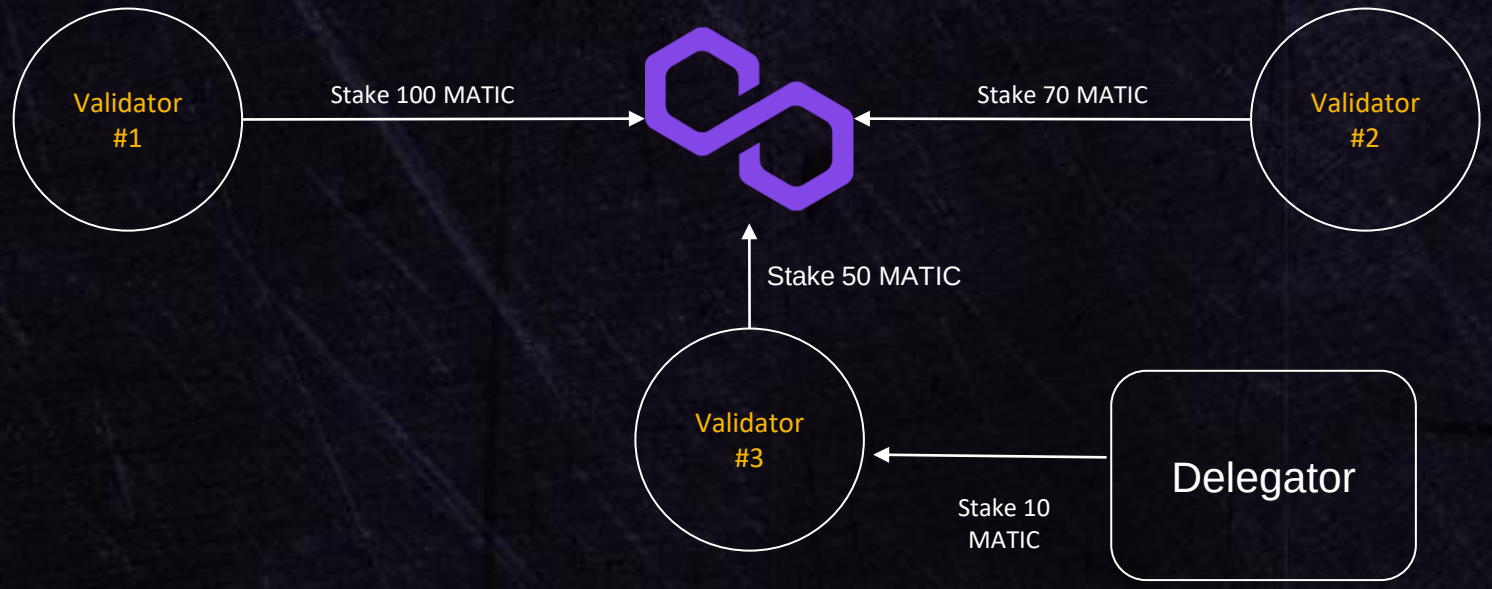
- The total staking power counter is a very important number
- Recap: A checkpoint can be accepted only if >= ⅔ * total staking power + 1 staking power has signed it

**What if we could bypass that consensus check somehow?**

# Breaking the bridge

- Validators can unstake when they want to
- Delegators can migrate when they want to
- Example:

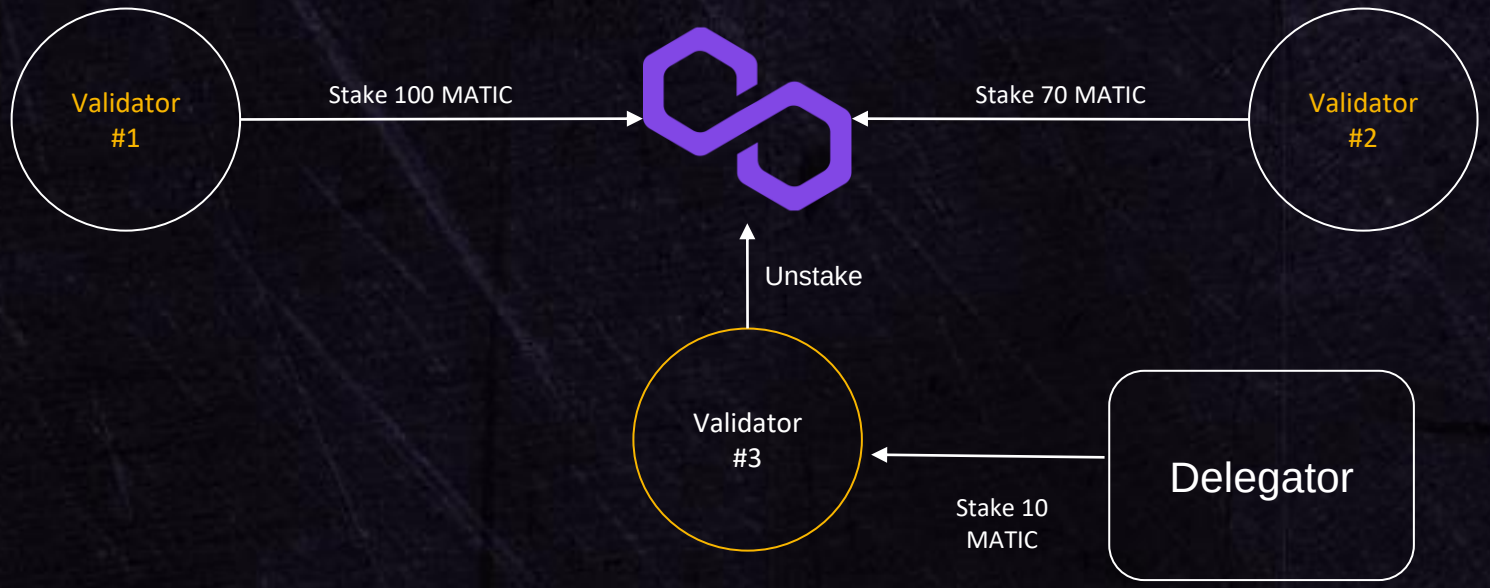
Total staking power: 230



# Breaking the bridge

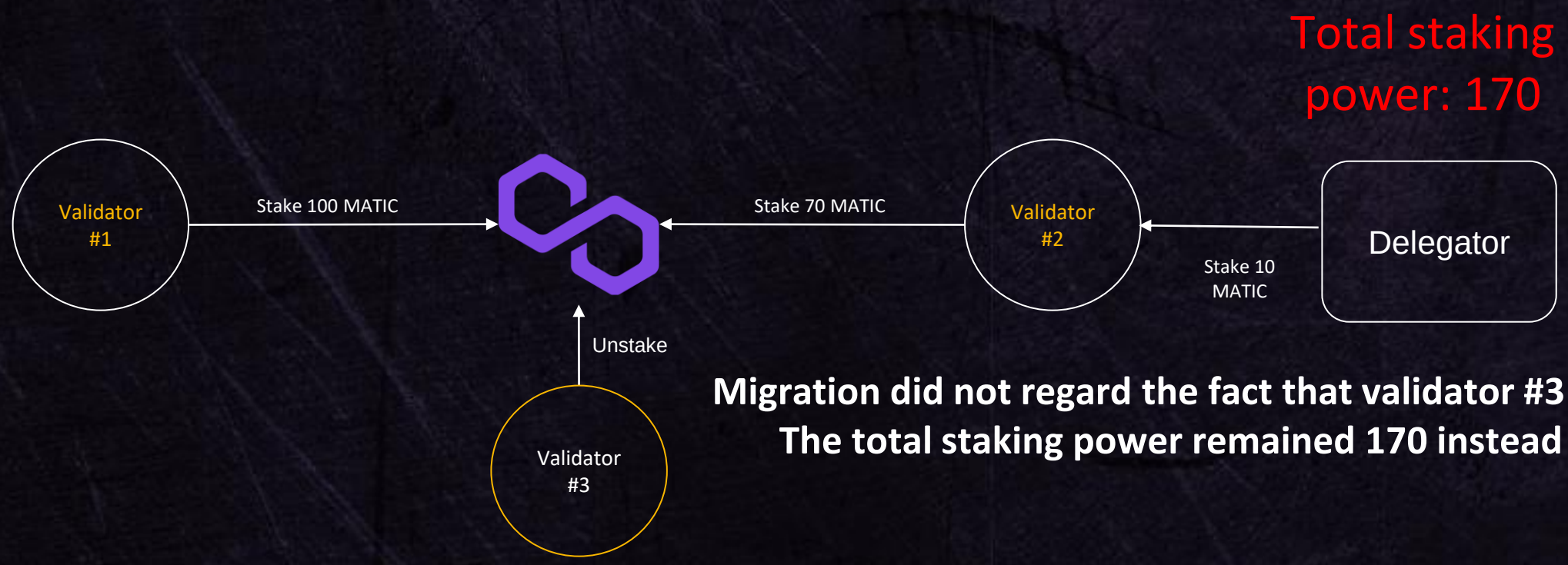
- Validators can unstake when they want to
- Delegators can migrate when they want to
- Example:

Total staking power: 170



# Breaking the bridge

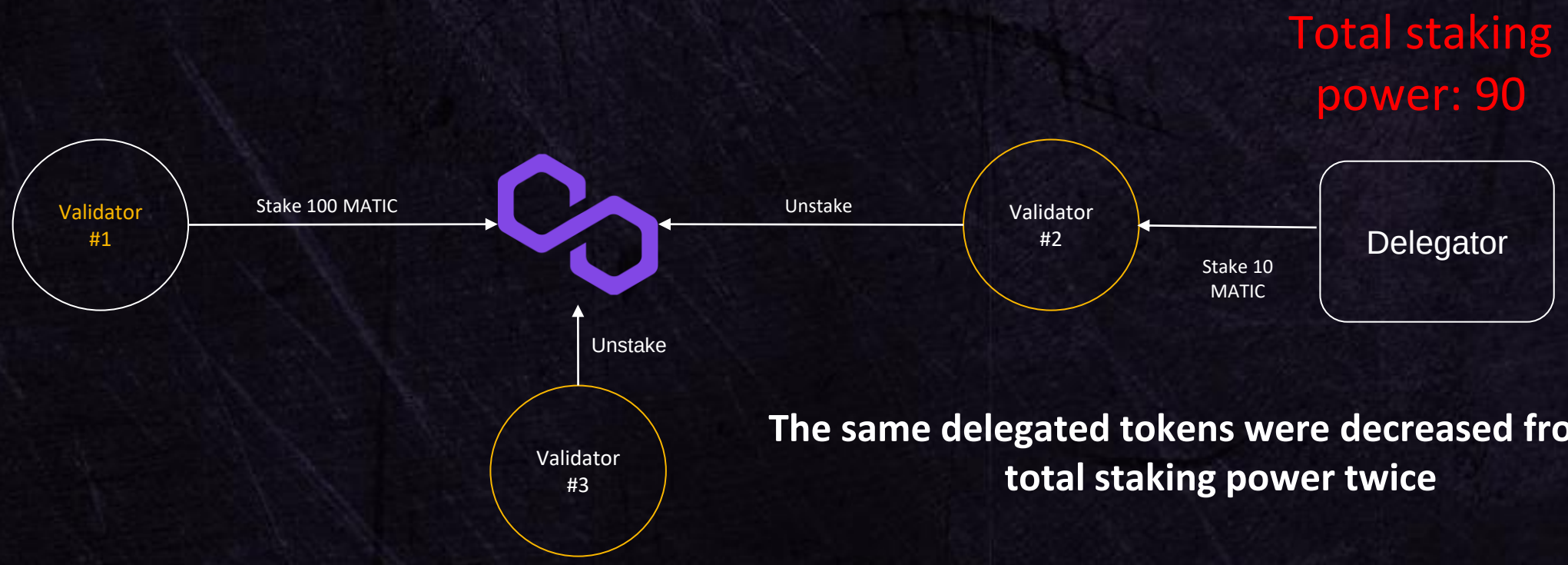
- Validators can unstake when they want to
- Delegators can migrate when they want to
- Example:




**Migration did not regard the fact that validator #3 unstaked!**
**The total staking power remained 170 instead of 180**

# Breaking the bridge

- Validators can unstake when they want to
- Delegators can migrate when they want to
- Example:

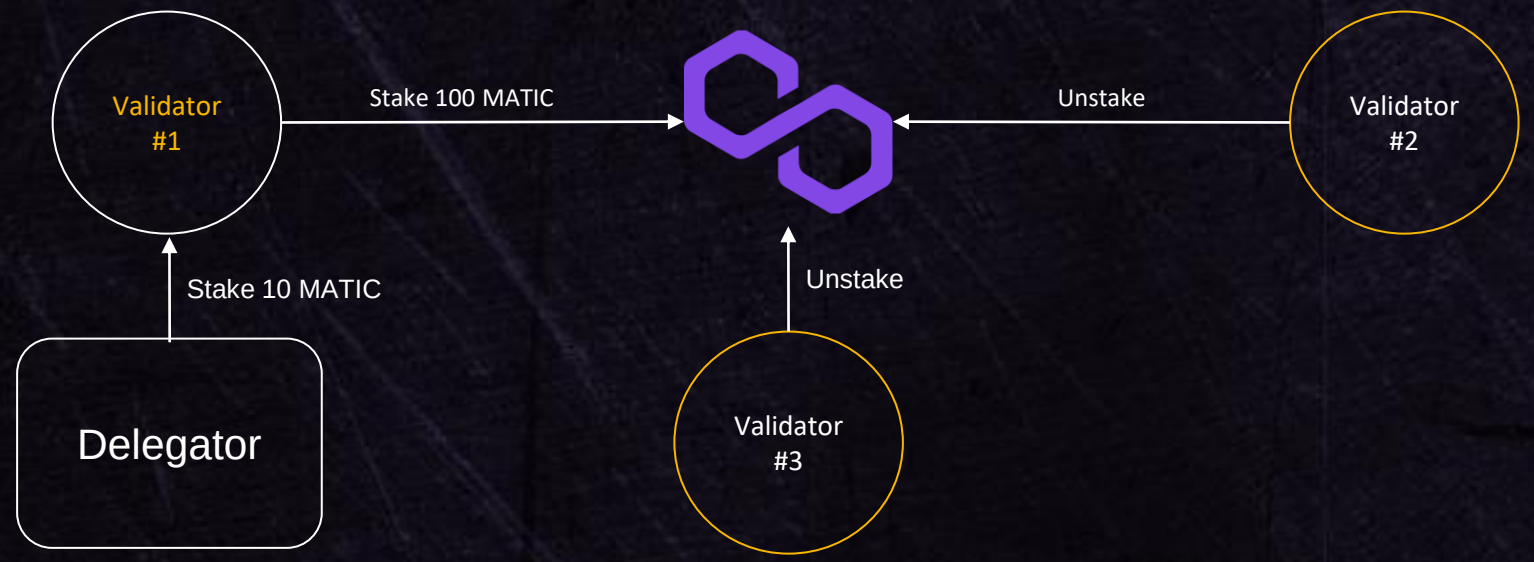



**The same delegated tokens were decreased from the total staking power twice**

# Breaking the bridge

- Validators can unstake when they want to
- Delegators can migrate when they want to
- Example:

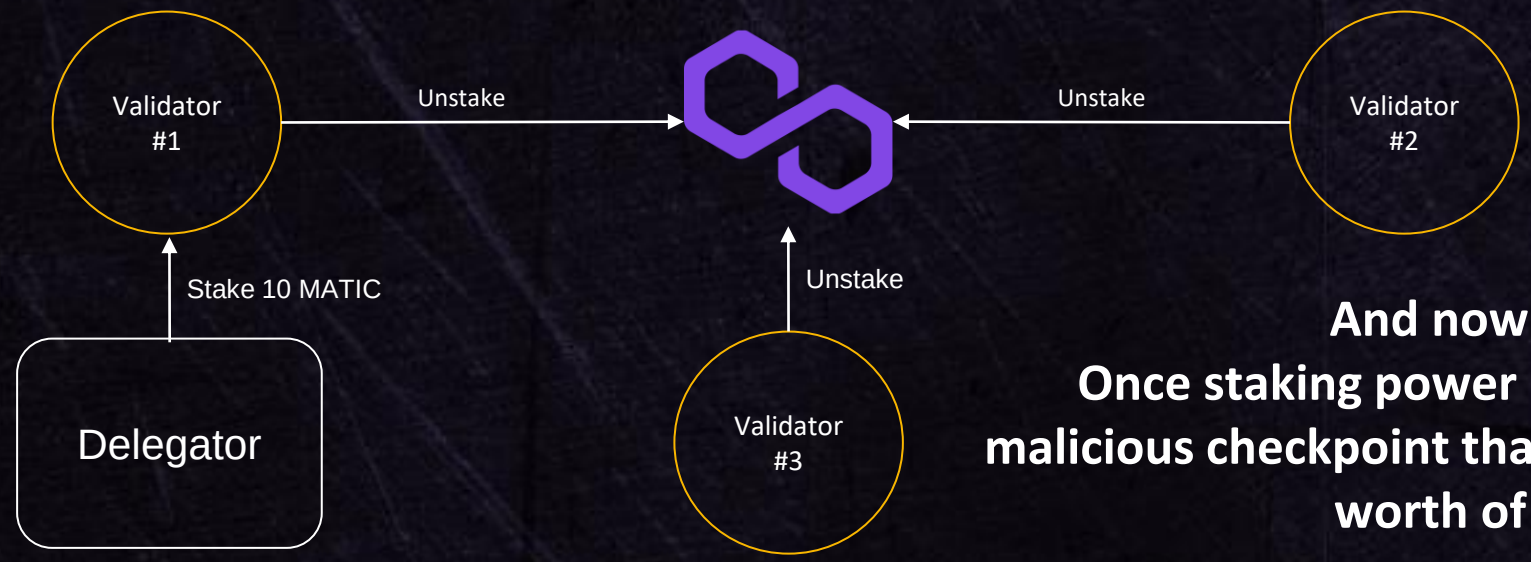
Total staking power: 90



# Breaking the bridge

- Validators can unstake when they want to
- Delegators can migrate when they want to
- Example:

Total staking power: -20




**And now for the third time.**
**Once staking power is low enough for you - send a malicious checkpoint that fakes that you burnt billions of $ worth of tokens in Polygon.**

# Draining the bridge

1. Delegate X tokens into some validator
2. Catch a validator slot
3. Migrate your X tokens into that validator
4. Unstake the validator
5. Repeat step 2 to step 4 until X >= ⅔ * total staking power + 1
6. Submit a checkpoint signed by only you that drains all deposited tokens in the bridge
7. Profit billions of dollars

# Summary

1. Bridges are complex constructs, possibly with a locked value of billions of people's funds
2. Security audits are nice and all but are insufficient
3. The industry needs more (whitehat) eyes on critical infrastructure

Thank you (: