ethereum

vienna

ethereum

Agenda

General Introduction

GridSingularity

CASPER - The friendly ghost

Socialising

ethereum

vienna

GridSingularity

ethereum

vienna

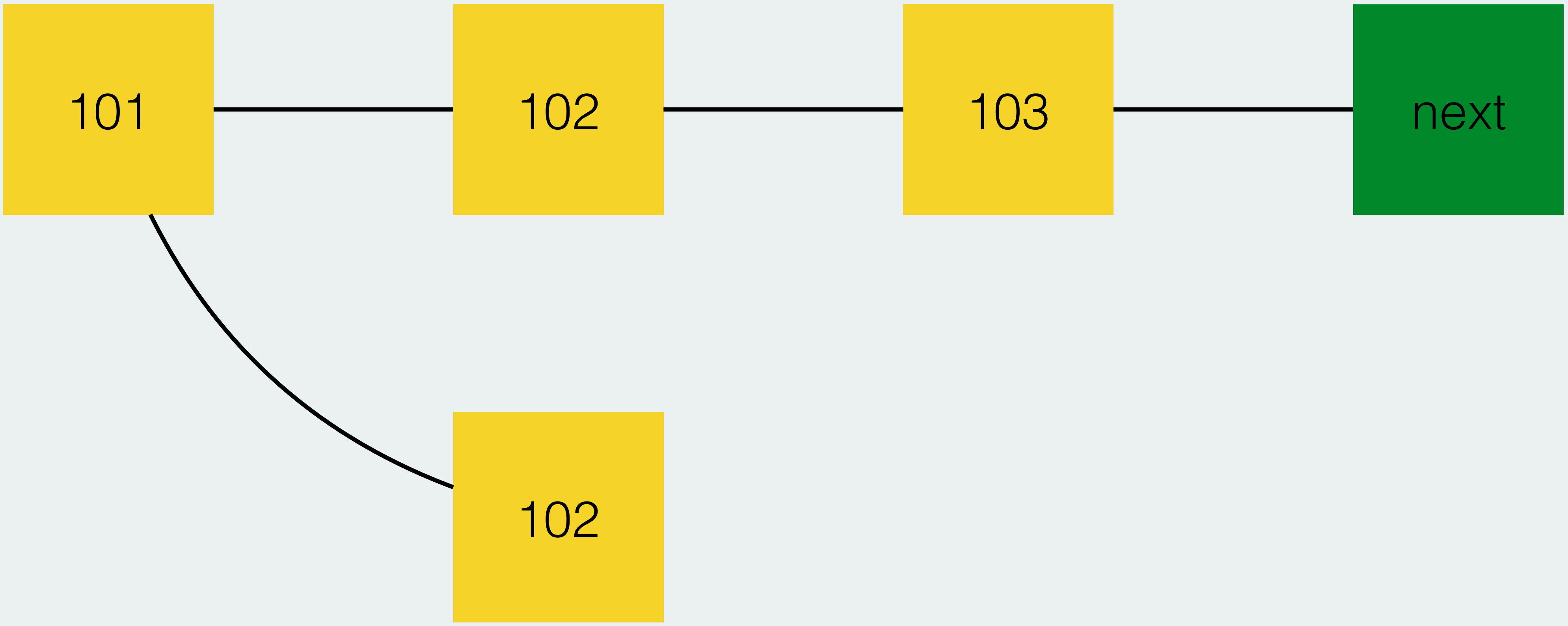
The Road to 2.0: Casper

PoS Consensus System

Proof of Work

Miner can spend hashing power on only one chain

Mining an alternate chain has cost and no profits

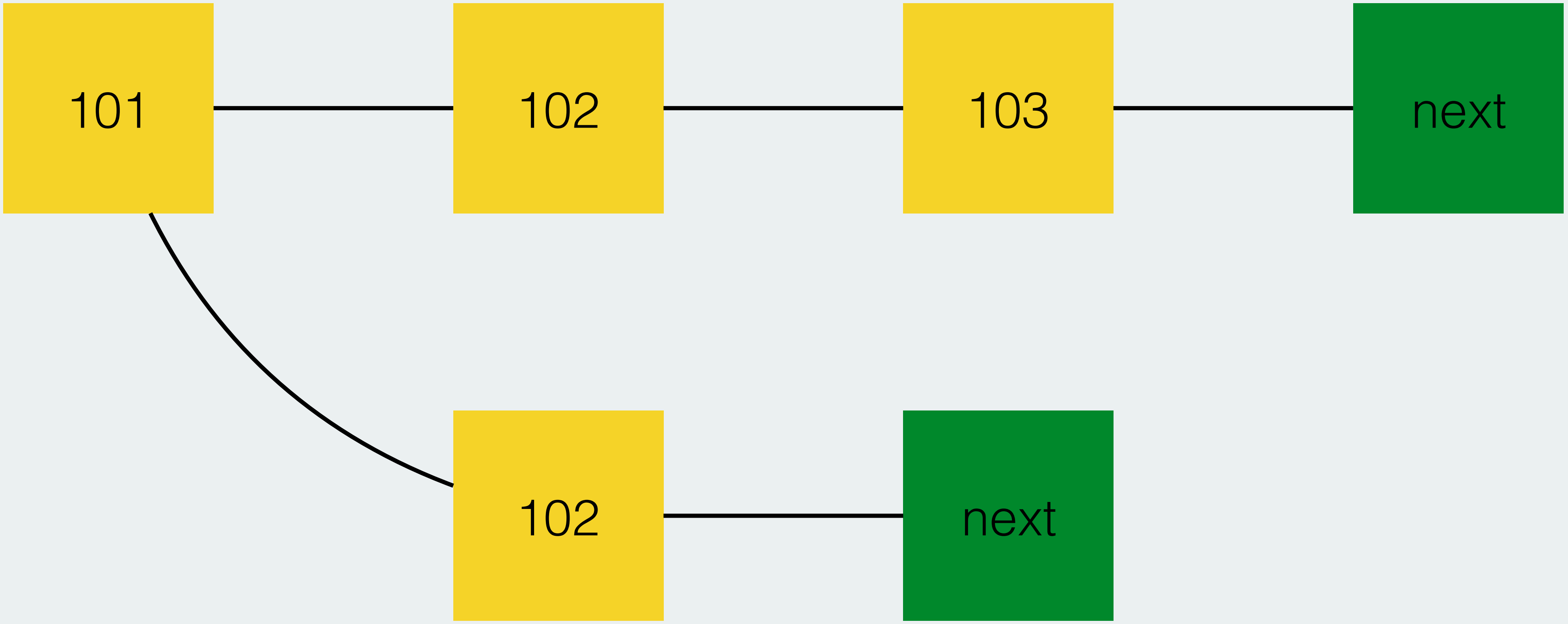


Proof of Stake

“Miners” vote with currency instead of hashing power

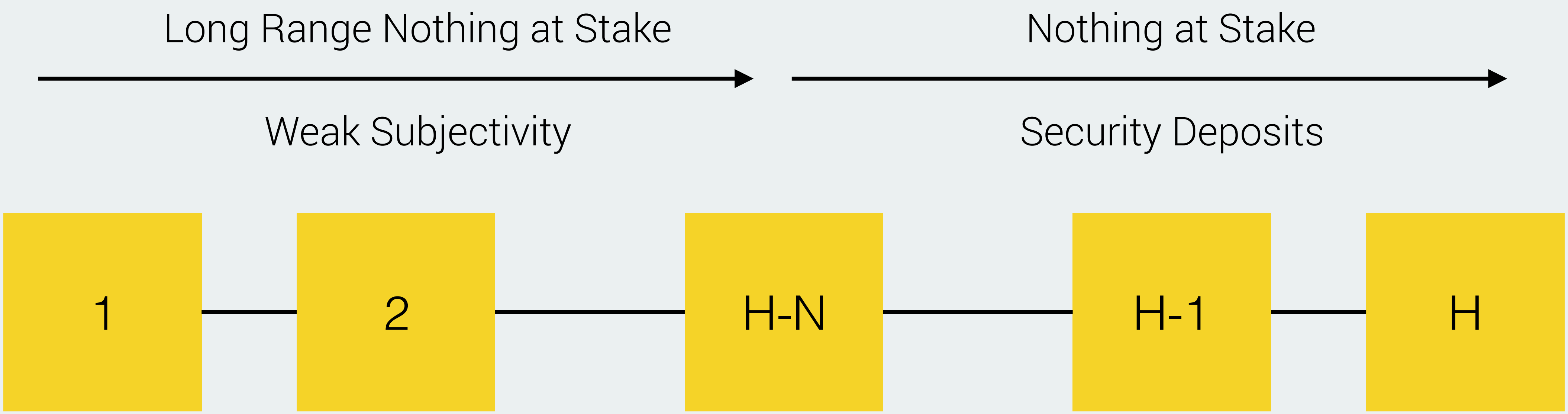
Mining an multiple chains has no cost (Nothing at stake)

Incentive to vote on all chains



Proof of Stake

Nothing at Stake problem split into two:



Security Deposits

Validators have to put down a security deposit

If misbehaviour is cryptographically provable

- The entire deposit is forfeited (“slashed”)
- Stake doesn’t count towards consensus?

Consensus by bet

Basic Idea:

- Bet for inclusion of a specific block at a height
  - Profit in all chains where it is included
  - Loss in all other chains

Incentive to bet on the chain most likely to win

Consensus by bet

Similar to Proof of Work:

- If you mine on a block
  - Profit in all chains where it is included (hopefully)
  - Loss in all other chains (electricity cost, etc.)

Consensus by Block

In Ethereum 1.0:

- Blocks contain hash of parent

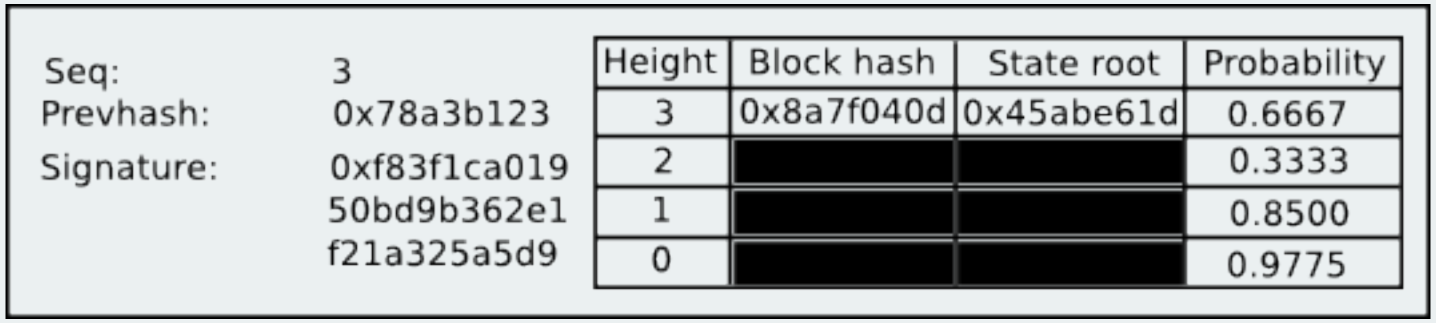
In Casper:

- Blocks are independent of each other
- Block with best bets at a certain height wins
- Validators bet on every block height individually

Betting

Scoring Rules & Revelation Principle

Validators bet with their “opinion” about the chance that the block will be confirmed



Seq: 3
Prevhash: 0x78a3b123
Signature: 0xf83f1ca019
50bd9b362e1
f21a325a5d9

Height	Block hash	State root	Probability
3	0x8a7f040d	0x45abe61d	0.6667
2	[redacted]	[redacted]	0.3333
1	[redacted]	[redacted]	0.8500
0	[redacted]	[redacted]	0.9775

The higher their estimated probability (“opinion”), the more risk and reward (up to 90% loss)

Finalisation

After a certain threshold of

- enough bets
- with high enough probability each

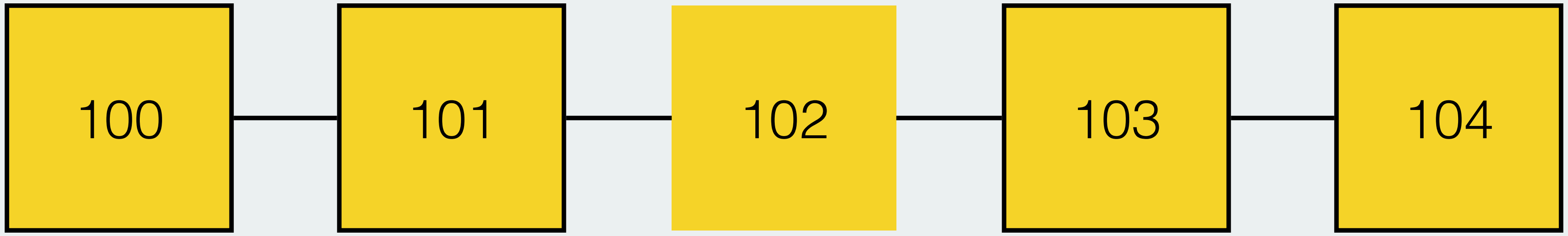
=> Majority of validators risking most of their deposit

=> Block is considered finalised

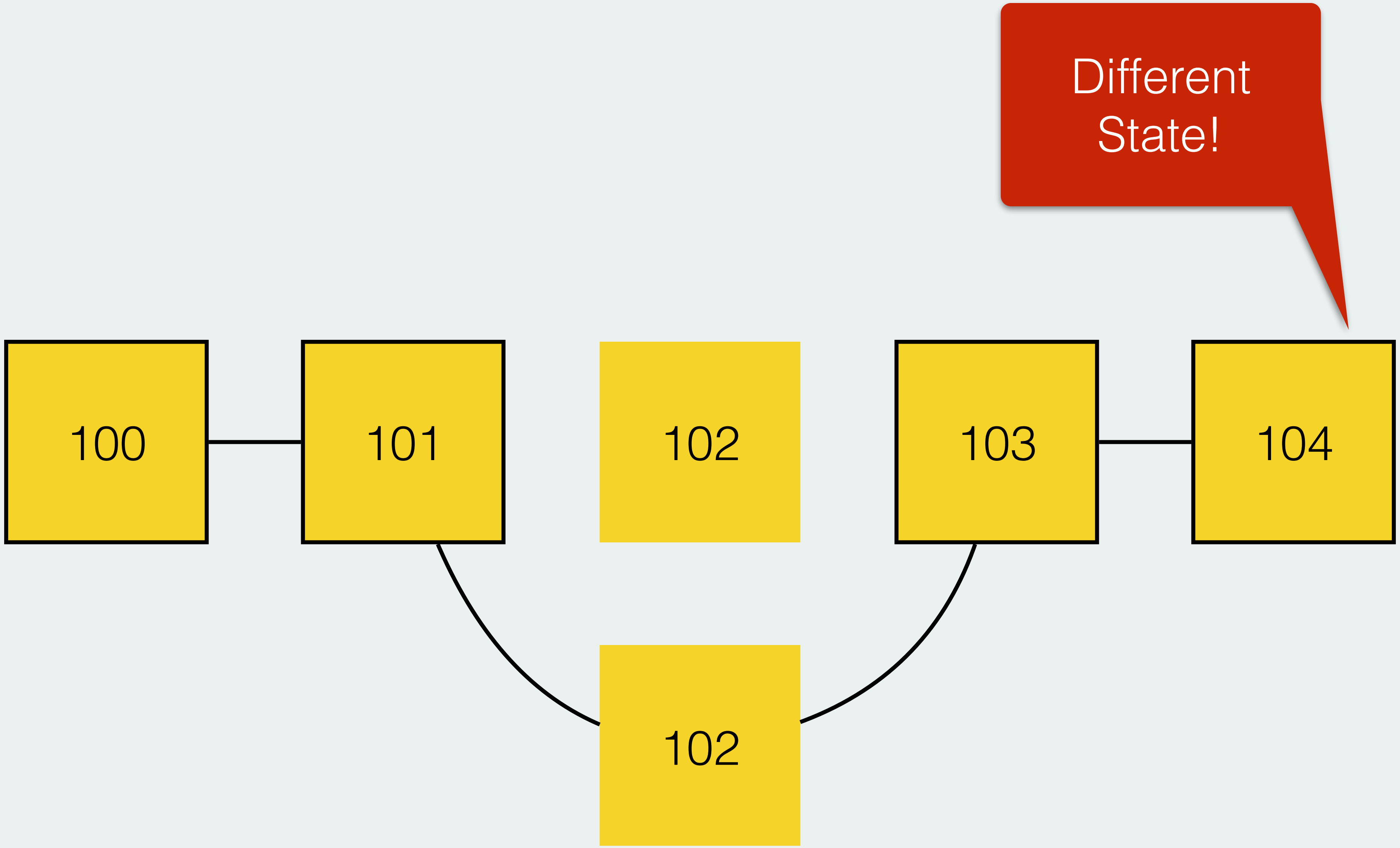
Clients will refuse any other block at that height

Invalid transactions?

Consensus by Block



Consensus by Block



Bonded Validators

Transactions for joining and leaving the validator pool

Minimum Deposit: 1250 eth

rises with number of validators

Maximum of 250 concurrent validators (currently)

Not profitable after some bonded time

At least 4 month wait time for withdrawal

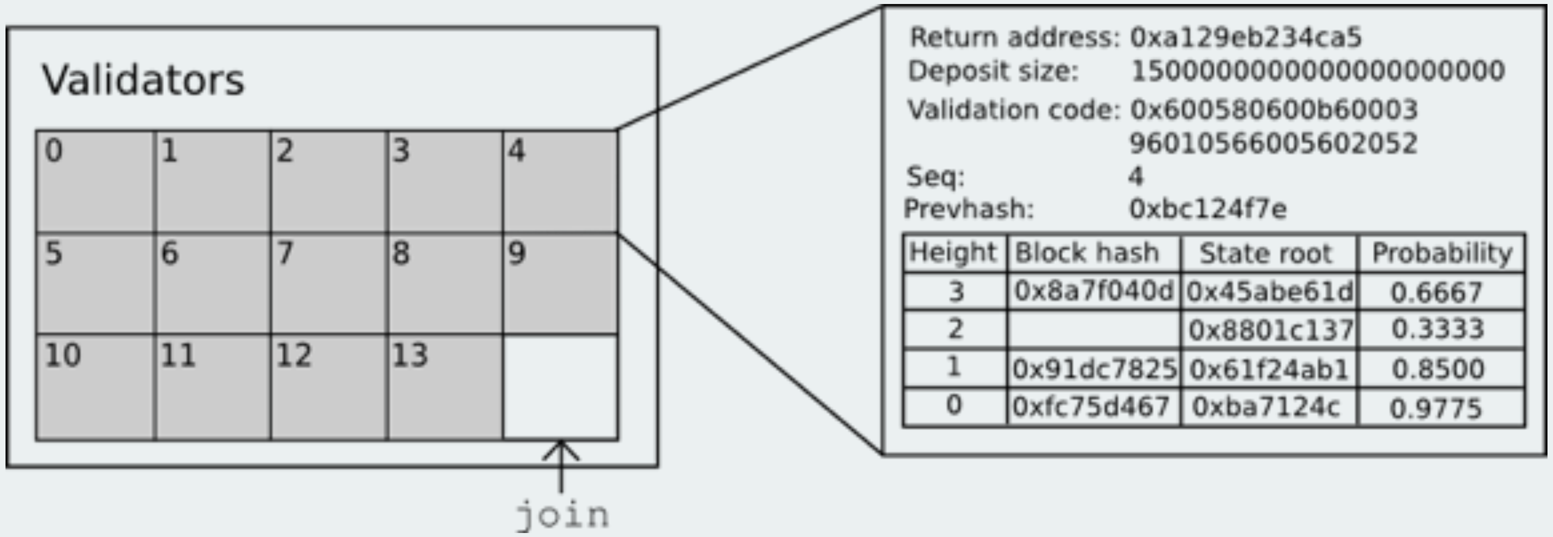
Casper Contract

Most of Casper implemented as a serpent contract

github.com/ethereum/pyethereum serenity branch

Keeps track of the validators and their opinions

Custodian of all security deposits



Return address: 0xa129eb234ca5
Deposit size: 1500000000000000000000
Validation code: 0x600580600b60003
96010566005602052
Seq: 4
Prevhash: 0xbc124f7e

Height	Block hash	State root	Probability
3	0x8a7f040d	0x45abe61d	0.6667
2		0x8801c137	0.3333
1	0x91dc7825	0x61f24ab1	0.8500
0	0xfc75d467	0xba7124c	0.9775

Block proposition

A specific validator is specified for a specific block

Timestamp: G + N *5

Missing proposers as source of entropy

Betting on missing blocks?

Weak Subjectivity

After the end of the withdrawal delay

- prior security deposits no longer owned by Casper
- no incentive not to start LRNaS attacks

If a node was offline longer than the withdrawal period:

- List of current validators needs to be fetched externally

POC-2

Casper implemented in POC2 in pyethereum

Also includes EIP 101 and EIP 105

Open Issues

Convergence is still not proven

Optimal validator strategies

More than 250 Validators

Disappearance of all current validators catastrophic

Still a lack of detailed specification

Lack of documentation on PoC

github.com/ahirner/ethereum