Hyperchains

æternity BLOCKCHAIN

Hyperchains

Unleashing the power of blockchain

Motivation

Why do we even care?

- Everyone should be able to create their own secure blockchain
- PoW systems require a lot of equally distributed computational power to be considered safe
- PoS systems are either unsafe or complicated... and in the end unsafe

Hyperchains

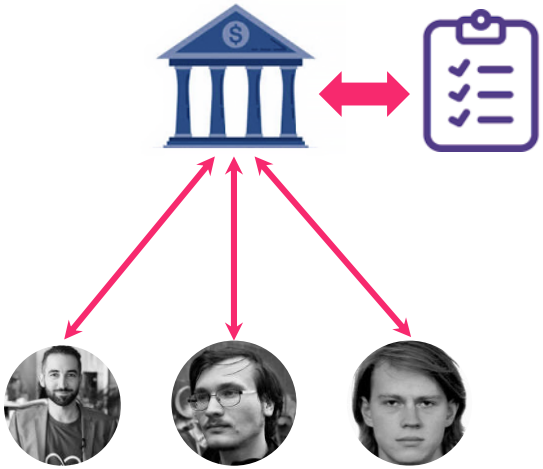
æternity BLOCKCHAIN

Short recap on basics

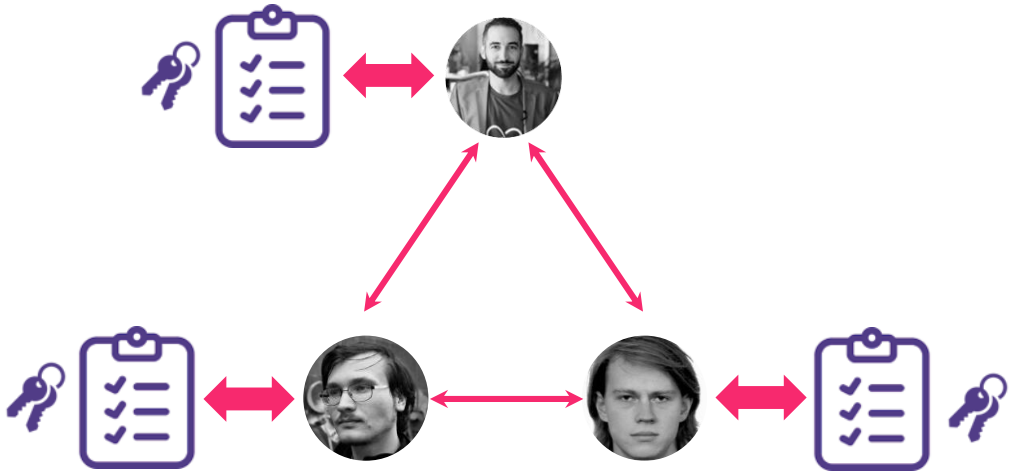
Hyperchains

æternity BLOCKCHAIN

Centralized vs Decentralized



Centralized



Decentralized P2P

æternity
BLOCKCHAIN

What do we want from a decentralized ledger?

1. Participants of the protocol need to have a common view on the state of the system
2. Mathematically impossible to imposter someone
3. Impossible to revert a operation or to change the order of two operations
4. The ability to verify the correctness of a operation
5. Asynchronous setting - no need to be online 24/7
6. Resilient to censorship

Hyperchains

æternity BLOCKCHAIN

Processing operations

Algorithm:

If the given operation is not valid according to some rules then do nothing, otherwise apply the operation to the current state and produce a new state.

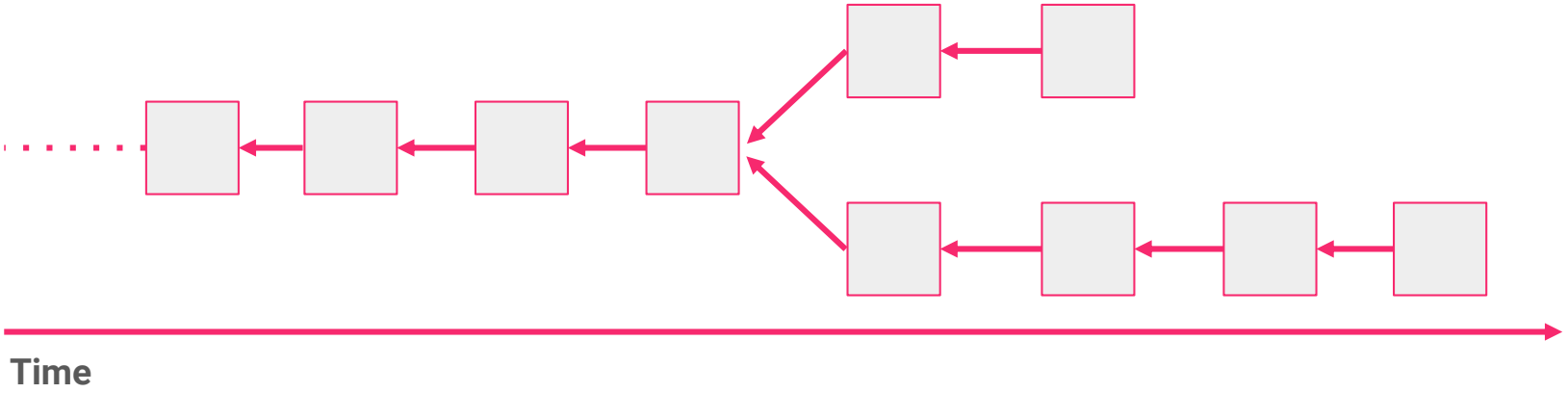
Let’s call those operations **“Transactions”**

Hyperchains

æternity BLOCKCHAIN

Grouping transactions

1. Participants in the network group transactions into packets called “blocks”
2. A block must be attached to a previous block which pinpoints the state
3. A block is valid if all enclosed transactions are valid at the given block
4. Blocks and transactions are gossiped in the network



Hyperchains

æternity BLOCKCHAIN

What is a consensus algorithm?

1. What chain of blocks should we trust?
2. What are the rules of block validation?
3. Who should produce the blocks?
4. What does it take to rewrite history?
5. Finality - the point in time when the block is considered immutable

Approaches:

- Proof of Work(AE, BTC, ETH...)
- Proof of Stake(Ouroboros, ...)
- Proof of Storage(Filecoin, ...)
- Proof of Bandwidth(Torcoin)
- ...
- Hybrids

Hyperchains

æternity BLOCKCHAIN

Proof of Work (PoW)

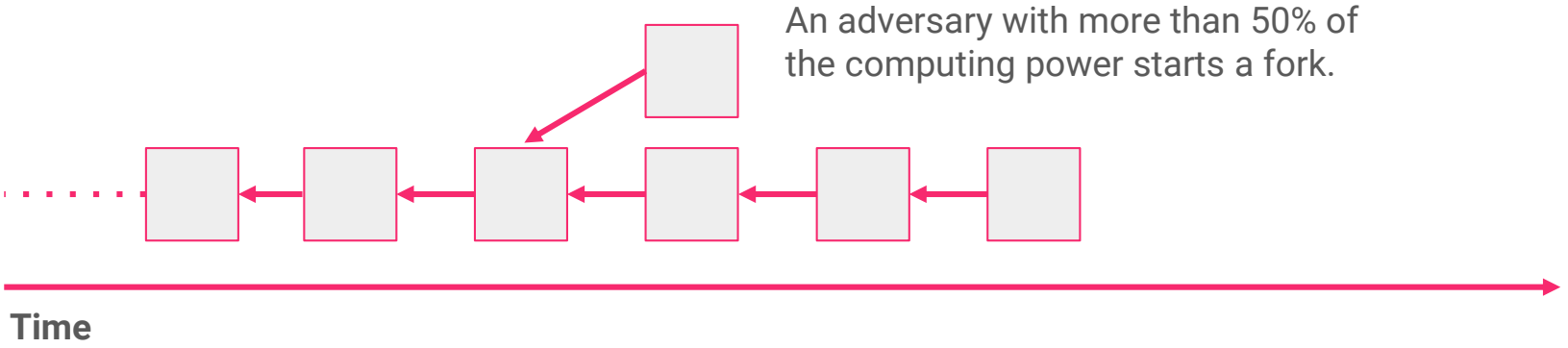
1. Valid blocks are computationally hard to generate
2. Always trust the chain with the most work attached
3. Persons willing to give computational power to the network are called “miners”
4. Miners are rewarded by giving them newly minted tokens
5. To rewrite history a attacker needs to control more than 50% of the computing power of the network!

Hyperchains

æternity BLOCKCHAIN

What does it take to rewrite history?

51% Attack



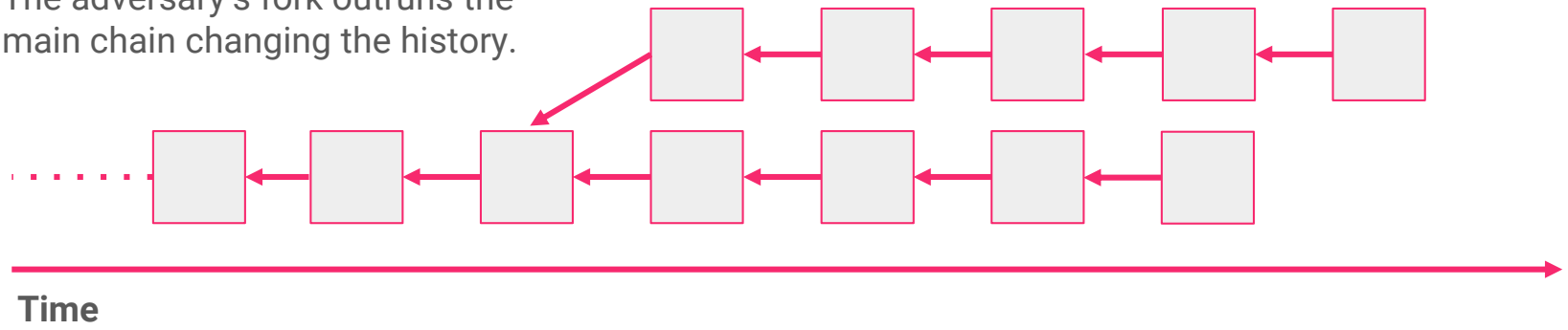
Hyperchains

æternity BLOCKCHAIN

What does it take to rewrite history?

51% Attack

The adversary's fork outruns the main chain changing the history.

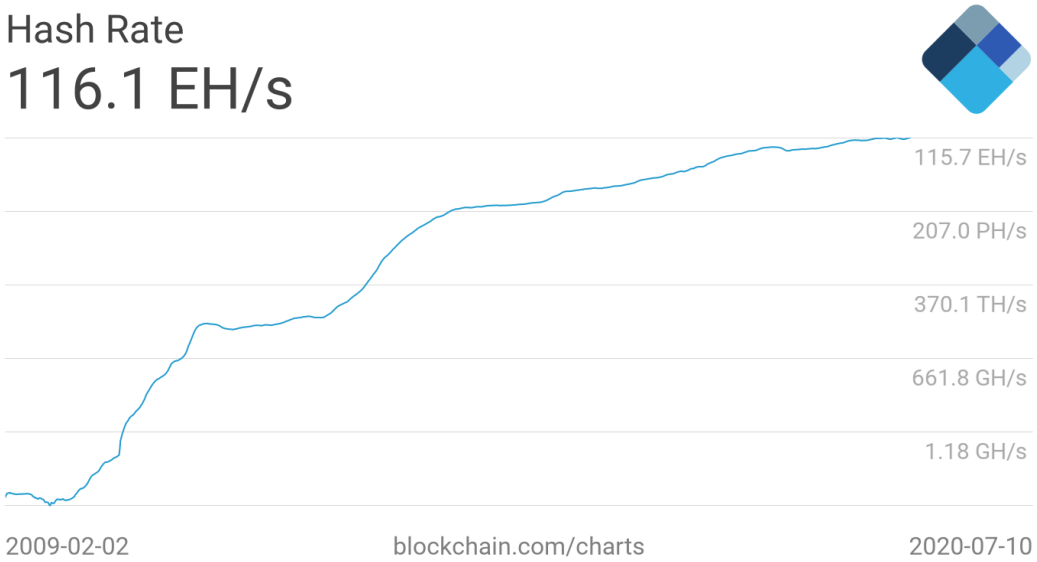


Hyperchains

æternity BLOCKCHAIN

Proof of Work - Pros

Safety

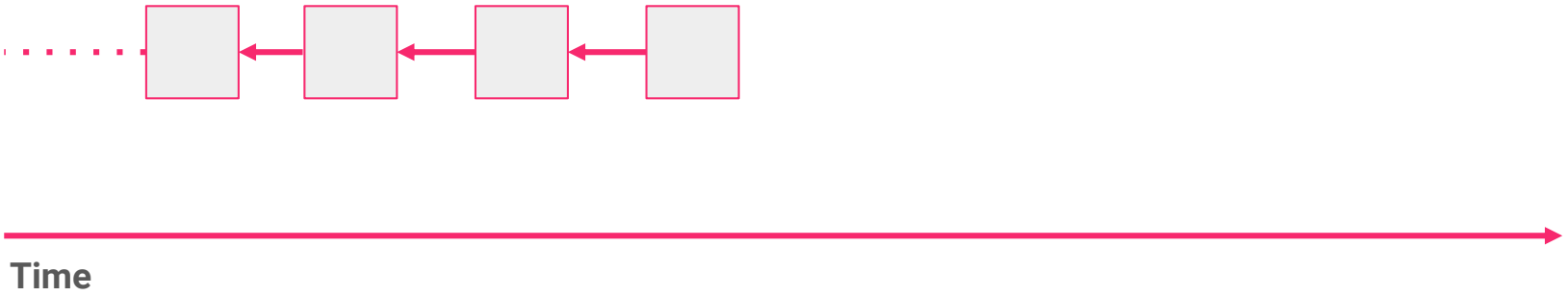


Hyperchains

æternity BLOCKCHAIN

Proof of Work - Pros

Resolving Forks

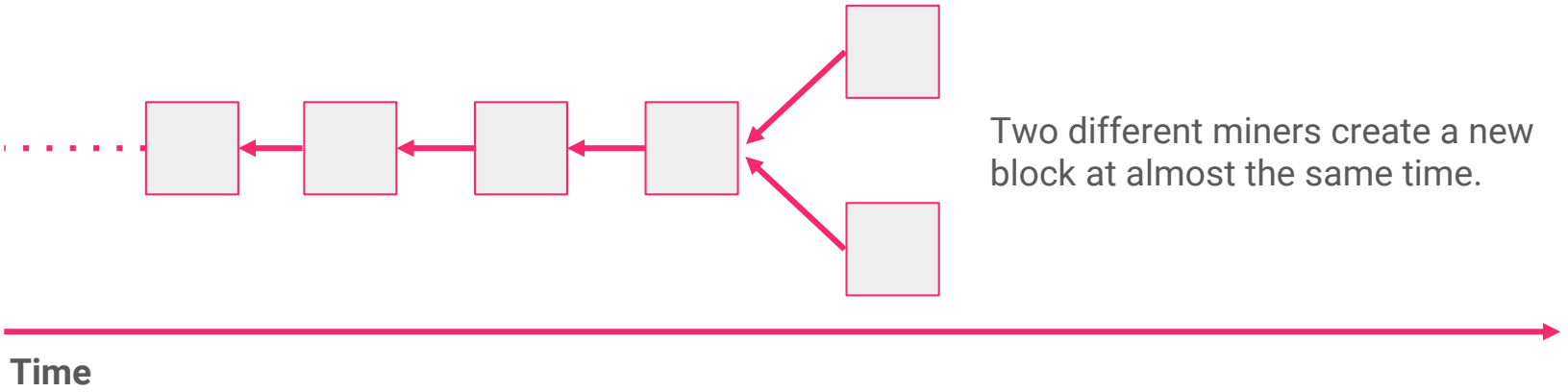


Hyperchains

æternity BLOCKCHAIN

Proof of Work - Pros

Resolving Forks

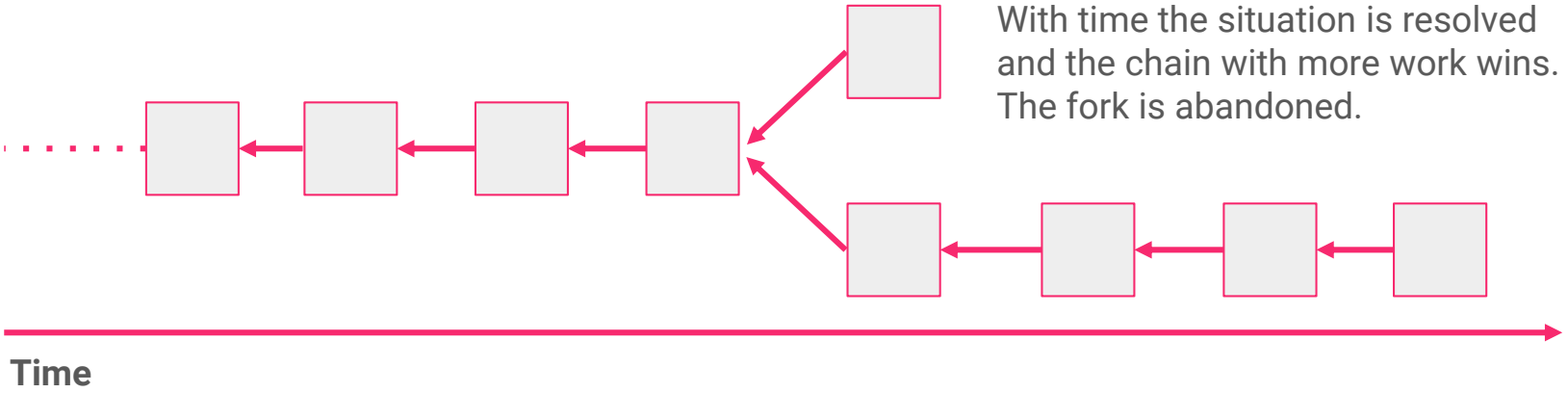


Hyperchains

æternity BLOCKCHAIN

Proof of Work - Pros

Resolving Forks



Proof of Work - Pros

KISS Principle

*"Complicated is easy, but **simple** is **hard**."*

- Robert Virding

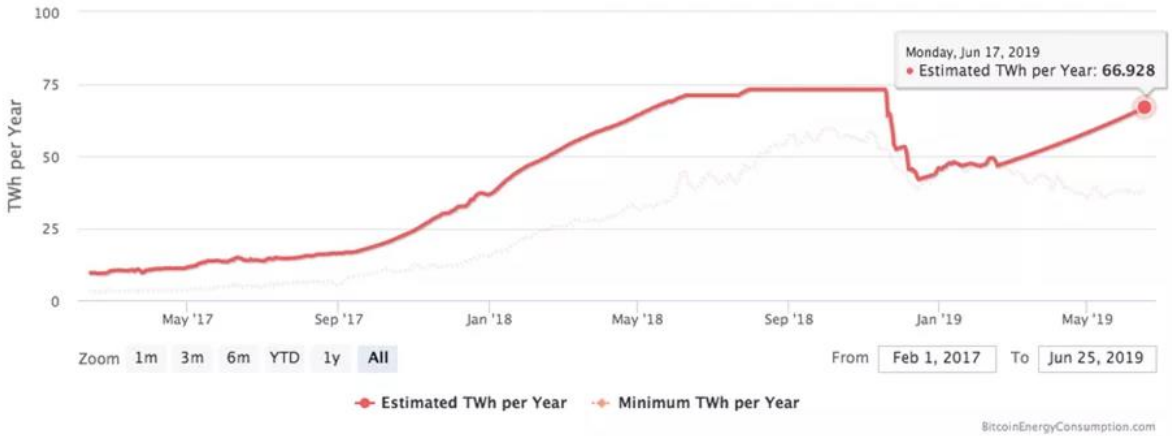
æternity BLOCKCHAIN

Hyperchains

æternity BLOCKCHAIN

Proof of Work - Cons

- Ridiculous waste of energy
- Centralization via mining pools



Hyperchains

æternity BLOCKCHAIN

Proof of Stake (PoS)

Basic Ideas

1. Transactions are processed by people who would lose the most if they were malicious
2. Blocks are generated by validators elected based on the “stake” in the blockchain
3. No waste of computational power - environment friendly
4. Easy to create hard forks if the validators agree

Hyperchains

æternity BLOCKCHAIN

Proof of Stake (PoS)

Problems To Solve

1. Who is allowed to participate in the election of the validator?
2. How do we prevent the validator from manipulating the blockchain to increase the odds of his reelection?
3. How do we calculate the stake of the validator in the network?
4. How do we choose the validator in a unpredictable, publicly verifiable, decentralized manner?

Hyperchains

æternity BLOCKCHAIN

Proof of Stake (PoS)

Example (Broken) Approach

1. Each user is eligible to become a validator
2. The more tokens the user has the more stake he has
3. A election is held each N minutes based on the hash of the most recent block

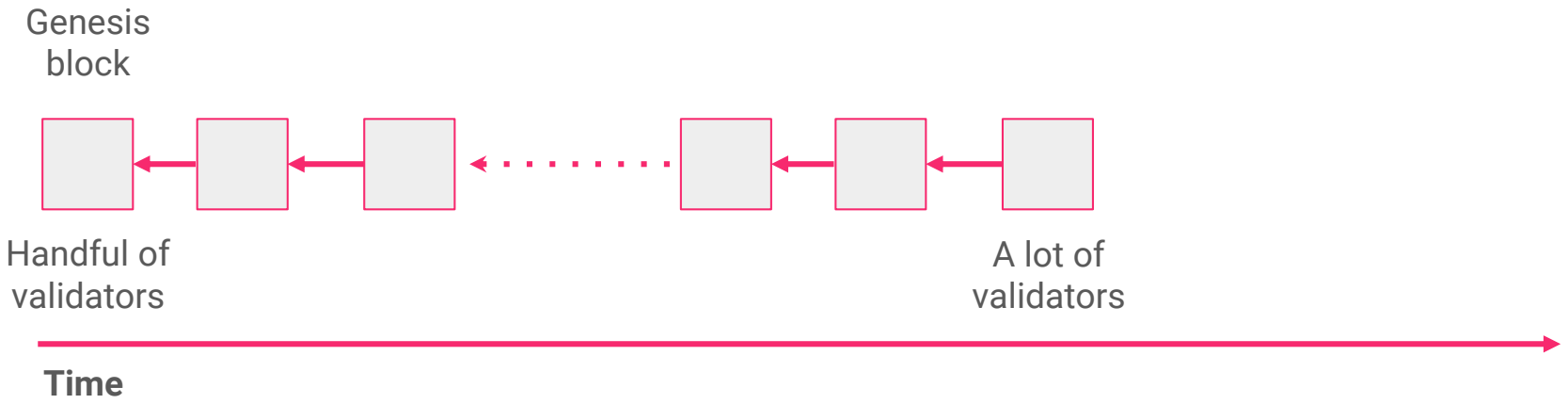
Hyperchains

æternity BLOCKCHAIN

Proof of Stake (PoS)

Long Range Attack

At the beginning of the chain there were few users who held most of the stake.

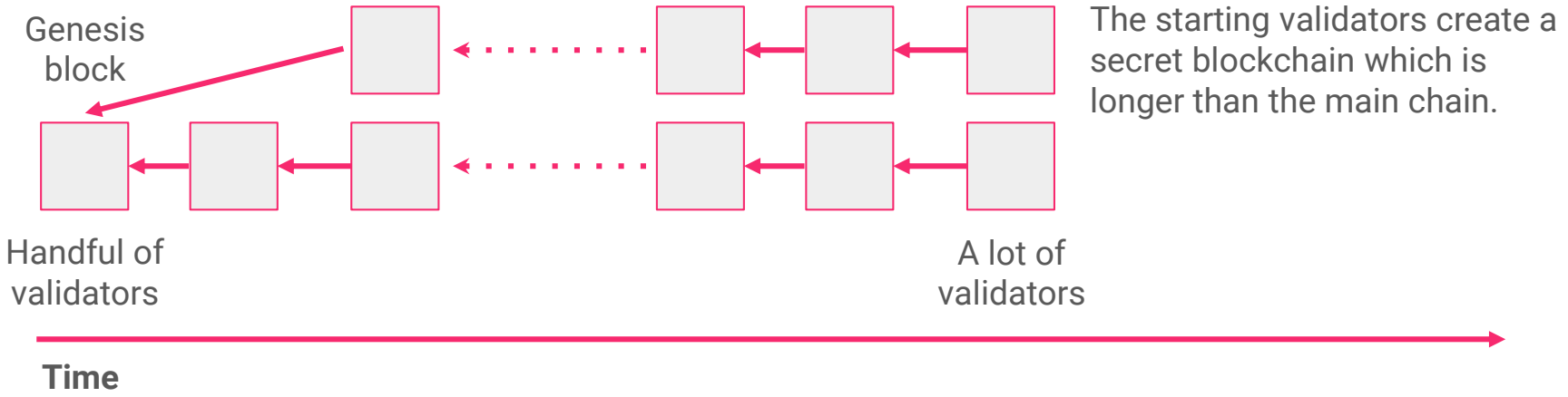


Hyperchains

æternity BLOCKCHAIN

Proof of Stake (PoS)

Long Range Attack



The starting validators create a secret blockchain which is longer than the main chain.

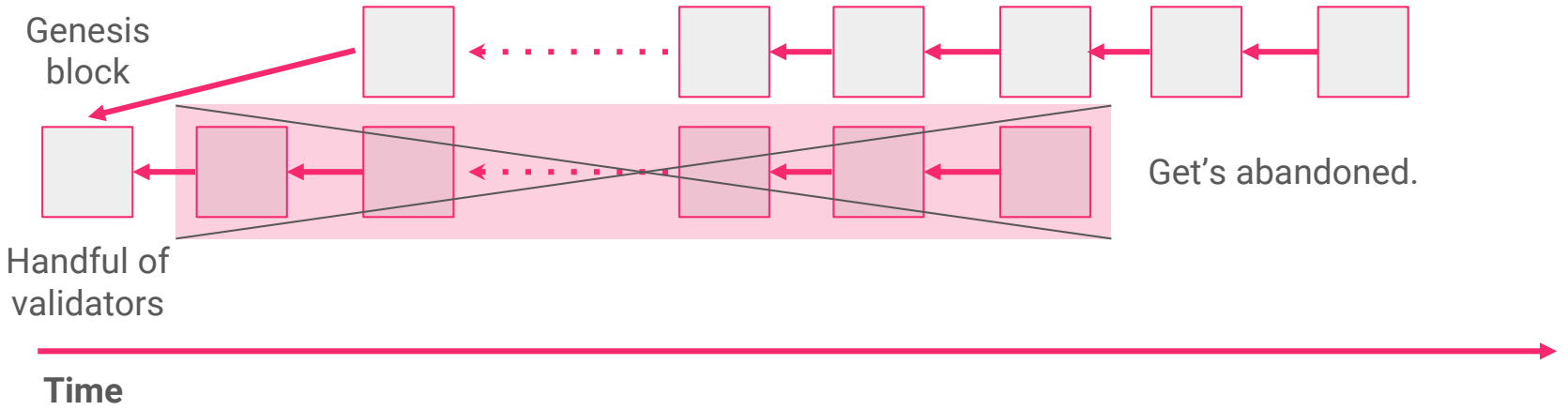
Hyperchains

æternity BLOCKCHAIN

Proof of Stake (PoS)

Long Range Attack

After some time the cartel publishes the secret chain and rewrites history.

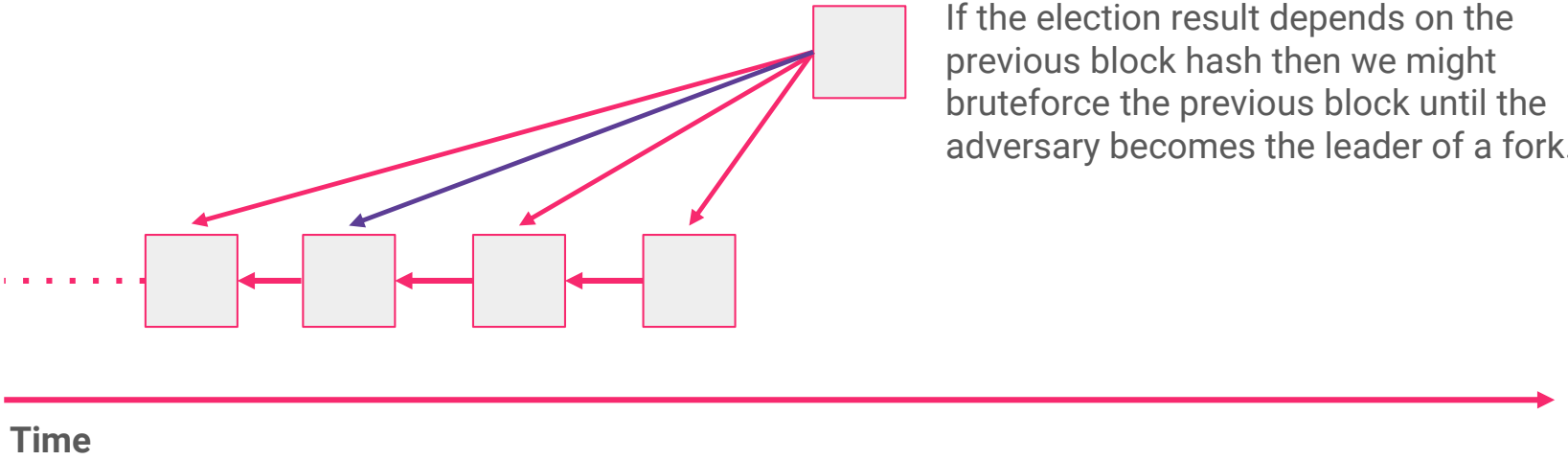


Hyperchains

æternity BLOCKCHAIN

Proof of Stake (PoS)

Stake Grinding



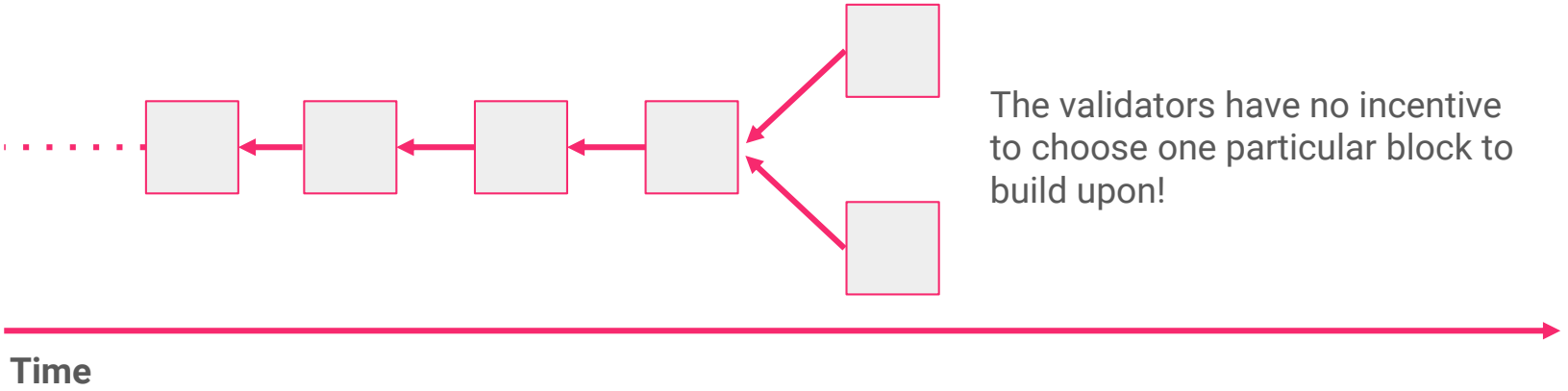
If the election result depends on the previous block hash then we might bruteforce the previous block until the adversary becomes the leader of a fork.

Hyperchains

æternity BLOCKCHAIN

Proof of Stake (PoS)

Nothing At Stake



The validators have no incentive to choose one particular block to build upon!

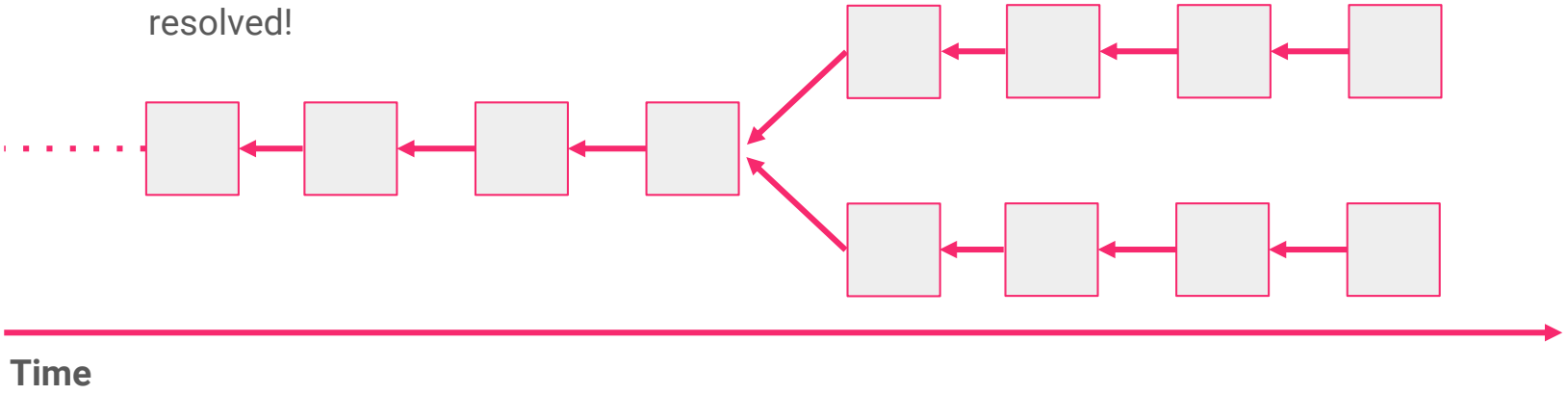
Hyperchains

æternity BLOCKCHAIN

Proof of Stake (PoS)

Nothing At Stake

They can build on both chains in parallel and the fork get's never resolved!



Hyperchains

æternity BLOCKCHAIN

Proof of Stake (PoS)

How To Make It Safe?

- Some sort of centralization
- Unbelievably complicated protocol which tries to create a decentralized and unbiasable RNG:
  - (PoS) Ouroboros white paper - 67 pages
  - (PoW) BTC whitepaper - 9 pages
- Hybrid PoW/PoS approaches such as Casper which rely on a finality gadget on a PoW blockchain

Hyperchains

æternity BLOCKCHAIN

Introducing

Hyperchains

… because why not both?

Hyperchains are blockchains featuring a hybrid PoW/PoS algorithm where a parent PoW blockchain is securing and checkpointing a PoS child blockchain and the elections of the validators on the child chain depend only on what happens on the parent chain.

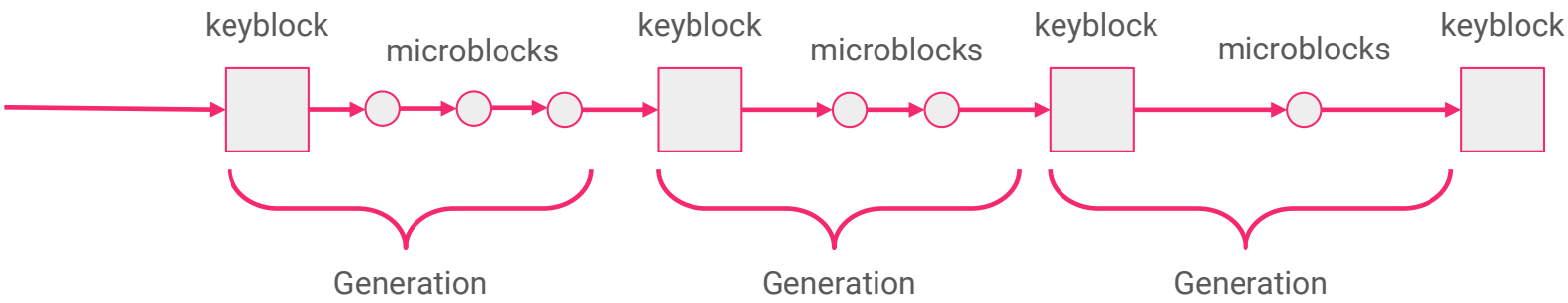
Hyperchains

æternity BLOCKCHAIN

The Current State Of AE

Bitcoin NG Consensus

Instead of mining blocks with transactions we use PoW mining to elect a leader which gains exclusive right for transaction processing until a new leader get's elected.



Block mining elects the new leader of the generation.

HYPERCHAINS

Basic Idea

1. Instead of electing the leader of the new generation via mining use PoS
2. Elections on the child chain happen every time a new key block on the parent chain is mined
3. People eligible for becoming the leader (called delegates) need to submit a commitment to the parent chain in which they acknowledge their current view of the child chain
4. To be considered for election a delegate needs to submit a commitment
5. Child keyblocks are valid only if they point to the key block submitted via the commitment

æternity BLOCKCHAIN

Hyperchains

æternity BLOCKCHAIN

HYPERCHAINS

Election Process

1. 100 people with most stake on the child chain are called delegates
2. To be considered for the next election on the child chain, delegates submit a commitment to the parent chain in which they acknowledge their current view of the chain
3. Once the generation on the parent chain is over all commitments and the new keyblock hash are feed to a transparent and verifiable function which elects the new leader (validator)

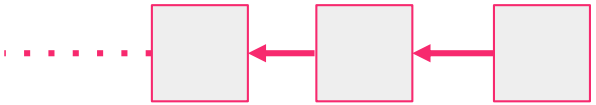
Hyperchains

æternity BLOCKCHAIN

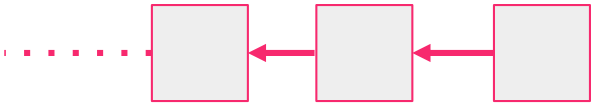
HYPERCHAINS

Example

Parent chain



Child chain



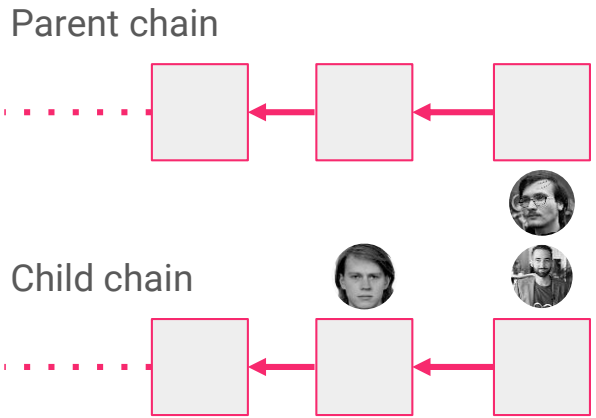
Eligible delegates

Delegate 1 Delegate 2 Delegate 3

Time

HYPERCHAINS

Example



Delegates submit commitments to the parent chain. The most recent keyblock of the child chain has not yet propagated to Delegate 2

Eligible delegates

Delegate 1 Delegate 2 Delegate 3

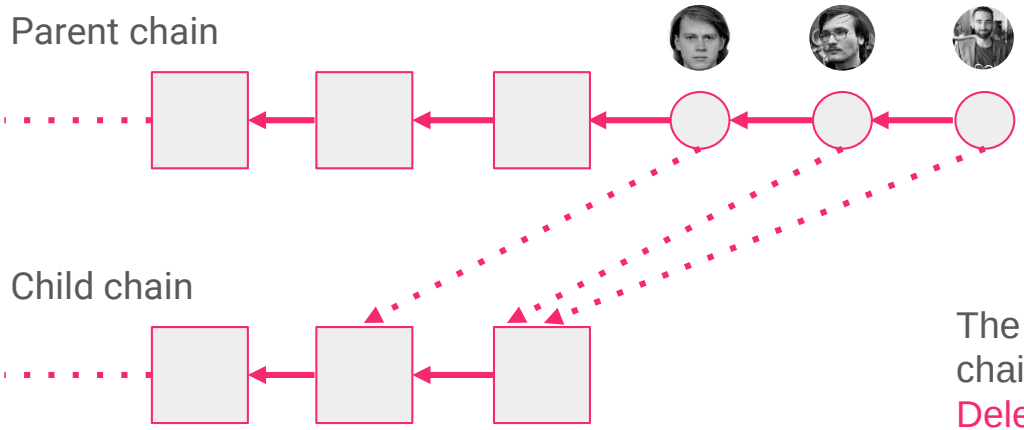
Time

Hyperchains

æternity BLOCKCHAIN

HYPERCHAINS

Example



The most recent keyblock on the child chain has propagated to Delegate 2. Delegate 2 resubmits his commitment.

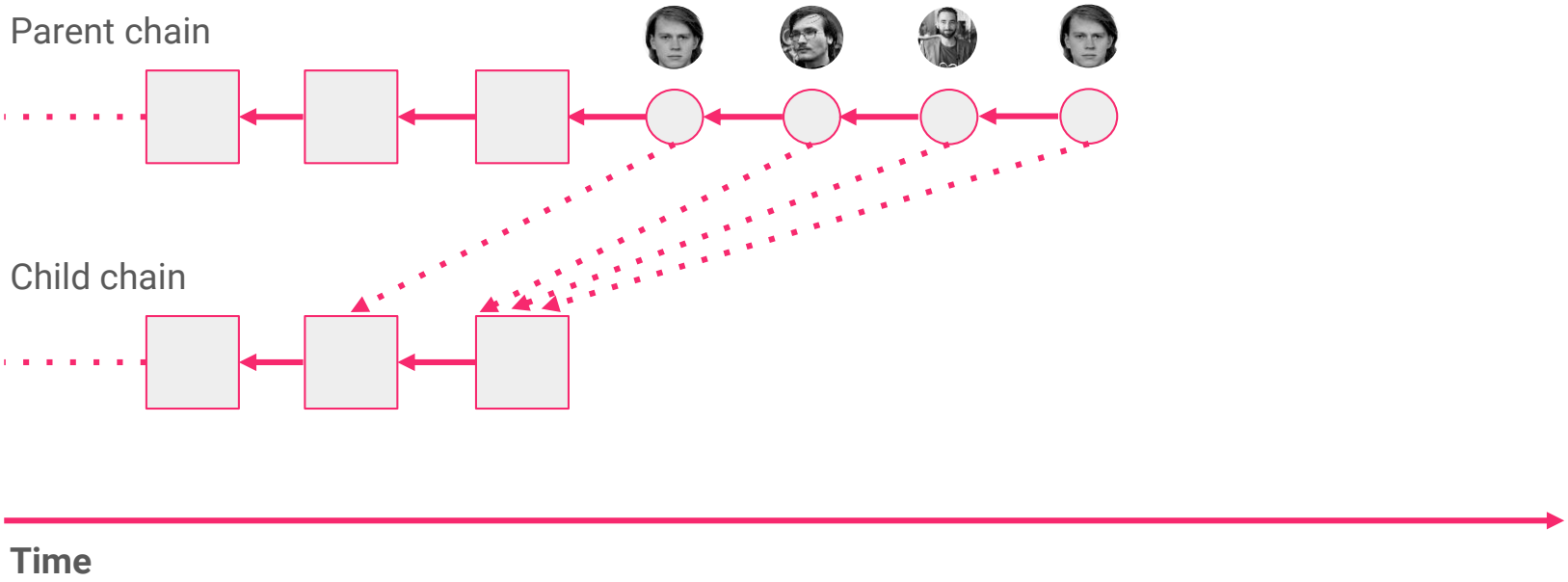
Time

Hyperchains

æternity BLOCKCHAIN

HYPERCHAINS

Example

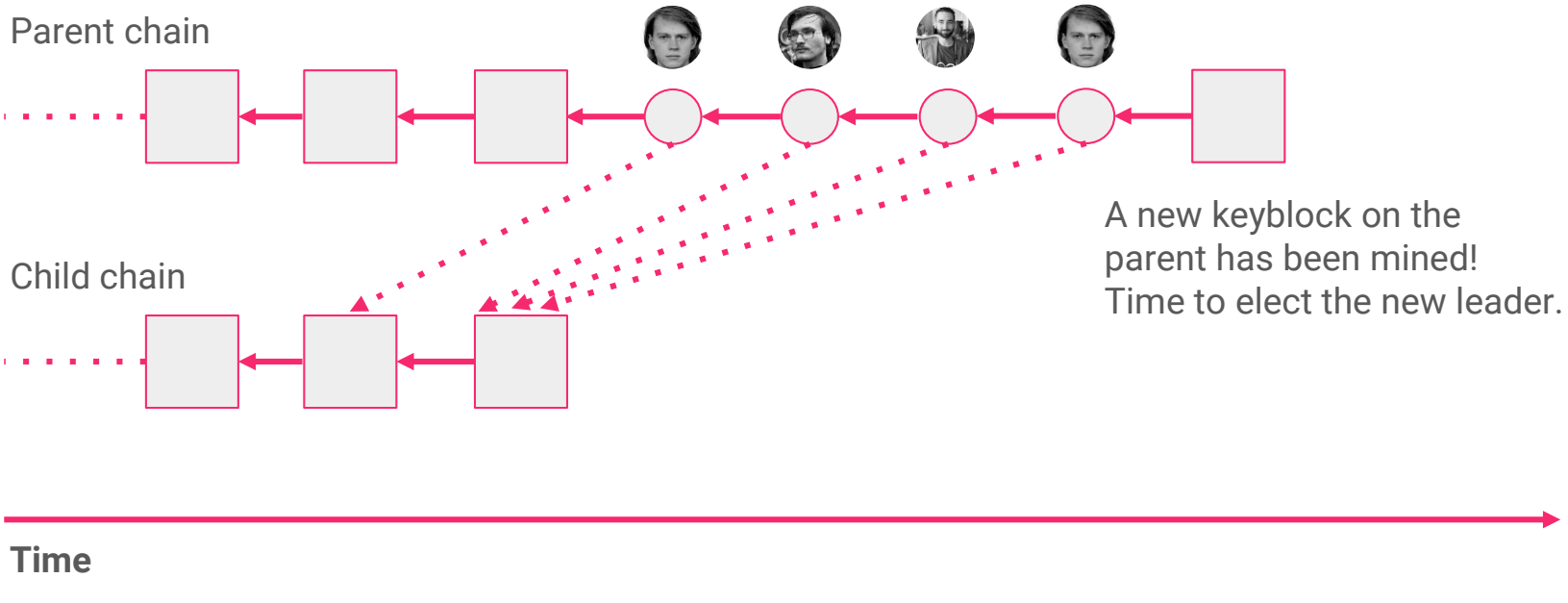


Hyperchains

æternity BLOCKCHAIN

HYPERCHAINS

Example

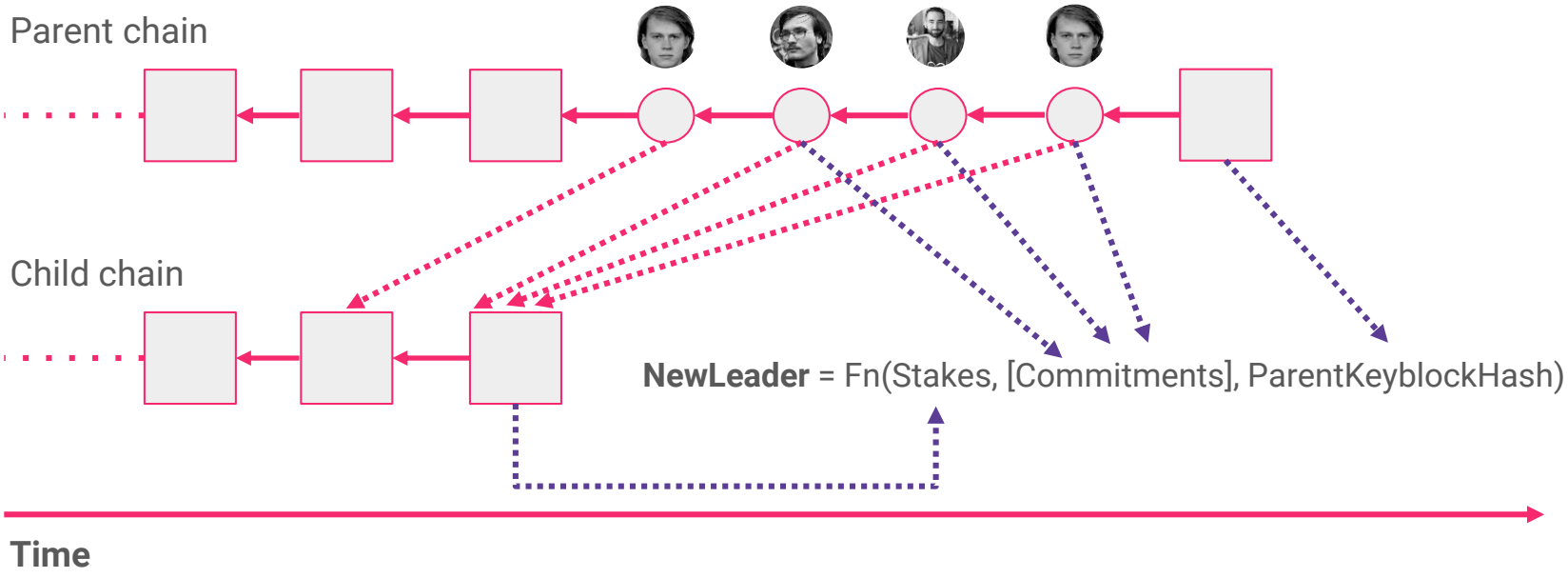


Hyperchains

æternity BLOCKCHAIN

HYPERCHAINS

Example

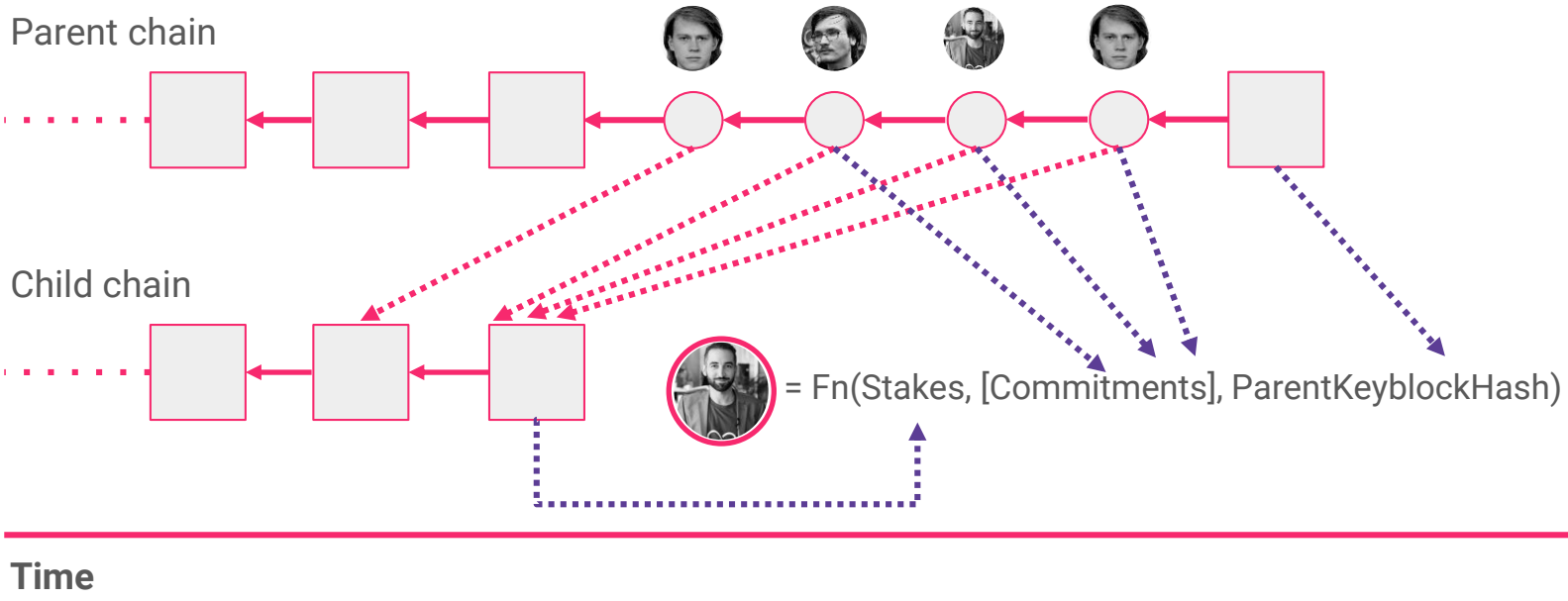


Hyperchains

æternity BLOCKCHAIN

HYPERCHAINS

Example

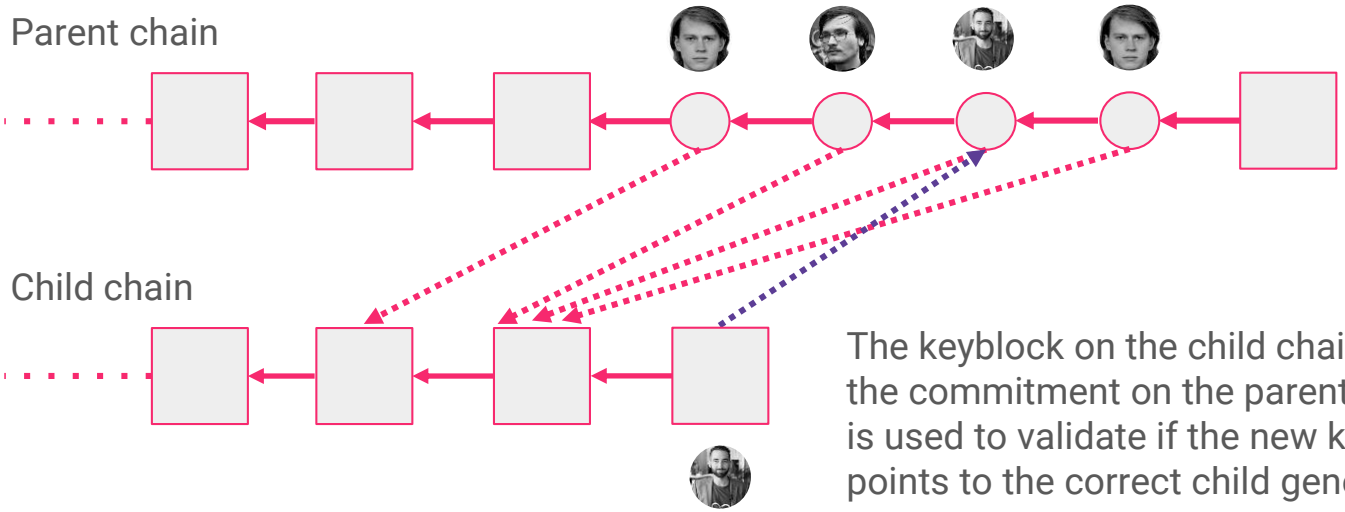


Hyperchains

æternity BLOCKCHAIN

HYPERCHAINS

Example



The keyblock on the child chain points to the commitment on the parent chain and is used to validate if the new keyblock points to the correct child generation.

Hyperchains

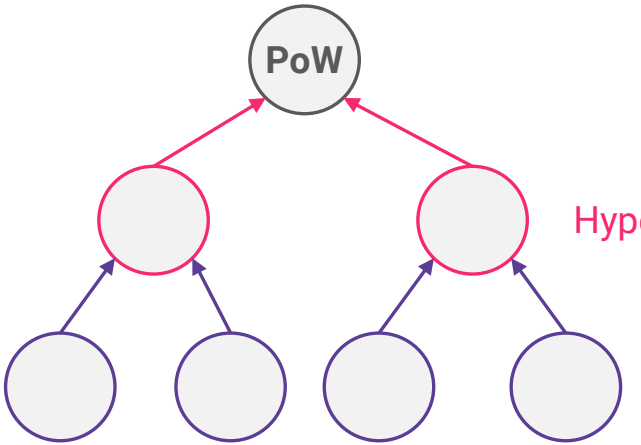
æternity BLOCKCHAIN

HYPERCHAINS

Infinite Scalability

Instead of using a PoW based chain for commitments we use another hyperchain

Hyperchains are cheap to run and we can easily scale up the network by stacking!



Hyperchains Backed by PoW

Hyperchains backed by another hyperchain

HYPERCHAINS

Avoiding Problems Of Naive PoS

- **Nothing at stake:**
  - Voting on both forks at once is punished by slashing the stake
  - We take only the last commitment on the parent chain
- **Microforks:**
  - Proof of Fraud from BitcoinNG
- **State grinding:**
  - The election does not depend on anything the adversary controls
- **Long range attack:**
  - Commitments for the unknown chain need to be published regularly so everybody would notice that someone is attacking the network and blacklist this person
- **Dictator problem:**
  - Unless the dictator controls more than 50% of the stake then if the dictator does not include your transaction which would benefit his opposition then the next validator will

Hyperchains

æternity BLOCKCHAIN

HYPERCHAINS

Use Cases

- Communities – on-chain data sharing on Superhero?
- Internal chains in companies – local governance
- Private business – exchange 10 MoonBugCoins for a coffee in MoonBugs Caffee!
- MMO games – The gold in World of Warcraft has some physical value*. Why not use blockchain there? (*funfact: greater than the Venezuelan Bolivar)

æternity
BLOCKCHAIN

Discussion

Questions?