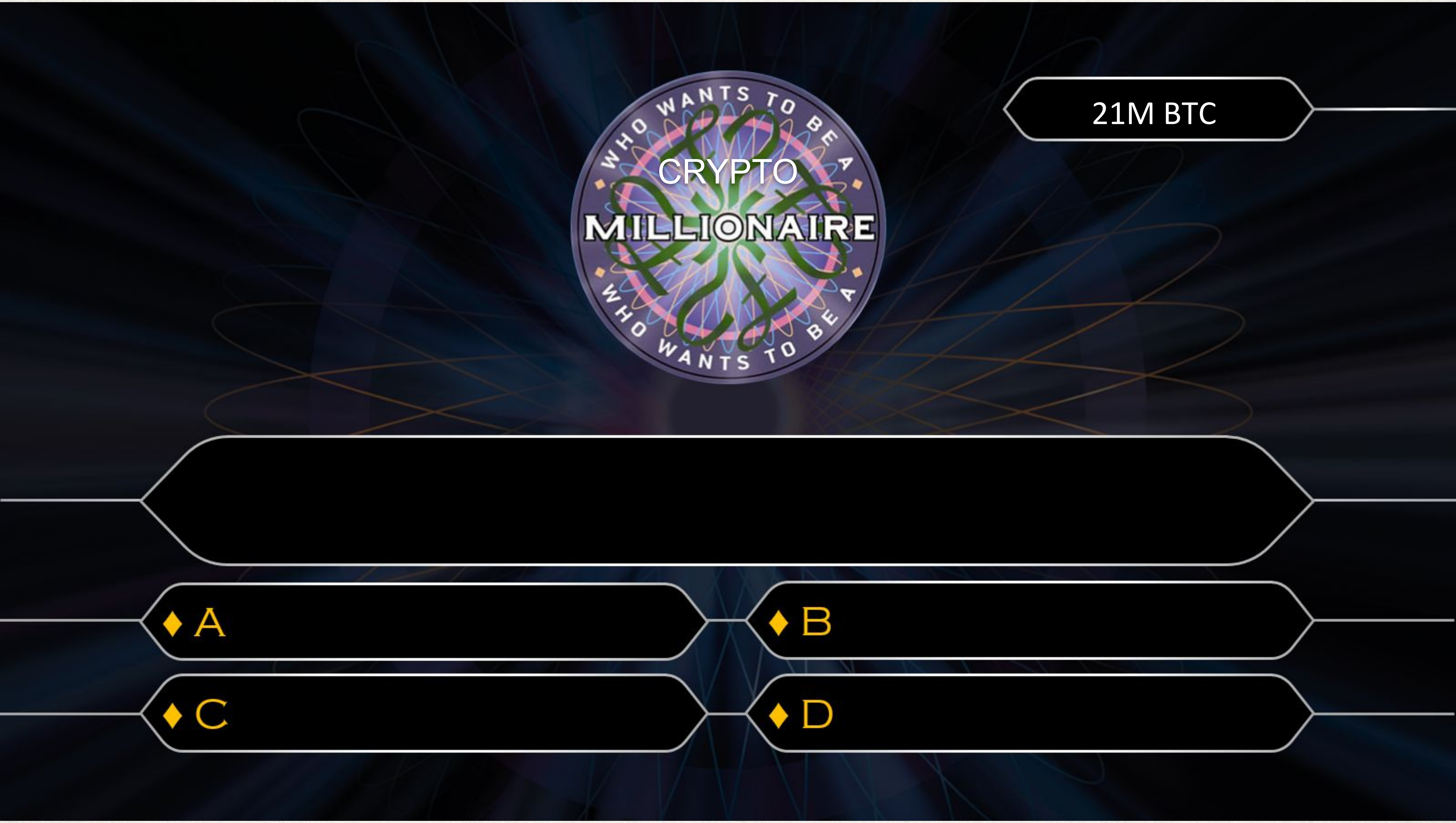
What Blockchains Can Do For Us

Peter Gaži
IOHK

Joint work with
Christian Badertscher
Aggelos Kiayias
Alexander Russell
Vassilis Zikas



21M BTC

♦ A

♦ B

♦ C

♦ D

WHO WANTS TO BE A CRYPTO MILLIONAIRE

21M BTC

What useful can blockchains give us, beyond a ledger?

♦ A

♦ B

♦ C

♦ D

WHO WANTS TO BE A CRYPTO MILLIONAIRE

21M BTC

What useful can blockchains give us, beyond a ledger?

♦ A world peace

♦ B

♦ C

♦ D

WHO WANTS TO BE A

CRYPTO

MILLIONAIRE

WHO WANTS TO BE A

21M BTC

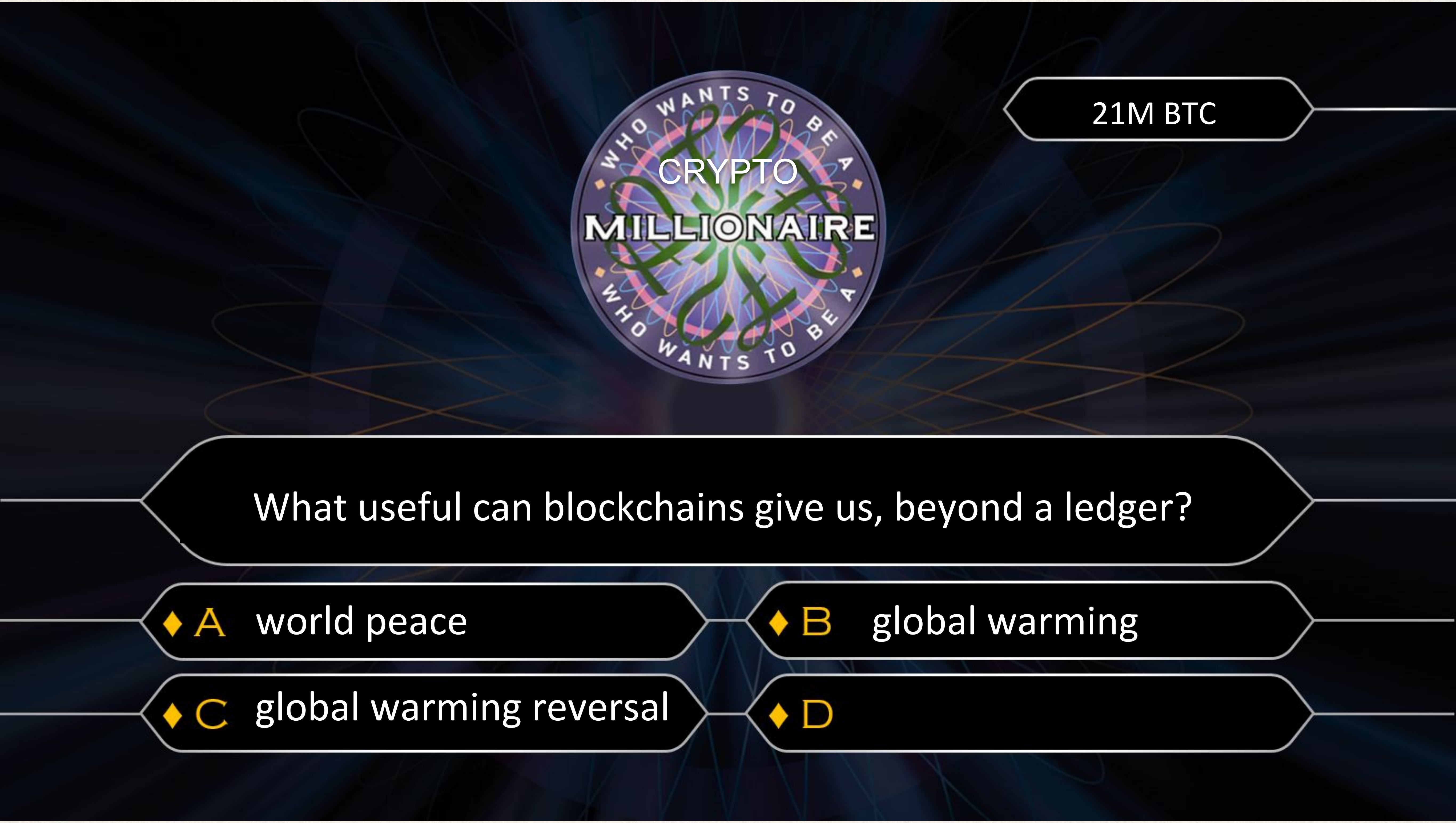
What useful can blockchains give us, beyond a ledger?

♦ A world peace

♦ B global warming

♦ C

♦ D



21M BTC

What useful can blockchains give us, beyond a ledger?

♦ A world peace

♦ B global warming

♦ C global warming reversal

♦ D

21M BTC

What useful can blockchains give us, beyond a ledger?

♦ A world peace

♦ B global warming

♦ C global warming reversal

♦ D global clock

WHO WANTS TO BE A
CRYPTO
MILLIONAIRE
WHO WANTS TO BE A

21M BTC

What useful can blockchains give us, beyond a ledger?

♦ A world peace	♦ B global warming
♦ C global warming reversal	♦ D global clock

Ouroboros Chronos

Like previous Ouroboroi:

- proof-of-stake protocol for permissionless blockchains
- same ledger as Bitcoin, without wasteful proofs of work

Ouroboros Chronos

Like previous Ouroboroi:

- proof-of-stake protocol for permissionless blockchains
- same ledger as Bitcoin, without wasteful proofs of work

What's new this time:

- no need to assume global clock!
- actually, can export one!

Why is that interesting?

Previous eventual-consensus PoS protocols need to assume global clock.

- to discard fake chains going “into the future”

Practical implementation: rely on NTP.

- additional trust assumption
- often neglected single point of failure

What does it Chronos achieve?

Assume:

- *same-speed* clocks for all parties
- bounded skew for initial parties
- bounded-delay network
- honest stake majority

Get:

- robust transaction ledger
- parties stay synchronized
- new parties can synchronize on join
- time can be exported to higher-level protocols

How does it work?

Synchronization procedure:

- executed periodically by all parties
- adjust local time based on timestamps of received blocks
    - how to aggregate from all blocks?
    - which blocks? (consensus+fairness needed here)

How does it work?

Synchronization procedure:

- executed periodically by all parties
- adjust local time based on timestamps of received blocks
    - how to aggregate from all blocks?
    - which blocks? (consensus+fairness needed here)

Joining procedure:

- executed by each newly joining party
- passive: observe network and wait
- gets in sync with old parties by next synchronization

Interested?

Talk to us!

...or check eprint soon.

C. Badertscher, P. Gaži, A. Kiayias, A. Russell, V. Zikas:
Ouroboros Chronos: Permissionless Clock Synchronization via Proof-of-Stake