Everything is a Race and Nakamoto Always Wins

Ertem Nusret Tas

Stanford University

de.crpyto seminar, spring 2021

This work appeared in ACM CCS 2020.
Ertem Nusret Tas is supported by The Stanford Center for Blockchain Research.

Amir Dembo
Stanford

Sreeram Kannan
U. Washington

David Tse
Stanford

Pramod Viswanath
UIUC

Xuechao Wang
UIUC

Ofer Zeitouni
Weizmann

Main Results

- Nakamoto's private double-spend attack is the worst attack: Bitcoin is secure if the private attack fails with high probability.

- Maximum tolerable adversary power is determined by the private attack threshold.

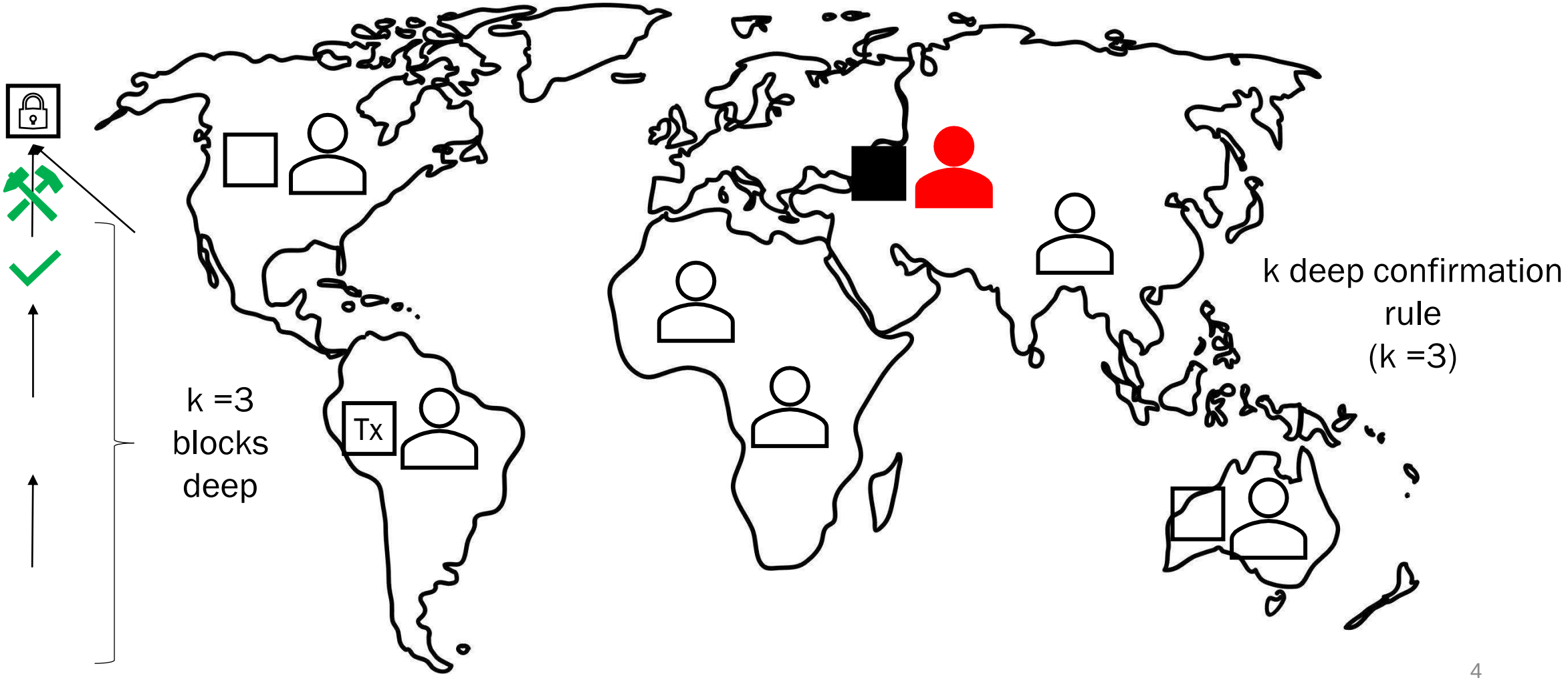
- This is true for three classes of longest chain protocols:
  - ✓ Nakamoto's original Proof-of-Work protocol
  - ✓ Ouroboros and Sleepy Proof-of-Stake protocols
  - ✓ Chia Proof-of-Space protocol

Let’s start with Nakamoto

Bitcoin: A Peer-to-Peer Electronic Cash System

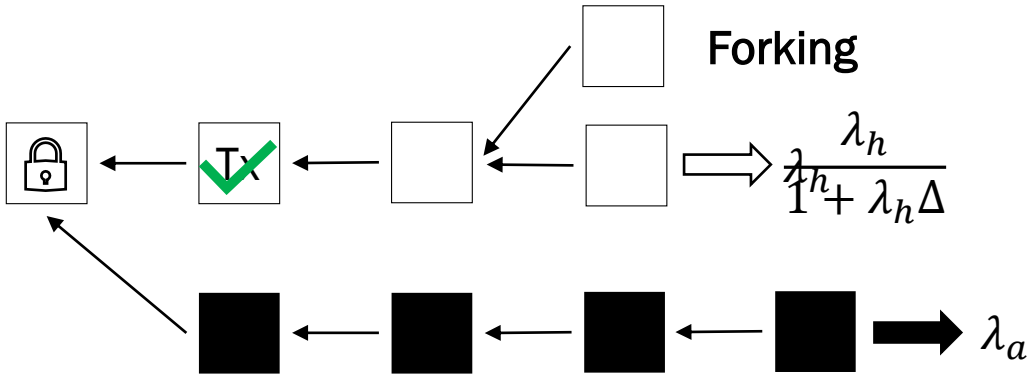
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Let's start with Nakamoto



Nakamoto's Private Attack

k deep confirmation rule
(k =3)



Private attack succeeds!

Safety: Once Tx is k-deep, Tx stays as part of the longest chain.

Liveness: Longest chain contains honest blocks.

Security

Private attack fails if $\lambda_a < \frac{\lambda_h}{1+\lambda_h\Delta}$

Private attack succeeds if $\lambda_a > \frac{\lambda_h}{1+\lambda_h\Delta}$

Can another attack succeed?

Network Model

- Synchronous network with delay Δ
- Total mining rate: λ
- Byzantine Adversary with mining rate $\lambda_a = \beta\lambda$
- Honest mining rate: $\lambda_h = \lambda - \lambda_a = (1-\beta)\lambda$
- Blocks arrive via a Poisson process of rate λ (in the limit size of time slots approach zero).

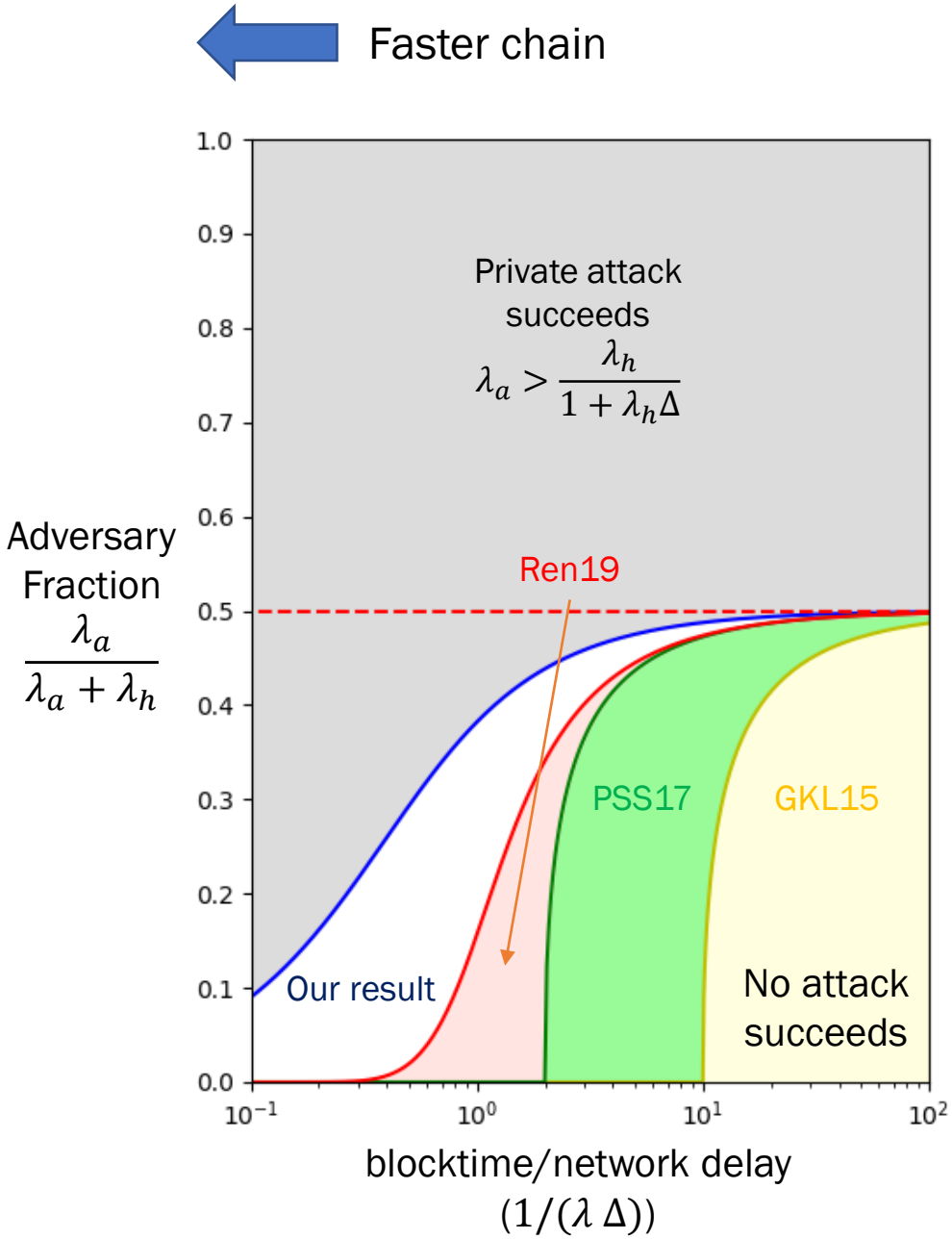
Closing the gap

Given $\beta = \lambda_a/(\lambda_a + \lambda_h)$ and Δ, for what values of blocktime $(1/\lambda)$, is Nakamoto's PoW longest chain protocol secure?

Nakamoto's longest chain protocol is secure if $\lambda_a < \frac{\lambda_h}{1+\lambda_h\Delta}$.

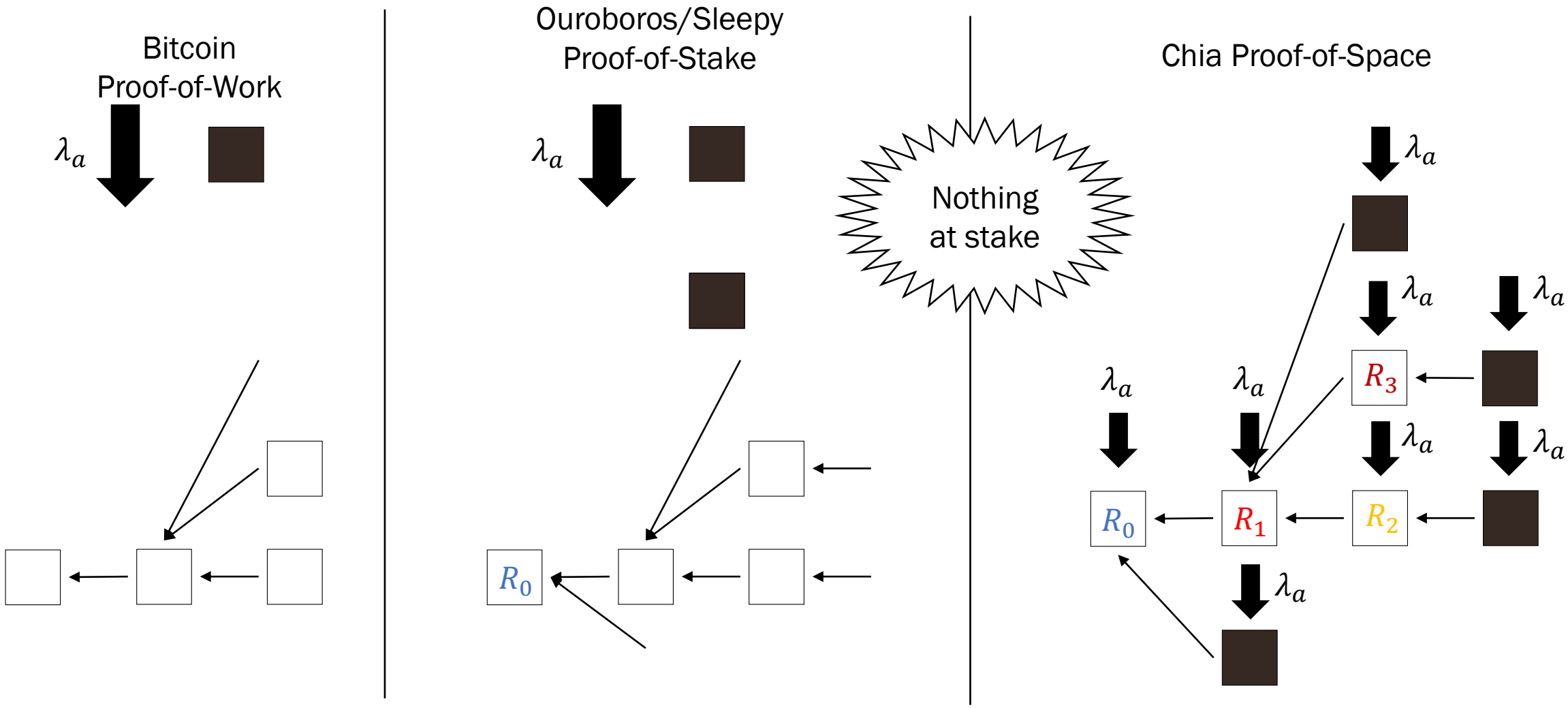
If $\lambda_a > \frac{\lambda_h}{1+\lambda_h\Delta}$, private attack succeeds.

Smaller blocktime = Faster chain!!



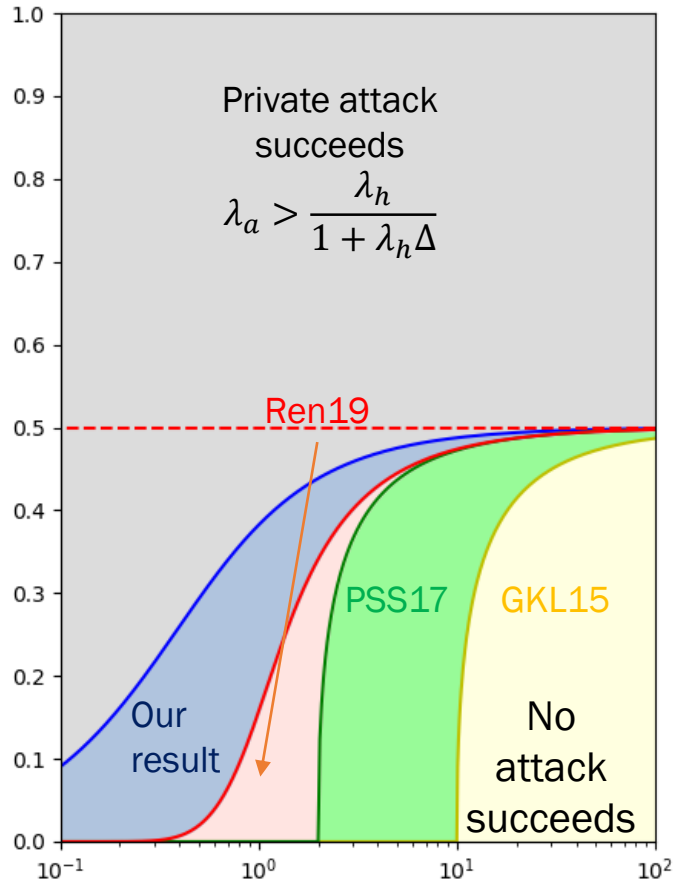
Other longest chain protocols

DGKR'17, DPC'19
CP'19

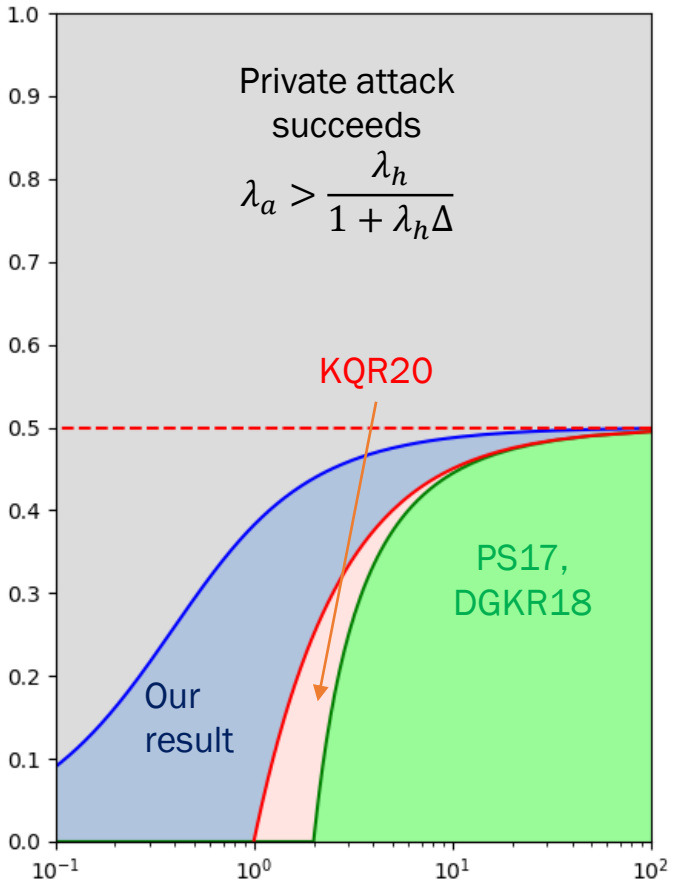


More results

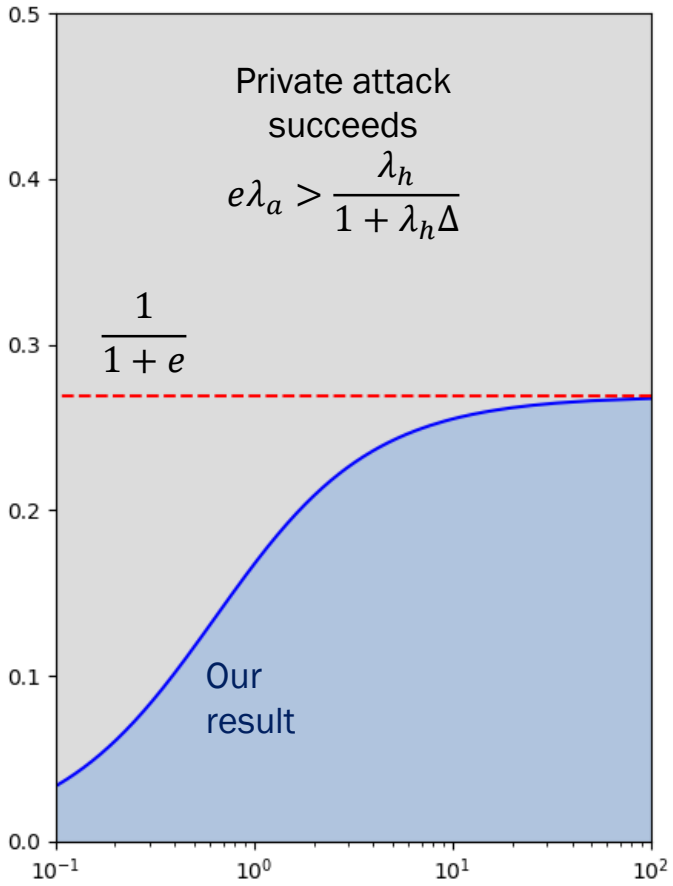
Proof-of-Work



Ouroboros/Sleepy



Chia Proof-of-Space

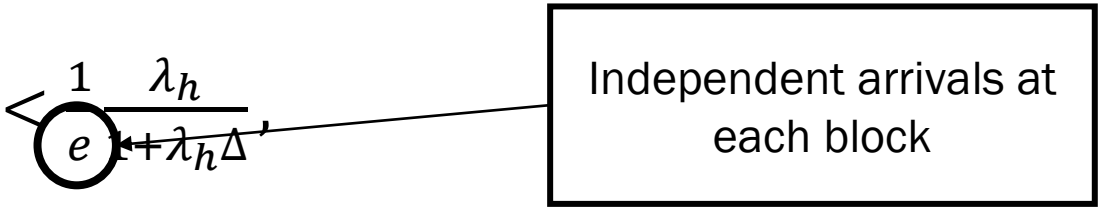


Main Theorems

- If $\lambda_a < \frac{\lambda_h}{1+\lambda_h \Delta}$,

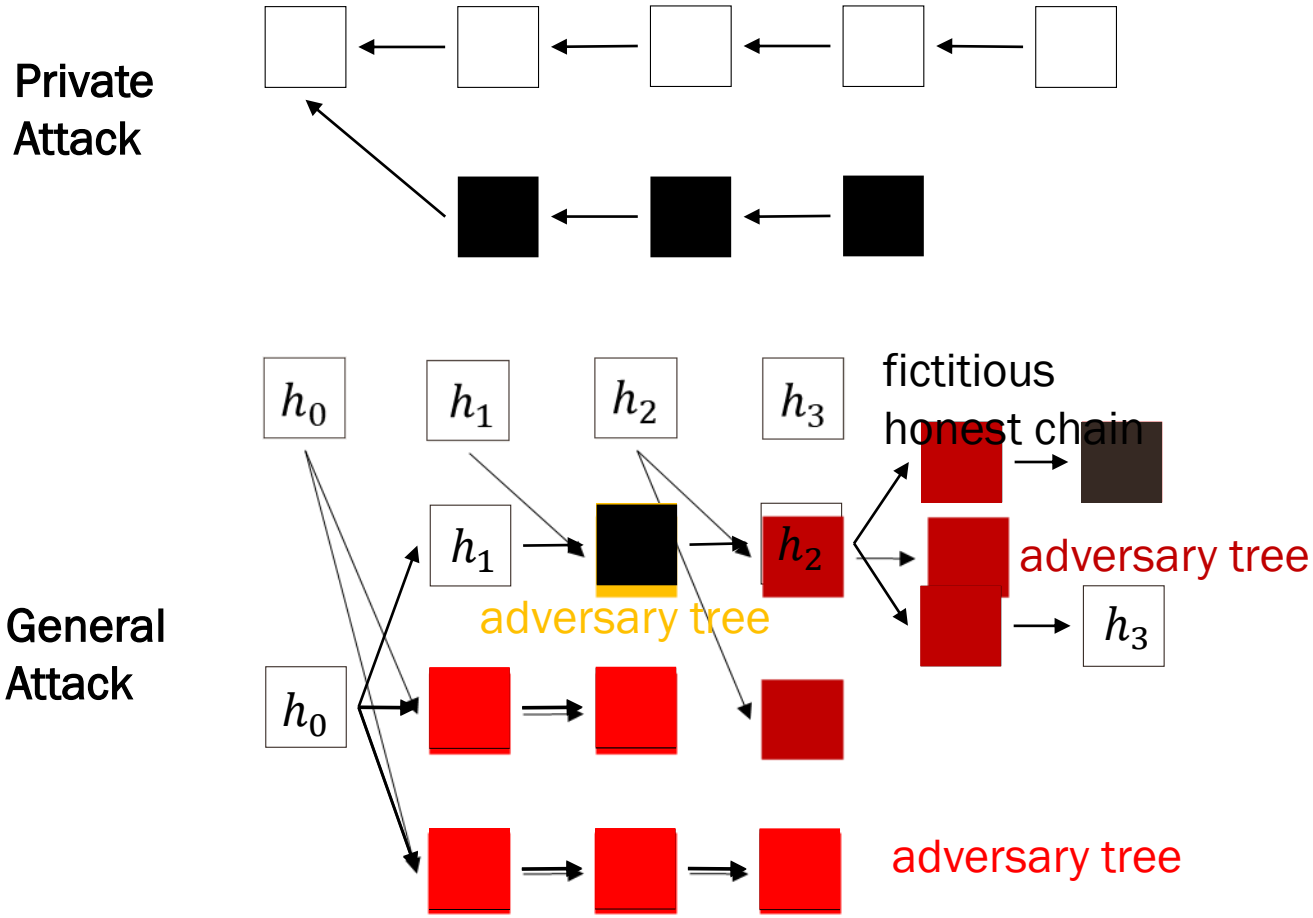
then the **Nakamoto Proof-of-Work** and the **Ouroboros/Sleepy Proof-of-Stake** protocols generate transaction ledgers such that each transaction *tx* satisfies safety and liveness (parameterized by σ) with probability at least $1 - e^{-\Omega(\sigma^{1-\varepsilon})}$, for any $\varepsilon > 0$.

- If $\lambda_a < \frac{1}{e} \frac{\lambda_h}{1+\lambda_h \Delta}$,

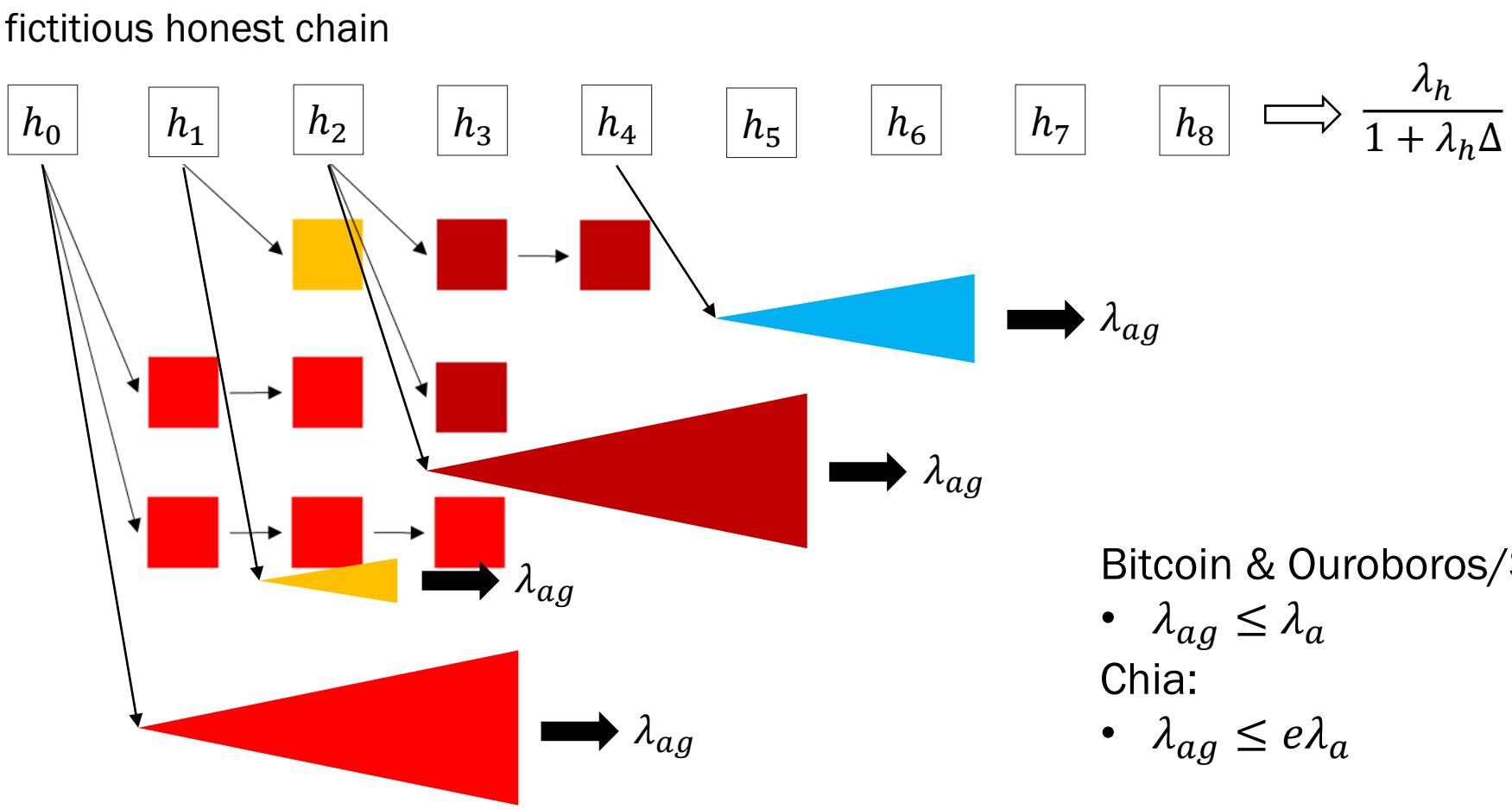


then the **Chia Proof-of-Space** protocol generates transaction ledgers such that each transaction *tx* satisfies safety and liveness (parameterized by σ) with probability at least $1 - e^{-\Omega(\sigma^{1-\varepsilon})}$, for any $\varepsilon > 0$.

Blocktree partitioning



Everything is a race



Bitcoin & Ouroboros/Sleepy:

- $\lambda_{ag} \leq \lambda_a$

Chia:

- $\lambda_{ag} \leq e\lambda_a$

And Nakamoto Always Wins

Nakamoto blocks stabilize its prefix!

Secure against private attack

$$\Downarrow$$

$$\frac{\lambda_h}{1+\lambda_h\Delta} > \lambda_{ag}$$

$$\Downarrow$$

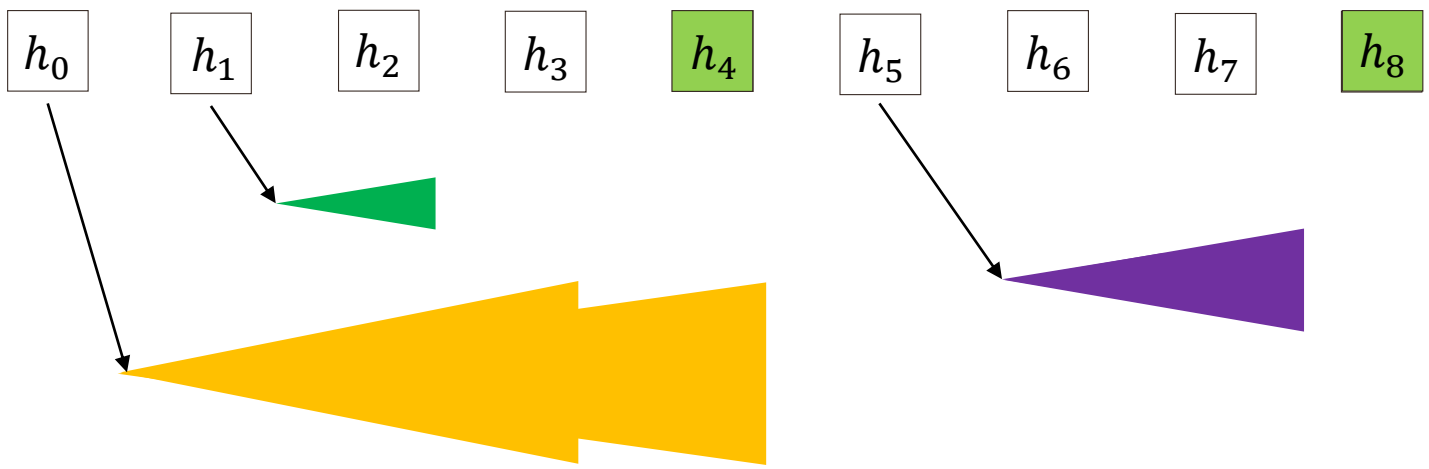
Nakamoto blocks exist and keep arriving.

$$\Downarrow$$

secure against all attacks

$$\Rightarrow \frac{\lambda_h}{1+\lambda_h\Delta}$$

fictitious honest chain



$$\Rightarrow \lambda_{ag}$$

Bitcoin & Ouroboros/SnowWhite:

- $\lambda_{ag} \leq \lambda_a$

Chia:

- $\lambda_{ag} \leq e\lambda_a$

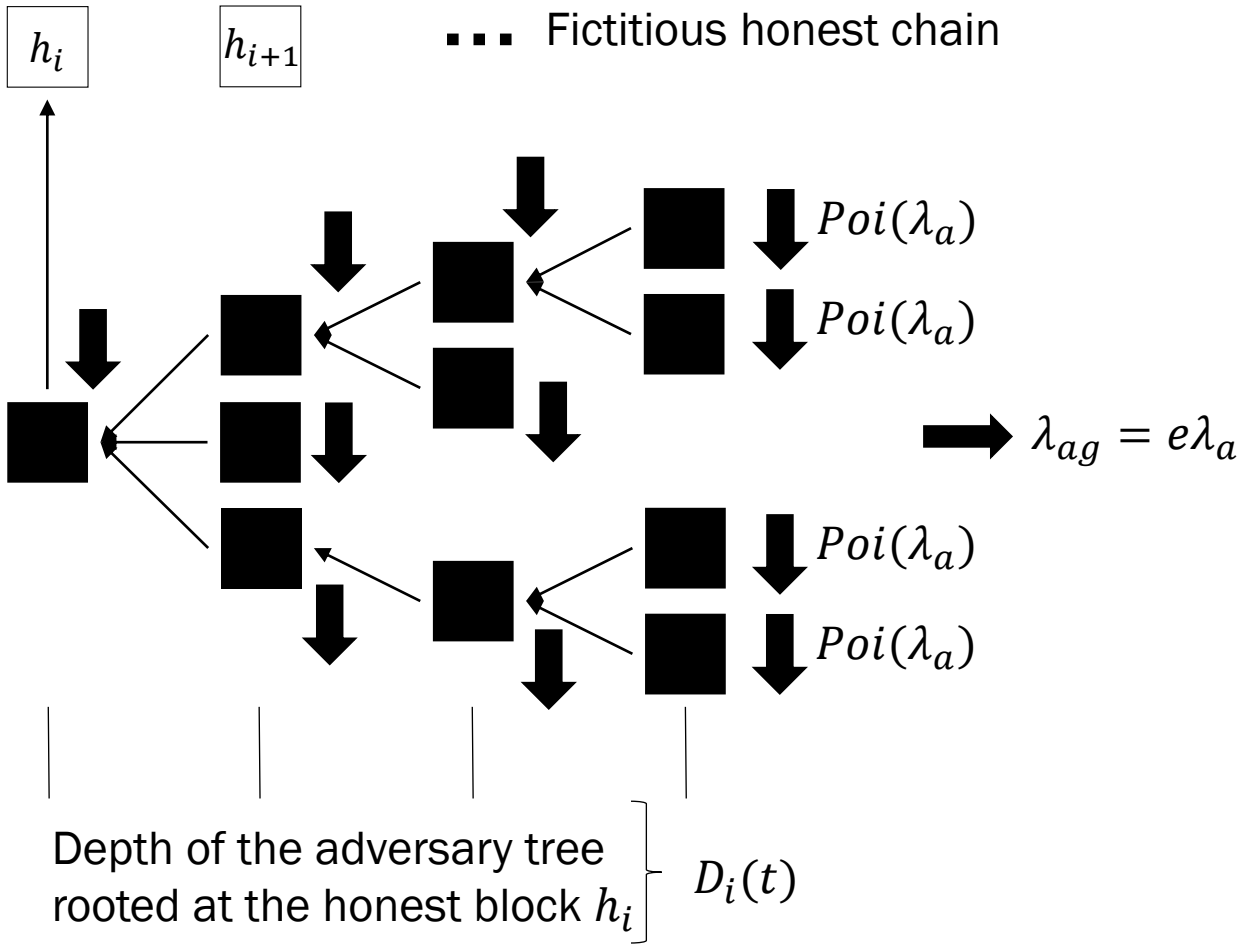
Other Methods

Method	Protocol	Work	Property
Backbone Analysis (block counting)	Nakamoto Proof-of-Work	GKL'15	First to show security for PoW, lock step round-by-round
Convergence Opportunities	Nakamoto Proof-of-Work	PSS'17	Tighter security for PoW, Δ-synchronous
Forkable Strings	Ouroboros Proof-of-Stake	KRDO'17, DGKR'18, BGK+'18, KQR'20	Tight security in the lock step round-by-round for PoS
Pivots	Sleepy/SnowWhite Proof-of-Stake	PS'17, BPS'16	Δ-synchronous
Blocktree Partitioning	**Any** longest chain protocol!	DKT'20	**Tight** security bound for PoW, PoS, PoSpace

Everything is a Race and Nakamoto Always Wins

https://arxiv.org/abs/2005.10484

Appendix: Branching Random Walk



Lemma: For $m \geq 1$, $P(D_i(t) \geq m) \leq \left(\frac{e\lambda_a t}{m}\right)^m$

Proof: (Branching Random Walk)

Appendix: Is private attack the worst attack?

In a statistical sense…

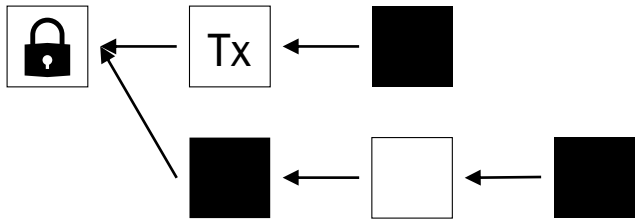
YES!

If the private attack fails, the protocol is secure with high probability.

In a deterministic sense…

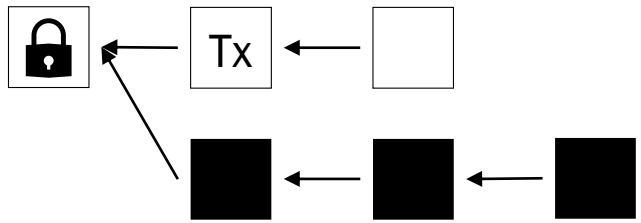
Only for the Proof-of-Work with network delay $\Delta = 0$.

Arbitrary Attack



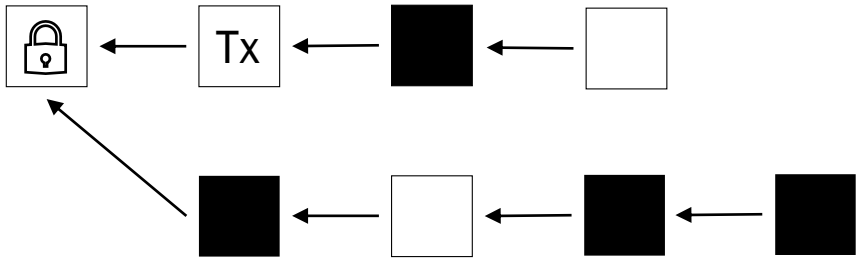
One honest block per level

Private Attack



Appendix: A Different Attack

k deep confirmation rule
(k =3)



Balance Attack succeeds!

Safety: Once Tx is k-deep, Tx stays as part of the longest chain.

Liveness: Longest chain contains honest blocks.