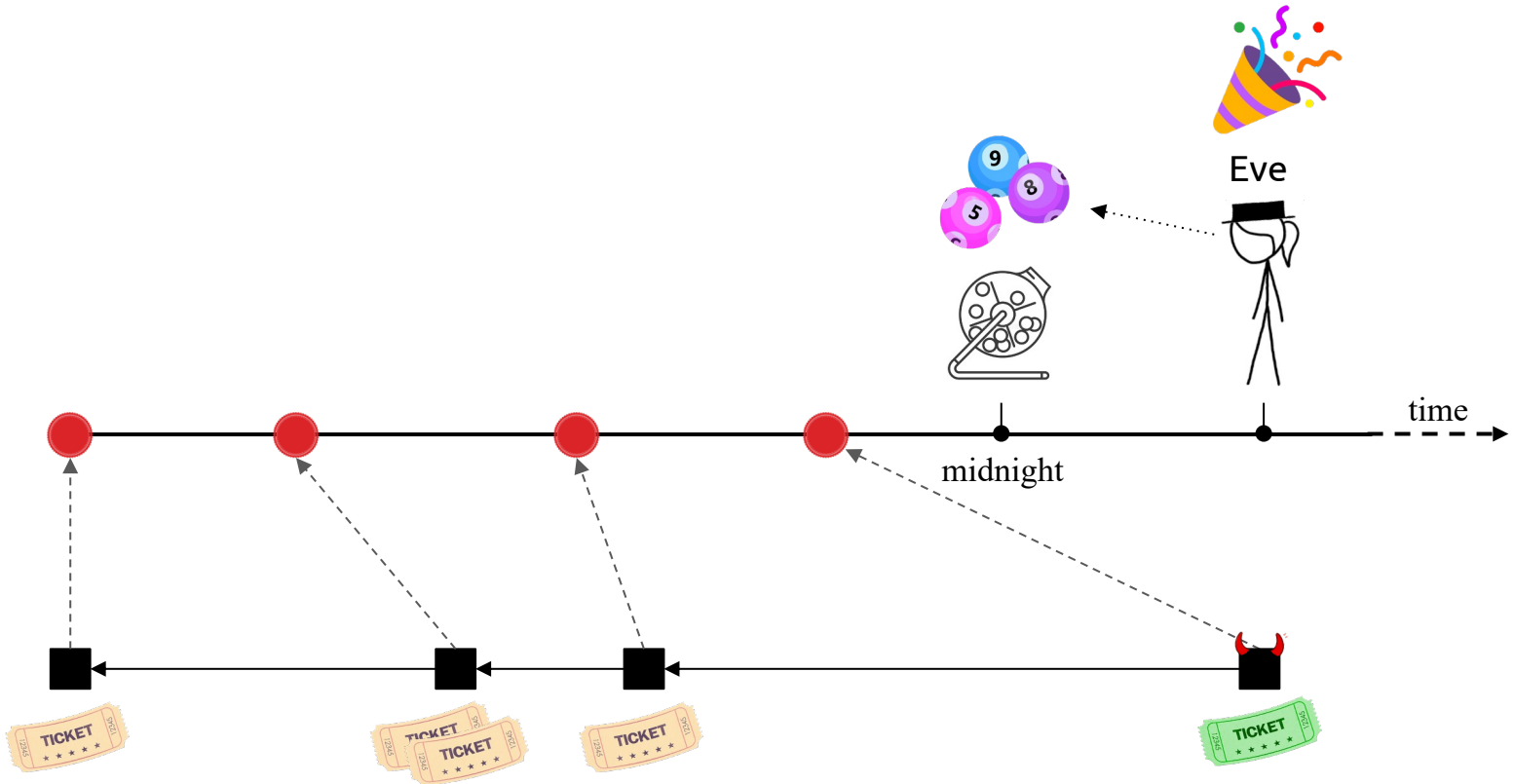
On-Chain Timestamps Are Accurate

Apostolos Tzinas, Srivatsan Sridhar, Dionysis Zindros



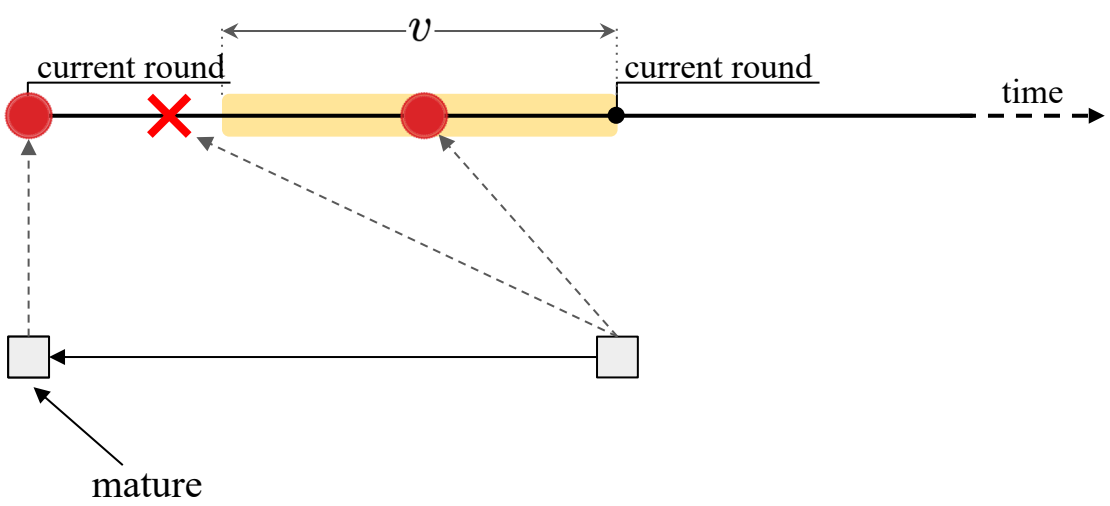
ATHECRYPT 2024

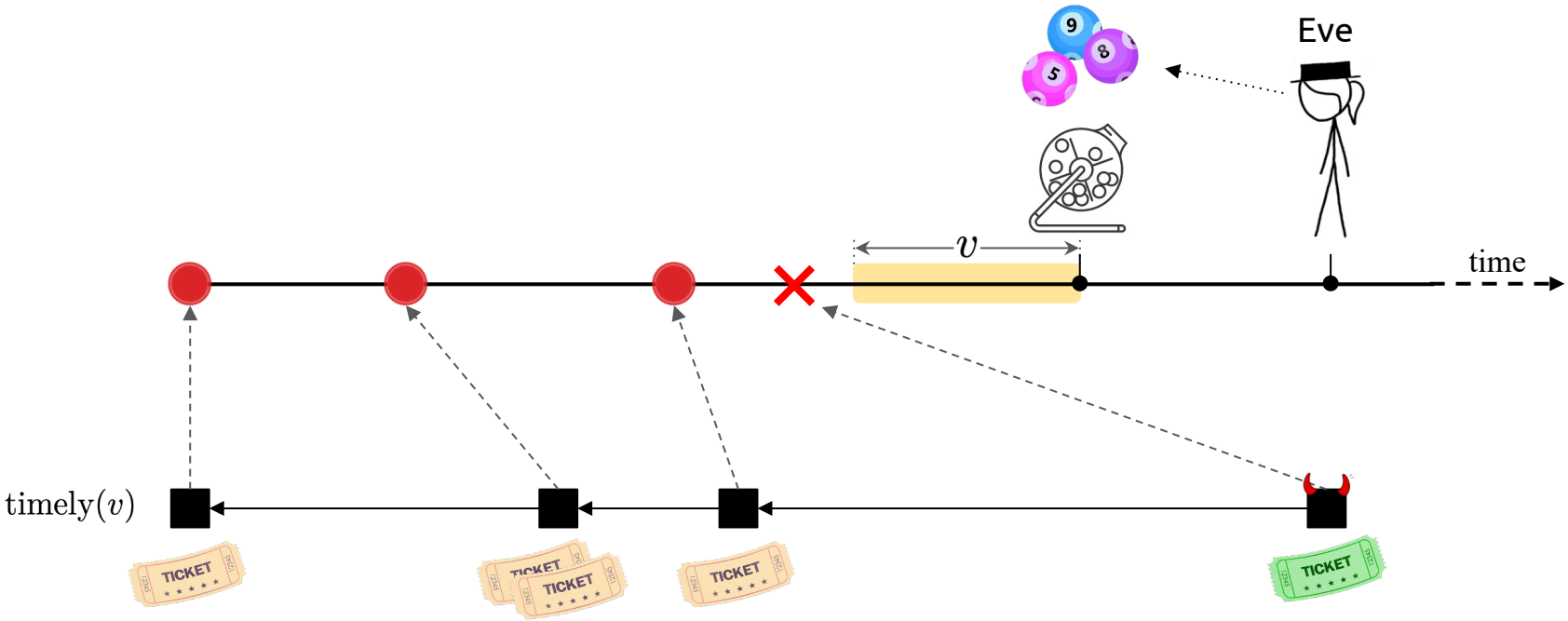
23 May 2024


Eve
time
midnight
TICKET
TICKET
TICKET
TICKET

Definition (Timeliness). *A blockchain protocol is* timely(v) *if for any honest party* P *and round* r*, the new blocks appearing in* P*'s stable chain at round* r *have timestamps between* $(r - v, r]$.

Timeliness(v).




Eve
v
time
timely(v)
TICKET
TICKET
TICKET
TICKET

Why timestamps?

- Block heights may be insufficient
- Timestamps tie the blockchain to the real world
- Universal clock.

Applications.

- Optimistic protocols with timestamp dispute periods.
- Multichain world.

CARDANO

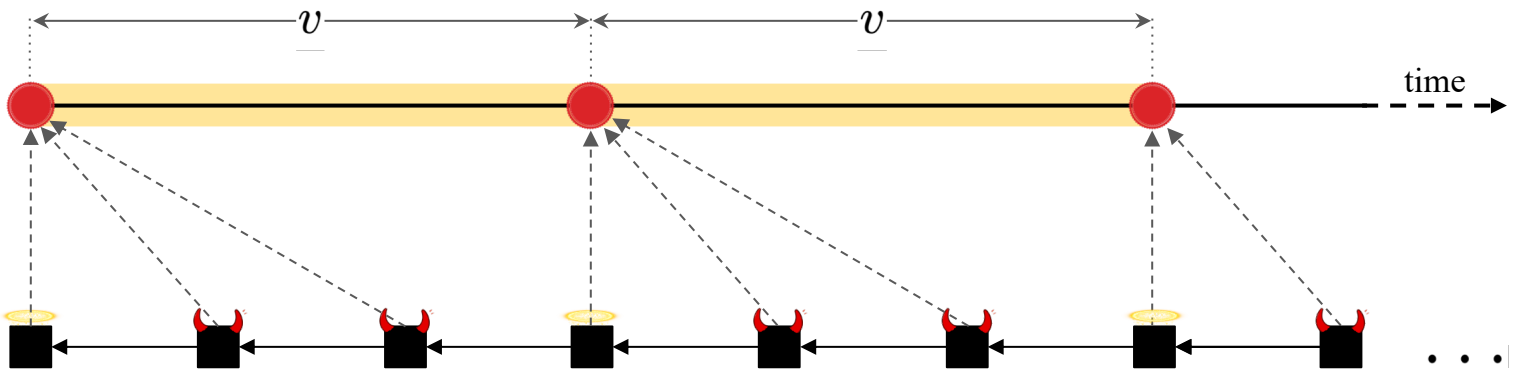
STREAMLET: Textbook Streamlined Blockchains

timely

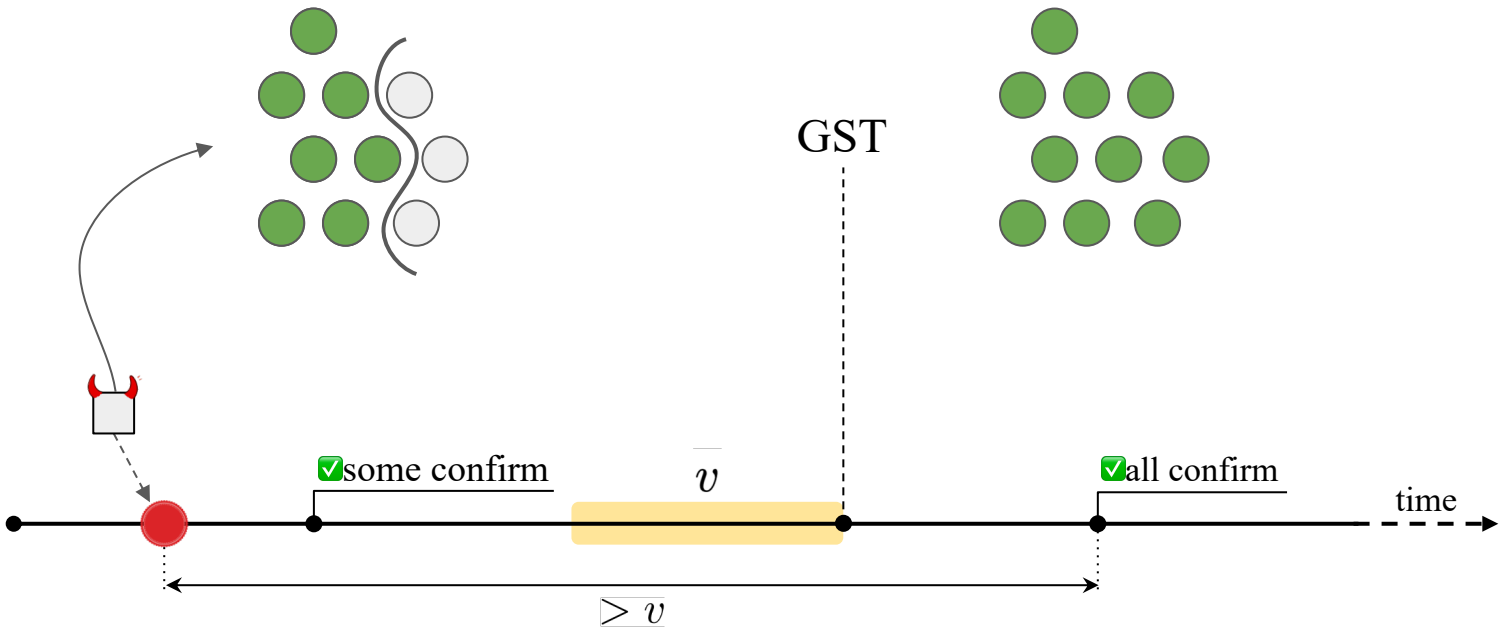
Synchronized clocks
&
Synchronous network

Theorem (Timeliness).

Proof. (Informal) Honest timestamps bound the timestamps that come after them.

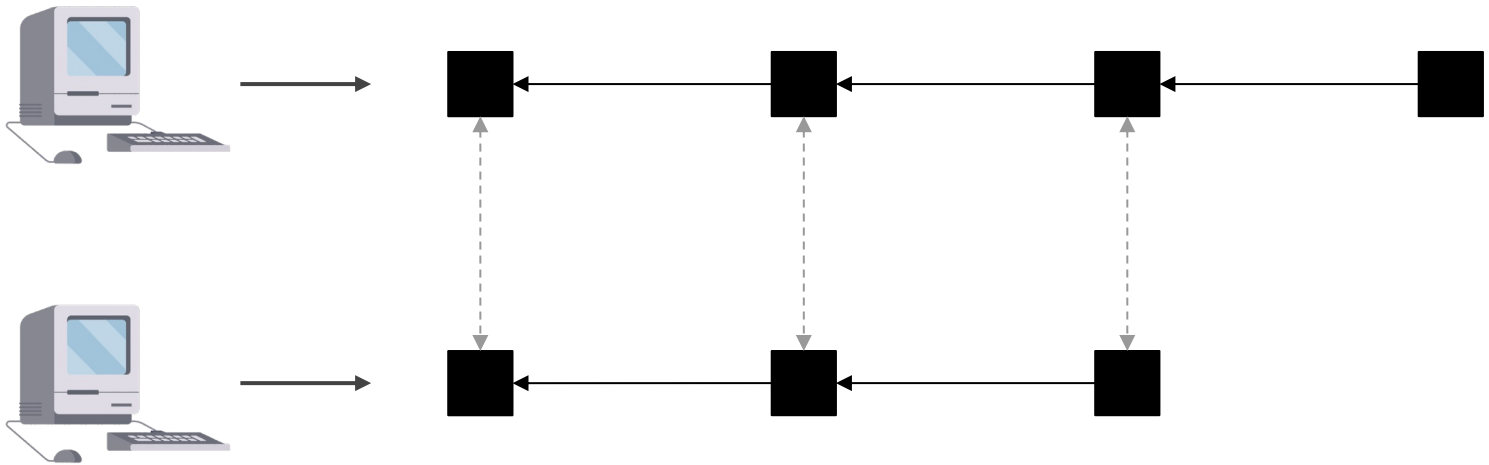


Timeliness is impossible before GST

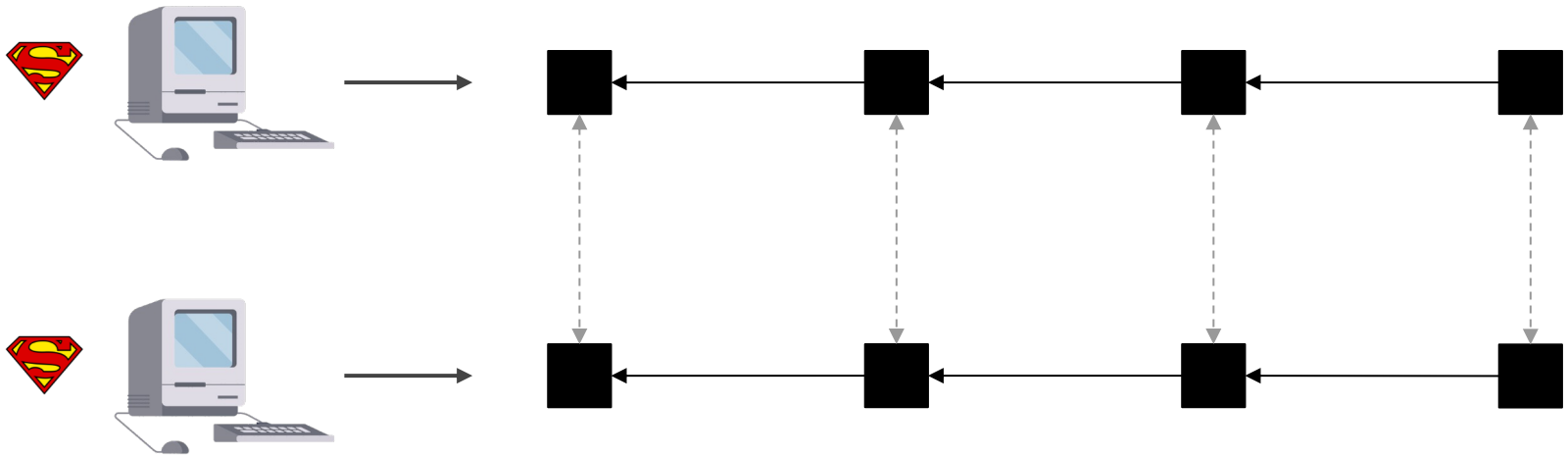


Definition (Supersafety). *A blockchain protocol is* supersafe *if all honest parties report the same stable chain at the same round.*

Safety.

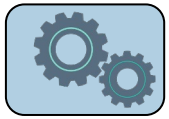


Supersafety.

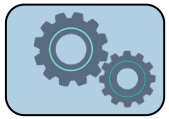


STREAMLET: Textbook Streamlined Blockchains

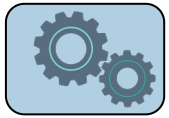
+



+



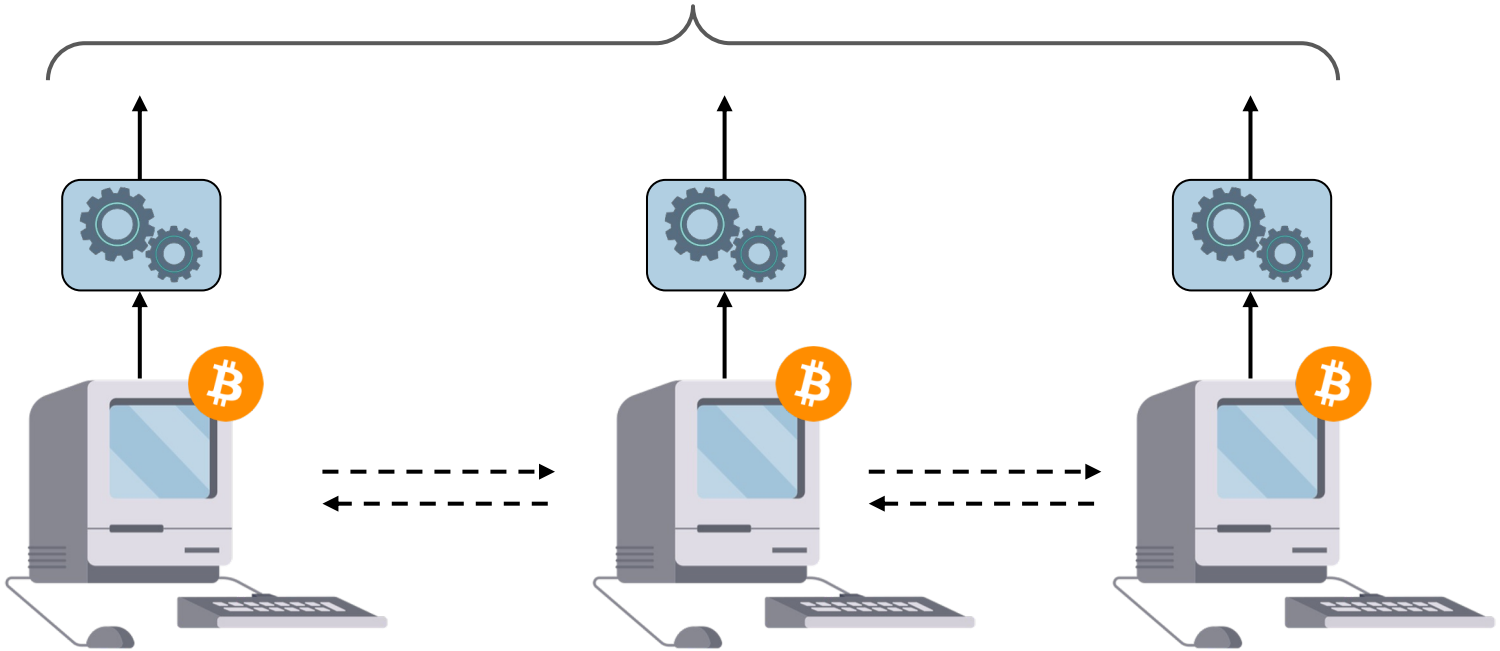
+



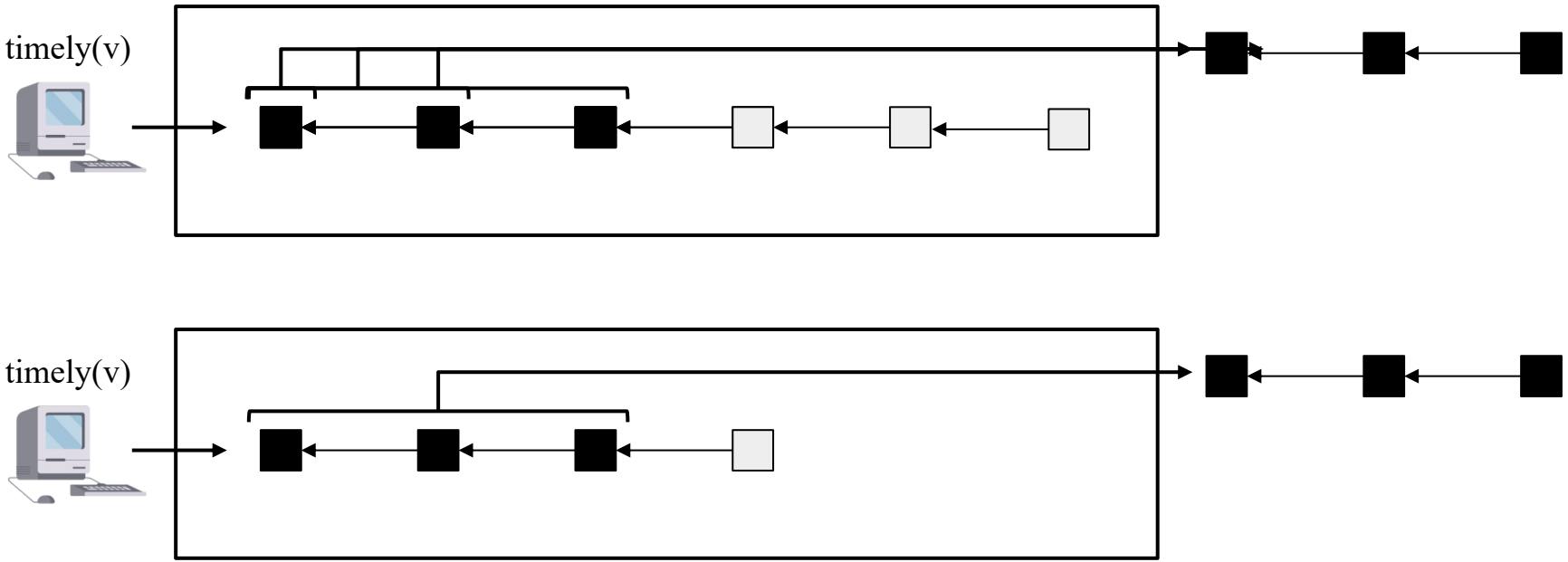
Supersafe

Synchronized clocks
&
Synchronous network

Supersafe



Timeliness → Supersafety



On-Chain Timestamps Are Accurate

- Deployed protocols rely on timestamp accuracy.
- **Timeliness** reflects timestamp accuracy.
- Popular blockchains are timely.
- Timeliness is impossible before GST.
- Timeliness → Supersafety

Questions?

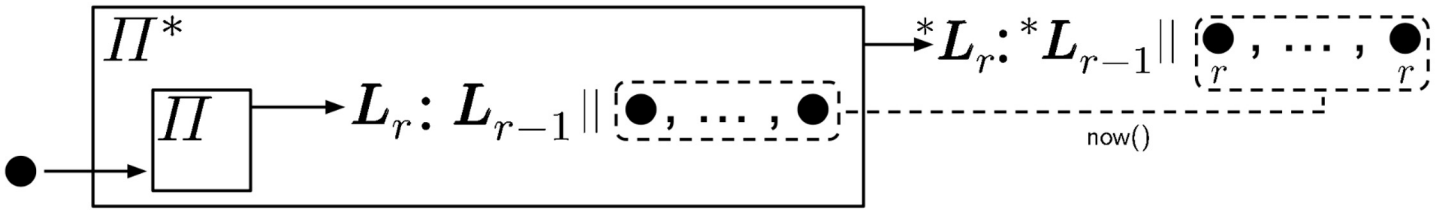


Fig. 7: The reduction from Supersafety (the Π protocol) to Perfect Timeliness (the Π^* protocol). New transactions of $\boldsymbol{L}_r$ are included in $^*\boldsymbol{L}_r$ with recorded round r.