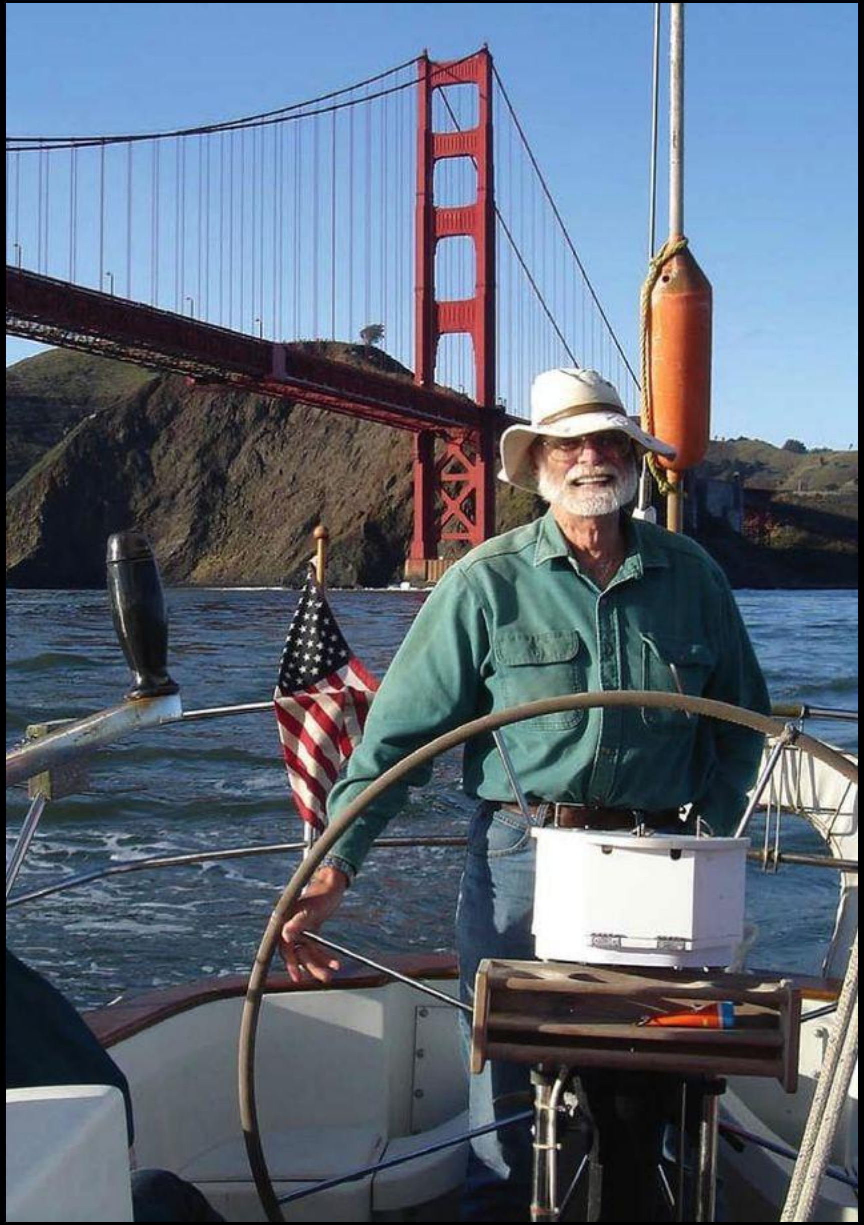
Paxos、PoW、VDF：a beautiful continuous

taoshengshi @ipfsforce

The Golden Line

What is distributed system?

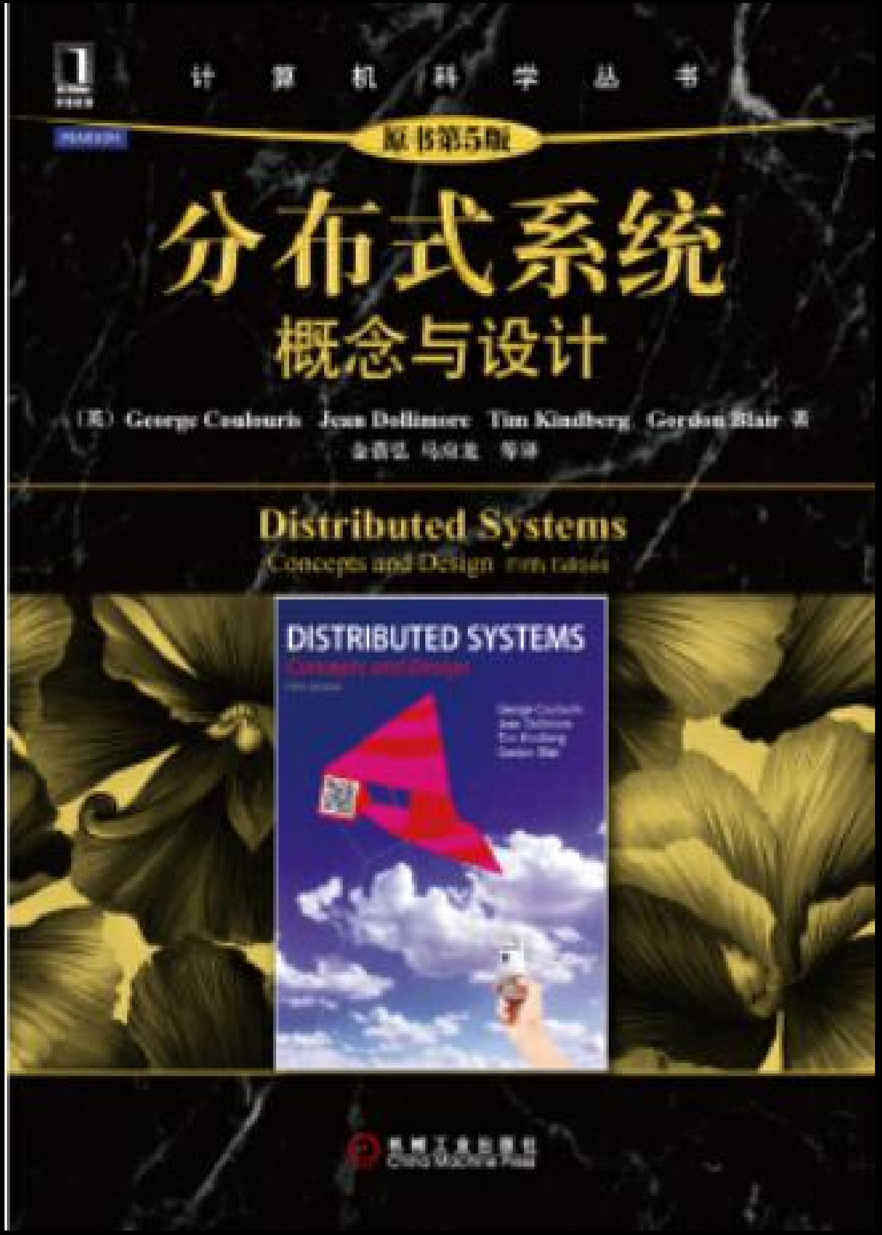
1. Turing award： Jim Gray
2. Distributed system vs Cluster
   - □ Homogeneity
   - □ Local
   - □ Trust



What is distributed system?

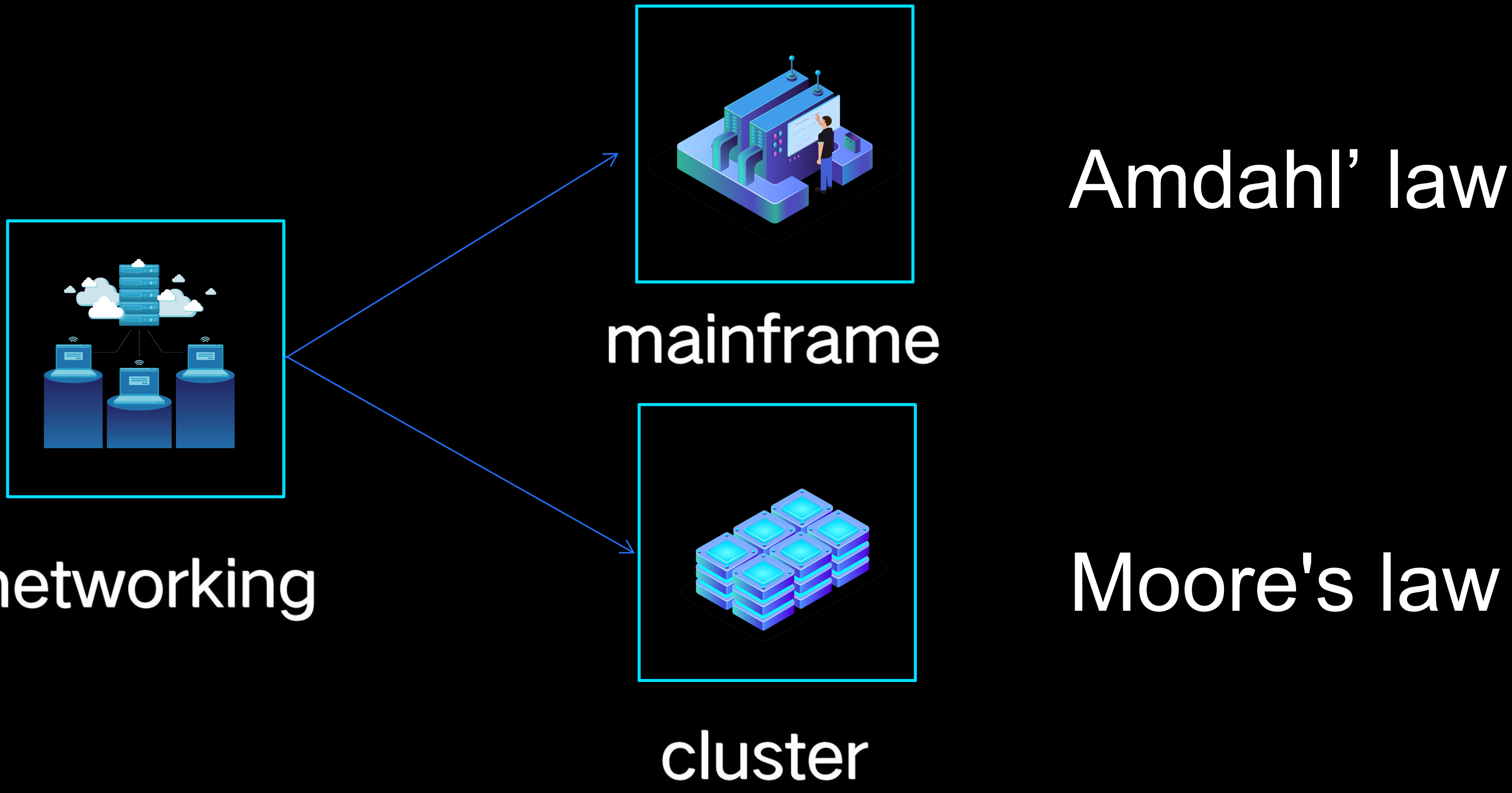
A distributed system is one in which components located at networked computers communicate and coordinate their actions only by passing messages.

——《DISTRIBUTED SYSTEMS Concepts and Design》 5th



Paxos thirty years:
Non-Byzantine fault tolerance

networking with laws



networking

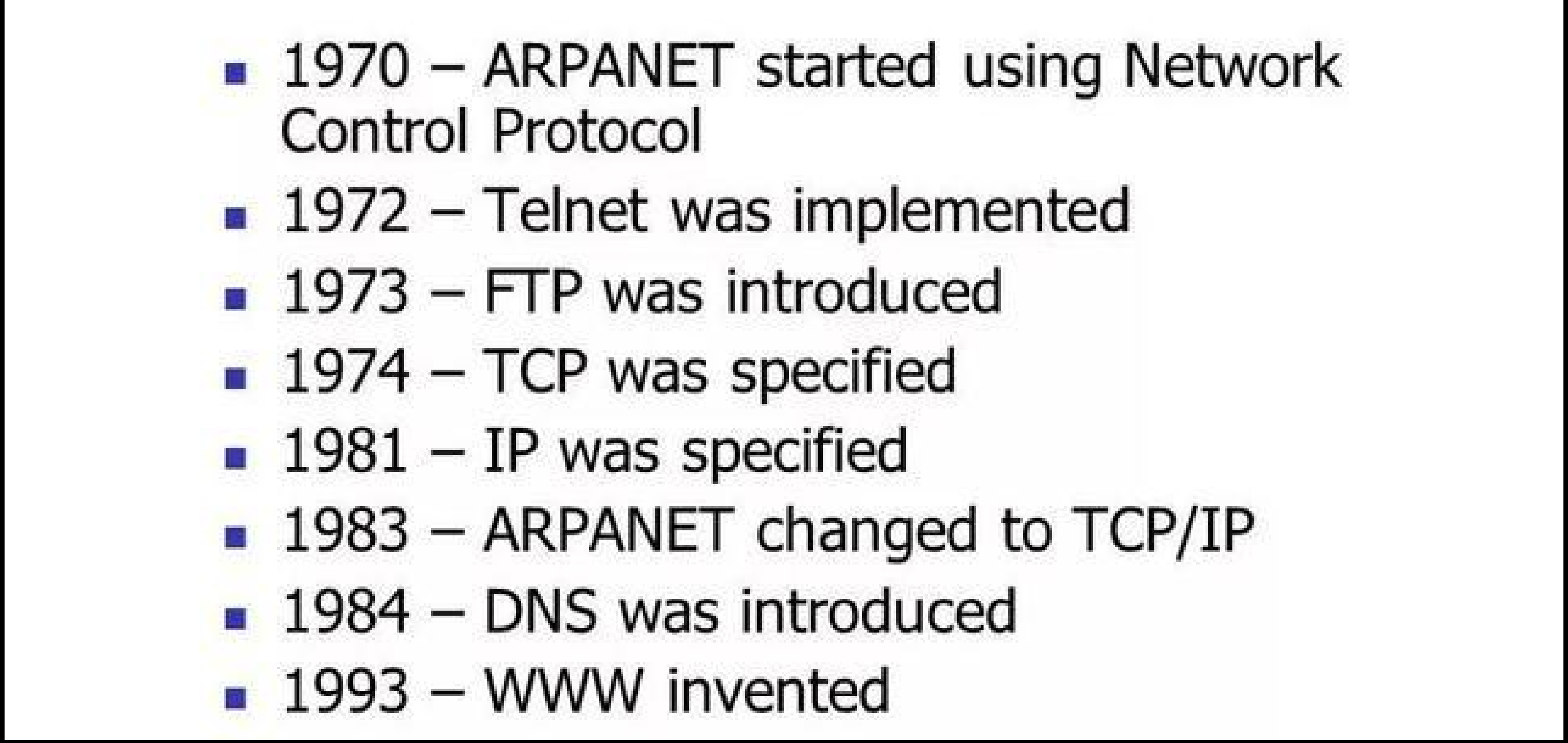
mainframe

Amdahl’ law

cluster

Moore's law

brief history of networking

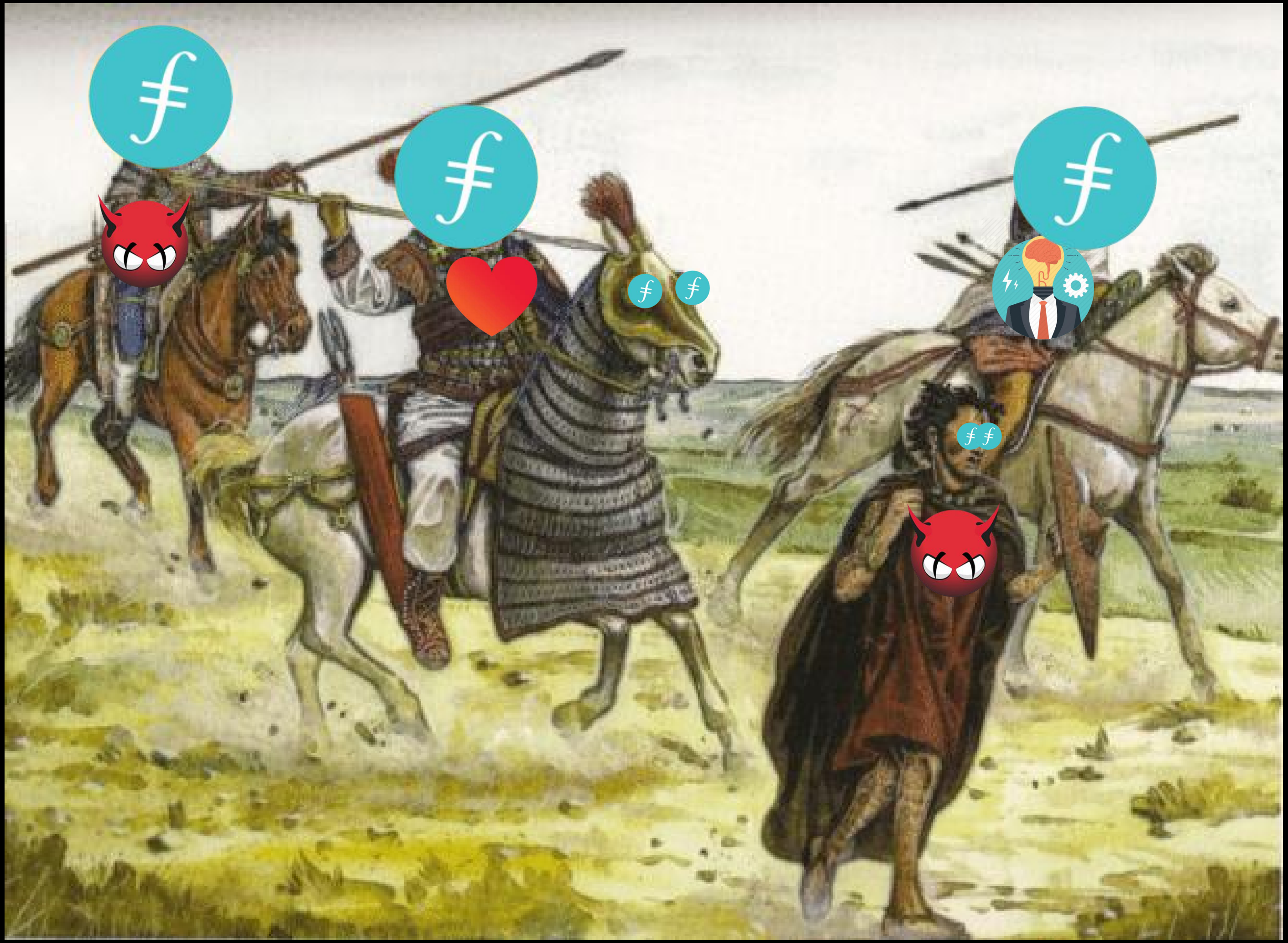


- 1970 – ARPANET started using Network Control Protocol
- 1972 – Telnet was implemented
- 1973 – FTP was introduced
- 1974 – TCP was specified
- 1981 – IP was specified
- 1983 – ARPANET changed to TCP/IP
- 1984 – DNS was introduced
- 1993 – WWW invented

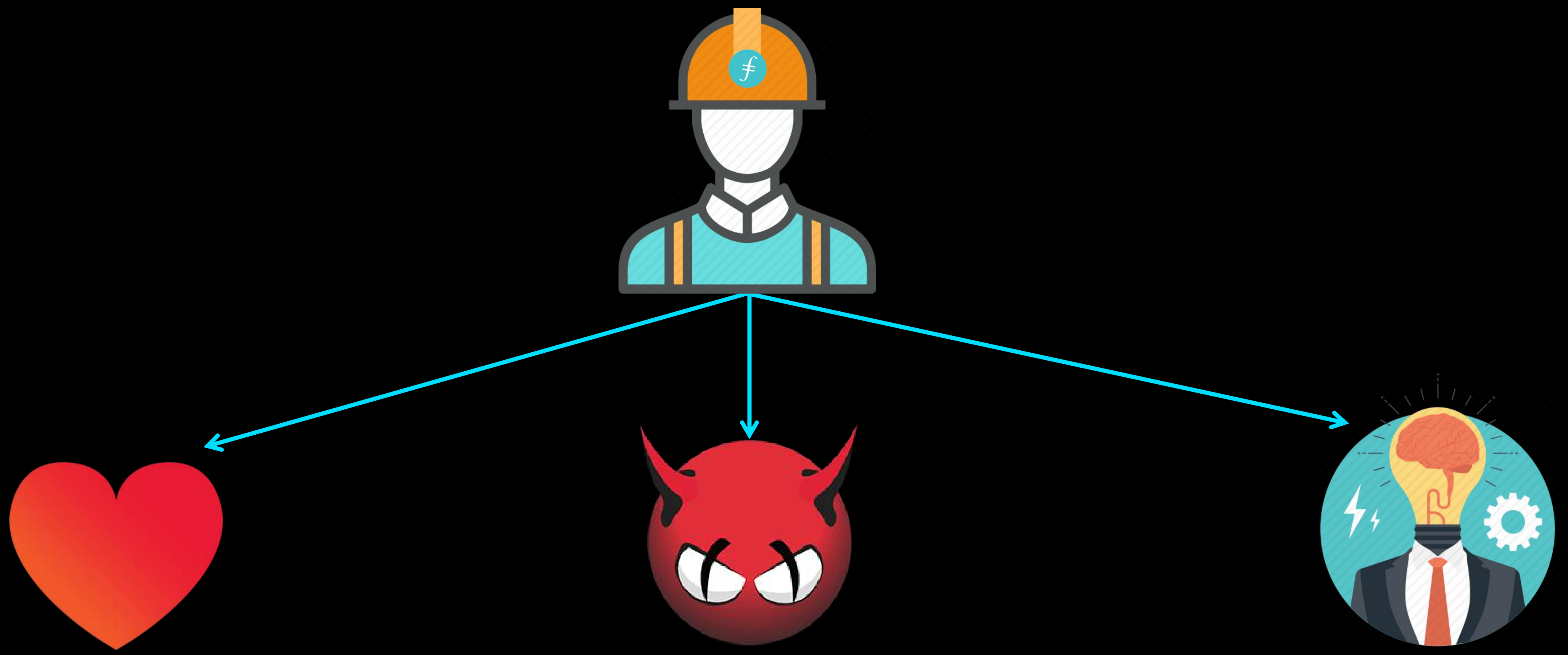
history of Paxos

1. 1978 - **Two Generals Paradox in** 《Notes on Data Base Operating Systems》 Leslie Lamport
2. 1978 - 《Time, Clocks, and the Ordering of Events in a Distributed System》 Leslie Lamport
3. 1982 - 《The Byzantine Generals Problem》 Leslie Lamport
4. 1985 - 《Impossibility of Distributed Consensus with One Faulty Process》 Fischer, Lynch and Patterson
5. 1989 - 《The Part-time Parliament》 Leslie Lamport

The Byzantine Generals Problem



The Byzantine Generals Problem in blockchain



honest
诚实节点

malicious
恶意节点

rational
理性节点

Leslie Lamport

conclusion

1. The theoretical solution vs the ngineering solution

   理论解 vs 工程解

1. The theory is ahead of its time, but it needs to be tested by engineering.

   理论领先于时代，但需要等待工程的检验。

1. If not now, when?

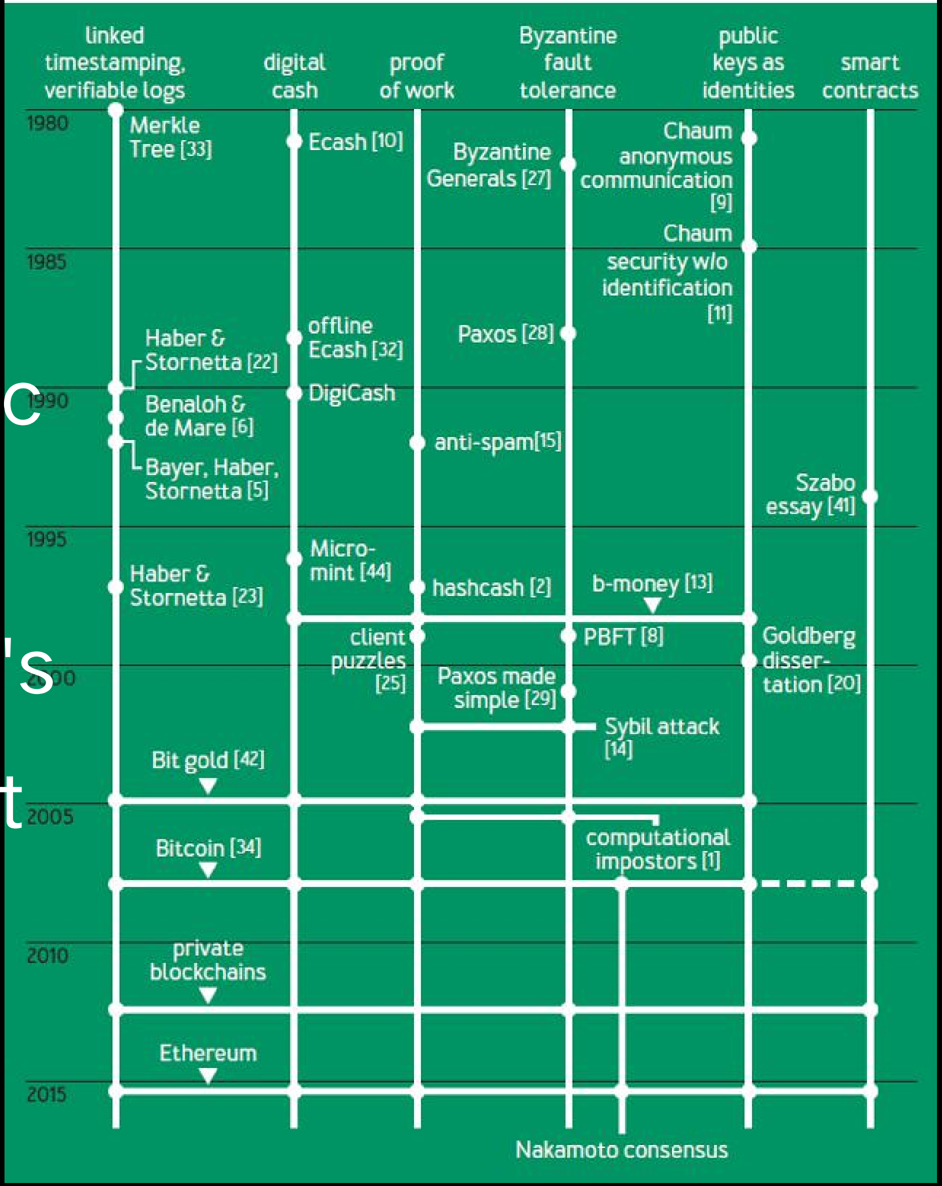
   此时此刻，恰如彼时彼刻

PoW ten years：
Byzantine Consensus

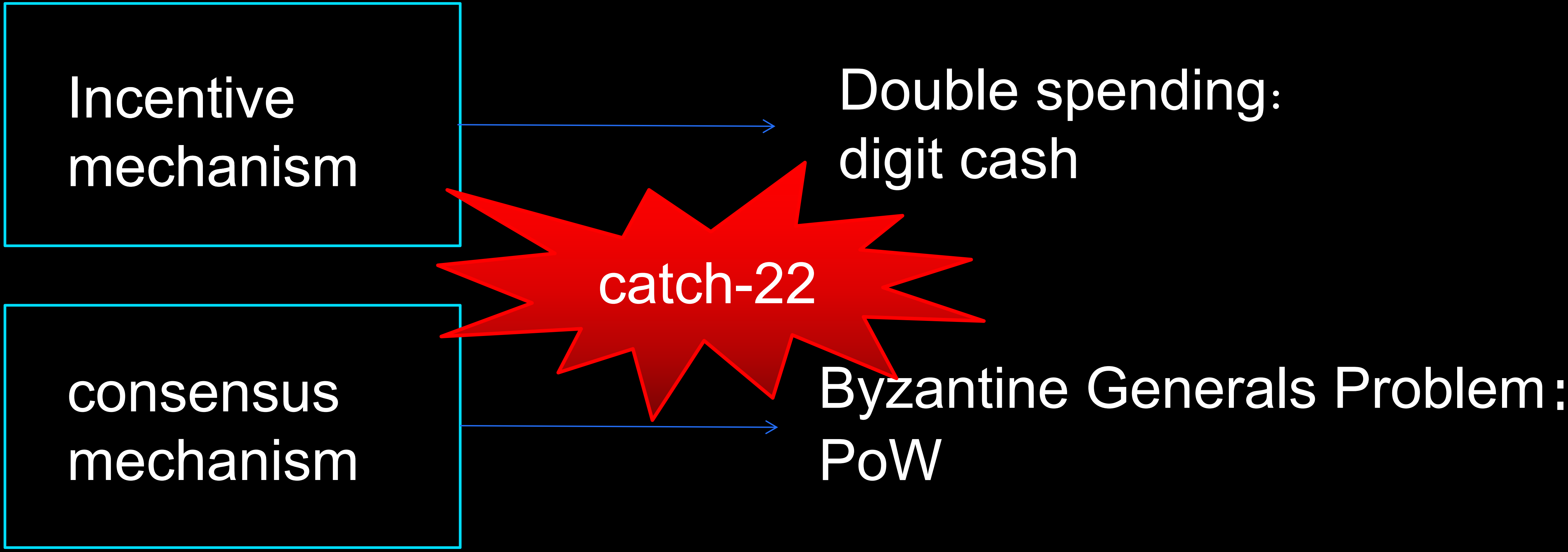
Nakamoto's bitcoin

1. the technical components of bitcoin originated in the academic literature of the 1980s and '90s
2. This is not to diminish Nakamoto's achievement but to point out that he stood on the shoulders of giants.

FIGURE 1: CHRONOLOGY OF KEY IDEAS FOUND IN BITCOIN



bitcoin of catch-22



Incentive mechanism

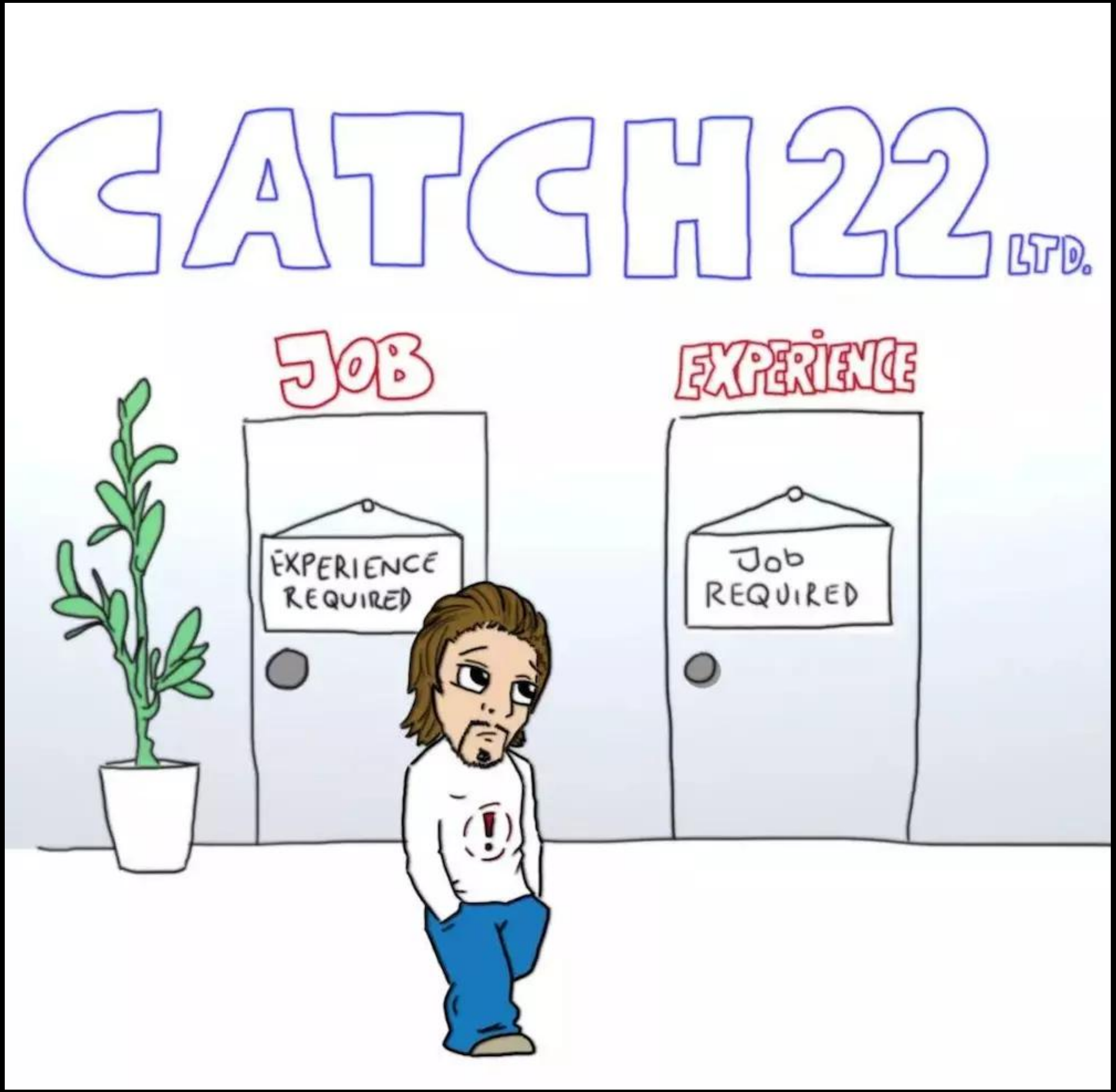
Double spending：digit cash

catch-22

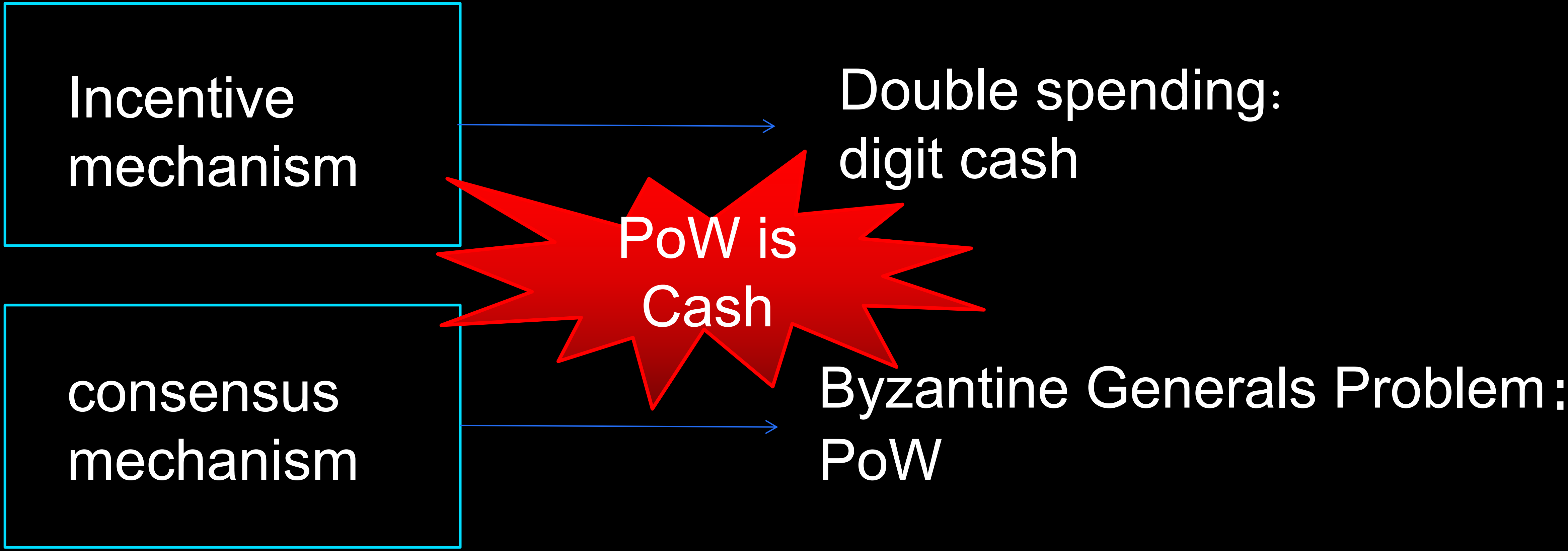
consensus mechanism

Byzantine Generals Problem：PoW

catch-22


CATCH 22 LTD.
JOB
EXPERIENCE
EXPERIENCE REQUIRED
JOB REQUIRED

Nakamoto's crude solution



Incentive mechanism

Double spending：digit cash

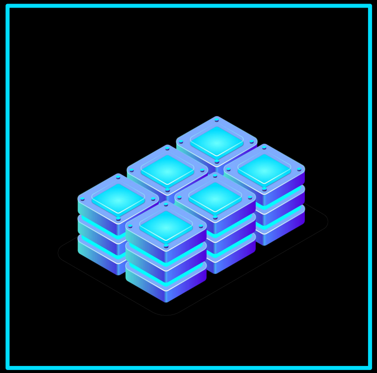
PoW is Cash

consensus mechanism

Byzantine Generals Problem：PoW

PoW conclusion

self bootstrapped



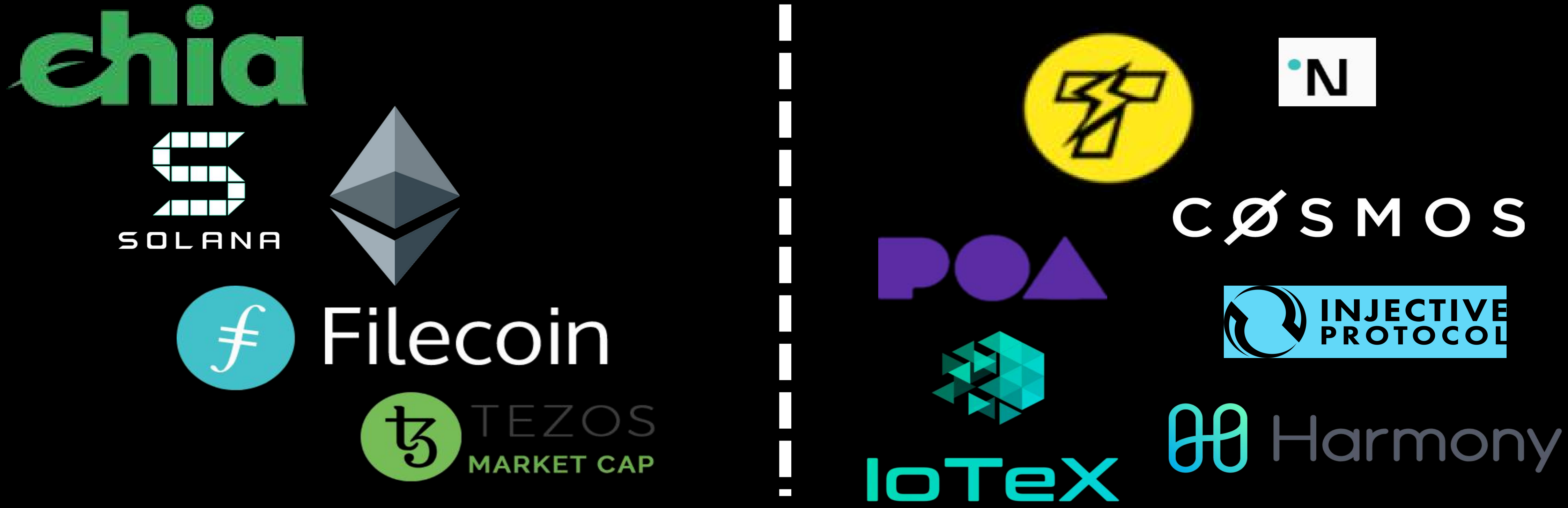
parallel

VDF: future is comming

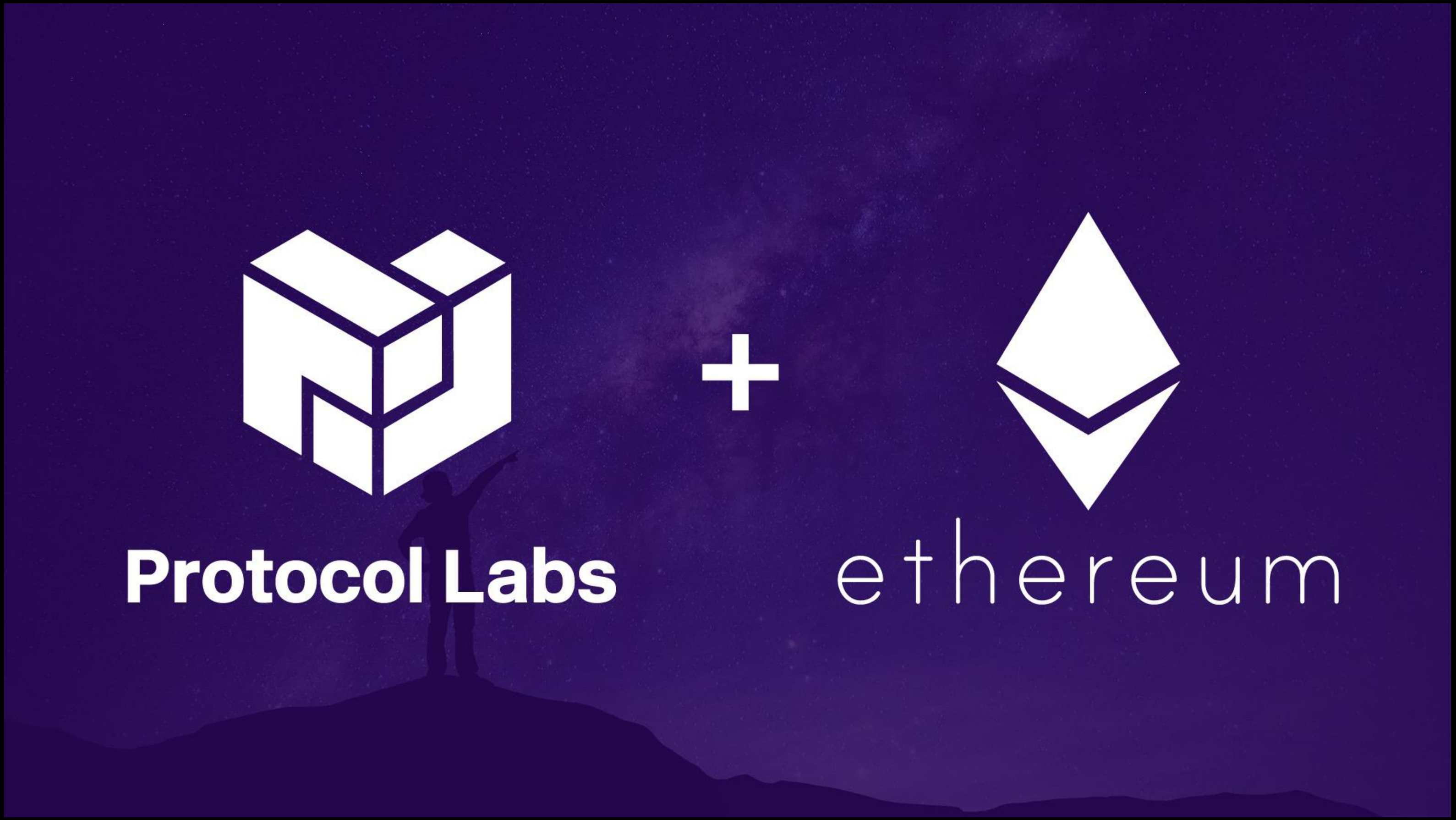
Five papers from June 2018

1. “Verifiable Delay Functions”—Boneh, Bonneau, Bünz, Fisch
2. “Efficient Verifiable Delay Functions”—Wesolowski
3. “Simple Verifiable Delay Functions”—Pietrzak
4. “A Survey of Two Verifiable Delay Functions”—Boneh, Bünz, Fisch
5. “Verifiable Delay Functions from Supersingular Isogenies and Pairings”—De Feo, Masson, Petit, Sanso

blockchain interest



VDF project management



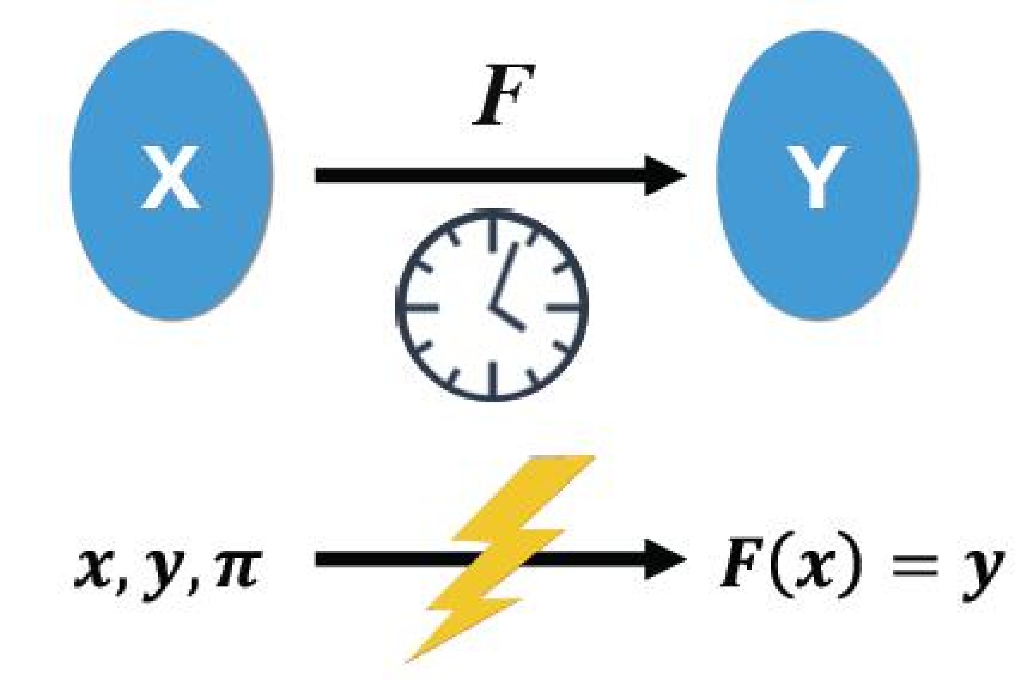
VDF project management

SUPRA
NATIONAL

VDF project management

What is VDF?

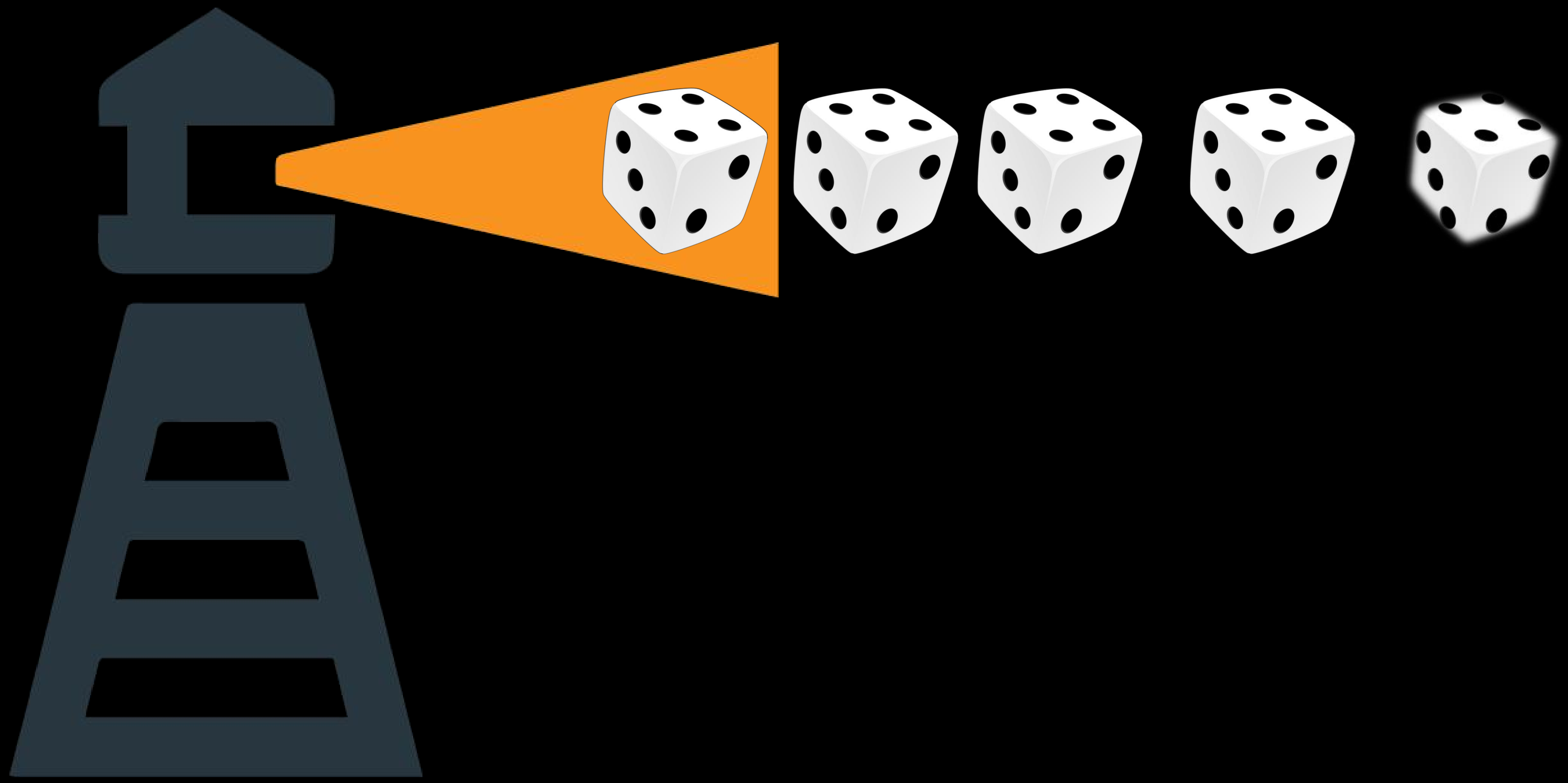
- ❑ Function:
  - unique output for every input
- ❑ Delay:
  - can be evaluated in time T
  - can not be evaluated in time <T on parallel
- ❑ Verifiable:
  - correctnees of output can be verified efficiently



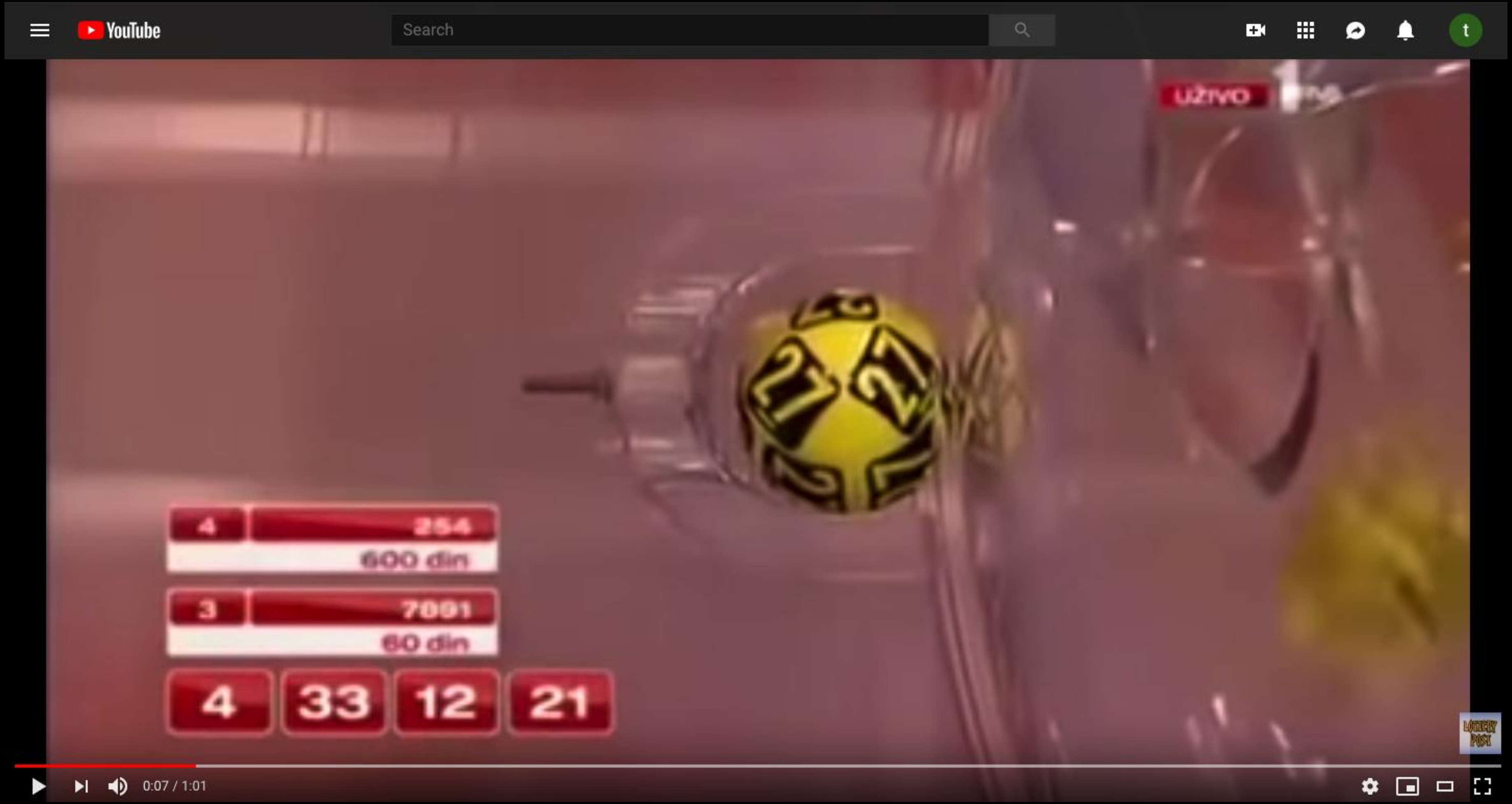
VDF in Filecoin

- ❑ Perhaps more importantly, the design and development of a secure and usable VDF construction would be a major breakthrough in applied cryptography and distributed systems, with applicability even beyond blockchains.

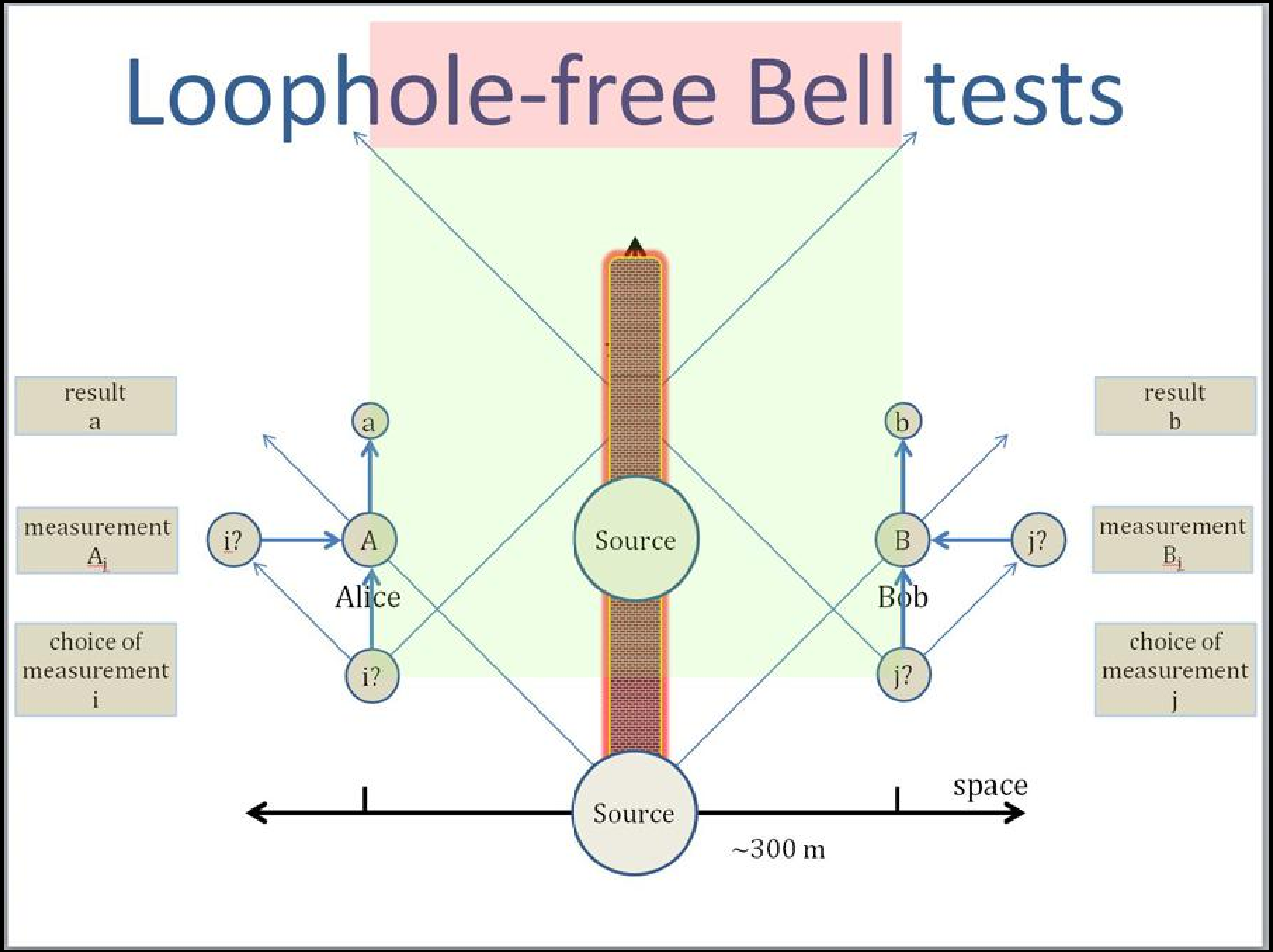
Randomness beacon



2015 Serbian lottery



NIST beacon

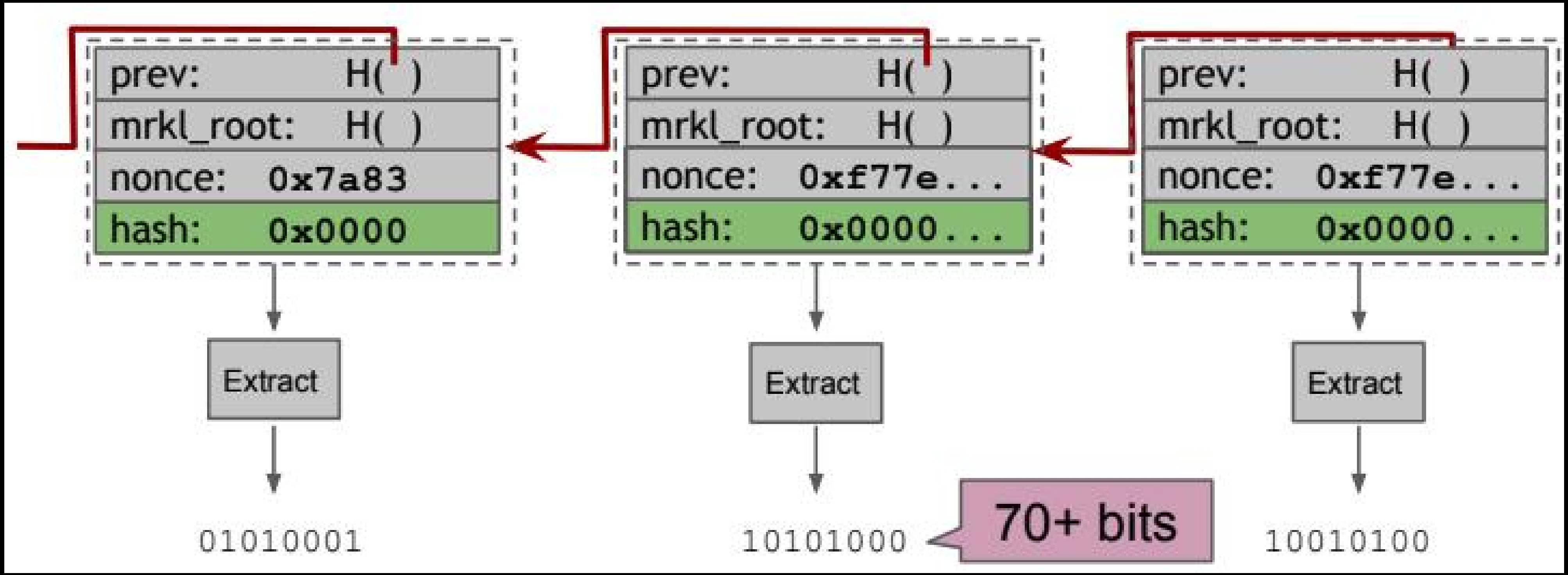


Loophole-free Bell tests

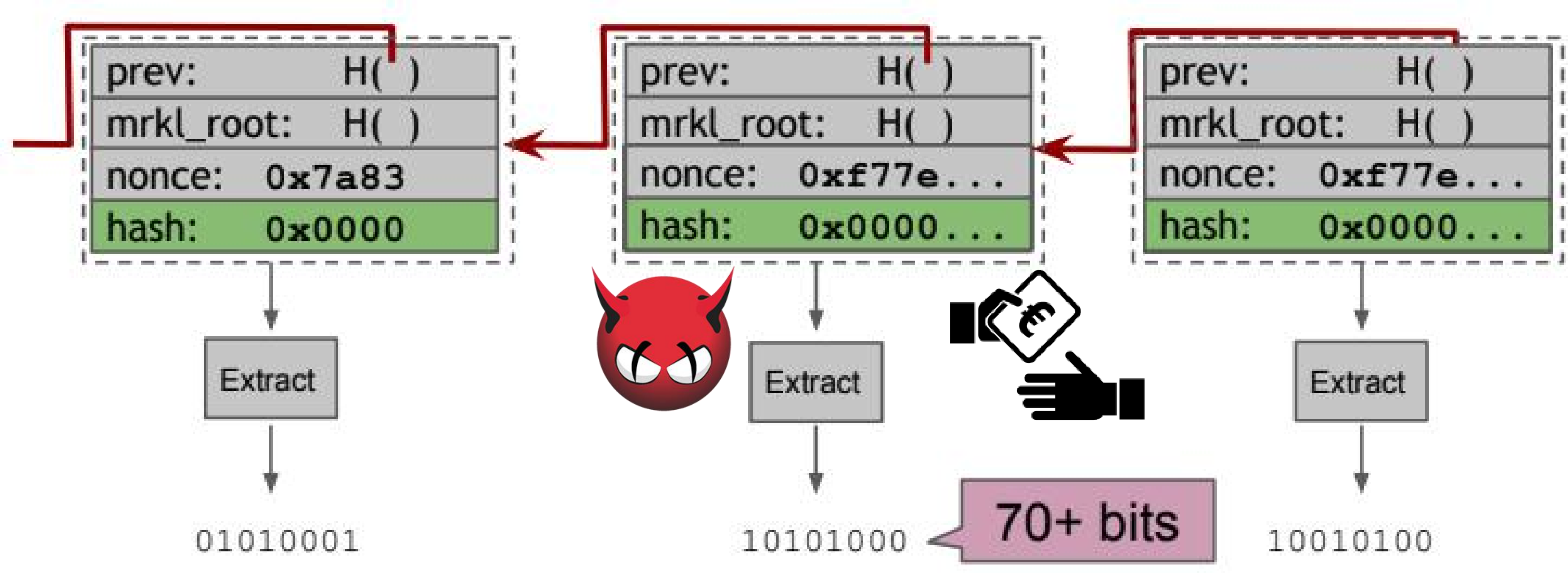
natural phenomena

Sun spots
Weather
Cosmic background radiation

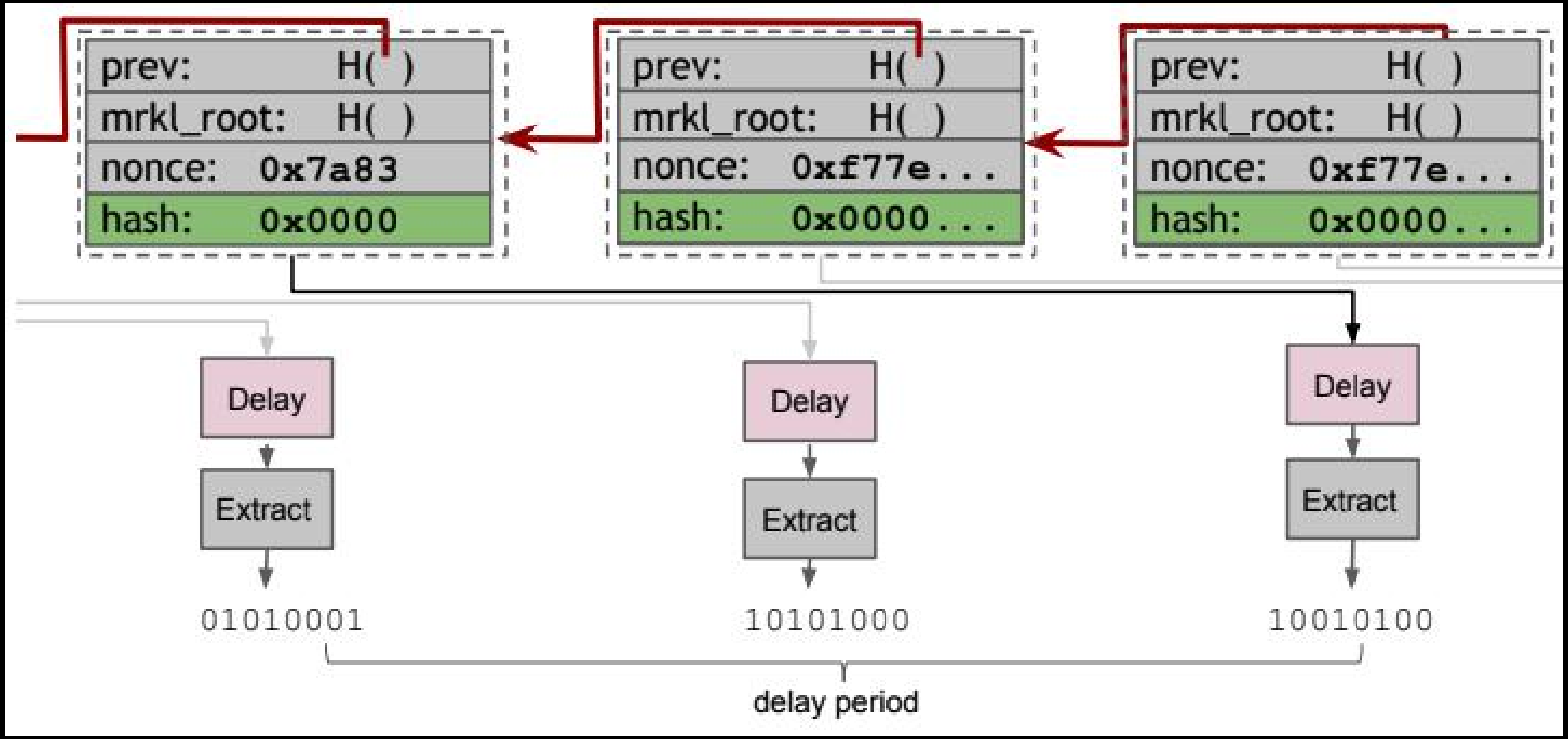
bitcoin beacon



problem


prev: H( )
mrkl_root: H( )
nonce: 0x7a83
hash: 0x0000
Extract
01010001
prev: H( )
mrkl_root: H( )
nonce: 0xf77e...
hash: 0x0000...
Extract
10101000
70+ bits
prev: H( )
mrkl_root: H( )
nonce: 0xf77e...
hash: 0x0000...
Extract
10010100

solution


prev: H( )
mrkl_root: H( )
nonce: 0x7a83
hash: 0x0000
prev: H( )
mrkl_root: H( )
nonce: 0xf77e...
hash: 0x0000...
prev: H( )
mrkl_root: H( )
nonce: 0xf77e...
hash: 0x0000...
Delay
Extract
01010001
Delay
Extract
10101000
Delay
Extract
10010100
delay period

VDF project management

LIGERO

Proof of Spacetime

challenge seed

Proof of Spacetime

time delay

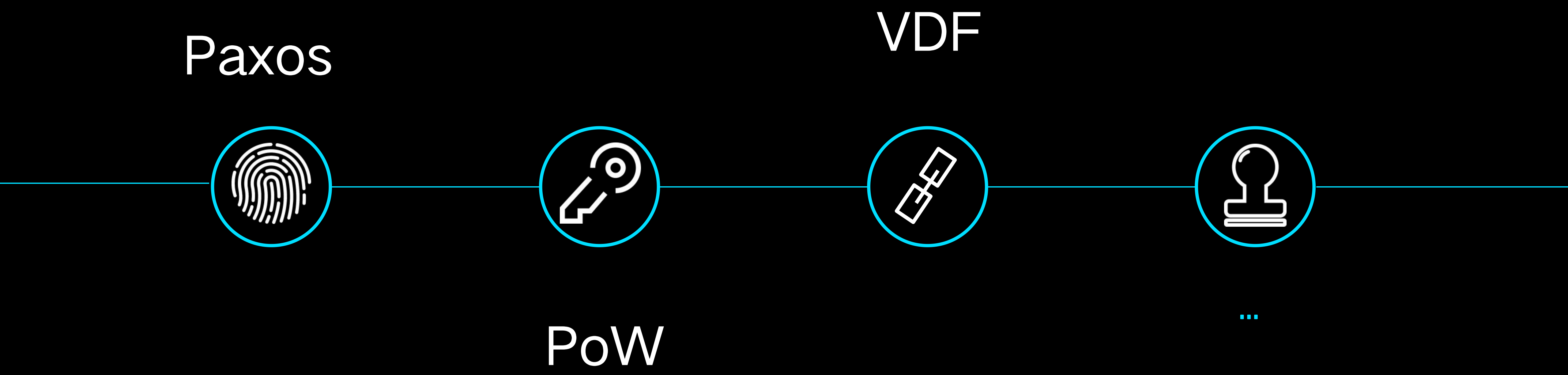
Proof of Spacetime

time delay

Proof of Spacetime

consensus from any proof of resource

beautiful continuous



Paxos

PoW

VDF

...

thank you!

The Golden Line