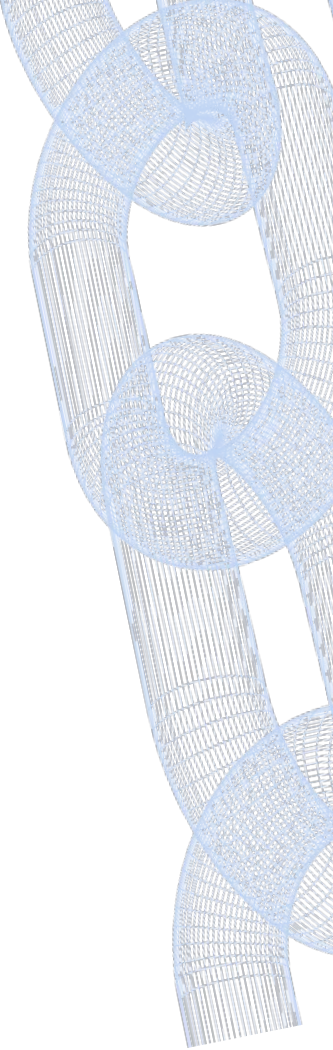
Streamlet:

A Textbook Blockchain Protocol

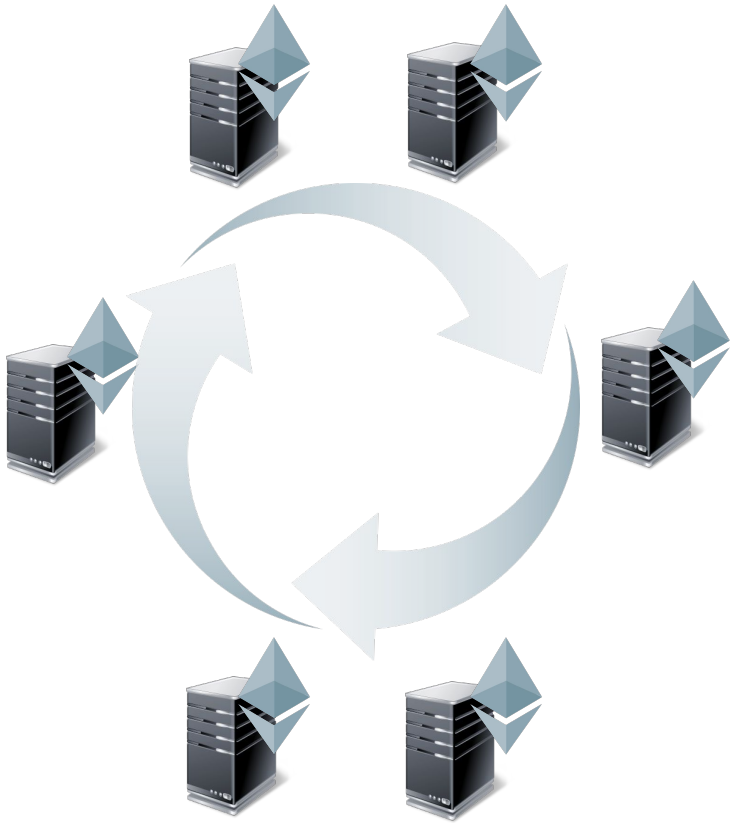
Elaine Shi

Joint work with Benjamin Chan



Blockchain

(a.k.a. state machine replication, consensus)

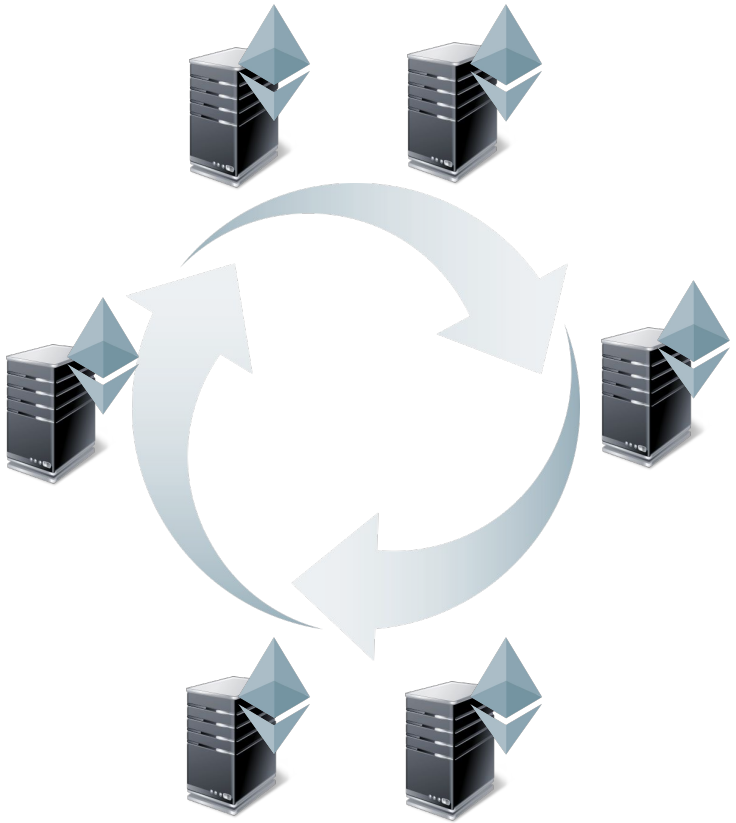


Blockchain

(a.k.a. state machine replication, consensus)

Consistency:
Honest nodes agree on log

Liveness:
TXs are incorporated soon



Blockchain: A 30-year-old Problem

YAHOO!

facebook

reddit

Apache Zookeeper

Solr

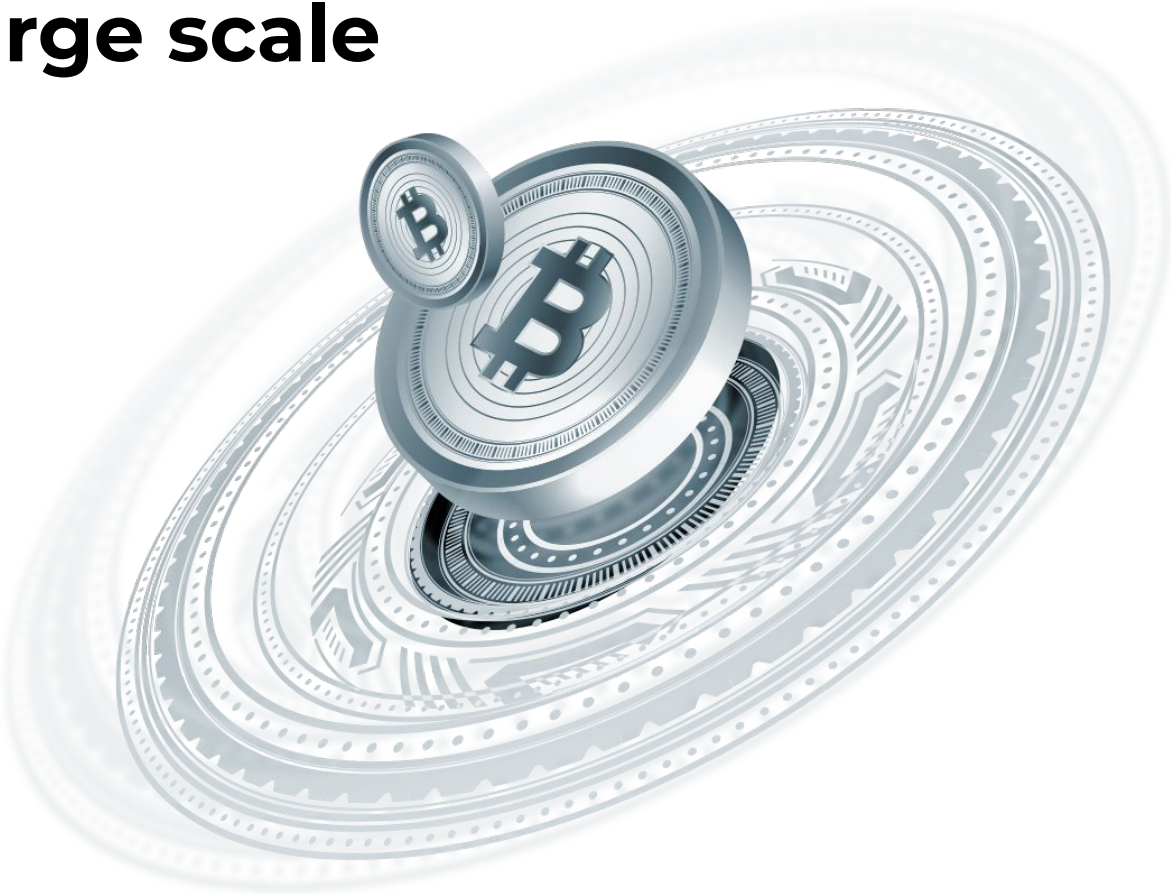
UBER

ebay

rackspace

NetApp

Cryptocurrencies brought consensus to a large scale



Proof of work

Enabled **permissionless** consensus

Proof of work

Proof of work

Proof of stake

parity

Rely on **permissioned** consensus

Proof of work

Proof of stake

parity

Consensus landscape 10 years ago

Complex
Difficult to understand
Error-prone to implement

"Paxos Made Moderately Complex"
[ACM Computing Surveys'15]

"Paxos Made Simple"

"The ABCDs of Paxos" [PODC'01]

"RAFT: In search of an understandable consensus algorithm" [Usenix ATC'14]

... ...

c.f. **Theoretical approach:** sequential/parallel composition of Byzantine Agreement

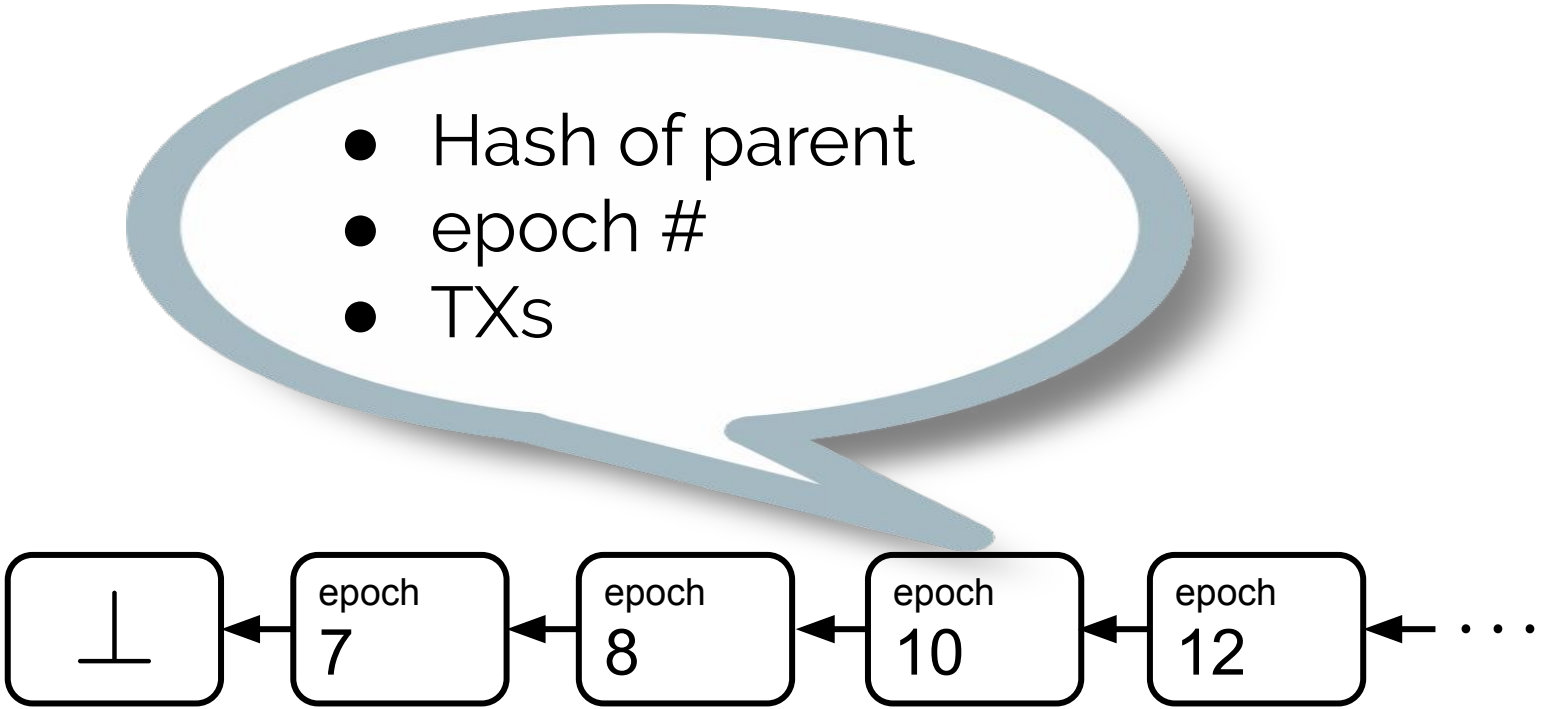
Streamlet

 Simple

 Natural

 Unified, for pedagogy & implementation

Block Format and Epoch



Streamlet

★ Assume: all msgs signed

★ **Notarized block**: voted by **2/3** processes

★ **Notarized chain**: all blocks notarized

In every epoch e

- **leader(e)**:

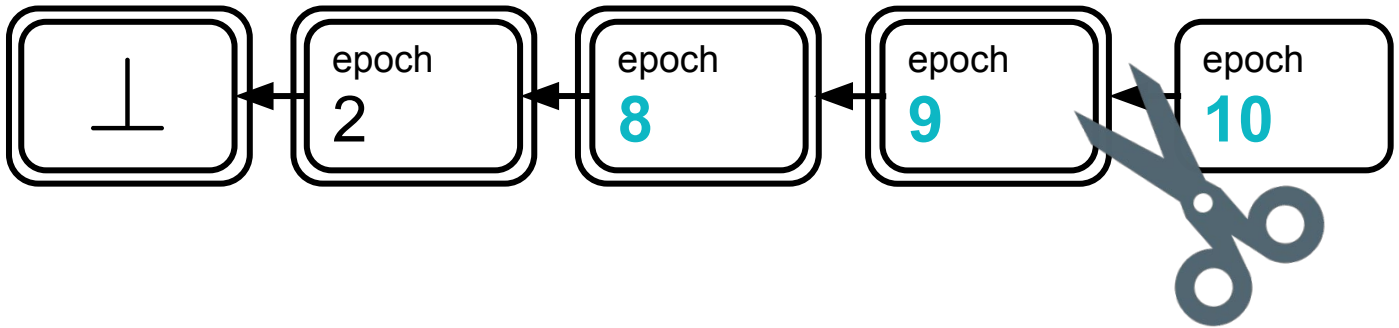
  Proposes a new block *b* extending longest **notarized** chain seen so far

- **everyone**:

  Votes for the first proposal *b* from leader(e)
  iff b extends a longest notarized chain seen so far

Streamlet Finalization Rule

Notarized chain ending with **3** adjacent blocks with **consecutive epochs**: **all but the last** are final



Streamlet achieves consensus for < ⅓ corruptions

Propose-vote, propose-vote…

No recovery path

Thank you!

Coming soon: new textbook

"Foundations of Blockchains and Distributed Consensus"

Other related work:
Casper, Hotstuff, Pili,Pala, Dfinity…