Streamlet: Textbook Streamlined Blockchains

Elaine Shi (CMU/Cornell)

Joint work with Benjamin Chan

Textbook: www.distributedconsensus.net
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

Apache Zookeeper

Logos of Yahoo!, Solr (from eBay), Uber, Facebook, Reddit, NetApp, and Rackspace.
Cryptocurrencies brought consensus to a large scale
Proof of work enables permissionless consensus.
Proof of work → Proof of stake

Proof of work: Bitcoin

Proof of stake: Aave, Infinity, Quickblocks, Ethereum, Parity
Rely on **permissioned consensus**

**Proof of work** → **Proof of stake**

- Bitcoin
- A
- Infinity
- Polkadot
- Ethereum
- Parity
Classical consensus landscape

PBFT
Paxos and variants

Complex
Difficult to understand
Error-prone to implement

“Paxos Made Moderately Complex”
[ACM Computing Surveys'15]

“Zyzzyva: Speculative Byzantine Fault Tolerance”
[Communications of the ACM'09]

“Paxos Made Simple”

“The ABCDs of Paxos”
[PODC'01]

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

... ...
Streamlet

Simple

Natural

Unified, for pedagogy & implementation
We can construct a blockchain through sequential composition of Byzantine Agreement (BA)
We can construct a blockchain through sequential composition of Byzantine Agreement (BA).

Direct blockchain construction (e.g., pbft, paxos)
Streamlet: a streamlined blockchain

Classical approaches (e.g., pbft, paxos)
Block Format

parent hash

epoch #

TXs
Assume: \( s \)'s increment in a valid blockchain.
Leader proposes block
2 Vote
Confirm upon \( \frac{2}{3} n \) votes
\[ \frac{2}{3} n \text{ votes: notarization} \]
Honest nodes vote *uniquely* each epoch
Must intersect at an honest node

Assume: \(< \frac{1}{3} n\) corrupt
Must intersect at an honest node.

Thus, \( \frac{2}{3} n \) = \( \frac{2}{3} n \).
Consistency

\[ \frac{2}{3} \text{ honest} \]

Liveness

honest

Liveness

Consistency
Liveness

$\frac{2}{3}$ honest

Consistency

Liveness
How do we achieve liveness?
Anatomy of classical consensus

Simple normal path

Complicated recovery path
Can we achieve **full** consensus (almost) as simply as the normal path?
Roadmap

Classical approaches (e.g., pbft, paxos)

Streamlet
Assume: \textit{epoch} = 1 sec \geq 1 \text{ roundtrip}
Leader rotation

Player $H(e) \mod n$ is the leader in epoch $e$

Easy to support any other leader-rotation policy
Assume honest nodes do the following

- receives msgs from the network
- echos every fresh msg seen
- updates its **longest notarized chain** every round
Propose
extend longest notarized chain

Vote
for 1st proposal from leader iff it extends from one of the longest notarized chains seen

Every epoch
Finalization: 3 consecutive epochs appear together in a notarized chain, all but last final
Finalization: 3 consecutive epochs appear together in a notarized chain, all but last final.

To prove: this cannot happen.
Consistency Proof

Liveness Proof

This talk
Height = “position in chain”
If everyone were honest
Real world

can skip epochs

1 3 4 5 7 9 11
Real world

can fork
Finalization: 3 consecutive epochs in notarized chain, all but last final

To prove: this cannot happen
Lemma: every epoch has at most 1 notarized block.
Proof:

many voted for 8 in epoch 8

“many”: > n/3 honest
Proof:

many voted for \(8\) in epoch 8

\(\Rightarrow\) many saw \(7\) notarized in epoch 8

“many”: \(> \frac{n}{3}\) honest
Proof:

many voted for \( \bullet 8 \) in epoch 8

\[ \rightarrow \] many saw \( \bullet 7 \) notarized in epoch 8

\[ \rightarrow \] they will not vote for \( \bullet 9 \) in epoch 9

“many”: \( > \frac{n}{3} \) honest
Proof:

many voted for $\mathcal{8}$ in epoch 8

$\rightarrow$ many saw $\mathcal{7}$ notarized in epoch 8

$\rightarrow$ they will not vote for $\mathcal{9}$ in epoch 9

$\rightarrow$ $\mathcal{9}$ cannot gain notarization

“many”: $> n/3$ honest
Proof:
many voted for $\bullet 5$ in epoch 5

“many” : $> \frac{n}{3}$ honest
Proof:

many voted for $5$ in epoch $5$

$\implies$ many saw $3$ notarized in epoch $5$

“many” : $> n/3$ honest
Proof:

many voted for \( \bullet 5 \) in epoch 5

\[ \rightarrow \quad \text{many saw} \quad \bullet 3 \quad \text{notarized in epoch} \quad 5 \]

\[ \rightarrow \quad \text{they will not vote for} \quad \bullet 6 \quad \text{in epoch} \quad 6 \]

“many” : > n/3 honest
Proof:

many voted for \( \bullet 5 \) in epoch 5

\( \rightarrow \) many saw \( \bullet 3 \) notarized in epoch 5

\( \rightarrow \) they will not vote for \( \bullet 6 \) in epoch 6

\( \rightarrow \) \( \bullet 6 \) cannot gain notarization

“many” : > \( n/3 \) honest
Proof:

many voted for $\bullet 5$ in epoch 5

---> many saw $\bullet 3$ notarized in epoch 5

---> they will not vote for $\bullet 6$ in epoch 6

---> $\bullet 6$ cannot gain notarization

“many” : > n/3 honest
Proof:

many voted for $\bullet 5$ in epoch 5

$\rightarrow$ many saw $\bullet 3$ notarized in epoch 5

$\rightarrow$ they will not vote for $\bullet 6$ in epoch 6

$\rightarrow$ $\bullet 6$ cannot gain notarization

“many” : $> n/3$ honest

Consistency does NOT depend on sync. assumptions!
Liveness Theorem

During a period of synchrony, honest players’ finalized chains grow whenever 5 consecutive epochs have honest leaders.

(and moreover the finalized chains grow by honest blocks)
Partial Synchrony

- Protocol knows a delay estimate $\Delta$
- Consistency is guaranteed even if actual delay arbitrarily long
- Liveness only during periods of synchrony
Partial Synchrony

Theorem:
Cannot tolerate $\frac{1}{3}$ or more corruptions
Summary: streamlined blockchains

- Every epoch allows leader-switch.
- Leader-switch embedded in a unified “propose-vote” paradigm.
Roadmap

$\frac{1}{2}$ synchronous

$\frac{1}{3}$ partially synchronous
Every epoch:

- Leader proposes a block extending longest notarized chain
- Vote on the first proposal iff it extends from one of the longest notarized chains seen
- A block with majority votes is notarized

Finalization:

- 6 consecutive at the end, no conflicting notarization, chop off 5
Read after me:

- Propose-vote, propose-vote, propose-vote
- Boom boom boom
- Don’t finalize upon notarization
- 3 consecutive epochs together, chop off the last and finalize the prefix

Thank You!
runting@gmail.com