Streamlet: Textbook streamlined blockchain protocols

Elaine Shi
Cornell

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

Apache Zookeeper
Cryptocurrencies brought consensus to a large scale
Proof of work
Proof of work enables permissionless consensus.
Rely on *permissioned* consensus

Proof of work → Proof of stake

Bitcoin → [Immutable, Infura, Parity, Ethereum]
Blockchain

Every round $t$, node $i$ outputs *longest final log* denoted $\text{LOG}_i^t$

**Consistency:** for any honest $i, j$, and $t, t'$,

$$\text{LOG}_i^t \prec \text{LOG}_j^{t'} \quad \text{or} \quad \text{LOG}_j^{t'} \prec \text{LOG}_i^t$$

Holds for 1-negl probability over the choice of execution
Blockchain

Every round $t$, node $i$ outputs *longest final log* denoted $\text{LOG}_{i}^{t}$

**Consistency:** for any honest $i$, $j$, and $t$, $t'$,

$$\text{LOG}_{i}^{t} < \text{LOG}_{j}^{t'} \quad \text{or} \quad \text{LOG}_{j}^{t'} < \text{LOG}_{i}^{t}$$

**Liveness:** if an honest node receives input $tx$ in round $t$, then in round $t + T(\lambda, n, \Delta)$, any honest node has $tx$ in its LOG

Holds for $1$-negl probability over the choice of execution
In PKI setting, equivalent to **BA** from a feasibility perspective
Blockchain

In PKI setting, equivalent to BA from a feasibility perspective

Is blockchain a meaningful abstraction?
Blockchain: 2 approaches

Sequential composition of BA

Direct blockchain construction
(e.g., pbft, paxos)
Blockchain: 2 approaches

- Sequential composition of BA
  - PODC, CRYPTO community

- Direct blockchain construction (e.g., pbft, paxos)
  - SOSP, NDSI, real-world community
Streamlet: a streamlined blockchain

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

parent hash

height

TXs
1 Proposer proposes block
2 Vote
Confirm upon \( \frac{2}{3} n \) votes
$\frac{2}{3} n$ votes: notarization
Honest nodes vote uniquely each height.
Must intersect at an honest node

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

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

Liveness

$\frac{2}{3}$ honest

Liveness
How do we achieve liveness?
Anatomy of classical consensus

Simple normal path

Complicated recovery path
Can we achieve full consensus (almost) as easily as the normal path?
Streamlined blockchains
(Casper, Dfinity, Hotstuff, Pili, Pala, Streamlet)

Classical approaches
(e.g., pbft, paxos)
Assume: $\text{epoch} = 1 \text{ sec} \geq 1 \text{ roundtrip}$
Proposer rotation

Node $H(i) \mod n$ is the proposer in epoch $i$

Easy to support any other proposer-rotation policy
If everyone were honest

Life is good
Real world

can skip epochs
Real world

can fork
Height = “position in chain”
Propose
- extend longest notarized chain

Vote
- no double-vote each epoch
- verify parent block notarized
- no conflicting notr at the height

Every epoch
Finalization: height $h$ final if heights $h-1$, $h$, $h+1$ have consecutive epochs & are notarized.

Height $h$
Consistency Proof

Liveness Proof

This talk
Finalization: height $h$ final if heights $h-1$, $h$, $h+1$ have consecutive epochs & are notarized.

To prove: this cannot happen.
Lemma: every epoch has at most 1 notarized block.
Proof:
many voted for $\mathbf{8}$ in epoch 8

“many” = at least $n/3$ honest
Proof:

many voted for $\bullet 8$ in epoch 8

$\rightarrow$ many saw $\bullet 7$ notarized in epoch 8

“many” = at least n/3 honest

Height $h$
Proof:

many voted for $\ast_8$ in epoch 8

$\rightarrow$ many saw $\ast_7$ notarized in epoch 8

$\rightarrow$ they will not vote for $\ast_9$ in epoch 9

“many” = at least $n/3$ honest
Proof:

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

--> many saw $\mathbf{7}$ notarized in epoch $8$

--> they will not vote for $\mathbf{9}$ in epoch $9$

--> $\mathbf{9}$ cannot gain notarization

“many” = at least $n/3$ honest
Proof:

many voted for 5 in epoch 5

“many” = at least n/3 honest
Proof:

many voted for 5 in epoch 5
--> many saw 3 notarized in epoch 5

“many” = at least $n/3$ honest
Proof:

many voted for $\mathbf{5}$ in epoch 5

$\implies$ many saw $\mathbf{3}$ notarized in epoch 5

$\implies$ they will not vote for $\mathbf{6}$ in epoch 6

“many” = at least $n/3$ honest
Proof:

many voted for [5] in epoch 5

--> many saw [3] notarized in epoch 5

--> they will not vote for [6] in epoch 6

--> [6] cannot gain notarization

“many” = at least n/3 honest

Height h-1
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” = at least \( \frac{n}{3} \) honest
Proof:
many voted for °5 in epoch 5
--> many saw °3 notarized in epoch 5
--> they will not vote for °6 in epoch 6
--> °6 cannot gain notarization

“many” = at least n/3 honest

Consistency does not depend on sync. assumptions!
Liveness Theorem

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

(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 proposer-switch.
- View change embedded in a unified “propose-vote” paradigm.
Roadmap

$\frac{1}{2}$ synchronous

$\frac{1}{3}$ partially synchronous
**Every epoch:**
- Proposer proposes a block extending longest notarized chain
- Vote on the first proposal if parent notarized and no other notarized block at same height
- A block with majority votes is notarized

**Finalization:**
- 6 consecutive at the end, no conflicting notarization, chop off 5
Optimistic Responsiveness

Best-possible partition tolerance

https://eprint.iacr.org/2018/981
https://eprint.iacr.org/2018/980
https://eprint.iacr.org/2019/179
Thank You!
elaine@cs.cornell.edu