Rational vs Byzantine Players in Consensus-based Blockchains

Yackolley Amoussou-Guenou[†,‡], Bruno Biais[◇],
Maria Potop-Butucaru[‡], Sara Tucci-Piergiovanni[†]

† CEA LIST – ‡ LIP6, Sorbonne Université – ◇ HEC

Tokenomics 2020

October 26 & 27, 2020
Toulouse

Objectives of Blockchains at the Beginning

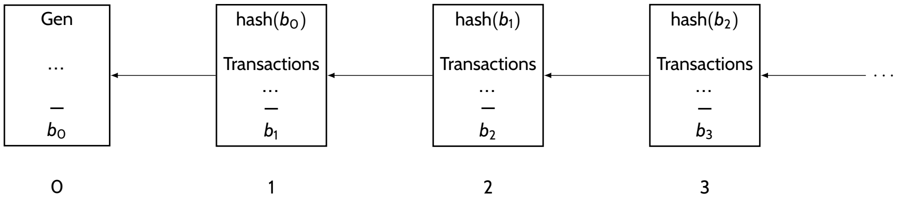
Players communicate by exchanging messages.

- **Distributed** ledger,
  - There is no central authority;
- **Tamper-resistant**,
  - Modification should be difficult, even impossible;
- Build in an append **only manner**.

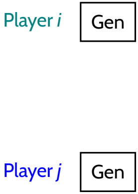
Objectives of Blockchains at the Beginning

Players communicate by exchanging messages.

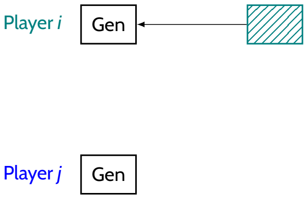
- **Distributed** ledger,
  - There is no central authority;
- **Tamper-resistant,**
  - Modification should be difficult, even impossible;
- Build in an append **only manner.**



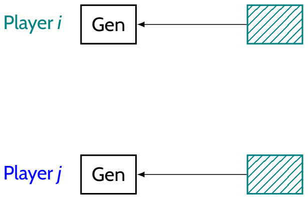
Building a Blockchain – Bitcoin's Style



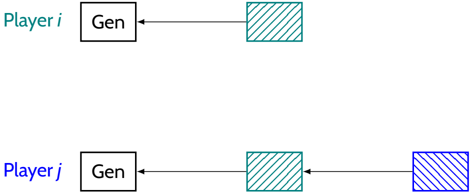
Building a Blockchain – Bitcoin's Style



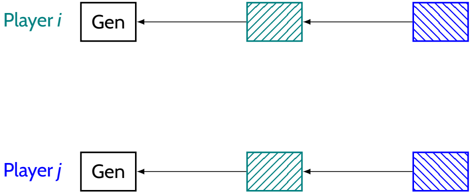
Building a Blockchain – Bitcoin's Style



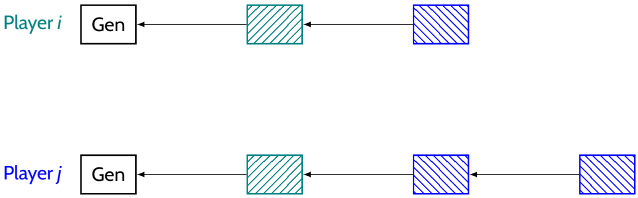
Building a Blockchain – Bitcoin's Style



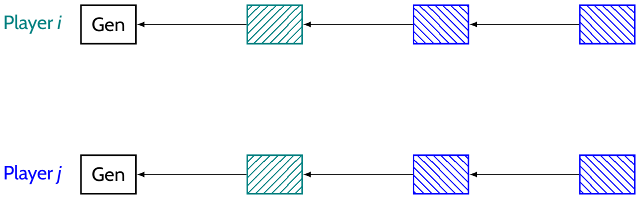
Building a Blockchain – Bitcoin's Style



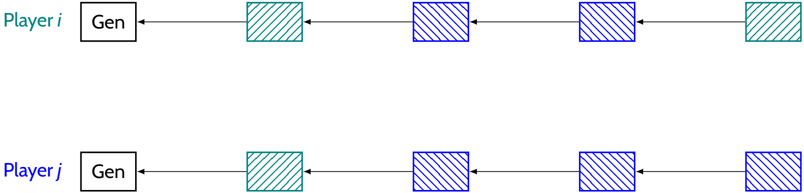
Building a Blockchain – Bitcoin's Style



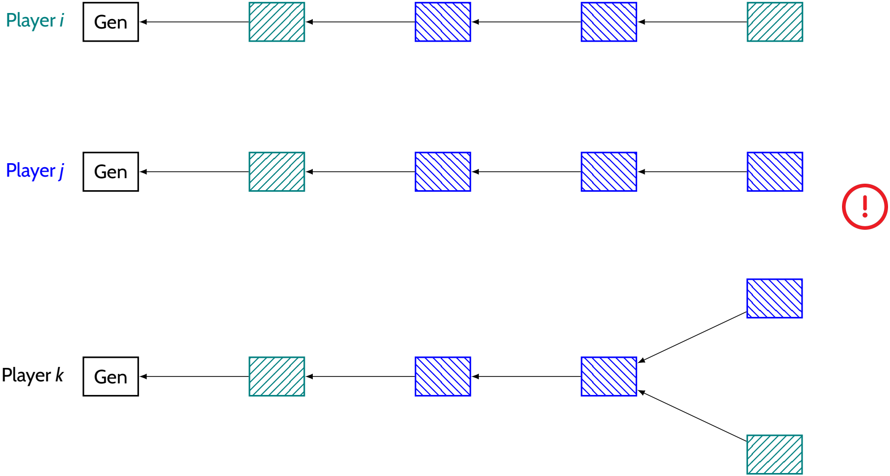
Building a Blockchain – Bitcoin's Style



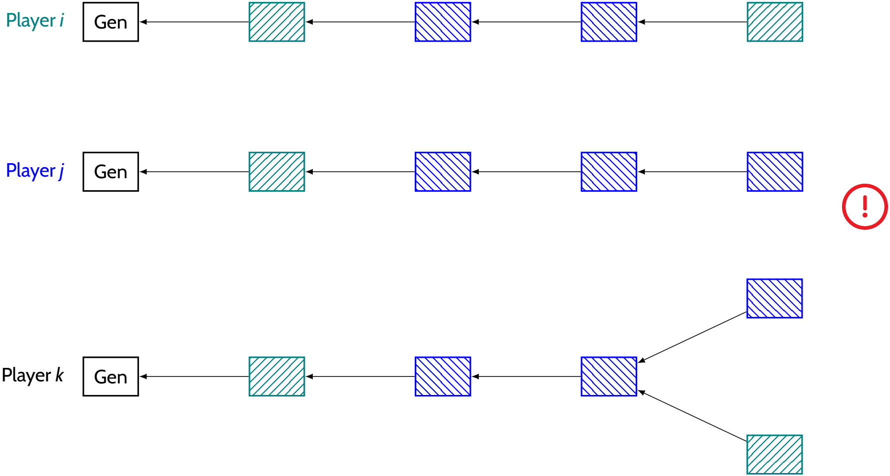
Building a Blockchain – Bitcoin's Style



Building a Blockchain – Bitcoin's Style



Building a Blockchain – Bitcoin's Style



Forks are undesirable for critical systems.

How to avoid forks ?

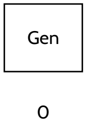
Consensus Problem

An algorithm implements the Consensus if the following properties are satisfied:

- **Termination.** Every obedient[1] player eventually decides some value.
- **Validity.** A decided value is valid, it satisfies the predefined predicate.
- **Agreement.** If two correct players decide respectively B and B', then $B = B'$.

[1] Obedient means which always executes the prescribed algorithm.

Build a Blockchain Using Consensus

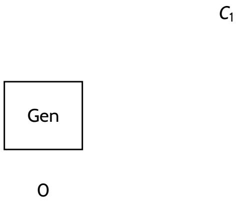


Each committee C_h is deterministically selected with respect to the blockchain up to height $h - 1$.

E.g. Tendermint, HotStuff, Libra, ...

Once a block at height h is produced, the committee C_h is rewarded (for instance those who accepted the block).

Build a Blockchain Using Consensus

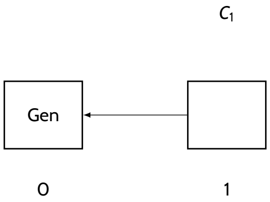


Each committee C_h is deterministically selected with respect to the blockchain up to height $h - 1$.

E.g. Tendermint, HotStuff, Libra, …

Once a block at height h is produced, the committee C_h is rewarded (for instance those who accepted the block).

Build a Blockchain Using Consensus

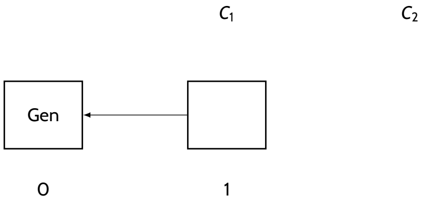


Each committee C_h is deterministically selected with respect to the blockchain up to height $h - 1$.

E.g. Tendermint, HotStuff, Libra, …

Once a block at height h is produced, the committee C_h is rewarded (for instance those who accepted the block).

Build a Blockchain Using Consensus

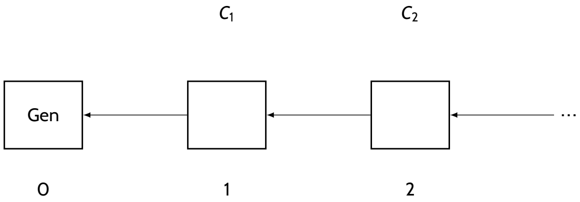


Each committee C_h is deterministically selected with respect to the blockchain up to height $h-1$.

E.g. Tendermint, HotStuff, Libra, ...

Once a block at height h is produced, the committee C_h is rewarded (for instance those who accepted the block).

Build a Blockchain Using Consensus

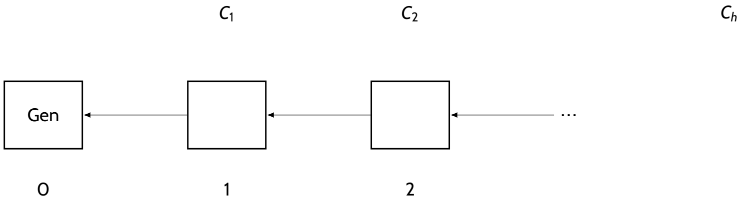


Each committee C_h is deterministically selected with respect to the blockchain up to height $h - 1$.

E.g. Tendermint, HotStuff, Libra, ...

Once a block at height h is produced, the committee C_h is rewarded (for instance those who accepted the block).

Build a Blockchain Using Consensus

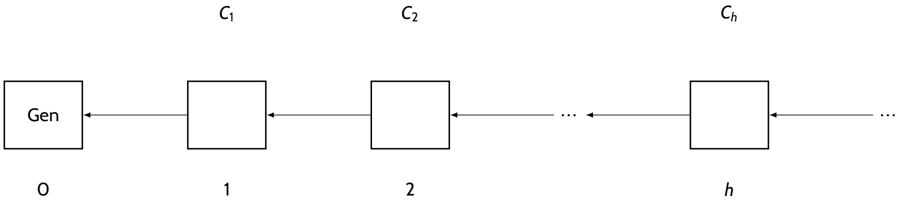


Each committee C_h is deterministically selected with respect to the blockchain up to height $h - 1$.

E.g. Tendermint, HotStuff, Libra, ...

Once a block at height h is produced, the committee C_h is rewarded (for instance those who accepted the block).

Build a Blockchain Using Consensus



Each committee C_h is deterministically selected with respect to the blockchain up to height $h - 1$.

E.g. Tendermint, HotStuff, Libra, ...

Once a block at height h is produced, the committee C_h is rewarded (for instance those who accepted the block).

Existing Analyses of Committe-based Blockchains

Tendermint

- Kwon (2014). Tendermint: *Consensus without mining*.
- Amoussou-Guenou, Del Pozzo, Potop-Butucaru & Tucci-Piergiovanni (OPODIS 2018). *Correctness of Tendermint-core Blockchains*.

HotStuff (Core of the Libra Blockchain)

Yin, Malkhi, Reiter, Gueta & Abraham (PODC 2019). *Hotstuff: BFT Consensus with Linearity and Responsiveness*.

Analyses above and most analyses consider only 2 types of players: **Obedient**, and **Byzantine** (any kind of bug, or specifically an adversary).

Are consensus properties guaranteed with the presence of rational players?

- Termination.
- Agreement.
- Validity.

Our Model[2] (Focus on One Single Committee)

- **Ordered** set of *n* players, the committee.
- Synchronous communication and **messages cannot be lost.**

We consider 2 types of players:

- Strategic ("Type S"): maximize their expected gain;
- Adversary ("Type A"): do anything to prevent consensus.

A player knows its type, and its index in the committee!

Players are evenly distributed in the committee.

Under this model we can always ensure Agreement.

[2] Amoussou-Guenou, Biais, Potop-Butucaru & Tucci-Piergiovanni (2020). *Rational vs Byzantine Players in Committee-based Blockchains*.

At each height, multiple possible rounds with 2 phases

At height *h*, players must reach consensus on which new block to add:

- Round 1:
  - Propose phase (Player 1 proposes block);
  - Vote phase (vote for block or not);
  - If sufficiently many votes ($\nu > 1$) in favor of proposed block, added to chain; otherwise go to next round.

At each height, multiple possible rounds with 2 phases

At height h, players must reach consensus on which new block to add:

- Round 1:
  - Propose phase (Player 1 proposes block);
  - Vote phase (vote for block or not);
  - If sufficiently many votes ($\nu > 1$) in favor of proposed block, added to chain; otherwise go to next round.
- Round 2:
  - Propose phase (Player 2 proposes block);
  - Vote phase;
  - If sufficiently many votes (ν), add block; otherwise next round.

$\vdots$

- Round n:
  - Propose phase (Player n proposes block);
  - Vote phase;
  - If sufficiently many votes (ν), add block; otherwise next round.

$\vdots$

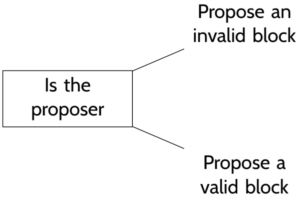
Different Actions in One Round

At round $t \in \{1, \ldots, n\}$:

- Propose phase:
  - Send step: Player t generates **valid block** and broadcasts it.
  - Delivery step: All player collect the proposal.
  - Compute step: Players **check validity** and set a vote **iff valid**.
- Vote phase:
  - Send step: Each player **broadcasts vote iff block valid**.
  - Delivery step: All players collect votes.
  - Compute step: If more votes than qualified majority ν, broadcast block, otherwise go to next round.

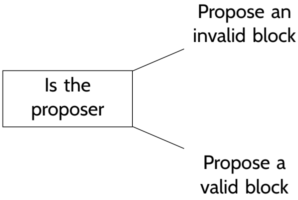
Action Space (At each Round, for each Player)

- Proposer: proposes valid or invalid block to the committee.

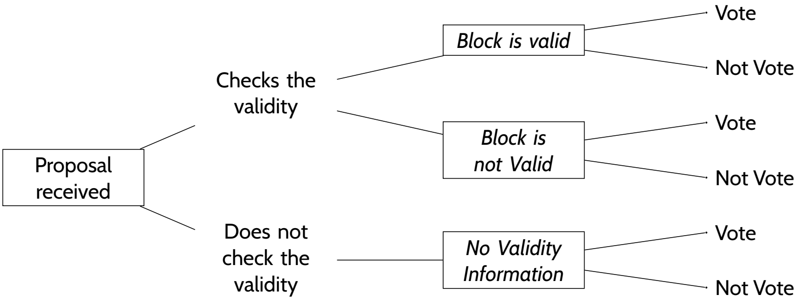


Action Space (At each Round, for each Player)

- Proposer: proposes valid or invalid block to the committee.



- As voter:



Strategics' Costs and Rewards

Cost to check validity (transactions, protocol, …) and to send vote: electricity, memory, . . .

- At each round:
  - Check validity (at cost c_{check}) or not;
  - Send vote message (at cost c_{send}) or not.
- After each round:
  - If block accepted (ν votes), each "Type S" who sent vote gets R:

$$R > c_{\text{check}} > c_{\text{send}} \geq 0;$$

  - If invalid block accepted, each "Type S" incurs cost $-\kappa$:

$$\kappa >> R.$$

Objective: Maximize expected gain.

Objective of Adversaries

Adversaries want to prevent consensus.

Adversaries have lexicographic preferences over the outcomes:

++ Accept an invalid block (no validity).
+ Accept no block (no termination).
- Accept one valid block (consensus).

Adversaries do not incur any costs.

Denote by $f \geq 1$ the number of "Type A" in the committee.

Information Sets and Strategies

- Public information: Votes in previous rounds.
- Private information:
  - Each privately knows whether it checks or not;
  - If checks, privately knows whether block valid or not.

Additional private information:

- A "Type *S*" knows its own type, not other's types;
- A "Type *A*" knows types of all players (and their index).

Solution Concept – Perfect Bayesian Equilibrium

Players have *incomplete* and *asymmetric* informations.

Exchanges are repeated through multiple rounds.
Suitable concept: (pure) *Perfect Bayesian Equilibrium*.

Each players:

- Deterministically choose actions maximising their objectives, anticipating rationally the actions of the others;
- Draw rational inferences from what they observed about players types, according to Bayes law;
- Always picking the best actions, no matter in which round they are.

Optimal Strategy for Proposers

“Type S”: Propose valid block (or no check & propose any block).

“Type A”: Propose invalid block; Check and always vote for invalid block.

Are consensus properties guaranteed in presence of rational players?

↓

Do the equilibria satisfy consensus?

(Validity & Termination)

Termination is Not Always Guaranteed

Proposition 1

Let $f \geq 1$ be the number of "Type *A*", and ν be the qualified majority to accept a block. When f **be a random variable** s.t. $f < \nu$, there exists a perfect Bayesian equilibrium s.t. **"Type *S*" neither check validity nor vote**, while "Type *A*" vote for invalid blocks only.

Termination is Not Always Guaranteed

Proposition 1

Let $f \geq 1$ be the number of "Type *A*", and ν be the qualified majority to accept a block. When *f* **be a random variable** s.t. $f < \nu$, there exists a perfect Bayesian equilibrium s.t. **"Type *S*" neither check validity nor vote**, while "Type *A*" vote for invalid blocks only.

In equilibrium no block is accepted: No termination.

Even Validity can be Violated

Proposition 2

Let $f \geq 1$ be the number of "Type A", and ν be the qualified majority to accept a block. When f **be a random variable** s.t. $f \in \{1, \ldots, n - \nu\}$, there exists an equilibrium where **"Type S" do not check validity but vote**, while "Type A" vote for invalid blocks only.

Even Validity can be Violated

Proposition 2

Let $f \geq 1$ be the number of "Type A", and ν be the qualified majority to accept a block. When f **be a random variable** s.t. $f \in \{1, \ldots, n - \nu\}$, there exists an equilibrium where **"Type S" do not check validity but vote**, while "Type A" vote for invalid blocks only.

In equilibrium, termination but not always validity:

- If a "Type A" is the proposer, invalid block is accepted $\rightarrow$ no validity;
- If a "Type S" is the proposer, valid block is accepted $\rightarrow$ validity.

Even Validity can be Violated

Proposition 2

Let $f \geq 1$ be the number of "Type A", and ν be the qualified majority to accept a block. When f **be a random variable** s.t. $f \in \{1, \ldots, n - \nu\}$, there exists an equilibrium where **"Type S" do not check validity but vote**, while "Type A" vote for invalid blocks only.

In equilibrium, termination but not always validity:

- If a "Type A" is the proposer, invalid block is accepted $\rightarrow$ no validity;
- If a "Type S" is the proposer, valid block is accepted $\rightarrow$ validity.

Remark

In Proposition 2, there is no assumption about f with respect to ν:
As long as $f \geq 1$, the risk that invalid blocks are accepted exists.

Is There a Good Equilibrium?

Players not pivotal $\rightarrow$ free riding.

Can this be avoided? Can players be pivotal?

In a “good” equilibrium, player should be pivotal specifically for check.

Is There a Good Equilibrium? What we Would Like

Players not pivotal $\rightarrow$ free riding.

Can this be avoided? Can players be pivotal?

In a "good" equilibrium, player should be pivotal specifically for check.

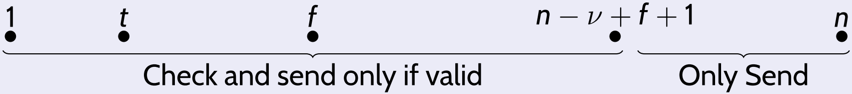
- if a "Type *S*" proposes: the block is valid and there are $n - f > \nu$ votes:
  - The block is produced.
- if a "Type *A*" proposes: the block is invalid and there are at most $\nu - 1$ votes:
  - The block is not produced.
  - If a "Type *S*" supposed to check deviates and send without checking:
    - Some chances it makes an invalid block accepted.

Both Validity and Termination can Hold

Players are ordered in the committee, and each knows its index.

Proposition 3

Assume ν **and** f **common knowledge** and $f < \nu < n - f - 1$.
If κ *large enough*, there exists an equilibrium where: at round $f + 1$ all "Type S" vote without checking; and at round $t < f$:



At round $f + 1$ all "Type S" vote without checking the validity.

It takes at most $f + 1$ rounds to accept a block (termination), and it is valid (validity).

Conclusions & Perspectives

- Analysis of rational behavior in committee-based blockchains against malicious players.
  - Good equilibrium but not unique;
  - Free-riding situation may occur.
- Extend the current work with more settings and less hypothesis, and study more reward schemes.

Merci !