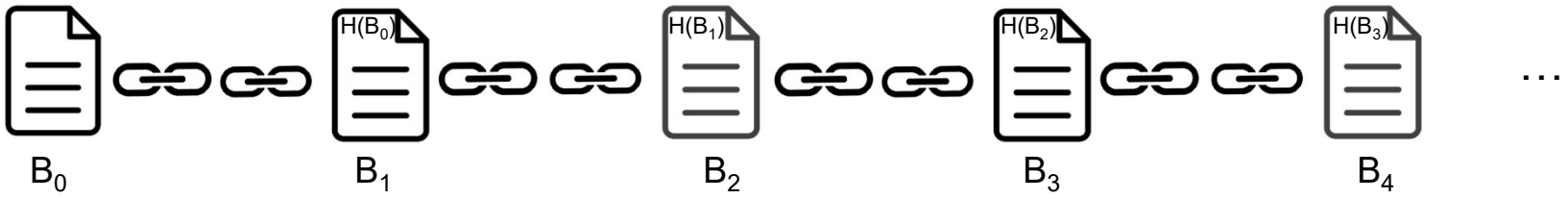
Rationals vs Byzantine Players in Committee-Based Blockchains

Y. Amoussou-Guenou[a,b], B. Bias[c],
M. Potop-Butucaru[b], S.Tucci-Piergiovanni[a]

[a] CEA, LIST
[b] Sorbonne Université, CNRS, Laboratoire d'Informatique de Paris 6
[c] HEC Paris

BLOCKCHAIN

- Potentially unbounded set of processes that communicate in a network through message passing
- **Distributed ledger**
- **Tamper-resistant**
- Build in an **append only** manner



CONSENSUS

- **Termination**

  Every non-faulty process eventually decides some value

- **Agreement**

  If there is a non-faulty process that decides a value B, then eventually all the Non-faulty processes decide B

- **Validity**

  A decided value is valid, it satisfies the predefined predicate

COMMITTEE-BASED BLOCKCHAINS

Committee

Dissecting Tendermint

Yackolley Amoussou-Guenou[1,2], Antonella Del Pozzo[1], Maria Potop-Butucaru[2], and Sara Tucci-Piergiovanni[1]

[1] CEA LIST, PC 174, Gif-sur-Yvette, 91191, France
[2] Sorbonne Université, CNRS, UMR 7606, LIP6, Paris, France

HotStuff: BFT Consensus with Linearity and Responsiveness

Maofan Yin, Cornell University, VMware Research
Dahlia Malkhi, VMware Research
Michael K. Reiter, UNC-Chapel Hill, VMware Research
Guy Golan Gueta, VMware Research
Ittai Abraham, VMware Research

- block to be appended
- Committees are rewarded for their work

RATIONAL BEHAVIOUR & SYSTEM MODEL

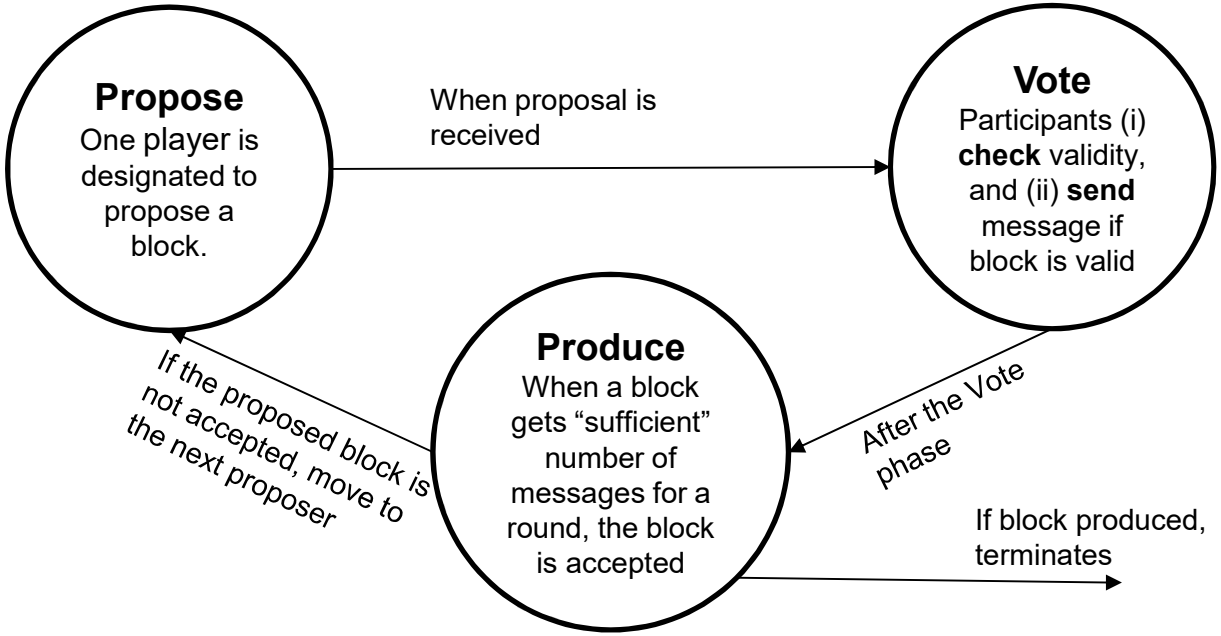
Q. *Are the consensus properties (Termination and Validity) guaranteed with the presence of rational participants ?*

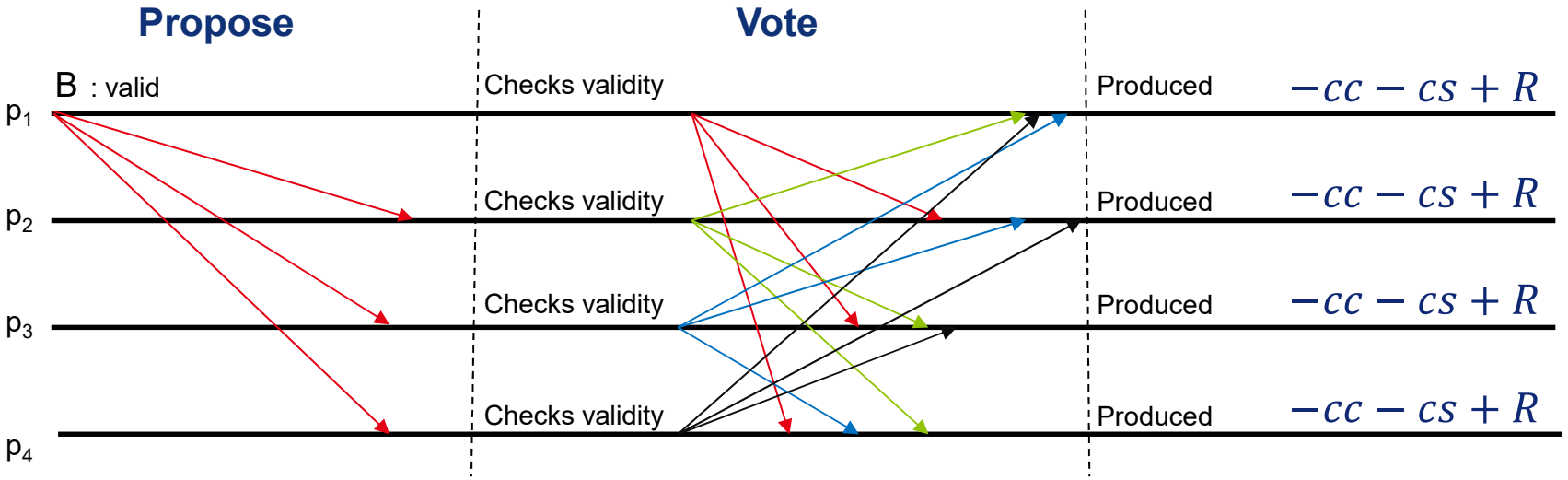
- Ordered set of n processes/players
- Messages are **signed** and signatures cannot be forged
  Processes cannot lie about who created a message
- Synchronous communication
  - Messages cannot be lost
- Following the BAR Model[1], participants are either
  - Rational
  - Byzantine

  Assumption: *There are more rational processes than Byzantine*

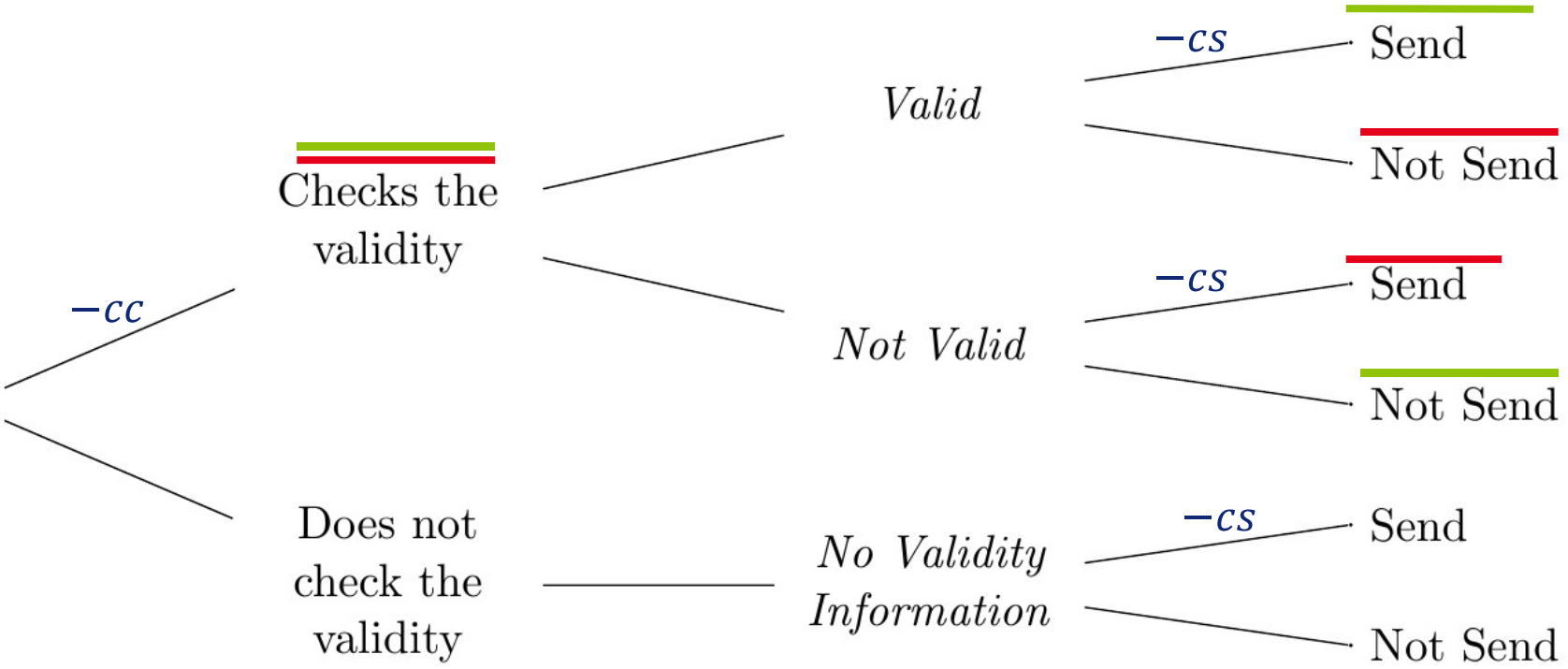
[1] A. S. Aiyer, L. Alvisi, A. Clement, M. Dahlin, J.-P. Martin, and C. Porth, 'BAR fault tolerance for cooperative services', in *Proceedings of the 20th ACM Symposium on Operating Systems Principles (SOSP'05)*, 2005, pp. 45–58.

CORRECT/PRESCRIBED BEHAVIOUR





OBJECTIVES

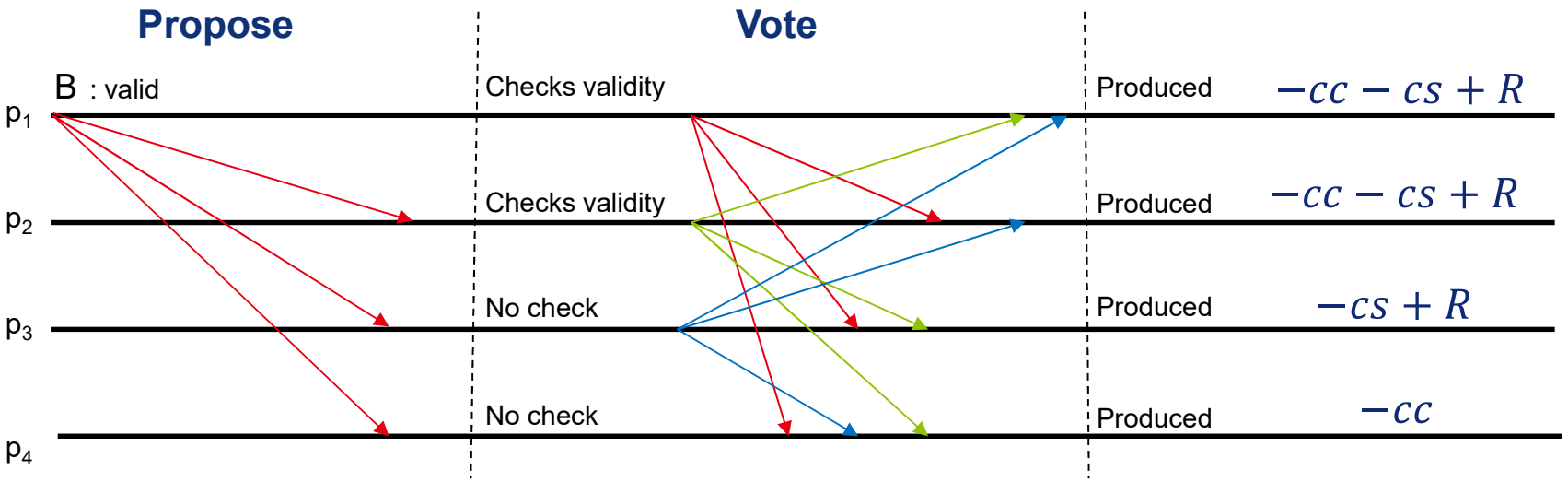


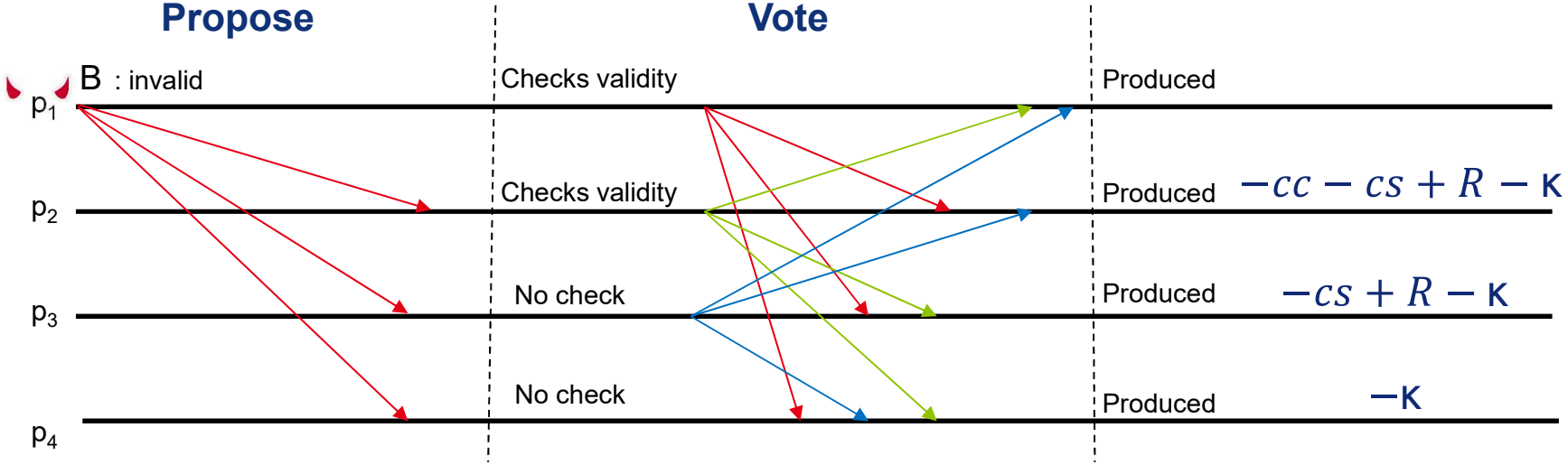
$$\left(R * \mathbb{1}_{(\sigma_i^{\text{send}}(H_i^T)=1)} * \mathbb{1}_{(\text{block accepted at } T)} - \kappa \mathbb{1}_{(\text{invalid block accepted})}\right) - \sum_{t=1}^{T} \left(c_{check} \mathbb{1}_{\sigma_i^{\text{check}}(h_i^t)=1)} + c_{send} \mathbb{1}_{(\sigma_i^{\text{send}}(H_i^t)=1)}\right)$$

$$\kappa > R > c_{check} > c_{send}$$

EXAMPLES OF EXECUTION

3 MESSAGES REQUIRED

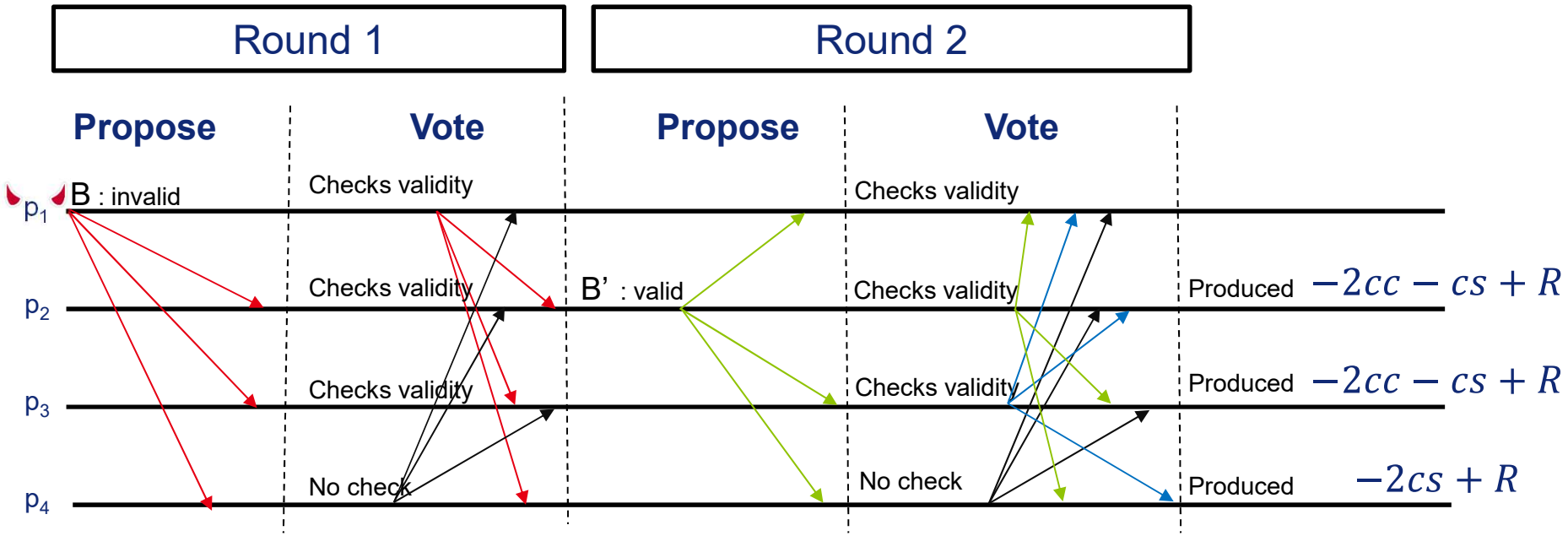




EQUILIBRIUM CONCEPT

Perfect Bayesian equilibrium

1. Choose actions maximizing their objective function,
2. Rationally anticipate the strategies of the others, and
3. Draw rational inferences from what they observe, using their expectations about the strategies of the others and Bayes law, whenever it applies.



CONSENSUS AGAINST RATIONALS

- **Q.** ***Are the consensus properties (Termination and Validity) guaranteed with the presence of rational participants ?***

n *is the total number of processes*

ν *is the minimum number of required messages for block's production*

f *is the number of Byzantine processes (f>1)*

EQUILIBRIUM WHEN TOO MANY BYZANTINES

- When $\mathbf{f \geq \nu}$, in equilibrium, all rational participants send a message without checking validity

- *Termination* holds
- *Validity* is not guaranteed

EQUILIBRIA WITH SMALL NUMBER OF BYZANTINES (1/2)

- When $\mathbf{f < \nu}$, there exists an equilibrium where all rational participants do not check block's validity, nor send a message

- *Termination* is violated
- *Validity* holds

EQUILIBRIA WITH SMALL NUMBER OF BYZANTINES (2/2)

- When **f < ν**, if the cost of producing an invalid block is “high enough”, there is an equilibrium where there is always a valid block produced
  - For a process **i**, if **i ≤ n-ν+f+1** then **i** checks block’s validity and sends a message iff the block is valid
  - For a process **i**, if **i > n-ν+f+n** (**i ≤ n**) **i** sends a message without checking block’s validity

- *Termination* holds
- *Validity* holds

CONCLUSIONS & PERSPECTIVES

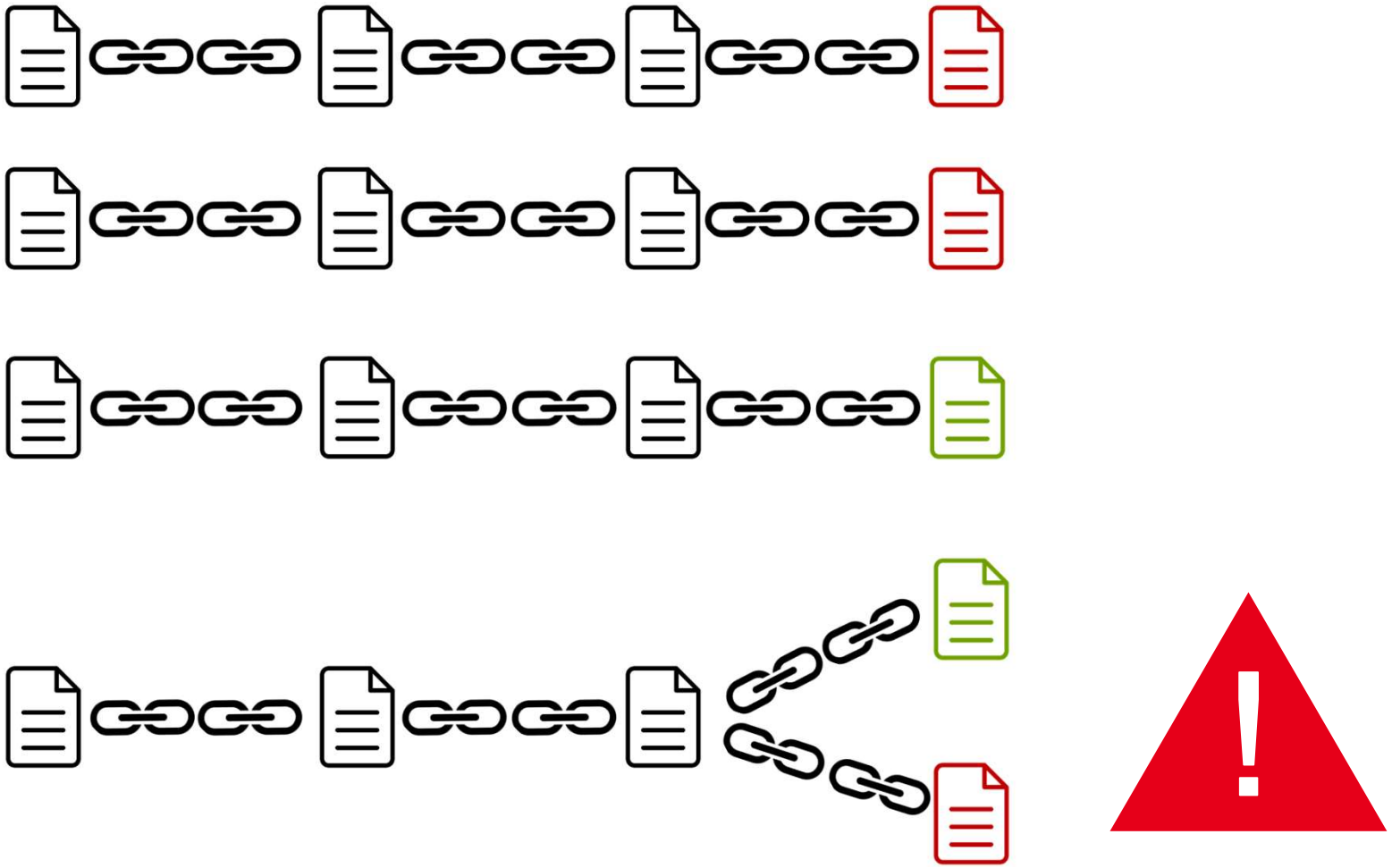
- **Analyse of rational behaviour in Committee-based Blockchains against Byzantine processes**

- **Extend the current work with more settings**

Merci !

Thank You !

HISTORY



EXAMPLE OF EXECUTION (1/2)

3 MESSAGES REQUIRED