FAST INTERNET COMPUTER CONSENSUS

Master’s Thesis Presentation

Supervisors: Jakub Sliwinski, Yann Vonlanthen, Prof. Roger Wattenhofer

Massimo Albarello - 6 April 2023

Motivation

Serve interactive web experiences directly to users

Motivation

vs.

Motivation

vs.

2 seconds

~ instant

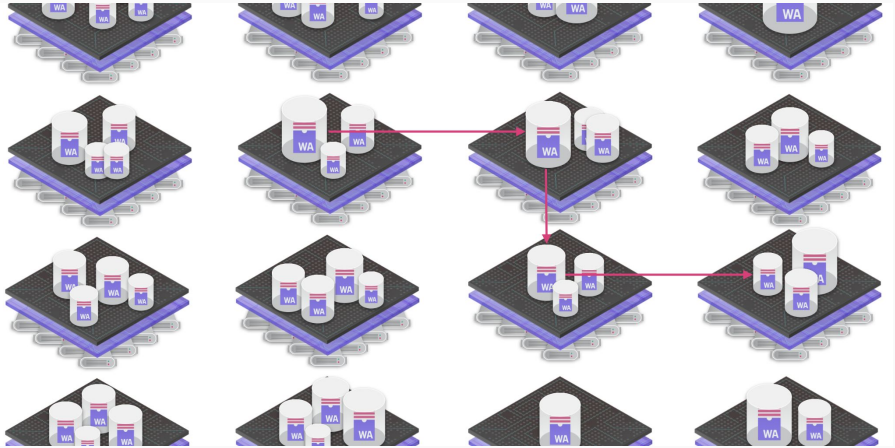
Motivation

User :(

vs.

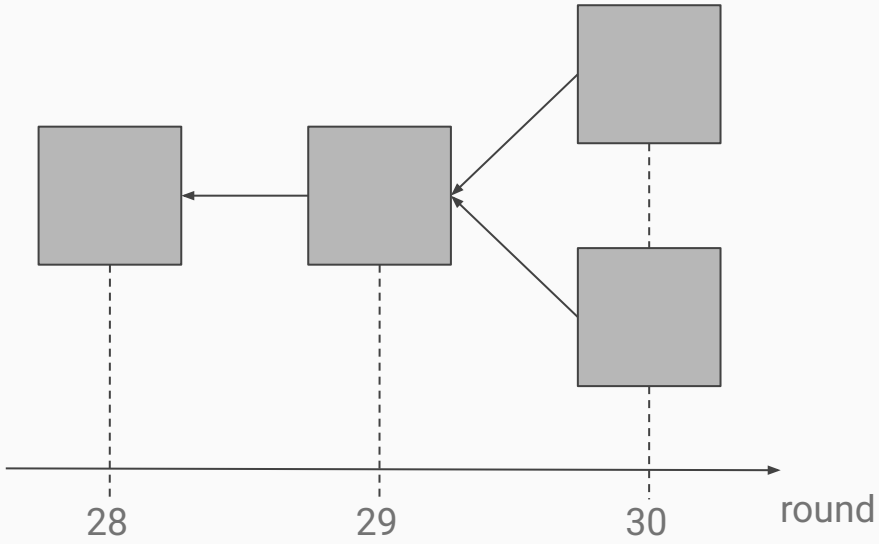
User :)

Internet Computer



Internet Computer Consensus (ICC) in each subnet

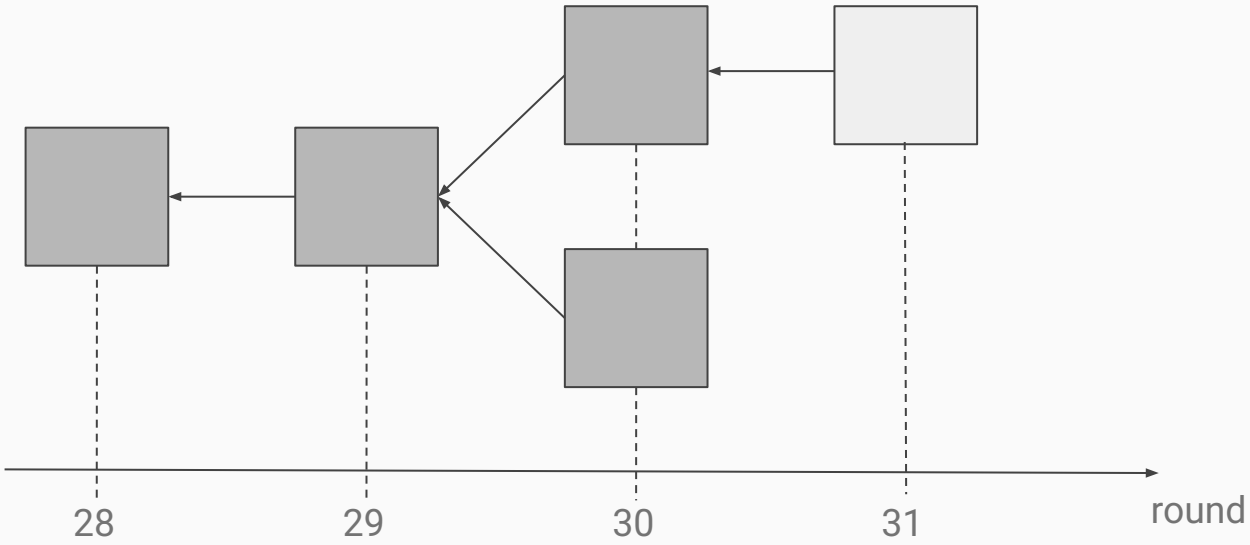
Internet Computer Consensus



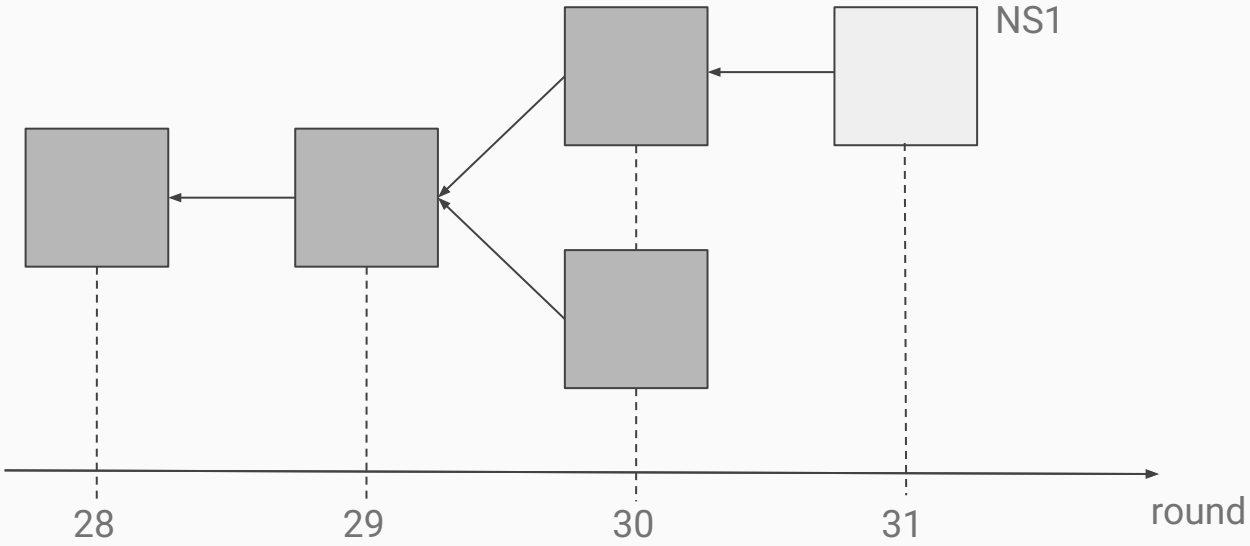
In each round:

1. Block proposal
2. Notarization
3. Finalization (eventually)

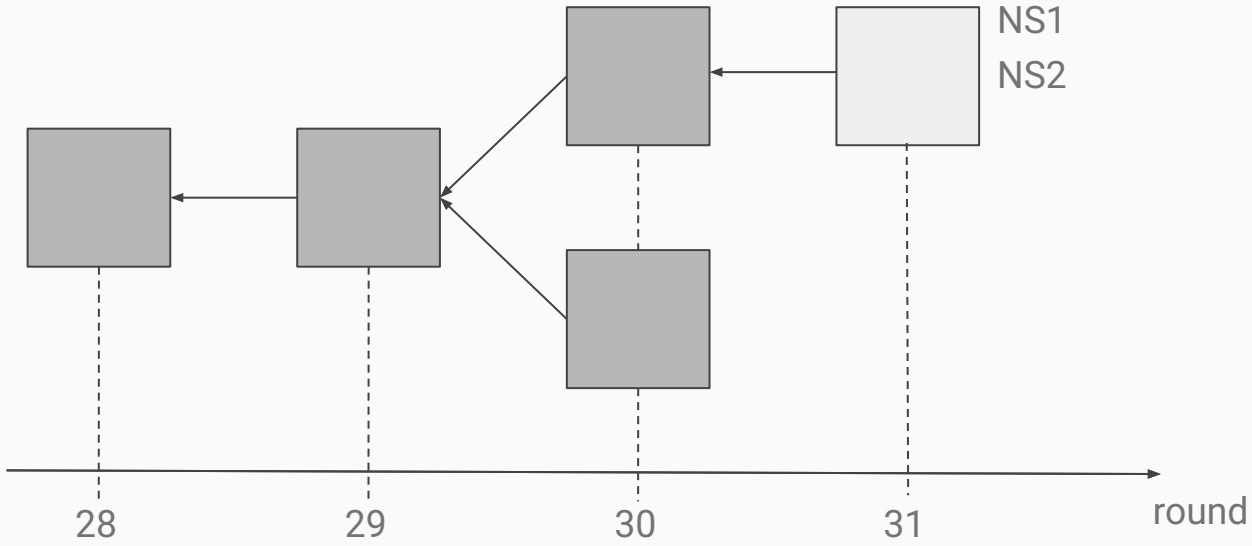
ICC: block proposal



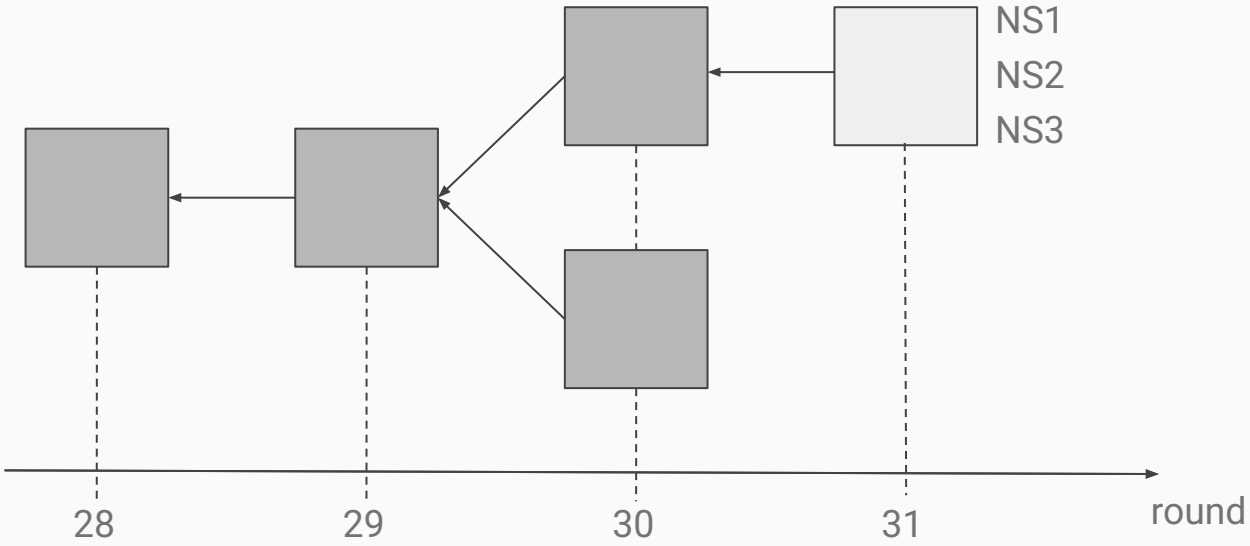
ICC: notarization



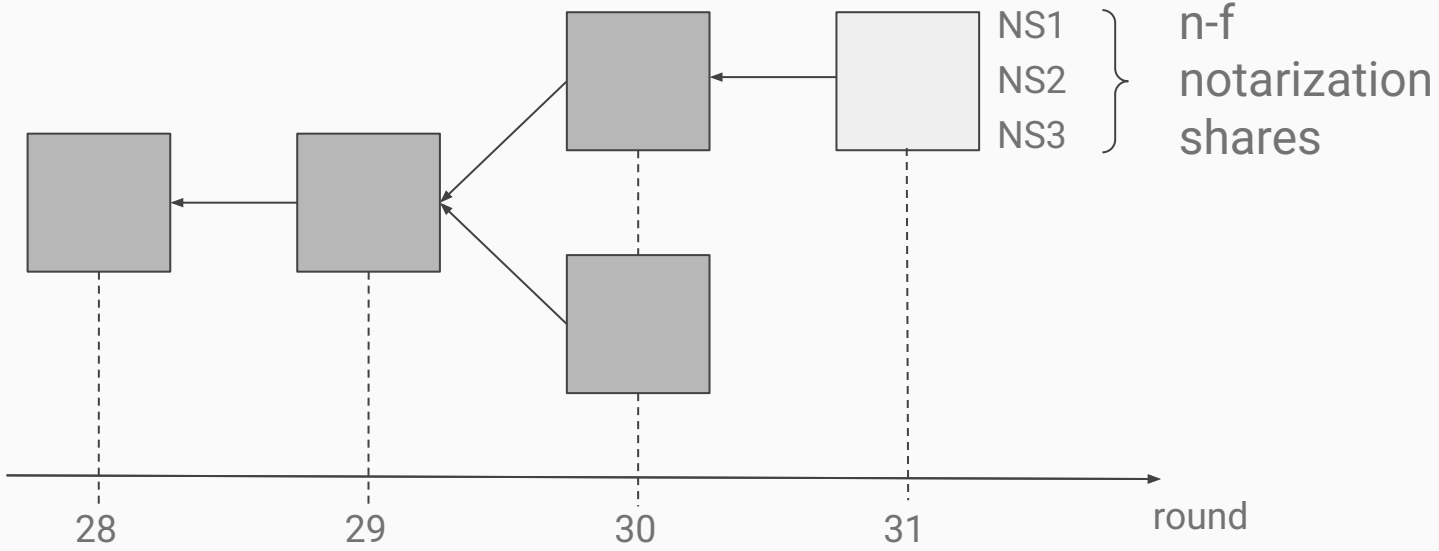
ICC: notarization



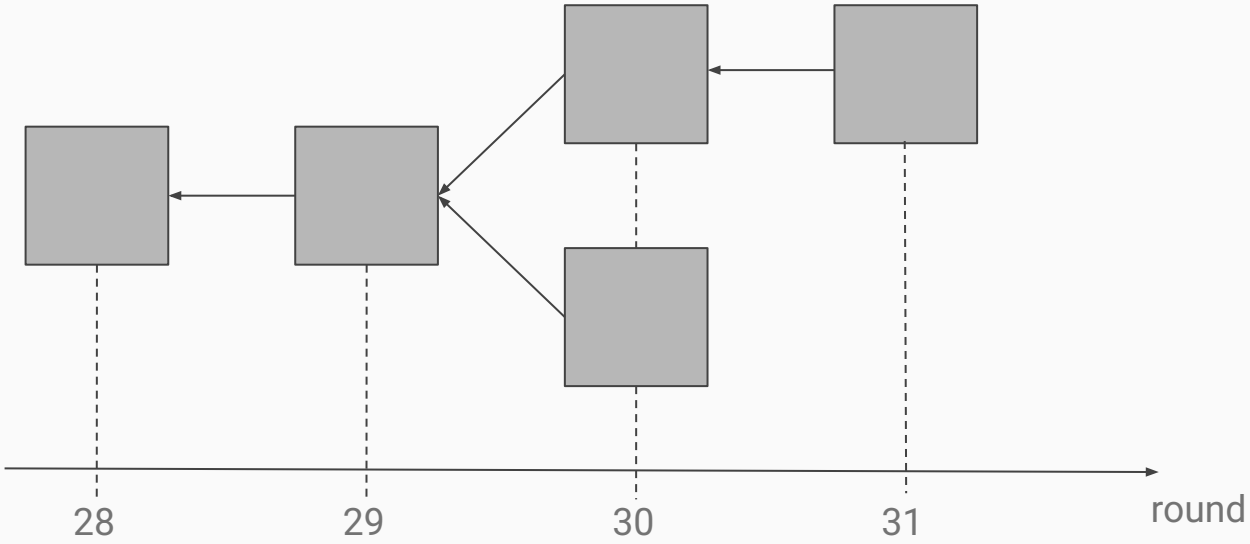
ICC: notarization



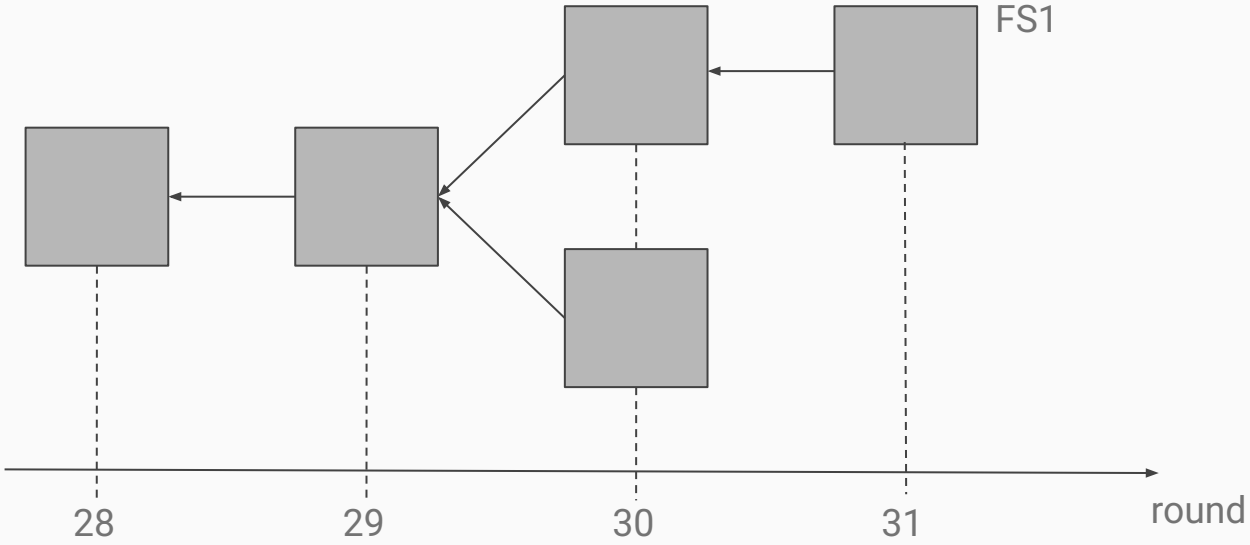
ICC: notarization



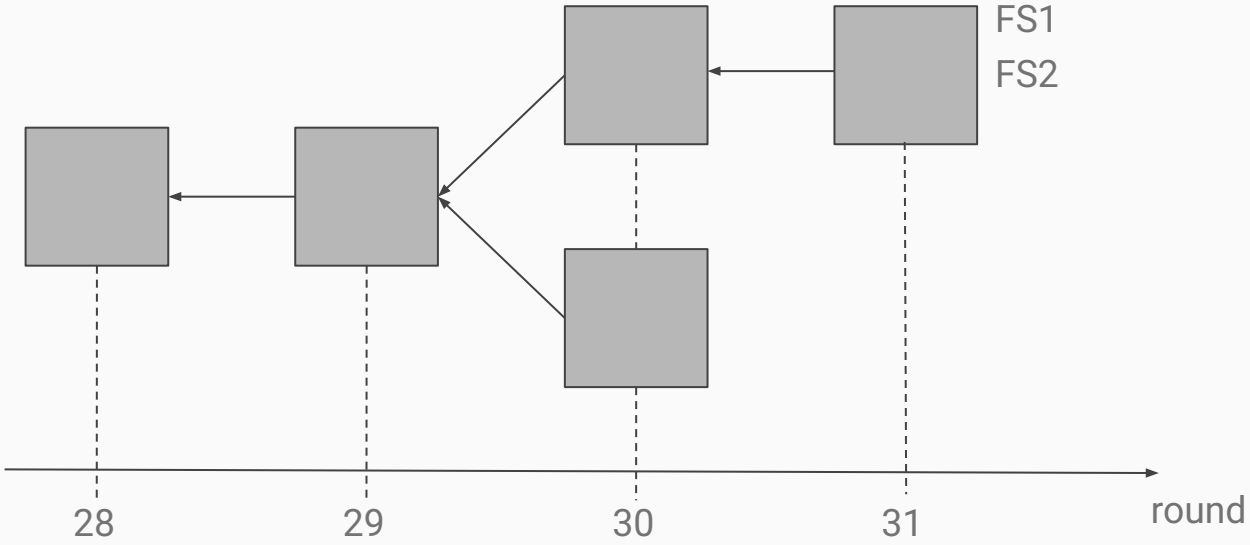
ICC: notarization



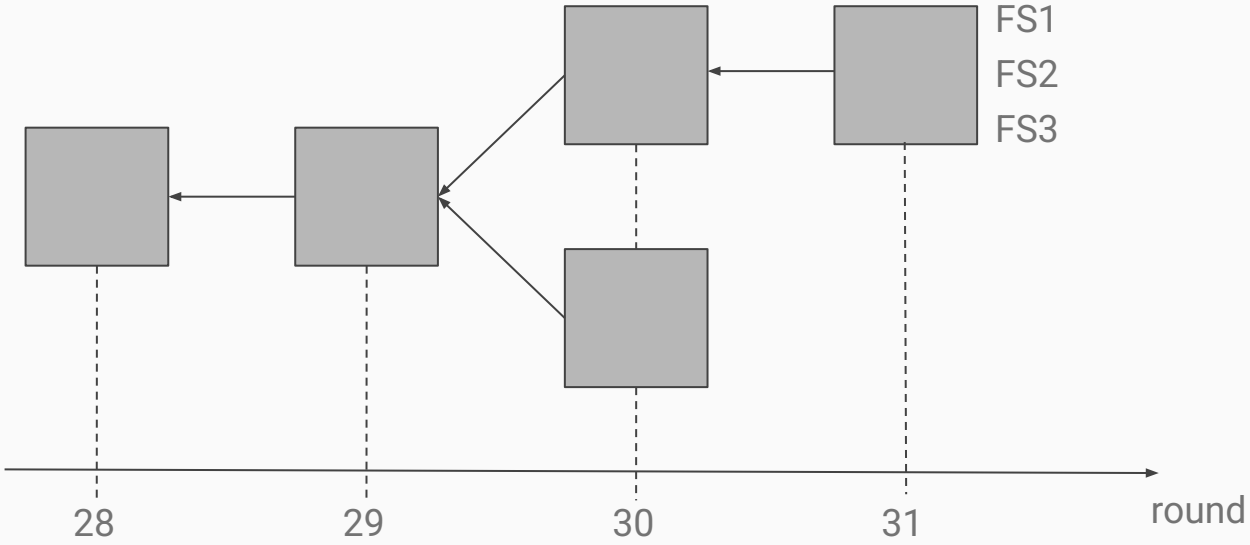
ICC: finalization



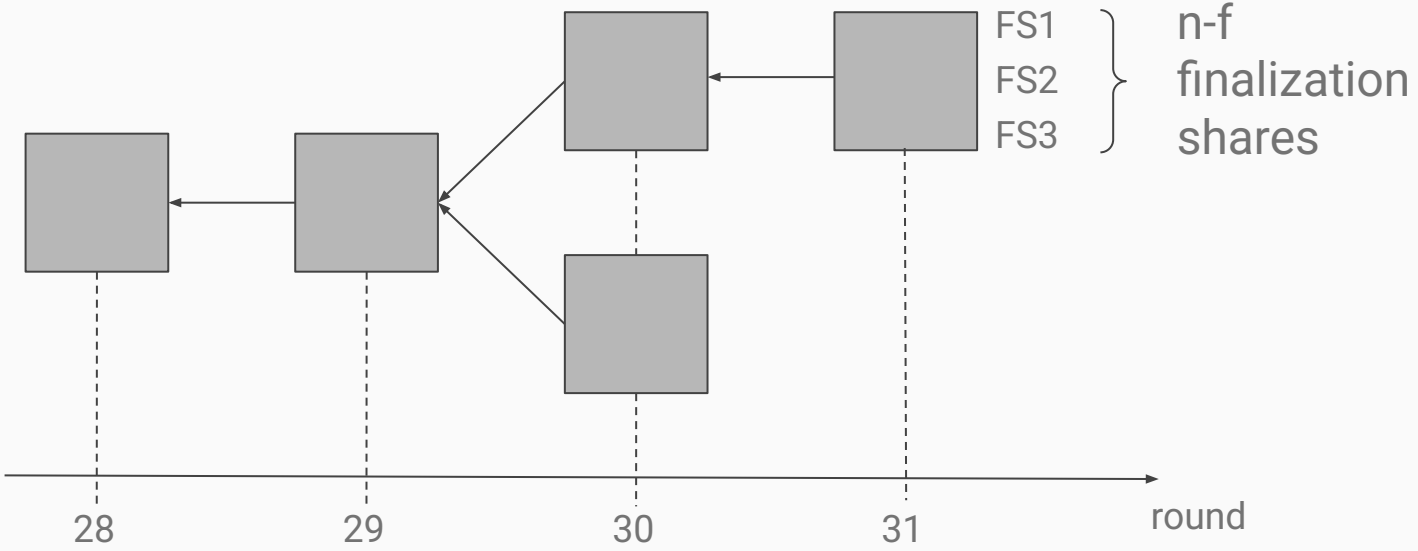
ICC: finalization



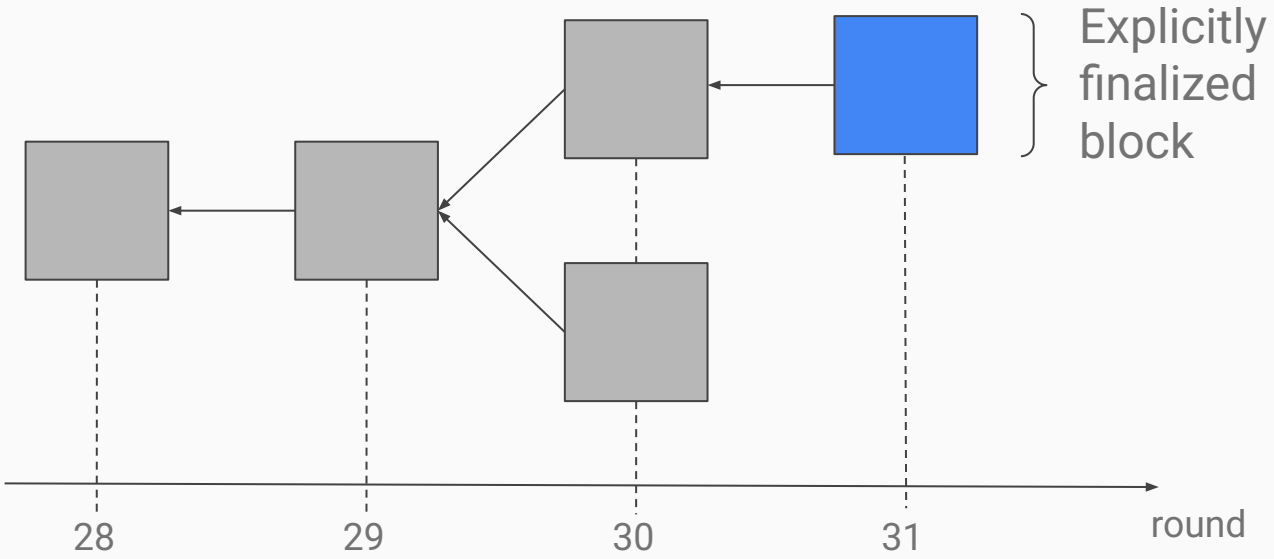
ICC: finalization



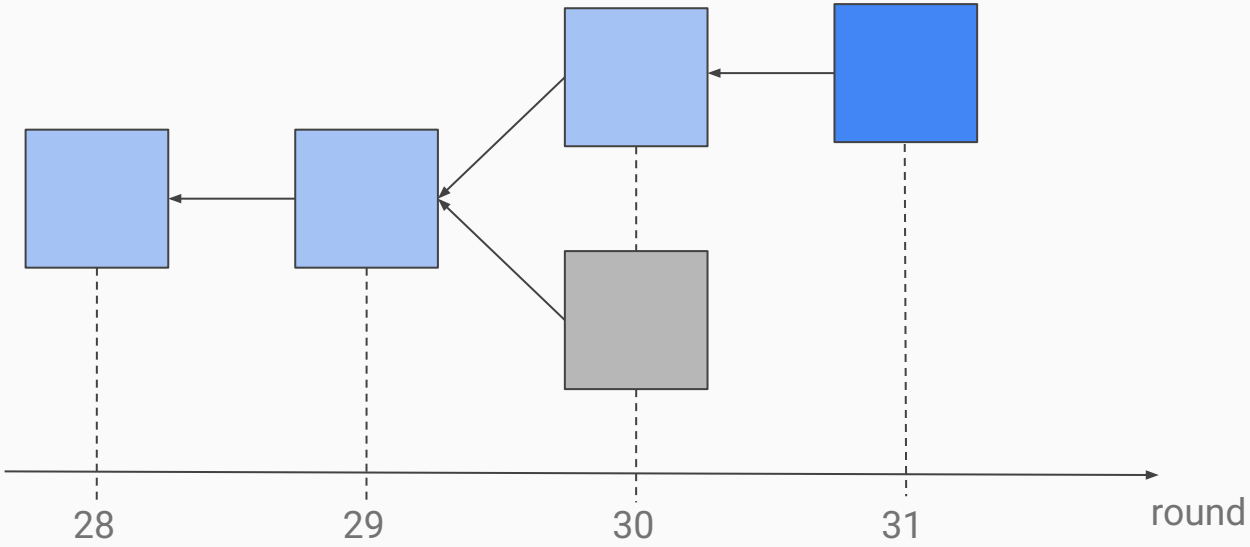
ICC: finalization



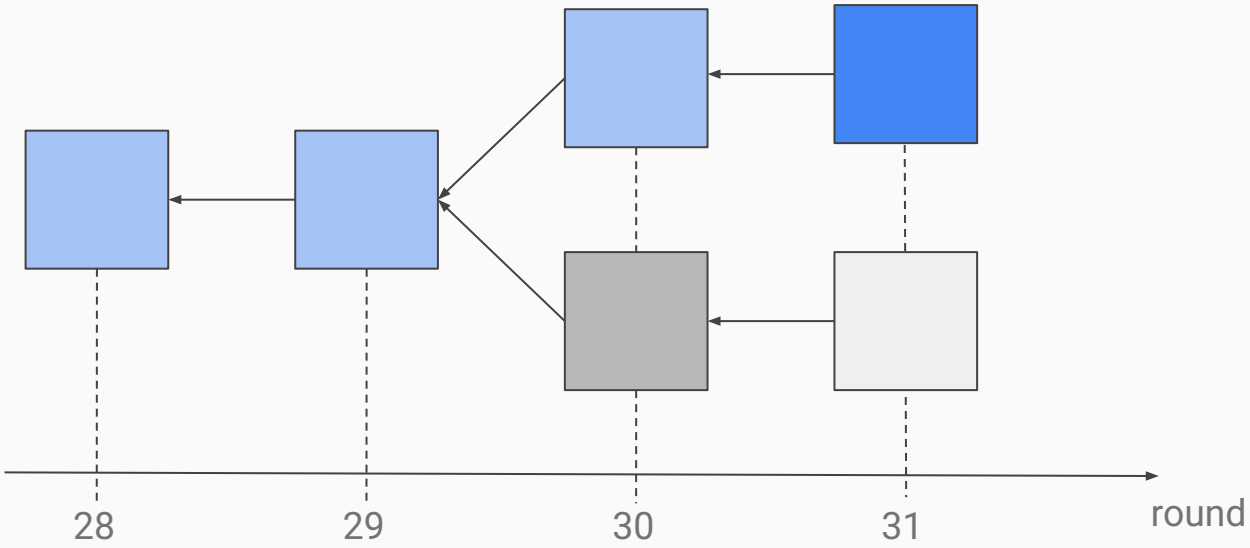
ICC: finalization



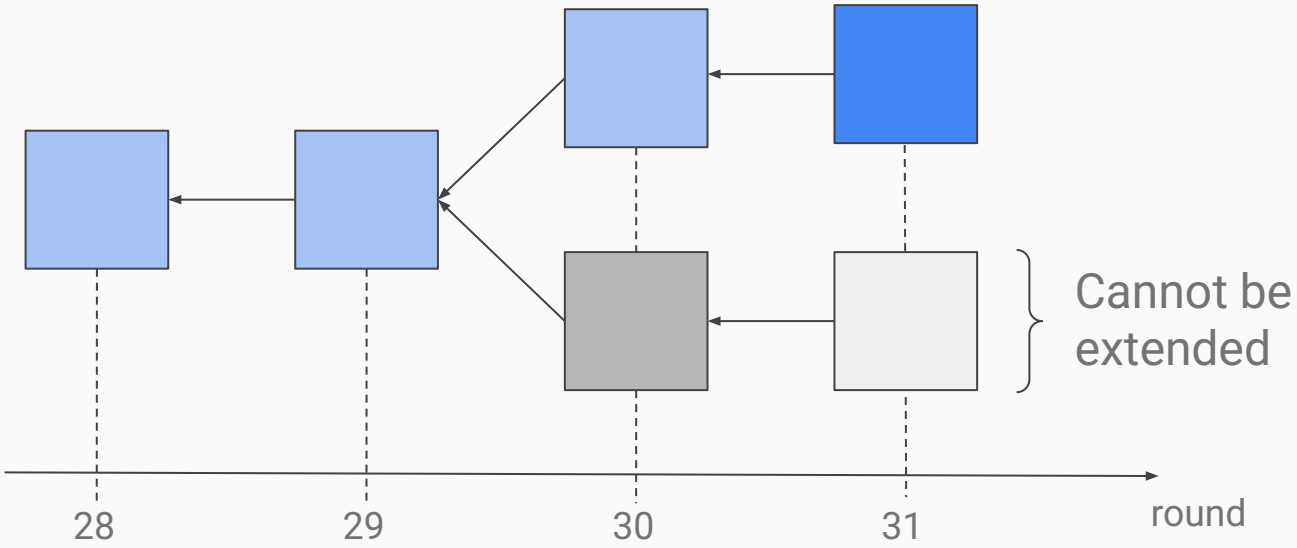
ICC: finalization



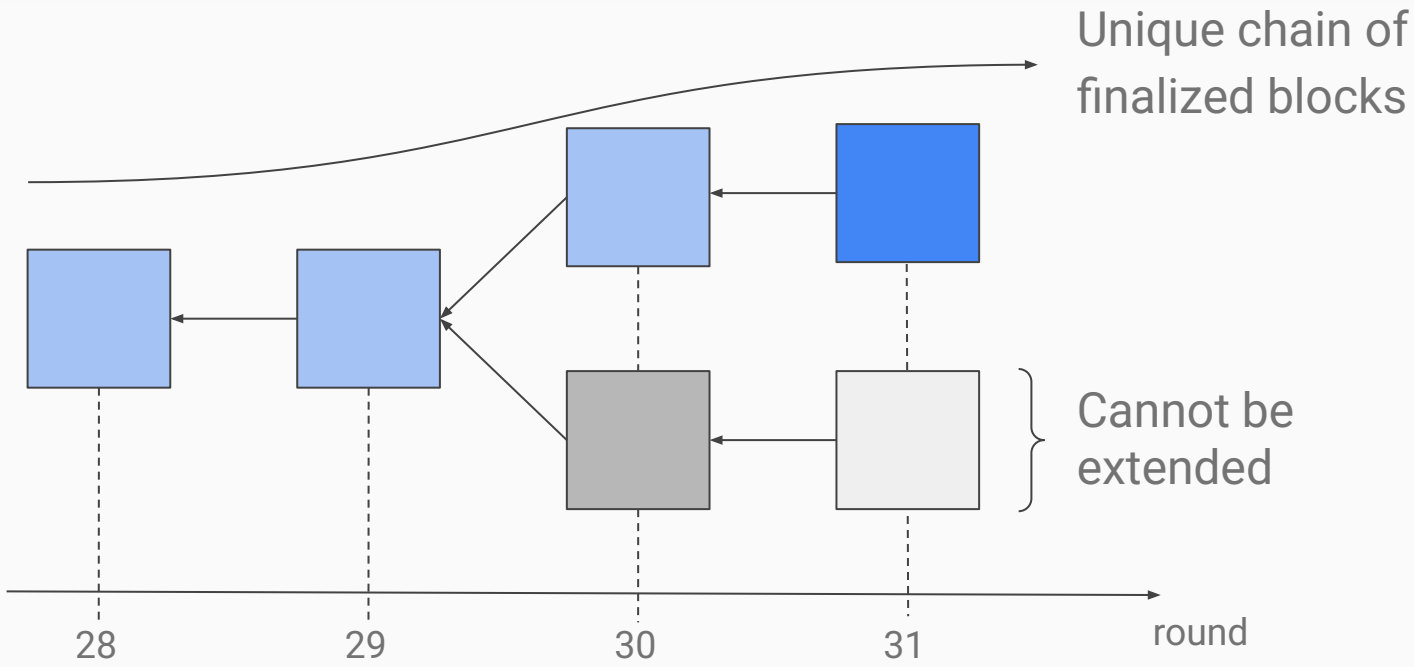
ICC: safety (n > 3f)



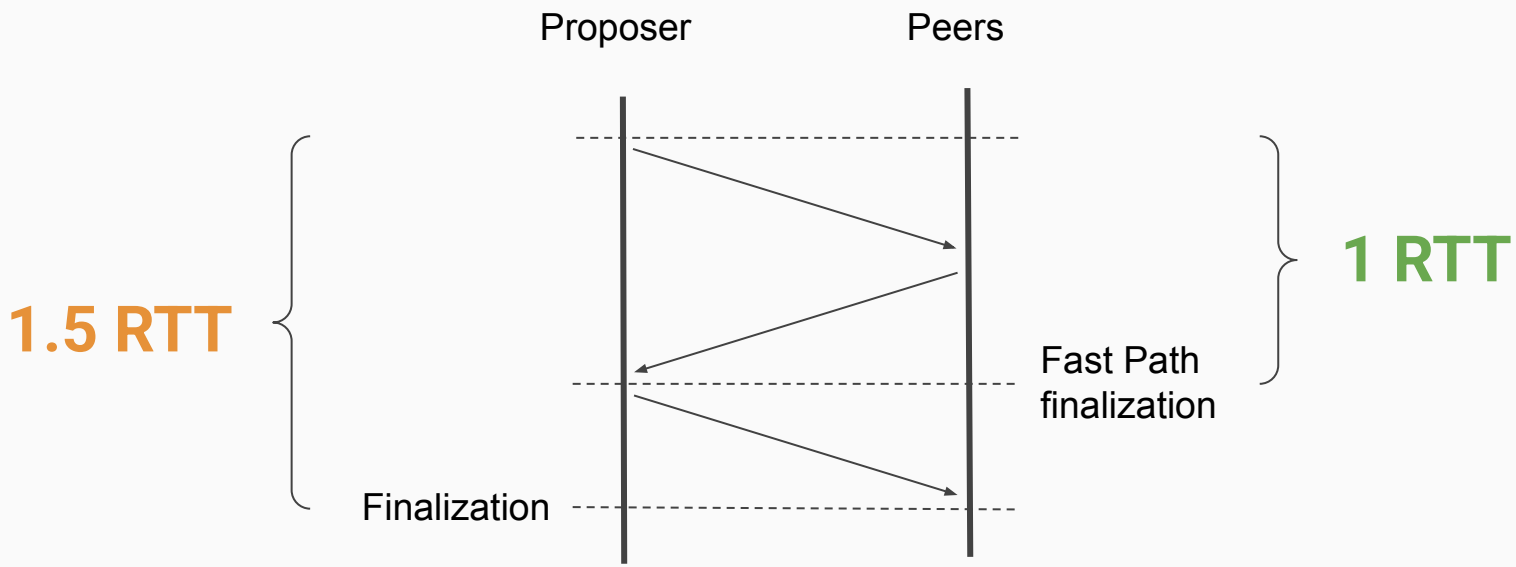
ICC: safety (n > 3f)



ICC: safety (n > 3f)



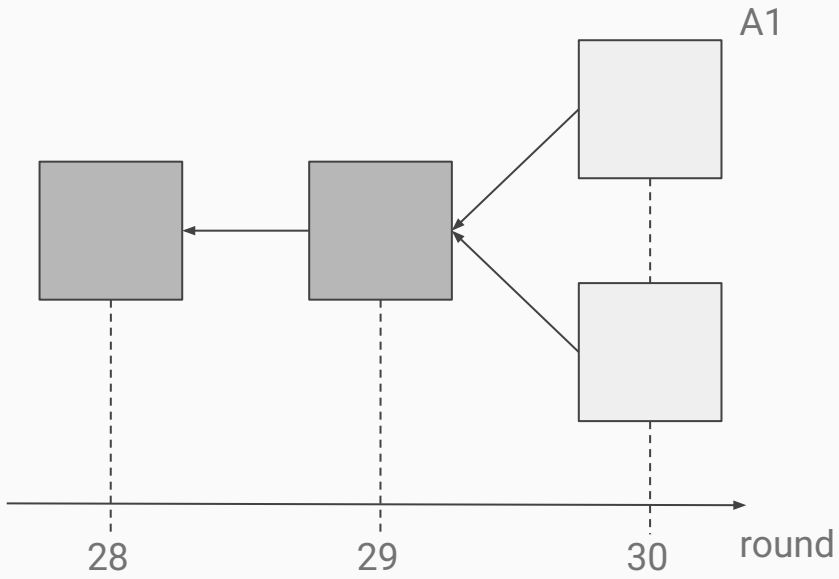
Fast Path


Proposer
Peers
1.5 RTT
1 RTT
Fast Path
finalization
Finalization

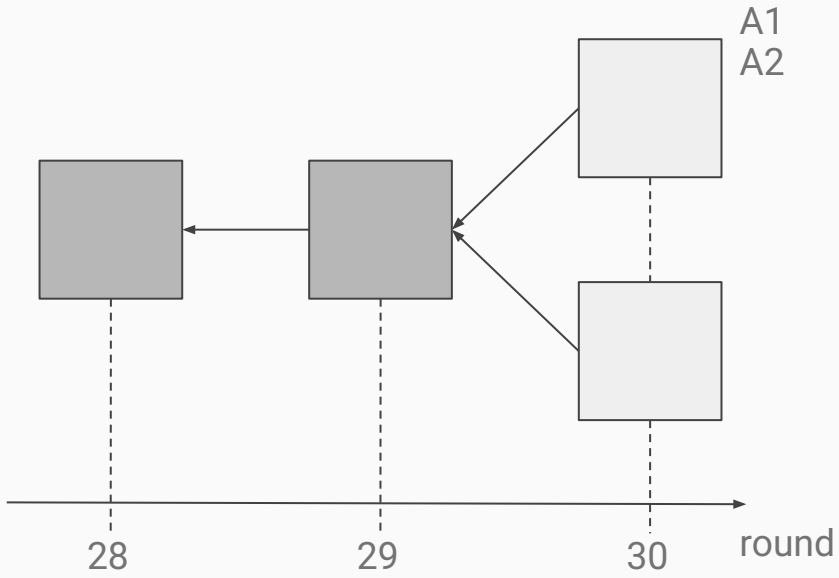
Consensus on Demand

Fast Path for any permissioned consensus protocol

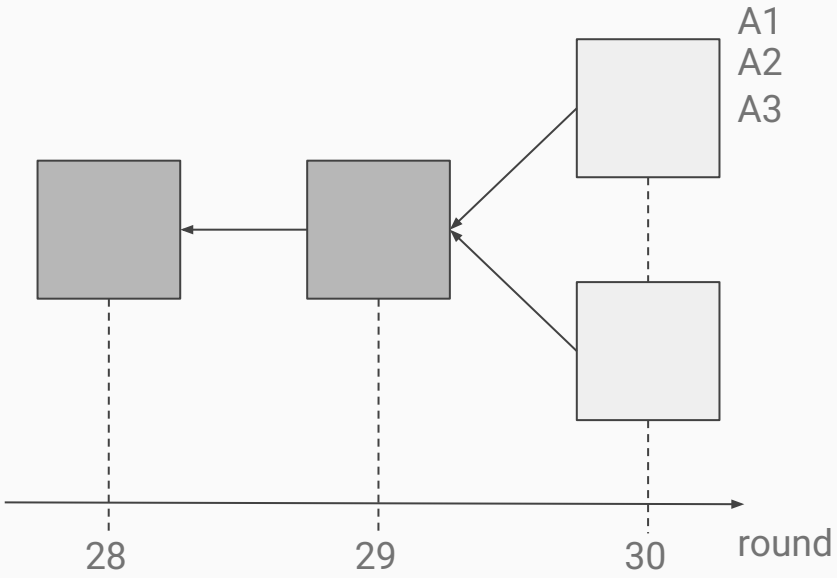
CoD: Fast Path



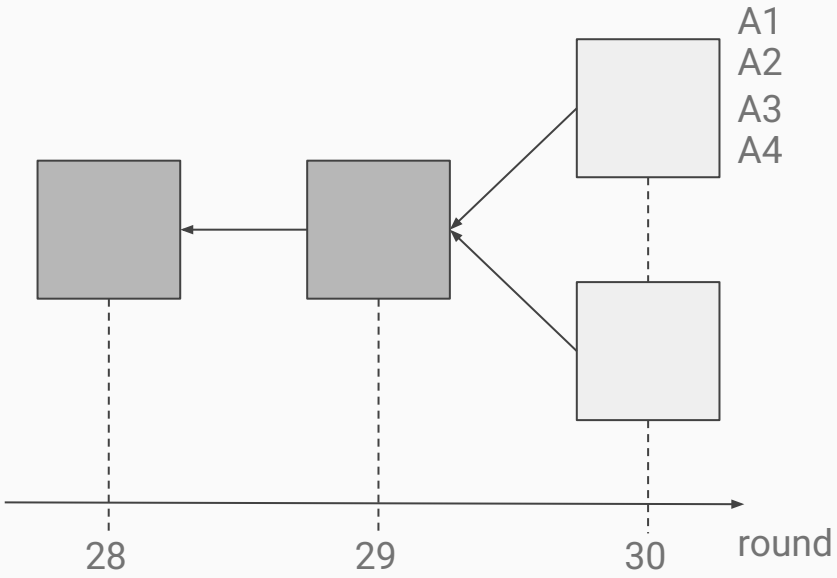
CoD: Fast Path



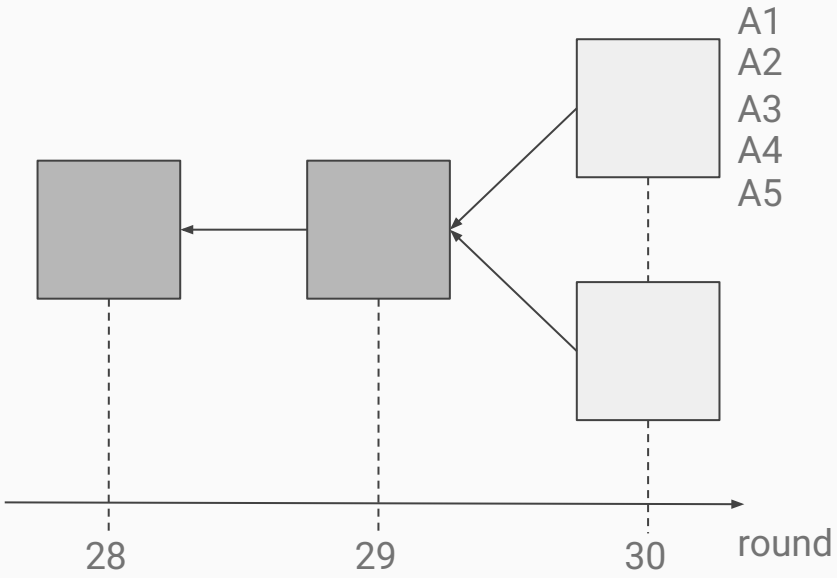
CoD: Fast Path



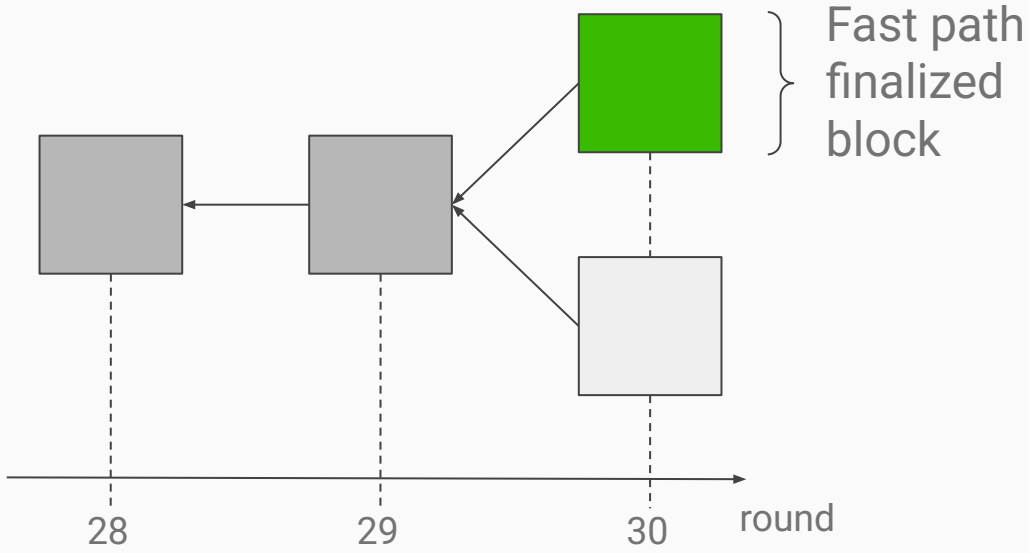
CoD: Fast Path



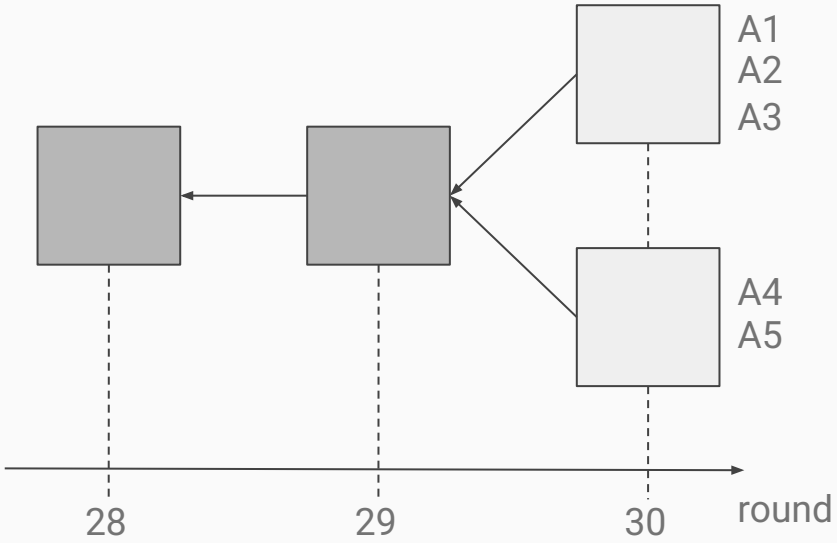
CoD: Fast Path



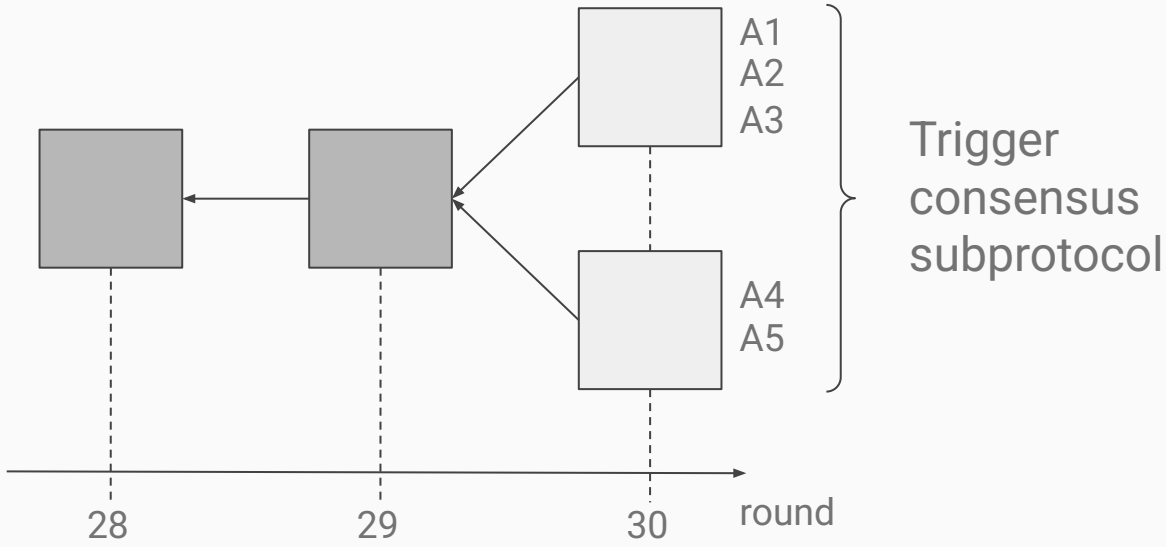
CoD: Fast Path



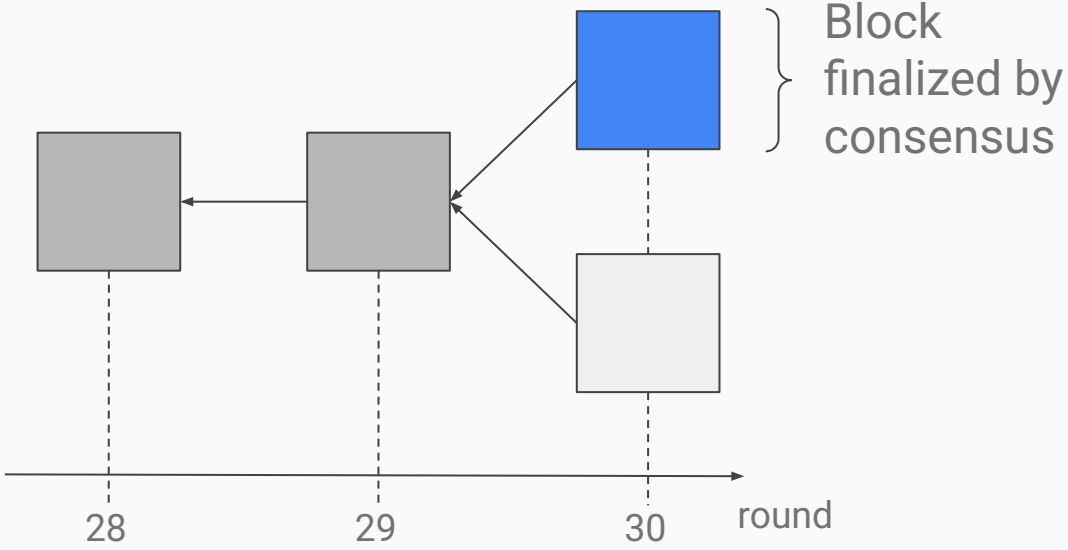
CoD: Consensus



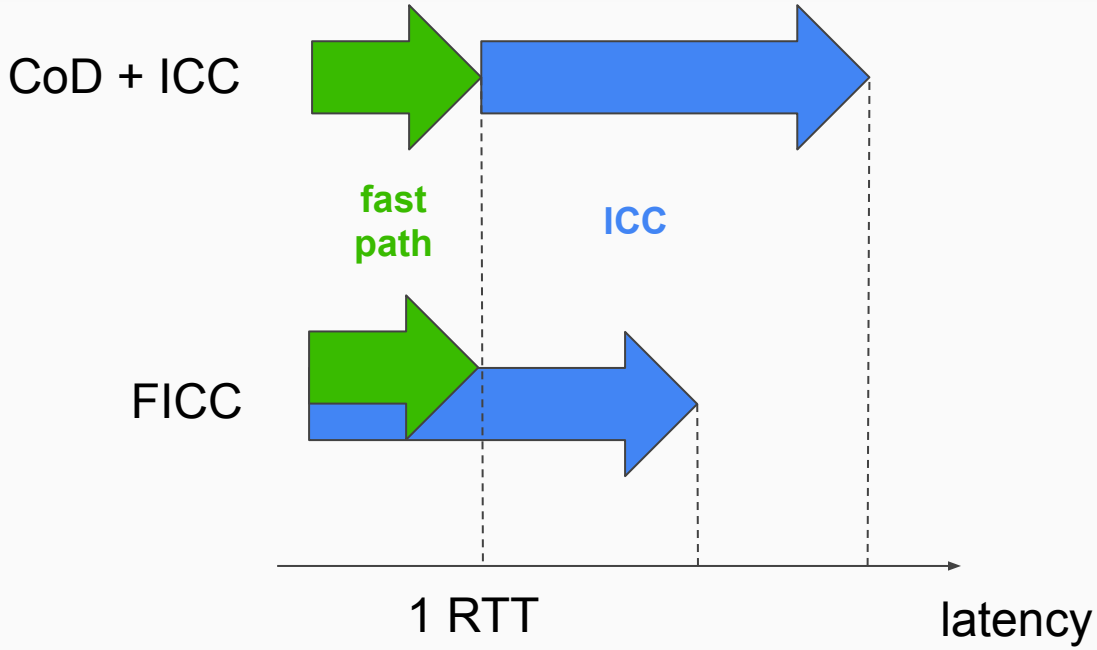
CoD: Consensus



CoD: Consensus



CoD vs FICC



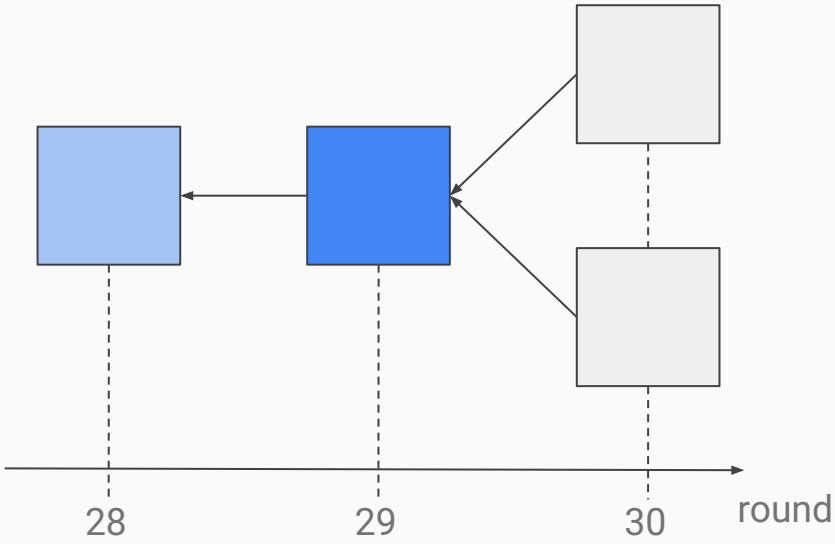
Fast Internet Computer Consensus

In each round:

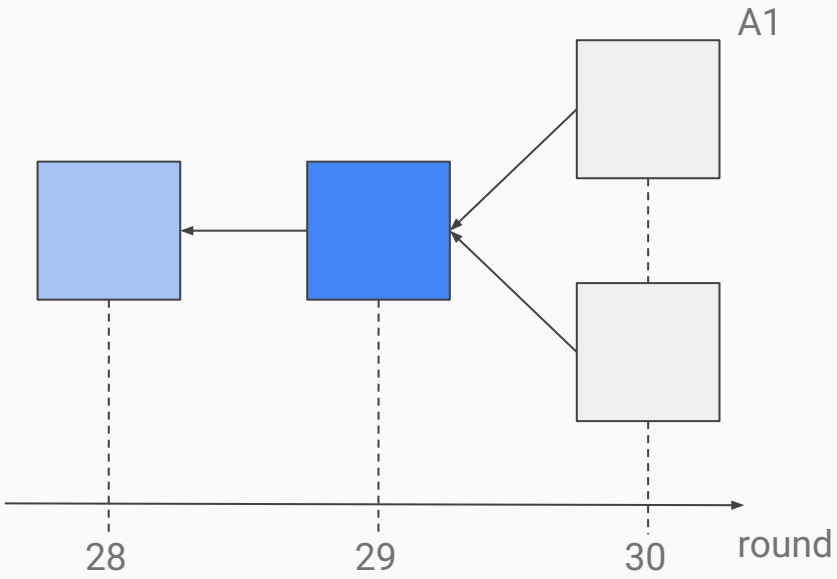
1. Goodify
2. Block proposal
3. Notarization*
4. FP-finalization
5. IC-finalization (eventually)

* modified

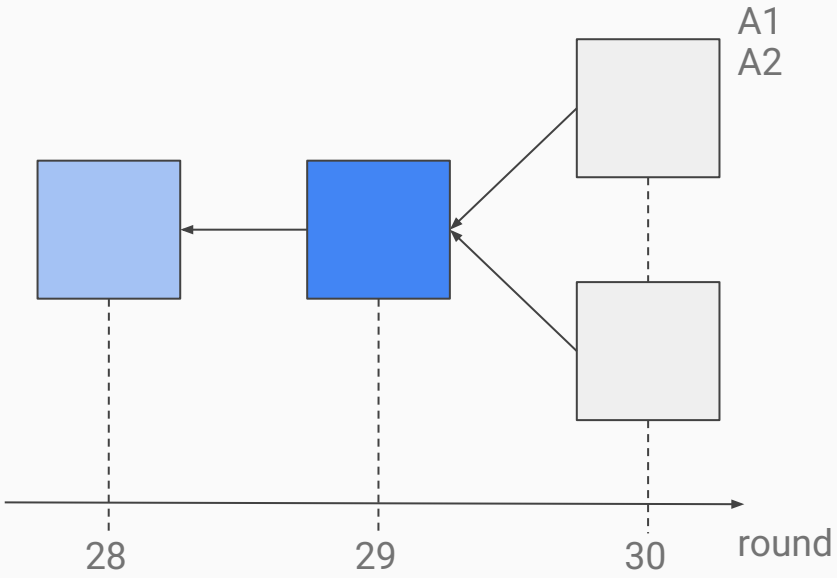
FICC: notarization



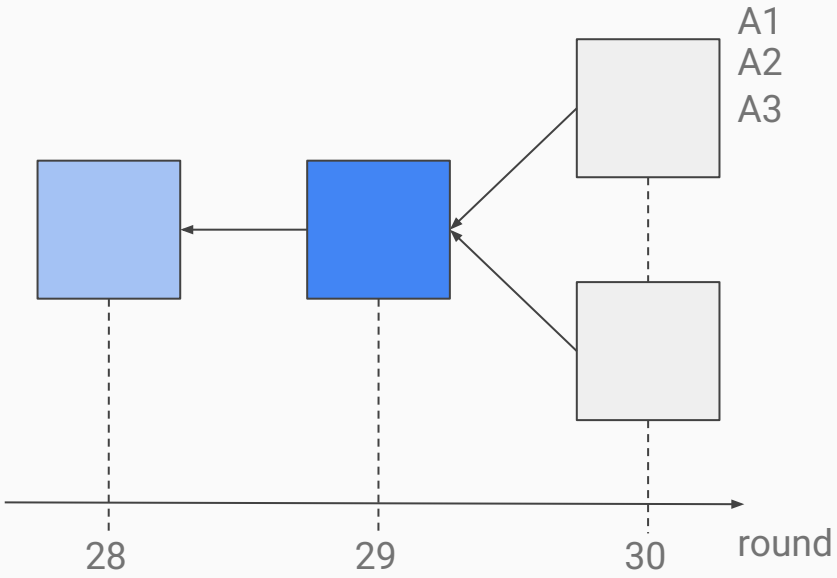
FICC: notarization



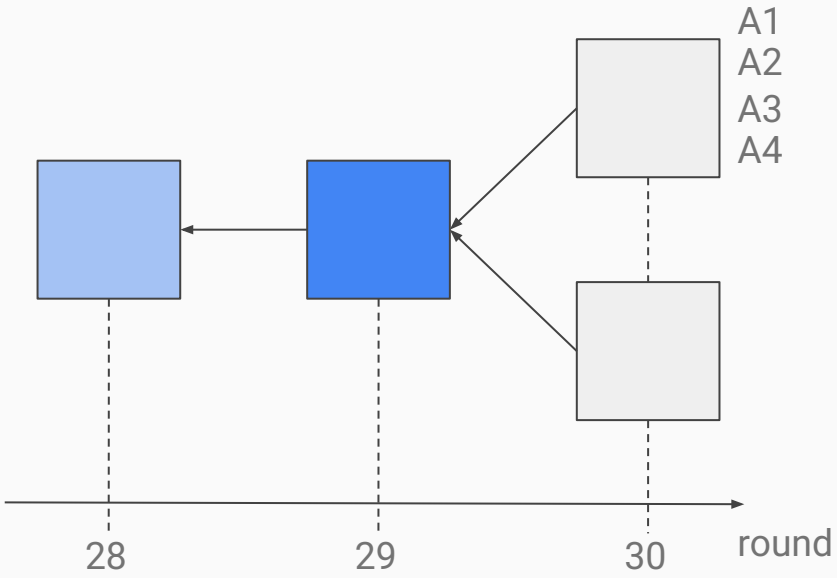
FICC: notarization



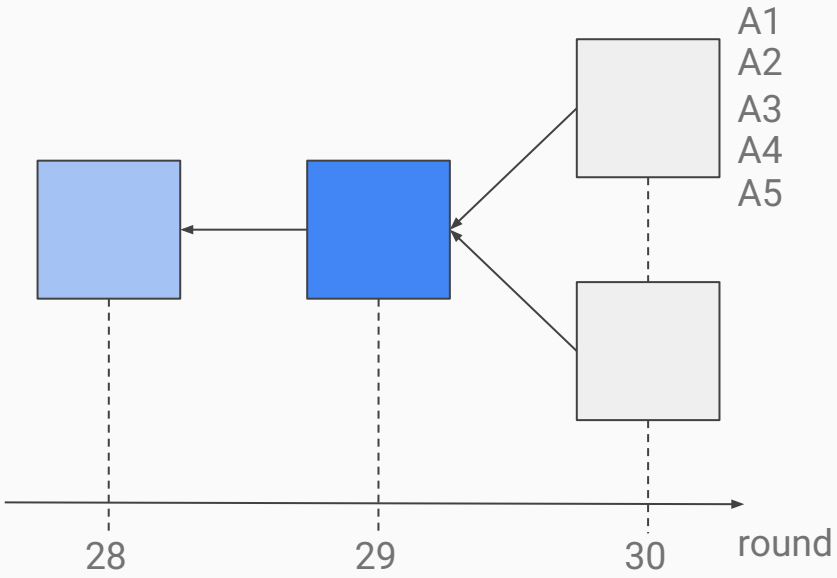
FICC: notarization



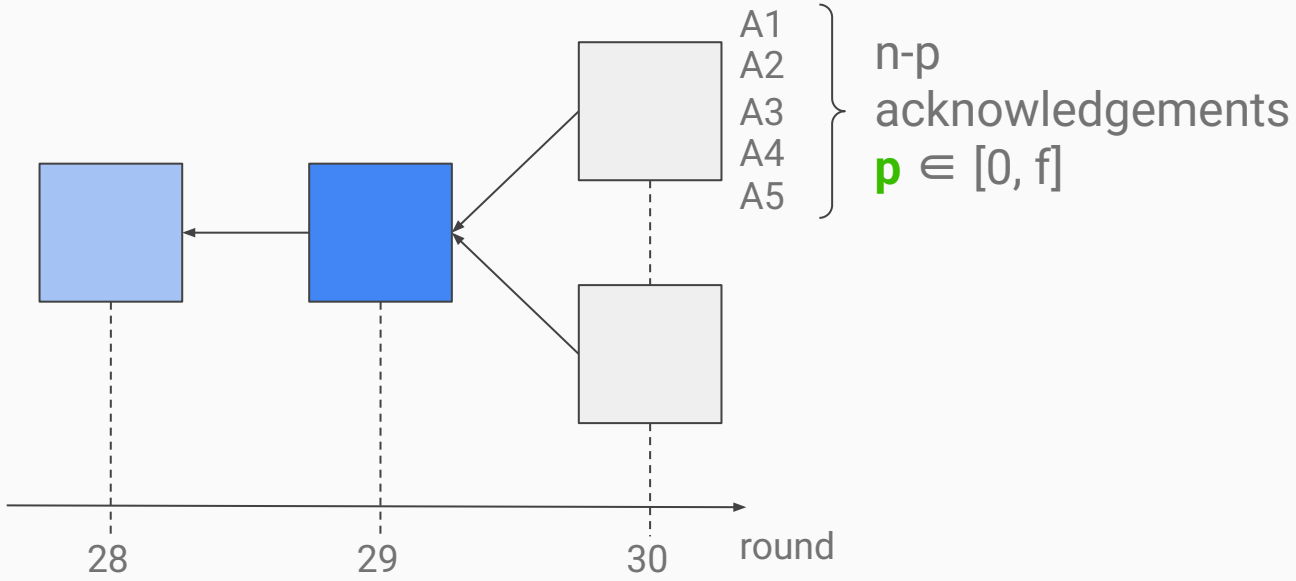
FICC: notarization



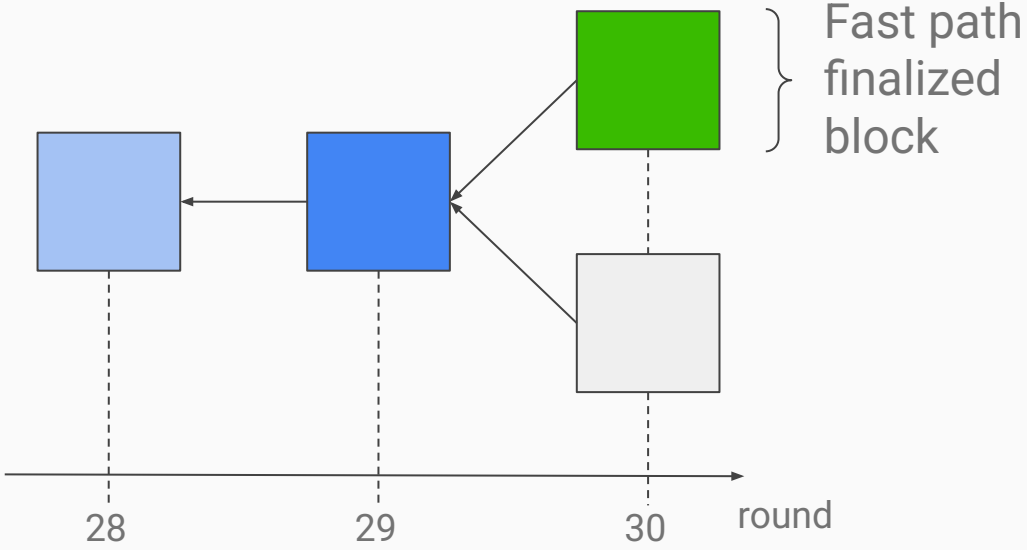
FICC: notarization



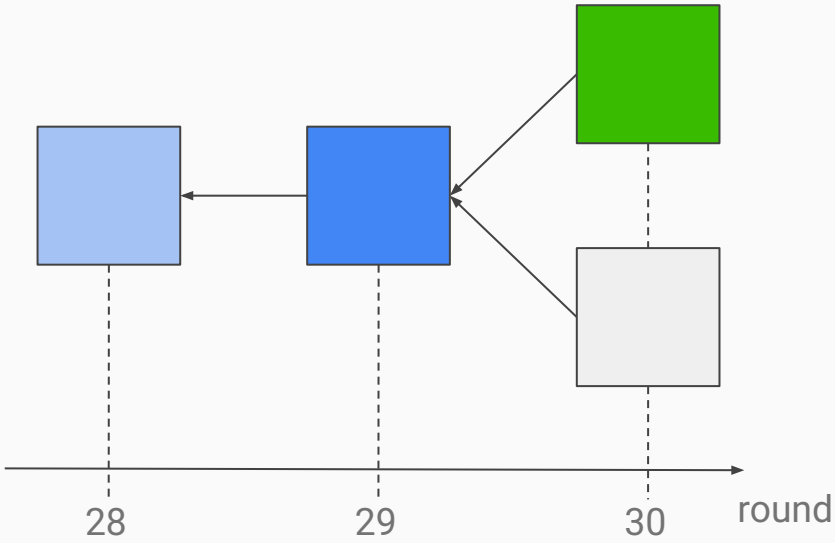
FICC: FP-finalization



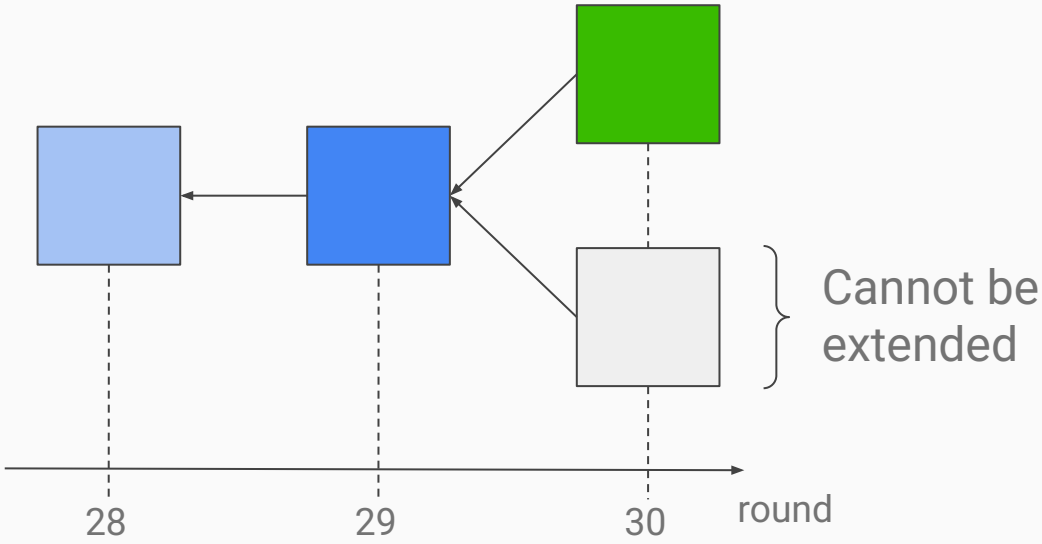
FICC: FP-finalization



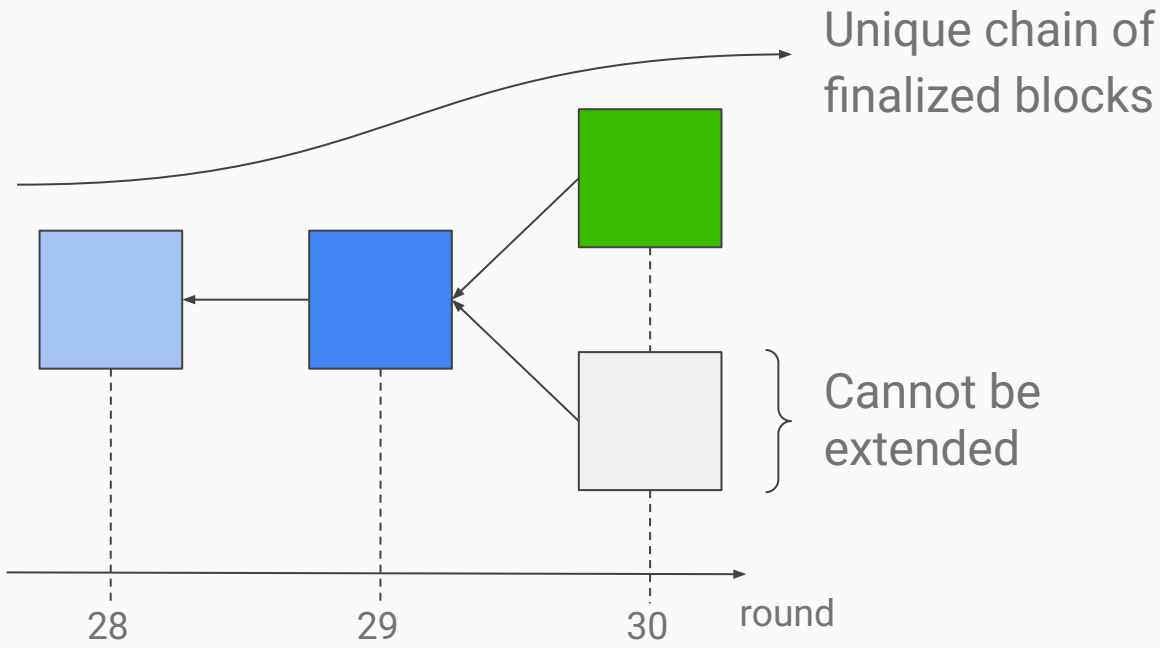
FICC: safety (n > 3f + 2p)



FICC: safety (n > 3f + 2p)

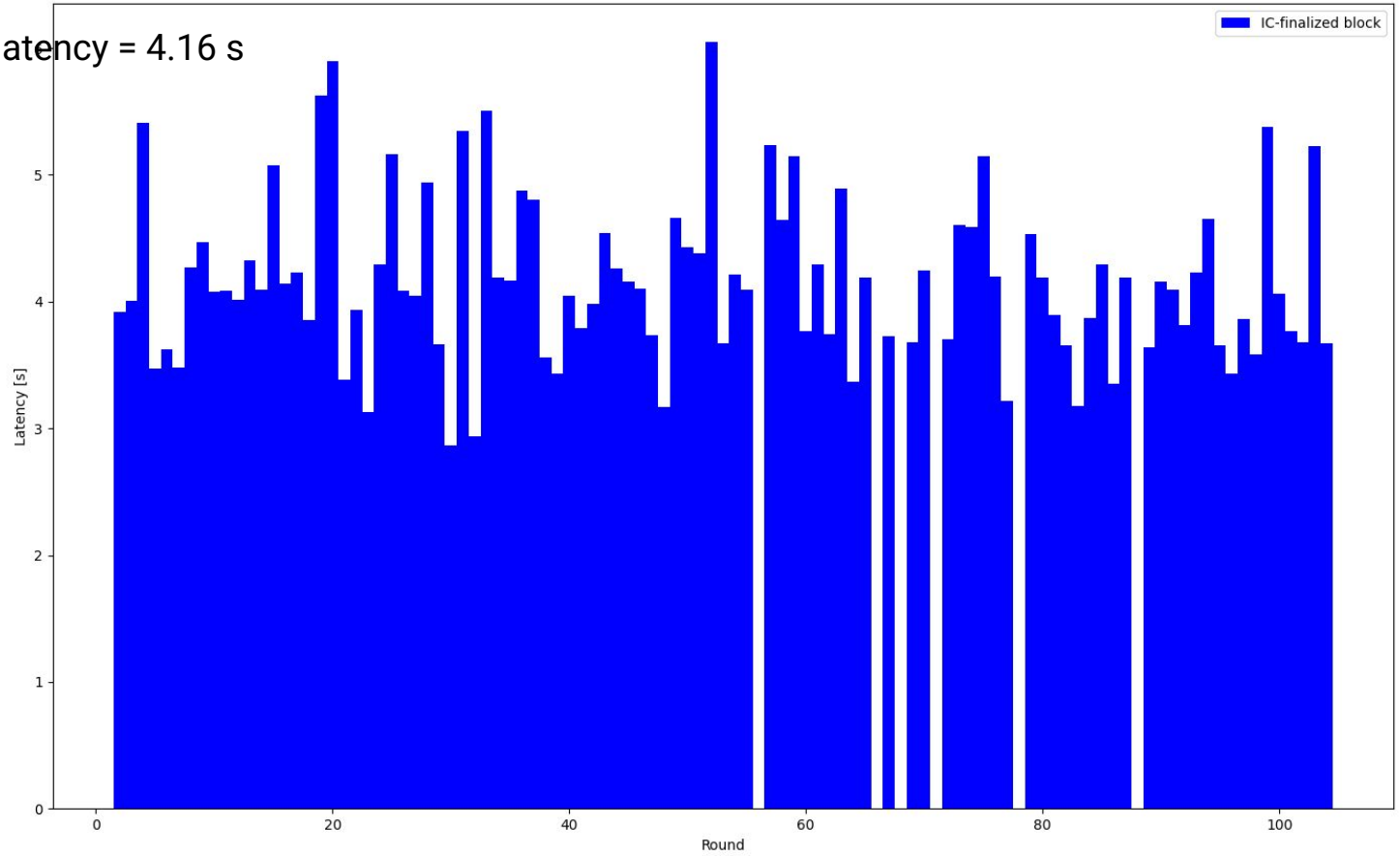


FICC: safety (n > 3f + 2p)

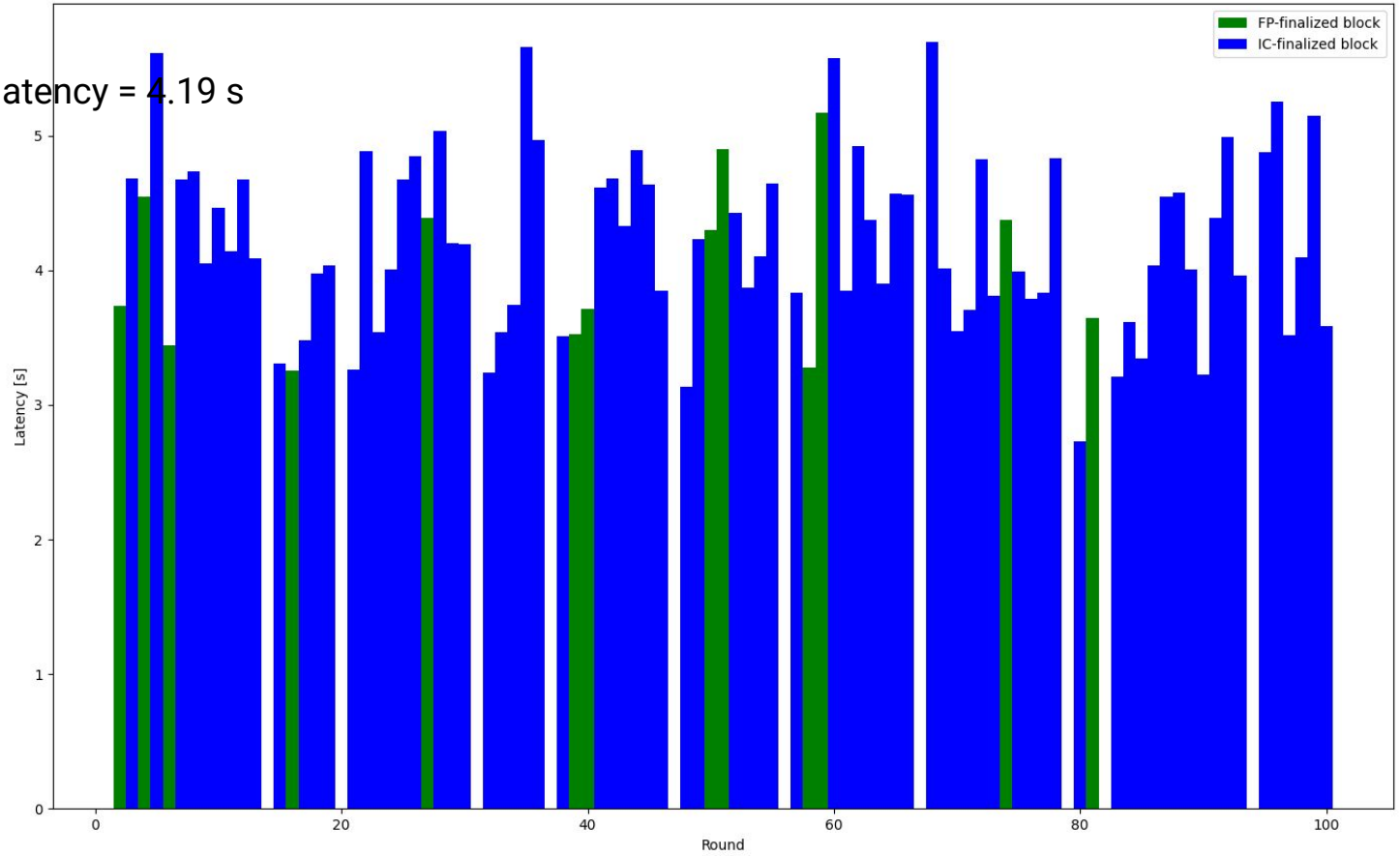


Benchmarks

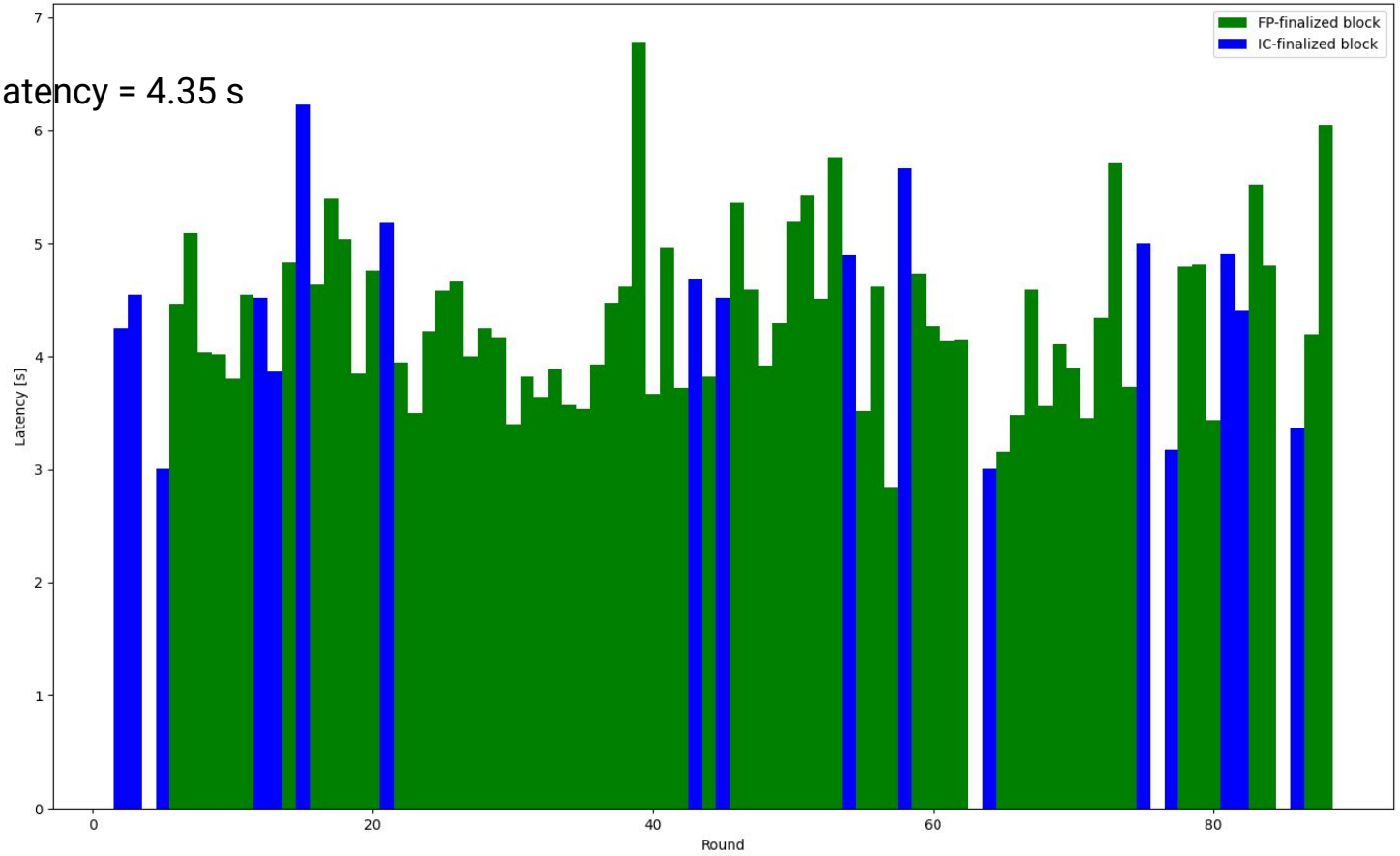
ICC
n = 16
f = 5
Average latency = 4.16 s



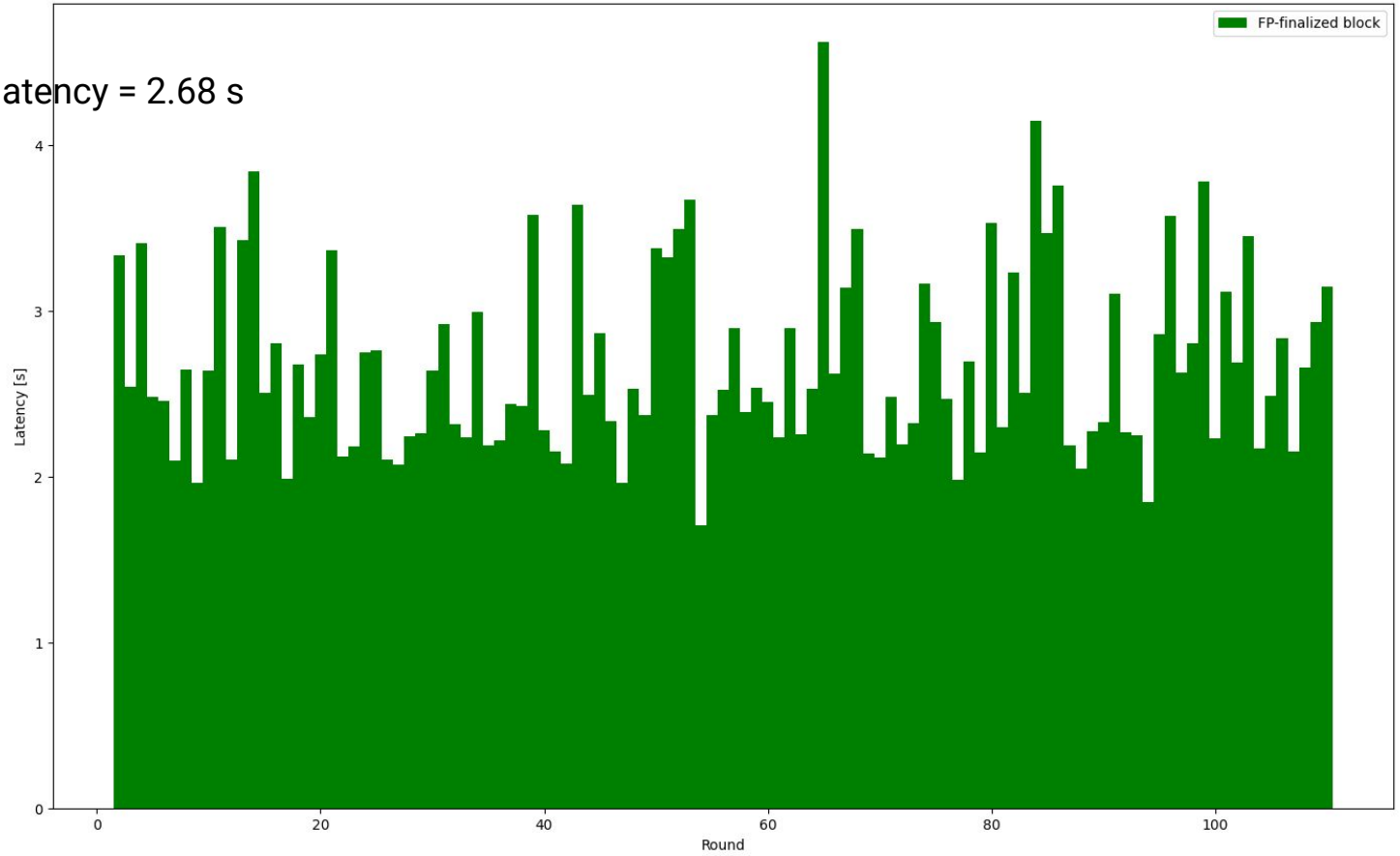
FICC
n = 16
f = 5
p = 0
Average latency = 4.19 s

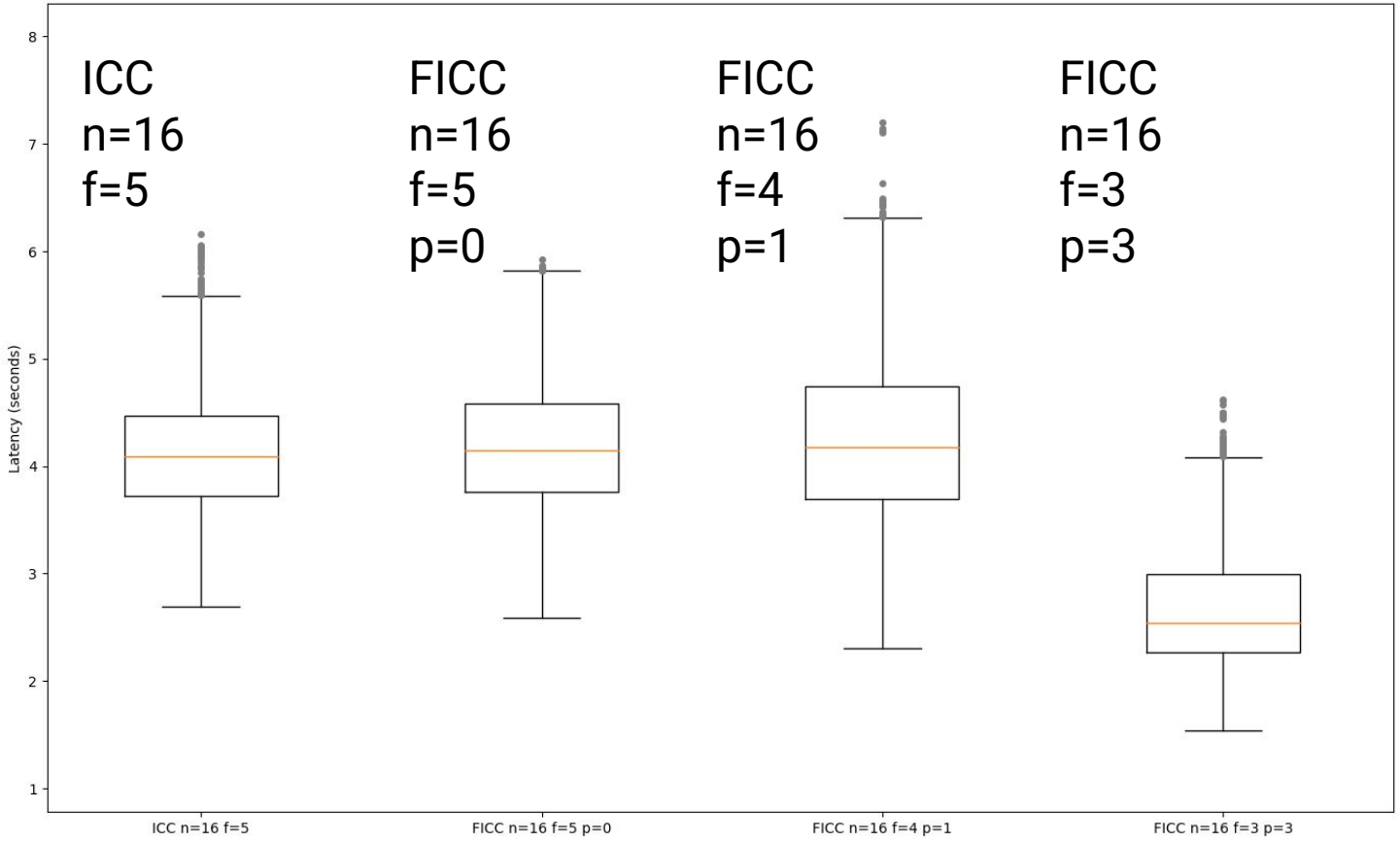


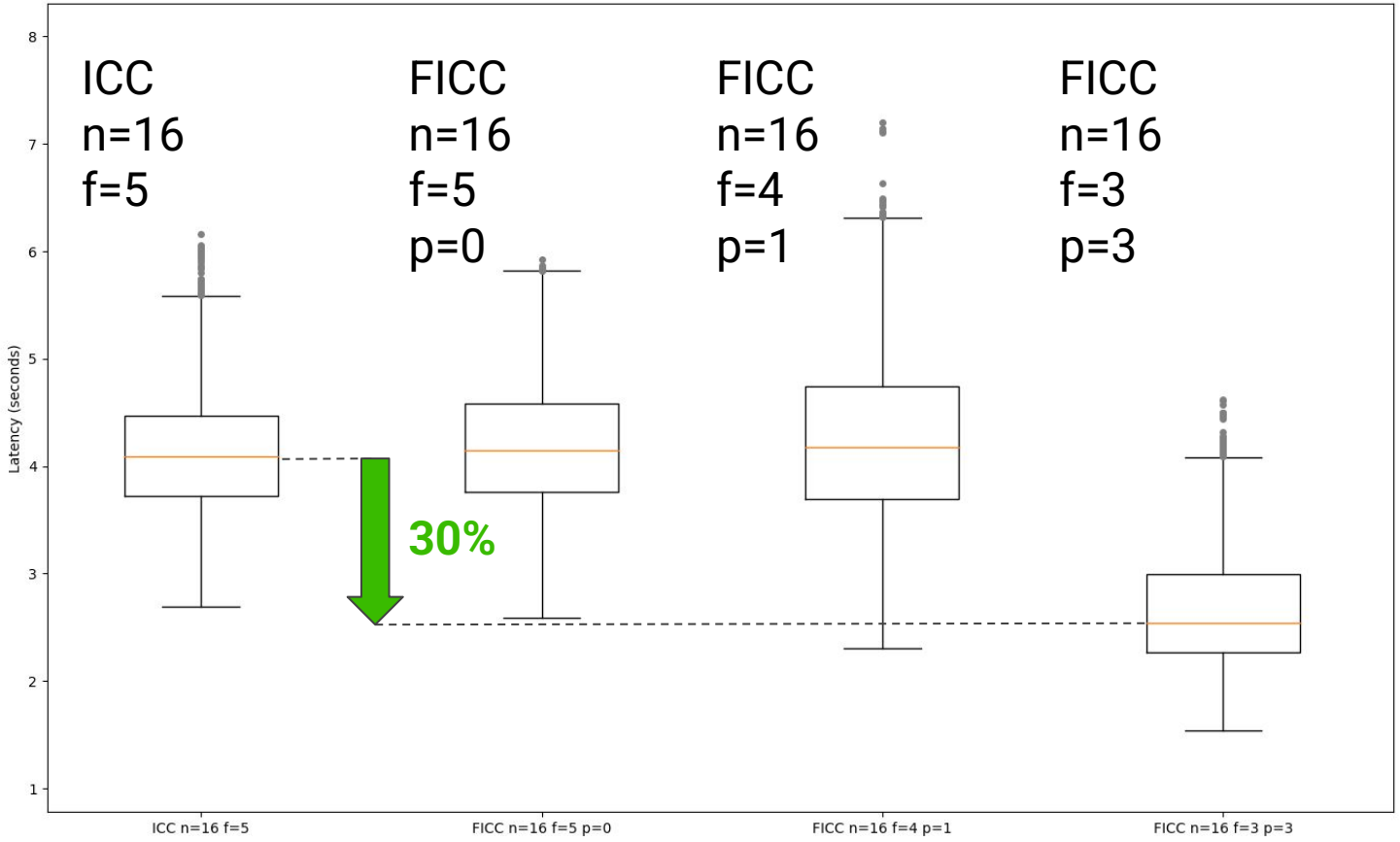
FICC
n = 16
f = 4
p = 1
Average latency = 4.35 s

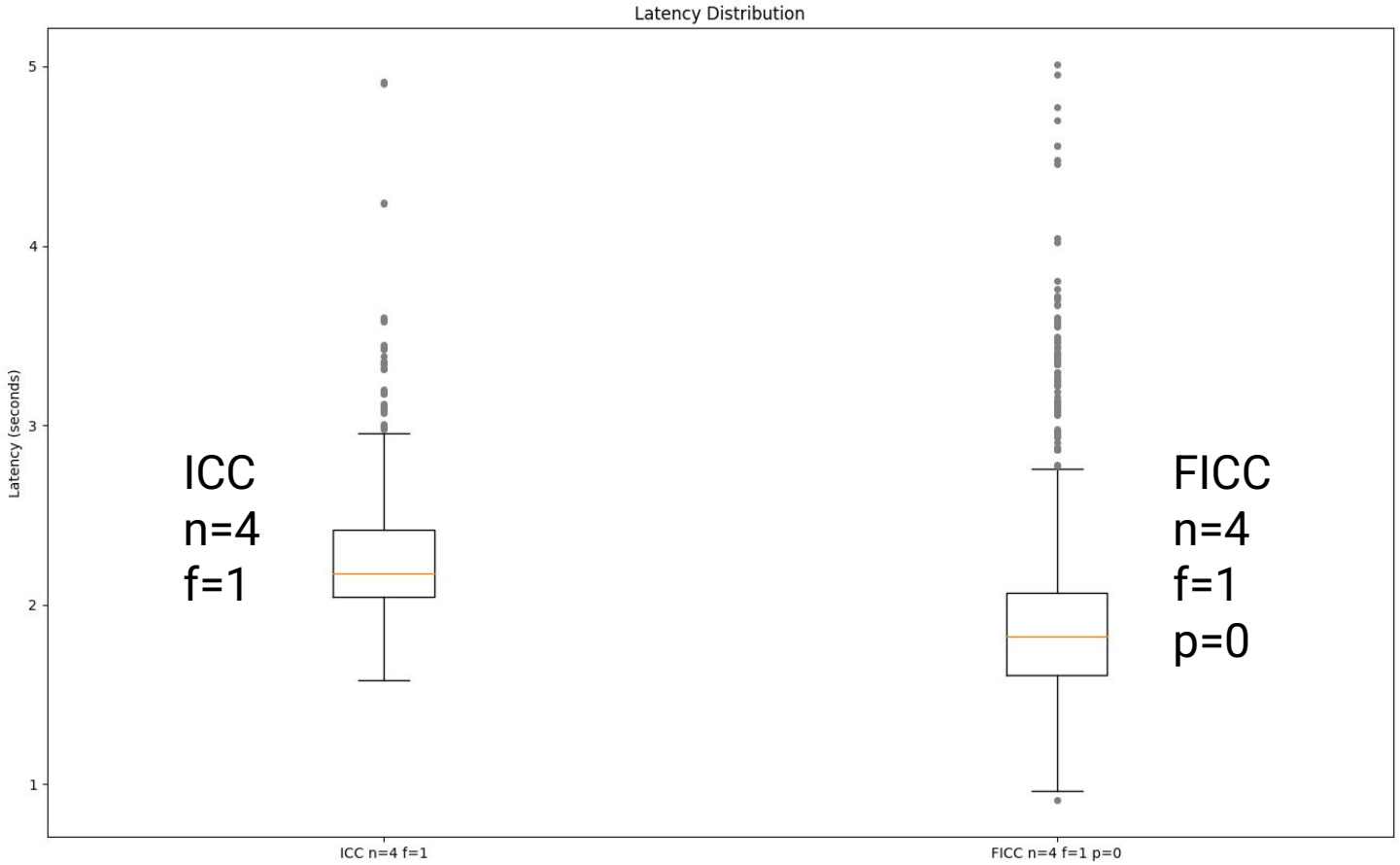


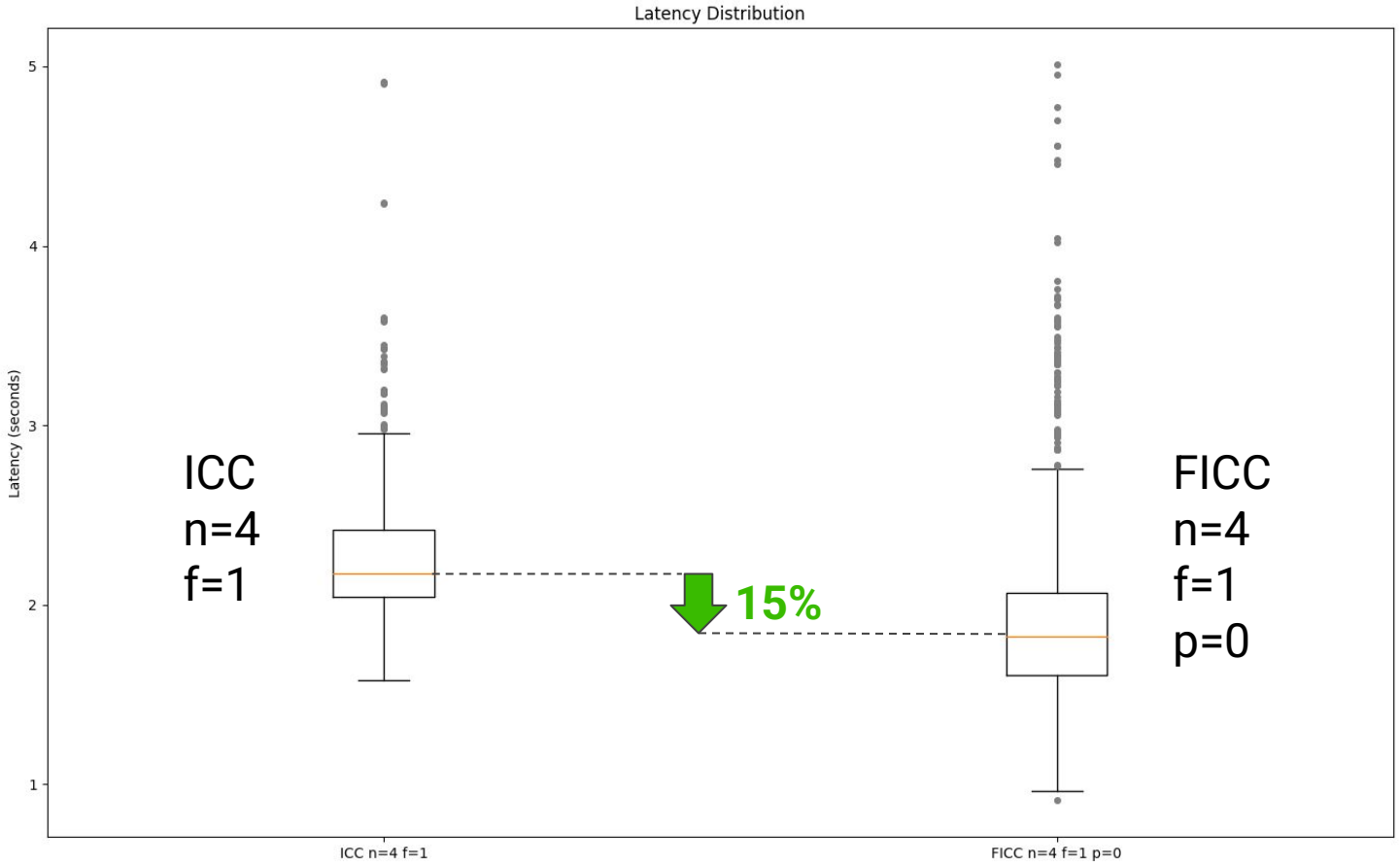
FICC
n = 16
f = 3
p = 3
Average latency = 2.68 s




ICC
n=16
f=5
FICC
n=16
f=5
p=0
FICC
n=16
f=4
p=1
FICC
n=16
f=3
p=3
Latency (seconds)
1
2
3
4
5
6
7
8
ICC n=16 f=5
FICC n=16 f=5 p=0
FICC n=16 f=4 p=1
FICC n=16 f=3 p=3


ICC
n=16
f=5
FICC
n=16
f=5
p=0
FICC
n=16
f=4
p=1
FICC
n=16
f=3
p=3
30%
Latency (seconds)
1
2
3
4
5
6
7
8
ICC n=16 f=5
FICC n=16 f=5 p=0
FICC n=16 f=4 p=1
FICC n=16 f=3 p=3


Latency Distribution
Latency (seconds)
5
4
3
2
1
ICC
n=4
f=1
FICC
n=4
f=1
p=0
ICC n=4 f=1
FICC n=4 f=1 p=0


Latency Distribution
Latency (seconds)
5
4
3
2
1
ICC
n=4
f=1
15%
FICC
n=4
f=1
p=0
ICC n=4 f=1
FICC n=4 f=1 p=0

Summary

FICC reduces latency

Summary

FICC reduces latency

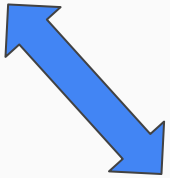
p = f

(implies f < n/5)

30%

Summary

FICC reduces latency



p = f

(implies f < n/5)

30%

p = 0 and

“localized” and

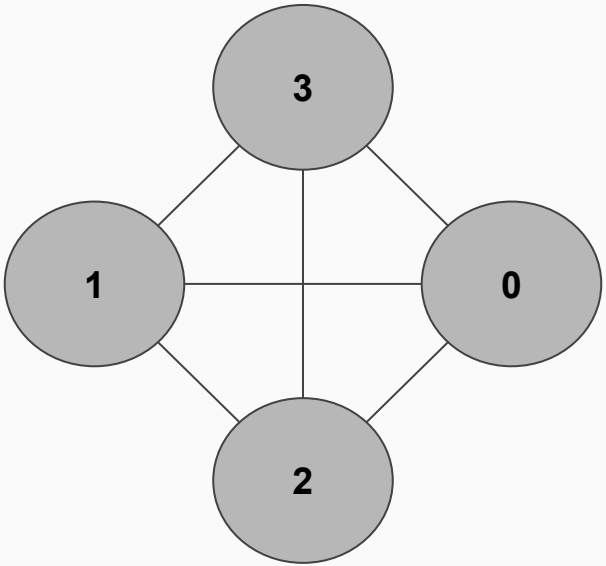
few replicas

Thank you :)

Q&A

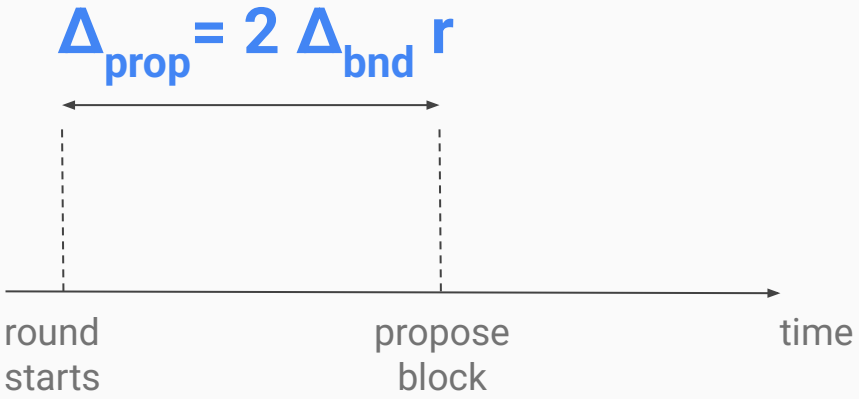
ICC

ICC: random beacon



Random ranking of replicas for each round

ICC: block proposal



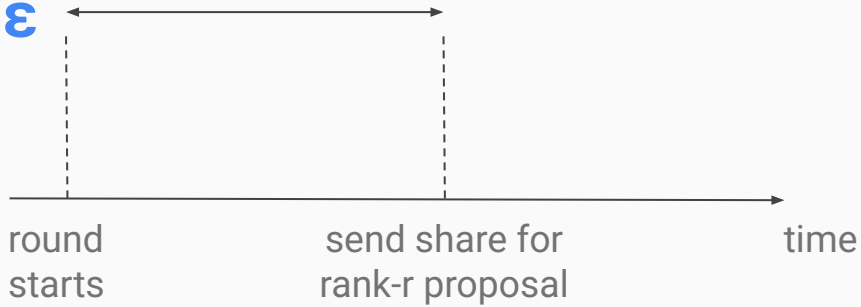
Δ_{prop}: proposal delay

Δ_{bnd} : network delay bound

r : rank of replica

ICC: notarization

$\Delta_{notar} = 2\,\Delta_{bnd}\,r + \varepsilon$

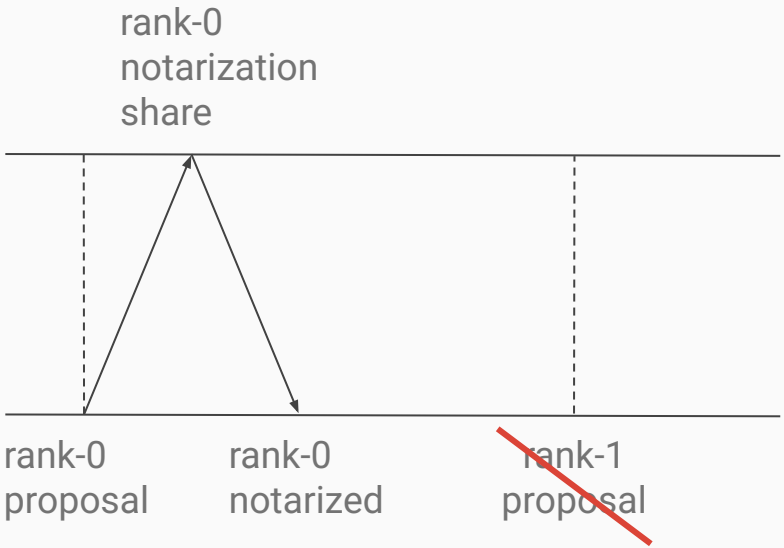


Δ_{notar} : notarization delay

Δ_{bnd} : network delay bound

r : rank of replica

Why these delays?



Synchronous network

One block added to the block tree

FICC

FICC: goodify

M_B: most acked child of block B

$p \in [0, f]$

FICC: goodify

M_B: most acked child of block B

$p \in [0, f]$

n-f acks on children of B

M_B is good

f+p+1 acks on children of B other than M_B

all children are good

Why goodness rules?

M_B only good child

M_B might get FP-finalized

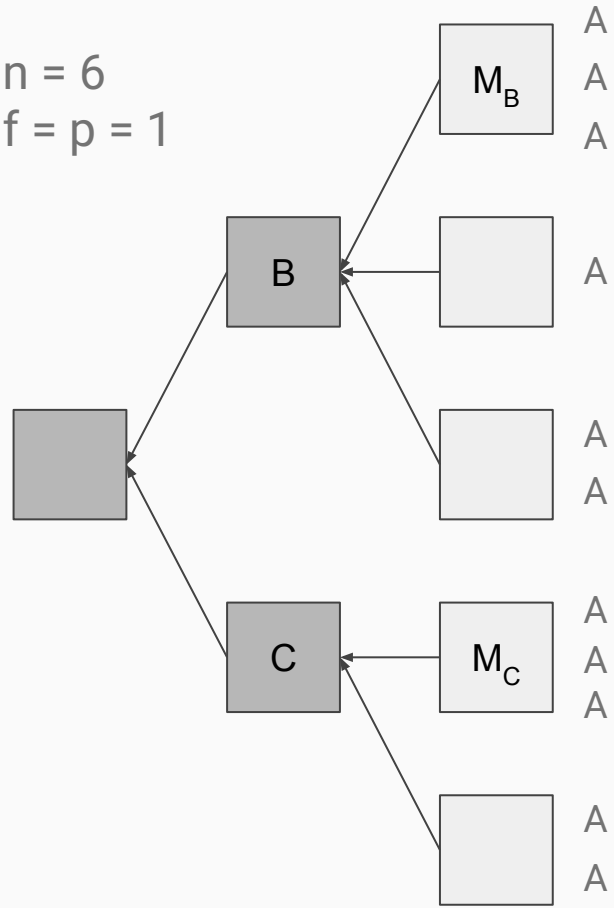
No other child extended

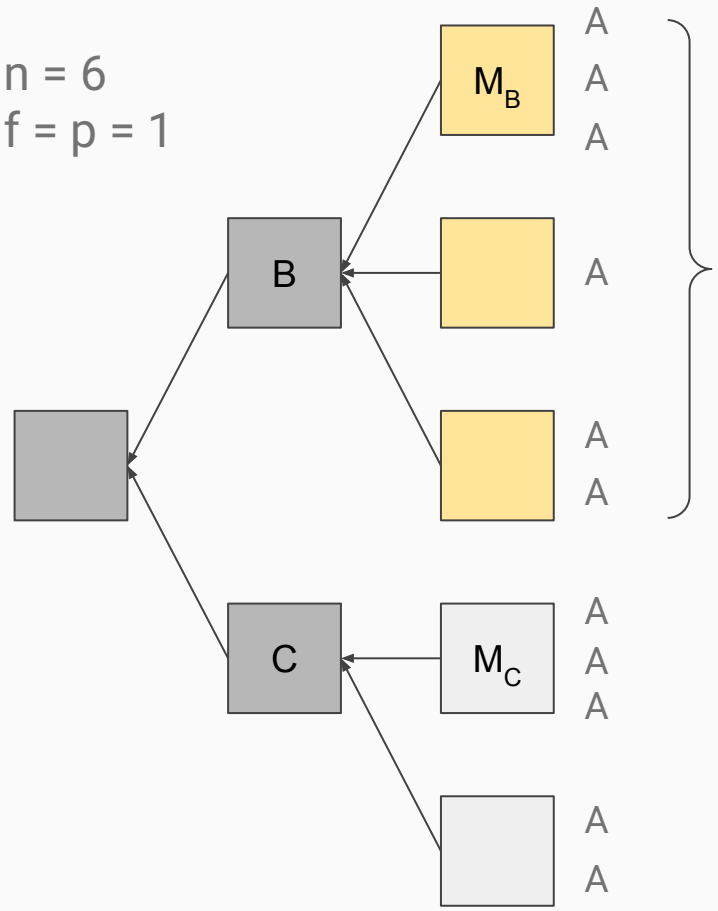
All children good

No FP-finalized child

Any child can be extended

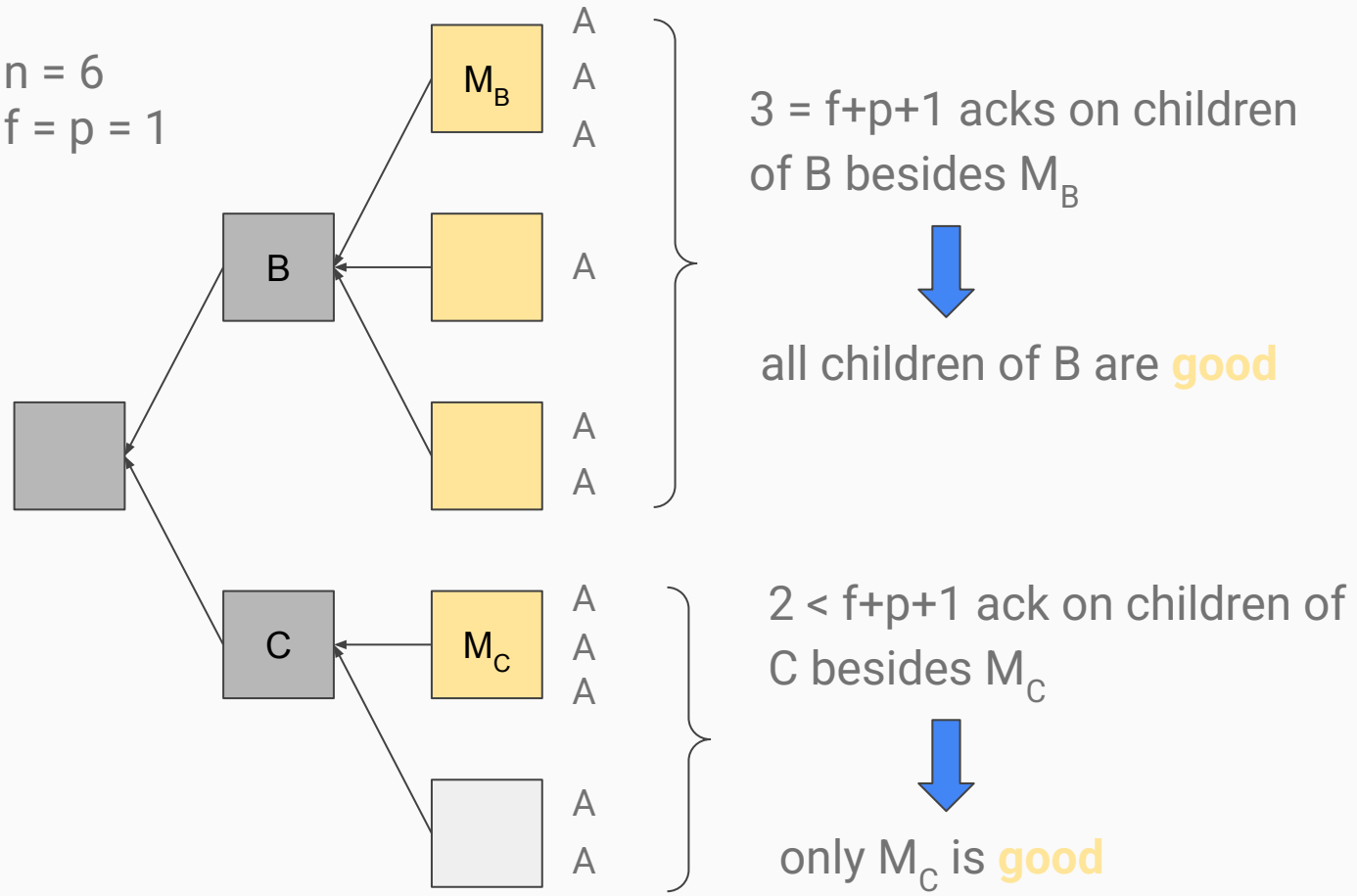
n = 6
f = p = 1

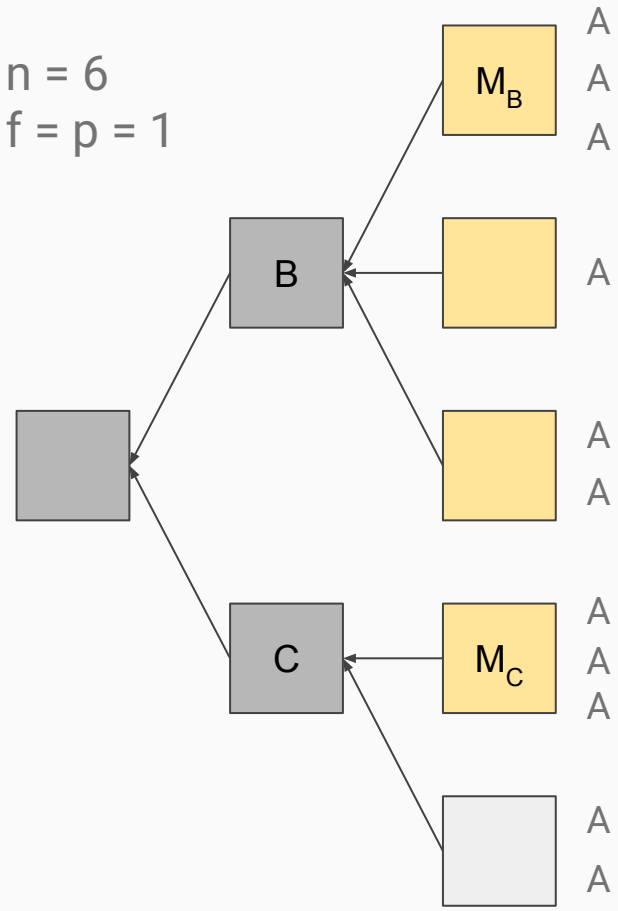


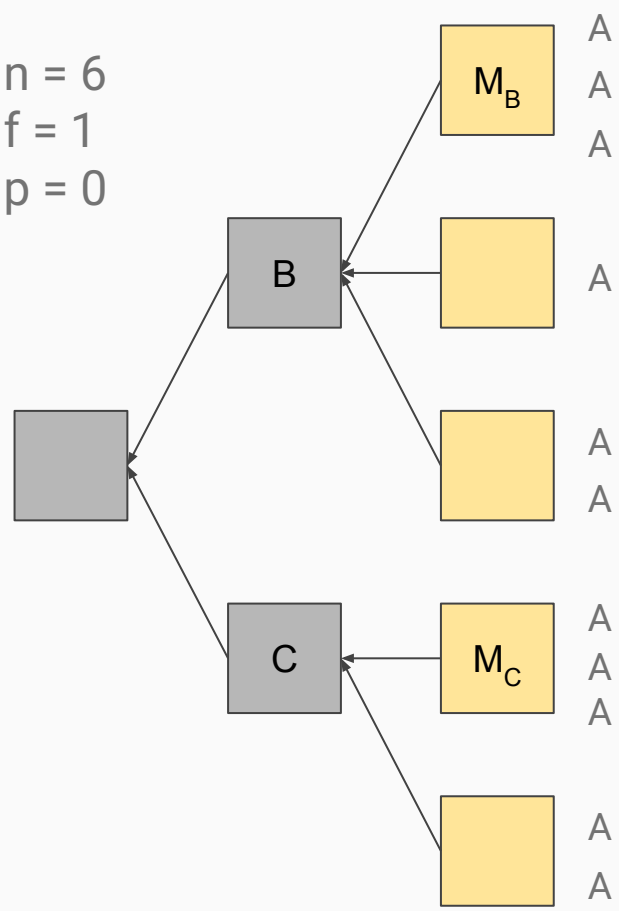


3 = f+p+1 acks on children of B besides M_B

all children of B are good


n = 6
f = p = 1
B
C
M_B
M_C
A
A
A
A
A
A
A
A
A
A
3 = f+p+1 acks on children of B besides M_B
all children of B are good
2 < f+p+1 ack on children of C besides M_C
only M_C is good


n = 6
f = p = 1
M_B
B
C
M_C
A
A
A
A
A
A
A
A
A
A
A


n = 6
f = 1
p = 0
M_B
B
C
M_C
A
A
A
A
A
A
A
A
A
A

FICC: acknowledgement

Notarization share for first child of any block

Acknowledgement

FICC: notarization

Same as ICC

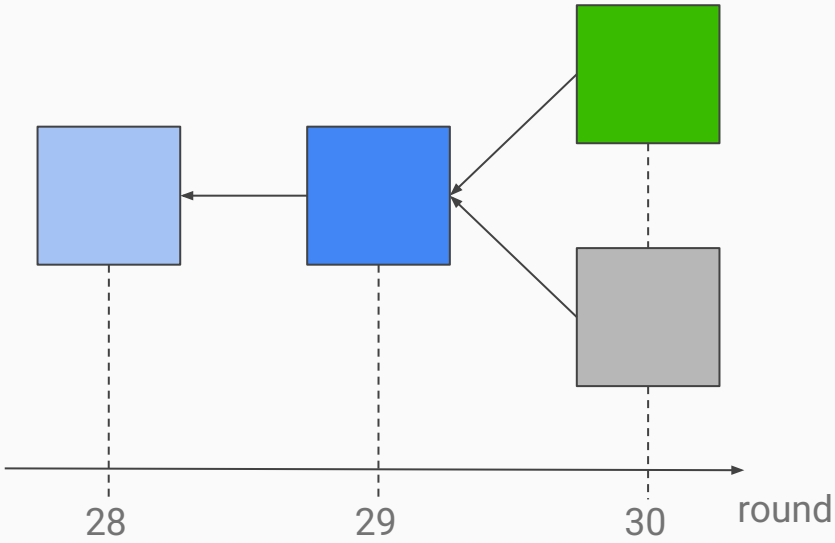
+

Acknowledgement of first child

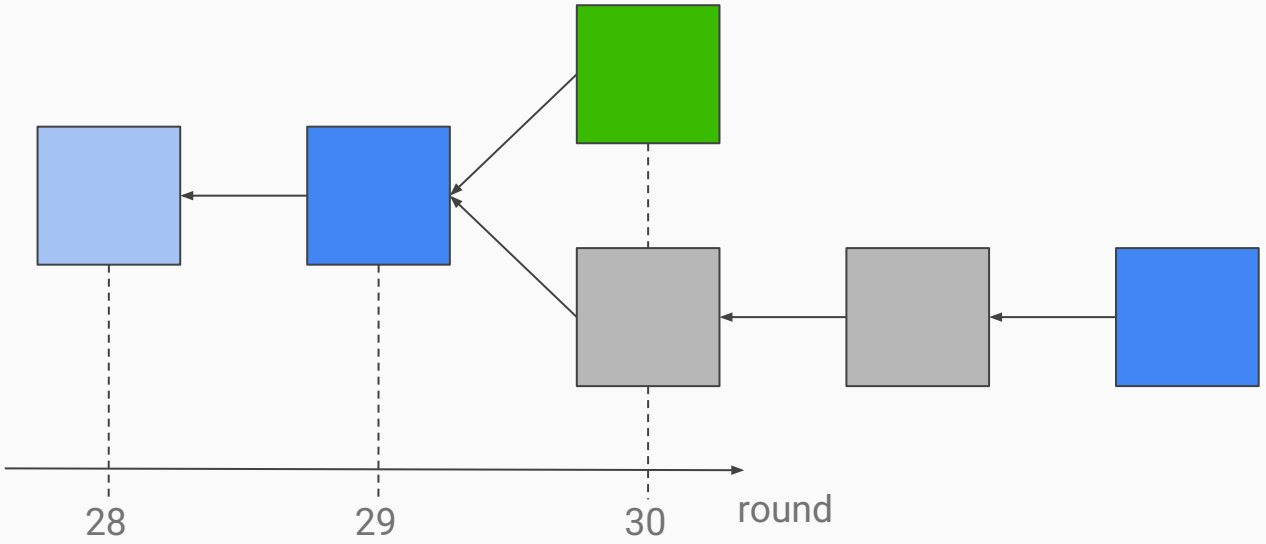
+

Aggregate shares only for good blocks

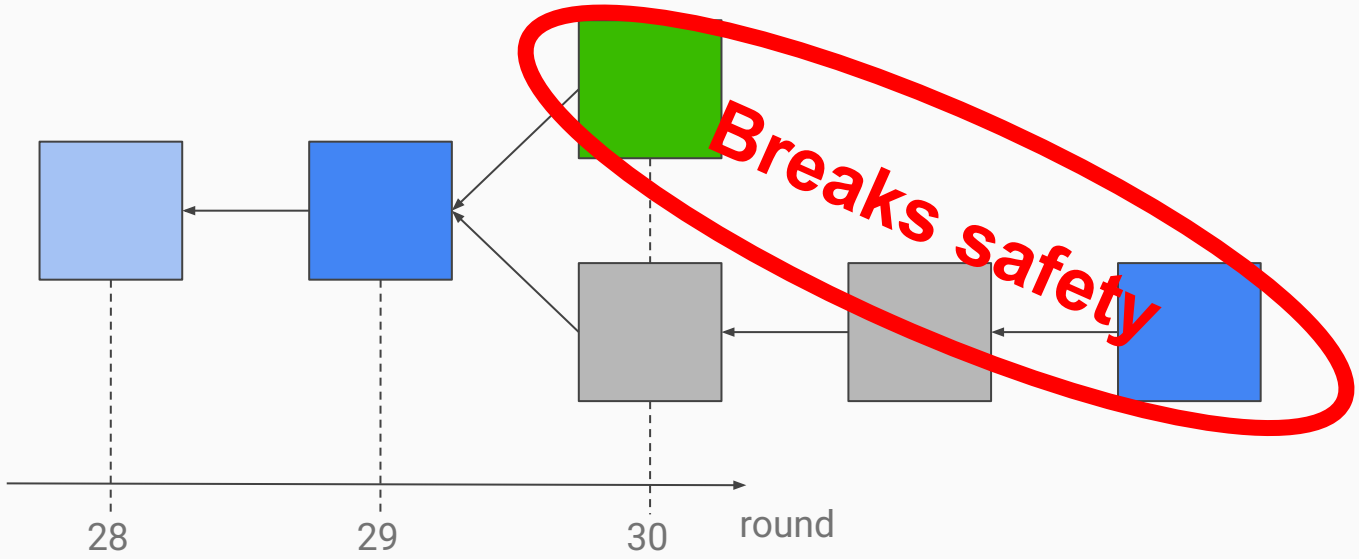
Why notarize only good blocks?



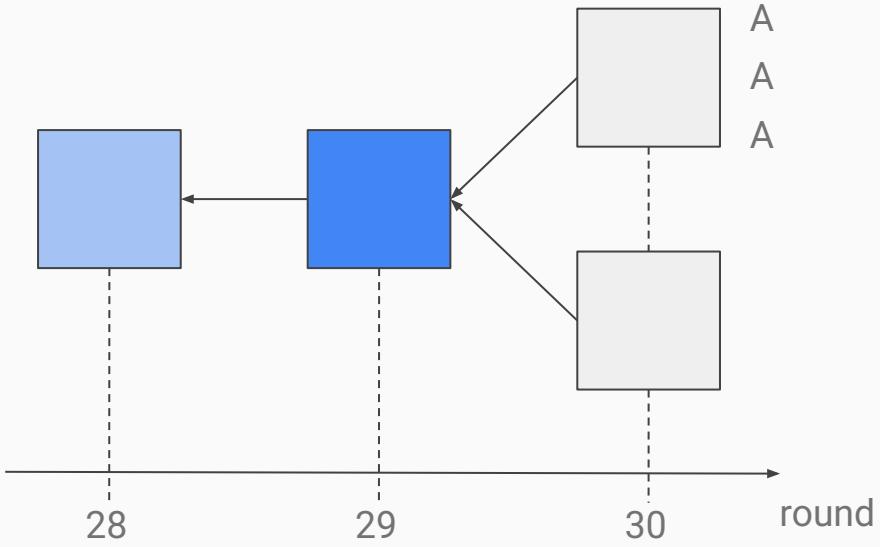
Why notarize only good blocks?



Why notarize only good blocks?



FICC: FP-finalization



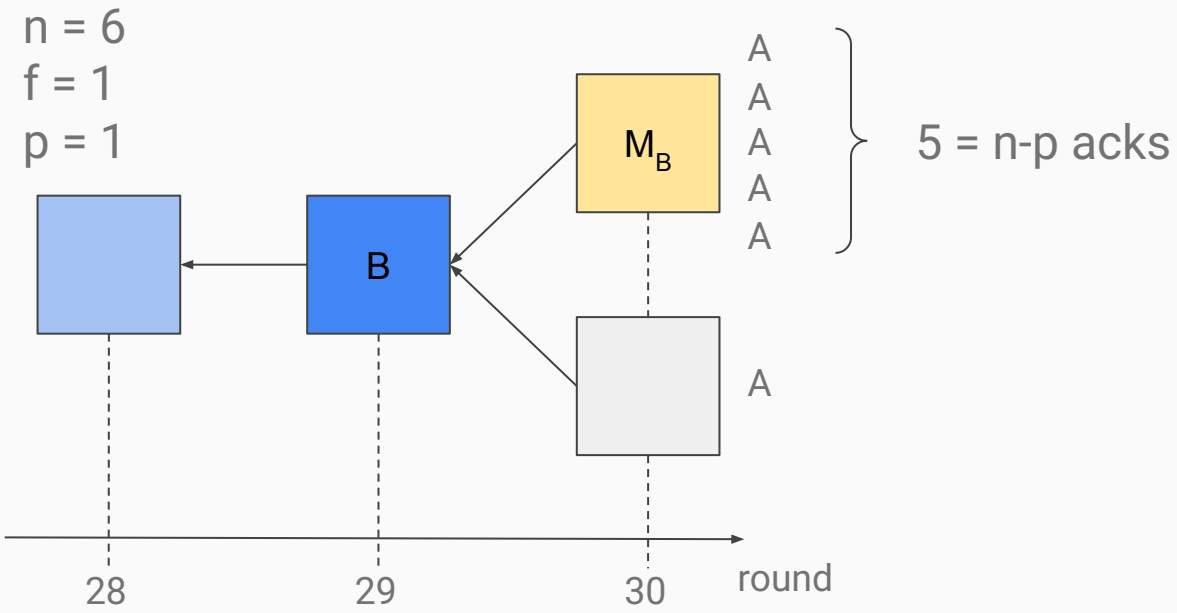
Parent is finalized

+

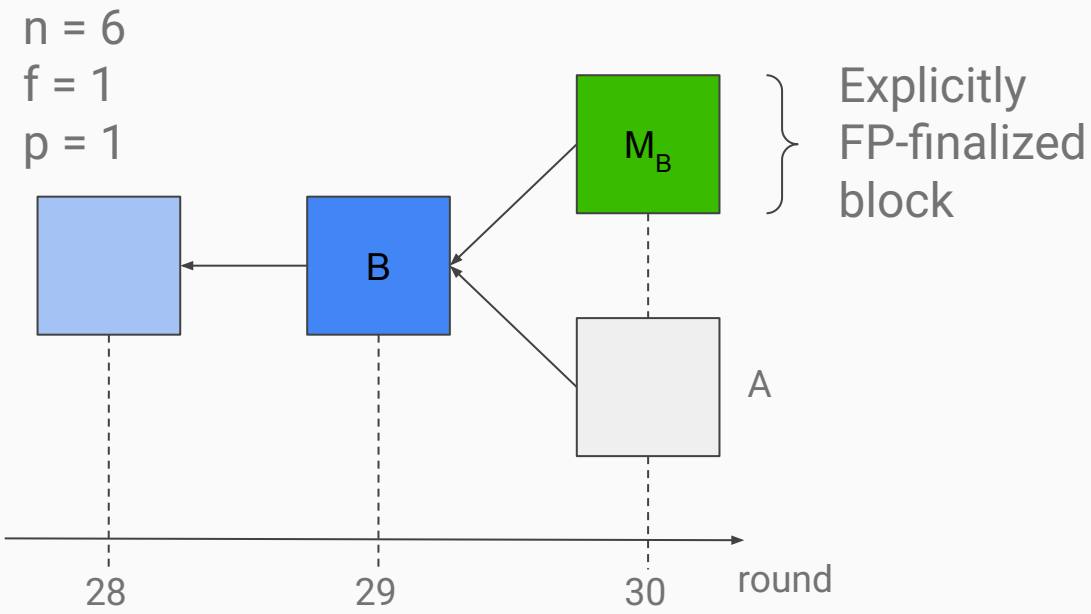
n-p acknowledgements

FP-finalized

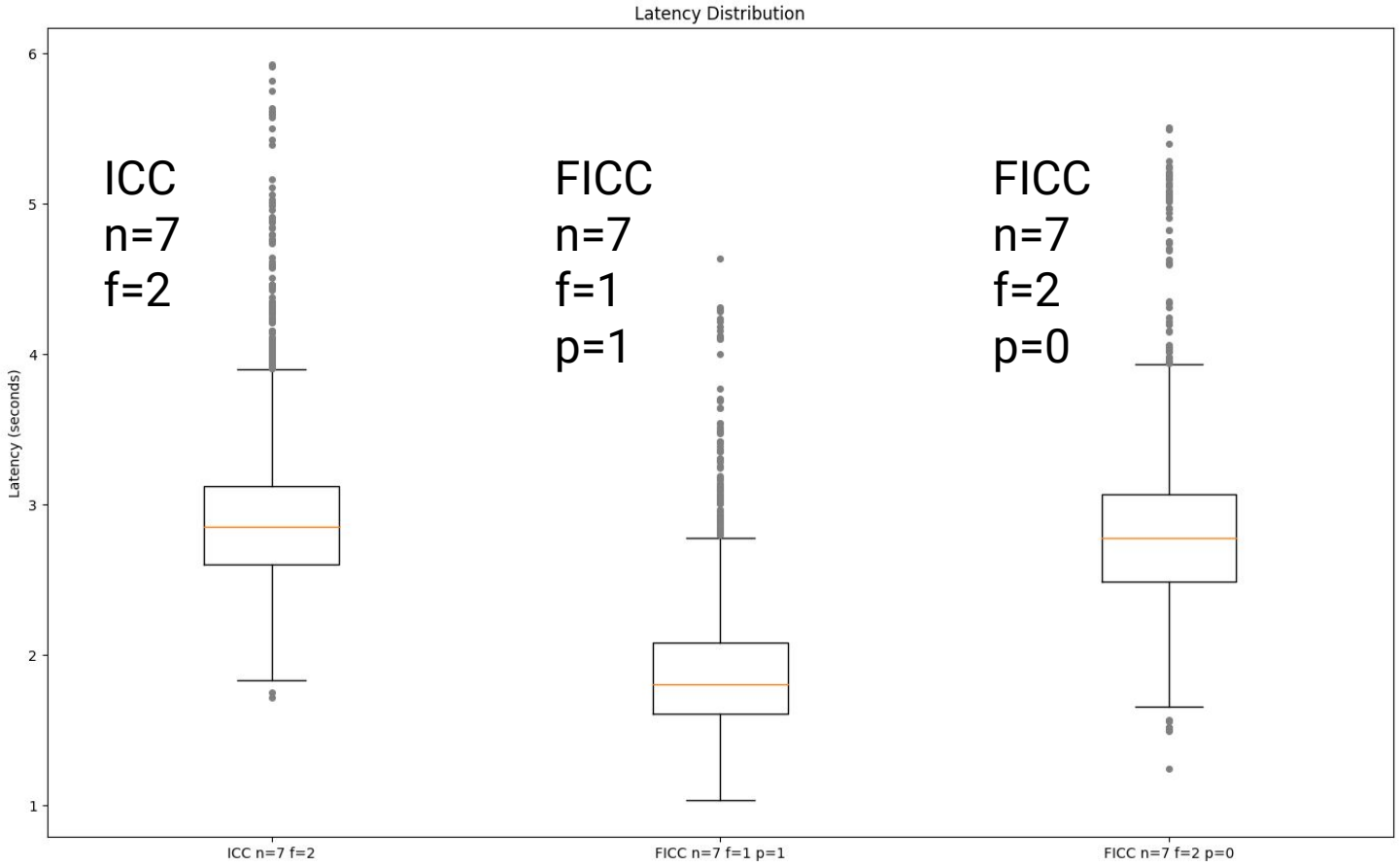
FICC: FP-finalization

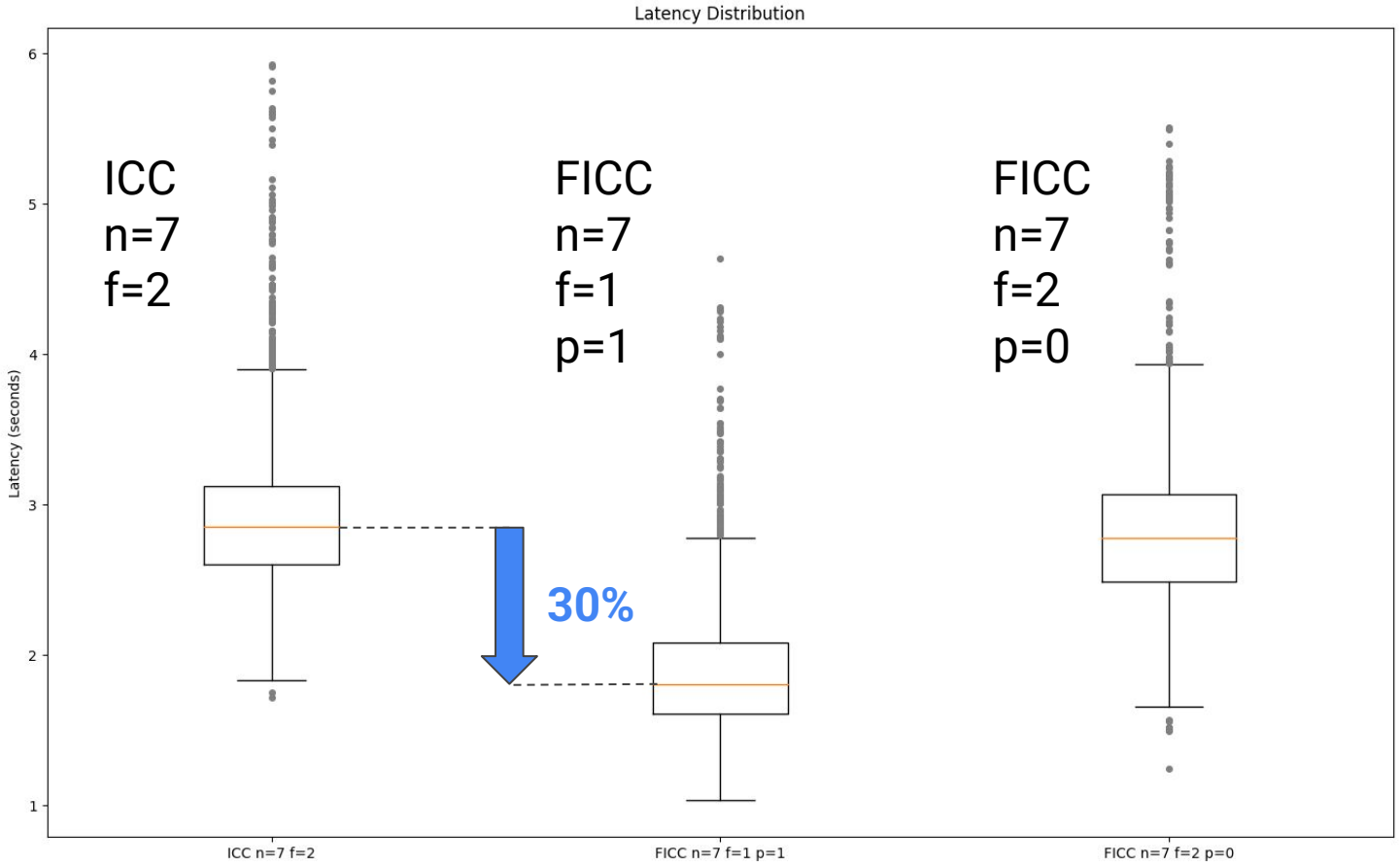


FICC: FP-finalization



More benchmark


Latency Distribution
Latency (seconds)
6
5
4
3
2
1
ICC
n=7
f=2
FICC
n=7
f=1
p=1
FICC
n=7
f=2
p=0
ICC n=7 f=2
FICC n=7 f=1 p=1
FICC n=7 f=2 p=0


Latency Distribution
Latency (seconds)
6
5
4
3
2
1
ICC
n=7
f=2
FICC
n=7
f=1
p=1
FICC
n=7
f=2
p=0
30%
ICC n=7 f=2
FICC n=7 f=1 p=1
FICC n=7 f=2 p=0

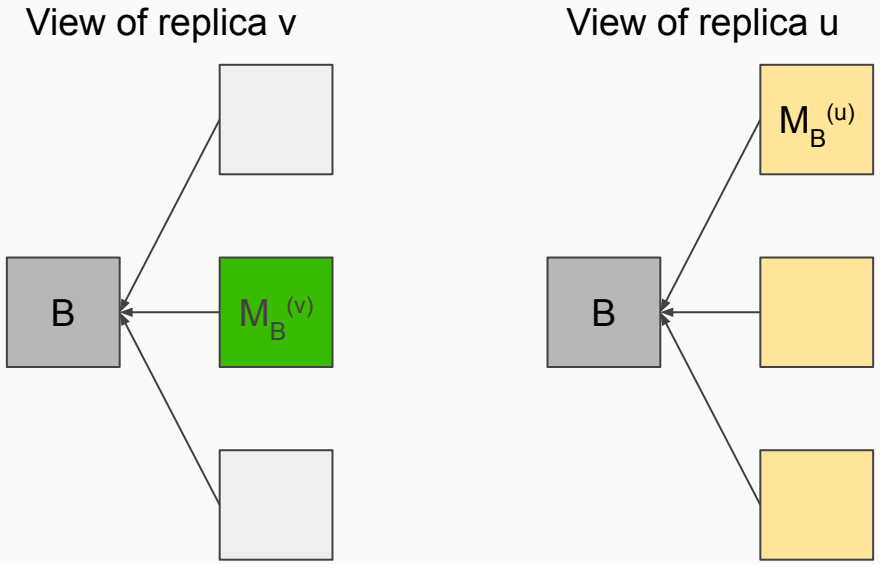
FICC safety

FICC safety

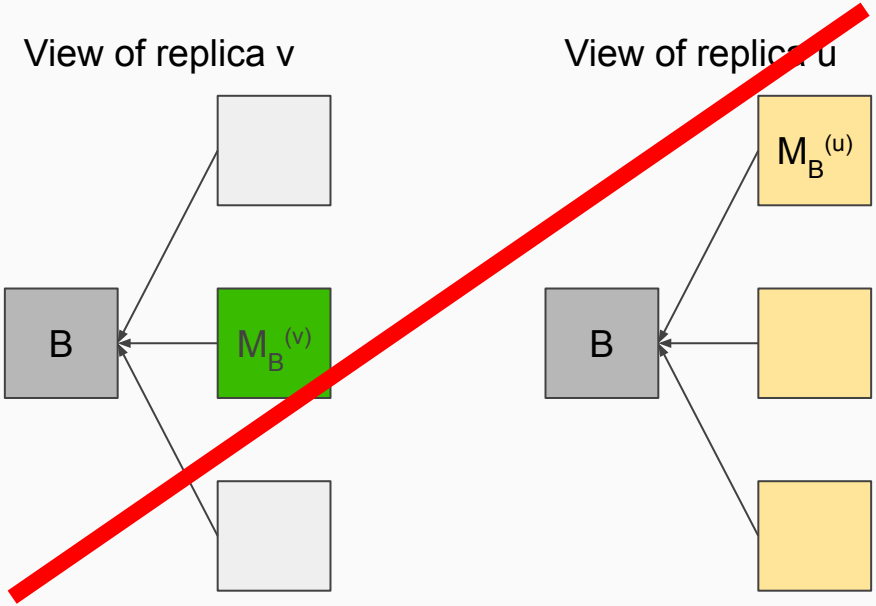
If a child of block B is **FP-finalized**:

1. no other child of B is good
2. no other good block at the same height

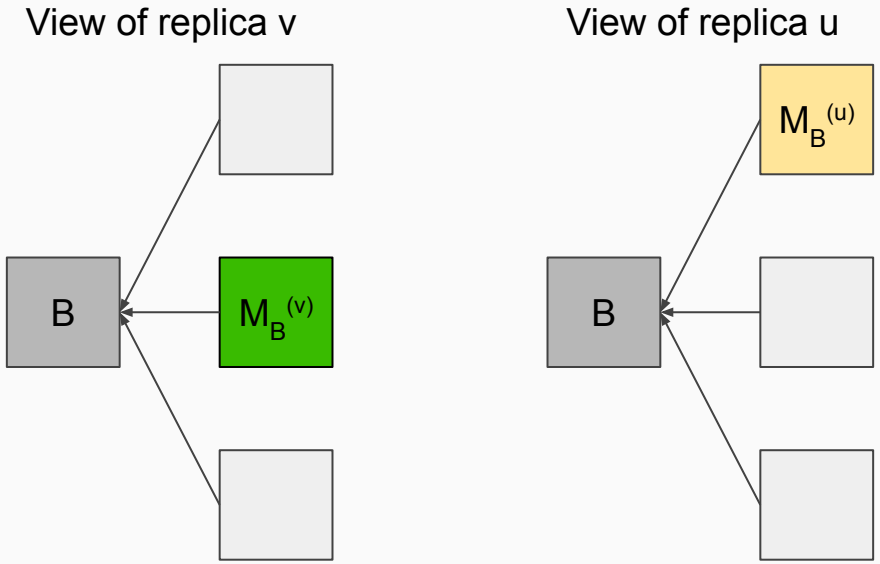
FICC safety: no other good child of B



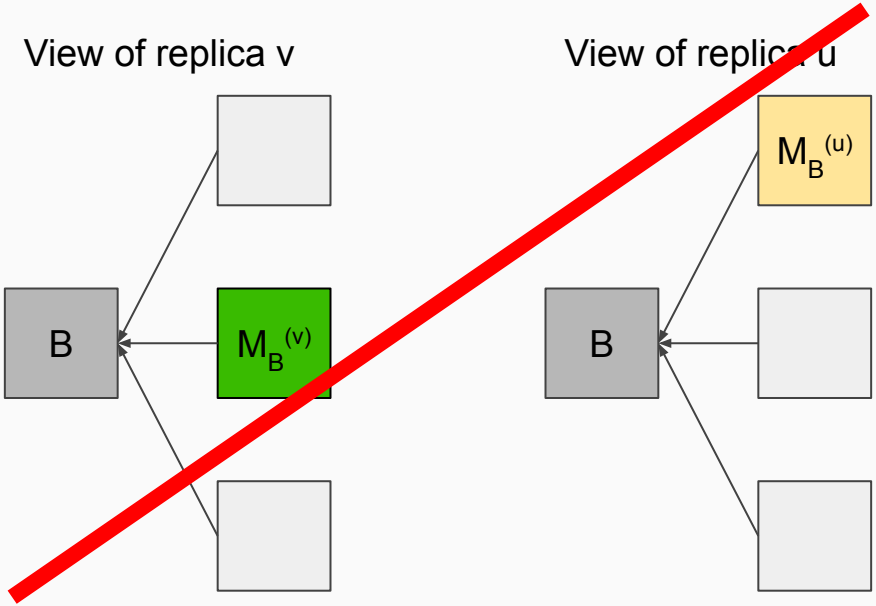
FICC safety: no other good child of B



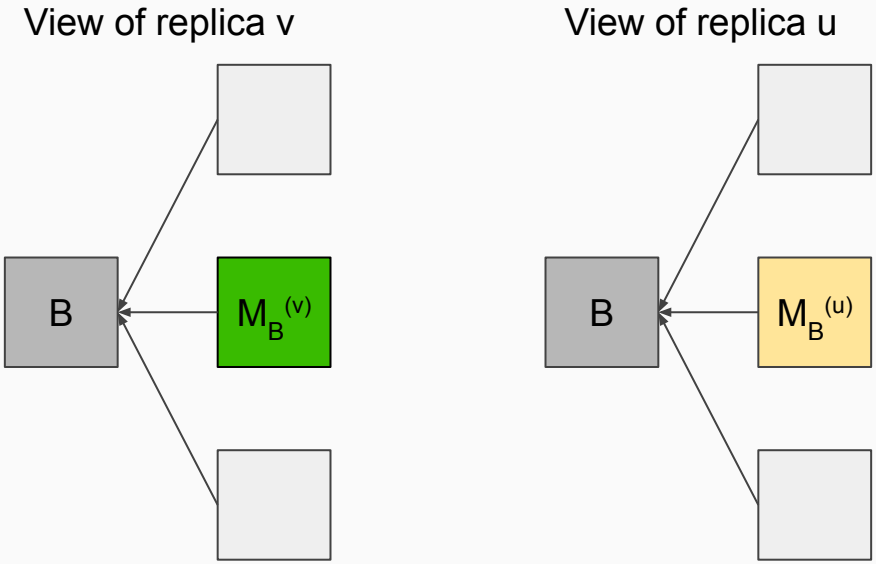
FICC safety: no other good child of B



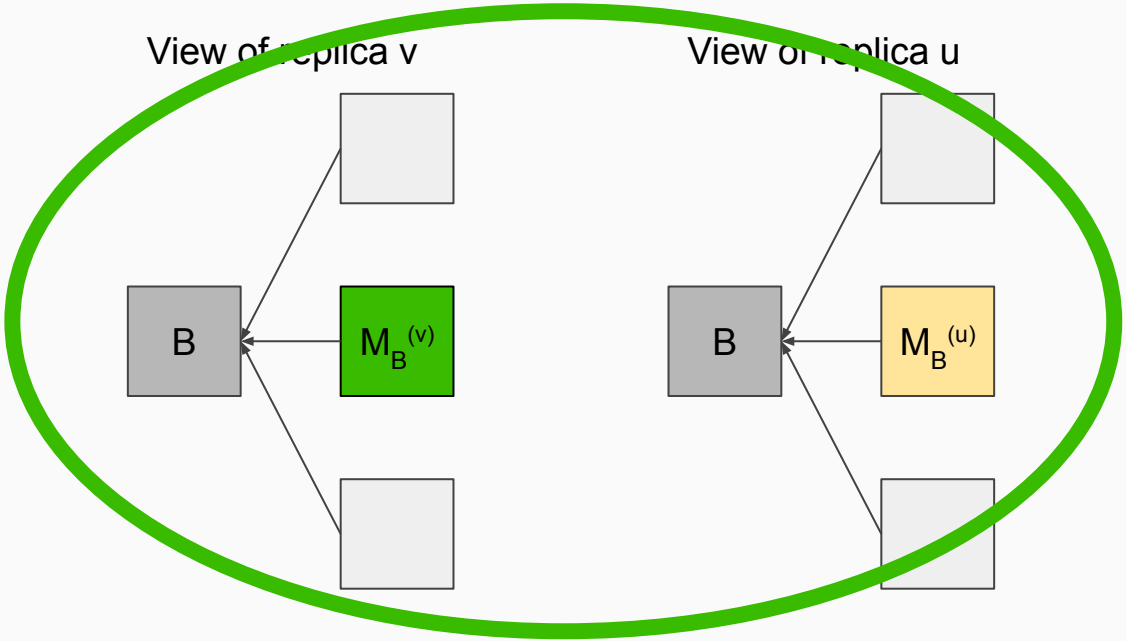
FICC safety: no other good child of B



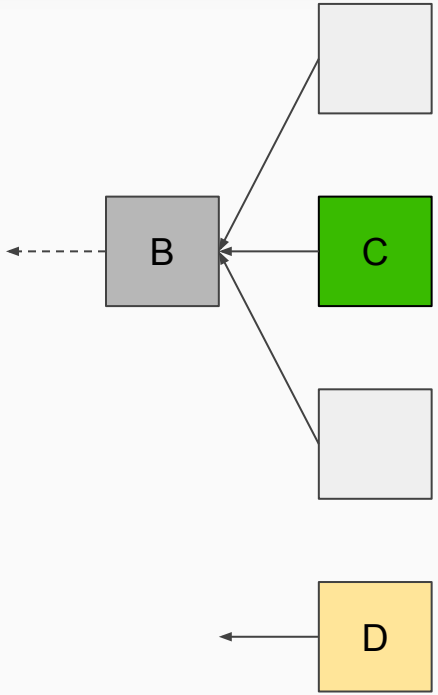
FICC safety: no other good child of B



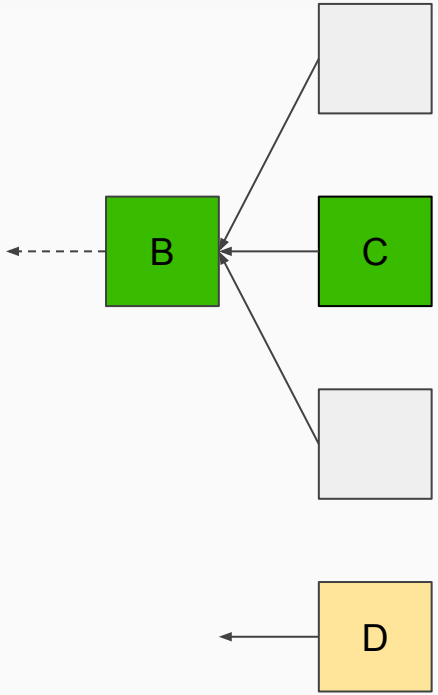
FICC safety: no other good child of B



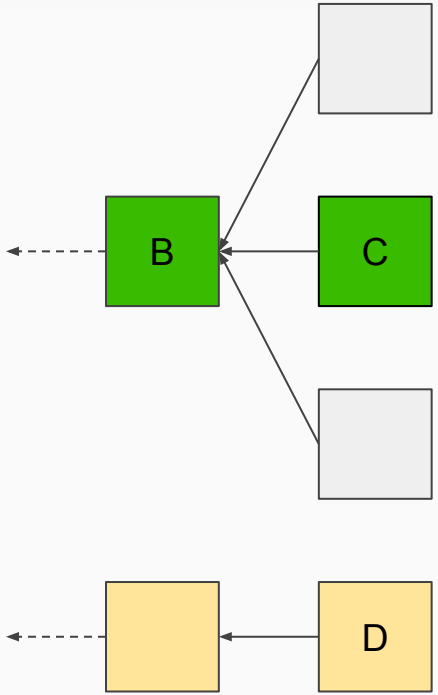
FICC safety: no other good block at same height



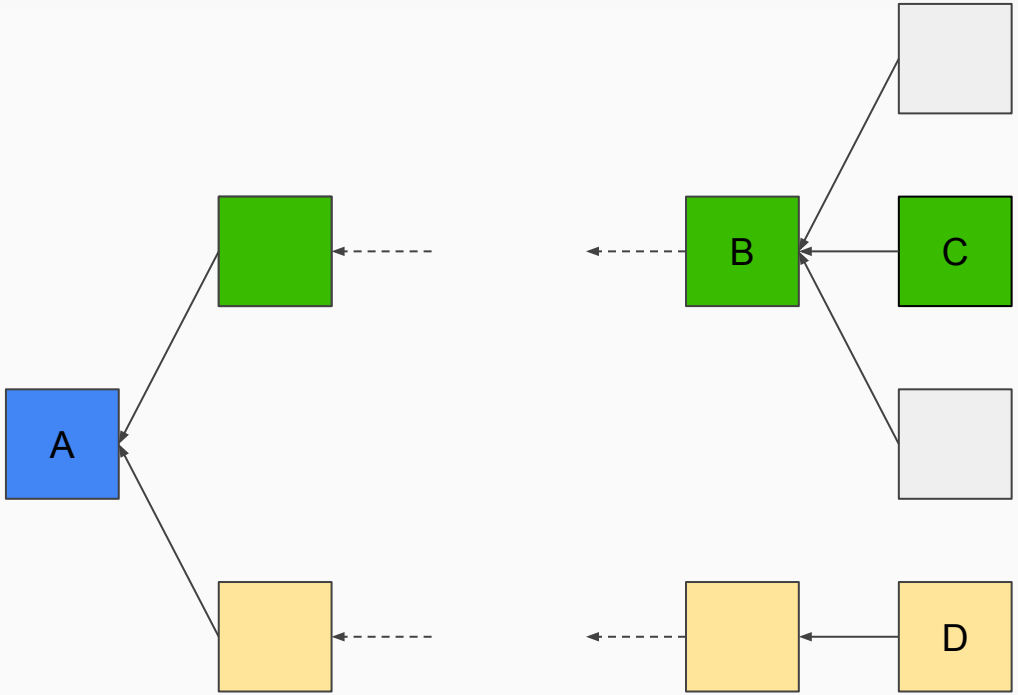
FICC safety: no other good block at same height



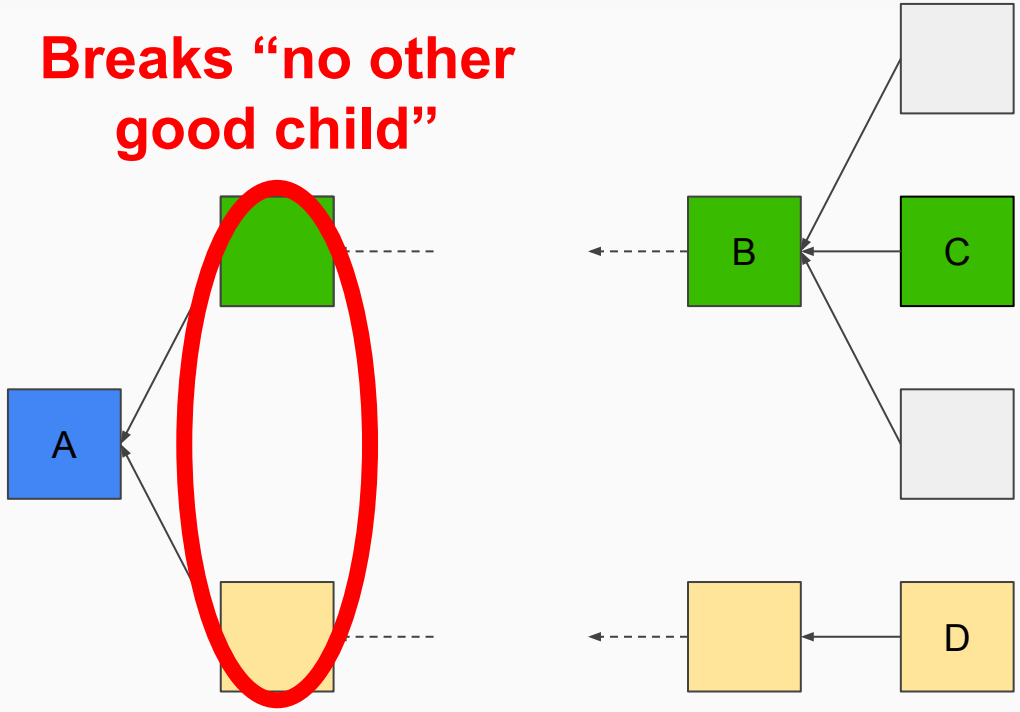
FICC safety: no other good block at same height



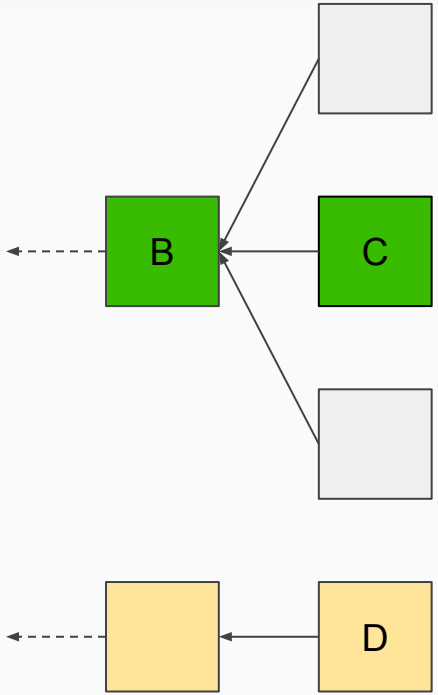
FICC safety: no other good block at same height



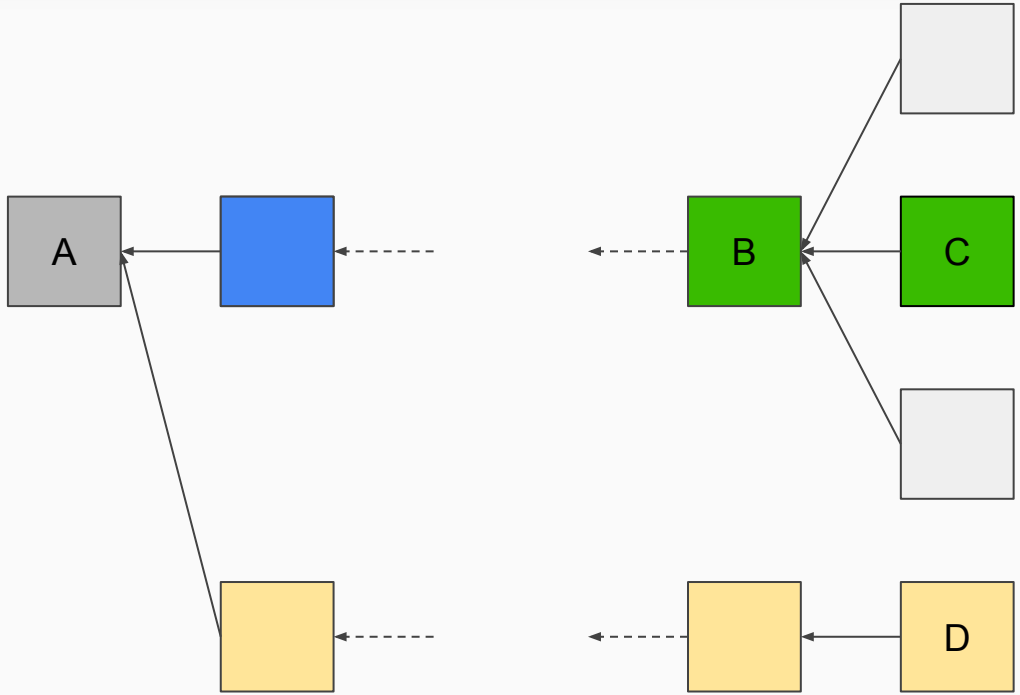
FICC safety: no other good block at same height



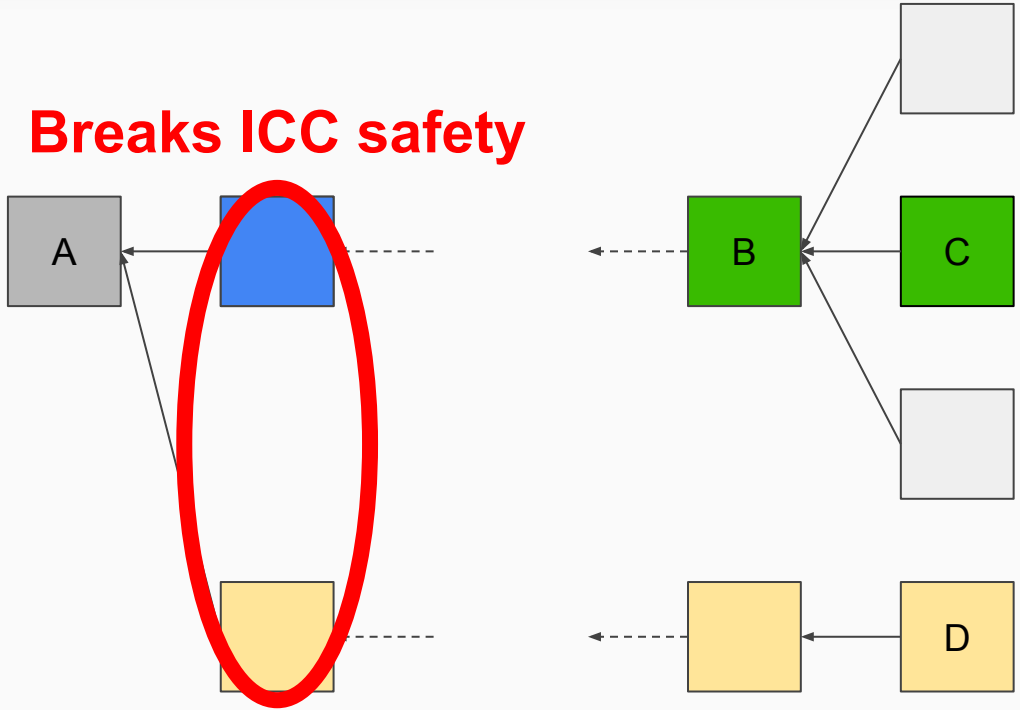
FICC safety: no other good block at same height



FICC safety: no other good block at same height



FICC safety: no other good block at same height



Comparison

ICC

Guarantee (n > 3f):

no **notarized** block at the same height of an explicitly finalized block

Unique chain of finalized blocks in the tree of **notarized** blocks

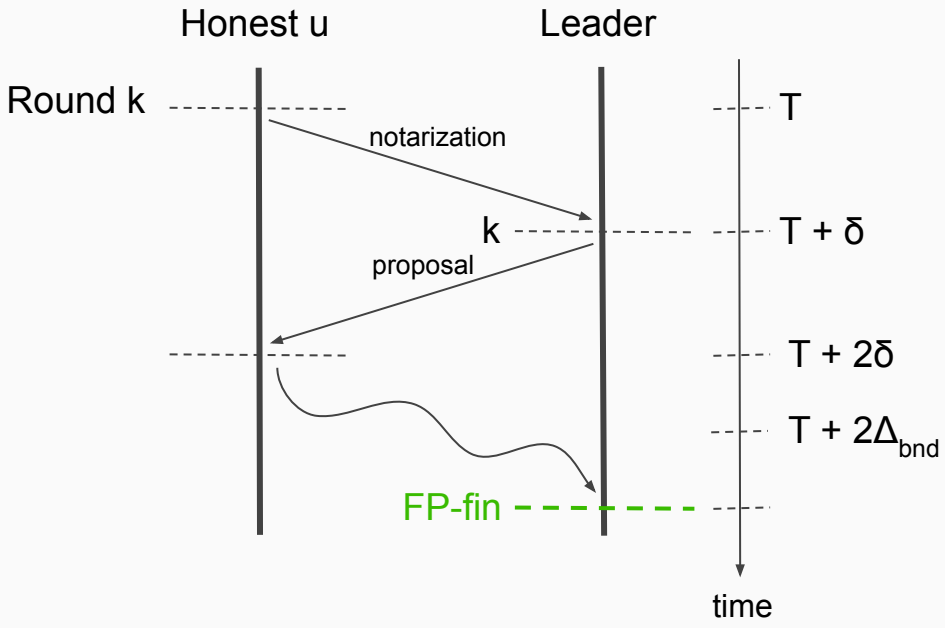
FICC

Guarantee (n > 3f+2p):

no **good** block at the same height of an explicitly finalized block

Unique chain of finalized blocks in the tree of **good** blocks

FICC Liveness

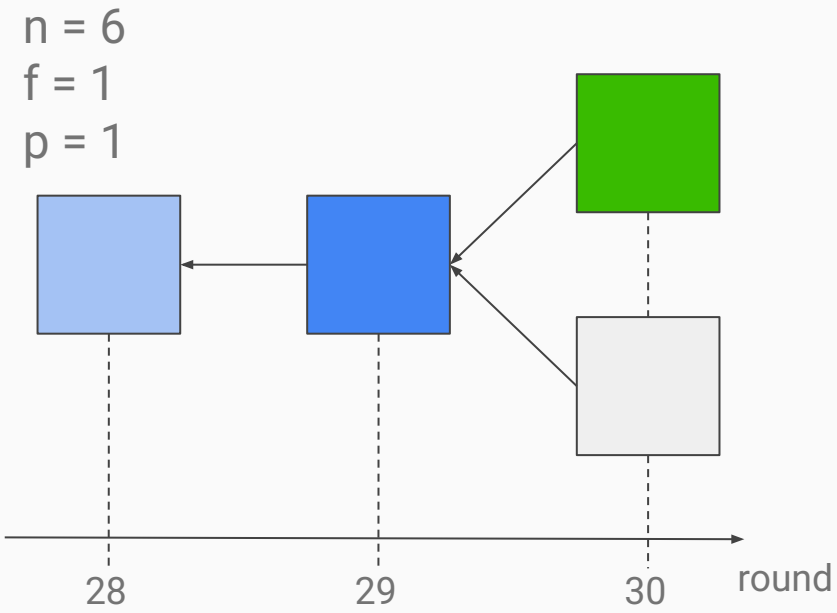


HP:

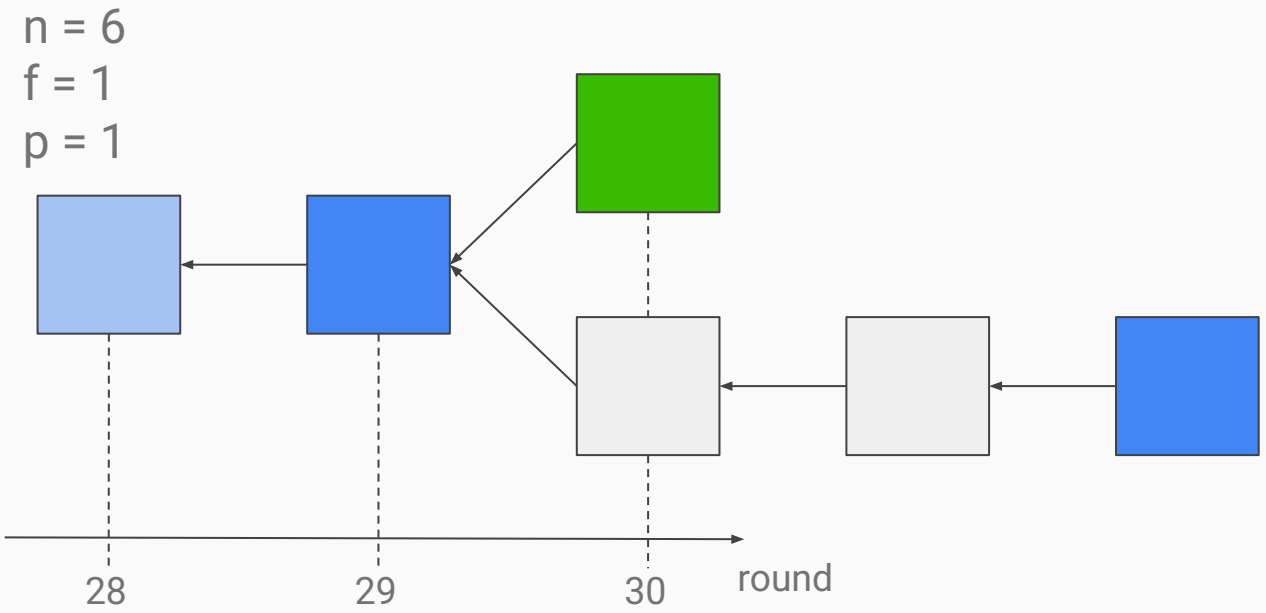
- $2\delta < \Delta_{notar}(1)$
- Synchronous in $[T, T+2\Delta_{bnd}]$

Extend only good blocks

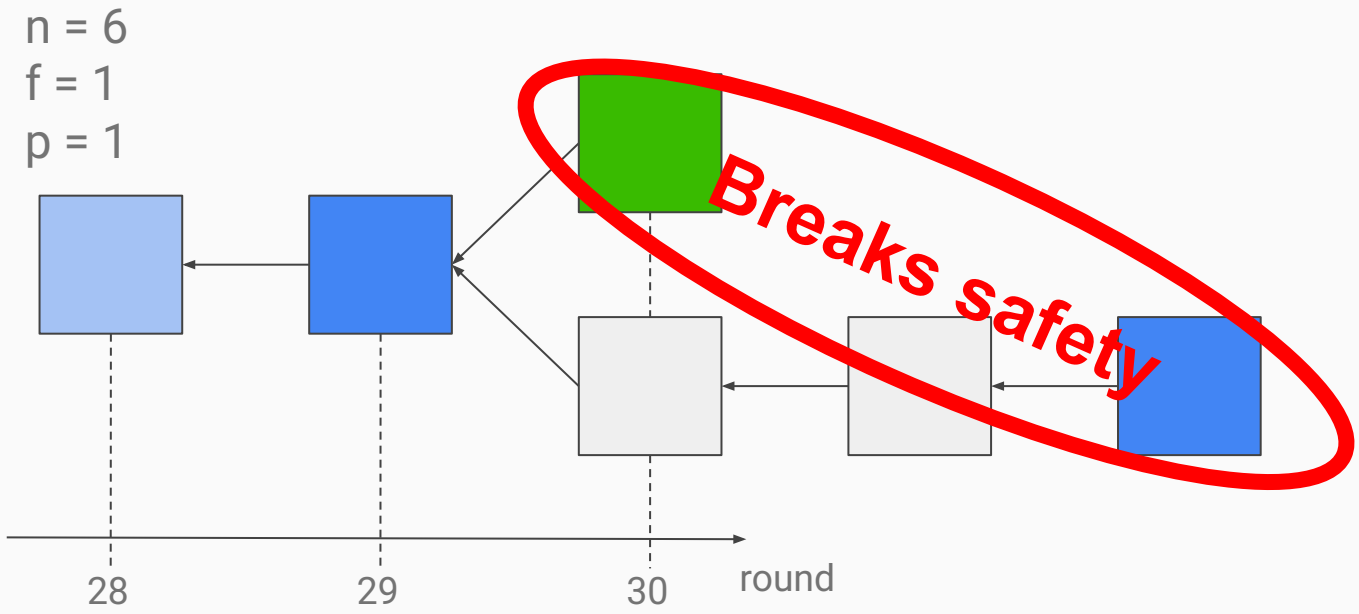
Why extend only good blocks?



Why extend only good blocks?

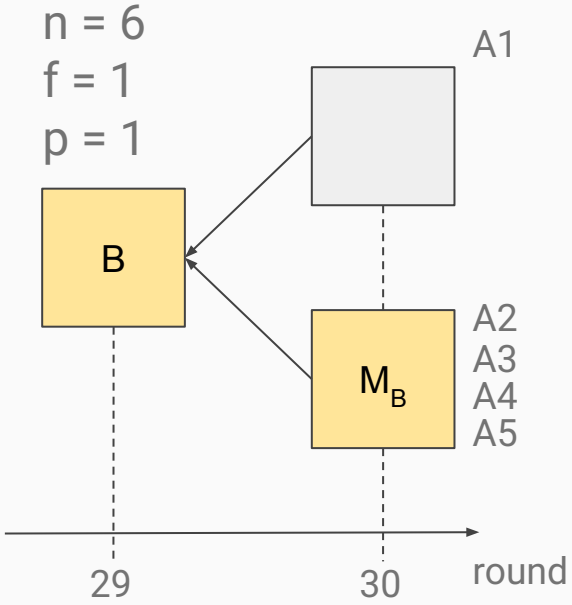


Why extend only good blocks?

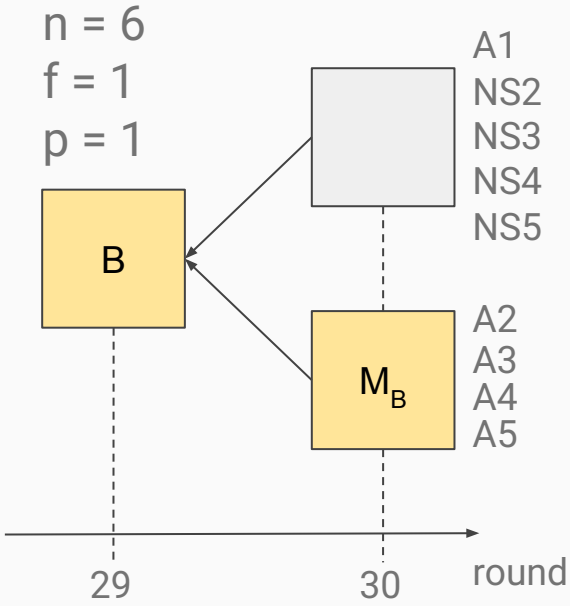


Notarize only good blocks

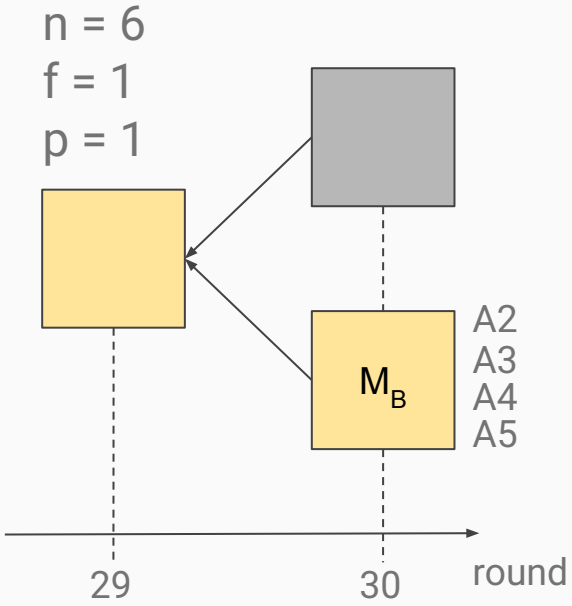
Why notarize only good blocks?



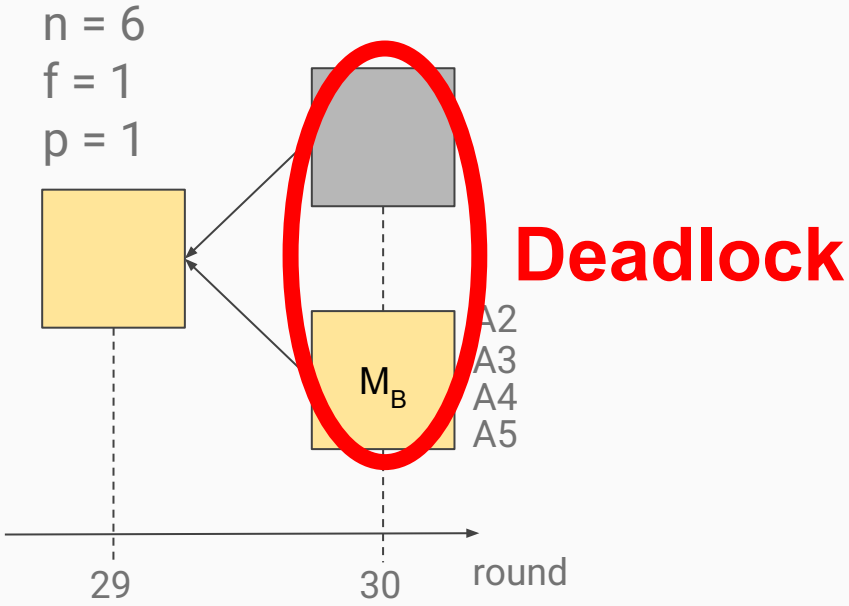
Why notarize only good blocks?



Why notarize only good blocks?



Why notarize only good blocks?



Why finalize only good blocks?