Asynchronous and Decentral Group Management in Messengers with Delegates Proof of Stake

Andreas Hellenbrand - 2020/03/17

Index

- Look back
- Updated Protocol
  - Elections
  - Forks
- Delivery Issues
- Conclusion

Look back

- Group Chats
- Delegated Proof of Stake

Group Chats

$$gr = (Id_{gr}, \mathcal{M}_{gr}, \mathcal{M}^*_{gr}, info_{gr})$$

Closeness

Privacy

Same State

Delegated Proof of Stake (DPoS)

- Stakeholders elect Delegates
- Delegates confirm Transactions with Blocks

Group Chats + DPoS

- Members elect Delegates
- Delegates confirm Suggestions with Blocks
    - (Add, Remove, Info)
- Blocks updates the Group

Open Issues

- Elections with *Voting Windows*
  - Synchronous
  - Complexity
- Forks
  - Can violate **Same State**
  - Information loss

Updated Protocol

- Asynchronous Elections
- Fork avoidance with *Server-Side-Timestamps*

Elections

$$V = (u_{id}, \mathcal{V}_{u_{id}}, Signature, BlockRef)$$

- $\mathcal{V}_{u_{id}} = \{v_1, \ldots, v_n\}$
- Send Votes any time
- Votes are included in the blocks
- $\mathcal{M}^*$ is recomputed on each block

$$\mathcal{V} = \{\mathcal{V}_1, ..., \mathcal{V}_m\}$$

$$x_{u_{id}} = \sum_{i=0}^{|\mathcal{V}|} \begin{cases} \frac{1}{|\mathcal{V}_i|} & \text{, if } u_{id} \in \mathcal{V}_i \\ 0 & \text{, else} \end{cases} \qquad \text{for all } u_{id} \in \mathcal{M}$$

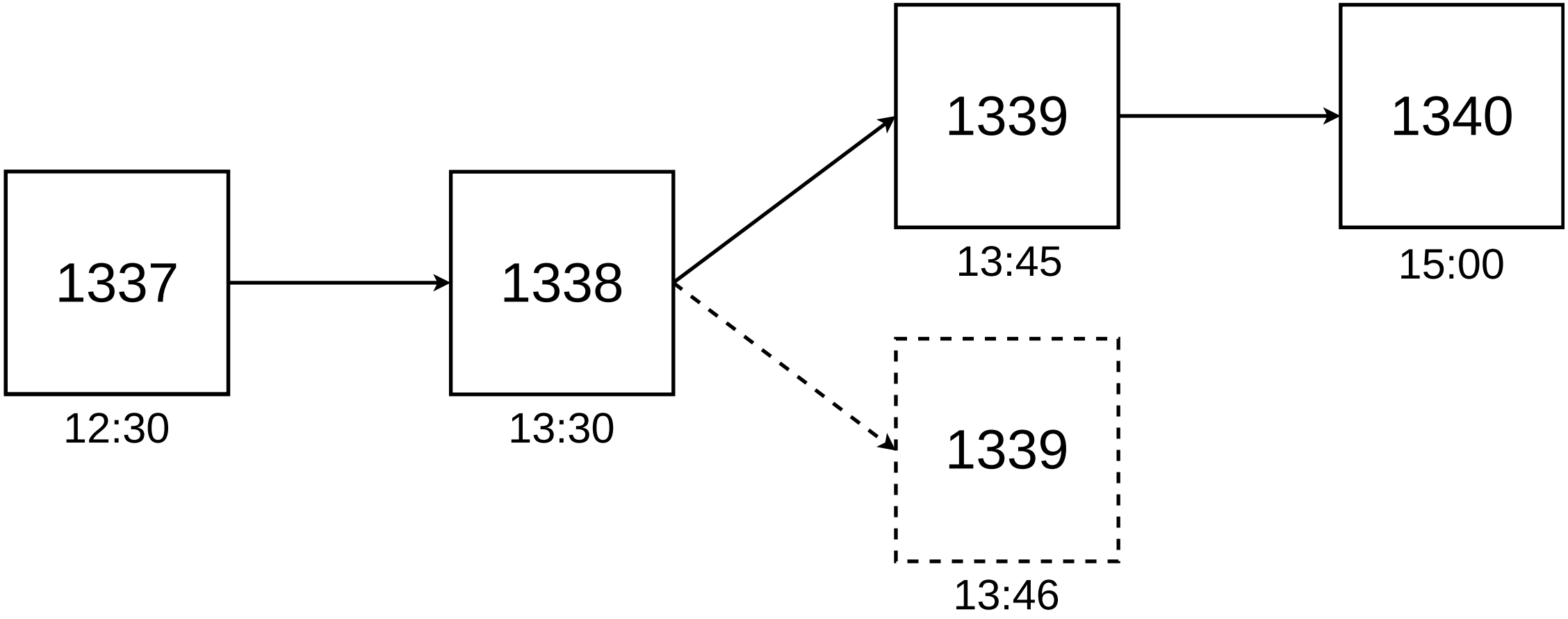
$$\mathcal{M}^* := \sqrt{|\mathcal{M}|}\, best\, x_{u_{id}}$$

Block

$$B_S = (b_{id}, pbh, S, sig, u_{id}, MVP, VMR, nVMR, votes)$$

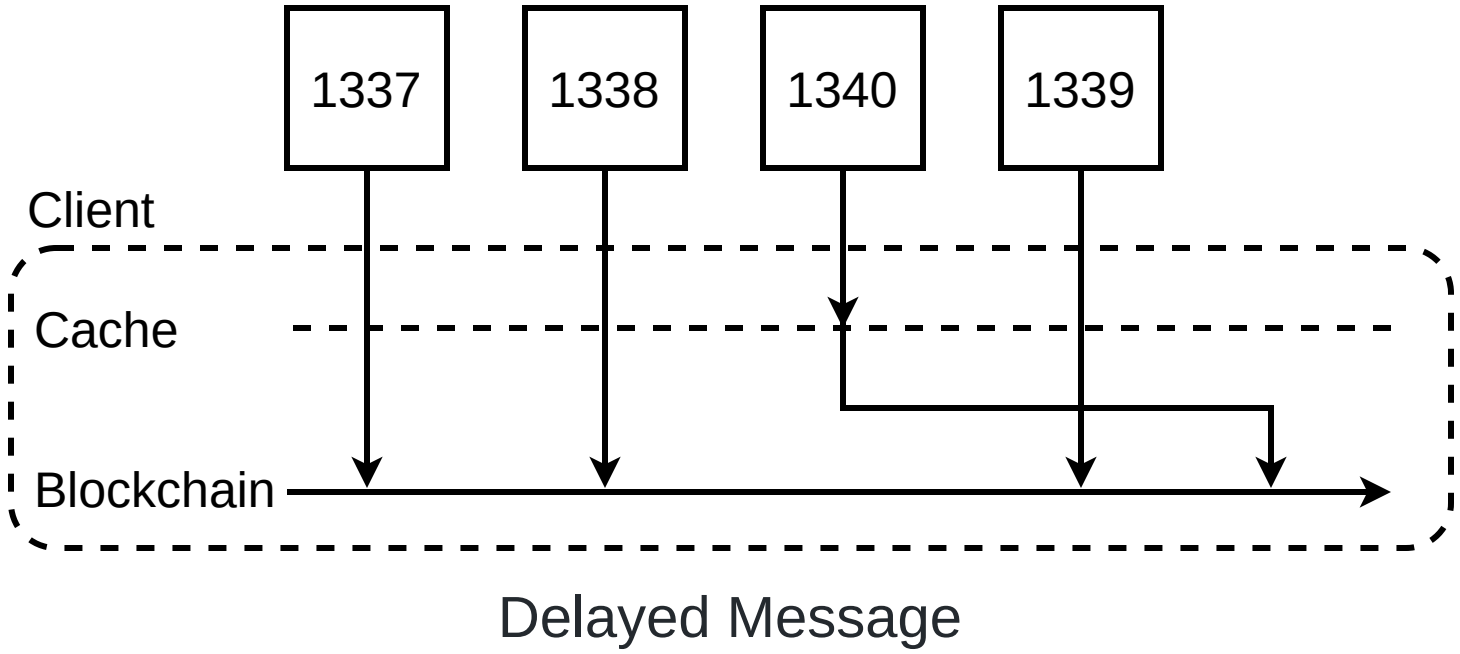
Fork avoidance

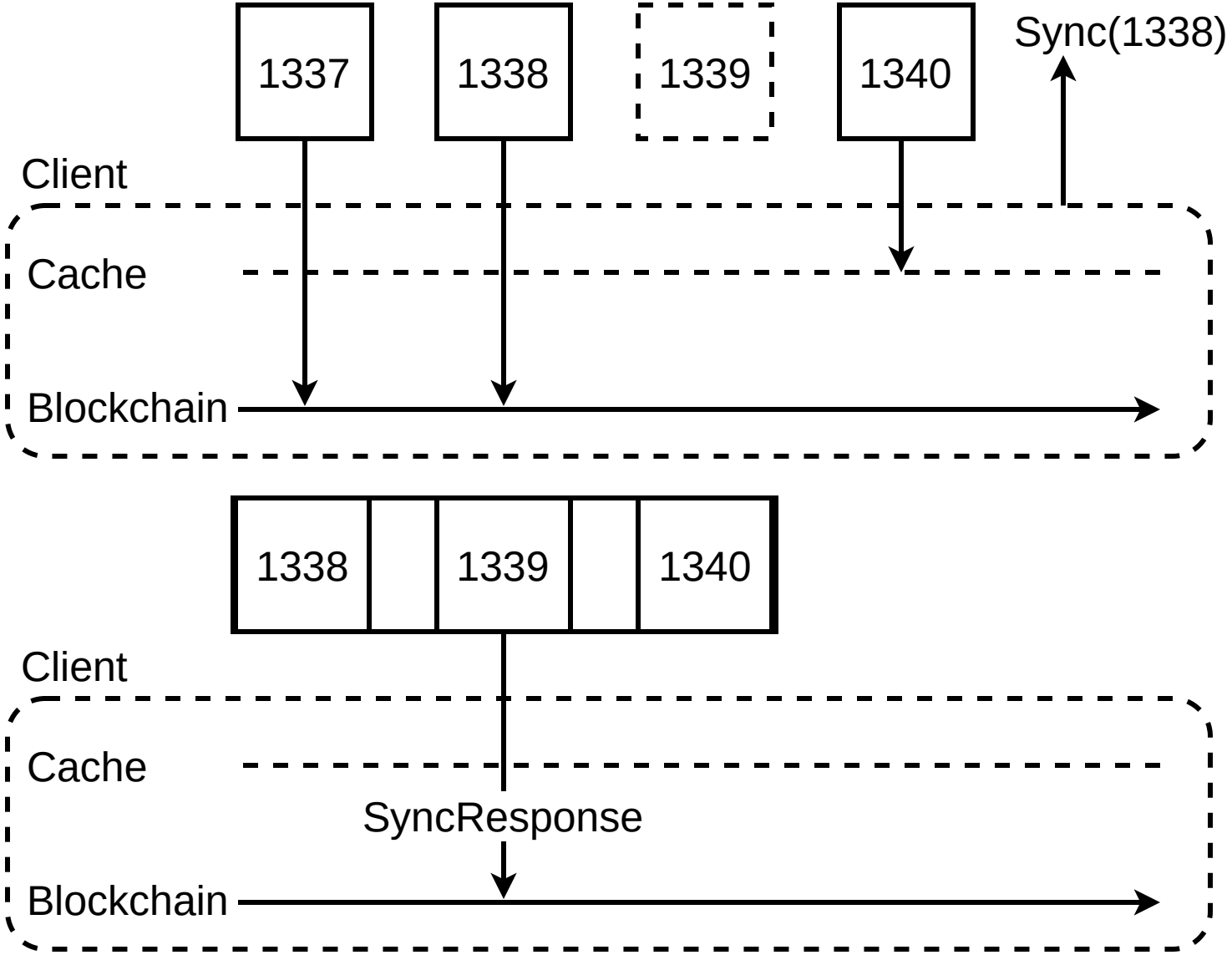
- Messages are tagged with *Server-Side-Timestamps*
- *SST* are used to detect the *first* block


1337
12:30
1338
13:30
1339
13:45
1340
15:00
1339
13:46

Delivery Issues

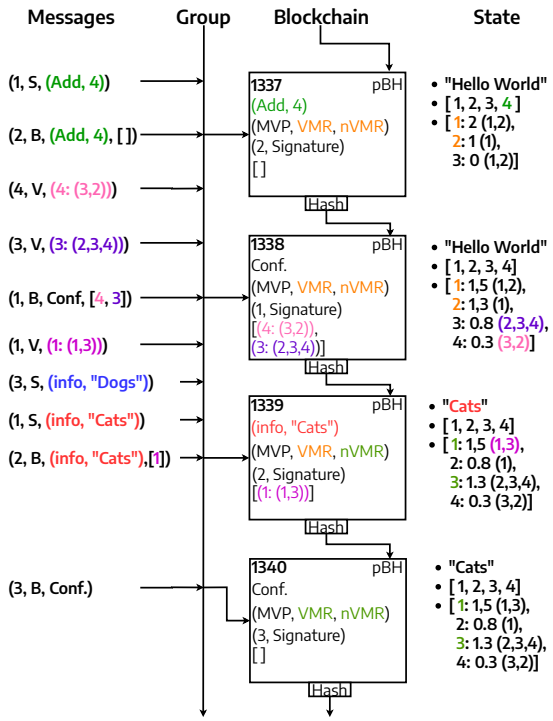
- Delayed Messages
- Lost Messages


1337
1338
1340
1339
Client
Cache
Blockchain
Delayed Message



Lost Message

Example


Messages
Group
Blockchain
State
(1, S, (Add, 4))
(2, B, (Add, 4), [ ])
(4, V, (4: (3,2)))
(3, V, (3: (2,3,4)))
(1, B, Conf, [4, 3])
(1, V, (1: (1,3)))
(3, S, (info, "Dogs"))
(1, S, (info, "Cats"))
(2, B, (info, "Cats"),[1])
(3, B, Conf.)
1337 pBH
(Add, 4)
(MVP, VMR, nVMR)
(2, Signature)
[ ]
Hash
• "Hello World"
• [1, 2, 3, 4]
• [1: 2 (1,2),
2: 1 (1),
3: 0 (1,2)]
1338 pBH
Conf.
(MVP, VMR, nVMR)
(1, Signature)
[(4: (3,2)),
(3: (2,3,4))]
Hash
• "Hello World"
• [1, 2, 3, 4]
• [1: 1,5 (1,2),
2: 1,3 (1),
3: 0.8 (2,3,4),
4: 0.3 (3,2)]
1339 pBH
(info, "Cats")
(MVP, VMR, nVMR)
(2, Signature)
[(1: (1,3))]
Hash
• "Cats"
• [1, 2, 3, 4]
• [1: 1,5 (1,3),
2: 0.8 (1),
3: 1.3 (2,3,4),
4: 0.3 (3,2)]
1340 pBH
Conf.
(MVP, VMR, nVMR)
(3, Signature)
[ ]
Hash
• "Cats"
• [1, 2, 3, 4]
• [1: 1,5 (1,3),
2: 0.8 (1),
3: 1.3 (2,3,4),
4: 0.3 (3,2)]

Conclusion

</Slides>