REPLY
SPIKE

Dario Lanfranco

Decentralized PKI based on blockchain

Introduction

- Traditional PKI
  - Hierarchy of CAs
  - Downsides:
    - Single point of failure
    - Laborious revocation mechanisms
- Distributed systems

Searching for decentralizing alternatives

- Decentralized Blockchain-based PKI
  - Theoretical
  - Web of Trust

PoC realization

Proof of Concept

- DBPKI UI
- Cryptographic accumulator
- DBPKI Nodes
- Blockchain → Consensus mechanism
- Dynamic trust weights
- PKCS#11
- HSM

Integration as a
Root of Trust

DBPKI User Interface

- Single machine
- Rounds

Setup

Round 1

Round 2

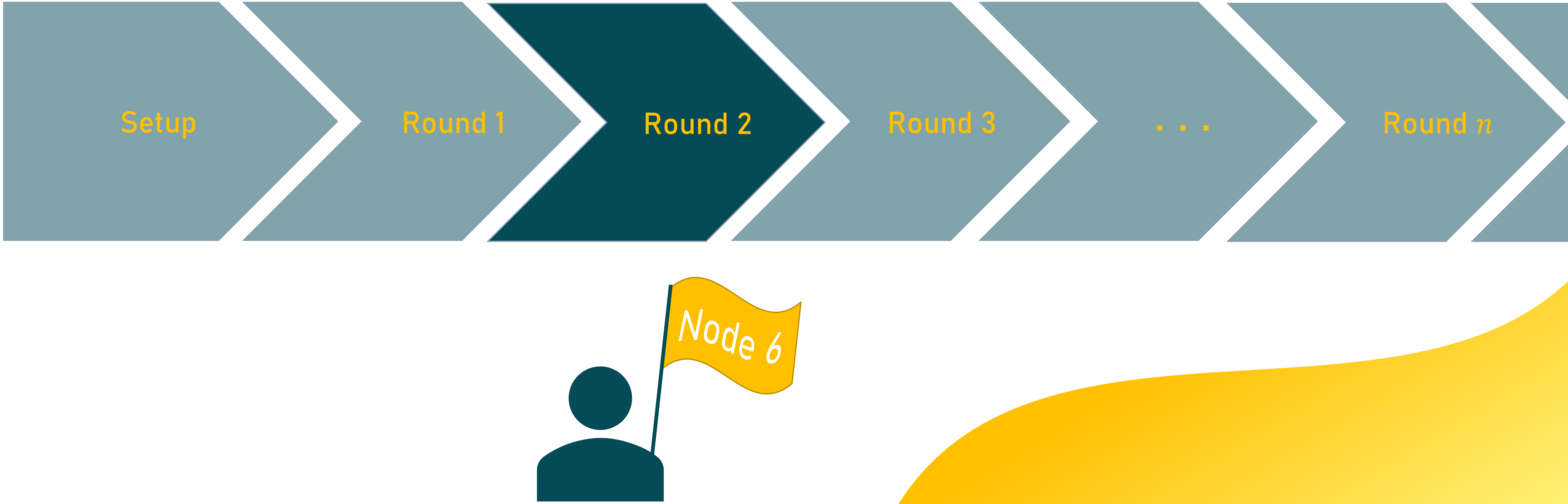
Round 3

. . .

Round n

DBPKI User Interface

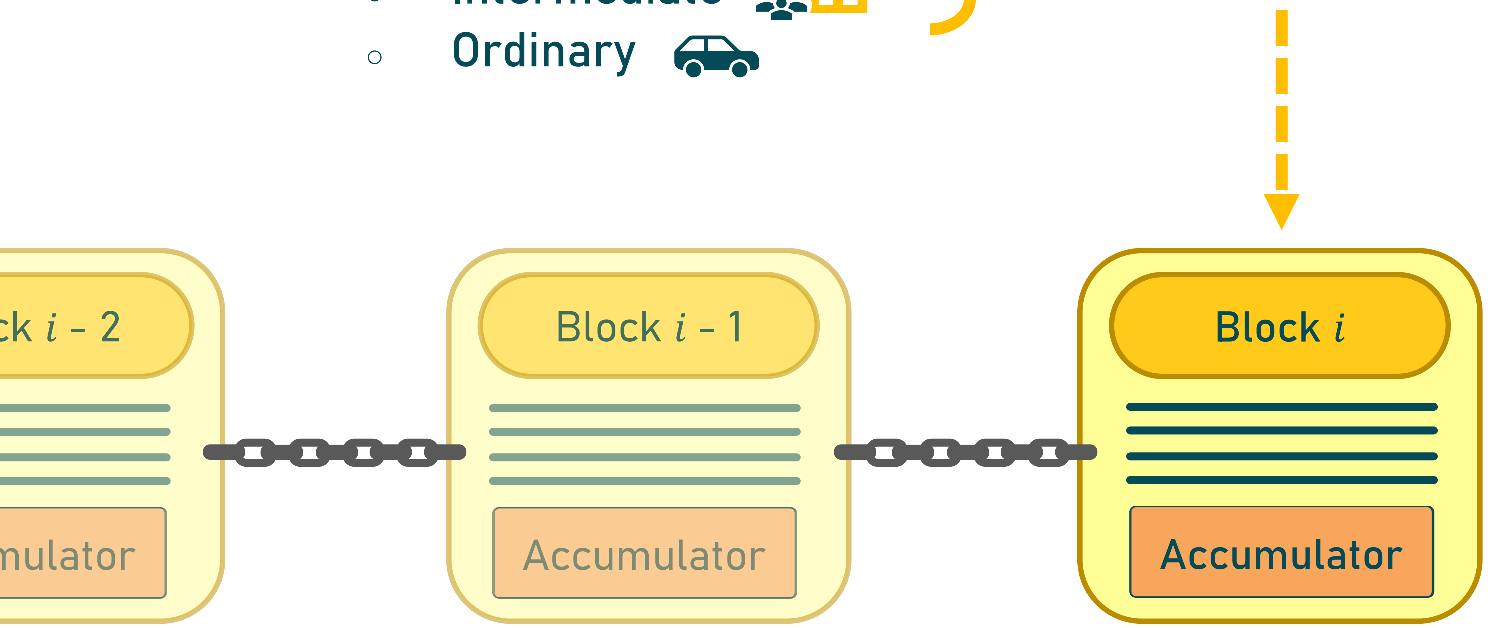
- Single machine
- Rounds


Setup
Round 1
Round 2
Round 3
. . .
Round n

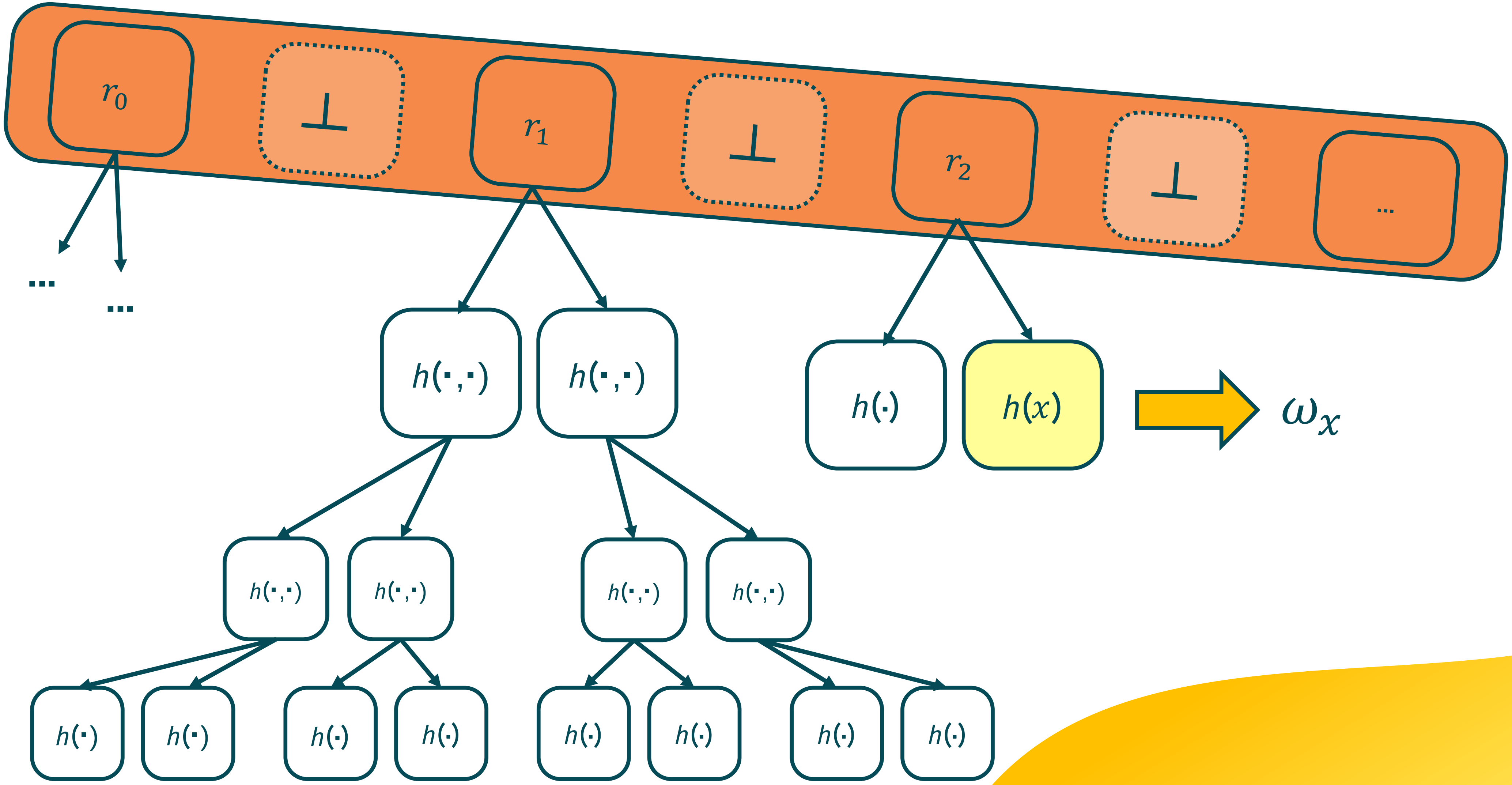
DBPKI nodes

- Asymmetric key pair
- Trust weight
- Role
  - Root
  - Intermediate
  - Ordinary

DBPKI consensus group

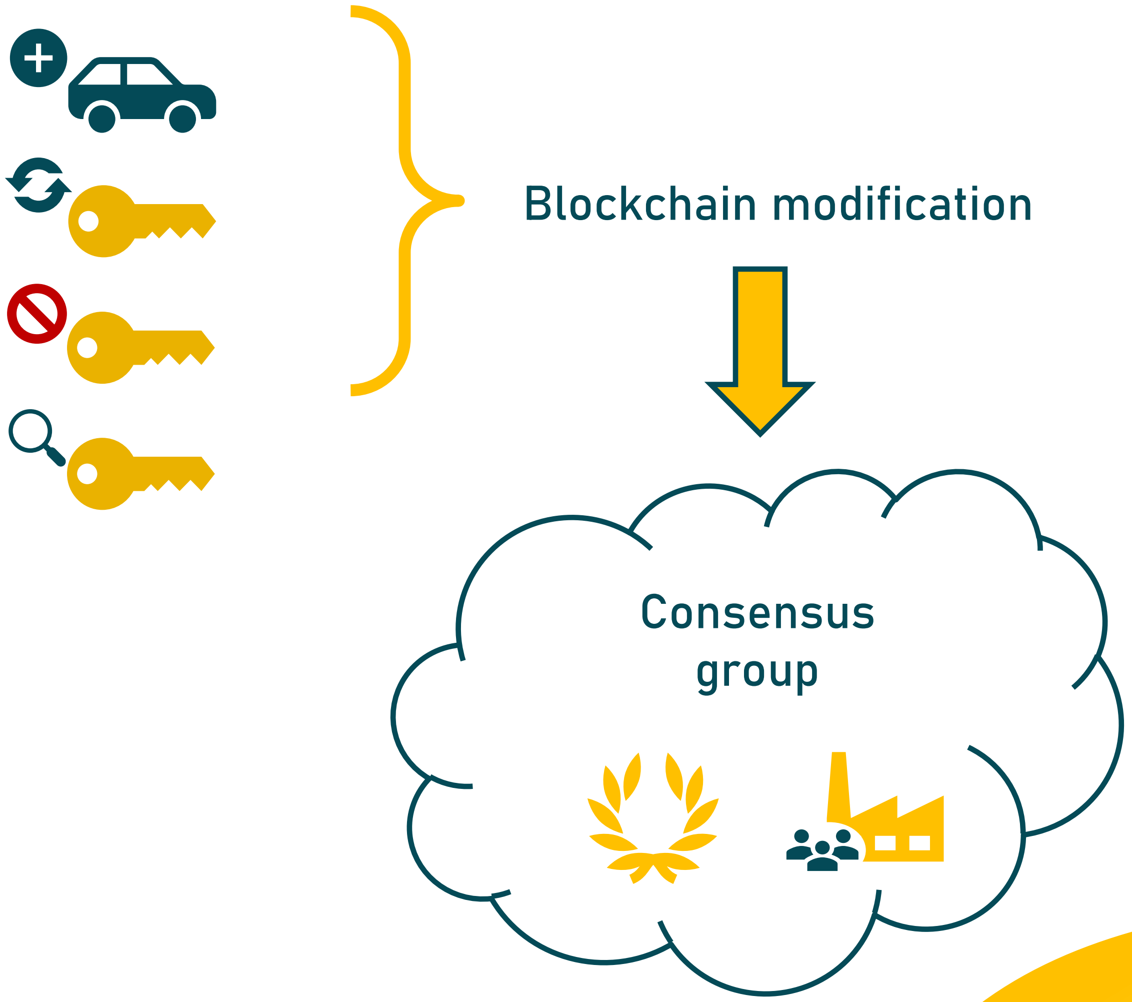


Accumulator



Procedures

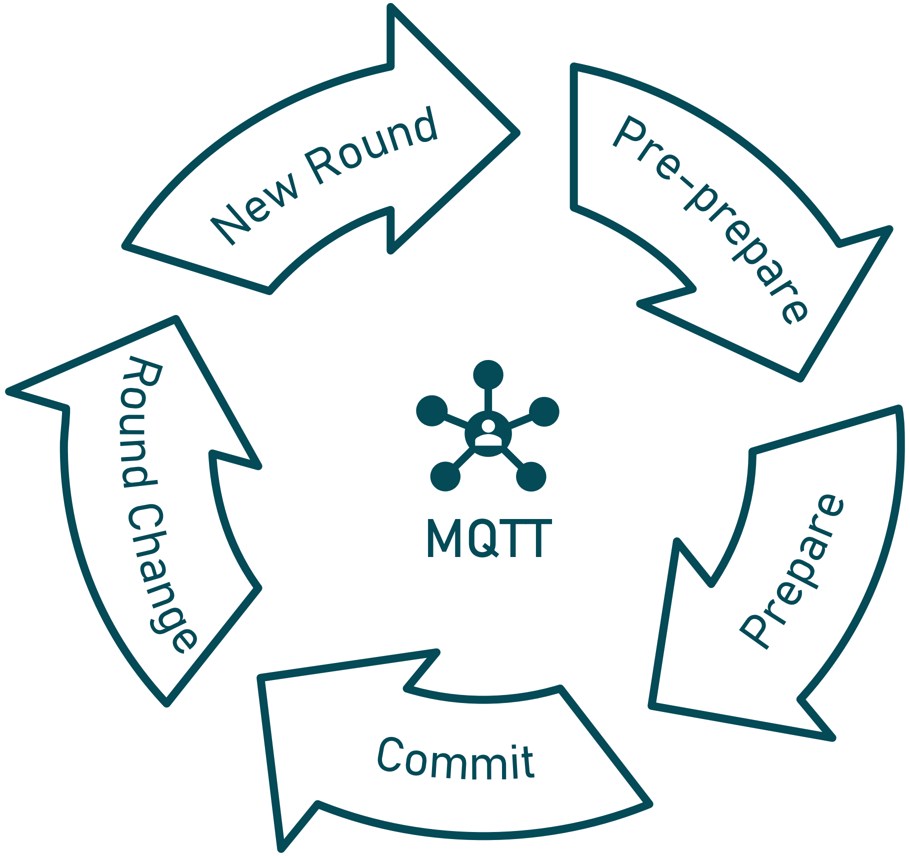
- *Enroll*
- *Update*
- *Revoke*
- *Verify*



Blockchain modification

Consensus group

Consensus mechanism: P.B.F.T.



New Round

Pre-prepare

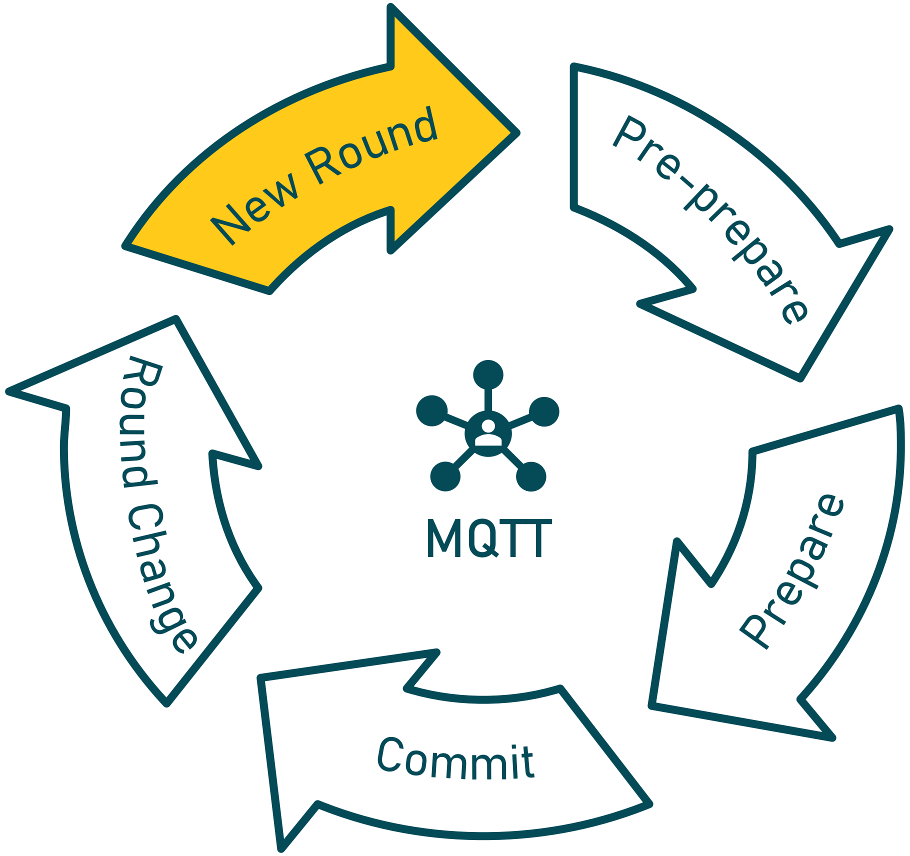
Prepare

Commit

Round Change

MQTT

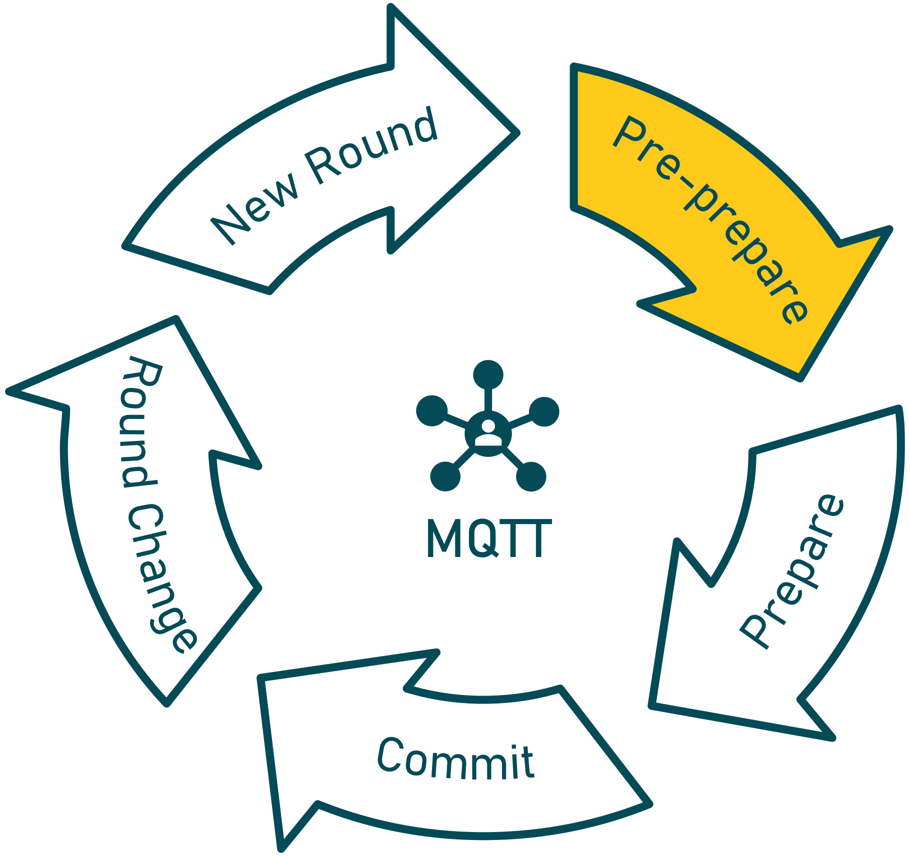
Consensus mechanism: P.B.F.T.



New round

- Leader node impersonation
- Operation selection

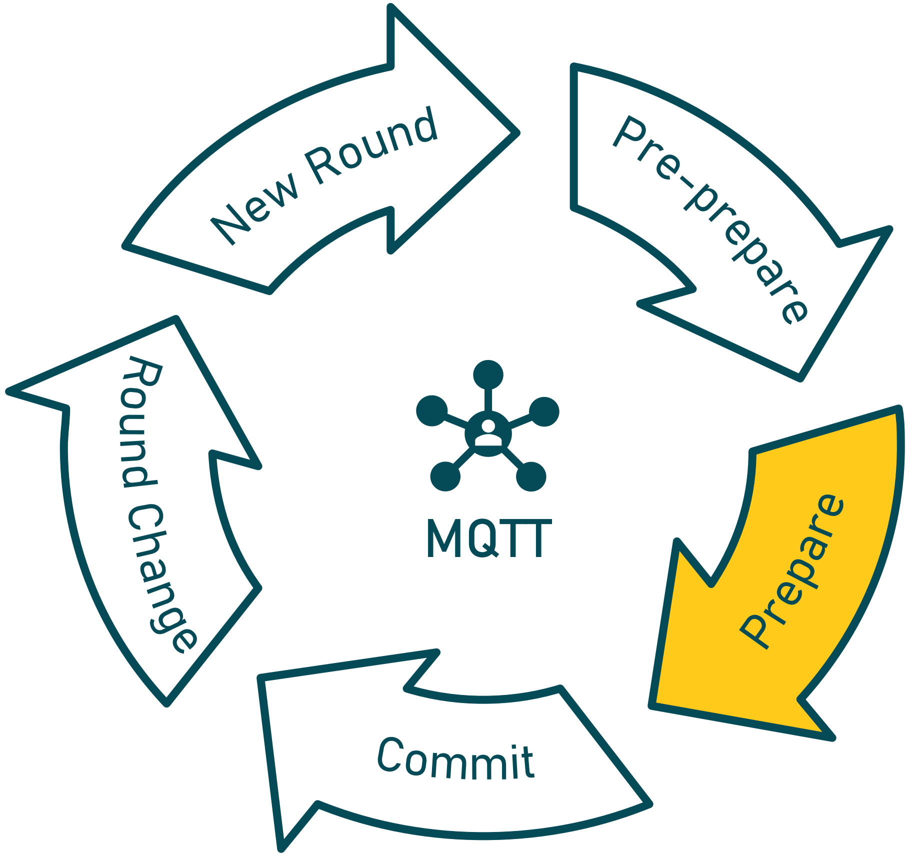
Consensus mechanism: P.B.F.T.



Pre-prepare

- New block proposal
- Signed multicast pre-prepare message to all validators

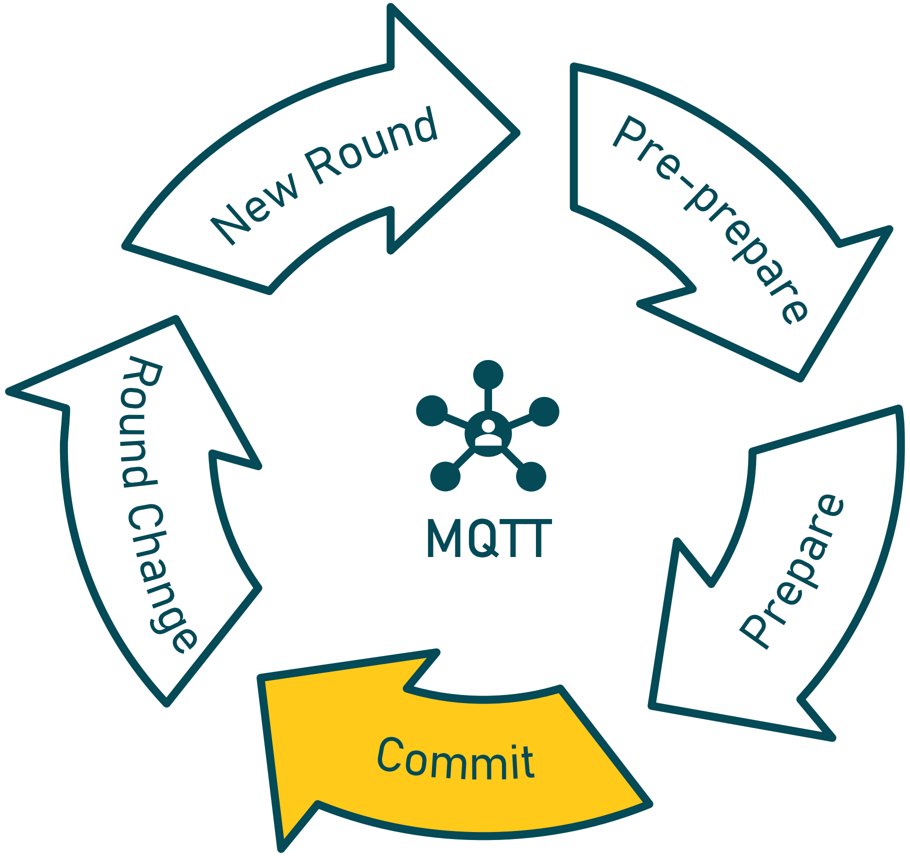
Consensus mechanism: P.B.F.T.



Prepare

- Validators check leader's proposal
- Approval / Rejection carried by prepare messages

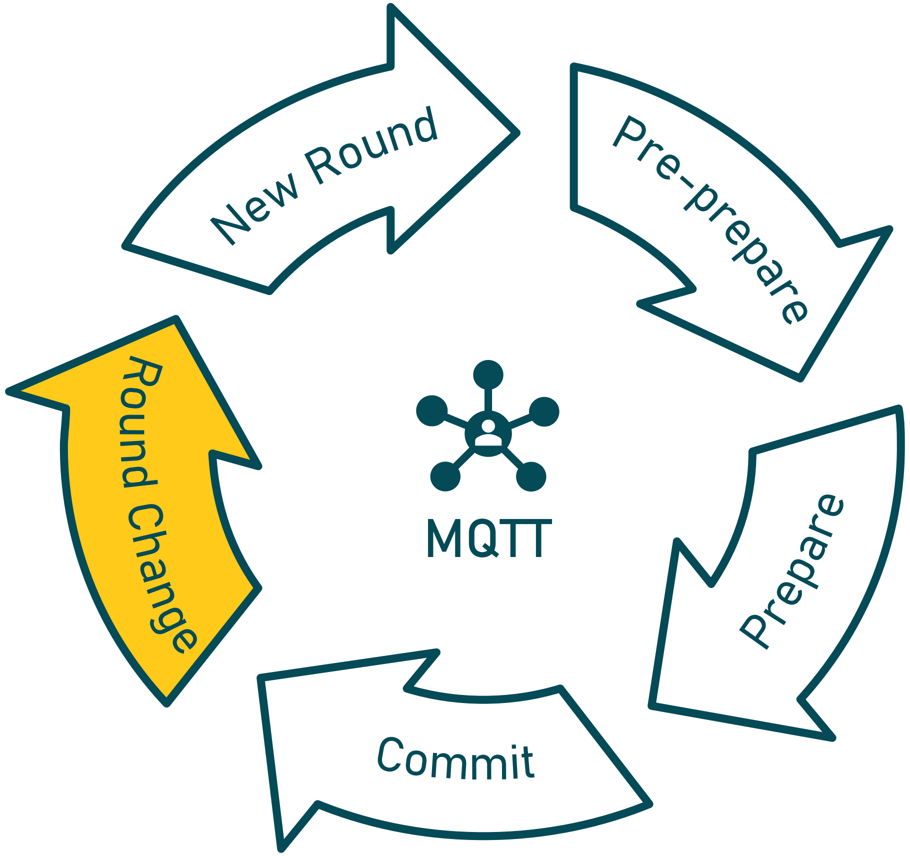
Consensus mechanism: P.B.F.T.



Commit

- Check of prepare messages
- If enough approvals:
  ⤷ Commit to blockchain ✓
- Else:
  ⤷ Failure ✗

Consensus mechanism: P.B.F.T.



Round Change

- Control left to DBPKI UI
- System gets ready for next round

Trust weights

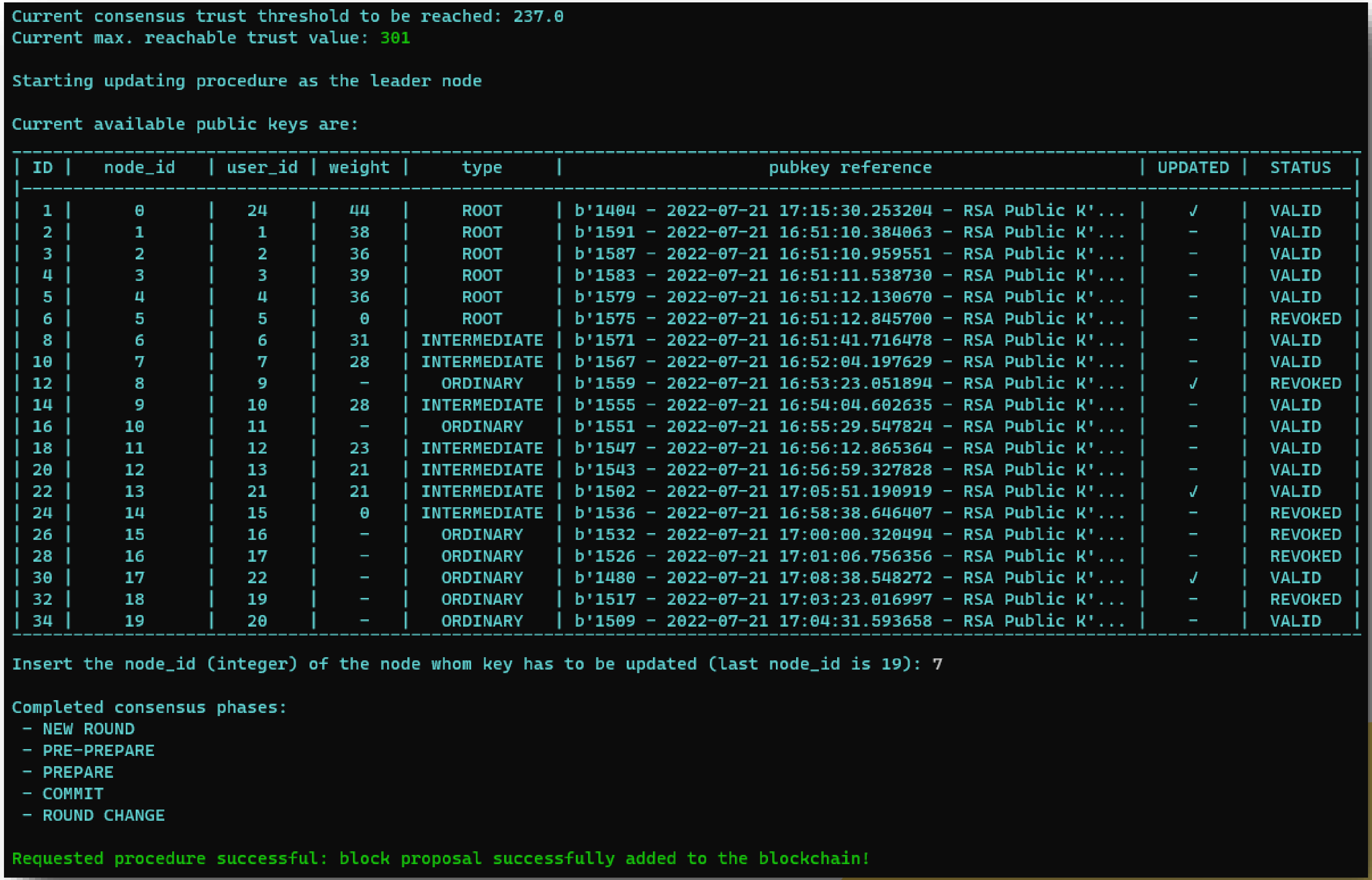
- Initial value depending on role type
- Weighted on time
- Reward-and-punishment mechanism

Commit successful if threshold

$$T = (2\lfloor t - 1 \rfloor + 1) \cdot \omega_{avg}^{i}$$

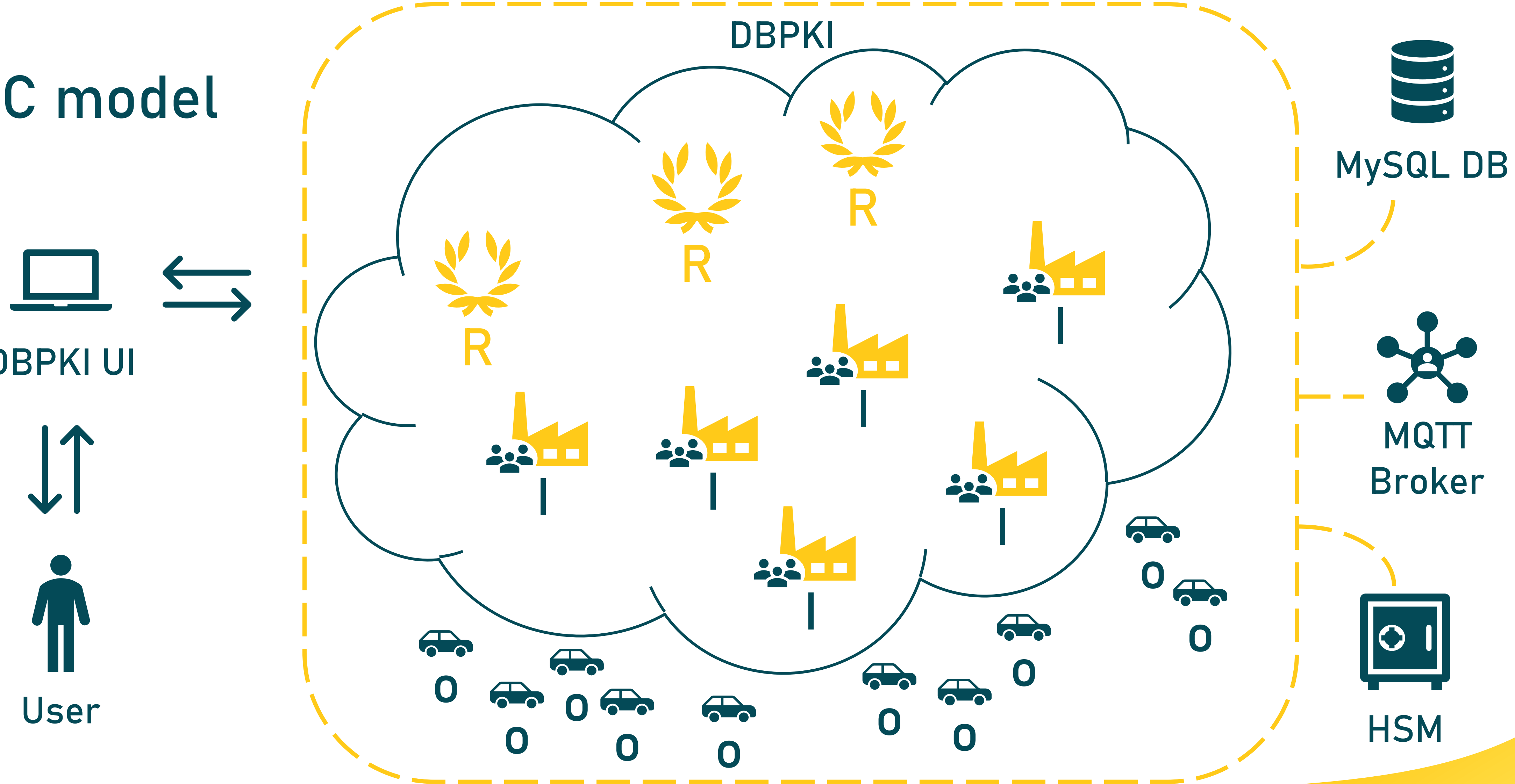
is reached

Trust weights



```
Current consensus trust threshold to be reached: 237.0
Current max. reachable trust value: 301

Starting updating procedure as the leader node

Current available public keys are:

-----------------------------------------------------------------------------------------------------------------------------------
| ID |    node_id    | user_id | weight |     type     |                    pubkey reference                      | UPDATED |  STATUS  |
|---------------------------------------------------------------------------------------------------------------------------------|
|  1 |       0       |   24    |   44   |     ROOT     | b'1404 - 2022-07-21 17:15:30.253204 - RSA Public K'... |    √    |  VALID   |
|  2 |       1       |    1    |   38   |     ROOT     | b'1591 - 2022-07-21 16:51:10.384063 - RSA Public K'... |    -    |  VALID   |
|  3 |       2       |    2    |   36   |     ROOT     | b'1587 - 2022-07-21 16:51:10.959551 - RSA Public K'... |    -    |  VALID   |
|  4 |       3       |    3    |   39   |     ROOT     | b'1583 - 2022-07-21 16:51:11.538730 - RSA Public K'... |    -    |  VALID   |
|  5 |       4       |    4    |   36   |     ROOT     | b'1579 - 2022-07-21 16:51:12.130670 - RSA Public K'... |    -    |  VALID   |
|  6 |       5       |    5    |    0   |     ROOT     | b'1575 - 2022-07-21 16:51:12.845700 - RSA Public K'... |    -    | REVOKED  |
|  8 |       6       |    6    |   31   | INTERMEDIATE | b'1571 - 2022-07-21 16:51:41.716478 - RSA Public K'... |    -    |  VALID   |
| 10 |       7       |    7    |   28   | INTERMEDIATE | b'1567 - 2022-07-21 16:52:04.197629 - RSA Public K'... |    -    |  VALID   |
| 12 |       8       |    9    |    -   |   ORDINARY   | b'1559 - 2022-07-21 16:53:23.051894 - RSA Public K'... |    √    | REVOKED  |
| 14 |       9       |   10    |   28   | INTERMEDIATE | b'1555 - 2022-07-21 16:54:04.602635 - RSA Public K'... |    -    |  VALID   |
| 16 |      10       |   11    |    -   |   ORDINARY   | b'1551 - 2022-07-21 16:55:29.547824 - RSA Public K'... |    -    |  VALID   |
| 18 |      11       |   12    |   23   | INTERMEDIATE | b'1547 - 2022-07-21 16:56:12.865364 - RSA Public K'... |    -    |  VALID   |
| 20 |      12       |   13    |   21   | INTERMEDIATE | b'1543 - 2022-07-21 16:56:59.327828 - RSA Public K'... |    -    |  VALID   |
| 22 |      13       |   21    |   21   | INTERMEDIATE | b'1502 - 2022-07-21 17:05:51.190919 - RSA Public K'... |    √    |  VALID   |
| 24 |      14       |   15    |    0   | INTERMEDIATE | b'1536 - 2022-07-21 16:58:38.646407 - RSA Public K'... |    -    | REVOKED  |
| 26 |      15       |   16    |    -   |   ORDINARY   | b'1532 - 2022-07-21 17:00:00.320494 - RSA Public K'... |    -    | REVOKED  |
| 28 |      16       |   17    |    -   |   ORDINARY   | b'1526 - 2022-07-21 17:01:06.756356 - RSA Public K'... |    -    | REVOKED  |
| 30 |      17       |   22    |    -   |   ORDINARY   | b'1480 - 2022-07-21 17:08:38.548272 - RSA Public K'... |    √    |  VALID   |
| 32 |      18       |   19    |    -   |   ORDINARY   | b'1517 - 2022-07-21 17:03:23.016997 - RSA Public K'... |    -    | REVOKED  |
| 34 |      19       |   20    |    -   |   ORDINARY   | b'1509 - 2022-07-21 17:04:31.593658 - RSA Public K'... |    -    |  VALID   |
-----------------------------------------------------------------------------------------------------------------------------------

Insert the node_id (integer) of the node whom key has to be updated (last node_id is 19): 7

Completed consensus phases:
 - NEW ROUND
 - PRE-PREPARE
 - PREPARE
 - COMMIT
 - ROUND CHANGE

Requested procedure successful: block proposal successfully added to the blockchain!
```

PoC model



DBPKI UI

User

DBPKI

MySQL DB

MQTT Broker

HSM

Results and conclusion

- Single machine
- Multicast messages

Up to 20 Root nodes during Setup ↔ Trade-off between security and efficiency

- Proposed solution removes the need of digital certificates and CAs
- MQTT central broker

→ Framework independent of communication protocol

Main improvements:

- Dynamic trust weights
- Reward-and-punishment mechanism
- PKCS#11 and HSM integration as RoT

The end

Thanks for your attention!