IA-CCF: Individual Accountability for Permissioned Ledgers

Alex Shamis\textsuperscript{1,2}, Peter Pietzuch\textsuperscript{1,2}, Burcu Canakci\textsuperscript{3}, Miguel Castro\textsuperscript{1}, Cedric Fournet\textsuperscript{1}, Edward Ashton\textsuperscript{1}, Amaury Chamayou\textsuperscript{1}, Sylvan Clebsch\textsuperscript{1}, Antoine Delignat-Lavaud\textsuperscript{1}, Matt Kerner\textsuperscript{4}, Julien Maffre\textsuperscript{1}, Olga Vrousoug\textsuperscript{1}, Christoph M. Wintersteiger\textsuperscript{1}, Manuel Costa\textsuperscript{1}, and Mark Russinovich\textsuperscript{4}

\textsuperscript{1}Microsoft Research, \textsuperscript{2}Imperial College London, \textsuperscript{3}Cornell University, \textsuperscript{4}Microsoft Azure
What is a permissioned ledger?

- Distributed system that provides a service for users
- Record events in a ledger
- Consortium members bring replicas
- Replicas operated by consortium members
- Only authorized users, members, and replicas can access the system
Properties of a permissioned ledger

• Byzantine Consensus Protocol
• Safety
• Valid when less than 1/3 replicas misbehave
• Ledger
• Events recorded in a ledger
• Omit transactions when 1/3 or more replicas misbehave
• Rewrite the ledger when 2/3 or more replicas misbehave
Auditing permissioned ledgers

• Auditing detects when a problem occurred
• All replicas and their members are blamed for the misbehavior.

• **Goal**: Individual accountability
Individual Accountability

• Misbehaviour results in consequences
• Misbehaviour must always be detectable
Co-designing the permissioned ledger

- Co-design
- Minimize signatures
  - One replica signature to commit a batch
  - Signature in receipts and ledger
- Receipts
  - Response in 2 round trips
  - Replicas commit to execution
IA-CCF and L-PBFT

25/03/2022
IA-CCF: Individual Accountability for Permissioned Ledgers
Sending a request
Early execution: Primary replica
Early execution: Backup replicas

Alice

Bank

Prepare

Pre-

Execute

Write to Ledger

Execute

Bank

Bank

Prepare

Write to Ledger

Bank

Bank

Write to Ledger

Bank
Agreement on execution
Creating a receipt
Committing the request
Example: Misbehaving replicas
Example: Banking transactions
Auditing: Banking transactions

Bob

Receipt

Receipt

25/03/2022

IA-CCF: Individual Accountability for Permissioned Ledgers

Ledger

Checkpoint

Deposit

Withdraw

25/03/2022
Auditing: Banking transaction
Auditing: Banking transaction

What if the malicious members also changed the replica set?
Changing the replica set

- Governance protocol
- Member propose change
- Members vote to accept change
- Reconfiguration
- Governance sub-ledger
Receipts and the active replica set

- Receipts
- Governance sub-ledger
- Genesis transaction to current replica set

- Details and *proof* in the paper
Implementation

- Built IA-CCF on top of *CCF*:
  - Transaction engine and key-value store
  - Ledger and receipts
  - Programmable Governance protocol
- IA-CCF co-designed:
  - Byzantine consensus protocol (L-PBFT), Ledger, Receipts, and Governance protocol

http://ccf.dev
Performance evaluation

• Smallbank benchmark
• Transfer funds between accounts
• LAN environment
• 1 datacenter
• WAN environment
• 3 geo-distributed Azure datacenters
Throughput vs Latency (LAN)

Throughput (tx/s)

Latency (ms)

IA-CCF

IA-CCF-PeerReview

IA-CCF-PeerReview

IA-CCF

25/03/2022

IA-CCF: Individual Accountability for Permissioned Ledgers
Scale-out (WAN)

Throughput (tx/s) vs Number of replicas

- IA-CCF
- IA-CCF-PeerReview

4 replicas

64 replicas

25/03/2022

IA-CCF: Individual Accountability for Permissioned Ledgers
Performance of IA-CCF features

Throughput (tx/s)

- HotStuff: 307,997
- L-PBFT: 299,321
- + Tx engine: 131,959
- + Ledger: 128,921
- + L-PBFT signatures: 111,926
- + Signed Requests: 51,209
- + Receipts (IA-CCF): 47,841
Conclusion

• Individual Accountability
• Only blame replicas that misbehave
• Co-design - Byzantine consensus protocol, Ledger, Receipts, and Governance
• 1 signature per batch
• Receipts returned to client in 2 round trips
• Auditing with individual accountability proof

http://ccf.dev