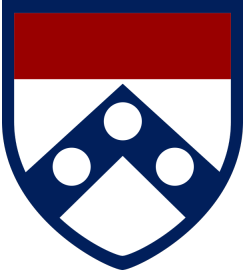


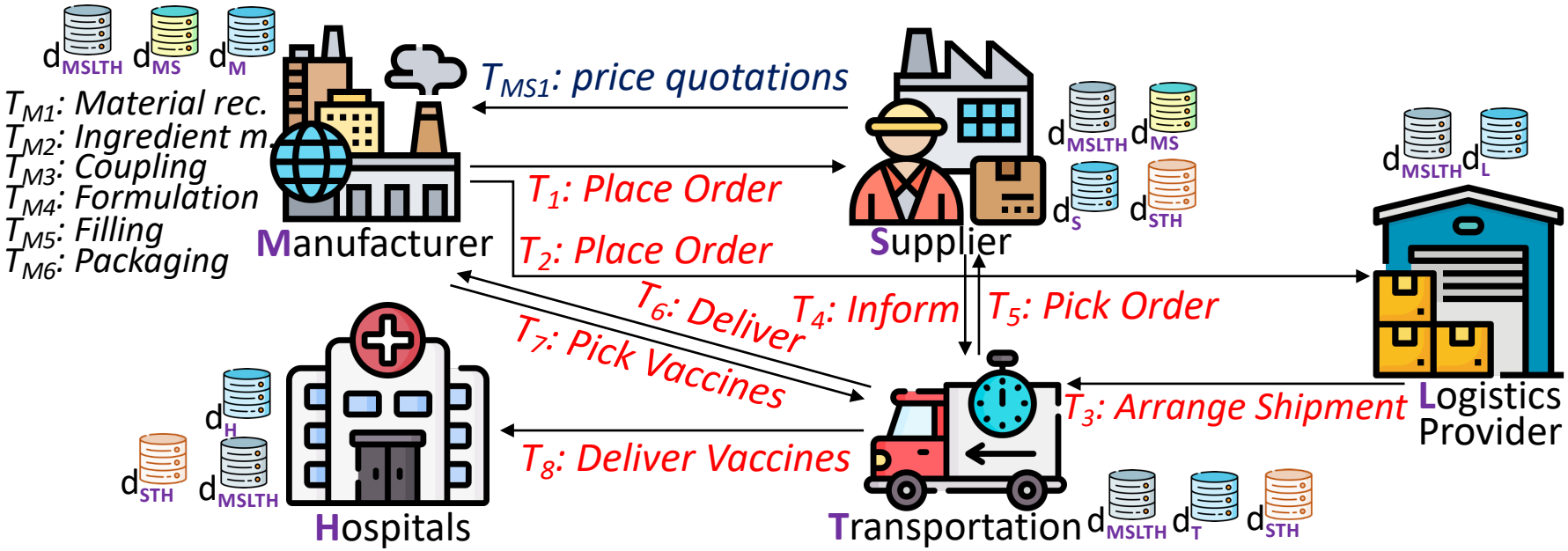
Qanaat: A Scalable Multi-Enterprise Permissioned Blockchain System with Confidentiality Guarantees

Mohammad Javad Amiri[1], Boon Thau Loo[1], Divyakant Agrawal[2], Amr El Abbadi[2]

[1]University of Pennsylvania, [2]University of California Santa Barbara

VLDB 2022

COVID-19 Vaccine Supply Chain



Requirements:

R1. Confidential collaborations across enterprises

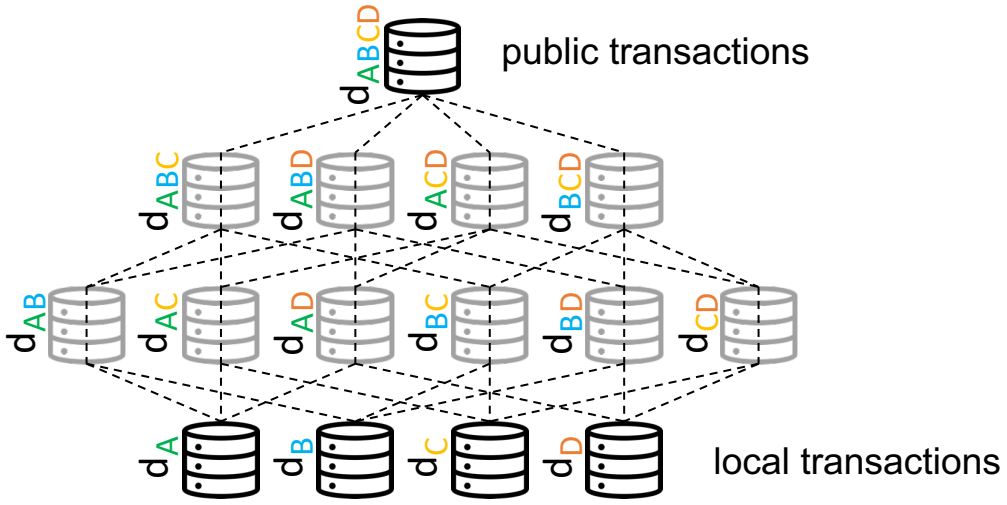
R2. Data consistency across collaboration workflows

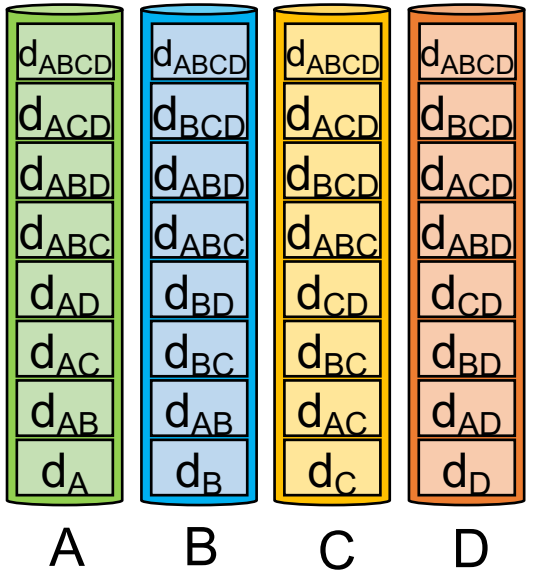
R3. Confidential data leakage prevention

R4. Scaling multi-shard enterprises

R1. Confidential Collaborations across Enterprises

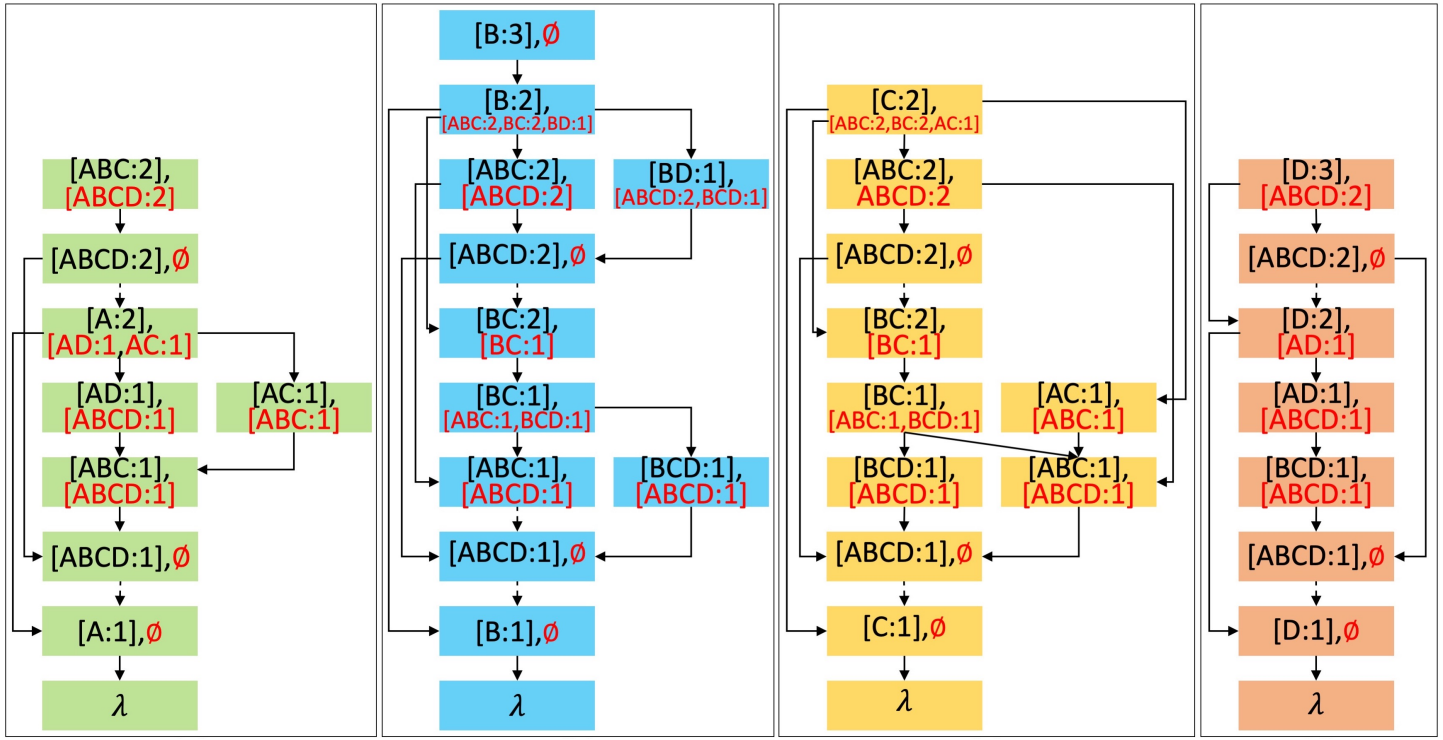
- A hierarchical data model consisting of a set of data collections
- Operational primitives
  - Write: transactions of d_X write only on the records of d_X
  - Read: transactions of d_X can read the records of d_Y if d_X is order-dependent on d_Y
    - d_X is order-dependent of d_Y if $X \subseteq Y$





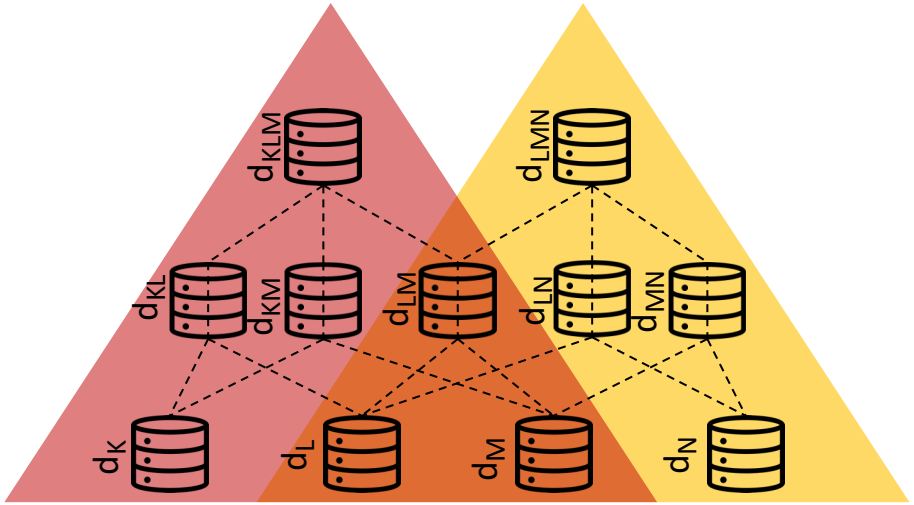
Qanaat Blockchain Ledger

- Guarantees two properties
  - Local consistency: enforces a total order on the transactions of each data collection
  - Global consistency: determines the transaction order of d_X considering the state of every data collection d_Y that d_X is order-dependent on ($X \subseteq Y$)
- Transaction ID = $\langle \alpha, \gamma \rangle$
  - local part α = $[X{:}n]$
  - Optionally, a global part γ:
    - for every order-dependent data collection d_Y, add $Y{:}m$



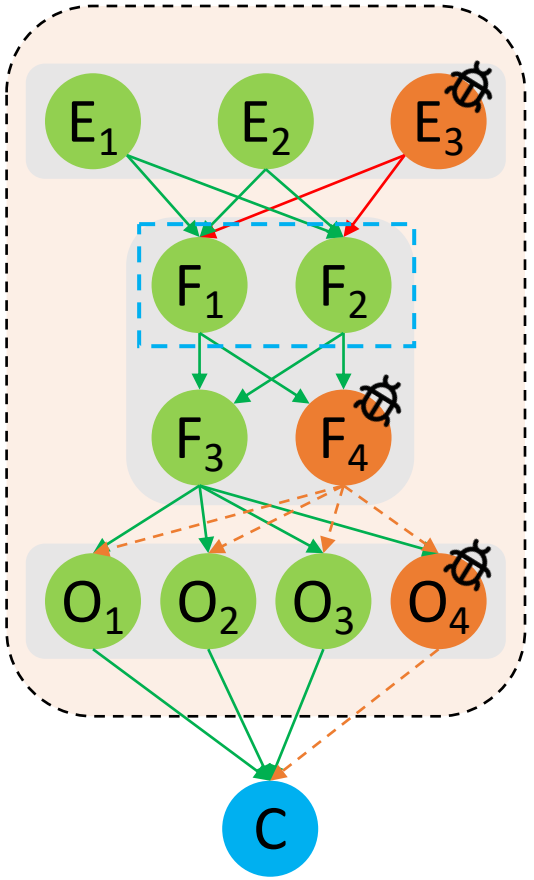
R2. Data Consistency across Collaboration Workflows

- An enterprise might be involved in multiple collaboration workflows (instances of Qanaat)
  - A supplier that provides raw materials for both Pfizer and Moderna vaccines
- Qannat creates a single data collection for each enterprise



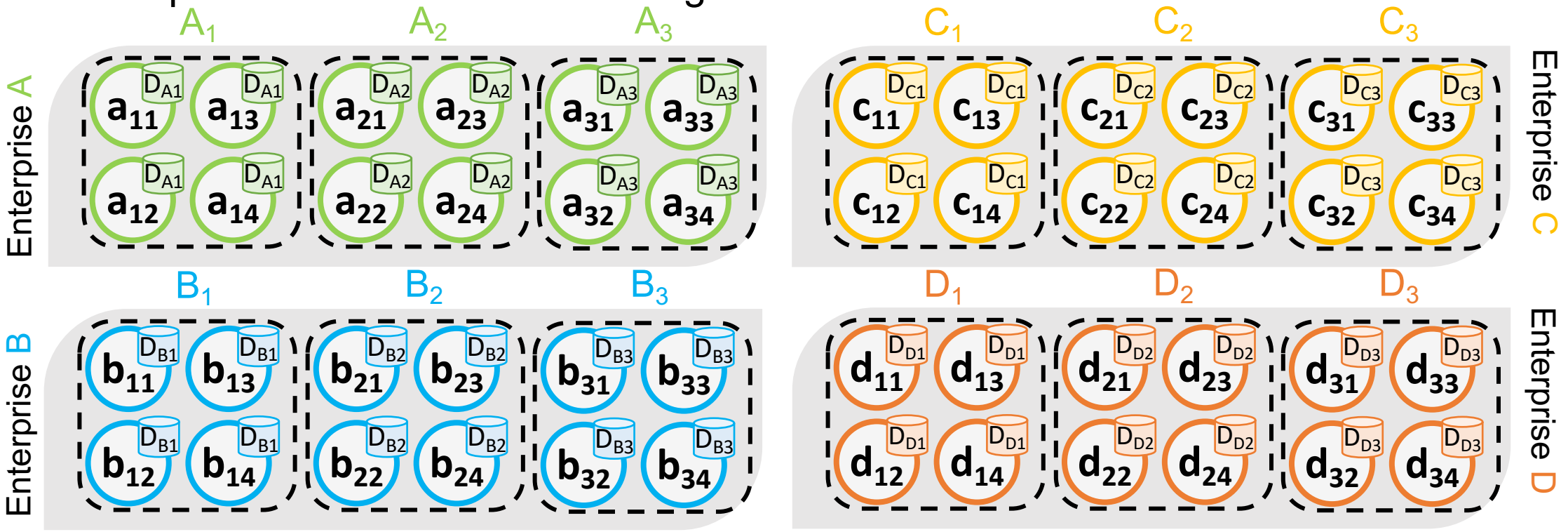
R3. Confidential Data Leakage Prevention

- Malicious nodes can violate data confidentiality
  - leaking requests, replies, or data stored and processed
- Privacy firewall mechanism
  - Separates ordering node from execution nodes
    - $3f + 1$ ordering nodes and $2g + 1$ execution nodes
      - Assuming f faulty ordering and g faulty execution nodes
  - Adds a privacy firewall in between
    - Consists of a set of $h + 1$ rows of $h + 1$ filters (h faulty node)
  - Network configuration physically restricts communication paths between ordering nodes, filters, and execution nodes
  - A malicious node can either access confidential data or communicate freely with clients *but not both*



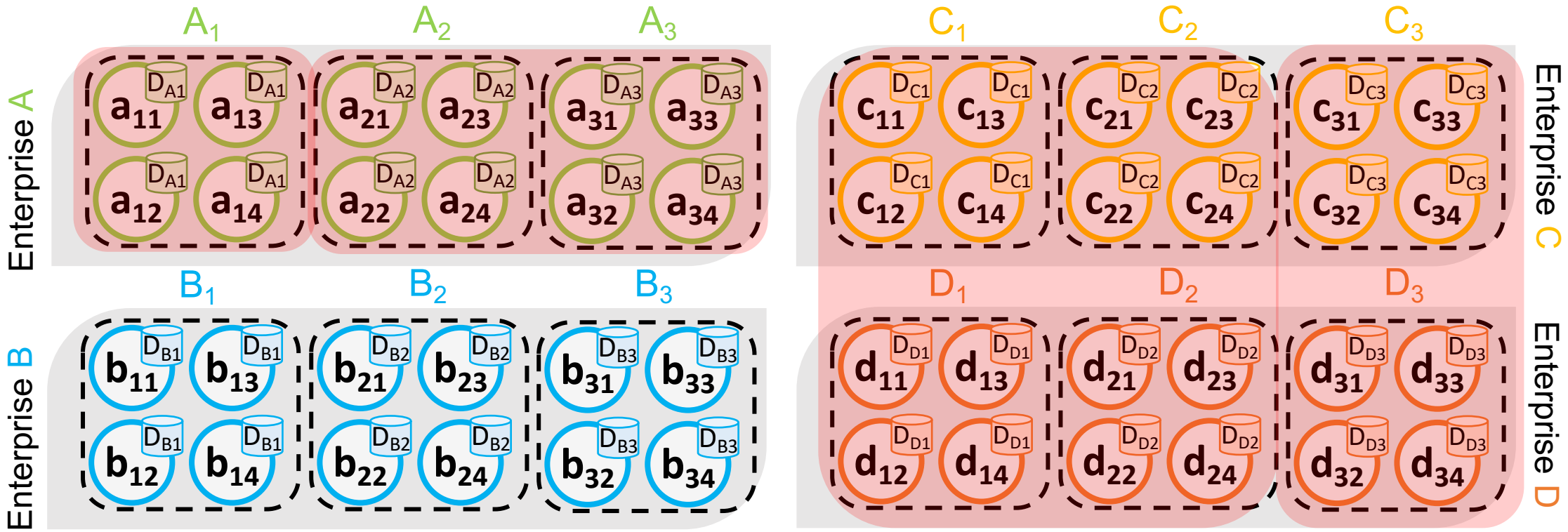
R4. Scaling Multi-Shard Enterprises

- The enterprise data is partitioned into different shards: D_{A1}, D_{A2} and D_{A3}
- Each shard is replicated on a cluster of execution nodes: D_{A1} on a_{11}, a_{12}, a_{13} and a_{14}
- Each cluster maintains a different ledger
- Enterprises use the same sharding schema for each shared data collection



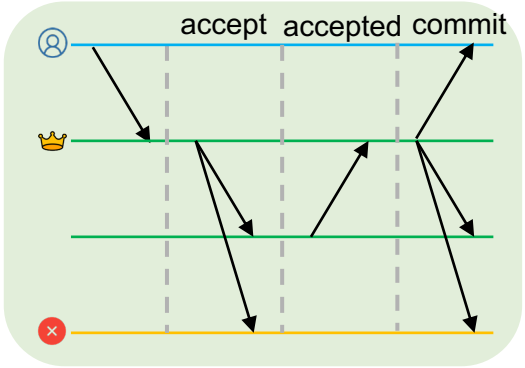
Transaction Processing

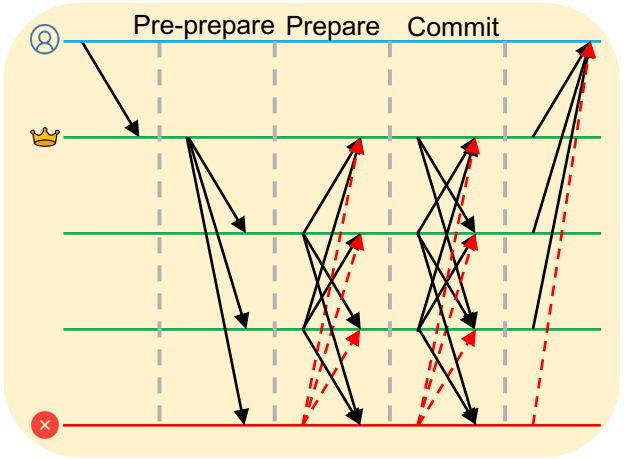
- Intra-shard intra-enterprise: **A_1**
- Intra-shard cross-enterprise: **C_3, D_3**
  - On a shared data collection shard D_{CD3}
- Cross-shard intra-enterprise: **A_2, A_3**
- Cross-shard cross-enterprise: **C_1, D_1, C_2, D_2**
  - Across two shared data collection shards D_{CD1} and D_{CD2}



Consensus Protocols

- Intra-shard intra-enterprise consensus
  - Crash failure: **Paxos**
  - Byzantine failure: **PBFT**

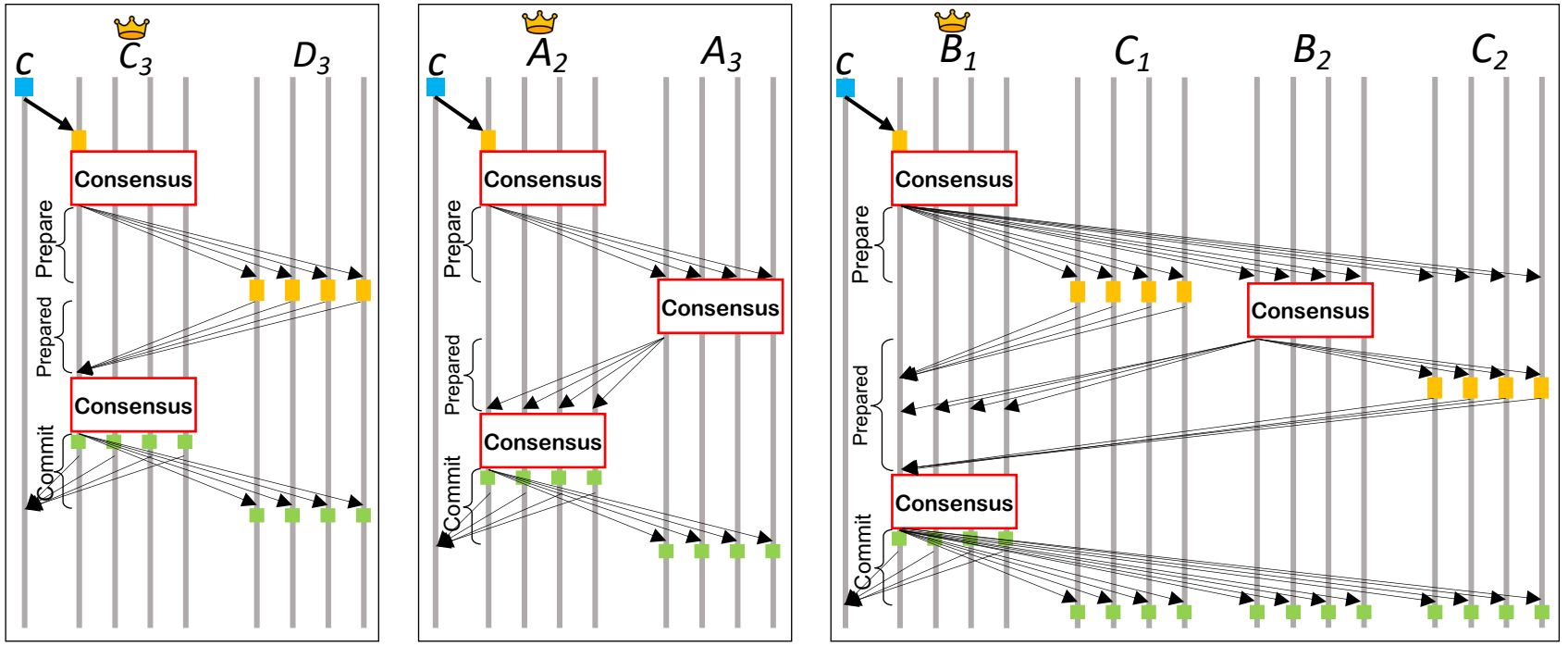




- Cross-cluster consensus
  - Coordinator-based
  - Flattened

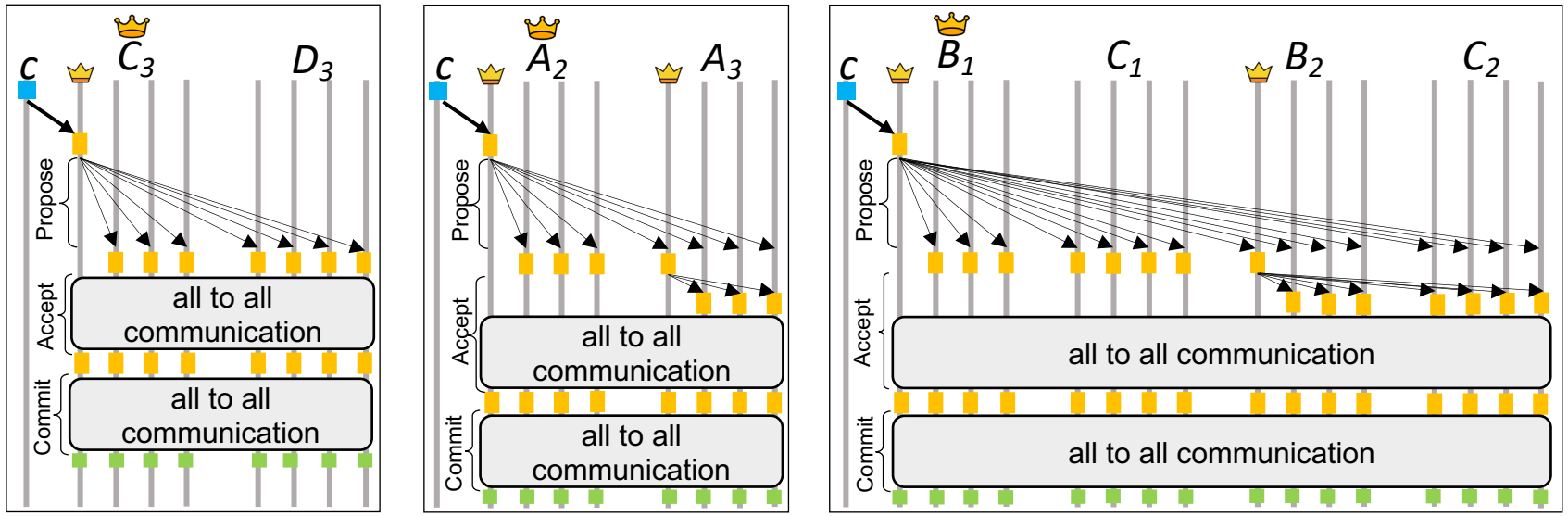
Coordinator-based Consensus Protocol

- Intra-shard cross-enterprise
- Cross-shard intra-enterprise
- Cross-shard cross-enterprise



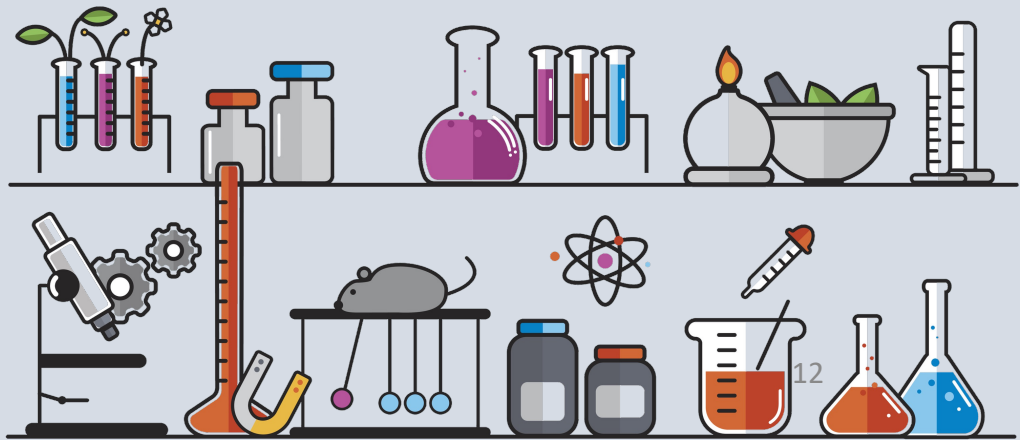
Flattened Consensus Protocol

- Intra-shard cross-enterprise
- Cross-shard intra-enterprise
- Cross-shard cross-enterprise

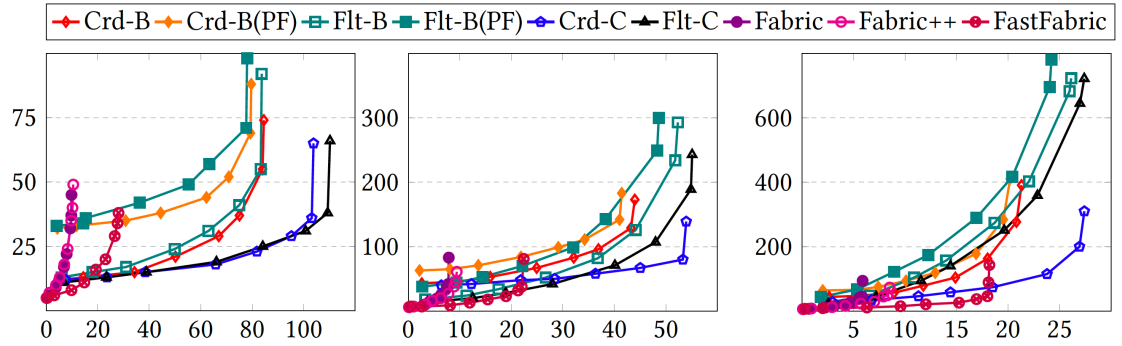


Experimental Settings

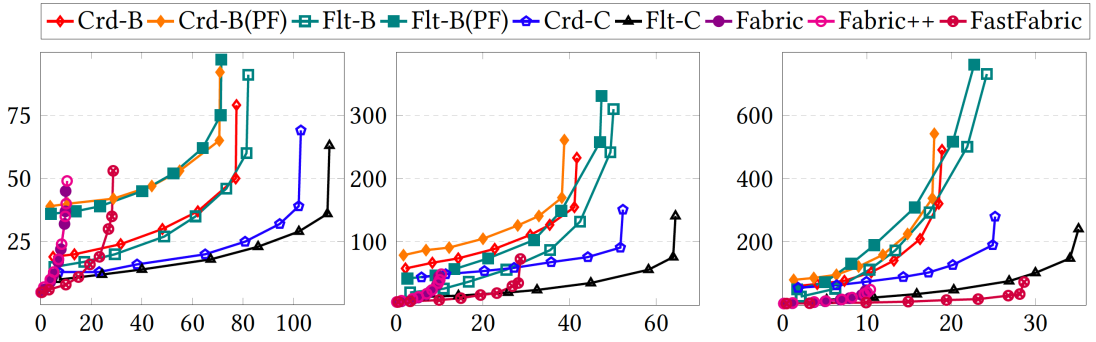
- Platform: Amazon EC2
- Measuring performance
  - Throughput & Latency
- Systems:
  - Hyperledger Fabric
  - Fabric++
  - FastFabric
  - Qanaat: Crd-C, Crd-B, Crd-B(PF), Flt-C, Flt-B, Flt-B(PF)



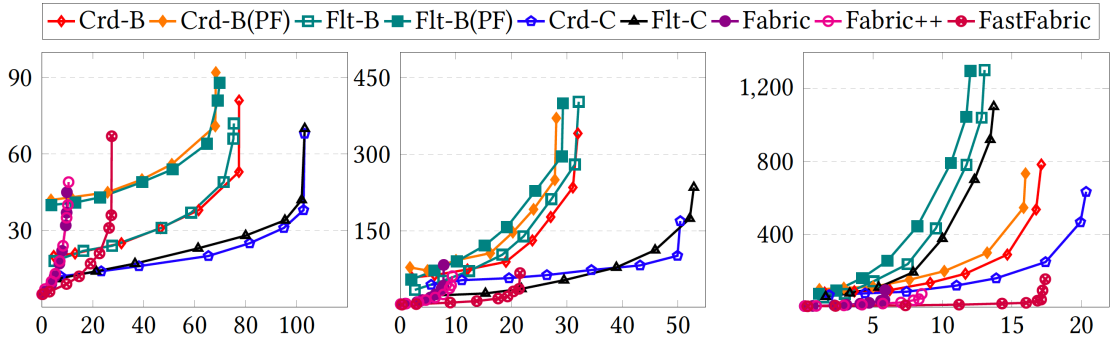
Experimental Results



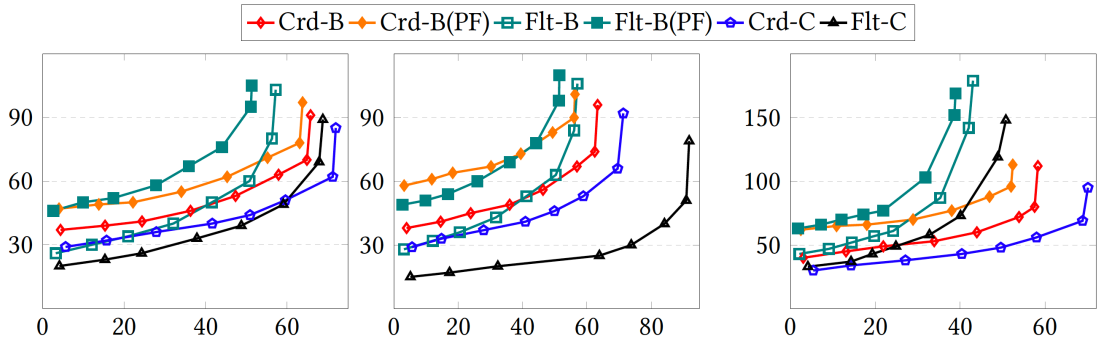
10%, 50%, and 90% Intra-shard cross-enterprise



10%, 50%, and 90% cross-shard intra-enterprise



10%, 50%, and 90% cross-shard cross-enterprise



Scalability over spatial domains

Qanaat Conclusion

- A permissioned blockchain system to support the scalability and confidentiality requirements of multi-enterprise applications.
- Presents a hierarchical data model consisting of a set of data collections for each collaboration workflow to support confidential collaboration.
- To prevent confidential data leakage, utilizes a privacy firewall mechanism.
- To support scalability, each enterprise partitions its data into different shards
- Presents a suite of consensus protocols is presented to process different types of intra-shard and cross-shard transactions within and across enterprises.

Questions?

mjamiri@seas.upenn.edu

Qanaat is a scalable underground network consisting of private channels to transport water from an aquifer to the surface