Fabric v1.2 新特性解析

IBM 郭剑南 @guoger

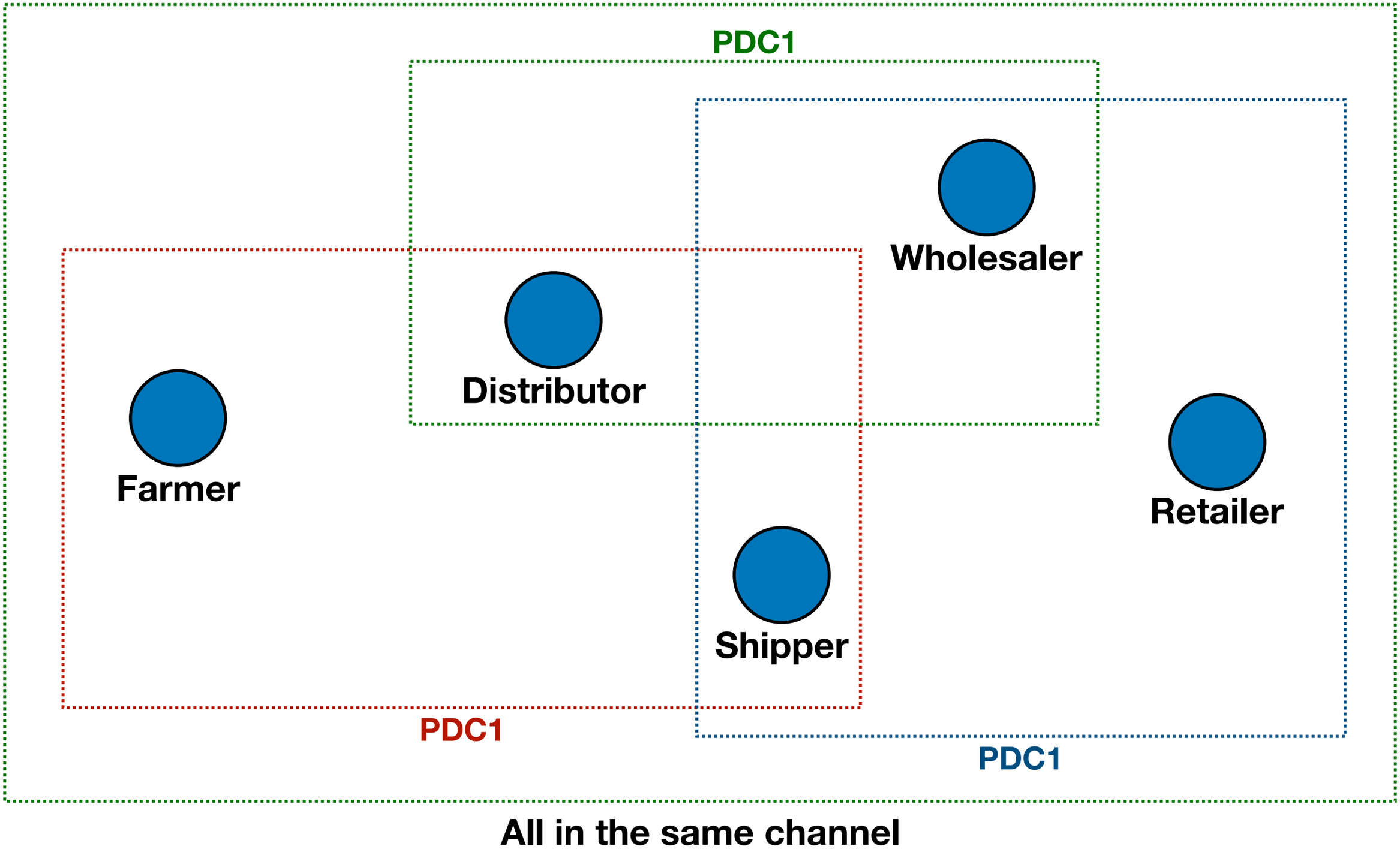
weather report

- Over 250 developers
- 37 companies and 87 individuals
- Over 7,000 commits
- Expect ~ quarterly releases

Agenda

- Private Date
- Service Discovery
- Pluggable e/v system chaincode

Private Data



Private Data

Fabric 1.0 has privacy across channels, but not within channels

Read/write set and sensitive data in transaction proposal are visible in the **chain of blocks**.

Ordering service doesn't parse transaction, but still has access to transaction, including read/write set (Orderer ledger stores blocks with transactions)

All peers in a channel have access to the transaction data.

Data privacy is required in many **use cases** such as

Health Care

KYC

Private Data

How can we provide **privacy for certain sensitive/private data** within a channel?

Sensitive data on the ledger should **remain *private*** from the
chain of blocks
ordering service, and
a subset of the peers in a channel

Only **evidence** needs to be
on the chain of blocks
sent to ordering service and distributed to all peers

Chaincode should be able to perform **query/update of private data** on authorized peers.

Private Data

Why can't we **encrypt/decrypt** data?

- **Key maintenance** and sharing of key is overhead.
- Even encrypted data is not completely safe – keys can be leaked, and tomorrow's computing advances may crack today's encryptions.

Why can't we use **channel between peers** who are taking part in the transaction?

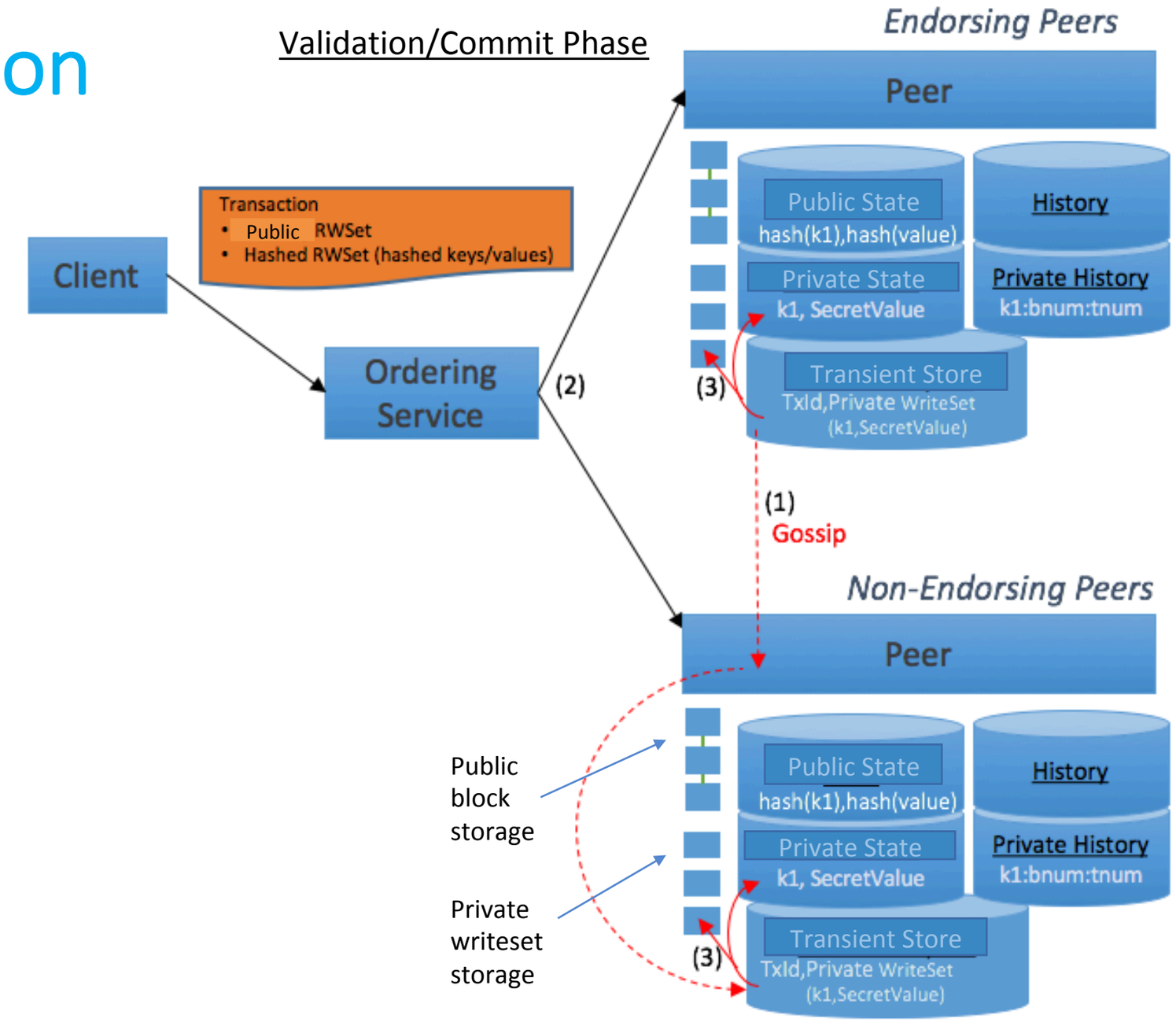
- **No sharing** of data between channels (single tx cannot modify two or more channel's ledger).
- Still the data would be **visible** to **ordering** service.

How about storing data in a separate data store and include only **hashes** on chain?

- Requires management of a **separate data store**
- **Data synchronization** and **access control** issues

Private Data Solution

1. Private data shared with authorized peers upon endorsement and stored in each peer's transient store.
2. Public channel data and hashes of private data included in transaction and distributed to all peers.
3. Upon validation/commit, private data moved to private state database and private writeset storage.



Service Discovery

- SDK needs a lot of information
  certificates, IP:Port, endorsement policies, location of cc

- React dynamically to network changes
  add/rm node/org, peer crash

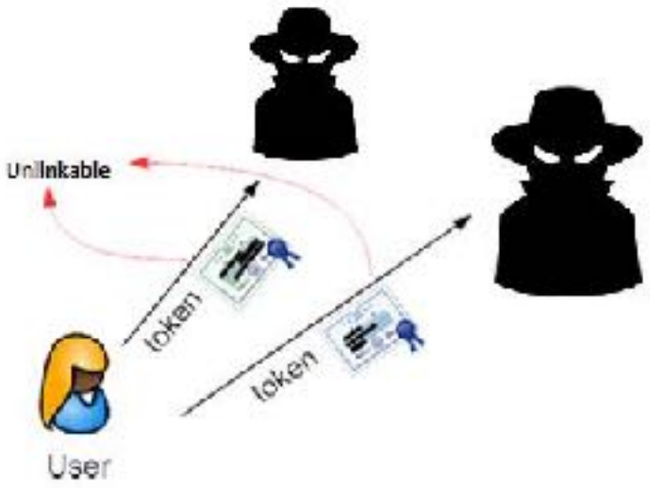
- Peers are not always in sync
  submit tx to peers with newest block

Service Discovery

SDK:

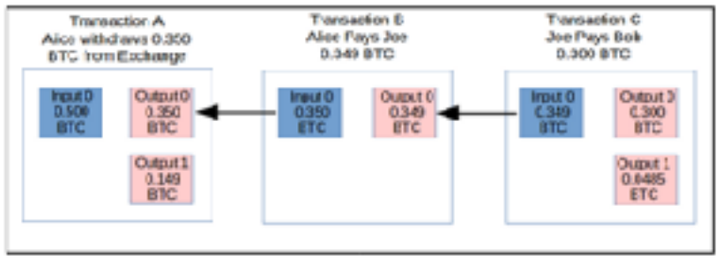
- connects to a trusted peer (typically in your org)
- queries configuration service (running on peer)
- selects peers based on criteria (specified in client)
- sends tx (as usual)

Pluggable E/V Syscc



Identity unlinkability

State based ownership



UTXO validation

Pluggable E/V Syscc

- Dynamic reconfiguration (hot-swap)

- Safe (consent and run same version)