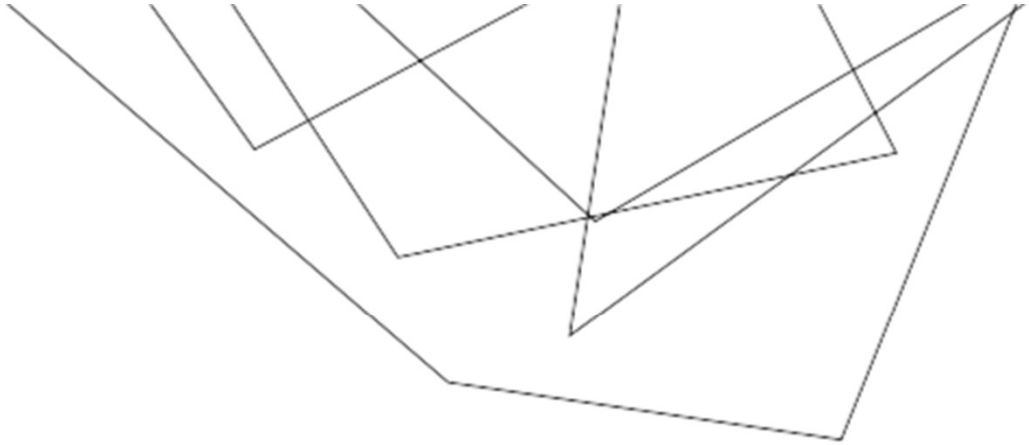
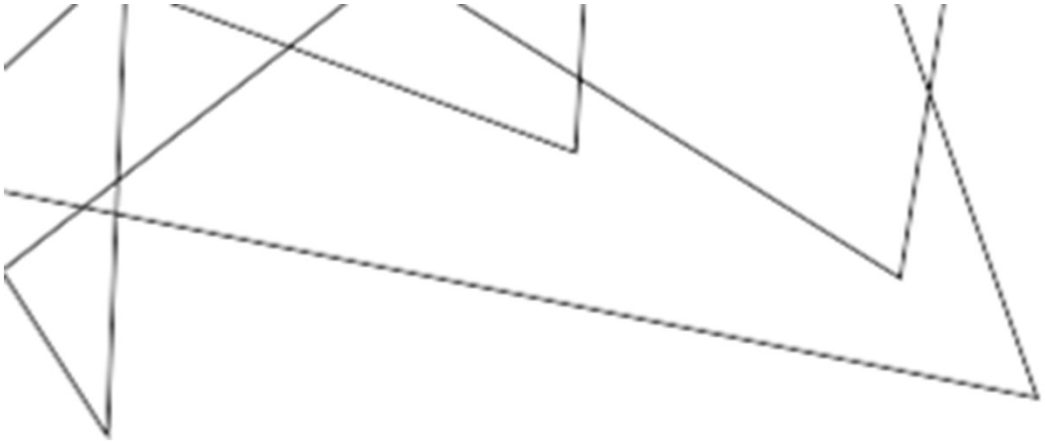


Emanuel Nunes
Samih Eisa
Miguel L. Pardal
Mário Calha

CONFIDENTIAL CHANNEL-TO-CHANNEL DATA EXCHANGE in a Permissioned Blockchain



OUTLINE

- Introduction
- Hyperledger Fabric
- Problem
- CC2C
- Use Case
- Next Steps
- Conclusion

Blockchain

- A decentralized, distributed ledger technology that records transactions securely, transparently, and immutably using cryptographic techniques:
  - Implemented in a distributed system
  - Peer-to-peer

- Blockchains decentralize control over data and code
  - Replace trusted third parties

ethereum

Blockchain Permissions

- Permissionless (Public Blockchain)
  - Open to anyone
  - No central authority

- Permissioned (Private/Consortium Blockchain)
  - Access is restricted to approved participants
  - Controlled governance
  - Example: Hyperledger Fabric

Hyperledger Fabric

- Permissioned blockchain platform
  - Designed for enterprise applications
  - Focus on privacy / confidentiality

Hyperledger Fabric - Key Concepts

- **Data Assets** - digital representations of tangible and intangible assets
- **Chaincode** - programs that enforce business rules
- **Ledger** - immutable record of all transactions
- **World State** - queriable database with current snapshot of ledger data
- **Channels** - private sub-networks/ledgers for data segmentation
- **Peers** - nodes that maintain the ledger and execute transactions
- **Consensus and Ordering** - mechanism for agreeing on transaction order

Blockchain technology can replace trusted intermediaries

- Permissioned blockchains authenticate who can access
  - e.g. Hyperledger Fabric

- But data owners want to retain control
  - Even with known partners
  - They may want to filter and transform data **before** it is shared

HL Fabric protects ownership…

- Mechanisms relevant for data ownership:
  - Channels
    - Isolate ledgers per group of partners
  - and Private data collections (PDCs)
    - Restrict record visibility to a subset of members in the same channel

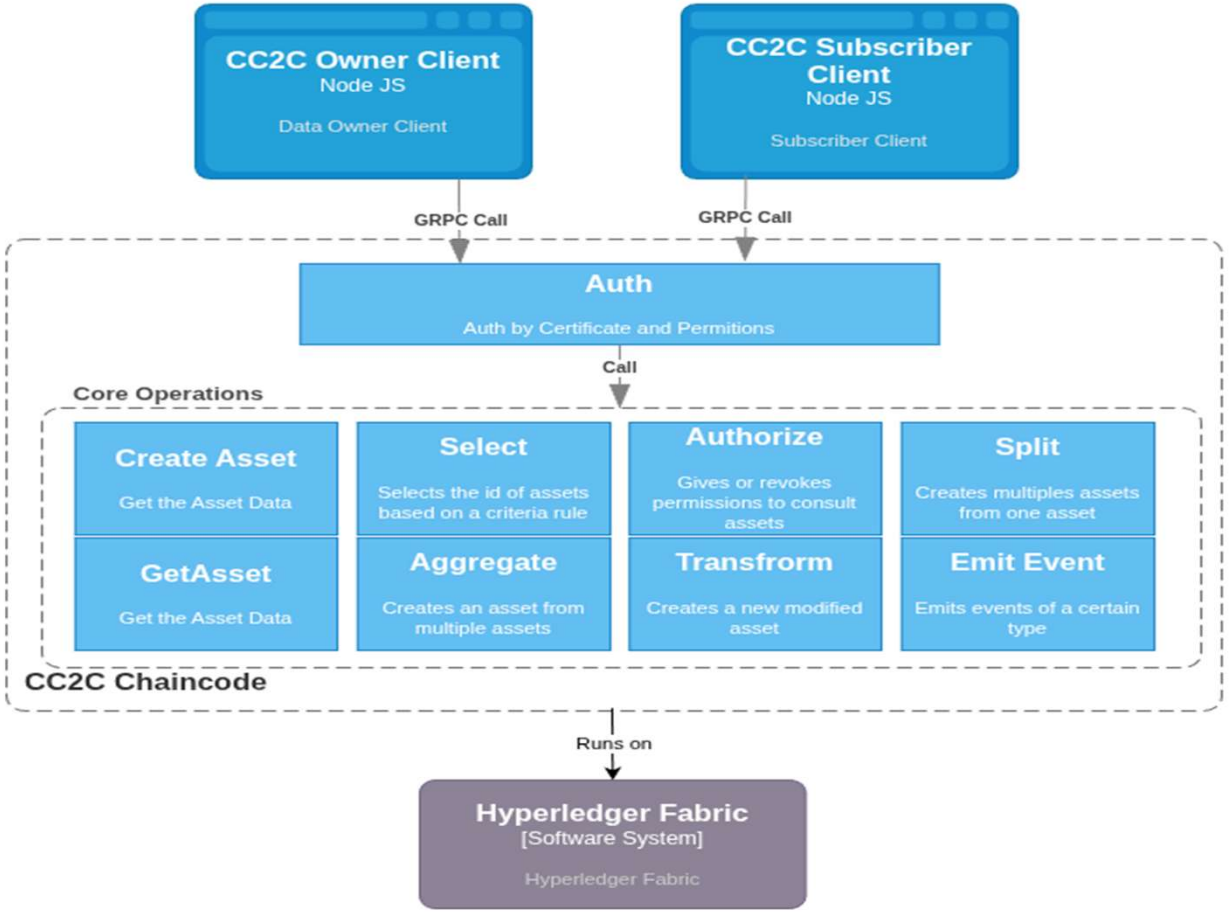
… but lacks fine-grained visibility controls

- Neither channels nor PDCs address the secure and controlled sharing of information **across** different channels
  - It is not just a matter of data visibility
  - The data contents themselves need to be modified
    - e.g. remove details that are not to be share
- Examples:
  - Share date, not time
  - Share region, not GPS coordinates
  - Share sold packages details, not all of the production

CC2C Proposal

- Confidential **Channel-to-Channel** Data Exchange in a Permissioned Blockchain.
- It leverages channels in Hyperledger Fabric to achieve data isolation but also includes the ability to filter and transform the data that is to be shared.
- It provides secure and confidential data sharing between separate blockchain organization groups.

CC2C - Architecture

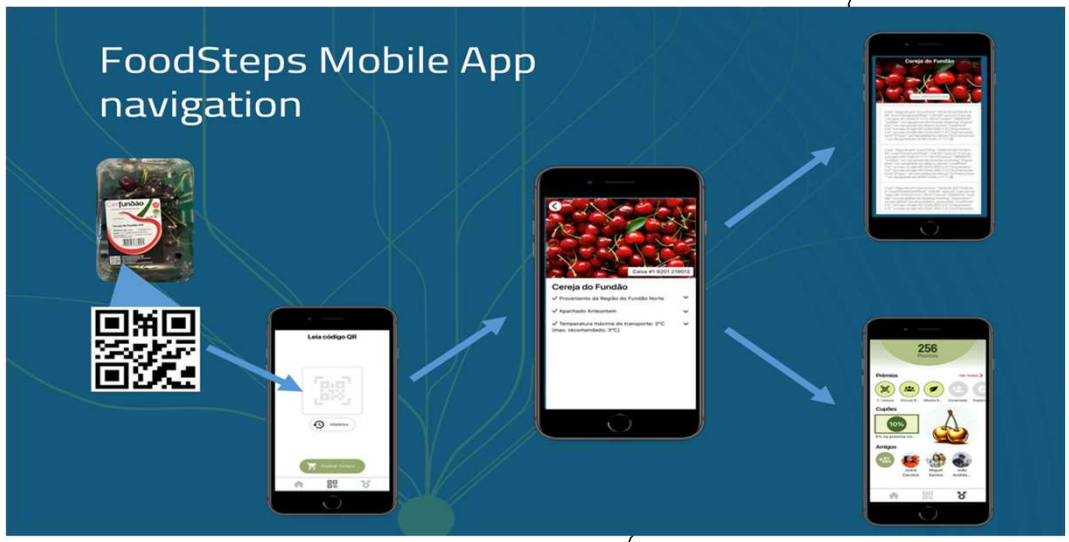


CC2C - Design Principles

- Data Confidentiality across **Channels**
- Granular Access Control
- Auditability
- Data Manipulation
- Resilience to Threats
- Scalability

Use Case: FoodSteps

- Blockchain Food-traceability system
- A solution under development for the reliable registration and sharing of information about food products
- Designed to provide trustworthy data about food traceability, ensuring transparency and integrity in the food supply chain
- Part of ongoing National Project with European Funds Agenda “Descentralizar Portugal com Blockchain”



FoodSteps - Current Challenges

- Foodsteps involves multiple organizations, and each organization has its own requirements of confidentiality.
- Each company wants to maintain control over sensitive information (quantities, margins, stocks).
- The client has access only to the information relevant to their transaction.

FoodSteps - Current Challenges

- The Cherry producers particularly impose the following requirements:
  - Data is shared only for cherries purchased by the supermarket chain, excluding shipments to other retailers;
  - Timestamps are resampled to daily granularity (date only);
  - Original source fields are aggregated and reported at the civil parish level in the region.
- Field and production data should be recorded in the factory's HLF channel.
- Sharing of information with the supermarket involves more than just granting visibility; it also requires specific **data transformations**.

Next Steps

1

- Threat modeling of the system
- Implementation on a real-world case scenario, FoodSteps
- Audit trail mechanisms to log transfers and verifiable records
- Integrity Check Module to guarantee data correctness

Slide 16

1 Add the next steps.
Samih Eisa; 06/11/2025

Blockchain PT
AGENDA DE INOVAÇÃO

Conclusion

In summary, our system enables secure and confidential exchange of information between blockchain channels, while respecting each stakeholder's privacy requirements.
At the same time, it maintains transparency by keeping every shared asset linked back to its original source, ensuring trust, integrity, and full traceability across the entire process

2 Add the conclusion

Samih Eisa; 06/11/2025

THANK YOU