SUPPLY-CHAIN SMART CONTRACT

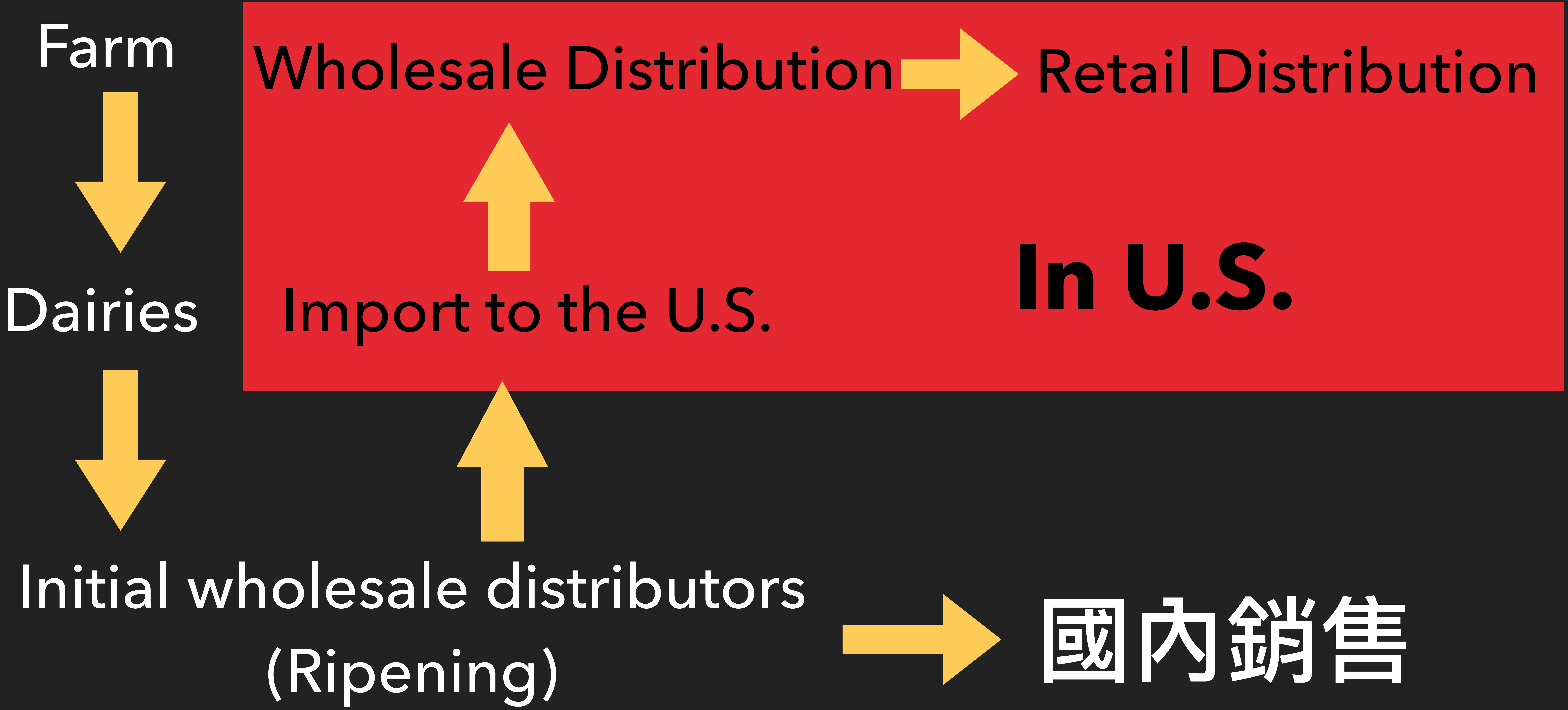
資工系大三 汪昱維

大綱

- 問題簡介
- 程式架構
- 程式DEMO

(一)問題簡介

- 帕馬森乾酪 (Parmigiano-Reggiano)生產流程：



Farm

Dairies

Initial wholesale distributors
(Ripening)

國內銷售

Import to the U.S.

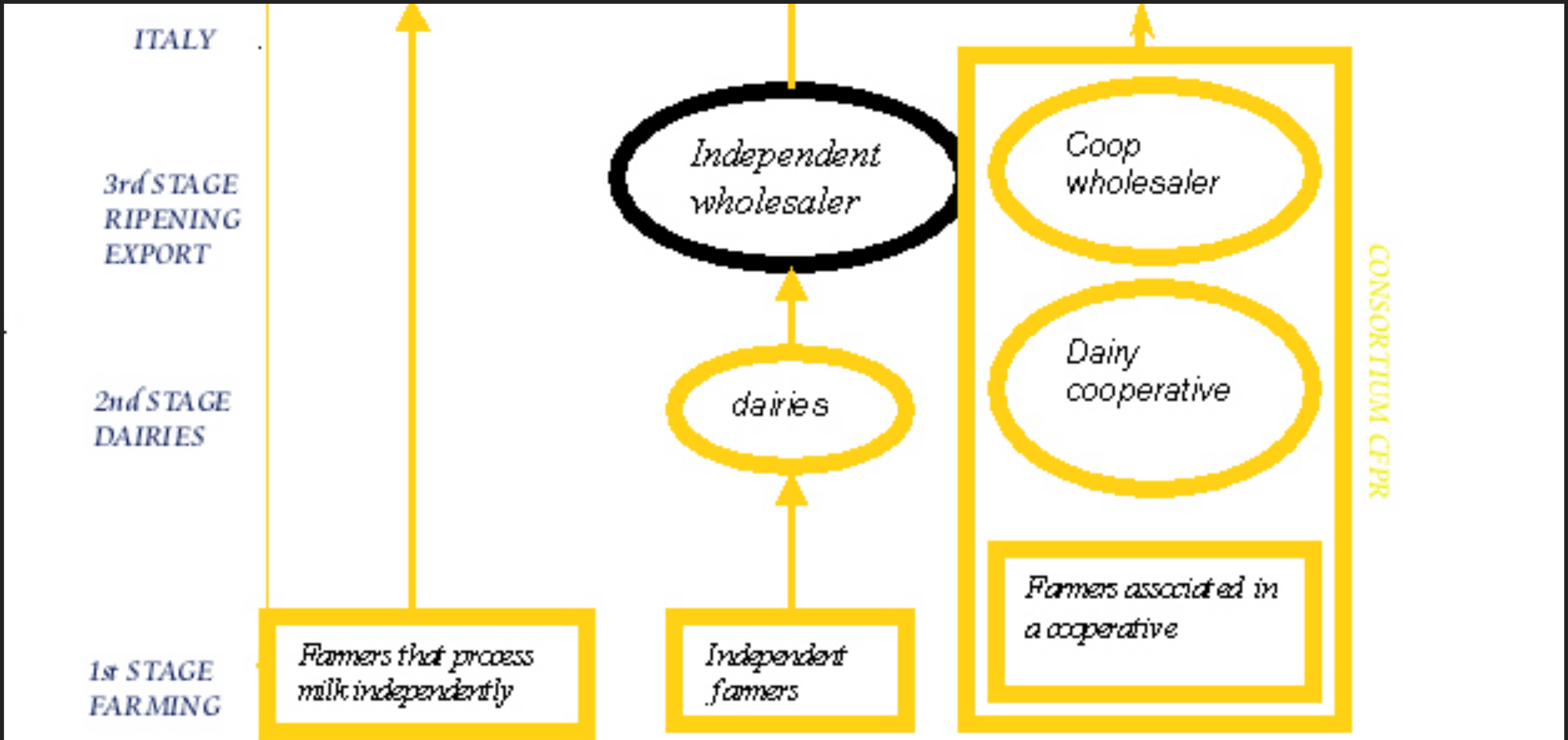
Wholesale Distribution

Retail Distribution

In U.S.

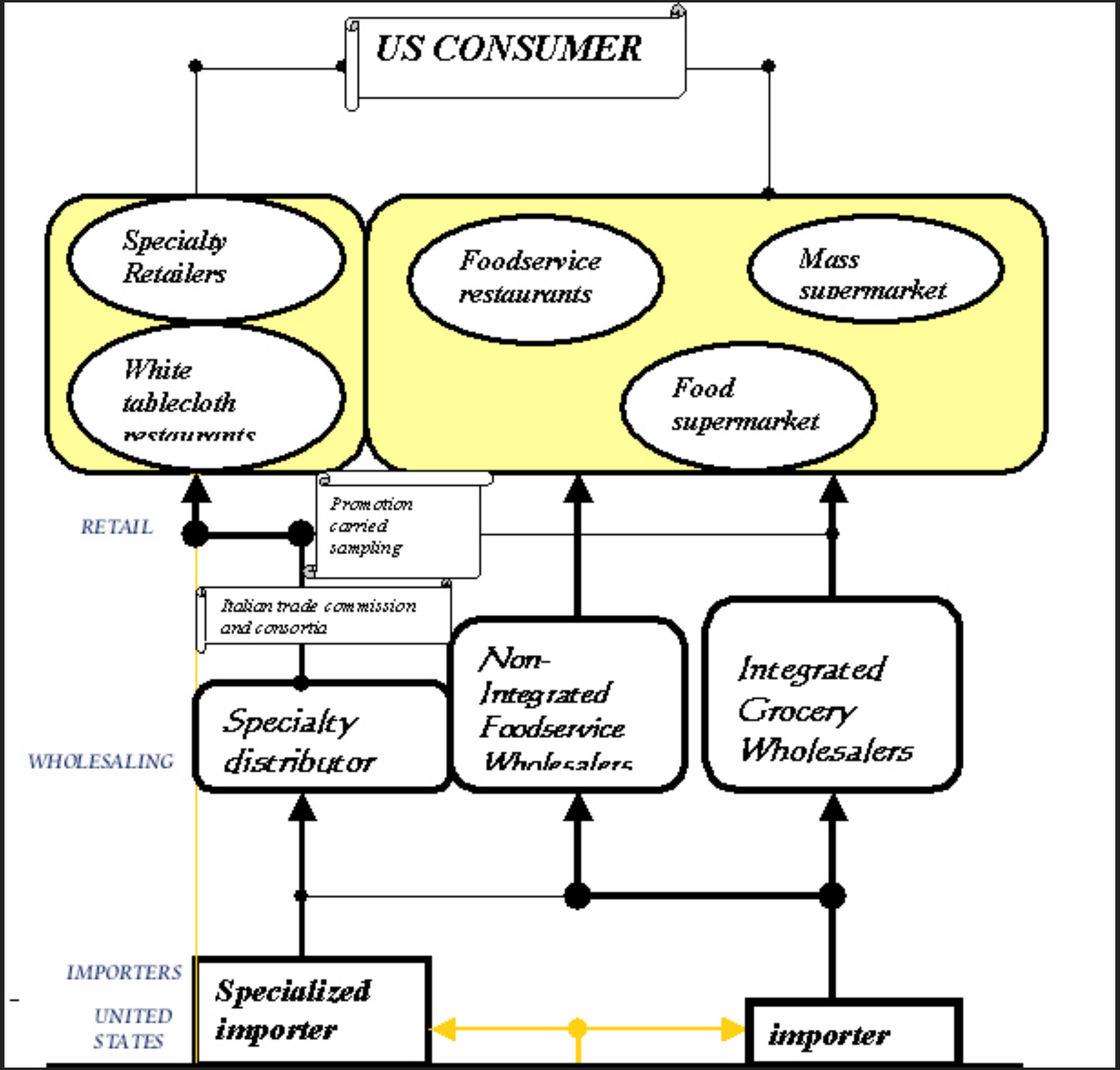
(一)問題簡介

- 帕馬森乾酪生產流程：



(一)問題簡介

- 帕馬森乾酪生產流程：



(一)問題簡介

- 問題彙整
  - 應映市價調整供應商
    ->Lottery(pickWinner)
  - 確保貨品品質符合規定（只跟符合廠商交易）
    ->事先跟特定廠商交換私鑰，並以此來在smart contract上交易
  - 不直接保存私鑰在合約上
    ->紀錄待更新的key（每筆交易都要更新）
  - Input Output 都是公開透明
    ->不直接輸入password，而是用key加密(XOR)後的樣子
  - 不綁定特定Address（同一客戶可用不同Address）
    ->用Address更新key，若是新Address不屬於該客戶，則該客戶無法再進行交易（會發現）

(二)程式架構

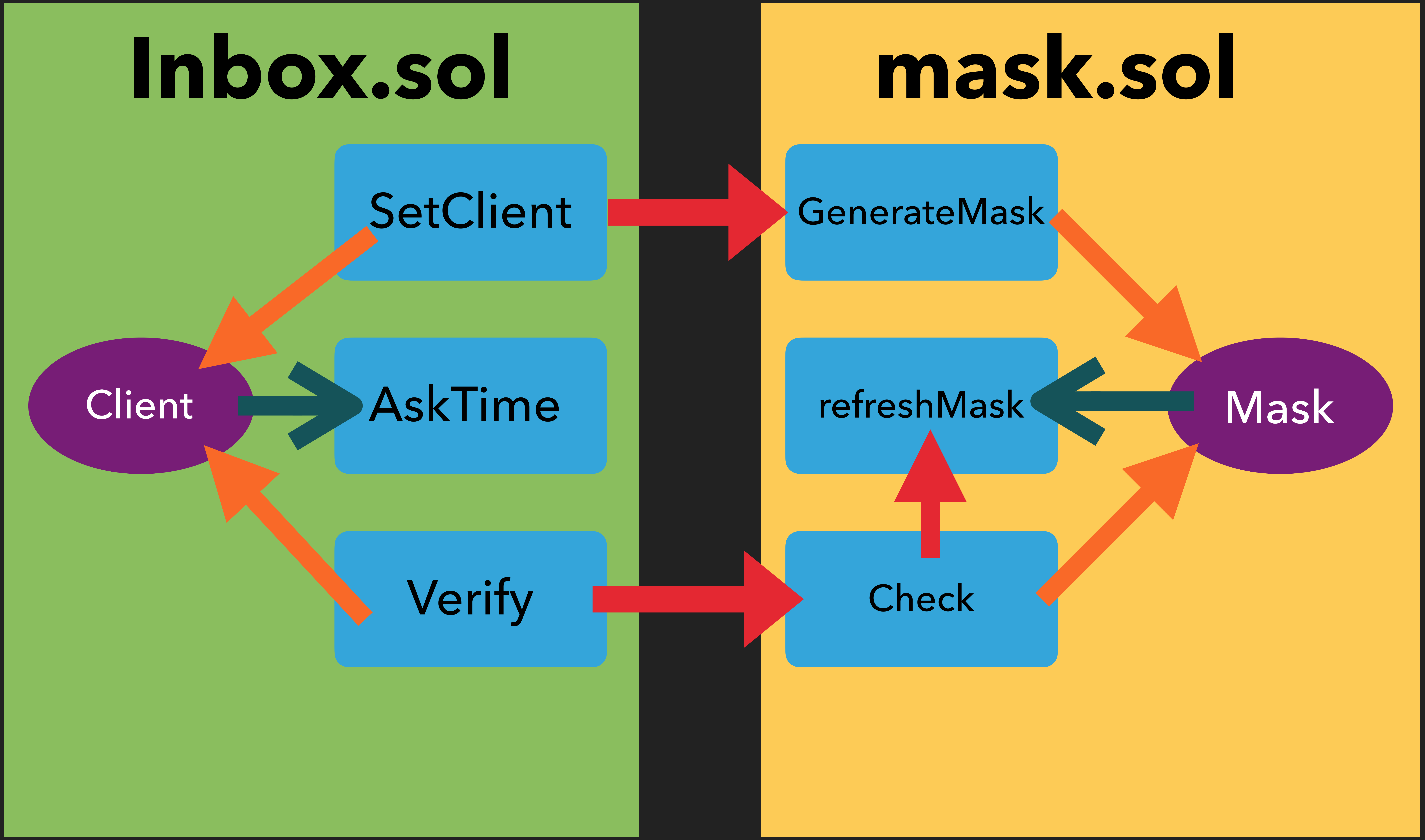
- Client:
    - password（bytes32）：Nonce–>用address更新
    - refreshTime（uint）：更新mask(私鑰)的次數
    - Account（address）：客戶最初綁定的位址
    - MaskAddress（address）：Mask(私鑰)的合約位址
    - lock（bool）：狀態紀錄

(二)程式架構

- **Inbox.sol：**
  - 設定client資料(SetClient)
  - 詢問mask更新次數(AskTime)
  - 驗證身份(Verify)

- **Mask.sol：**
  - 生成私鑰（GenerateMask)
  - 更新mask(refreshMask)
    –> hash(sha256)
  - 協助確認（Check)

(二)程式架構


Inbox.sol
mask.sol
SetClient
GenerateMask
Client
AskTime
refreshMask
Mask
Verify
Check

程式Demo

1.部署合約

2.設定Inbox的合約地址（SetAddress）

3.設定client資料(SetClient)

4.AskTime(詢問更新Key次數)

5.計算密碼

6.驗證

Q&A

REFERENCE

- THE SUPPLY CHAIN FOR PARMIGIANO-REGGIANO CHEESE IN THE UNITED STATES (Andrea Berti, Maurizio Canavari ,and Robert P. King)
- https://github.com/MitchTODO/Ethereum-SupplyChain
- https://github.com/Azure/supply-chain-smart-contracts