DEFenD

A Secure and Privacy-Preserving
Decentralized System for Freight Declaration

@

13th WORLD CUSTOMS ORGANIZATION
PICARD CONFERENCE

Matthijs Bijman

Leon Overweel

Max Pigmans

Wouter Raateland

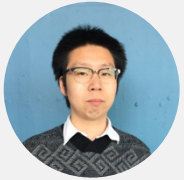
Daniël Vos

Jelle Vos

Supervision

Zekeriya Erkin

Mourad el Maouchi



Zhijie Ren

Introduction

- Millions of shipping containers move around the world every day
- Customs agencies make selection to audit
  - Usage of risk analysis
- Centralized data
  - Potentially vulnerable to manipulation and malpractice
- Privacy of operators important at all times!

Outline

- Problem statement
- Related work
- Requirements
- Our contribution
- Prototype
- Conclusion

Problem statement

Problem statement

- Customs agencies agencies receive **unverified data**…
  - Large shipping manifest
  - Problems must be traced **through 3rd party** (shipping company)
- … and must use it to make **risk analysis** decisions
  - Are there **smuggled goods** in this container?
  - Were the contents of this container **declared properly**?

→ They need **better data**

The actors

- **Customs agency:** The customs agency of a country, operating in a port of that country.
  - E.g. *Rotterdam Port Customs (Douane)*
- **Economic operator:** Any party that moves containers between countries or transfers goods in or out of containers.
  - E.g. *A.P. Moller - Maersk* and *Evergreen Marine Corp*

Related Work

Existing solutions such as ConTraffic

Problem: current solution combines **centralized** services

- Companies could **alter** the data
- **Exclude** or **mistreat** customs agencies or economic operators
- ConTraffic has to be **trusted** by all parties

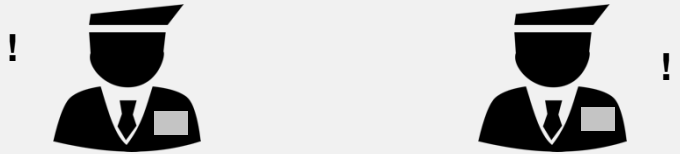
→ Centralization is not an option

Requirements

Operators trust their own country's customs agency

Assumption 1

Customs agencies do not trust customs outside their trade bloc

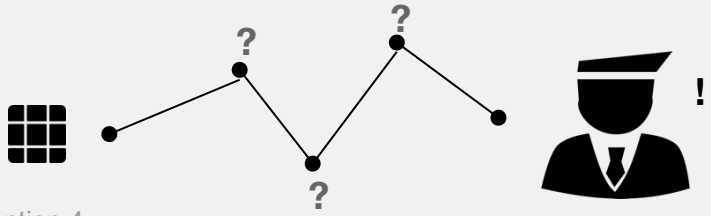


Assumption 2

Packages in the system may only move by shipping container

Assumption 3

The route packages take to their destination is unknown beforehand

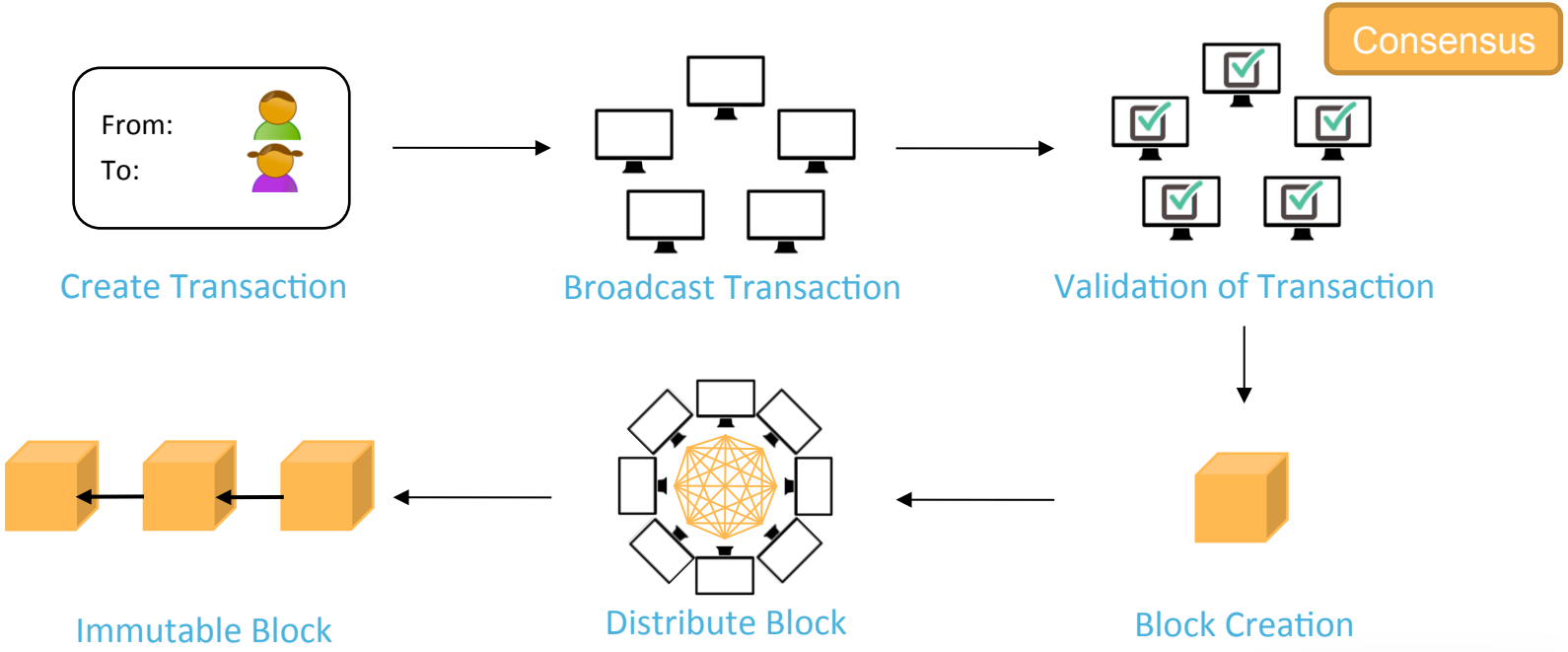


Assumption 4

Requirements

- **Customs agencies** want to be able to:
  - See data about packages and containers entering their country
  - Have control over which operators from their country can participate
- **Operators** want to:
  - Get a benefit out of sharing their data
  - Be guaranteed that their data is only seen by the appropriate customs agency

Requirements - Decentralization

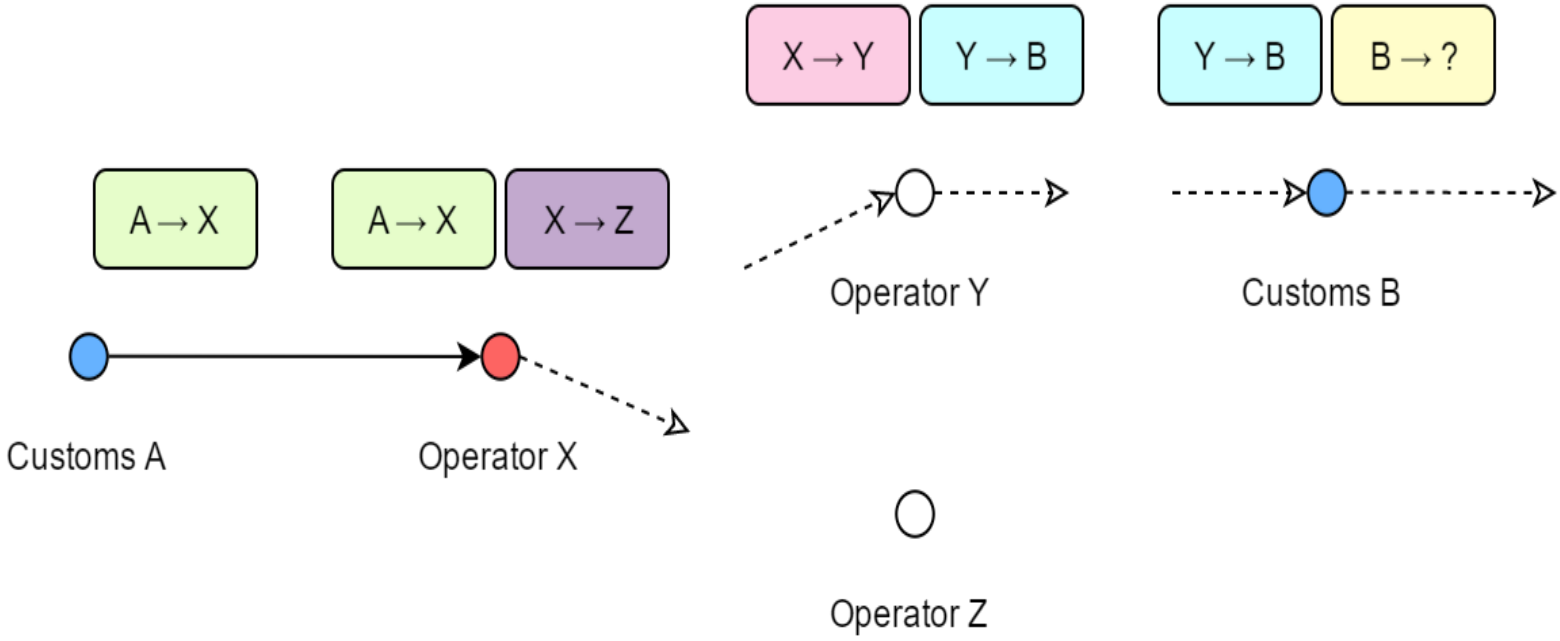


Our Contribution:
A Decentralized Protocol

Blockchain Setup

- **Operators** run nodes that can broadcast **claims** to the network
  - “I, operator A, shipped container X to operator B.”
  - “I, operator B, received container X from operator A.”
  - “I, operator C, put package Y into container X.”
- **Customs agencies** run nodes that can add claims to the blockchain

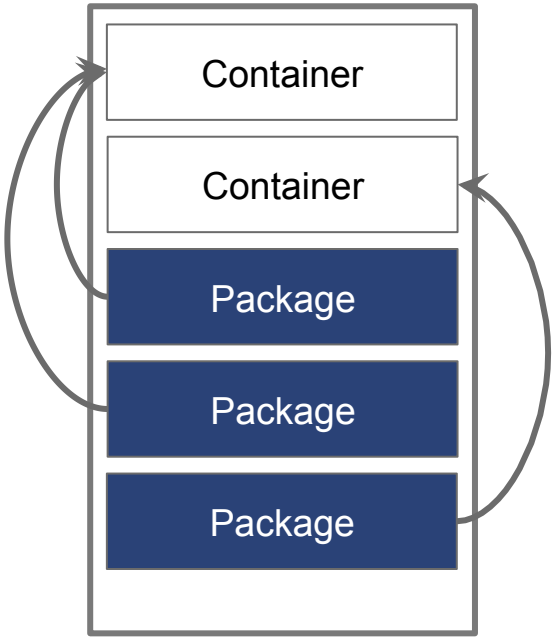
Trusted chains



Privacy on the Blockchain

- Customs agencies issue **certificates** to operators
- Operators **sign** claims they make...
  - … with the certificate issued by their customs agency
  - → Ensures non-repudiation
- Operators **encrypt** claims about **packages**…
  - … with the public key of the **final** destination customs agency
  - → Limits data visibility to appropriate customs agency
- Customs agencies decrypt claims about their country

Block format



Unencrypted

Encrypted

What about validation?

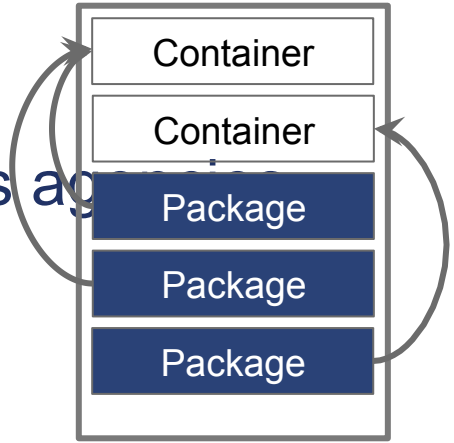
- Claims about **packages** cannot be validated…
  - Because they are encrypted, and privacy-sensitive
- … but claims about **containers** *can* be!

- Check for “double spending” containers
  - “I, operator A, shipped container X to operator B.”
  - “I, operator A, shipped container X to operator C.”

Prototype:
System Design

System Design

- **Nodes**: customs agencies & operators
- **Operators** sign and encrypt claims
- Containers move through different customs ag
- Final/destination customs agencies then…
  - Decrypt package content
  - Verify claims on packages



Blockchain Implementation Choice

- **Private, permissioned** blockchain
  - Controlled by customs agencies
- **Hyperledger…**
  - Private blockchain, permission levels
  - Large community
- **…v1.0**
  - Multiple channels, built in security features
  - Current community focus

Conclusion

Results

- Prototype shows that DEFenD is suitable for real-world application
  - Successfully demoed at **TU Delft**
- Pitched to
  - Dutch customs agency (Douane)
  - Rotterdam Port Authority
  - YES!Delft

Limitations

- Prototype limitations (Hyperledger)
  - Not enough tx/s in practice
- DEFenD requires participation of many parties to be effective
  - At least several customs agencies
  - Many operators
- No current support for opening encrypted packages by intermediary customs agencies

DEFenD

A Secure and Privacy-Preserving
Decentralized System for Freight Declaration

@

13th WORLD CUSTOMS ORGANIZATION
PICARD CONFERENCE

Requirement Analysis

Requirements:

1. Private blockchain
2. Levels of permissions
3. Java support
4. Open source
5. Custom consensus model
6. Large community, well documented

Name	1	2	3	4	5	6
Hyperledger - Fabric						
Hyperledger - Iroha						
Hyperledger - Sawtooth Lake						
Tendermint						
Ethereum						
Chain						
Kadena						
Ripple						
Symbiont Assembly						
Openchain						
MultiChain						
NaiveChain						
Quorum						

System Design