Blockchain Workshop/Conference

15 Oct 2018 - Hangzhou

A solution looking for a problem?

Steven Capell:

Enterprise Architect,

Australian Government Department of Home Affairs

steven.capell@homeaffairs.gov.au

UNECE

UN / CEFACT

Summary

Over the last year or so, the Department of Home Affairs has been experimenting with various blockchain initiatives. Sometimes as an interested observer, sometimes as a participant, and sometimes as a leader.

This presentation tells a story of lessons learned during our journey and suggests an answer to the question :

What kind of business problem is a good fit for a blockchain based solution?

Blockchain Vital Statistics

It's distributed : every node has a full copy.

- So it's a good way to share data without a central database.
- But all nodes can see the data so be careful what you put on the chain.
  - In a pubic ledger, anyone can see the ledger.
  - In a private ledger, only authorised members can see the ledger.
- Luckily, most sensitive data can be kept « off chain »

Blockchain Vital Statistics

It's verified : new transactions must be confirmed by a majority of nodes ("consensus").

- So it's a good way to enforce rules ("smart contracts") that all nodes agree to.
- But that means that all nodes must share a common problem because they all run the same verification.
- And if nodes are not independent, they could collude. So nodes must be independent for consensus to have any value.

Blockchain Vital Statistics

It's transactional : a blockchain transaction represents a change or transfer of digital assets.

- So it's a good way to track real world assets of value such as diamonds or sea containers.
- But that means you need to be tracking something of genuine value – or there's no point.
- Worth noting that the owners of the assets (eg a consignee) don't need to be node operators. But they do need to trust the network.

Blockchain Vital Statistics

It's permanent : Each new block summarises all past blocks – that's what makes it a "chain"

- It's very hard to re-write history so it's a great notary ("proof of existence").
- Unless you can take over the network…
  - For the leading public ledgers (eg bitcoin) that needs enormous computer power.
  - For private ledgers it needs the node operators to collude.
- So the more independent nodes, the higher the integrity of the network.

The Right Kind of Problem

A blockchain is a natural fit to

- **a digital asset management problem**
- **where there is a network of independent entities**
- **that share a cohesive business domain**
- **and have limited or zero trust in each other**

"Capell's first blockchain rule"

The Balancing Act

Integrity vs privacy for permissioned (i.e. “private”) ledgers:

- The more on-chain data you have, the smarter the stuff you can do with it.
- But the more on-chain data, the greater the impact of information leakage
- Also, useful blockchain network must have multiple independent nodes – or there’s no integrity.
- But the more independent nodes, the more the likelihood that your ledger will become public.

The Balancing Act

Assume your permissioned ledger on-chain data is public and design your off-chain security model accordingly.

Because if you are sure it's all safe then you probably aren't running a really useful blockchain network.

"Capell's second blockchain rule"

The Balancing Act?

How can there be a “leader” among equals?:

- In a public ledger, anyone can run a node and participate in consensus.
- In a private ledger, you need to be invited by the “owner” of the network.
- But if all nodes are equal then how do you pick an owner?
- You need a trusted and auditable governance model to add / remove nodes.
- Like the bishop of the church. Or, more realistically, like an industry association or peak body.

The Leader of the Club?

Membership governance for your permissioned ledger "club" should ideally match the membership governance in your real world club.

Or you probably won't trust it.

"Capell's third blockchain rule"

Use Case: Certificates of Origin

A Certificate of Origin (CoO) is a document issued by an accredited organisation (usually Chambers of Commerce) that asserts that the goods in a specific shipment comply with the terms of a free trade agreement (FTA). Most FTA require that a CoO must accompany every shipment in order to claim a reduced duty rate. At present most CoO are paper documents that are slow and expensive to produce, presenting a non-tariff barrier to exporters.

Electronically verifiable digital origin evidence will help streamline the process, reduce costs, and reduce compliance issues at the border.

Although initially focussed on FTA exports from Australia any good solution should be scalable to support;

- Other certificate types – such as the phytosanitary certificate for agricultural goods
- Other countries and their FTAs, whether with Australia or any other country.
- Other origin compliance processes such as Declarations of Origin.

Digital CoO Challenges

- Multiple countries must agree. Always a challenge! So minimise what they need to agree to by maximising their autonomy.
- Importing country needs to trust certificate issuers in exporting country. That's hard! Better if the importing government only needs to trust the exporting government.
- Governments "sorta" trust each other. But not much really. Better if there was an auditable way for countries to "keep each other honest".
- Certificates are specific to a single shipment and a specific FTA and cannot be re-used. So there needs to be a way to transfer and acquit a certificate like a digital asset.
- FTAs may specify a language for CoOs. But customs officials in various countries are most likely not multi-lingual. An ideal solution would let each country deploy user interfaces in their local language.
- National data sovereignty rules that will usually require the CoOs to be physically hosted in the exporting country. But the importing country still needs to discover and access them.
- Funding models for centralised solutions are notoriously difficult to achieve. Therefore, the ideal solution would be a distributed system that not require any shared infrastructure.
- Although an FTA is an agreement between two governments, the implementation must recognise that some countries are divided into relatively autonomous provinces that may separately issue and assess CoOs.

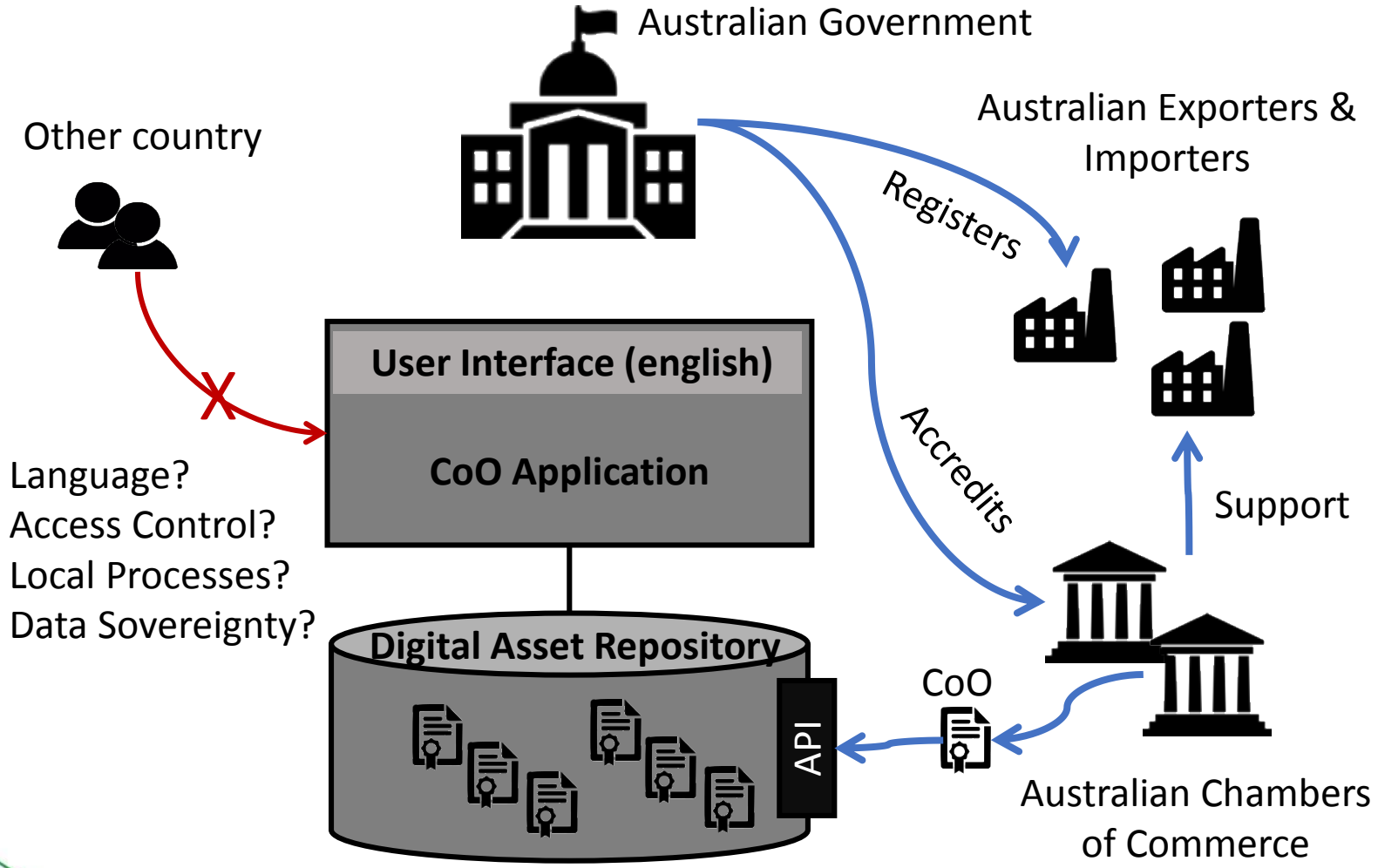
Sounds Like a Blockchain?

All those challenges (ie problems) sound a bit like a blockchain might be a good fit!

Lets see if we can design a solution that meets all requirements and also complies with Capell's blockchain rules!

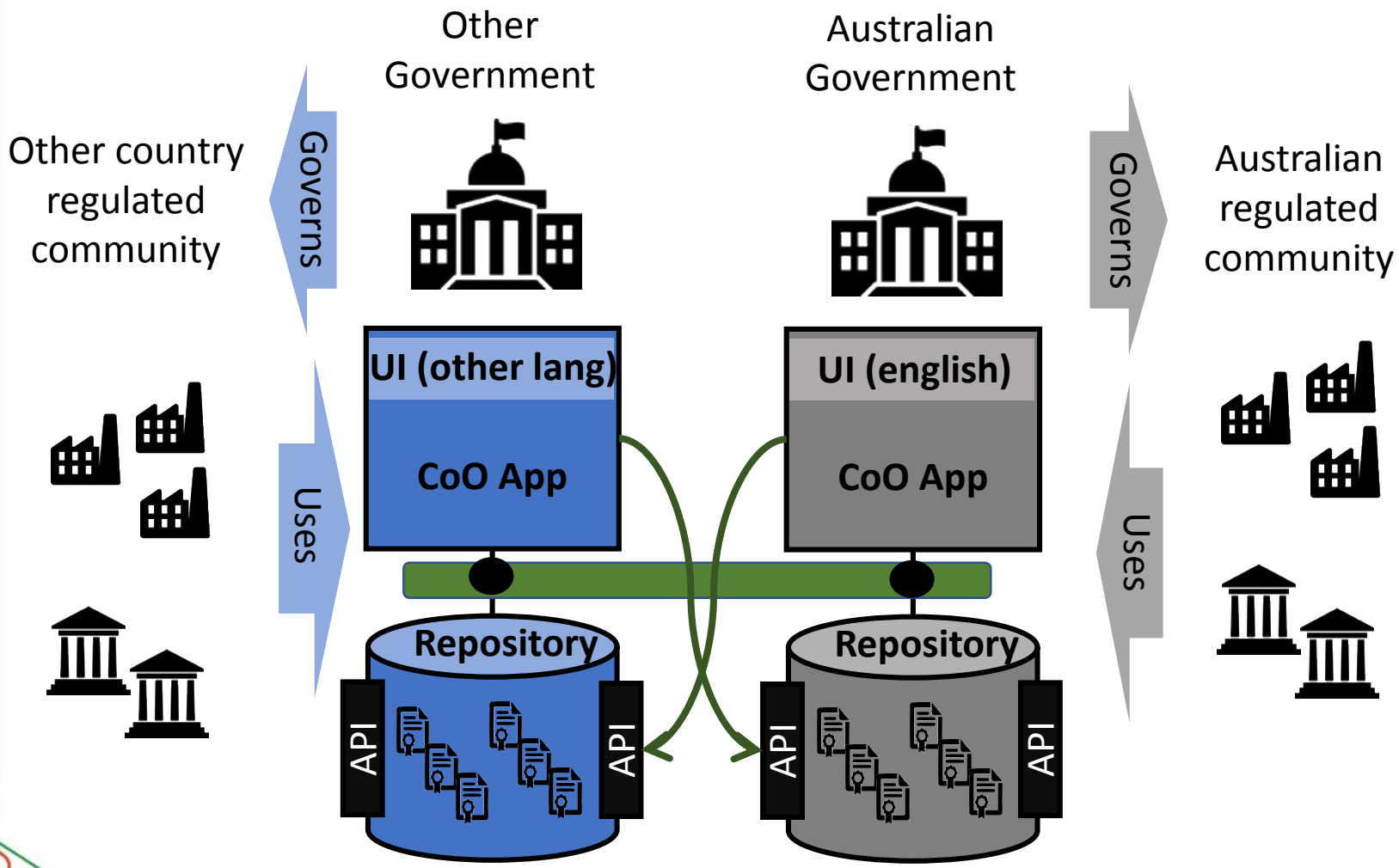
The Inter-Customs Ledger

A National CoO Solution



The Inter-Customs Ledger

A Bilateral CoO solution with some blockchain magic



UN / CEFACT

The Inter-Customs Ledger

Just 2 things to agree (and lets make them UN/CEFACT standards?):

On Chain Data

Transaction type = “CoO”

Transaction hash = “kfESTOv24o31skyXUrhGXTD+j1kZ6FAvLlqCOu1Yhh4=”

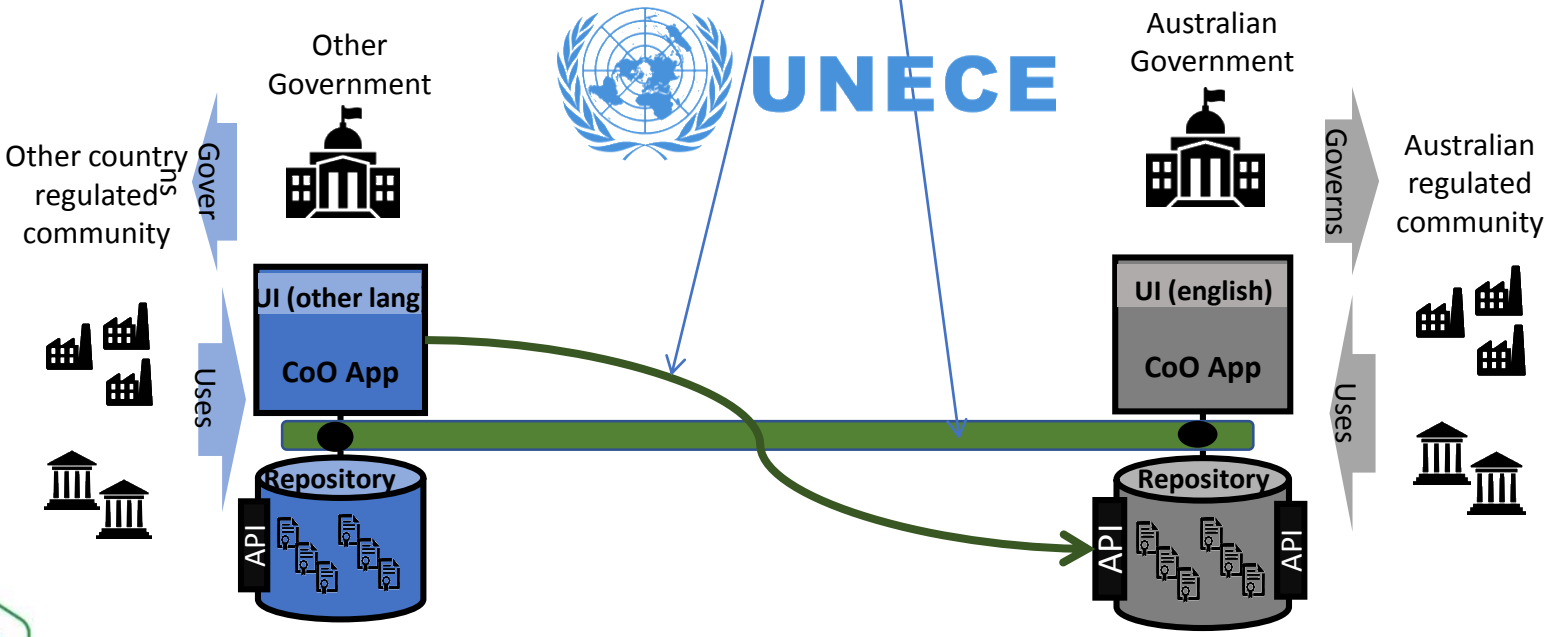
Exporting Jurisdiction = “AU”

Importing Jurisdiction = “CN”

Status = “New”

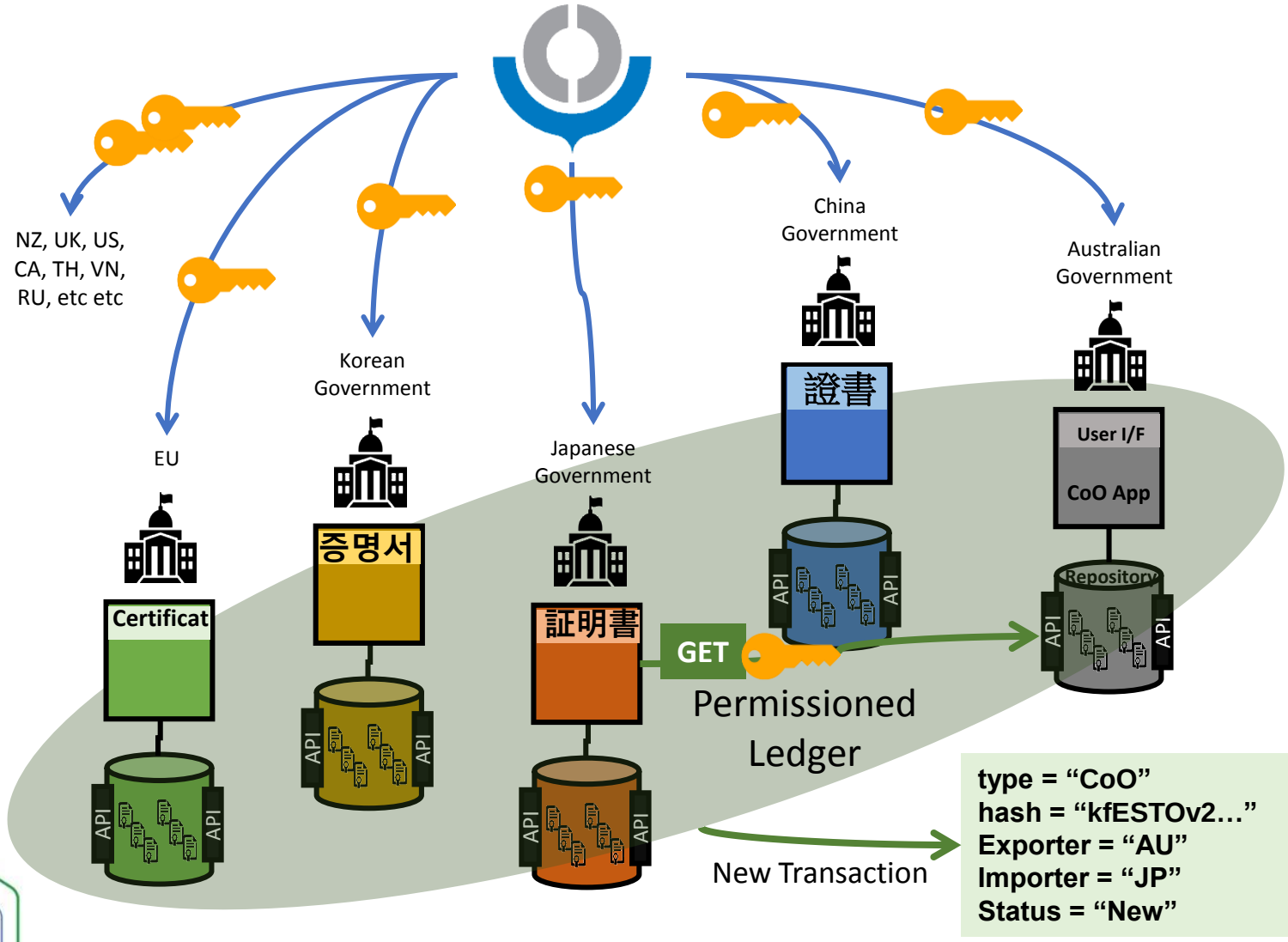
Repository API

GET repository.gov.au/digitalassets/kfESTOv24o31skyXUrhGXTD+j1kZ6FAvLlqCOu1Yhh4=



The Inter-Customs Ledger

A multilateral CoO sharing solution



The Inter-Customs Ledger

Does it meet requirements?

Requirement	Met?
Maximise autonomy	Yes
Each jurisdiction manages their own community	Yes
Auditable transactions drive trust	Yes
CoO can be transferred & acquitted	Yes
Localised languages	Yes
National hosting supports data sovereignty	Yes
No central funding needed	Yes
National or provincial implementation feasible	Yes
Scalable to any bilateral or multilateral trade	Yes
Scalable to other certificate types (eg ePhyto)	Yes

The Inter-Customs Ledger

What about Capell's rules?

Rule	Met?
Is it a digital asset management problem?	Yes
Is there a network of independent entities?	Yes
Is it a cohesive business domain?	Yes
Do entities have limited or zero trust in each other?	Yes
Is on-chain data ok to be public?	Yes*
Is there a matching real world governance model?	Yes

**** What are your views? Is the on-chain data ok to be public?***

The Inter-Customs Ledger

Status of the project?:

- We have a design idea and some funding.
- We would like to build a free open source reference implementation that any other jurisdictions can take and customise as required.
- We'd like to contribute the blockchain specification and API specifications to UN/CEFACT.
- We hope that WCO would like to do membership management (ie key management).
- But we need one or two other FTA countries to agree to give it a try because it wont work with just us.
- This is a **very informal**, no commitment, invitation to have a chat.

Thank you

Q&A

Steven Capell:

Enterprise Architect,

Australian Government Department of Home Affairs

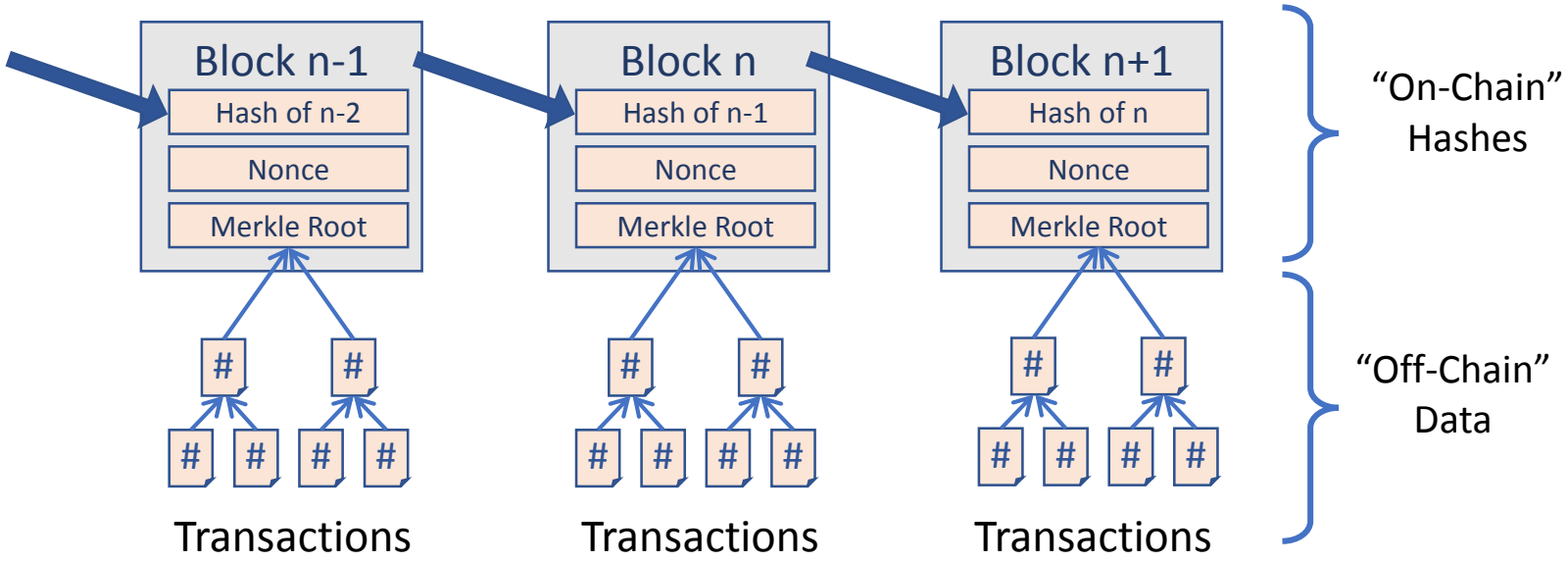
steven.capell@homeaffairs.gov.au

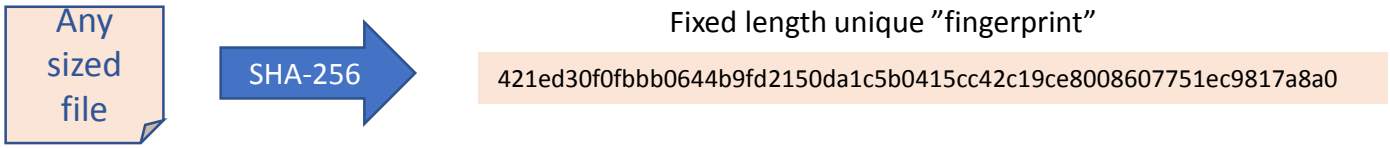
UNECE

UN / CEFACT

What's a Blockchain?

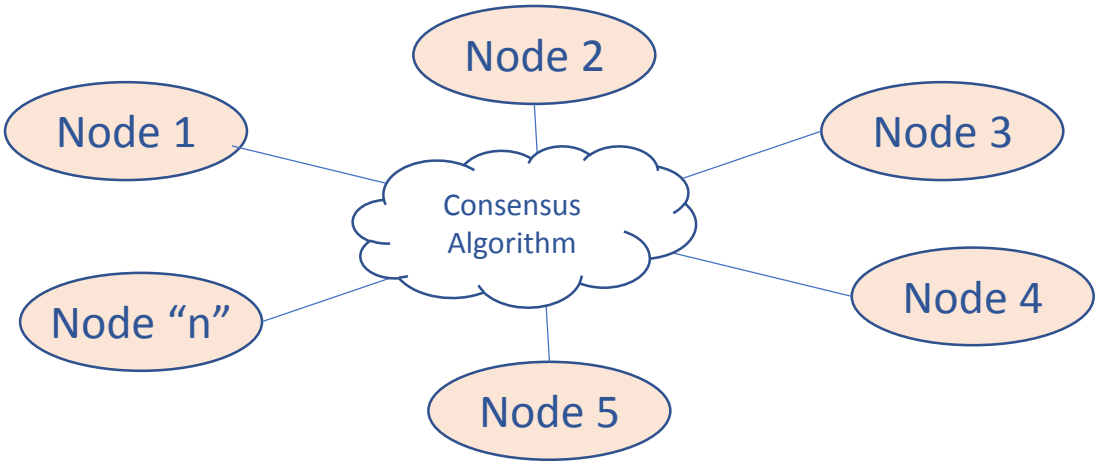
- The actual data is not on the chain. Only the hashes (fingerprints) that verify the data.





Consensus and Trust

- It's a "distributed ledger" because each node has a full copy of the chain – kept aligned by the consensus algorithm.
- Trust is ensured because each node operator can check on every other node operator.



Two kinds of blockchain

Public Ledgers – low bandwidth, very hard to compromise

- Bitcoin – you'd need more compute power than 50% of world miners. But very low bandwith and very simple transactions.
- Ethereum – not quite as valuable. Slightly higher bandwith. Complex "turing complete" transactions.

A bit like the internet

Private Ledgers – high bandwidth, variable trust

- "Hyperledger" is an open standard. Sawtooth is an open source implementation.
- There are others more focused on finance & currencies.
- Most global trade digitisation platforms are private ledgers.
- Trust depends on number of nodes and who is participating in consensus.

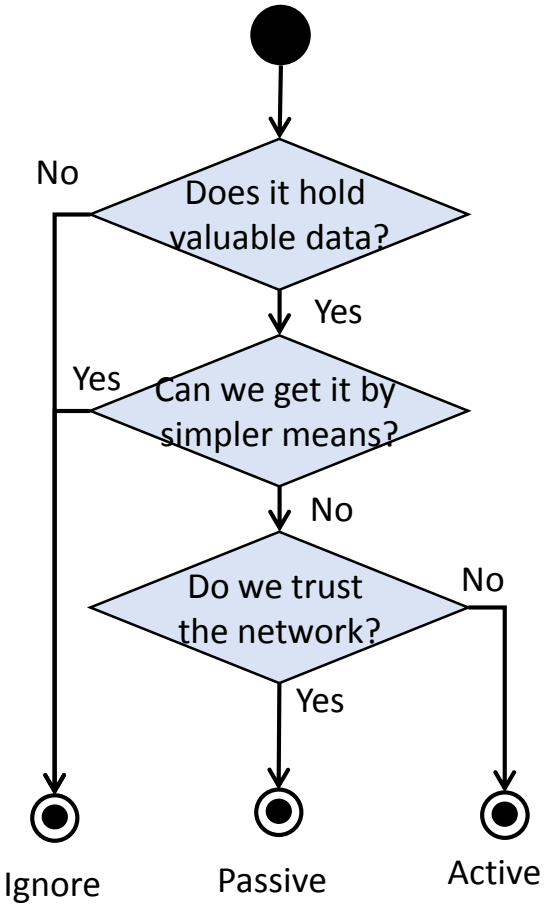
More like a corporate intranet

UNECE

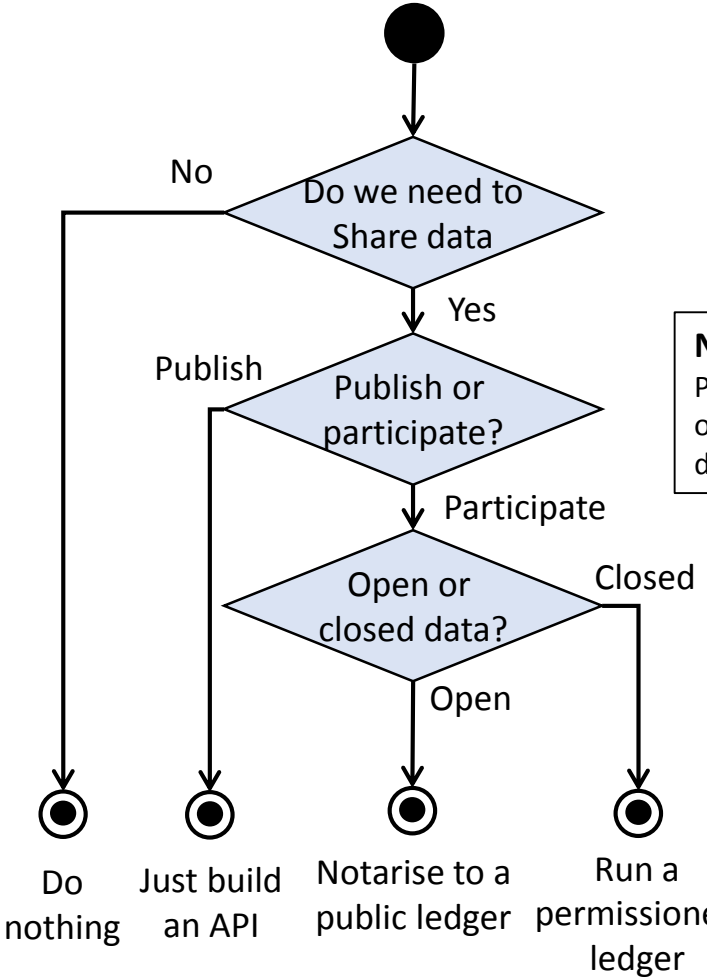
UN / CEFACT

A blockchain decision tree

When to participate in a chain?



When to lead / build a chain?



Note
Proof can be open even if data is private

UNECE

UN / CEFACT