

# Blockchain Workshop/Conference

26 April 2018

## Inter-Blockchain Interoperability - A discussion -

Steve Capell: Enterprise Architect, AU Dept of Home Affairs



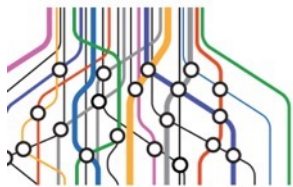
UN / CEFACT





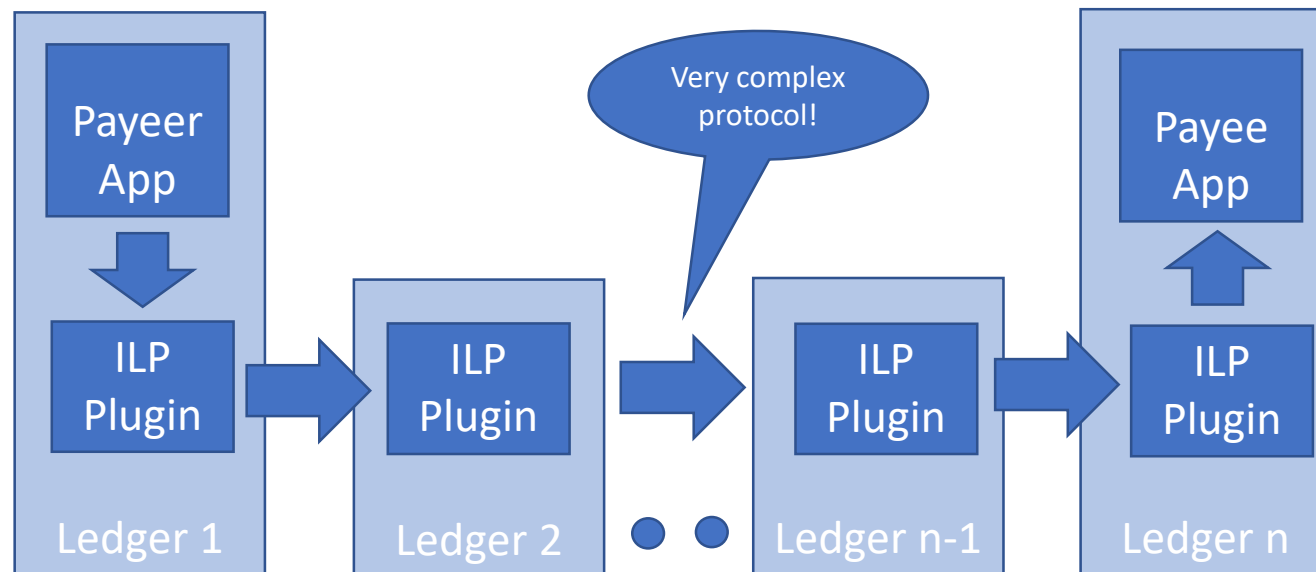
# Why does this matter?

- There's already over 200 blockchain projects around the world, many related to the international supply chain in some way.
- Even a single consignment is likely to touch multiple ledgers.
  - Some focussed on finance
  - Some on goods provenance
  - Some on transport logistics
  - Some on compliance & certification
- In their rush to dominate their sector, most blockchain projects don't even think about standards.
- So a profusion of non-interoperable platforms seems highly likely!
- So, what should UN/CEFACT do about this?



# There are already inter-ledger specs!

- Interledger.org supports payments across cryptocurrencies. The pattern looks like this:



Bitcoin



Ripple

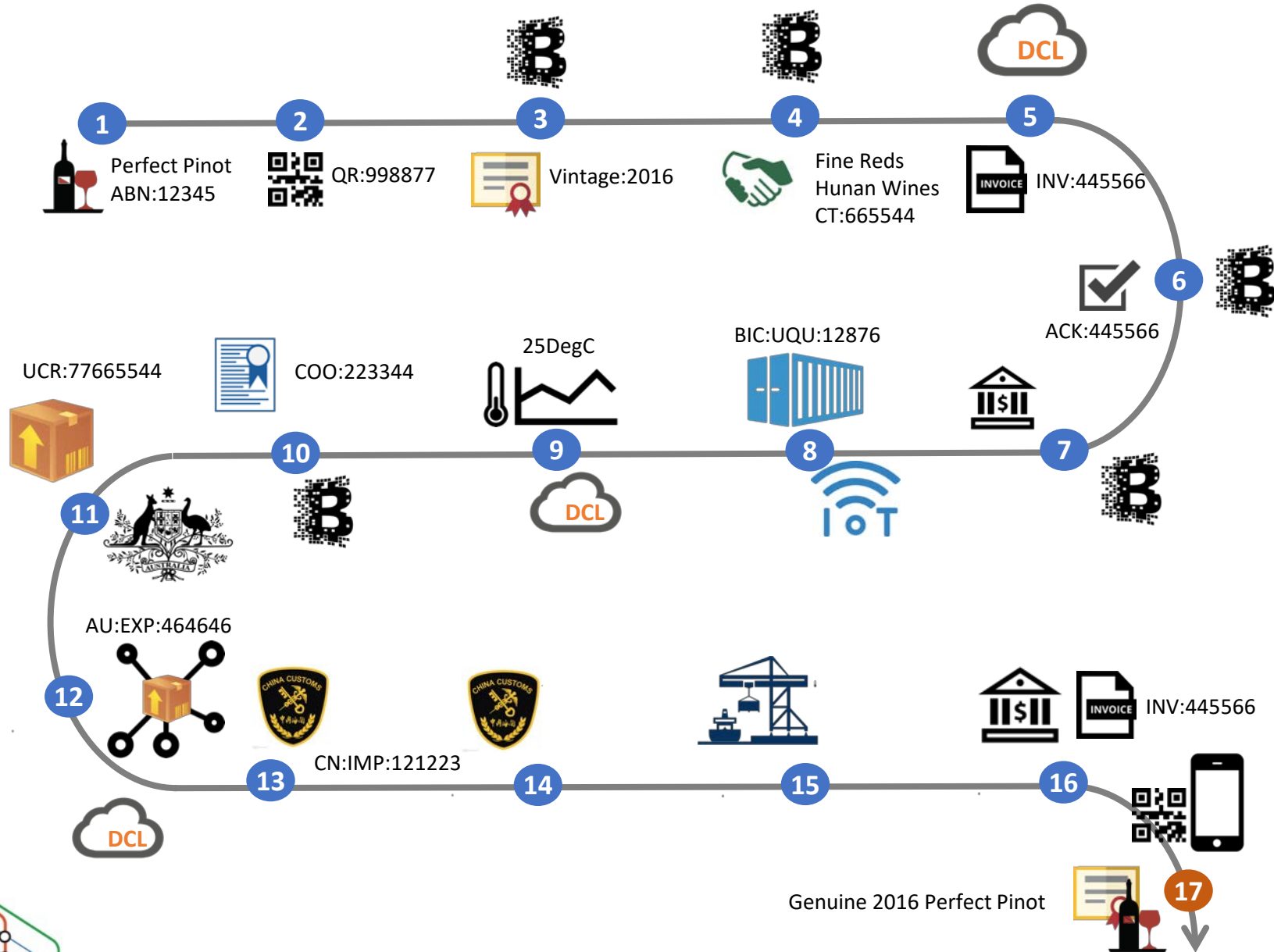


Ethereum



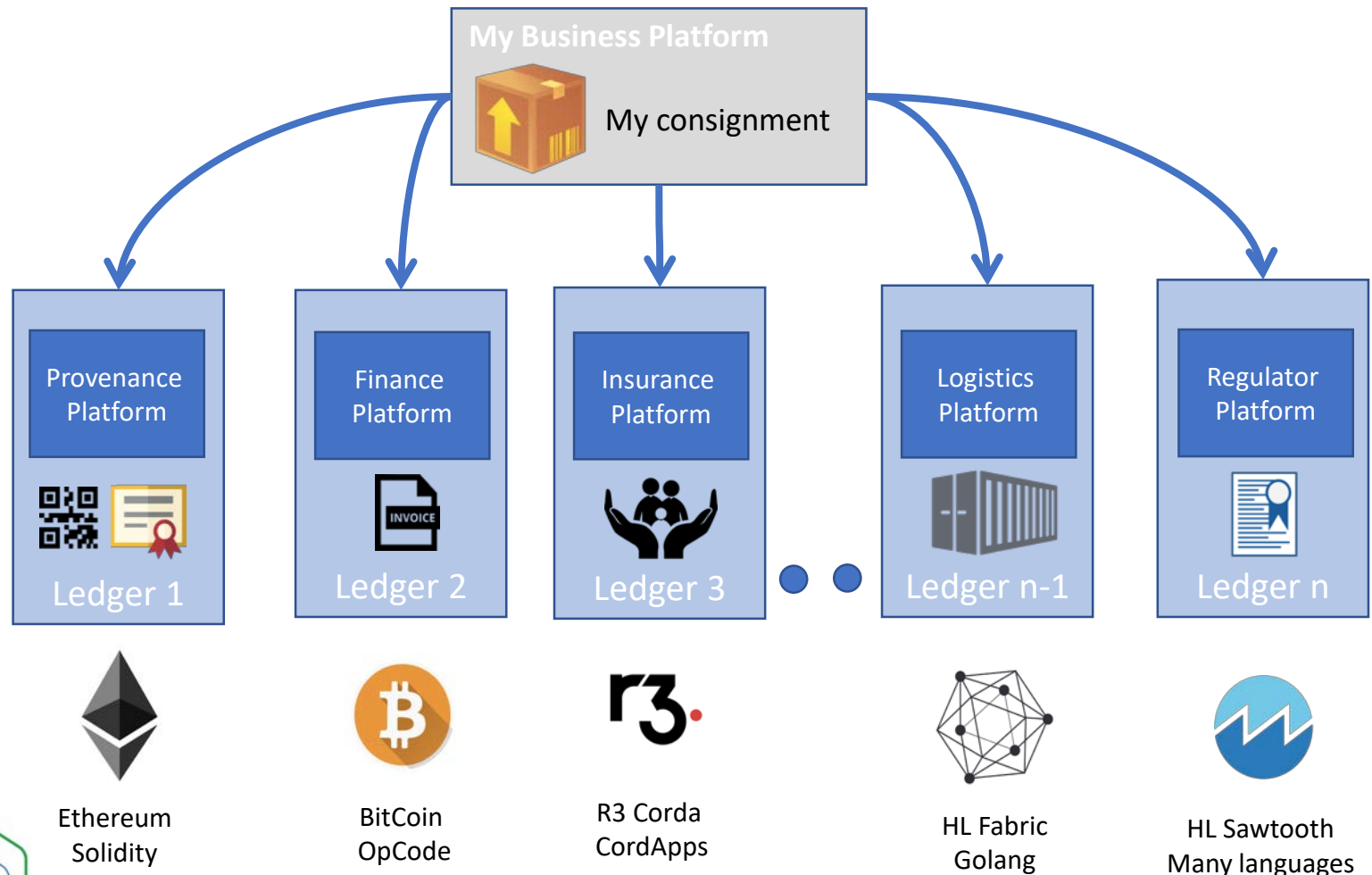
Litecoin

# But – Remember this Scenario?



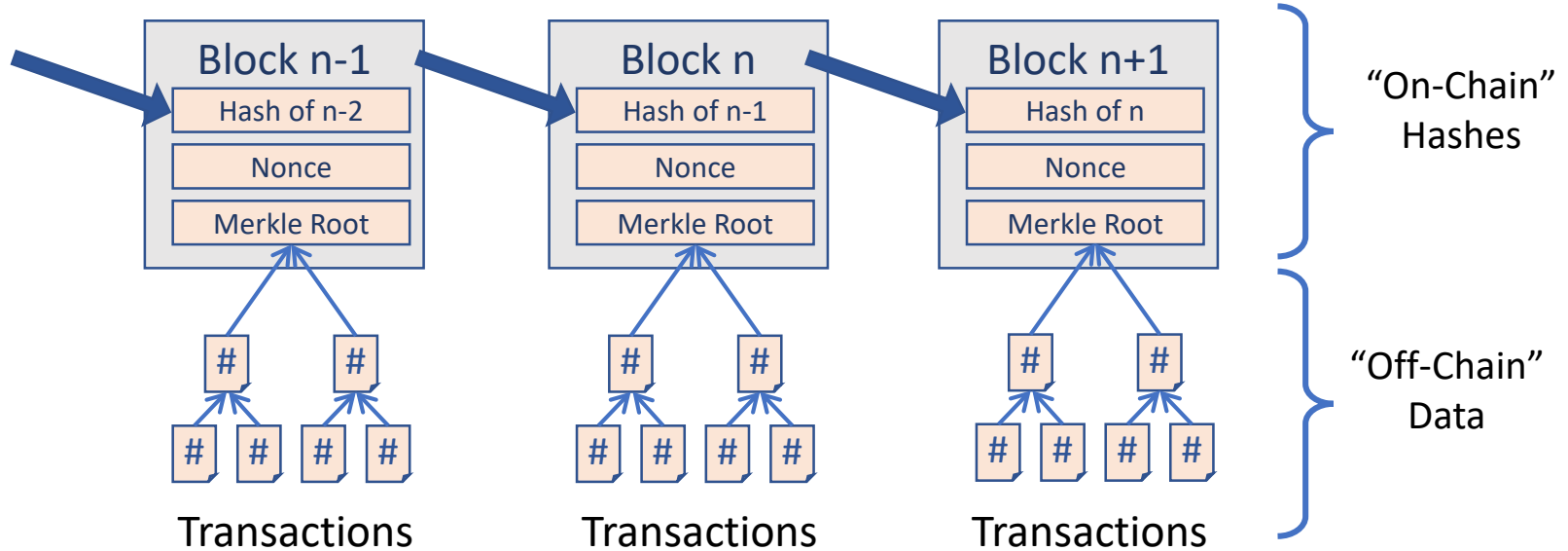
# It's a different pattern

- International Trade's main use of blockchain is NOT cryptocurrency payments. It looks more like this:



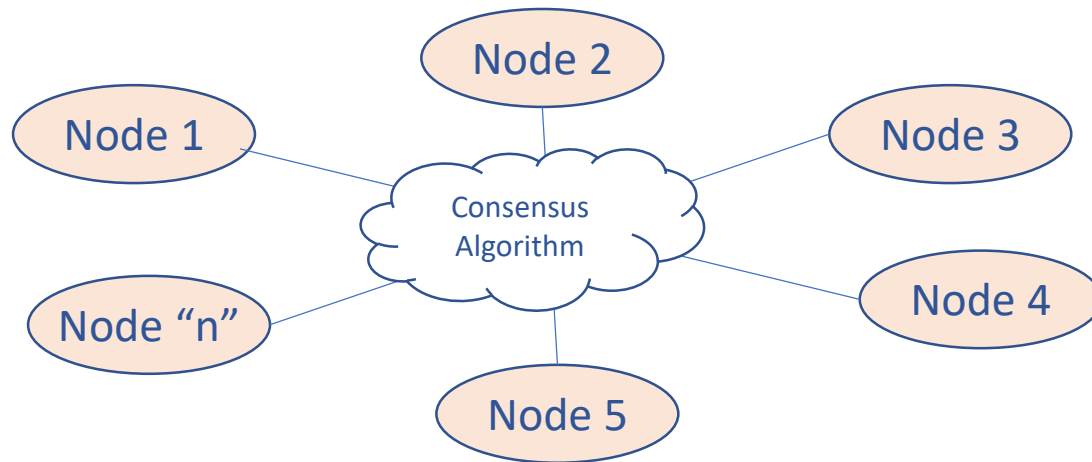
# Some Quick Revision!

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



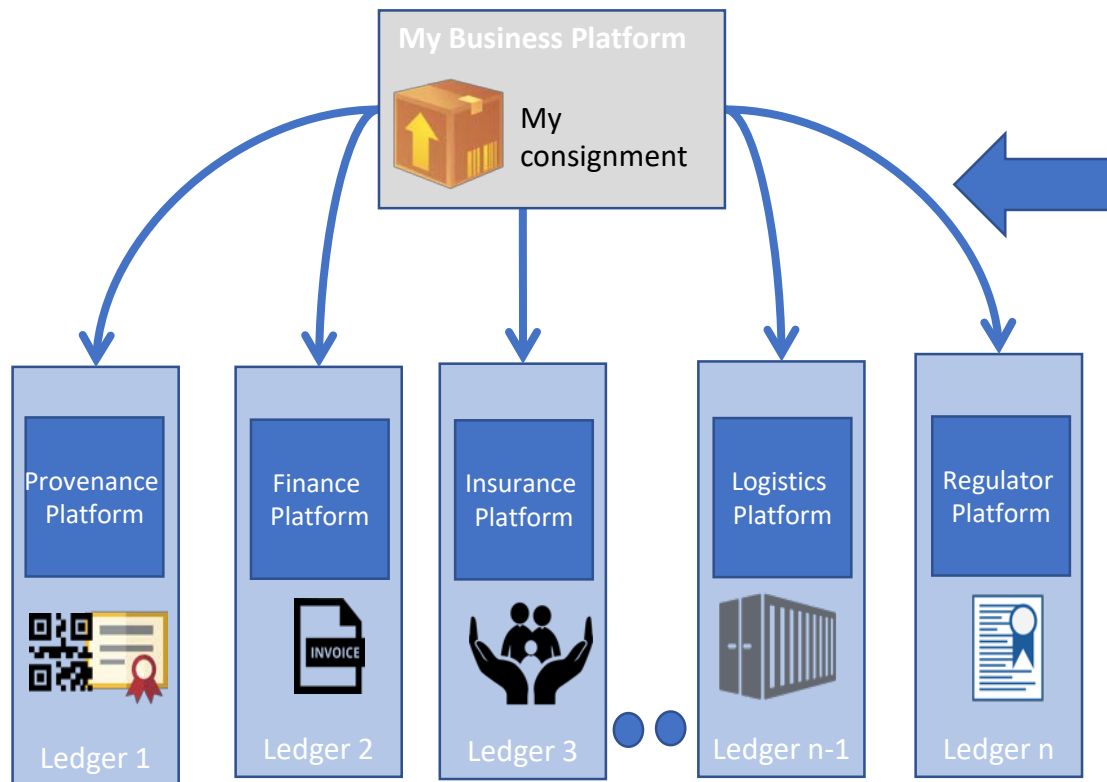
# Some Quick Revision!

- 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.





# So, back to our supply-chain model



This bit is just the data and could follow existing UN/CEFACT standards

This bit is where blockchain node operators run consensus and check on each other. You can't verify unless you host a node! (don't need to participate in consensus).

UN / CEFACT



Ethereum  
Solidity



BitCoin  
OpCode



R3 Corda  
CordApps



HL Fabric  
Golang



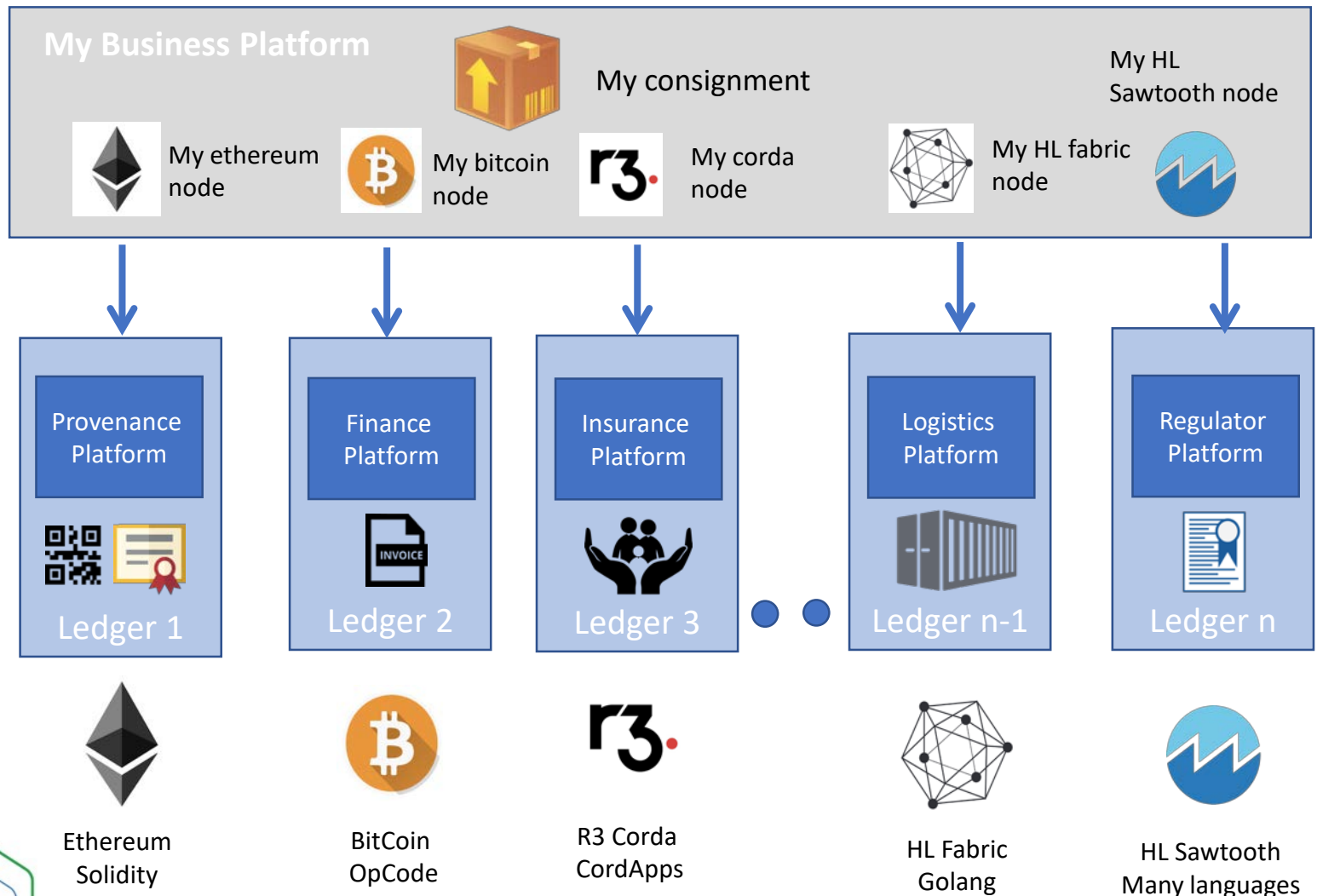
HL Sawtooth  
Many languages





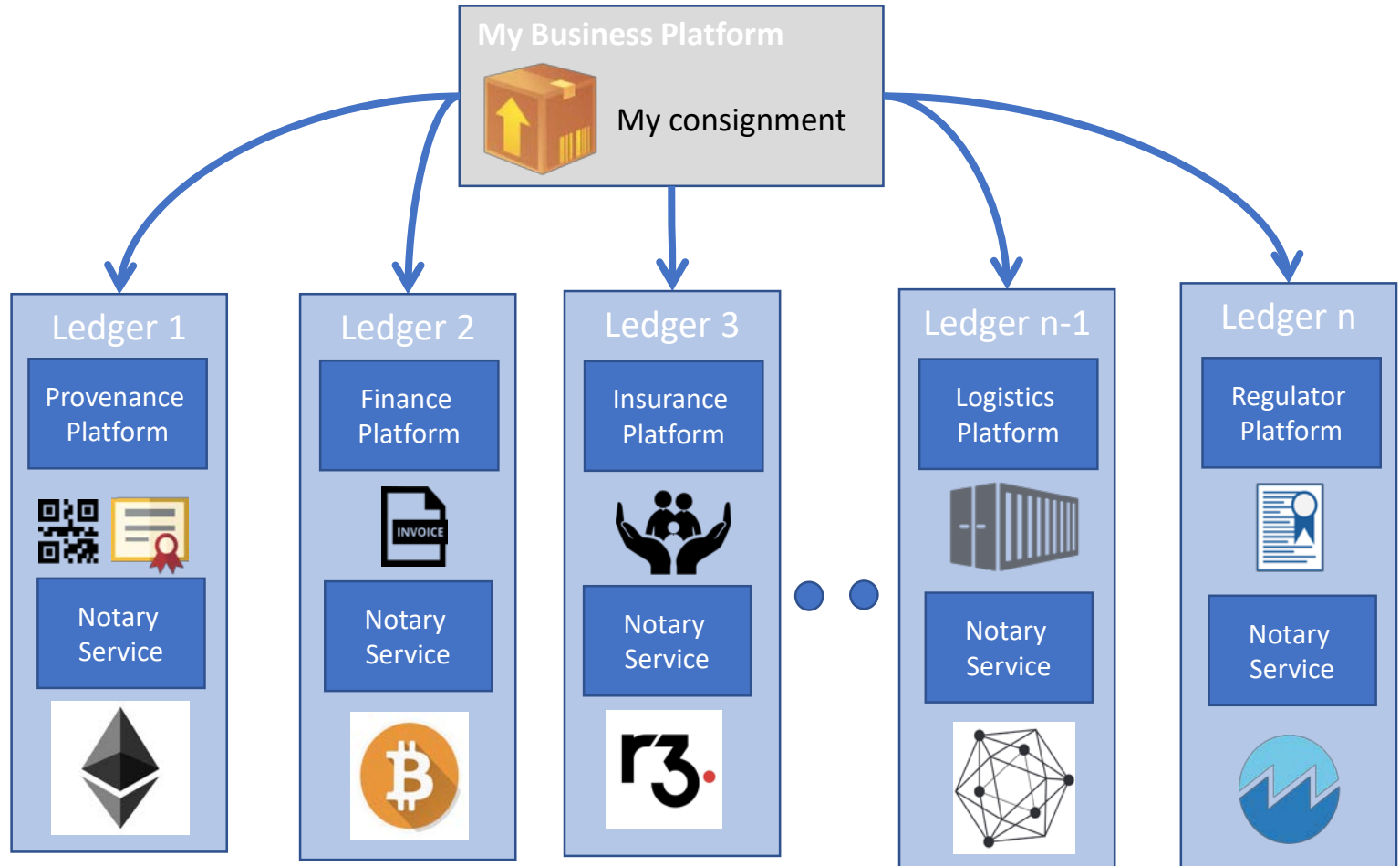
# But that means you'd have to do this

- Which is not a practical proposition!



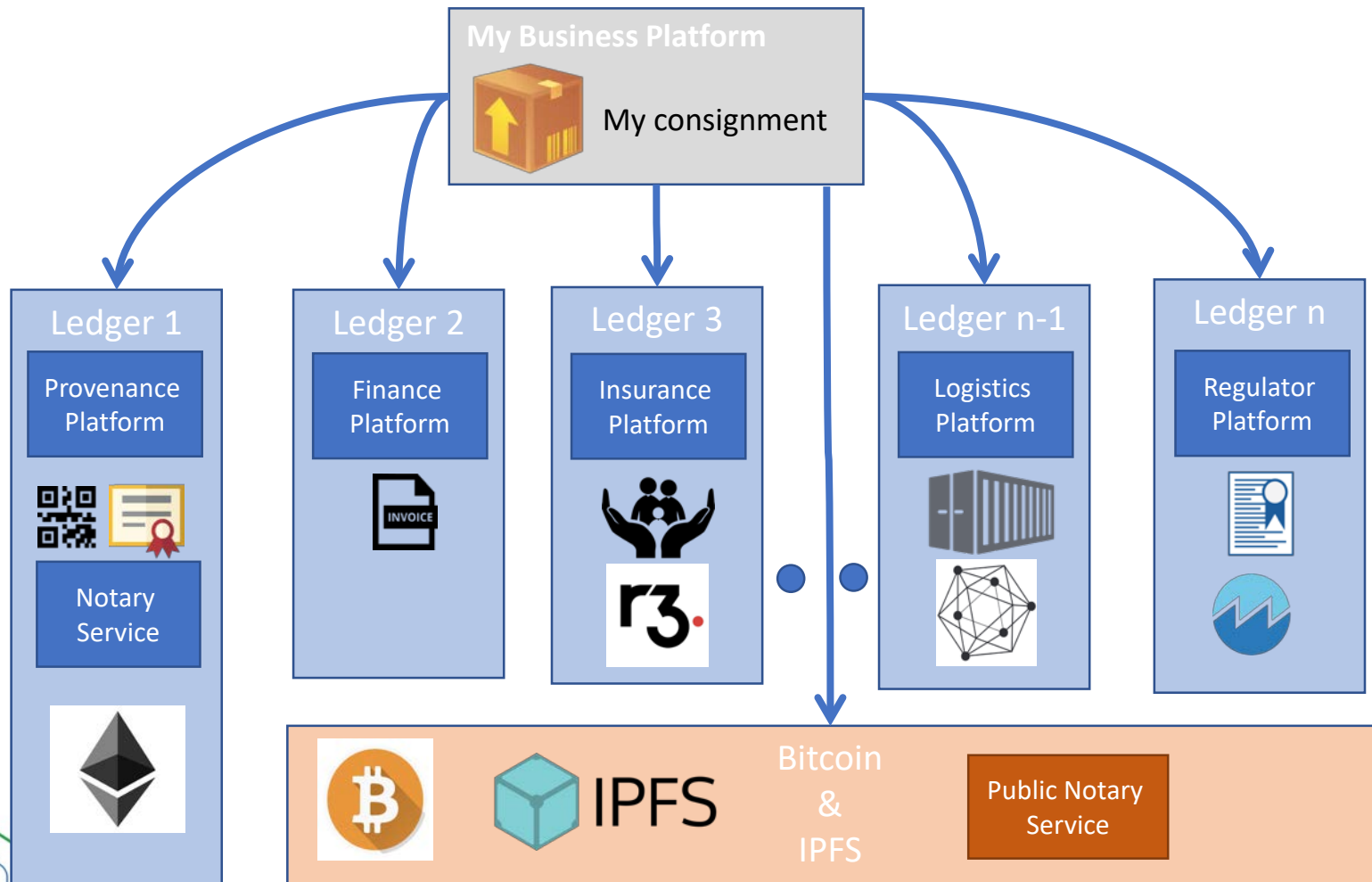
# Unless...

- There was a standard way to notarise / verify a transaction, irrespective of the blockchain network.

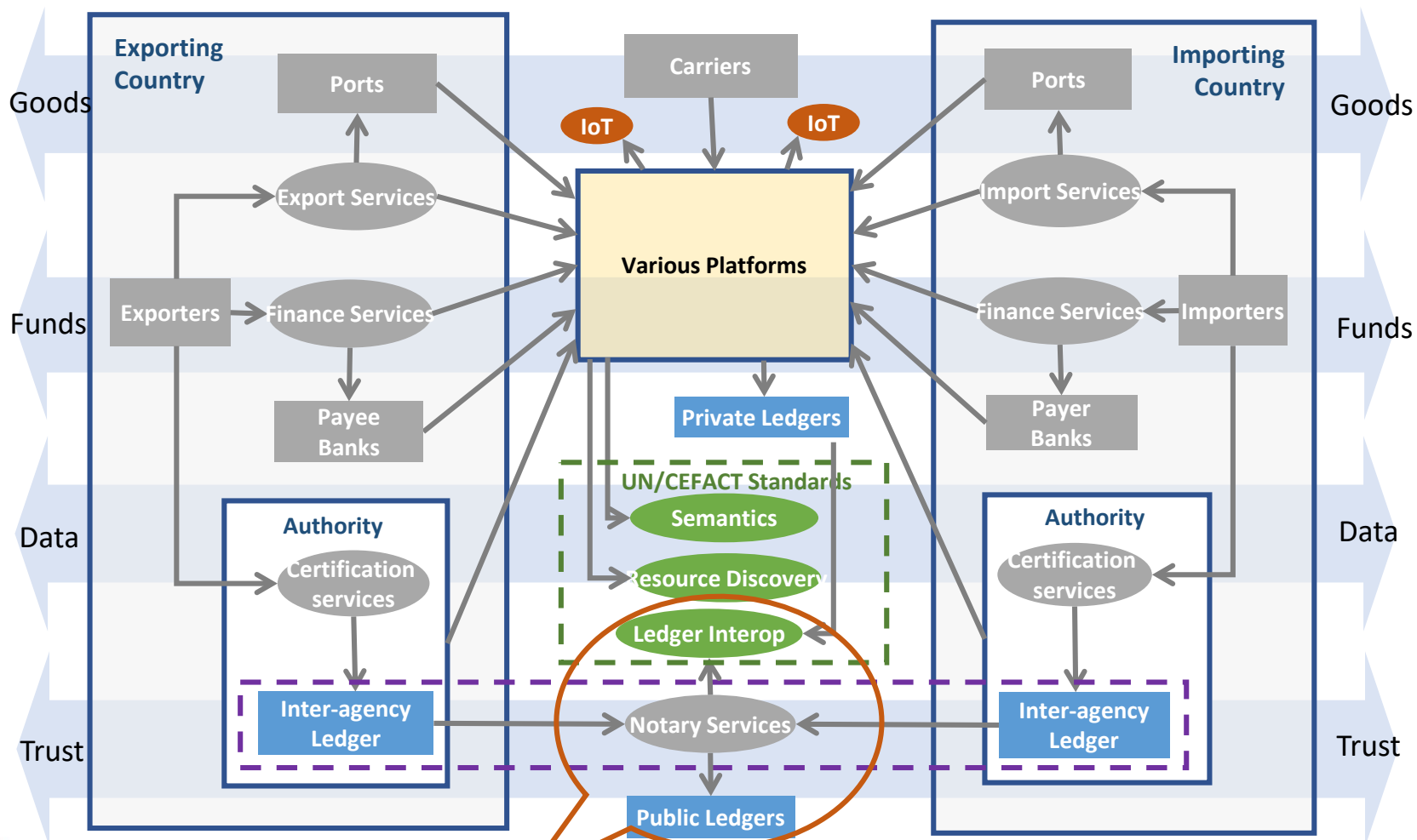


# Better, but there's still a problem

- Some “private ledgers” are not very trustworthy.  
Better an independent notary using a public ledger:



# Which is why this is in the whitepaper:



UN/CEFACT Ledger Interop / Notary Specification

Thank you – now lets  
discuss!

[steven.capell@homeaffairs.gov.au](mailto:steven.capell@homeaffairs.gov.au)

A graphic consisting of a dense bundle of vertical lines in various colors (blue, green, yellow, orange, red, purple, grey) that extend from the top of the slide down to the text 'UN / CEFAC'.

**UN / CEFAC**





# Notary Service – Discussion Notes

- A notary service is a parallel "proof of coexistence" mechanism that allows data from multiple ledgers (including private ledgers) to be independently linked
- Even though a notary should use a public ledger for strongest integrity, it can still be a system that restricts access to data based on permissions.
- Notaries can use multiple public chains - which makes the notary stronger - only one has to survive to preserve integrity.
- It is not a honey pot, the only thing the notary must store is hashes/addresses of content in other systems (data pointers, not the data itself) plus any restrictions on who is allowed to access that reference

