Inter-government Ledger

A journey from paper to decentralized trust and what it means for cross border trade & traceability

UNECE 22 Oct 2021

Inter-Government Ledger

Scope – a blockchain based solution for the exchange of preferential certificates of origin (and other document types)

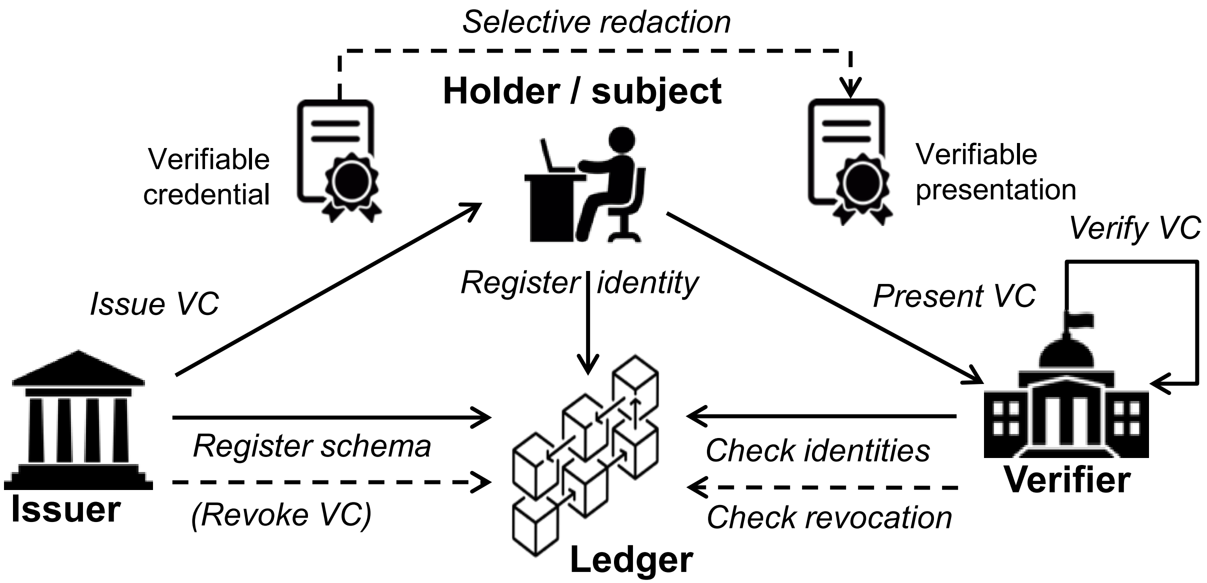
Started with the thought that a private permissioned ledger between governments would be a good idea. We even wrote a draft technical spec and built a working prototype. Almost drowned in complexity.

But soon realised (with some wise guidance from our friends in Singapore) that this was a bad idea – really a solution looking for a problem. No benefit, more complexity, may as well just do G2G XML.

So switched to a much more decentralised model using the W3C "Verifiable Credentials" and "Decentralised Identifiers" standards.

And that was a good decision. There's a lot of benefits – which I'll cover off now.

But what is a Verifiable Credential?



Selective redaction

Holder / subject

Verifiable credential

Verifiable presentation

Verify VC

Issue VC

Register identity

Present VC

Register schema

(Revoke VC)

Check identities

Check revocation

Issuer

Ledger

Verifier

VC Data Model

- Metadata
- Claims
- Proof

A VC is a privacy-preserving digital document that contains a set of claims (eg “has BSc in engineering”) about a subject (eg “john smith”) made by an issuer (eg “Oxford University”) together with a proof (eg digital signature) linked to the issuer identity. **VCs are decentralised - each holder keeps their own data without any need for centralised data stores.**

W3C®

Standard	https://www.w3.org/TR/vc-data-model/
Use Cases	https://www.w3.org/TR/vc-use-cases/

But note! You have to think differently

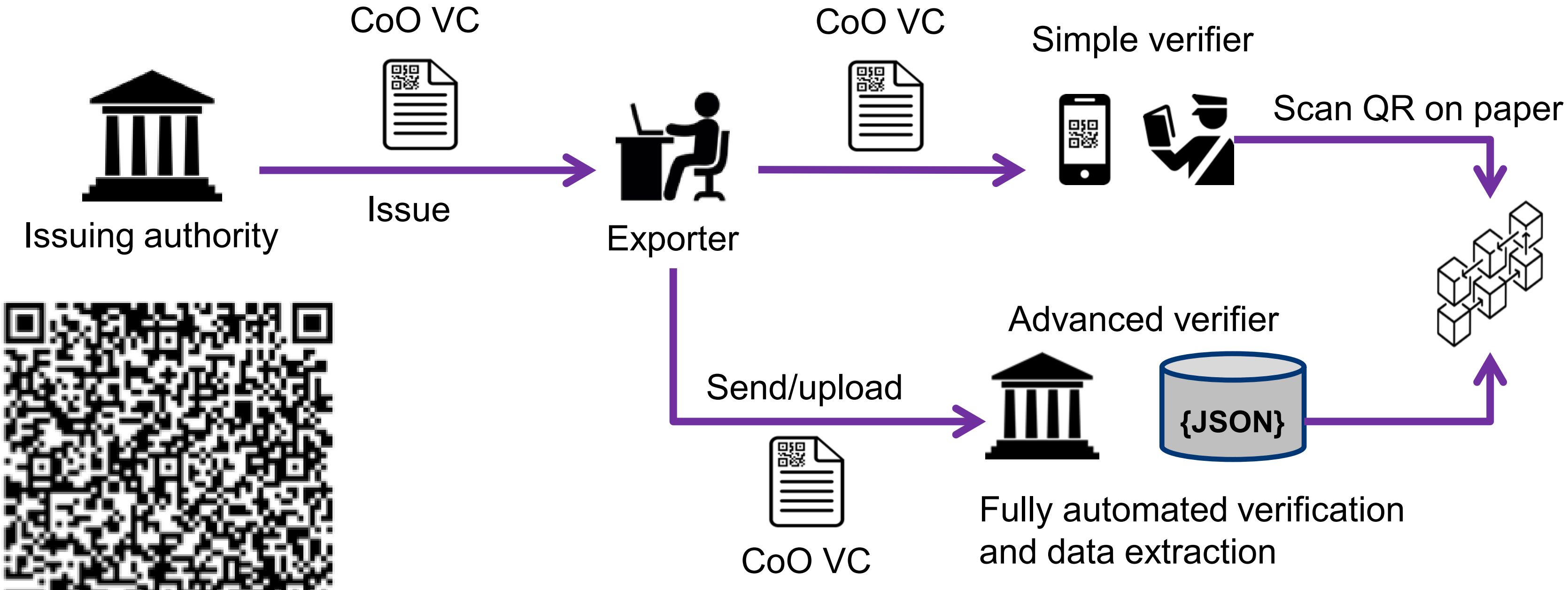
- A VC must comply with a standard model (metadata, claims, proof) but says nothing about how it is exchanged. Case aside pre-conceptions about B2B message channels or hubs / pipelines. I can email you my VC, or upload it to a portal, or show it to you as a piece of paper with a QR on it.
- Anyone to whom a VC is presented can verify it and extract the data from it – without any contact with the issuer. It's a self contained digital credential. Traditional PKI key exchange is not needed either – that's where DID/Ledgers come in.
- A VC is stored wherever the holder wants to store it. A wallet, a cloud store, even a printed piece of paper.
- A VC can be selectively redacted by the holder. Got a drivers license but just want to prove your age without exposing other private data? VCs can do that.
- VCs are tamper evident and revocable.

A useful analogy is your e-passport. Your country issues it, you carry it, any other country can verify it and read the data. VCs are like putting a verification chip into any trade document.

The biggest benefit : decoupling

Setting up G2G document exchange channels can be rather costly and time-consuming. Both sides need to have funded projects and bilateral MOUs. For example, Australia has taken about 10 years to setup e-Cert exchange with about 10 trading partner nations.

But with VCs (using Certificates of Origin as an Example):



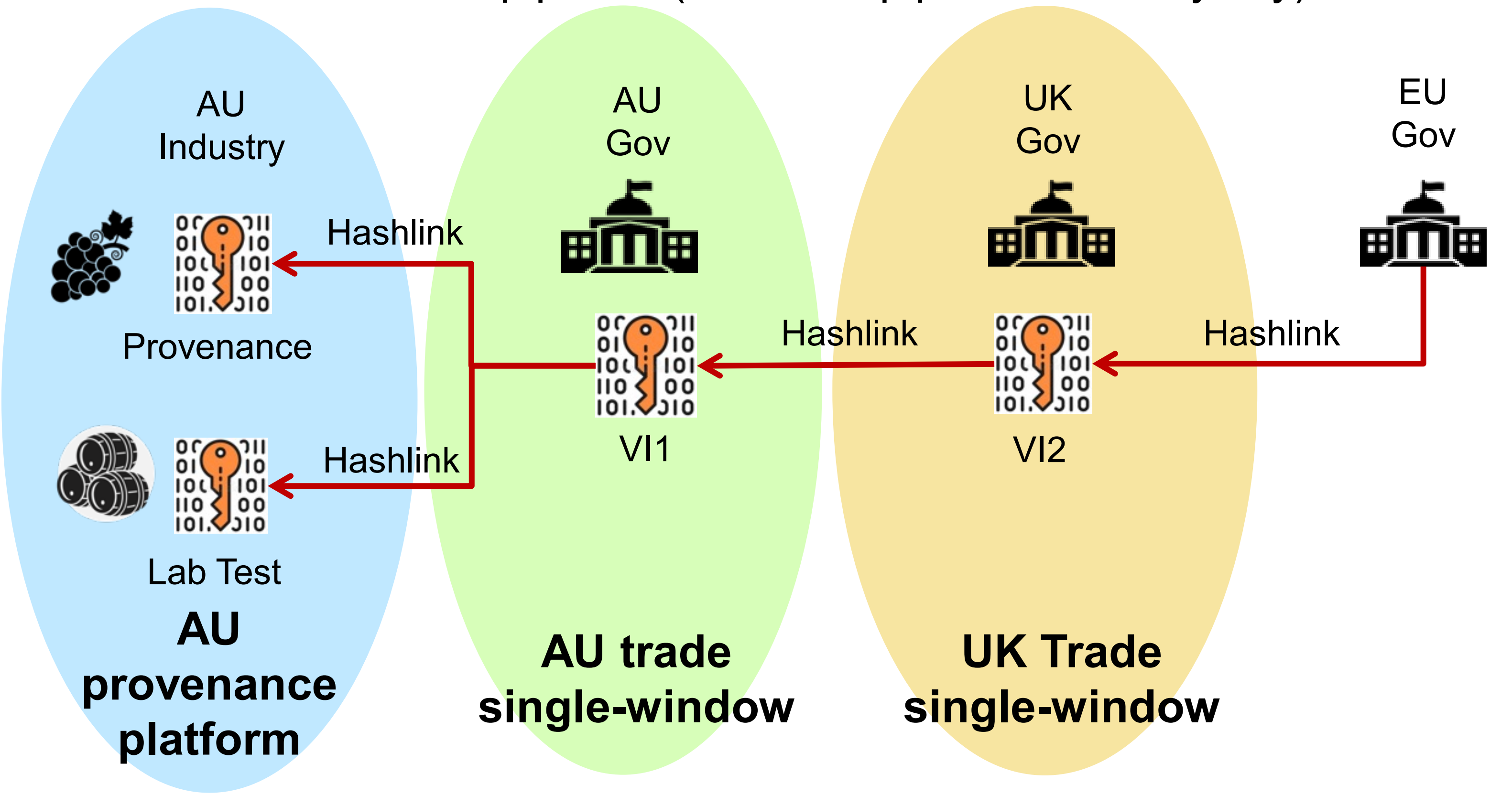
So you can just go digital as an issuer

Since VCs provide a seamless path from paper and simultaneously allow a low tech verifier to just scan a QR and a high tech verifier to do a full automated verification and data extraction (as if the digital data had been sent G2G)…

An issuing agency can just go 100% digital without dependency on trading partner readiness!

Another huge benefit - traceability

Traceability can cross multiple platforms – there's no need for everyone to use the same hub or trade data pipeline (with is a "pipe-dream" anyway)



Platforms / hubs still exist – but they service their functional / geographic domain – and credentials are the glue between them. In reality this scenario would also have port community systems, trade finance systems, etc

So what is the role for UN/CEFACT?

When there's thousands of issuers and millions of verifiers, all using their own preferred technology products, interoperability becomes CRITICAL

- US DHS is running "plug-fests" at the technical level to prove that a credential issued by technology tool A can be verified by technology tool B
- BUT what's even more important is that both issuer and verifier understand the semantics of the claims in the credential. This is the role for UN/CEFACT.

Verifiable credentials use JSON-LD to specify the meaning of the data in the credential.

Just like the way https://schema.org defines web semantics that bring consistency to google searches, so UN/CEFACT should define trade semantics in JSON-LD. Good news is there is a draft.

- https://service.unece.org/trade/uncefact/vocabulary/uncefact/

The other thing we should do is write all this up as guidance for national regulators to help them implement. **That's this project purpose.**

Thanks

steve.capell@gmail.com

UNECE 22 Oct 2021