

A traceability model that works at scale

Using *verifiable credentials*

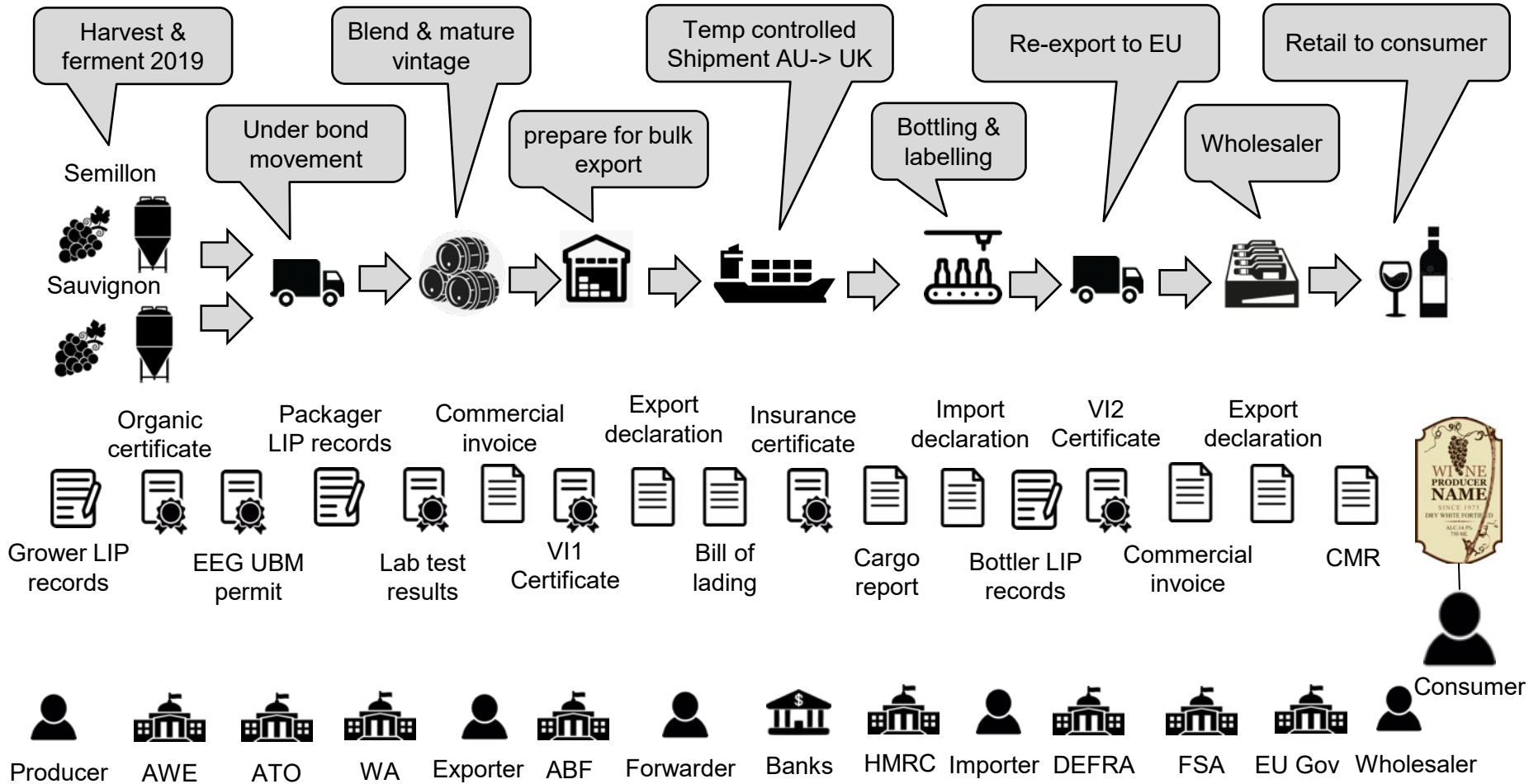
This is NOT a blockchain pitch! – they are useful but not essential in this model.

The logo for UN / CEFAC, featuring the text 'UN / CEFAC' in a bold, blue, sans-serif font. The logo is positioned at the bottom of a vertical stack of colorful lines that transition into a network diagram at the very bottom of the page.

UN / CEFAC

Recently we looked at wine traceability

Barossa Valley Organic Semillon Sauvignon 2019 vintage -> UK -> EU



It would look similar for cotton growers -> fabric makers -> garment producers

Effective traceability needs

Evidence

Documents or data that provides evidence of each step in the chain without breaks.

Trust

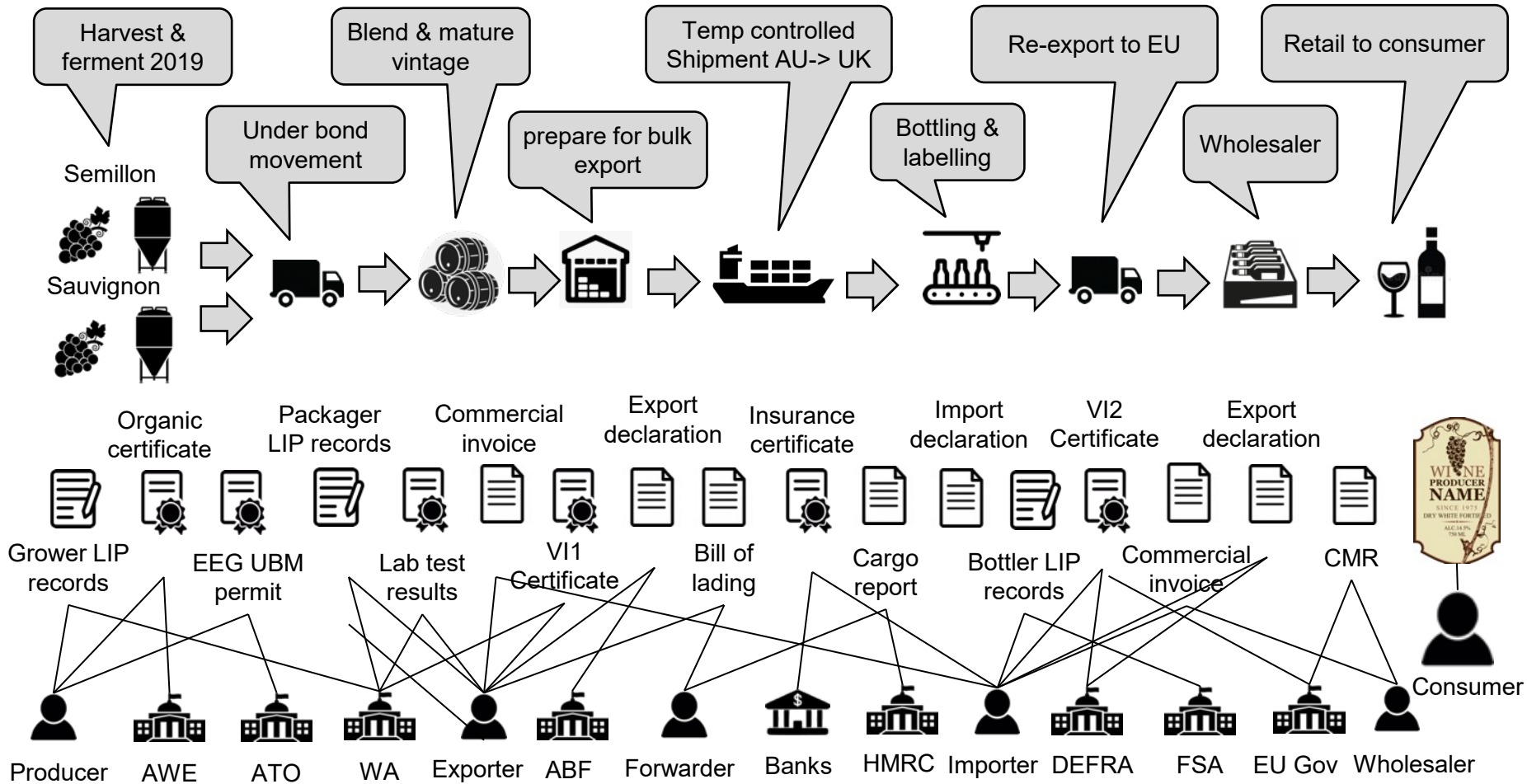
That the document trail is real and that things like identity & quality claims are true.

Automation

That the assessment of evidence and trust can be automated so that traceability can be managed at scale.

The pathway – paper world

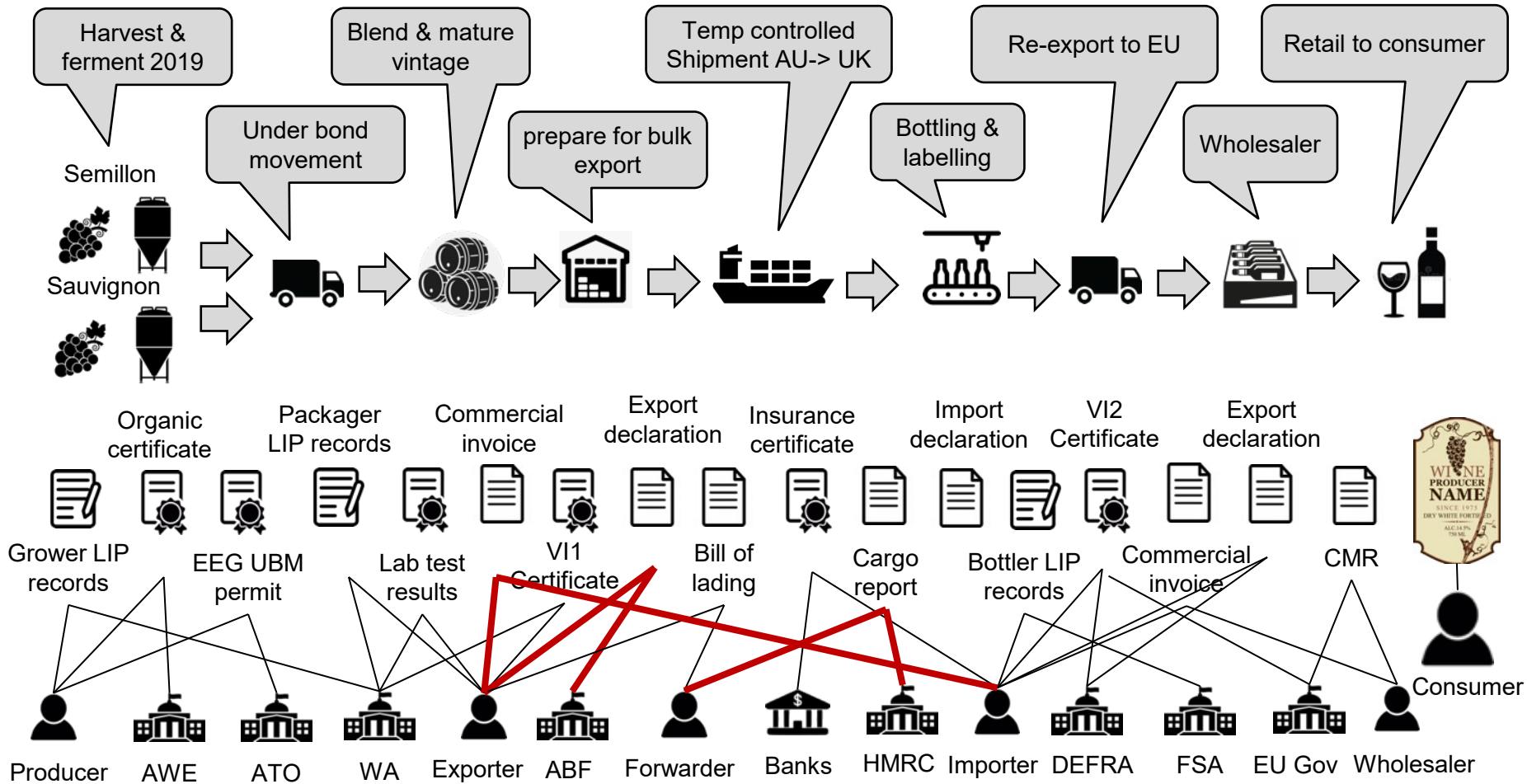
Trust comes from signatures and wet seals.



It's a lot of paperwork – it's inefficient and relatively easy to fake.

The pathway – with some EDI

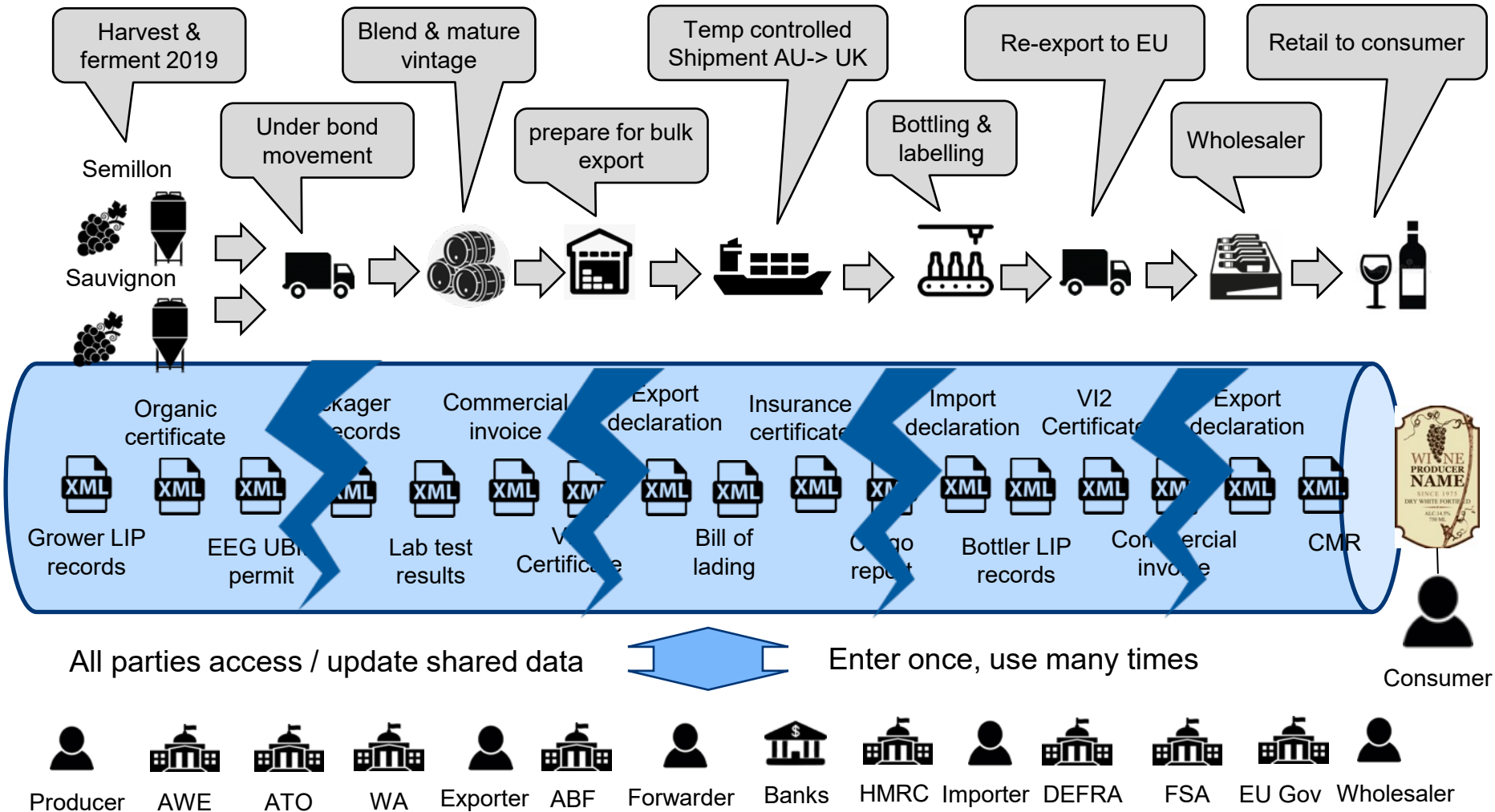
Trust comes from mutual authentication over a bilateral channel.



Traditional EDI (whether EDIFACT, XML, or JSON) is only feasible at volume.

The pathway - with pipelines

Trust comes from identity registration of all parties to the pipeline.



No one pipeline will ever cover the entire supply chain – even one consignment.

There is another way

Verifiable Credentials

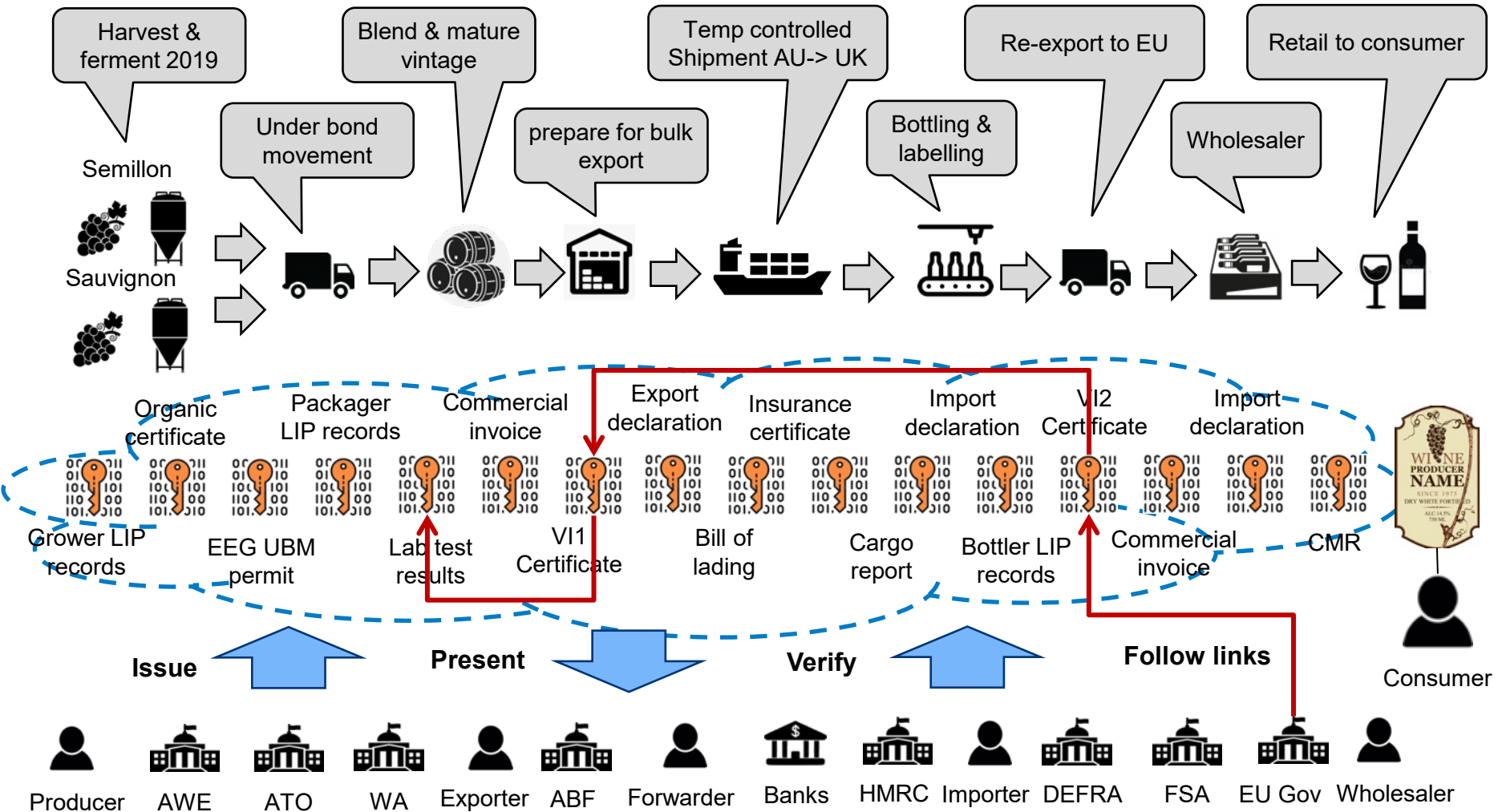
A decentralised model based on new technology standards from the W3C and semantic standards from UN/CEFACT

There's no dependency on EDI messaging and no need for everyone to use the same hub/pipeline and no disruption of long standing paper based processes or existing business relationships.

Like the chip in your e-passport, verifiable credentials make any trade document digitally verifiable and readable by **both** humans and machines.

The pathway – with verifiable credentials

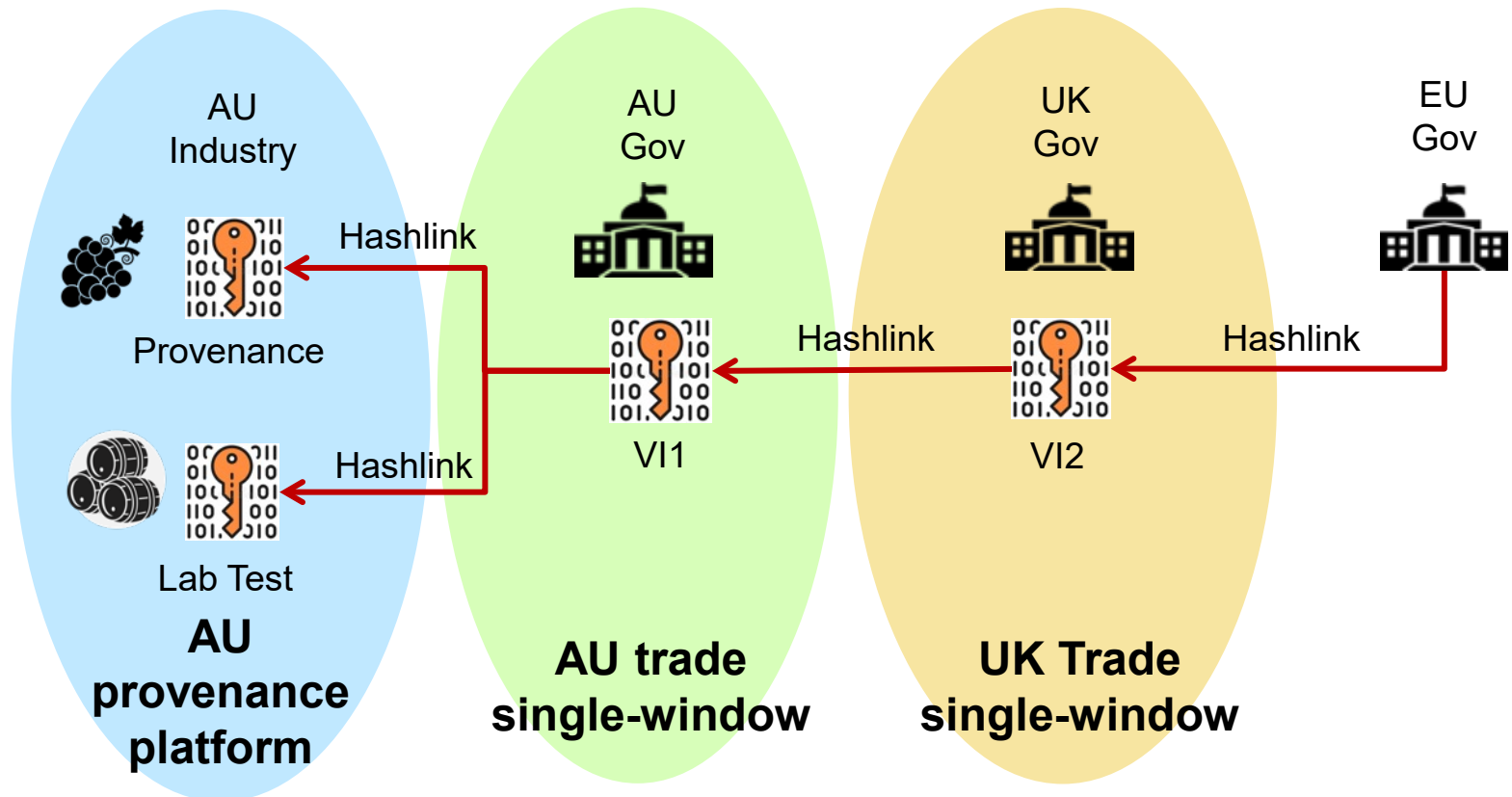
Trust comes from digital signatures linked to national “trust anchors”



The role of the regulator is to be the “trust anchor” – of identity & authority

So digitization could look more like this

What matters is the digital (verifiable) document, not the transport.



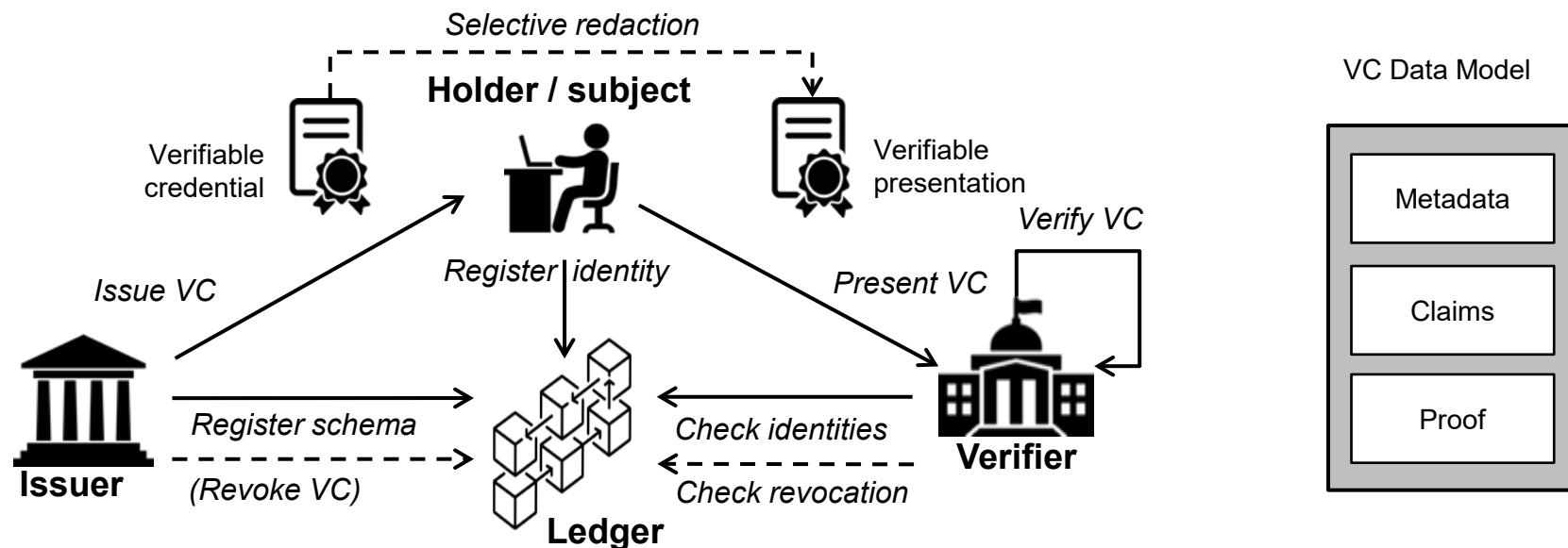
Platforms / hubs still exist – but they service their functional / geographic domain – and credentials are the glue between them. In reality this scenario would also have port community systems, trade finance systems, etc

Thank you

Steve.Capell@gmail.com

The logo for UN / CEFACT, featuring the text 'UN / CEFACT' in blue capital letters. The logo is positioned between a vertical bar of multi-colored lines above and a network diagram of multi-colored lines below.

And what is a Verifiable Credential?



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.



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

Which solves a pressing problem

Everyone wants to rule the world – and no-one will. This is how to coexist.

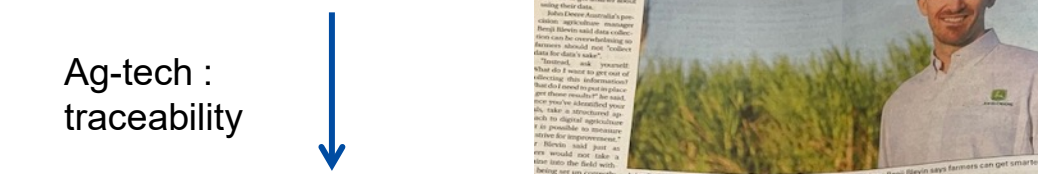
In just one issue of the land..



Ag-tech : monitoring

Ag-tech : sustainability

Ag-tech : traceability



Sharing data as VCs solves the problem

And why are they important?

- Tamper proof : Impossible to change without invalidating the document.
- Identity linked : Strongly linked to the identity of issuer and subject (eg trader)
- Revocable : Revoked documents will show as invalid even after issue.
- Redactable : Holder can redact private or commercially sensitive data.
- Verifiable : By any party even if unknown to the issuer.
- Automatable : high volume verifiers can automate verification & ingest full data
- Interoperable : even with millions of independent issuers & verifiers
- Secure : from all plausible attack vectors & ASD ISM/cyber compliant.
- Cost effective : No shared infrastructure needed.

Analogy – like the chip in your passport, a VC allows any human readable document to embed a digitally verifiable proof of integrity.

Here's an example...

AU – SG CoO using OA Protocol

Open attestation (OA) Adds a few useful extensions to the basic VC framework for the cross border trade use case.

- PDF compatible: One time secret embedded in QR code allows secure storage of the original data that is still accessible by any verifier to which the QR enabled PDF is presented. This means:
 - Existing supply chain processes can continue, just swap the paper “original” for a PDF with QR.
 - Any verifier can confirm integrity just by scanning the QR.
 - Mature verifiers can still retrieve and process the underlying digital data and proofs.
- Batch notarisation: Open Attestation depends on the Ethereum public ledger and each transaction costs about \$1. Batching allows 1000's be be notarised with a single blockchain transaction, reducing costs to near zero.
- Holder managed redaction: The holder of the open attestation can redact any data element without recourse to the issuer.



Scan me!

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.**