UN/CEFACT 40th Forum : Seminar
Future of Digital Standards for Sustainable Supply Chains
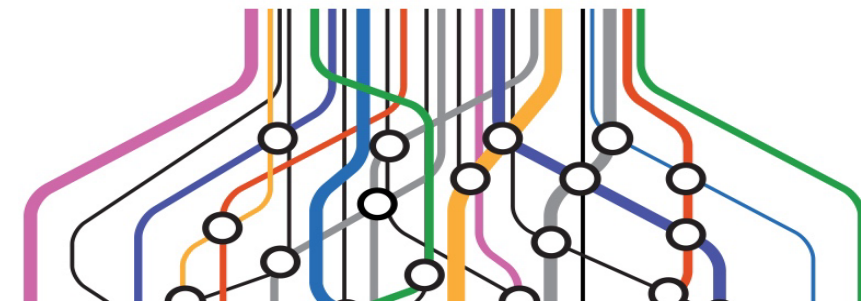
Implementing Digital Trust
Guidance for policymakers

Steve Capell
steve.capell@gmail.com

UNECE

UN / CEFACT

Why should we care about digital trust?

As regulatory and consumer pressures drive up demand (and justify premium prices) for sustainable goods, so the commercial incentive to make fake sustainability claims will increase.

EC investigation : 59% of environmental claims had no evidence and 42% were deemed false or deceptive.

Fast Company: 68% of executives admit their company is guilty of greenwashing.

Survey: 78% of consumers believe that companies should be environmentally responsible and are willing to pay premiums for confidence in those claims.

Secretary General Guterres at COP27 2022 : **"Zero Tolerance for Greenwashing"**

https://www.un.org/sites/un2.un.org/files/high-level_expert_group_n7b.pdf
https://ec.europa.eu/commission/presscorner/detail/en/ip_21_269
https://www.fastcompany.com/90740501/68-of-u-s-execs-admit-their-companies-are-guilty-of-greenwashing
https://blog.gitnux.com/greenwashing-statistics/
https://www.un.org/en/delegate/%E2%80%98zero-tolerance-greenwashing%E2%80%99-guterres-says-report-launch

What could be the consequences of greenwashing?

There is already a significant difference between consumer expectation and market behaviour. There are two plausible pathways out of this:
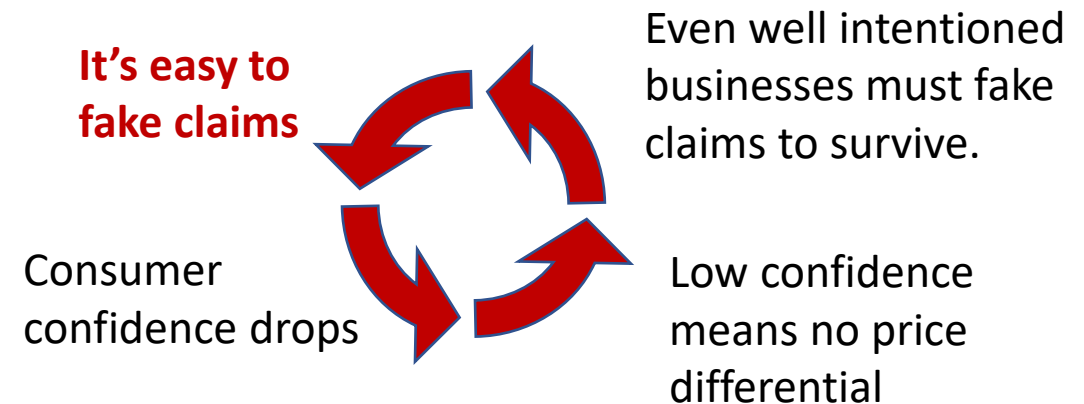
Either : A race to the top
Greenwashing is rare and has nowhere to hide

It's hard to fake claims

Consumer confidence improves

Higher prices are justified

Business is motivated to make provable claims

Or : A race to the bottom
Greenwashing is ubiquitous and undetectable

It's easy to fake claims

Even well intentioned businesses must fake claims to survive.

Low confidence means no price differential

Consumer confidence drops

So we should be motivated to make it hard to fake claims! That is the focus of this presentation.

So how can we trust sustainability claims?

There are three ways that sustainability claims might be verified. They can and should work together

I say it's true :
prove me wrong!

*Make claims public
and rely on activism
to call out fakes.*

**Important starting point
but easiest to fake.**

They say it's true :
do you trust them?

*Trusted authorities
accredit certifiers who
audit the claims.*

**Good, but you've got to trust the
audit process and the auditor.**

It's self-evidently true:
I can see the proof myself.

*Digitally verifiable
traceability & transparency
supports the claims*

**We'll focus on the this one
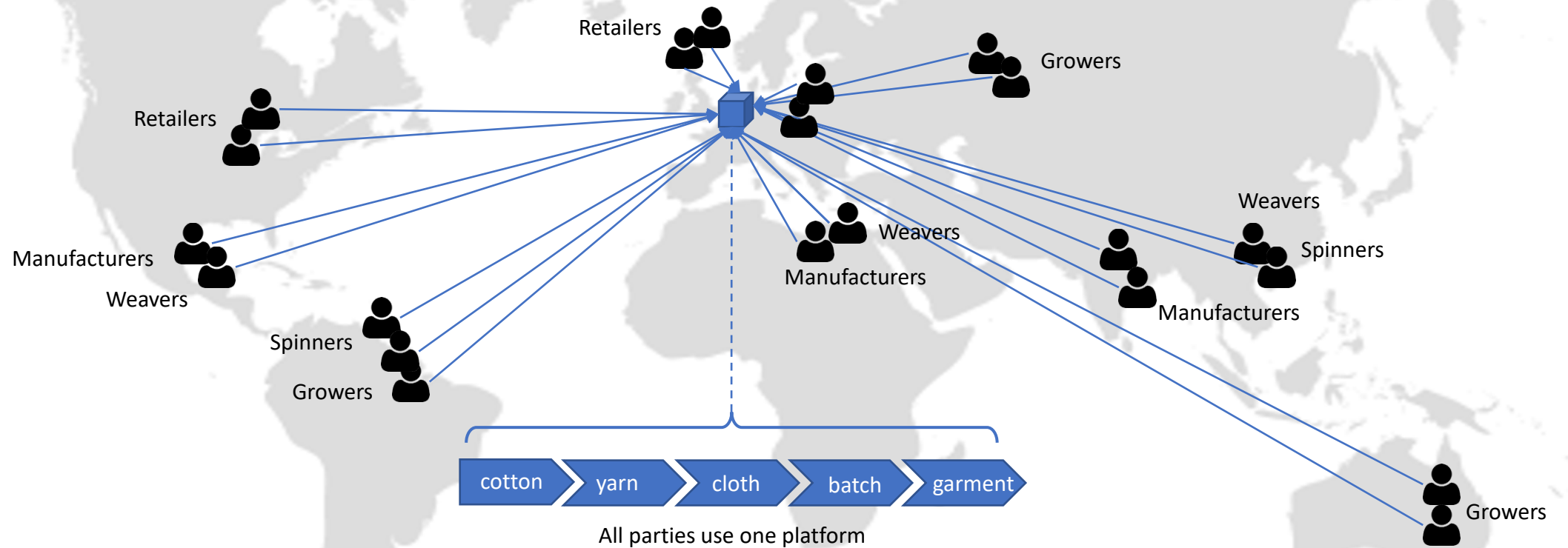because it's the hardest to fake**

But how to connect up complex global supply chains?

Textile & leather simple example
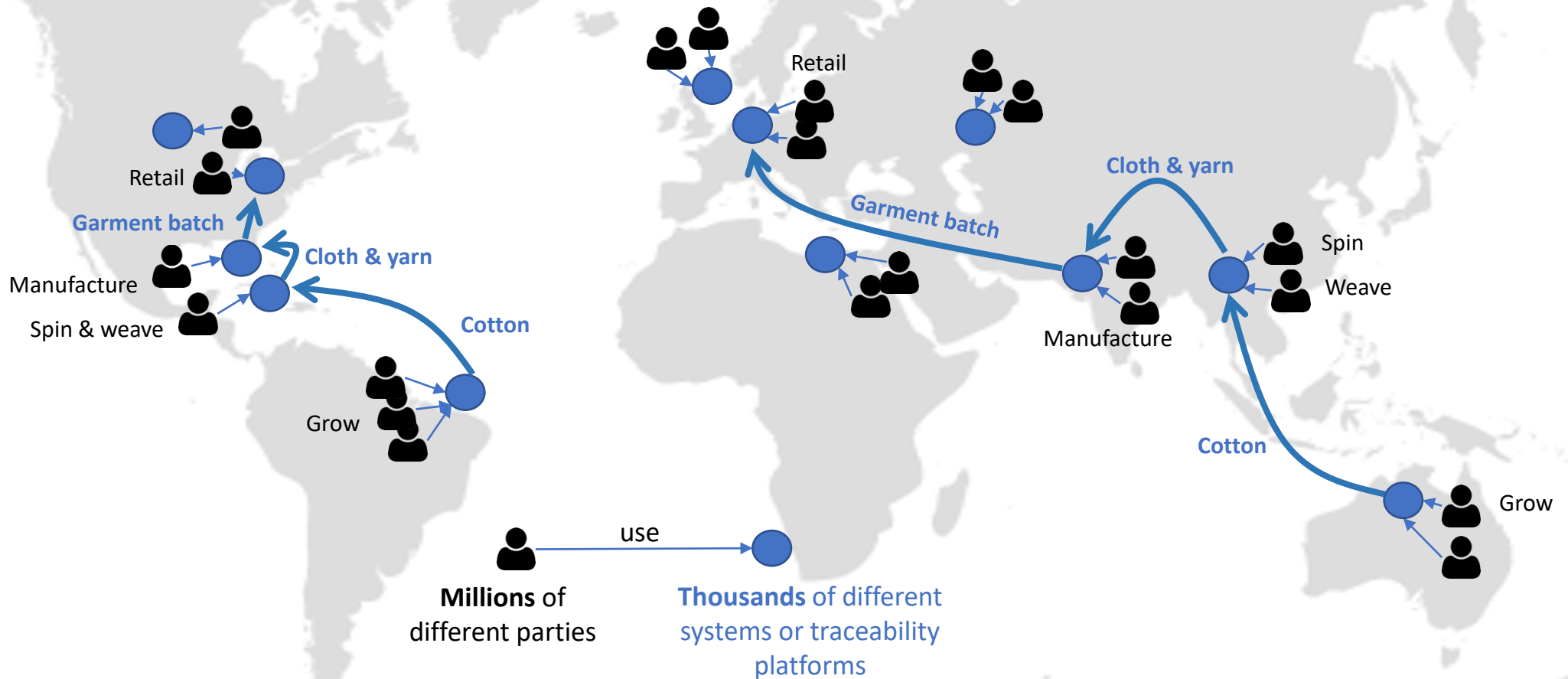
Some have suggested something like this

Everyone should use my blockchain

cotton ⟩ yarn ⟩ cloth ⟩ batch ⟩ garment

All parties use one platform
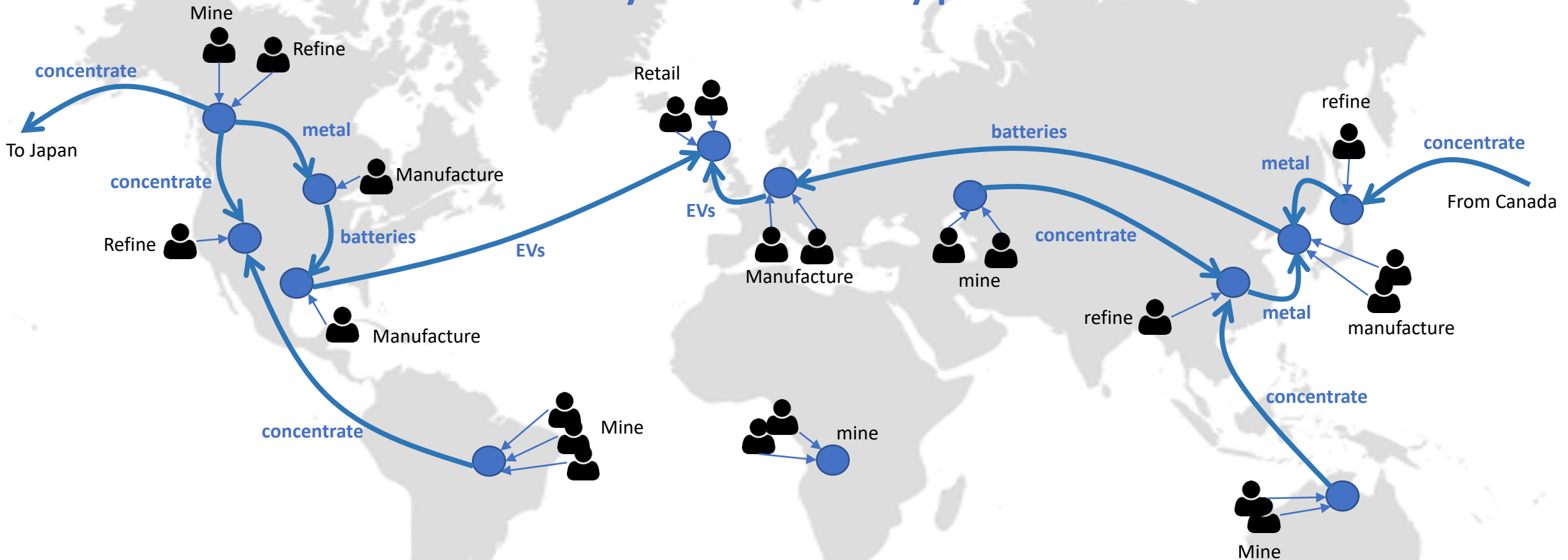
This approach will never work at scale.

But there will never be one platform.

Each blue dot is a platform – and there are thousands of them.

And there are many different industry sectors.
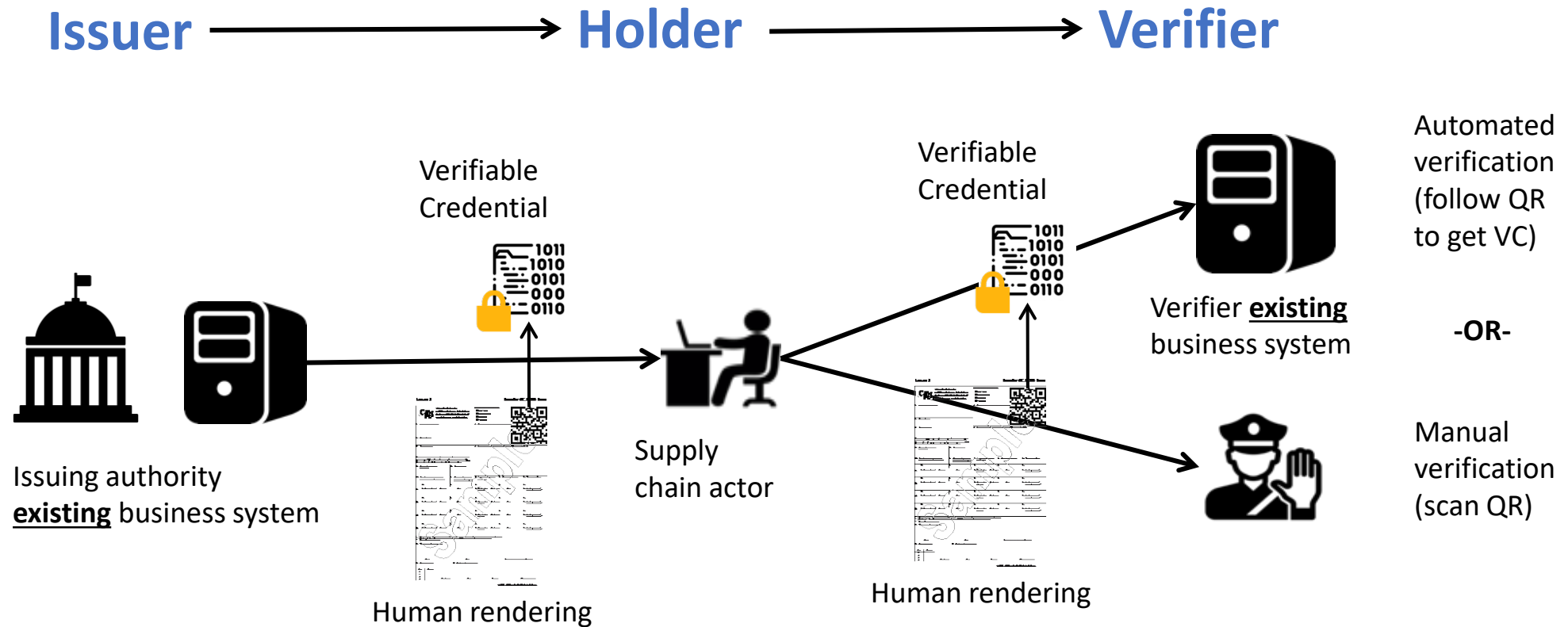
And each industry sector has many platforms to choose from

So the key question is how to connect up the blue dots

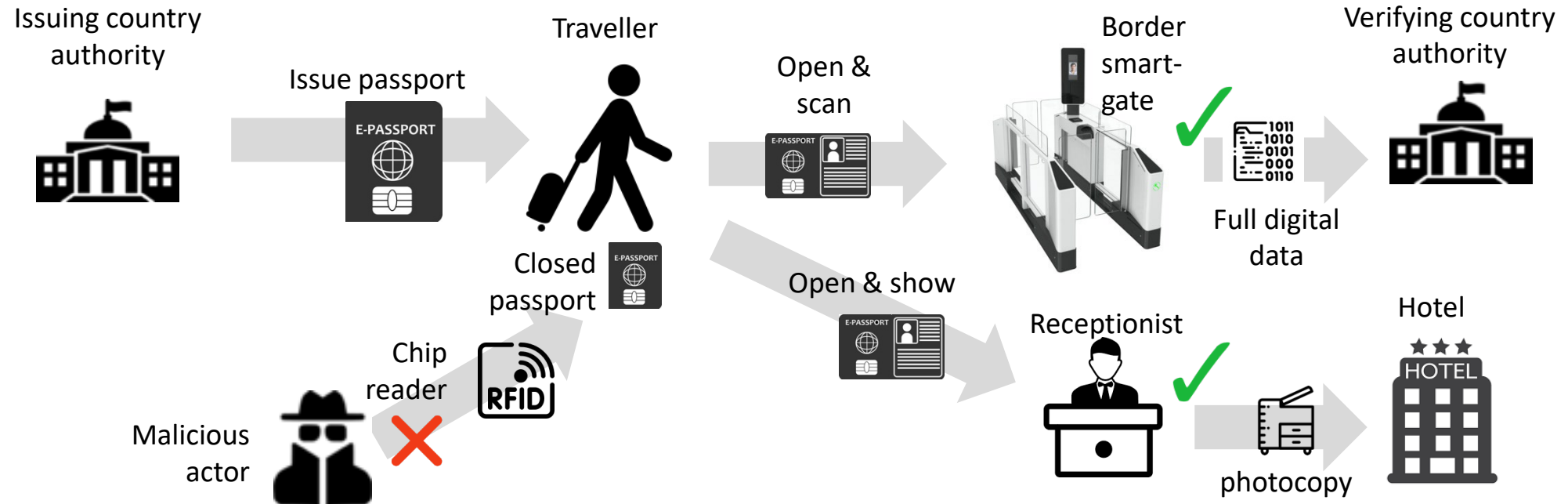# Introducing a solution - verifiable credentials (VCs)

A VC is a self-contained and <u>portable</u> packet of verifiable data that includes a human rendering.

VCs help overcome many barriers to scalability of traceability & transparency solutions.

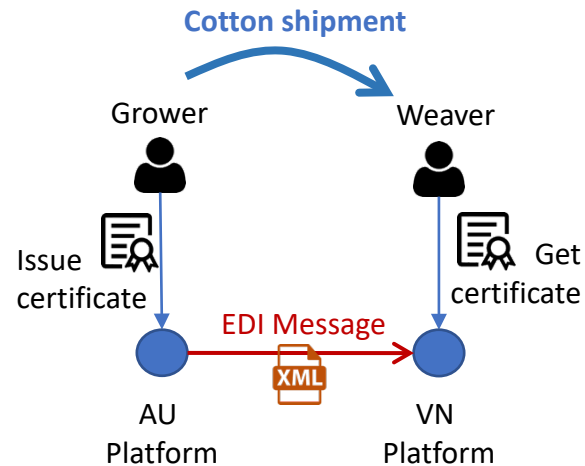# But first an analogy – to help to understand VCs

A verifiable Credential is like the chip in your e-passport – but for any trade document or certificate

Why are VCs the most scalable way to join the dots?

Lets consider 3 options for exchange of an organic cotton certificate AU -> VN

EDI Messaging

Cotton shipment

Grower — Weaver

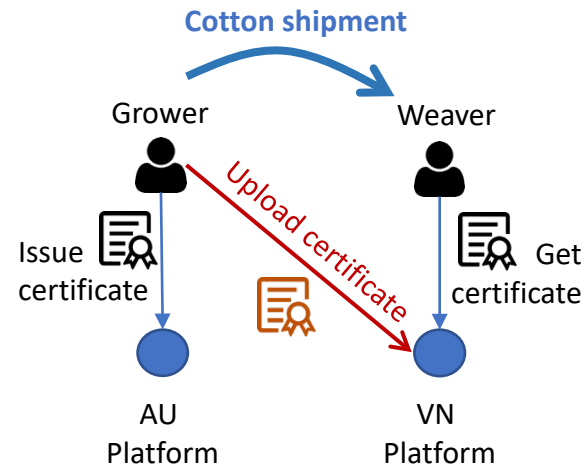Issue certificate — Get certificate

EDI Message — XML

AU Platform — VN Platform

But when there's 1000 blue dots
- ~100k separate and costly integrations needed
- Grower needs weaver technical routing info
- Different business flow for connected / not connected dots.
- EFTI style register helps but has it's own major problems.

User Registration

Cotton shipment

Grower — Weaver

Issue certificate — Upload certificate — Get certificate

AU Platform — VN Platform

But when there's 1000 blue dots
- If grower has 100 customers then may need 100 separate platform accounts.
- Complex identity & commercial issues (does VN platform charge AU grower?)
- Different business flows for different platforms.
- A very small number of giant global platforms helps but that has it's own major problems

VC exchange

Cotton shipment

Grower — Present — Weaver

Issue VC — verify VC

AU Platform — VN Platform
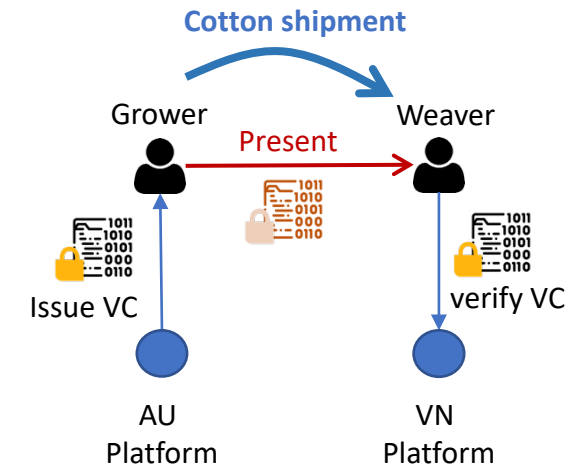
But when there's 1000 blue dots
- Nothing changes, grower just sends the same VC to any weaver.
- Grower and weaver continue with their own platforms and need no knowledge of each other's systems.
- Same business flow irrespective of platform or stakeholder technical maturity / capability. The portable, verifiable, paper friendly VC is totally self-contained.

VCs can be verified simply by scanning a QR

Signed and encrypted, placed in public store

Any Verifier Service

Retrieve, decrypt, and verify the VC

Redirect to hosted verifier service

Issue permit as VC

Issuing country authority

Issue document as PDF with QR

Trade document

Scan QR

Verification
✓ No Tampering
✓ Not revoked
✓ Authorised Issuer

Importing authority verifies document
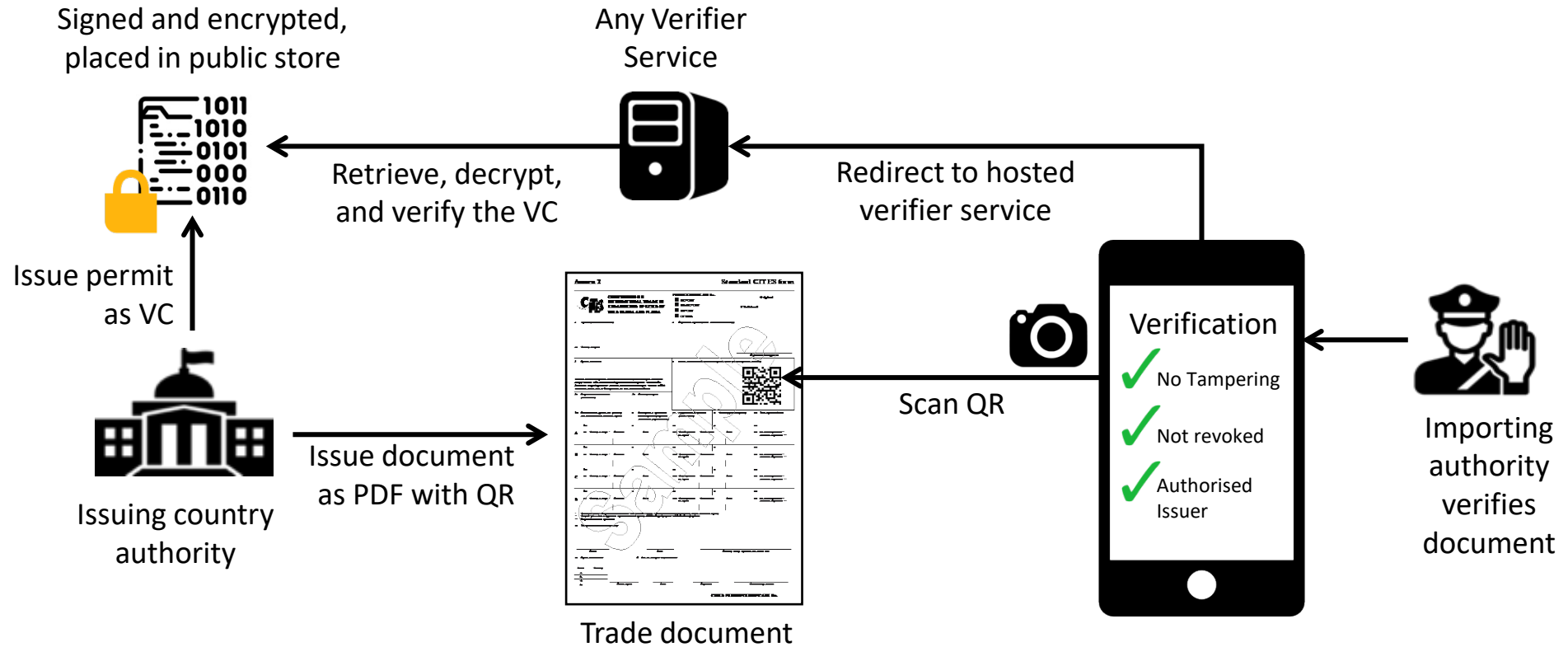
But advanced verifiers can still get all the data.

Signed and encrypted,
placed in public store

Retrieve, decrypt, verify the VC
and ingest full digital data

Authority business system
with VC capability

Issue permit
as VC

Uses

Issuing country
authority

Issue document
as PDF with QR

CITES permit

Permit
submitted to

QR
processed
by

verifying country
authority

Importing
authority
verifies
document
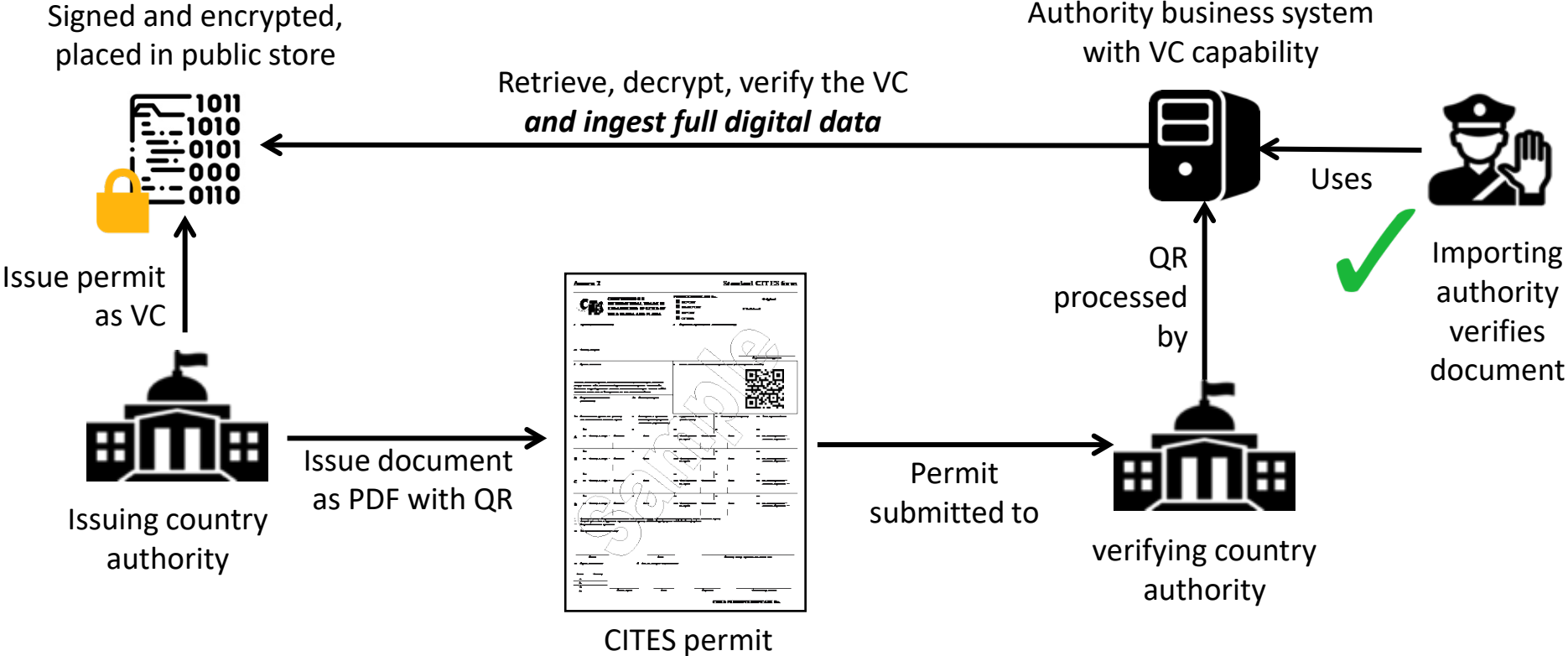
Wait, the <u>same</u> document is both paper <u>and</u> digital?

web link with decryption key

Encrypted, signed, and
published digital VC

PDF or HTML
rendering of the
digital document
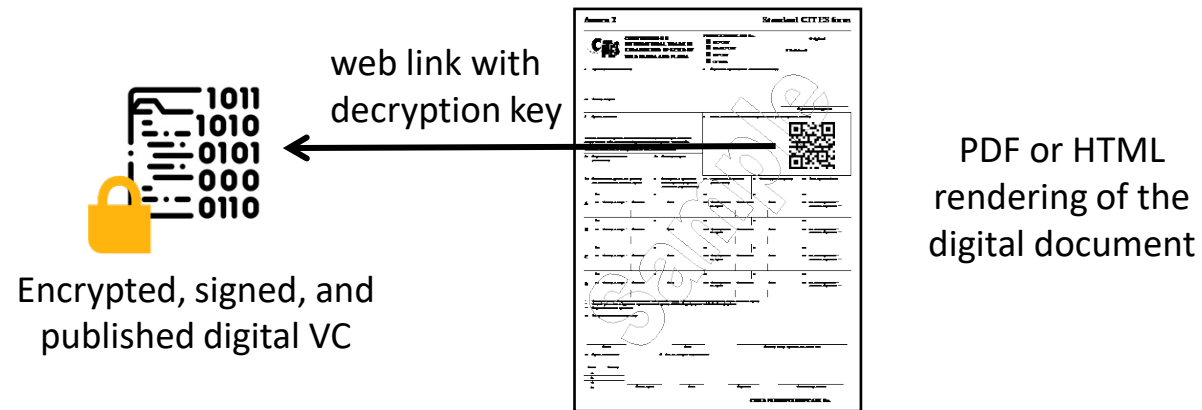
Yes! – and this removes another key blocker to scalability. As an issuer, you can go 100% digital <u>without any dependency</u> on holder or verifier digital maturity

VCs also solve another barrier - commercial sensitivity

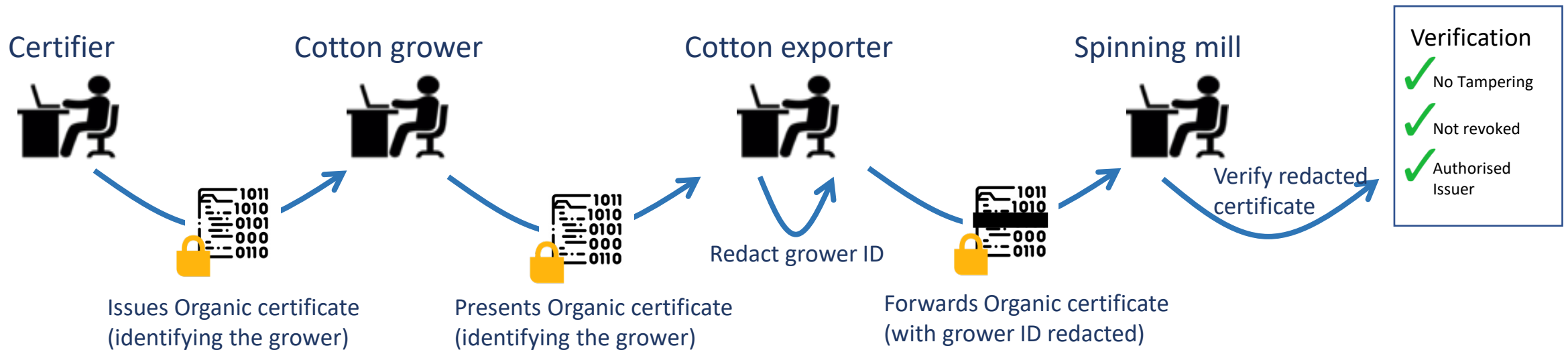One major challenge for supply chain traceability & transparency solution is commercial sensitivity. If stakeholders risk revealing sensitive information like prices or customer lists when providing sustainability evidence then they are likely to withhold key sustainability data.

VCs allow holders to selectively redact information before presenting the VC to verifiers without breaking cryptographic integrity. For example:

Certifier

Cotton grower

Cotton exporter

Spinning mill

Verify redacted certificate

Redact grower ID

Issues Organic certificate (identifying the grower)

Presents Organic certificate (identifying the grower)

Forwards Organic certificate (with grower ID redacted)

Verification
✓ No Tampering
✓ Not revoked
✓ Authorised Issuer

This capability removes the need for complex data access controls. Each participant passes on the subset of VC information that they deem appropriate to meet market and regulatory requirements.

It's not a competition. VCs amplify the value of platforms

A platform that cannot issue or verify VCs remains an island. But if you issue VCs to your users then you empower them and retain them. If you accept VCs as inputs you can add integrity and reduce costs of your internal processes.
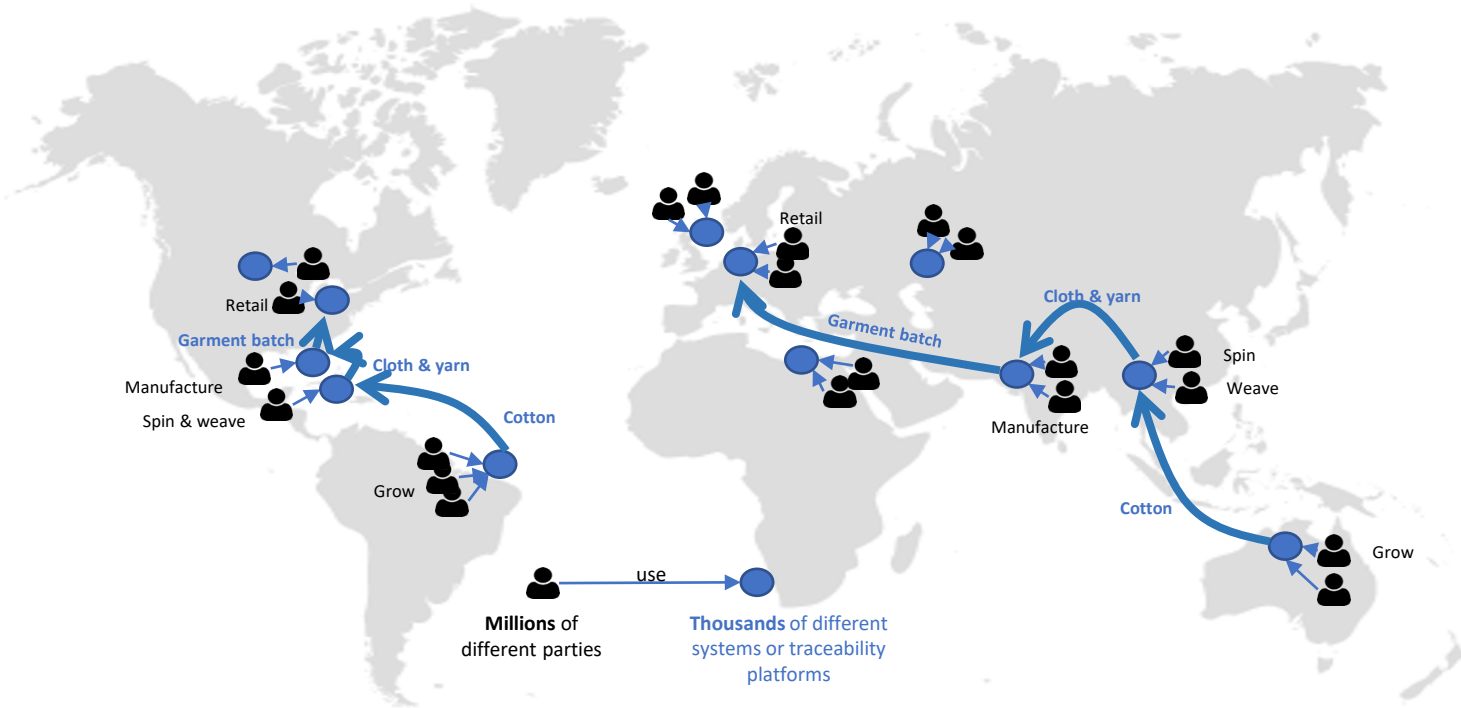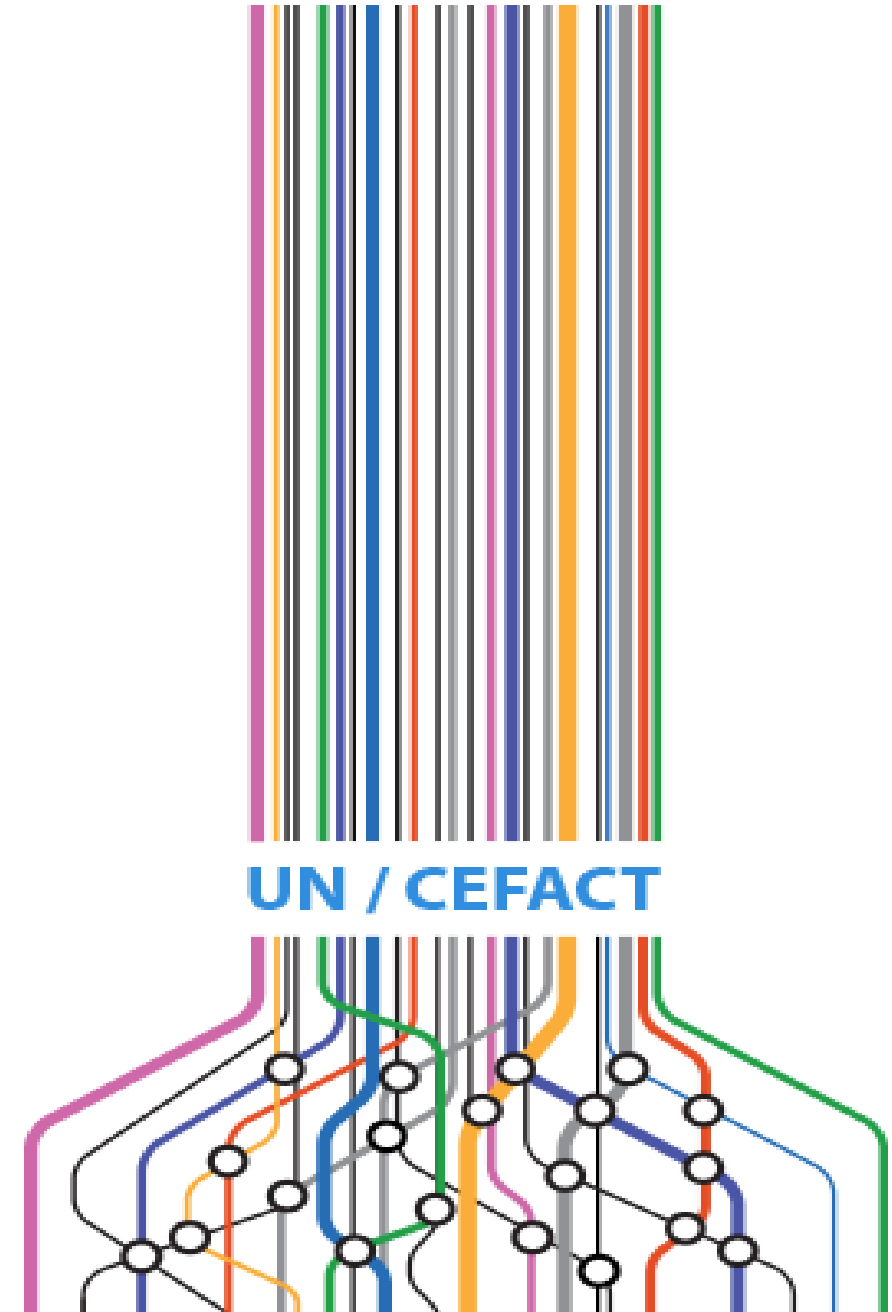
For example:
- Certifying authorities that issue conformity certificates as VCs empower their customers to prove product compliance through the supply chain.
- Identity providers (eg regulators and banks) that issue identity VCs allow their users to prove their identity whilst protecting their privacy.
- Phytosanitary / fumigation certificates as VCs would allow food safety regulators to automate import permit processes.

Retail

Garment batch

Manufacture

Spin & weave

Cotton

Grow

Millions of different parties

use

Thousands of different systems or traceability platforms

Retail

Garment batch

Cloth & yarn

Manufacture

Spin
Weave

Cotton

Grow

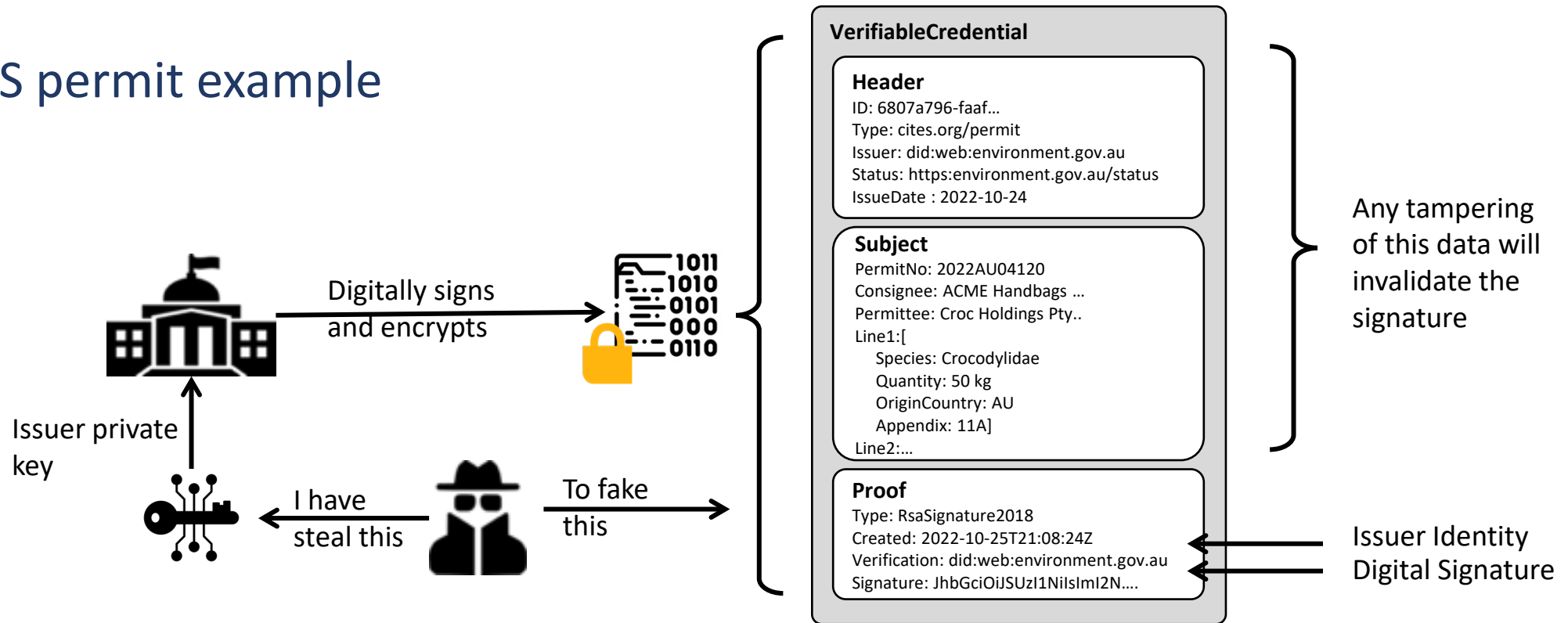VCs are the glue between diverse systems and platforms. Blue dots that support VCs will amplify their value.

OK, that was all about scalability

Now what about trust?

Lets start by looking at a single VC in more detail

CITES permit example

Digitally signs and encrypts

Issuer private key

I have steal this

To fake this

VerifiableCredential

Header
ID: 6807a796-faaf...
Type: cites.org/permit
Issuer: did:web:environment.gov.au
Status: https:environment.gov.au/status
IssueDate : 2022-10-24

Subject
PermitNo: 2022AU04120
Consignee: ACME Handbags ...
Permittee: Croc Holdings Pty..
Line1:[
    Species: Crocodylidae
    Quantity: 50 kg
    OriginCountry: AU
    Appendix: 11A]
Line2:...

Proof
Type: RsaSignature2018
Created: 2022-10-25T21:08:24Z
Verification: did:web:environment.gov.au
Signature: JhbGciOiJSUzI1NiIsImI2N....

Any tampering of this data will invalidate the signature
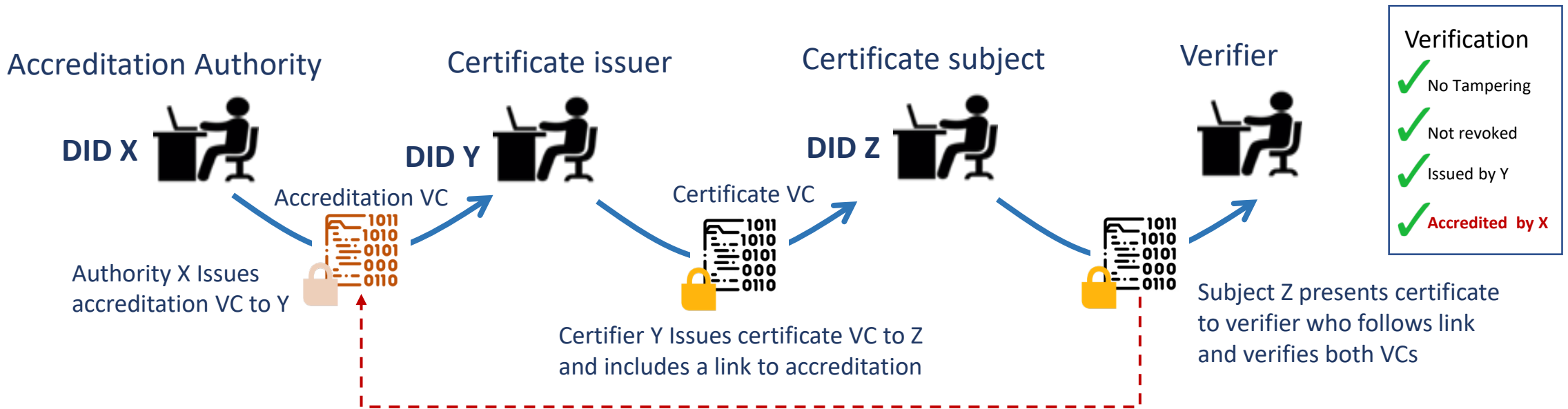
Issuer Identity
Digital Signature

What can I actually trust?

✓ That the VC really was issued by the identified issuer
✓ That the VC is non-repudiable (issuer cant say they didn't issue it)
✓ That the VC data / claims have not been changed or tampered-with.
❓ But can you trust that the claims are true?

How can we be confident that VC claims are true?

A fake certifier might issue "technically valid" credentials. They'll verify ok but still might be telling lies. If I don't already know and trust the certifier then I may have limited confidence that the claims are true.

The answer is that the claim needs to be linked to another claim that is issued by a party you can trust. For example, national accreditation authorities already have the job of auditing and accrediting certifiers to issue specific certificate types. This is implemented in VCs using chained credentials.

Accreditation Authority

DID X

Certificate issuer

DID Y

Certificate subject

DID Z

Verifier

Accreditation VC

Certificate VC

Authority X Issues accreditation VC to Y

Certifier Y Issues certificate VC to Z and includes a link to accreditation

Subject Z presents certificate to verifier who follows link and verifies both VCs

Verification
✓ No Tampering
✓ Not revoked
✓ Issued by Y
✓ Accredited by X

Wait, what is a DID?

A DID is a "Decentralised Identifier", sometimes called a "Self-Sovereign Identifier". Which basically means that it's an ID created by anyone to identify themselves. It is usually a string of numbers and characters that has no meaning.

Why is that useful? Because a DID has an associated public / private key-pair that, through the magic of asymmetric cryptography, allows the DID holder to prove to anyone that they really do own that DID.

Why is that useful? Because DIDs are the cryptographic glue that connect chained credentials. Back to the previous example:

Accreditation Authority	Certificate issuer	Certificate subject	Verifier
DID X	DID Y	DID Z	

Verifies ownership of DID Y and issues accreditation to DID Y, signed by X **2**

Proves ownership of DID Y and requests accreditation from X **1**

Presents certificate VC from Y to verifier **4**

Does not know or trust Y but does trust X. Verifies that certificate is issued by DID Y and also that the same DID Y is the subject of accreditation VC from X **5**

Issues certificate VC to DID Z signed by Y and linked to accreditation VC **3**

Which brings us to trust graphs & trust anchors

A trust graph is a set of chained credentials that, taken together deliver more verifiable trust than an individual credentials. For example the certificate VC -> accreditation VC is a small trust graph of two chained credentials.

A trust anchor is special kind of VC issuer that has the quality that what they say can be trusted. For example the accreditation authority says that the certifier is accredited. Or a regulator attests to the identity of a registered business.

We've developed a notation for this. Here's an example for origin claims. Ellipses represent entities heavy outlines are trust anchors), rectangles represent things (yes, they can have DIDs too). Arrows represent VCs with direction from issuer DID to subject DID.
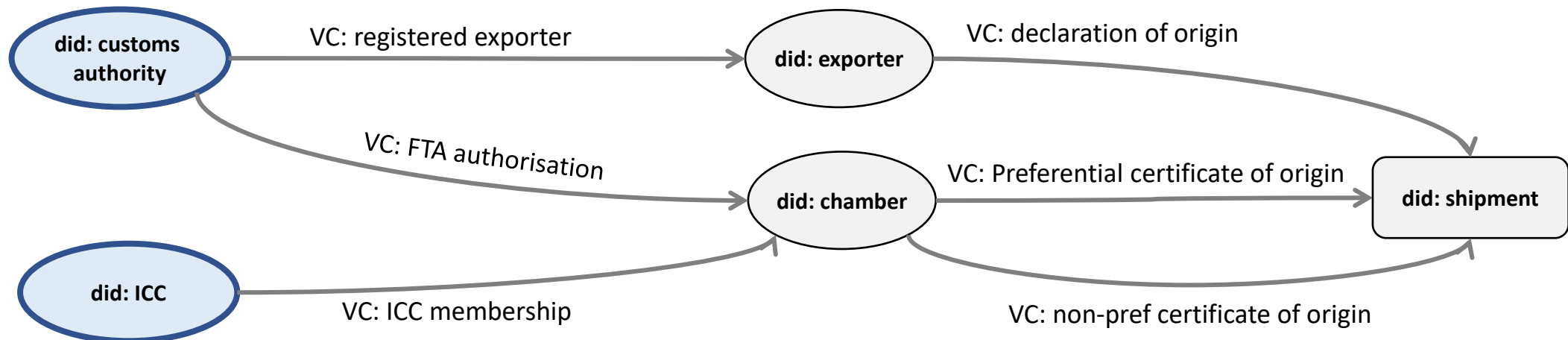
Here's one for documentary letters of credit

With the VCs shown, a trade finance institution can automate the documentary letter of credit process with high confidence because they have verifiable invoice data, bill of lading data, seller identity, carrier identity, and a link between the financial and logistics transactions.
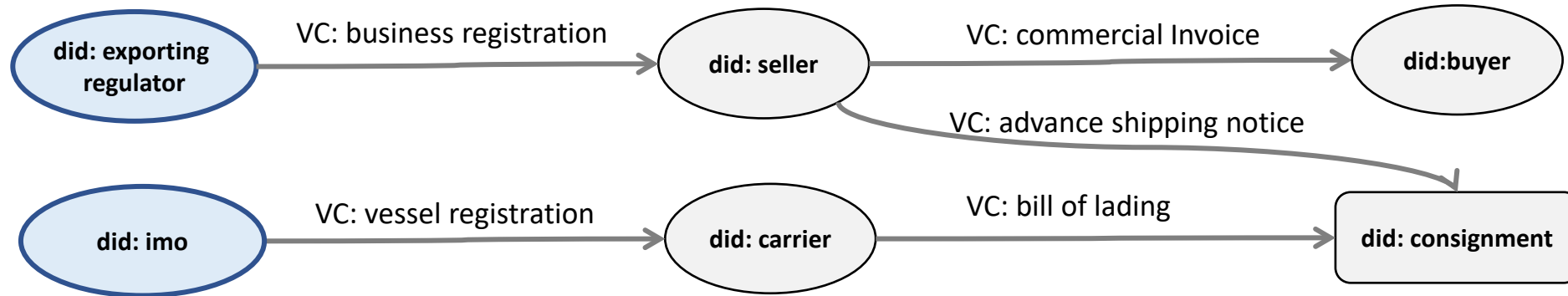
Interesting fact – the Asian Development Bank estimates a global trade finance gap (ie finance that is desired and available but applications are rejected) of around $2Tn. The main reason for rejection of finance applications is inadequate identity confidence and poor document integrity.

And here's one for the entire textile supply chain

Yes, it's complex. But remember, it doesn't need to all be in place at once. And machines are good at making sense of complex graphs. The DPP in the diagram could be issued without the evidence of the traceability graph – but is stronger if backed by this evidence.
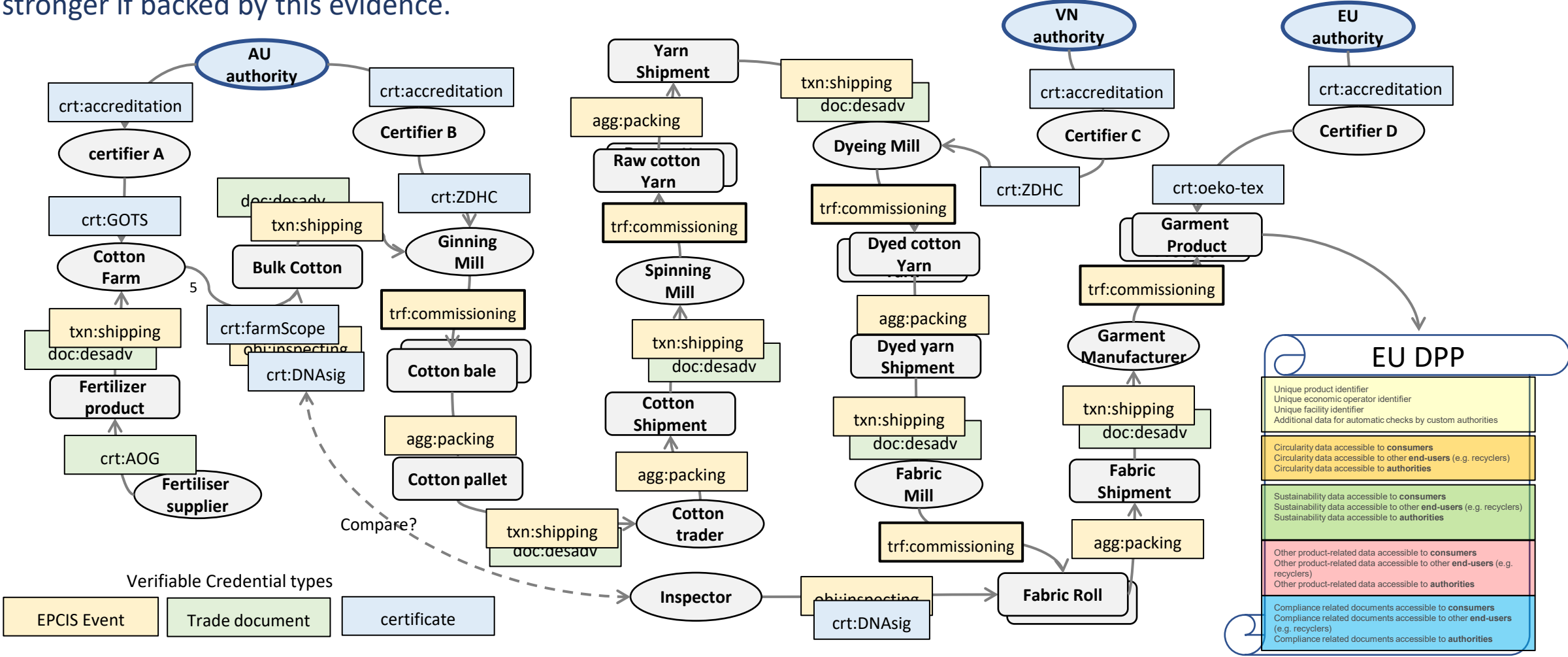
Another kind of trust problem

Up to this point we've been talking about trusting that entities are who they say they are and are authorised to make the claims they are making. But what if I can see a high integrity trust graph, but it's not about the product I'm buying? For example:

- **Product substitution.** A devious distributor might present high integrity digital proof of sustainability about a specific type of battery – but the actual shipment contains batteries of similar type but not the same origin.
- **Mass balance fraud**. A malicious manufacturer might buy 10 Tons of genuine sustainable and organic cotton and blend it with 90 tons of cheaper un-sustainable cotton – then re-sell the 100 Tons to 10 different clients, re-presenting the same evidence 10 Tons of sustainable cotton evidence to each.

Is solved with physical-digital links & VC aquittals

Attacking product substitution and mass balance requires a strong and verifiable connection between the digital evidence and the physical goods.

- **For manufactured products** the ideal solution is serialised identifiers such as GS1 SGTINs that are unique for each instance of the product and can be correlated to the digital evidence. In some cases, a unique key can be used to acquit (ie spend once) the digital evidence.
- **For bulk products** it is often less feasible to serialise products. A variety of innovative intrinsic marker technologies are rapidly becoming commercially feasible including DNA markers for agri/food and chemometrics for minerals. High cost means that these methods are usually used for occasional audits or high value shipments.

VCs can support acquittals - When a serialised physical product is "spent" (ie consumed in a manufacturing process or purchased by a buyer) then the corresponding VC can be revoked or acquitted, preventing double spend.

And with quotas using extended VC status

Another way to attack mass balance fraud is with quotas. There are many types of quotas in use already.

- **Multiple use licenses** are often issued by regulators that allow a given quantity of restricted goods to be exported or imported. For example CITES appendix II goods allow exporters to self-issue permits up to a maximum licensed quota. Typically managed by one regulator with a separate quota for each exporter.
- **FTAs often prescribe quotas** for specific goods but these apply at country level by one regulator but shared across multiple exporters.
- **Mass balance** can be managed in much the same way by product certifiers.

The VCs status end point that is used for revocation / acquittal of individual items can also be extended for use as a decentralised quota management solution by using license/quota VC status as a draw-down counter.

OK, that was all about trust

There's one last challenge to discuss before we finish:

SEMANTICS

Sorry, what do you mean when you say that?

Sustainability is a global concern but is usually addressed by local entities that follow local standards.

- Some standards are supported by formal accreditation and independent certification frameworks. Others are self-assessed industry consortia or less formal certification frameworks.
- The International Trade Centre (ITC) has assessed over 300 sustainability standards and has mapped them to a harmonised vocabulary – you can see their excellent work at https://www.standardsmap.org/en/identify. However the mapping is intended to support producers in their choice of standards rather than for machine interpretation of actual compliance claims.

The core challenge is that the language used by different standards is different and also the thresholds applied are different. A VC that represents a compliance certificate for a specific entity or shipment will include criteria about things like water usage, carbon intensity, etc. But each will use slightly different language when talking about the same thing. A wide scale high volume adoption of traceability and transparency solutions will require machines to understand what these claims actually mean.

Ah, I see, that's what you meant!

Making sense of sustainability claims that are made for billions of shipments of millions of different products against thousands of different sustainability criteria will require machine automation. It's likely that two kinds of artificial intelligence tools will be used.

- **Semantic web ontologies**. These are standardised reference vocabularies that provide harmonised terms for sustainability criteria and allow every regional standard to map their criteria to the harmonised vocabulary. In this way a machine can read the claims in a VC and use the ontology to map them to the harmonised language. UN/CEFACT has published an early draft harmonised machine readable web vocabulary based on ITC standards mapping work. See https://vocabulary.uncefact.org/sustainability/
- **Large language models.** Unlike web ontologies that require humans to define the semantic models that machines can then use, large language models process large amounts of textual data (such as a sustainability standard PDF document) and derive meaning by comparing the words to very large models – for example the entire content on the web. This is how tools like ChatGPT work.

These two technologies are not mutually exclusive. They can be used together. For example large language models can be "seeded" with manually developed sustainability ontologies and then continue to maintain and extend them at scale. This will be a focus areas for UN/CEFACT projects this year.

So what should you do now?

Check out what others are doing

Singapore – TradeTrust https://www.tradetrust.io/

An early leader in decentralised trust and the innovators behind the "paper friendly" QR and the selective redaction protocols that support real scalability across supply chains. TradeTrust is being used in many innovative ways.

Canada – BC Digital trust https://digital.gov.bc.ca/learning/case-studies/energy-mines-digital-trust-pilot/

A great example of a regulator that has understood the power of digital credentials to release innovation. BC is acting as a trust anchor to assure the integrity of sustainability claims from the critical raw materials sector.

USA – SVIP https://t.ly/LJj5

The US department of homeland security (DHS) was one of the first to realise the potential of digital and has funded vendor interoperability testing which has ensured that we have several commercial and open source software choices.

EU – DPP

The EU has already understood that the Digital Product Passport is best implemented as a Verifiable Credential that can hold manufacturers to account. When supported by evidence from chained traceability and conformity VCs, the DPP is likely to be a world-leading exemplar of how regulators can act to ensure that sustainability is in a race to the top.

GS1 https://www.youtube.com/watch?v=iDkANArgdKI

The GS1 Global Trade Identification Number (GTIN) is the identifier of almost all manufactured products in the world. GTINs as barcodes or QR codes will play a critical role in the digital-physical link solution described earlier. Not only that but GS1 is a trust anchor that can provide verifiable evidence that a manufacturer really is the owner of a product GTIN.

And many more examples.

Start issuing verifiable credentials!

Where are your blue dots?

Governments
- Any agency that issues certificates, permits, licenses, or registrations of any kind should do so digitally.
- Identity providers should link DIDs to national citizen & business identity
- Trade single windows are blue dots. Don't even try to build "regional" windows – just exchange VCs through holders.
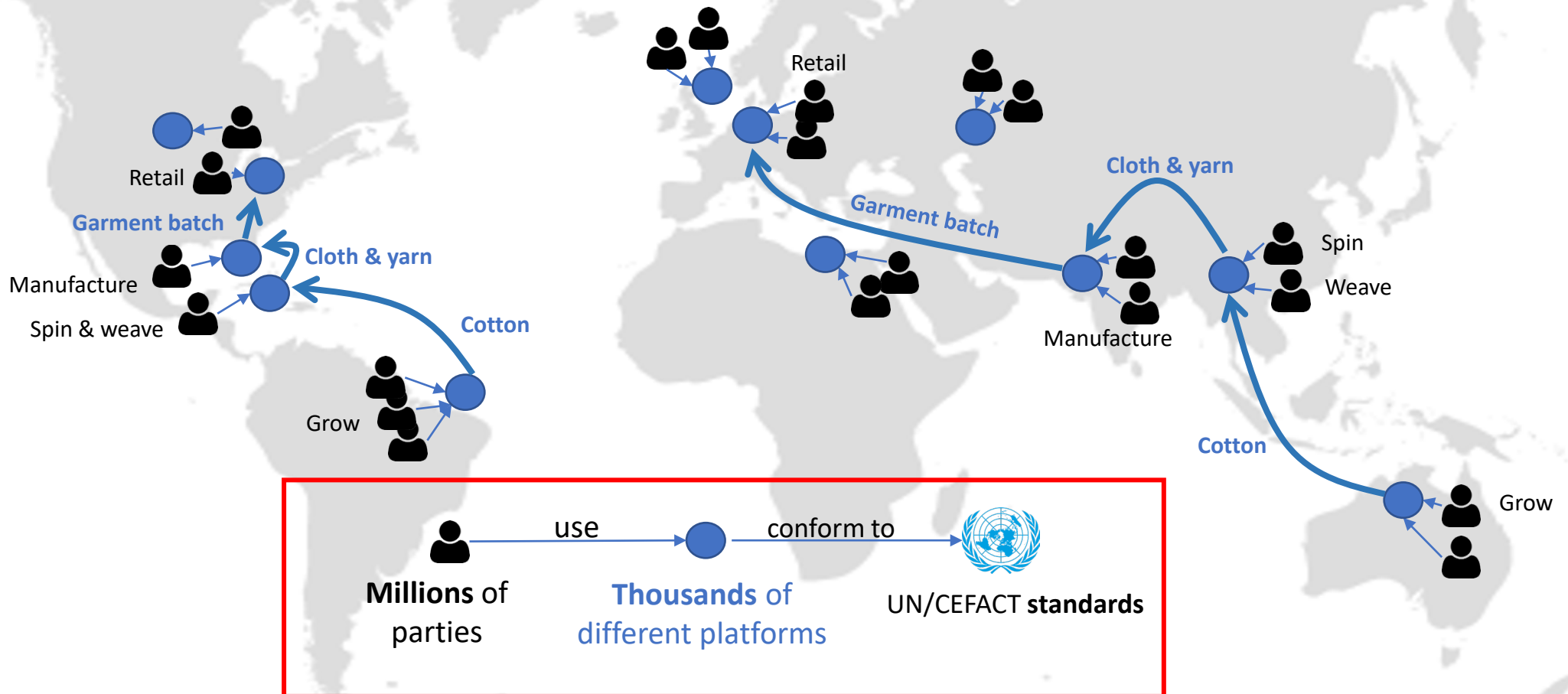
Industry
- Accreditors and certifiers are top of the priority list to issue VCs to support verifiably sustainable supply chains.
- Commercial platform operators can issue trade documents like invoices and waybills as VCs so that your customers can provide high integrity documents through their supply chains.

- **Simple change management.** The subjects of your issued documents will see the same thing they always have – just with a special kind QR in the corner that links to the digital credential.
- **Empowering innovation.** You'll be empowering your clients or constituents with digital trust that they can leverage in all kinds of innovative ways – especially if you are a trust anchor!
- **It's not that hard.** No change to business processes, no new IT systems, just plug VC issuing / verifying tools on to your existing systems & processes.

Decentralisation is good but needs standards.

UN/CEFACT's mission is to provide those standards.

Millions of parties → use → **Thousands** of different platforms → conform to → UN/CEFACT **standards**

Here's what we have so far

https://unece.org/trade/traceability-sustainable-garment-and-footwear
Provides the business requirements and detailed traceability and transparency data models that supported the world-leading work of this team.

https://vocabulary.uncefact.org
Provides the JSON-LD semantic vocabulary for the claims to put into your VCs. Use this vocabulary so that others can understand the meaning of your claims.

https://test.uncefact.org/vckit
Is an open source VC issuer & verifier that is free for you to use. Alternatively you can use any other software so long as it is interoperable.

https://unece.org/sites/default/files/2022-09/WhitePaper_VerifiableCredentials-CBT.pdf
A white paper that describes much of the material presented today in more detail and with specific recommendations for policy makers.

Some new projects that may interest you

CRM sustainability & resilience.

https://uncefact.unece.org/display/uncefactpublic/Critical+Minerals+Traceability+and+Sustainability

Building on experience from the Textile & Leather traceability work and guided by the principles in the VC white paper, this project will deliver the digital standards to support both sustainability & resilience in the Critical Raw Materials sector. It will also cover areas such as trust graphs, physical-digital links and semantic mapping and so will also establish useful patterns for other sectors.

Digital Identity.

https://uncefact.unece.org/display/uncefactpublic/Digital+Identity+Standardization+for+Trade+Facilitation

Confidence in the identity of supply chain actors and the goods they exchange is fundamental to establishing trustworthy sustainability claims. This project will develop a white paper that provides best practice guidance on verifiable digital identity for entities and the subjects of their claims.

UNECE recommendation #47 – "Nowhere to hide"

Building on UNECE Rec#46 which defined standard processes and data structures for textile & leather traceability & transparency and guided by principles in the VC white paper, this new recommendation will provide guidance for nations on scaling traceability, transparency and trust in supply chains so that unsustainable practices have nowhere to hide.

And finally a special call-out for Australian participation

I've got the stage and I'm Australian so please forgive this indulgence..

ABF and the DVP	Australian Industry
The Australian Border Force (ABF) is implementing a Digital Verification Platform (DVP) that seeks to improve both facilitation and compliance outcomes for cross border trade. ABF is keen to run pilots with other nations for use cases like • Certificates of Origin as VCs • AEO mutual recognition using AEO identity VCs • Natural business documents (invoices & waybills) as VCs to increase compliance & efficiency. • CITES permits as VCs • Agri-food safety documents such as fumigation & phytosanitary VCs • Any other cross-border VC use cases you'd like to test with Australia.	Australian Industry is waking up fast to the opportunity to add digital integrity to verifiably sustainable products. • NATA and JAS-ANZ, our national accreditation bodies have delivered a national platform (au.conformity.id) for product conformity certificates and are keen to use VCs to allow this data to be portable & verifiable across borders. • An Australian Structural Steel Certifier will be assisting steel industry to issue steel certificates and seeks importing/exporting economy partners. • The Agri-food industry and Mining Industry are working to establish mechanisms to map Australian credentials to things like the EU DPP.

Please contact me if you see cross border collaboration opportunities!

Thanks for listening.

Questions?

steve.capell@gmail.com