Securing Digital Assets

Ian Taylor

- CEO and Cofounder at SIMBA Chain
- Full research professor of Notre Dame (on leave)

SIMBA

UNIVERSITY OF NOTRE DAME

Gridlab Workshop.
20-22 Dec, Zakopane, Poland

Outline

1. Background in DIDs/VCs
2. Using DIDs/VCs for data
3. RDF and Graph DBs for Provenance
4. Use Cases
    a. Anti counterfeiting
    b. Air Force and Supply Chain
    c. Coffee Traceability

SIMBA Chain

Incubated at the University of Notre Dame in 2017 after winning a DARPA grant, SIMBA Chain has grown to be the trusted name in decentralized data exchange in Government and Enterprise.

Founders are Jarek, myself, and Joel and Gary Neidig.

SIMBA allows for secure, verifiable and access controlled data across any system.

But SIMBA started out as a simple API for smart contract based applications, which is what Gridlab tried to do for Grid applications...

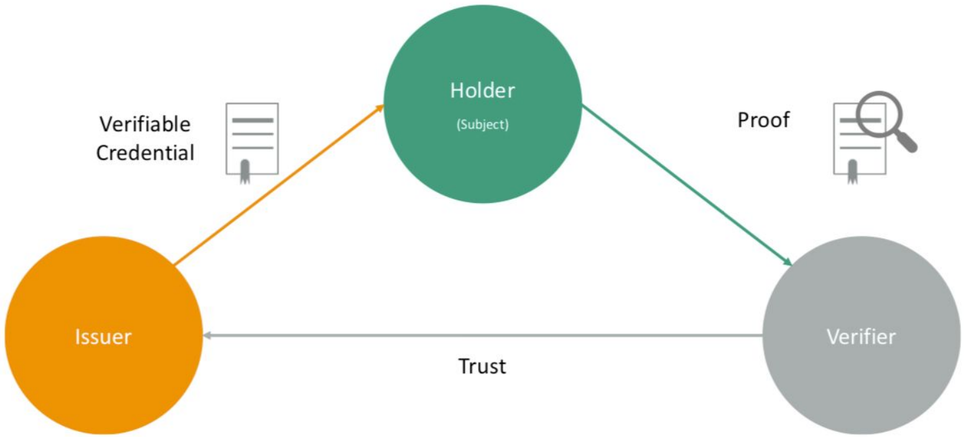
SECTION ONE

Background in DIDs/VCs

01

DIDs and VCs

- We use **Decentralized Identifiers (DIDs)** to create identities for people and Data
  - DIDs are resolvable - like web address (URL) e.g. did:btcr:abcdefgh12345678
  - A DID has public/private keys associated with it, used to prove ownership and secure exchanges of information
- **Verifiable Credentials (VCs)** are used to issue digitally signed documents
  - Credentials provide proof of something - a qualification, access control, an age, etc.
  - If the Verifier trusts the Issuer, then all checks out
- A **Verifiable Presentation** involves an exchange with a verifier where a presenter (DID VC owner) presents a VC, along with proof that they are the owner of the DID



- DID spec is a W3C standard: https://www.w3.org/TR/did-core/ and VCs are https://www.w3.org/TR/vc-data-model/

SECTION TWO

Using DIDs/VCs for data

02

SIMBA

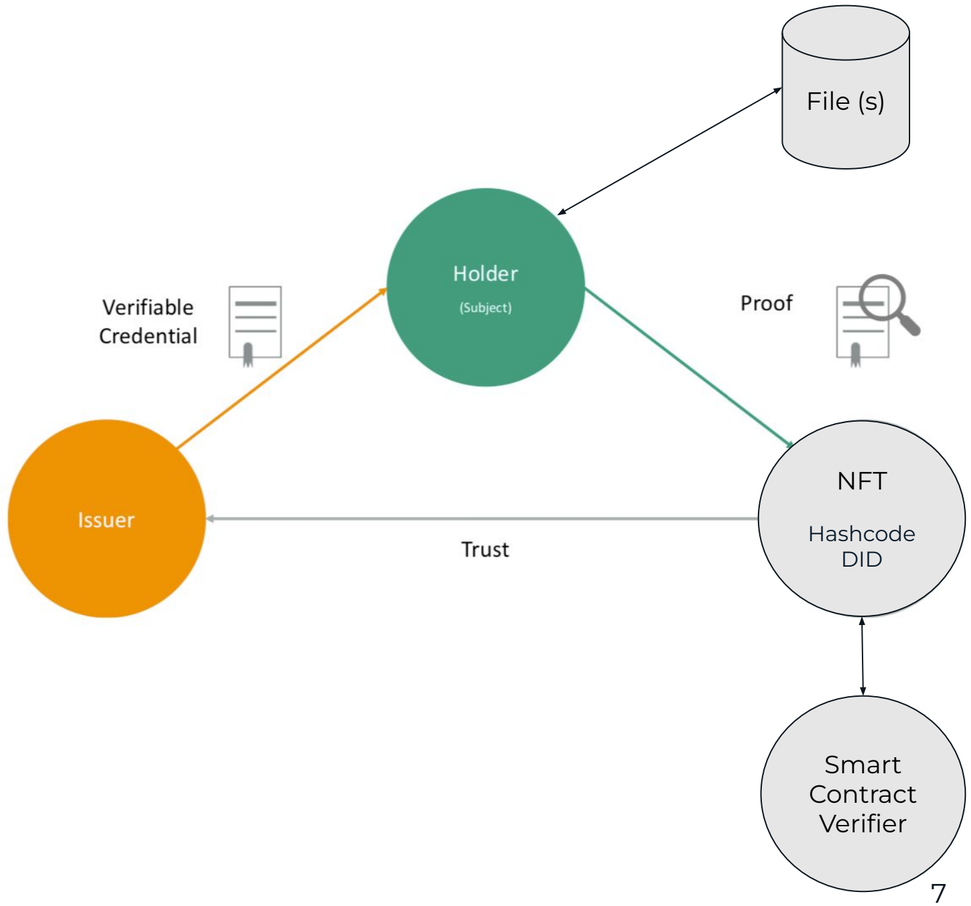
CHAIN OF TRUST

DIDs/VCs for Data

Secure mission critical data exchange across systems/ organizations.

- SIMBA marries the power of decentralized identifiers (DIDs) and verifiable credentials (VCs) with the security assurance of NFT transactions.

- SIMBA's **verifier is coded as a smart contract** accessible from an NFT:
  - Contains a content based pointer to the data
  - Data can be stored off chain
  - Non repudiable - access control cannot change
  - NFTs are issued a DID - VCs can be issued to that NFT, representing that data
- VCs can **grant controlled access** to the data for specific stakeholders, matching against policies defined in the NFT
- VCs can also **assert verifiability** to the data i.e. a third party can verify the data is accurate



Trust and Differentiation

Broadly

- Lack of trust between participants
- Requirement for standardization in the protocol/formats
- Technical complexity
- Cost

User Specific

- Technical expertise and infrastructure required
- Focus on creating new business models
- Regulatory and compliance concerns
- Lack of Interoperability
- Required ecosystem traction

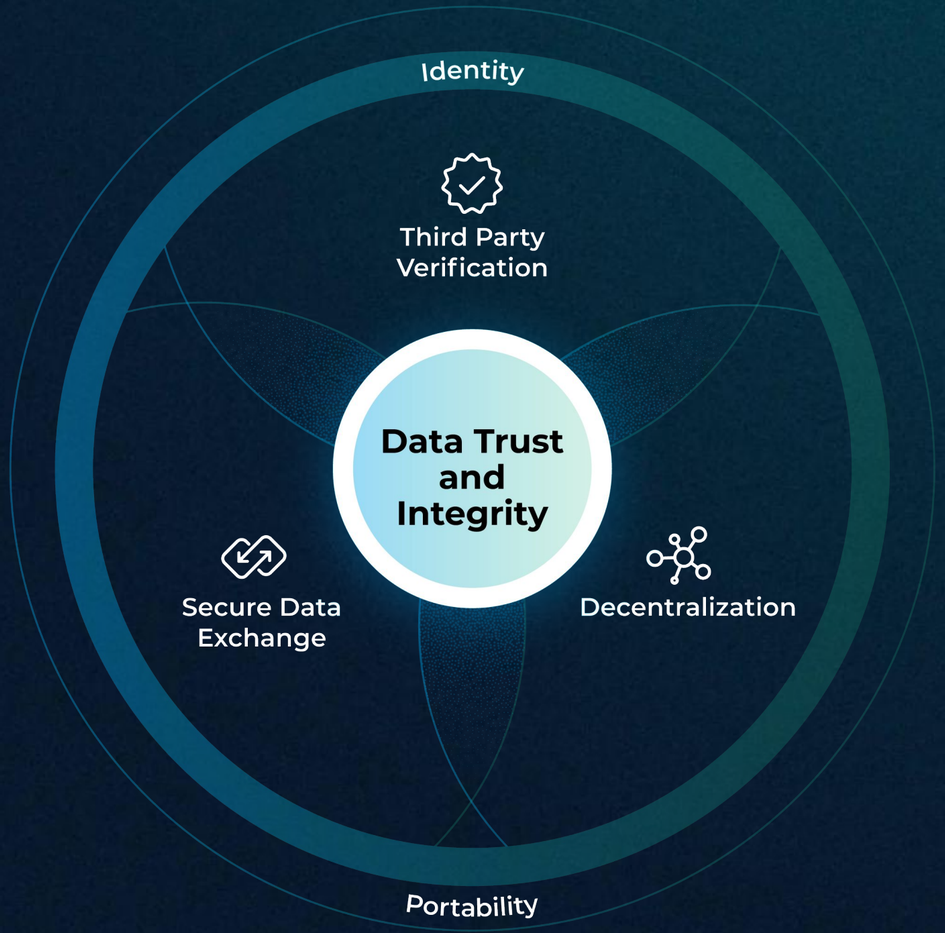
Broadly

- Facilitated trust between participants
- No need for data standardization
- Reduced technical complexity
- Lower Cost
- Incentivized Participation

User Specific

- No need for Technical expertise or infrastructure
- Focused on solving business problems
- Codified Regulatory and compliance procedures
- Interoperable by design
- No required ecosystem traction

Enables



A comparison: other data sharing implementations versus SIMBA

SECTION THREE

RDF and Graph DBs for Provenance

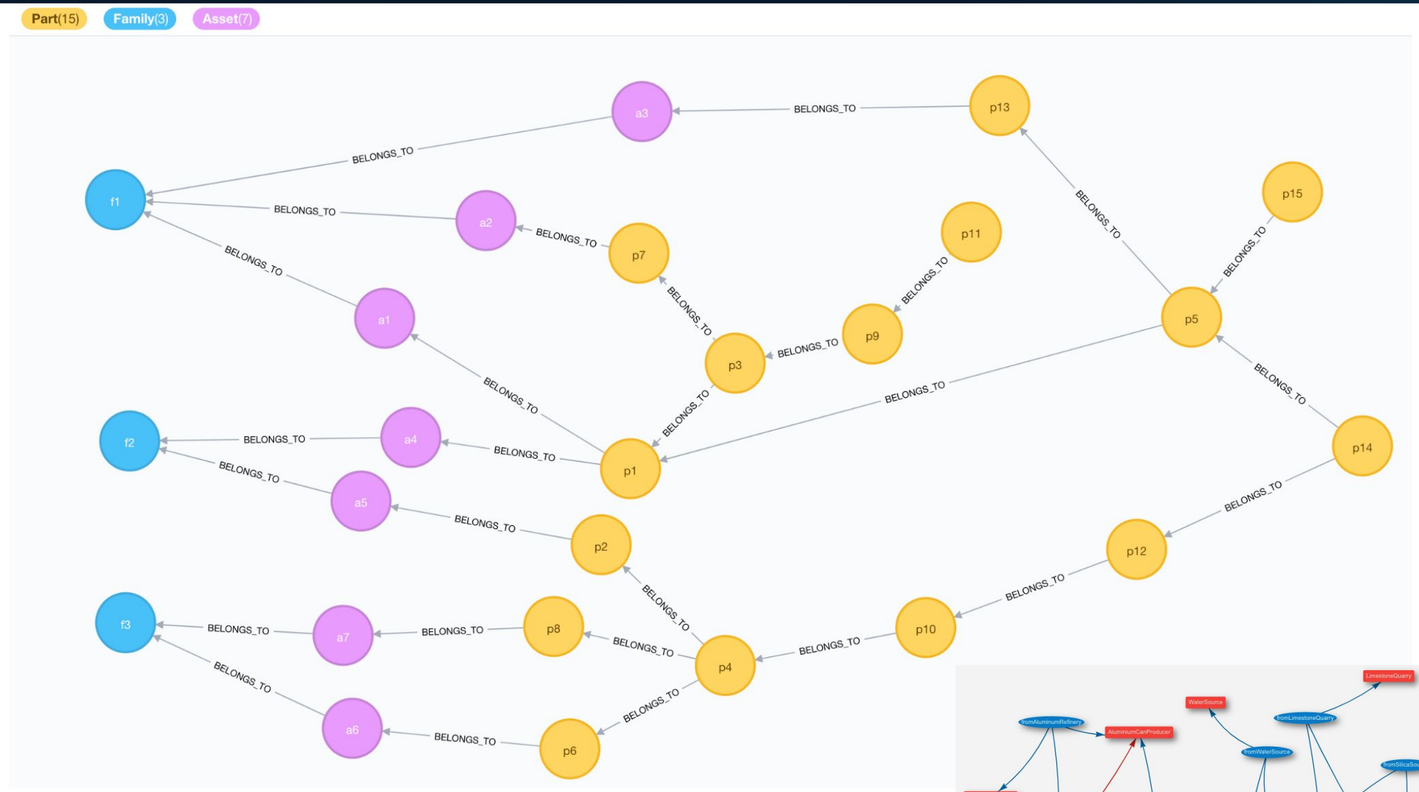
03

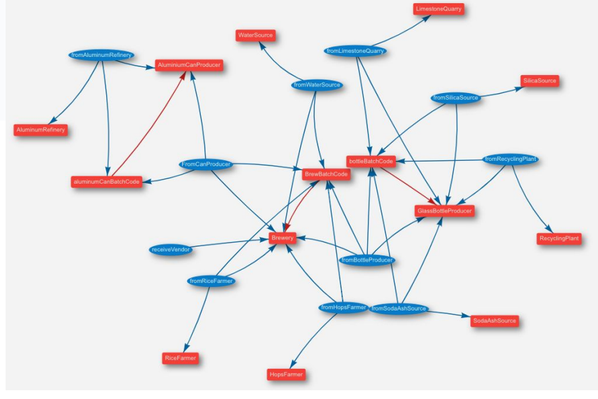
Web3 Version of NFTs

- Many NFTs are part of a game (e.g. CryptoKitties, Bored Apes)
- Or for selling images or music (Euler Beats)
- They are rarely used to represent real-world assets
- Or relationships between those assets

Our Version of NFTs

- NFTs uniquely represent digital assets like data files, IP usage
- Or physical assets, using feature prints, and tracked through numerous secondary sales
- Or to represent a **Bill of Materials (BoM)** - a list of parts and assemblies.
- Each assembly contains another BoM, and so on
- Complex relationships across different suppliers in the supply chain
- We developed the asset graph model to automatically collect such relationships





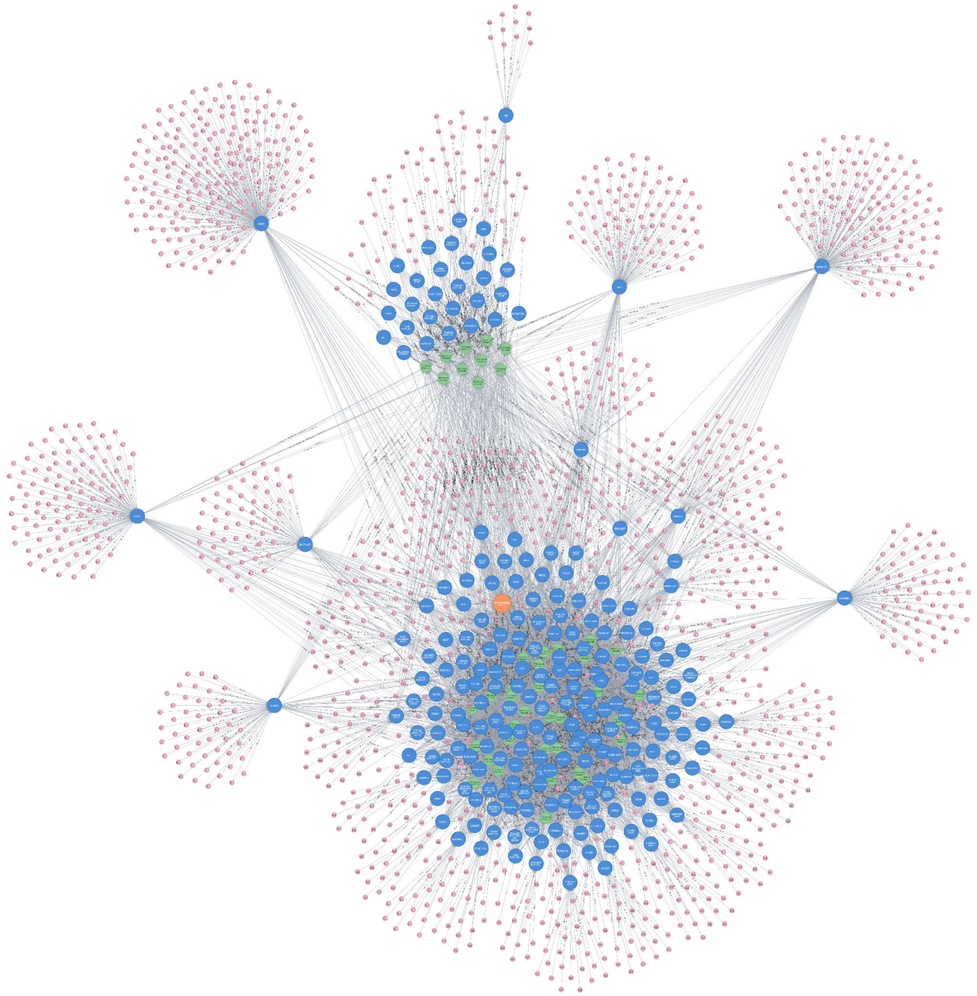
Provenance of applications?

- Prior examples, **like The Graph**, focused on curators building schemas and using those to index data
  - Using **GraphQL**
  - Very **restricted** by GraphQL on what you can represent
- We've focused on **Graph DBs** and **RDF**, which are **subject-predicate-object** triples, to express descriptions of resources e.g. inter NFTs relationships and state changes
- NFTs, once deployed could run forever
  - You can change RDF relationships as application is executing

Asset Graph Implementation

Integrating Semantic Web Resource Description Framework (RDF) oriented Asset Triple models with Neo4J graph database

- Extracts transactions from chain and creates binary relationships between entities represented in transactions.
- Adds these relationships to an evolving graph.
- Provides an open-world, schema-agnostic view of events on chain.
- Provides the basis for analytics (E.g. STRATFI)



SECTION FOUR

Use Cases

04

Existing Defined Use Cases

	Intended Use Case	Access Control	Attribute Based Access Control	Verifiability	Work In Progress
Secure Collaboration with Suppliers	Enable suppliers to collaboratively share IP protected data e.g. design files.	✓	✓	✗	✓
The Sharing of Personal Information	Enables secret sharing of PII/other data while maintaining self sovereignty	✓	✗	✗	✓
Third Party Verification / Attestation	Provide access to data e.g. ESG, and provide publicly verifiable transparent claims	✓	✓	✓	✗
Circular Plastics Economy	Enables the recycling of plastics into crude oil for reuse	✓	✓	✓	✓
CUI – Controlled Unclassified Information	Implement controls needed to share CUI data - record who had access to what and when	✓	✓	✓	✗
Maintenance, Repair and Overhaul	To provide an provenance trail for MRO activities to create a continuous auditing capability	✓	✓	✓	✗
Controlled Supply Chain Visibility	Suppliers to share data on a common network but maintain data self-sovereignty	✓	✓	✗	✓
Authentication of Physcial Items	Enable counterfeits be positively identify using physical characteristics of parts	✓	✓	✓	✓

SECTION FOUR

Air Force and Supply Chain

04a

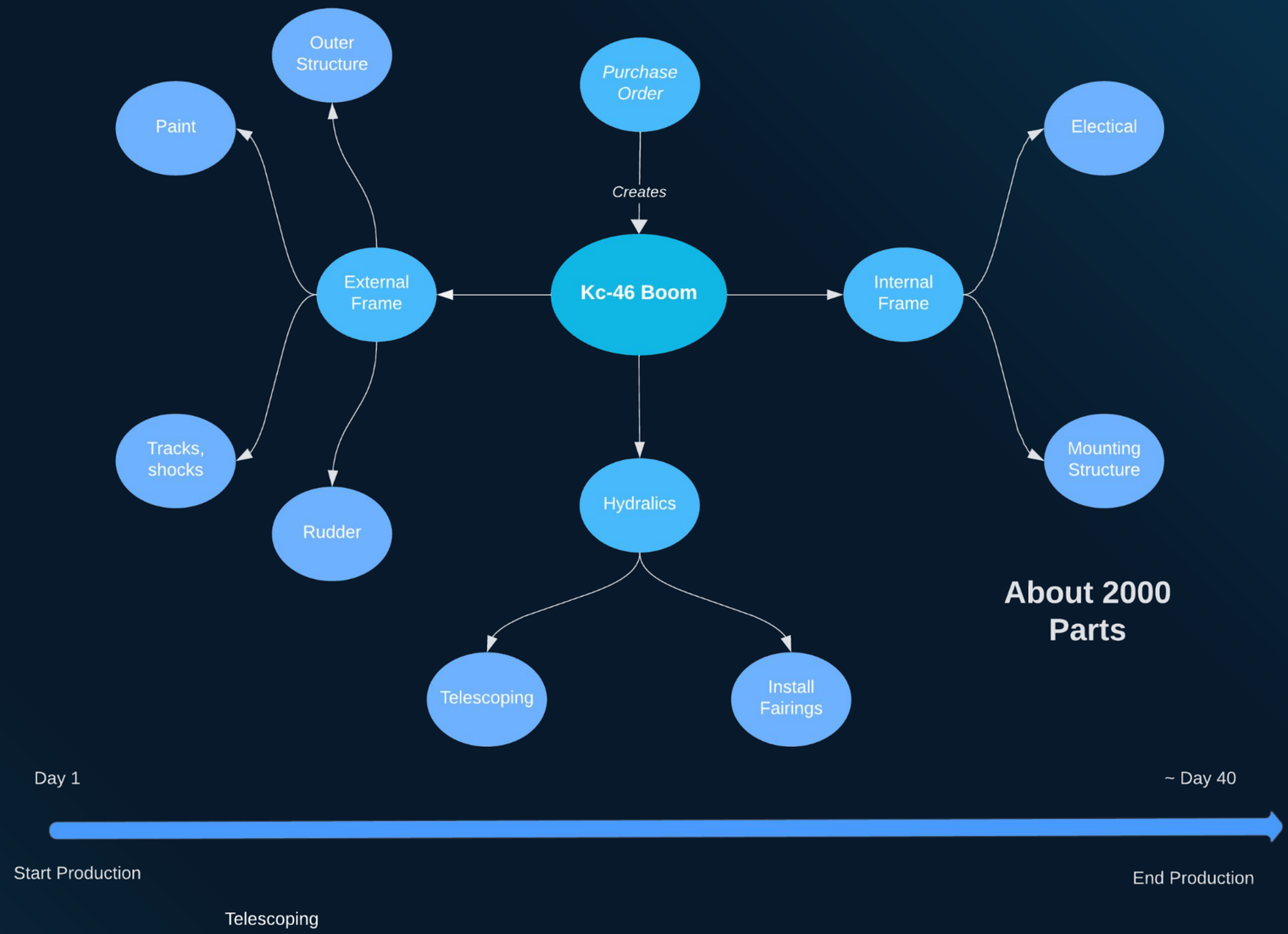
Air Force Earth 616 STRATFI Program

- Provide a **PoC Secure Distributed Ledger Technology** based environment to give near real-time visibility and traceability.
- **Digital assets need to be secured** for parts and data from an interconnected Tier1 <> Tier2 and Tier1/Tier 2 > Air Force.
- Initial support will be for **KC-46** production systems, but can extend to other platforms.
- PoC hosted in an **IL-5 secure environment** and made available to customers across the Department of Defense (DoD).
- **Primary Program Goal:** Support scenario-based predictive modeling using DoD connected data stores in a secure environment, enabling DoD entities to utilize common resources to complete the shared goal of ensuring the warfighter’s ability to complete their mission.
- **Funding:** 15.6M, SIMBA lead, 5 subcontractors.

The Pegasus KC-46 Aircraft

KC-46 Boom

- Opposite - very high level view of boom
- Data coming in every day from ERP/MES/PLM
- Full visibility into production data
- Details on work performed and how long it took
- Track ERP ordering to sub-tiers
- A full picture of the entire manufacturing process
- Complex relationships



STRATFI Secure Assets

Use Cases:

- Tier1 sharing production schedule with Air Force
- Tier2 sharing production schedule data with Tier1

SIMBA

- Secures assets in IL-5 environment, using NFTs, on-chain and off-chain data with hashcode in the NFT - non changeable and tamper evident
- Provides secure access control for that data
- Dynamic Access Control verification is performed in the NFT and cannot be hacked

SECTION FOUR

Coffee Traceability

04b

SUSTAINABLE COFFEE

- Launched (Oct 2020) to track coffee for 20 farms in Tacana using SIMBA Chain and Quorum
- In partnership with University of Notre Dame

KEY POINTS

- They wanted to rewire the supply chain to drive more revenue to those communities
- Toks promotes sustainability practices, working directly with cooperatives of small farmers
- They needed proof by tracking beans from farms to ~220 Toks restaurants
- Eliminate counterfeit coffee

COFFEE TRACKING APP

FARMER

Divides coffee in ”Good” and “Bad” coffee grades. Each batch is a minimum of 100KG

COOPERATIVE

Generates 1 barcode per batch for the blockchain and tracks shelled beans

Chiapas

TO DESHELLER

App scans barcode and add transaction to track beans to the desheller

FROM DESHELLER

App scans barcodes and tracks the returned deshelled beans

App Transaction

TO ROASTER

Scans barcode to identify batch and adds transaction when deshelled beans are sent to roaster

ROASTER

Scans barcode and tracks arrival of beans and tracking across the roasting process

Mexico City

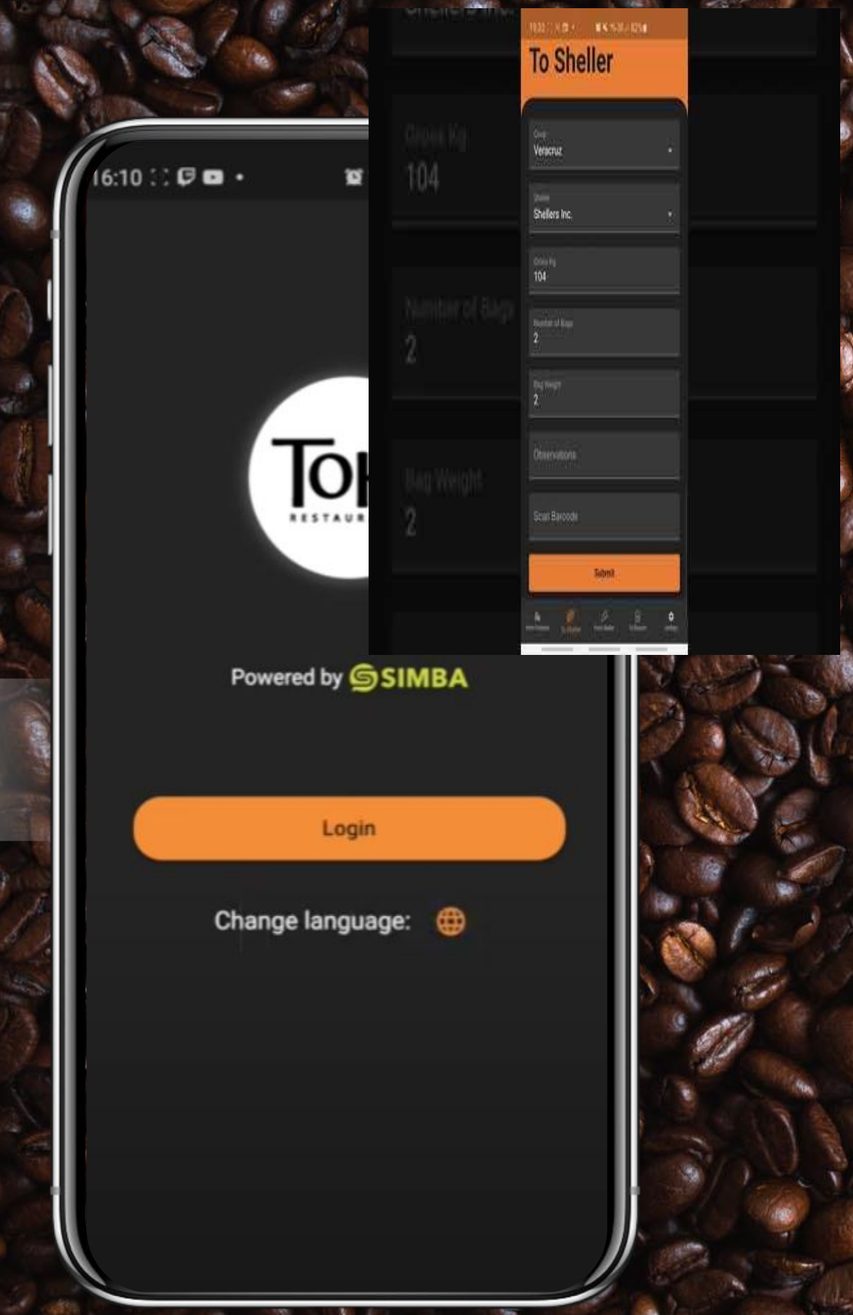
WAREHOUSE

Bagged/boxed beans stored in warehouse

TO RESTAURANT

Boxed beans sent to a restaurant

Toks Transaction



SECTION FOUR

Anti counterfeiting

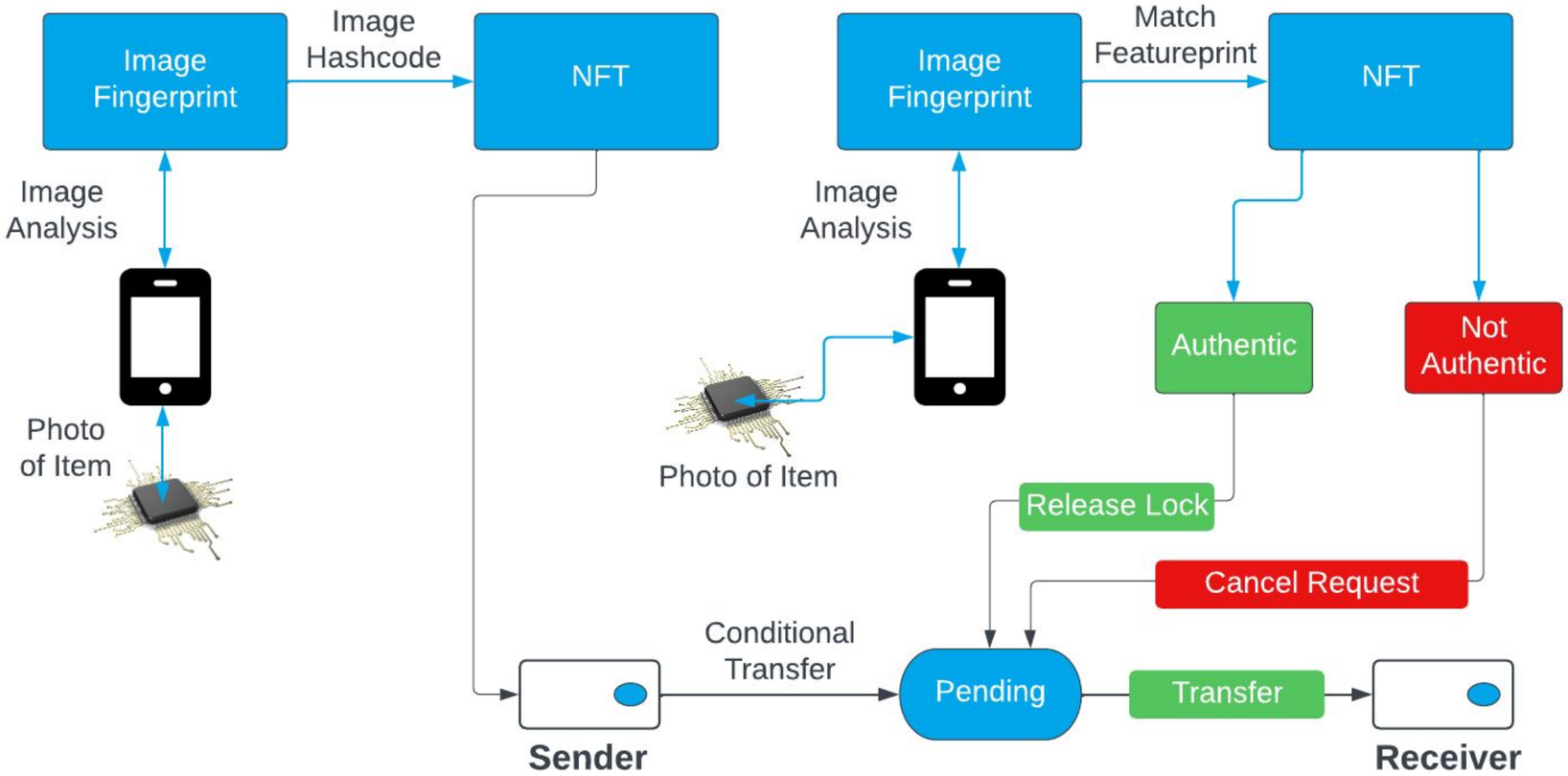
04c

Physical Digital Signatures

- We take a **digital fingerprint** that **uniquely** maps to the **physical item** and **deterministically map** this fingerprint into the NFT
  - The NFT therefore incorporates the unique physical characteristics that uniquely points to the physical item
  - The blockchain transaction is also digitally signed by the user that created it e.g. the manufacturer
- This solution effectively provides a means of **digitally signing physical items**
- And being an NFT, it means that you can use the **standardized NFT transfer** function to **change ownership** of the item as it traverses from manufacturer to customer
- In the same way that a digital signature can guarantee that data has not been changed, we can also prove a physical item has not been changed during transportation
- This approach can eliminate counterfeits because at any point in the supply chain the authenticity of the part can be proven

Transferring NFTs of Physical Parts

- Before the NFT is transferred, it is possible to authenticate the item beforehand
- This provides a way of effectively putting the NFT in escrow before the customer authenticates it and establishes ownership of the part
- If authenticity is not proven then they can reject ownership, providing a way of rejecting counterfeits



Thank You!

Learn more about SIMBA Chain

SIMBA®