Hyperledger Climate Action SIG

On Designing out Waste and Pollution:
Full Disclosure & Accounting of Emissions

"Trust, but Verify"
September 2020

Contacts: Dr. Carsten Stöcker, +49 1520 8930 990, carsten.stoecker@spherity.com

Agenda

1) On Greenhouse Gas Emissions

2) GoO Certification of Electricity

3) Energy Asset Master Data Register (regulated registries)

4) Green Power Purchase Agreements (case for automation)

5) From Green Certificates for EVs for Carbon Credit Trading

6) Retrofitting of Exiting Legacy Infrastructures

7) Green Washing

8) Longer term vision: Circular Cloud

9) Spherity Tech Stack, Wallet and APIs,

Carsten Stöcker

accenture

RWE

WORLD ECONOMIC FORUM

innogy

Hyperledger Climate Action & Accounting Special Interest Group presents

On Designing out Waste and Pollution: Full Disclosure & Accounting of Emissions

Carsten Stöcker
Founder of Spherity GmbH

Online | September 8, 2020 at 8:00 AM Pacific

Born: Average **CO_2 329 ppm** (1973)

(CO_2 expressed as a mole fraction in dry air, micromol/mol, abbreviated as ppm, Source: NASA)

SPHERITY

dena
Deutsche Energie-Agentur

DUBAI CARBON

Abstract

Due to the fact that the vast majority of humans are driven **by greed**, money and individual short term maximisation goals a transition towards carbon neutral, circular systems and the successful implementation of UN SDGs is impossible, unless strict policies frameworks are defined, implemented, monitored and enforced.

Policy frameworks that put a hard stop on the extract-burn-produce-use-dump economy. Policy frameworks that protect vulnerable ecosystems, eliminate greenhouse gas emissions and stop deforestation. Both**, enforcement of circular policy frameworks** and transition towards sustainable supply chain systems need instruments for back-to-birth thing/data/energy provenance and process compliance.

As **provenance** requires identity and verifiable data sets we at Spherity are significantly investing into R&D about energy provenance for climate accounting as well as sustainable and circular identity tech. such tech solutions can only be built upon open protocols that enable network-of-network effects.

Time of my presentation: Average CO_2 414 ppm (CO_2 expressed as a mole fraction in dry air, micromol/mol, abbreviated as ppm, Source: NASA)
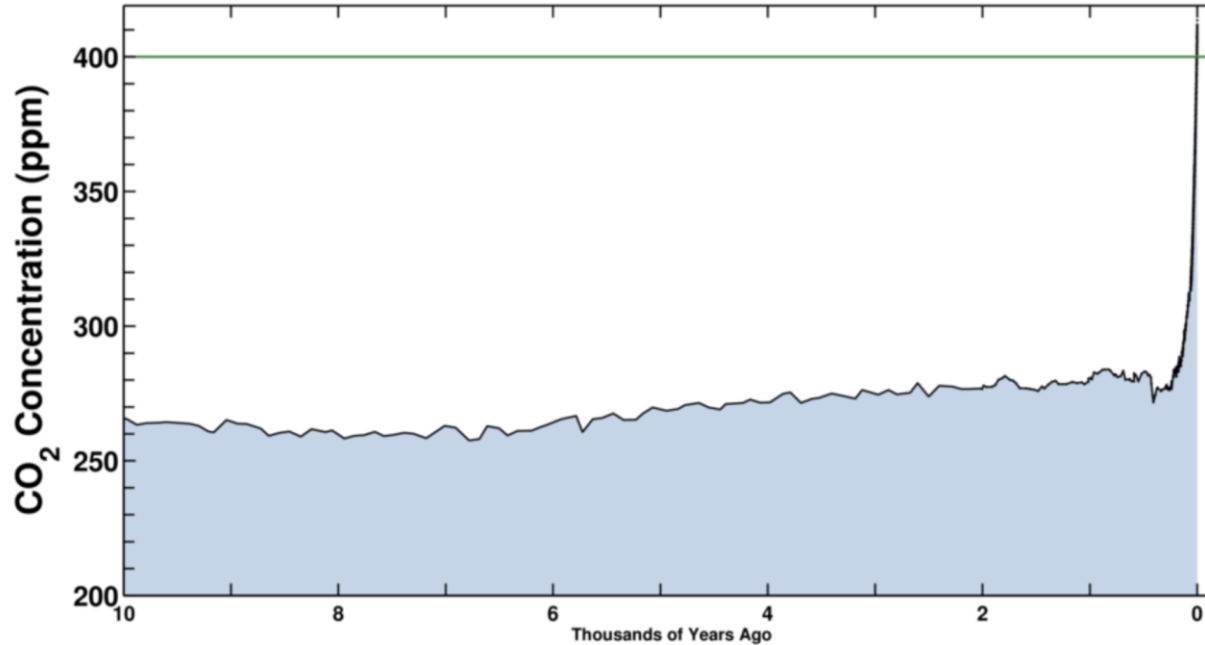
Average CO_2 Concentration over Time

Latest CO_2 reading
May 11, 2019

415.26 ppm

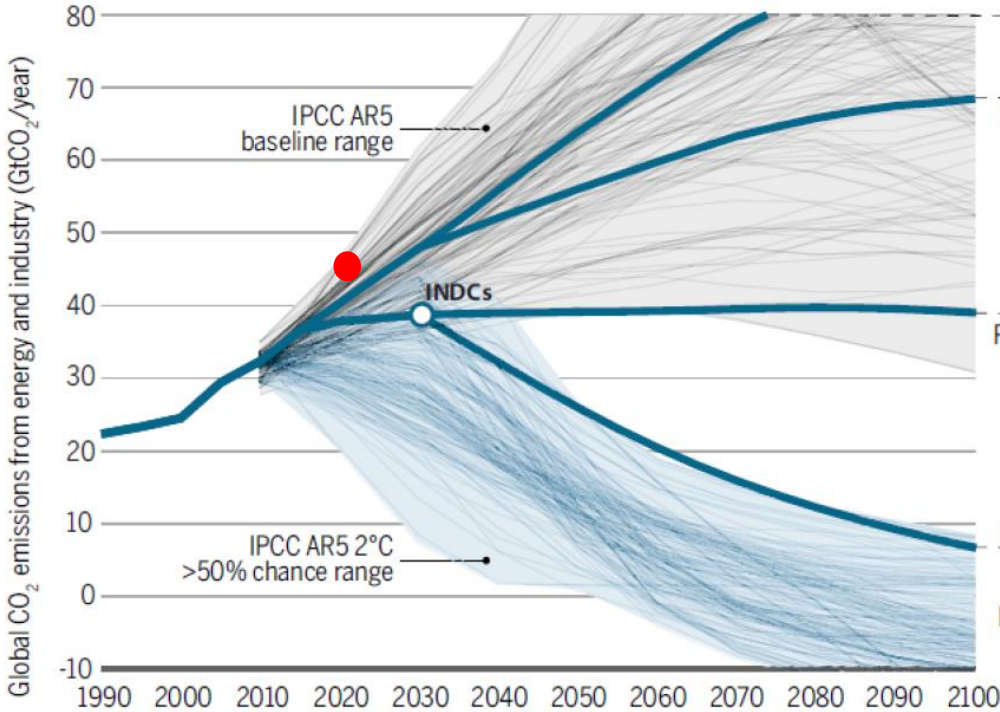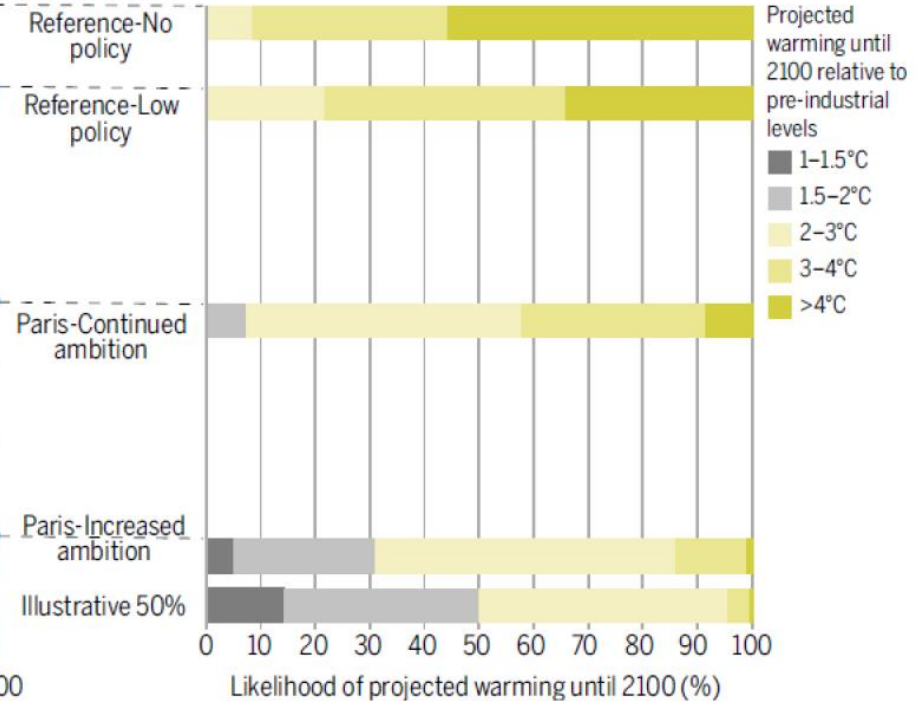**Ice-core data before 1958. Mauna Loa data after 1958.**

SPHERITY

Source: Intergovernmental Panel on Climate Change IPCC, Jae Edmonds, Joint Global Change Research Institute, ICEF 2017

Projections (already outdated)
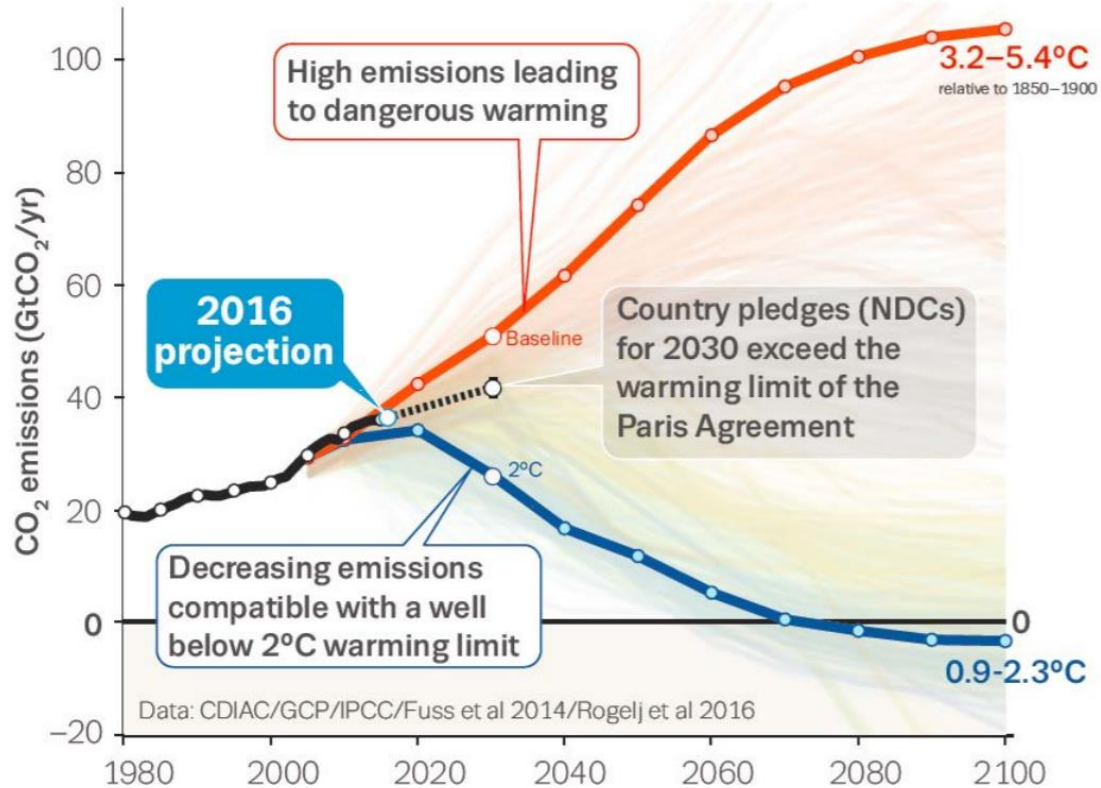
Global Greenhouse Gas Emissions by Economic Sector

- Electricity and Heat Production 25%
- Agriculture, Forestry and Other Land Use 24%
- Buildings 6%
- Transportation 14%
- Industry 21%
- Other Energy 10%
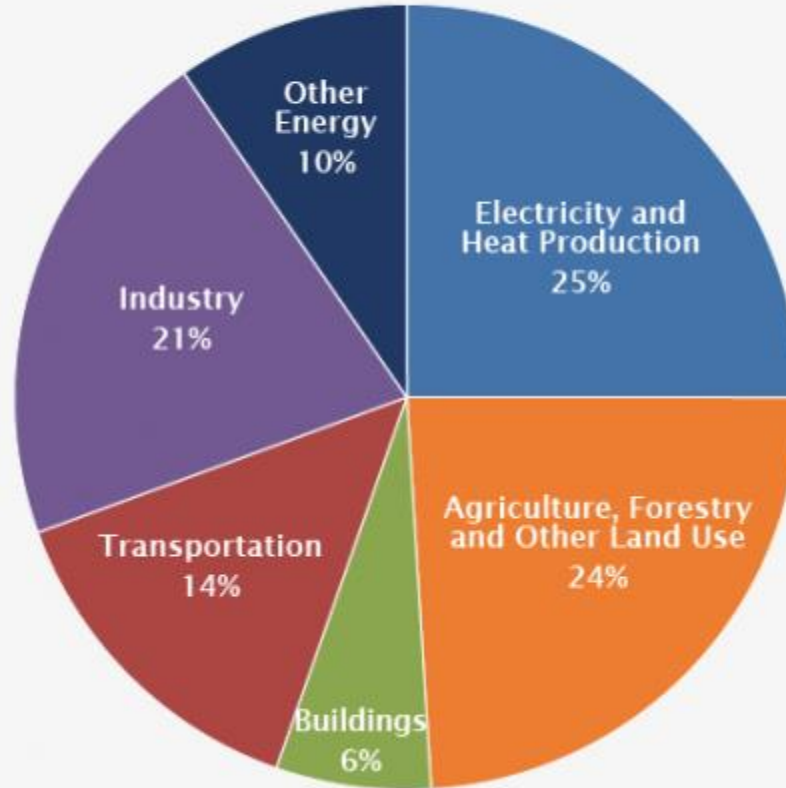
Source: IPCC (2014); based on global emissions from 2010.

Relative Warming Effect of GHG Types

Green House Gas	Warming Effect on the Earth
Carbon Dioxide	1
Methane	25
Nitrous Oxide	298
Chloroflurocarbon-12	10,900
Hydrofluorocarbon-23	14,800
Nitrogen Trifluoride	17,200
Sulfur Hexafluoride	22,800

Source: Intergovernmental Panel on
Climate Change IPCC, 2007

Renewable Energy Certificate Tracking Systems in North America

KEY

- **ERCOT:** Electric Reliability Council of Texas
- **MIRECS:** Michigan Renewable Energy Certification System
- **M-RETS:** Midwest Renewable Energy Tracking System
- **NAR:** North American Renewables Registry
- **NC-RETS:** North Carolina Renewable Energy Tracking System
- **NEPOOL-GIS:** New England Power Pool Generation Information System
- **NVTREC:** Nevada Tracks Renewable Energy Credits
- **NYGATS:** New York Generation Attribute Tracking System (in development)
- **PJM-GATS:** PJM EIS's Generation Attribute Tracking System
- **WREGIS:** Western Renewable Energy Generation Information System
- **No tracking system formally adopted.** NAR allows registration from generators located anywhere in the U.S. and Canada. Other tracking systems may allow registrations from outside their geographic territory.

Revised May 5, 2015

10
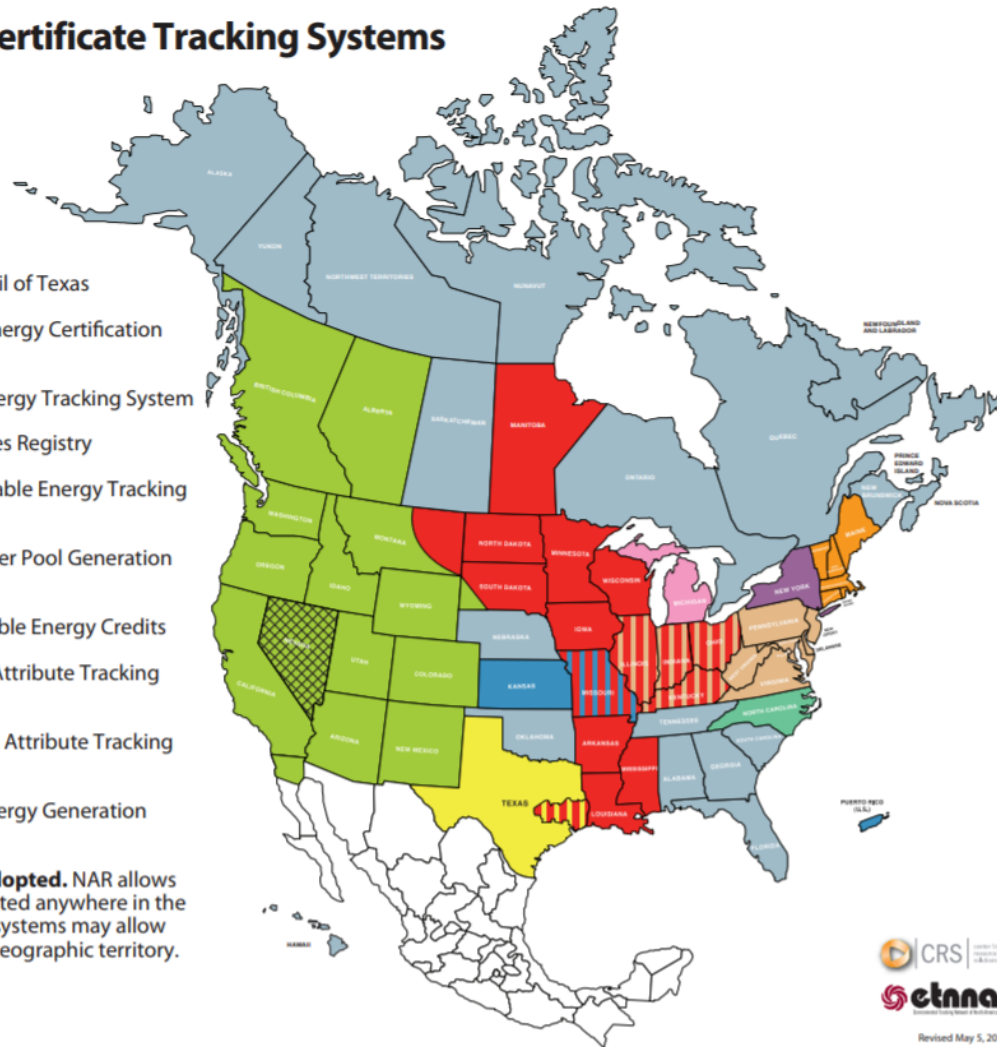
The problem to be solved
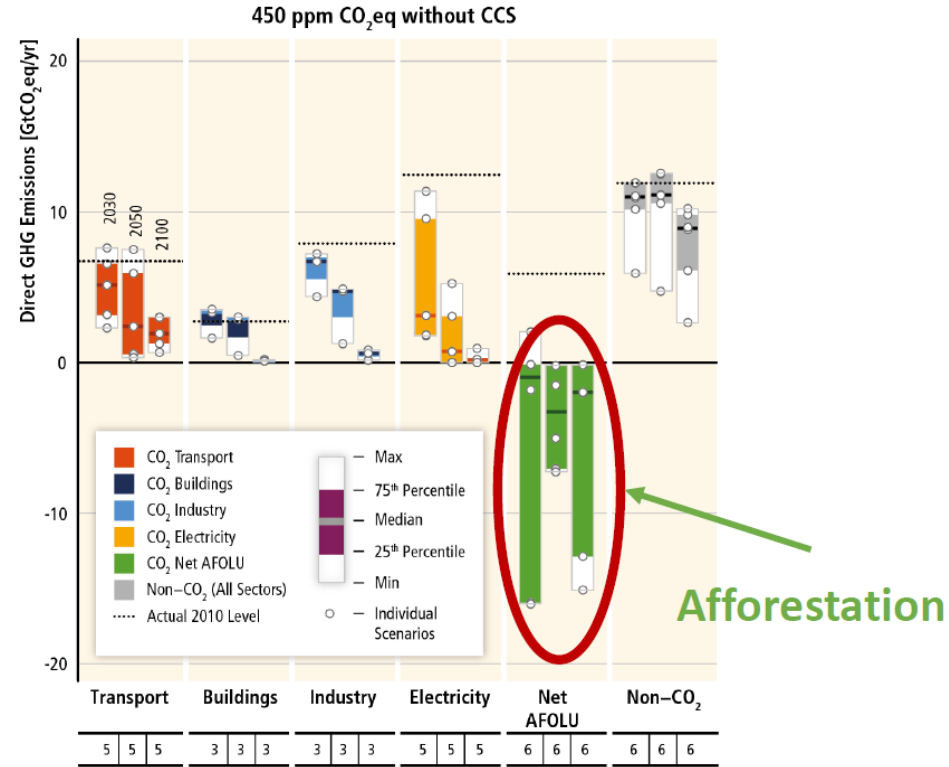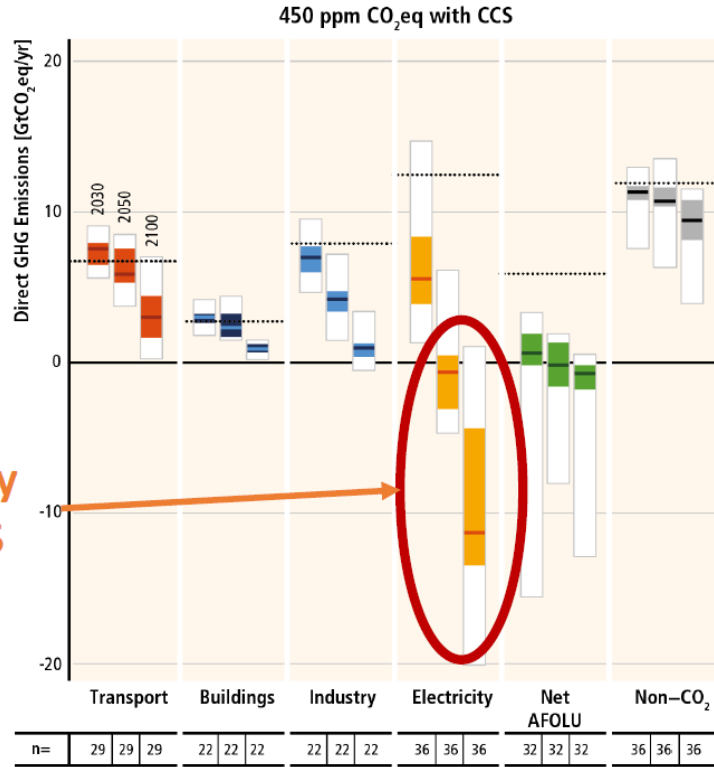
Source: Jae Edmonds, Joint Global
Change Research Institute, ICEF 2017

GoO Certification of Electricity

CERTICIFATION OBJECTIVES[1]

- Providing reliable, secure and **user-friendly** certification of electricity

- Facilitating **full disclosure** in the broadest sense (supply & production, centralised & decentralised, grey & green)

- **Integrating urban**, plant- and asset-specific CO_2 **emissions**

- Providing **real-time** information on the production and use of sustainable electricity

Full Disclosure

Green

P2P Certificate Network

Generation

Consumption

Grey

[1] Source: CertiQ Annual Report 2017
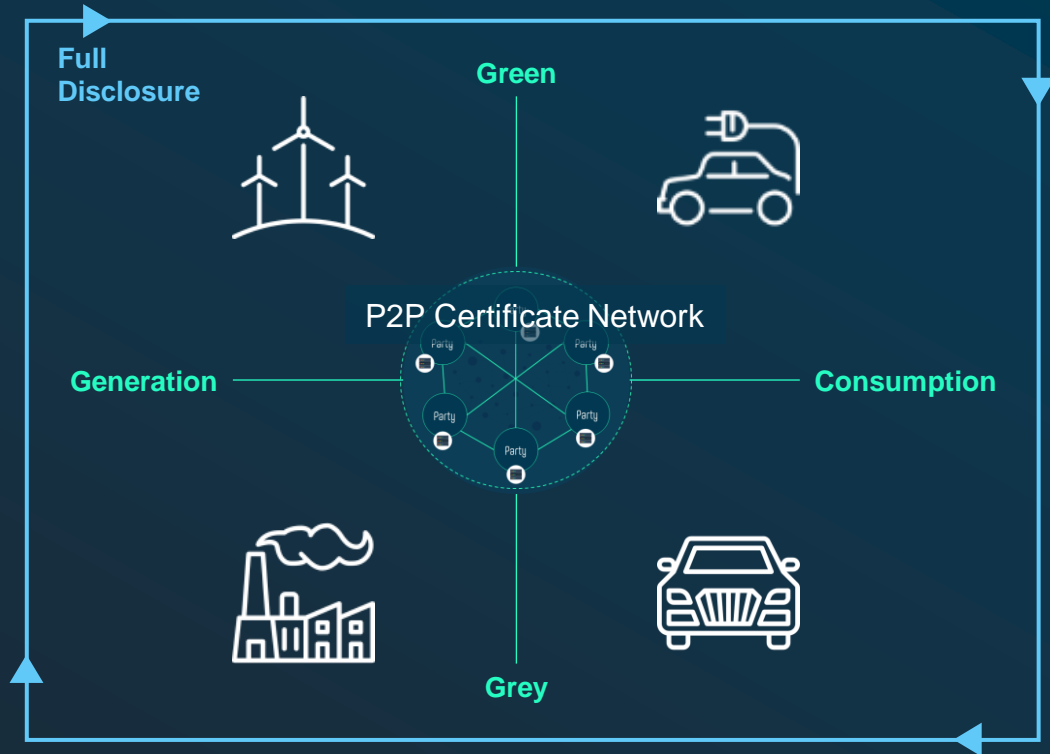
GHG Components

1) Asset Master Data

2) GoOs

3) Applications

Energy Asset Master Data (Consumption, Generation, Emissions, CCS)
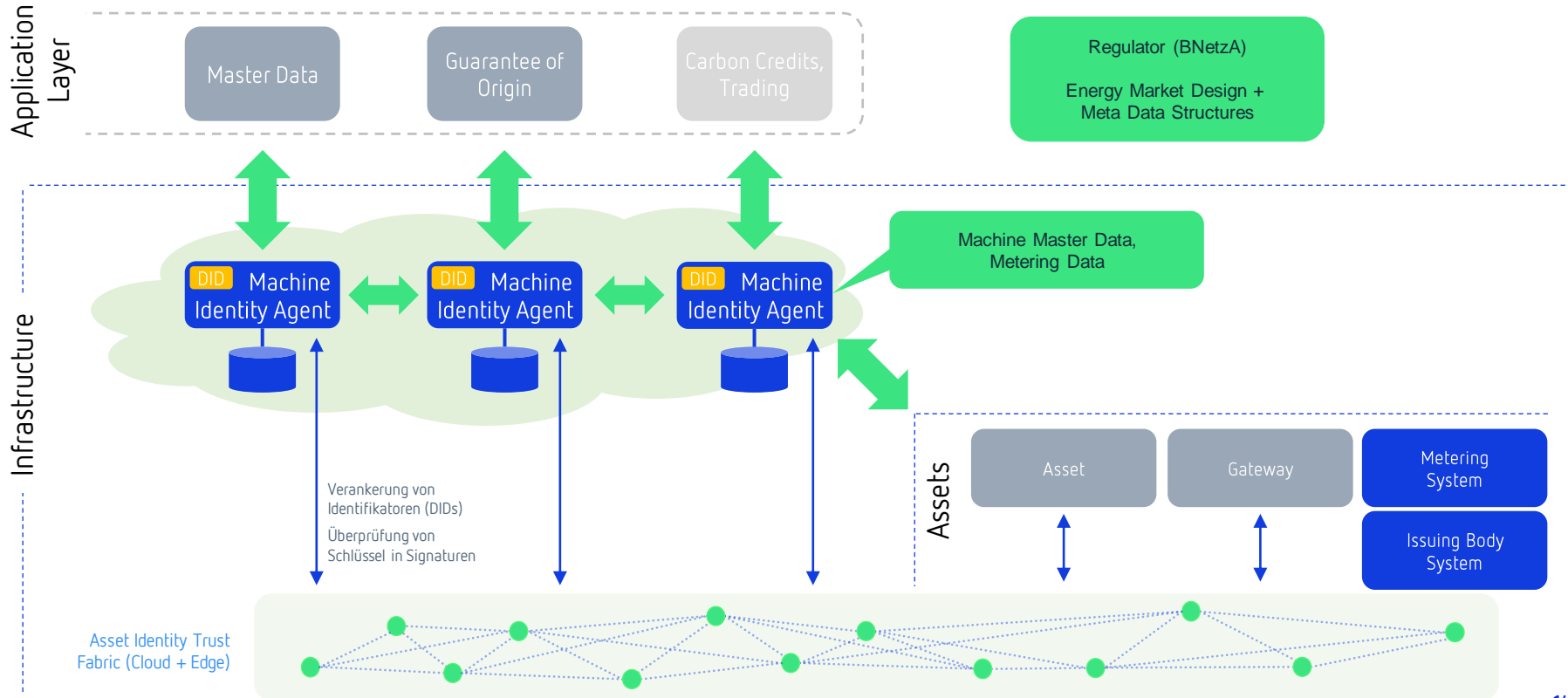
Application Layer

Master Data

Guarantee of Origin

Carbon Credits, Trading

Regulator (BNetzA)

Energy Market Design + Meta Data Structures

Infrastructure

DID Machine Identity Agent

DID Machine Identity Agent

DID Machine Identity Agent

Machine Master Data, Metering Data

Verankerung von Identifikatoren (DIDs)

Überprüfung von Schlüssel in Signaturen

Assets

Asset

Gateway

Metering System

Issuing Body System

Asset Identity Trust Fabric (Cloud + Edge)
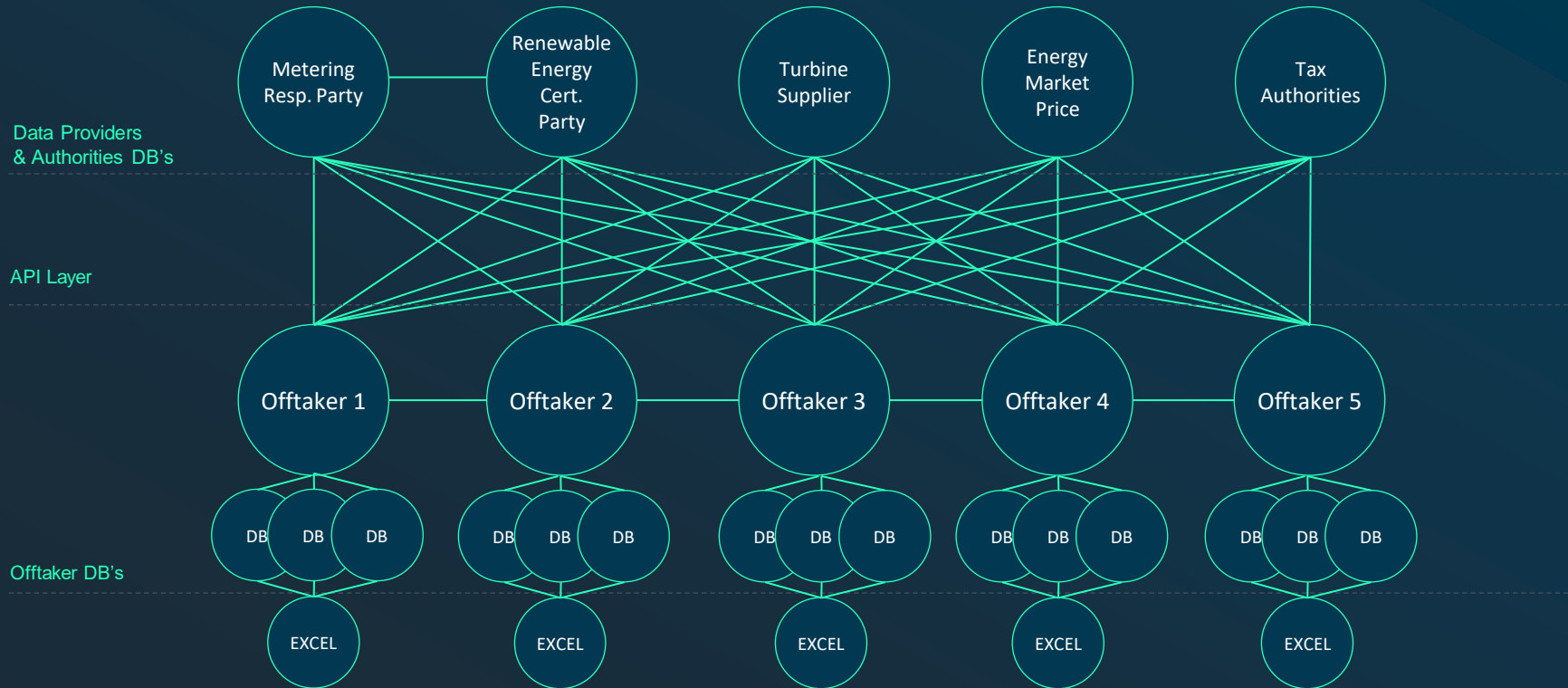
The Spherity PP Solution

P2P Audit Trail Network
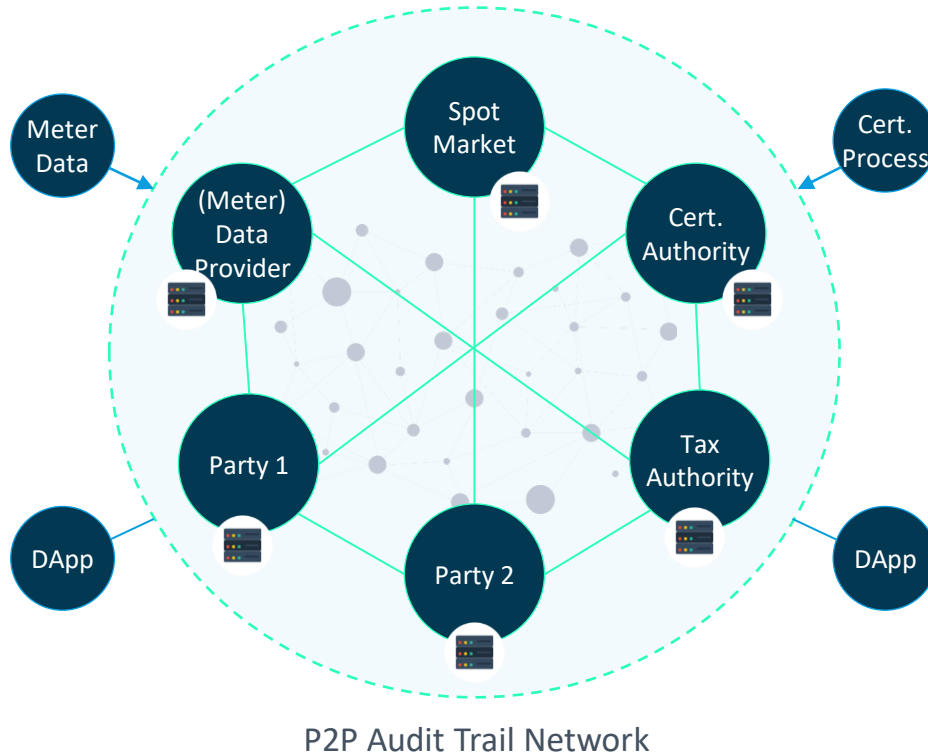
Establish a decentralized shared data environment where each market participant can trust the data's provenance and authenticity.

The trusted data environment connects all kind of market players with the benefit of easily accessible, secure, traceble and immutable data. On top of the shared data environment decentralized PPA applications are built upon a shared audit trail and verifiable data chain infrastructure.

Potential technology building blocks

Decentralized Data Storage	Unique Digital Twinning	Role Based Access Control
DIDs/VCs	Multi Party Computing	Cloud-Edge
On-chain vs Off-chain	Privacy Techonoloy	Renewable Energy Certificates

SPHERITY
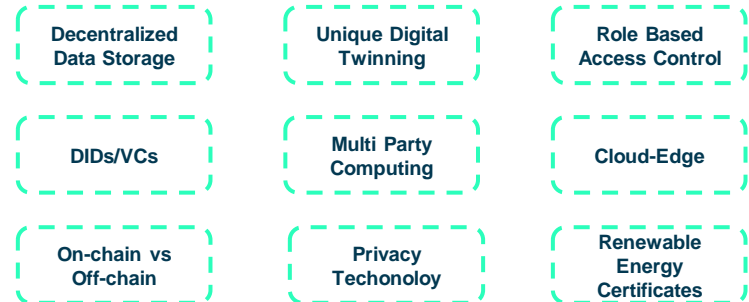
Wind Production Data Clearing Process in NL
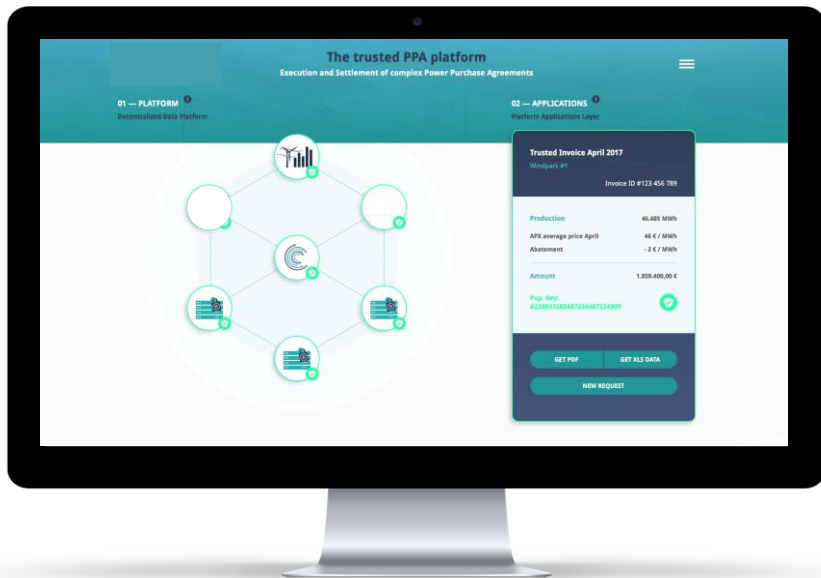
- All relevant data is assigned centrally to a Digital Twin of a Windmill (single source of truth)

- The Digital Twin and the assigned data are stored decentralized in addition to relevant market data

- If permission assigned, stakeholders could see the data assigned to the Digital Twin

- Automated PPA and REC settlement

On Audit Trails

- Data Authenticity (Meter ID)
- Meter Meta (Location, Type of Energy)
- Meter Readings
- Data Hashes (Integrity)
- Timestamps

Audit Trail Data

Digital Twin

GHG Distributed Ledger/
P2P Certificate Network

Public GRID

Public GRID

- Guarantee of Origin
- tCO2e Emission Monitoring
- Energy Certificate Token
- Credit Value
- Secure certificate transfers & trading

SPHERITY
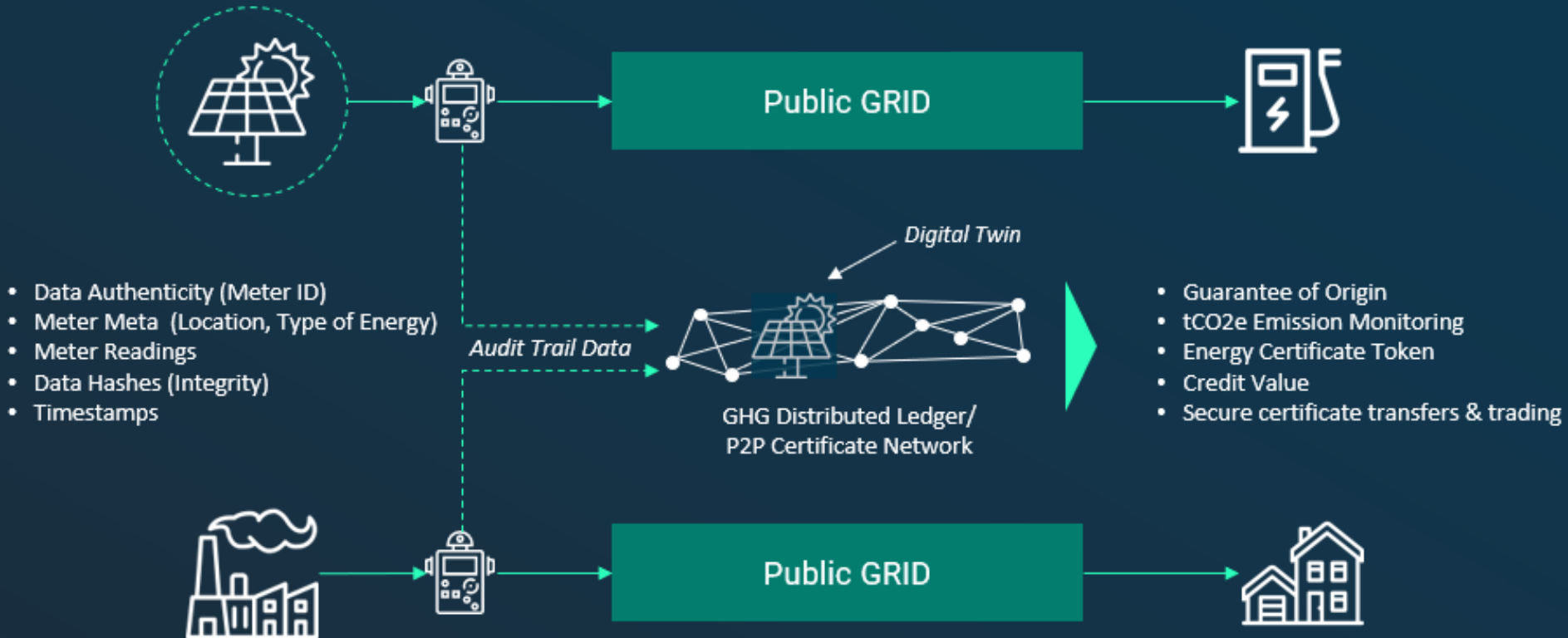
Green Energy *Guarantee of Origin* for EV Charging

P2P Audit Trail Network

Meter Identity, Energy Provenance — **DIGITAL TWIN**

Party · Party · Party · Party · Party · Party · Party

Charge Pole Identity — **DIGITAL TWIN**

Vehicle Identity — **DIGITAL TWIN**

Audit Trail · Audit Trail · Audit Trail

Renewable Energy Certificate — Transformation → LCFS Credits — Ownership Transfer → LCFS Credits — Transfers/Trading

E2E Audit Trail Certificates of Origin

EV Charging & LCFS Credit Generation Process

SPHERITY

A Generation/ Energy

B LCFS Credit Generation

C Monetization of LCFS Credits

PV → Public Grid

Energy +
Guarantee of Origin

PV → EV-Charger

On-premise

Owned
by Utility/
Other Entity?

Person Account → Zero-Emission Credits are generated

Car →

- Time Stamp
- Guarantee of Origin
- Quantity in kWh
- Credit Value

Any LCFS Credit
Substitute?

3rd party
(e.g. Walmart's EV Charging Equipment)

Trading Mechanism
(entities allowed own/trade LCFS credits)

Transaction Platform

What kind of platform is required?

? **Who can be authorized to trade LCFS credits?**

Charging blockchain ledger

1 Register with Charging Station

Tied to car and/or person

2 Start Charging
- Register Time stamp
- Charger Property (PV or not)
- Car Property
- User/Customer

Determine LCFS Factor
- Source
- Time

Repetitive Process

3 Collect Source Data
- Store % or kWh generated per source

Frequency?
Seconds/ Minutes/ Quarterly

?

4 Finished Charging
- Final Calculation, kWh consumed

? Capture the data on aggregate level (charge-pole fleet) or individual level

6 Bill Customer

Customer billing

?

5 Generate LCFS Credits
- Per Transaction/Day Basis
- Calculate Credits
- Post to LCFS Ledger

Interface to trading platform

?

+

Process of registering generated LCFS Credits with CARB Authority

END

There are three principal areas for the use of blockchain in EV Charging Project

A Energy Provenance

B EV Charging Process

C Tokenized LCFS Credits

- Guarantee of Origin of the energy that is transferred into the EV
- Two implementation alternatives
  1. **Renewable Energy Token (not an official REC, w/o CEC)**
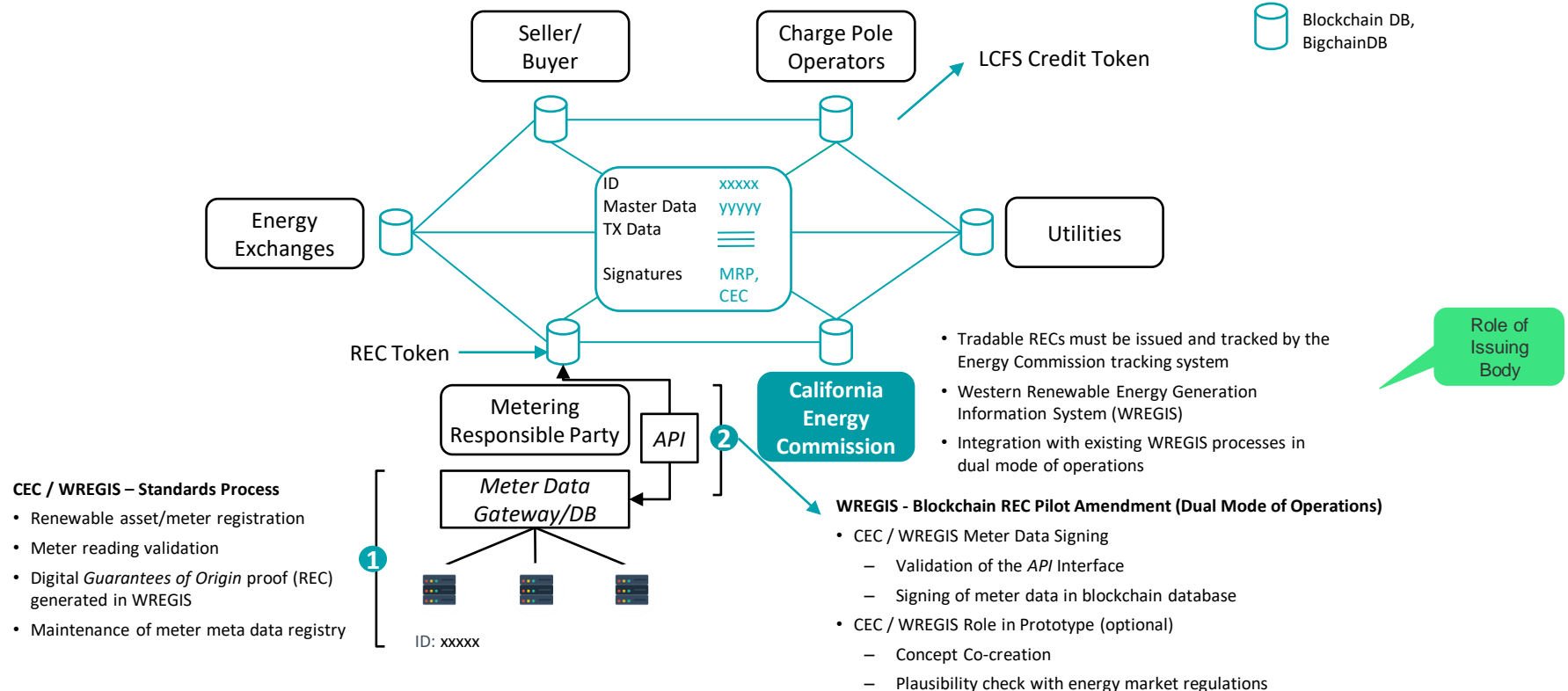 2. Renewable Energy Certificate (cooperation with CEC)

- Authentication
- Settlement and Billing (Smart Contract Escrows or Token Streaming)
- Two implementation alternatives
  1. CPO Charging Pole Fleet
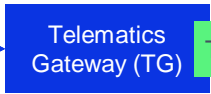 2. Private Charging Poles

- Generation of LCFS Credit Token
- Audit trail of LCFS Credit assignments to users/cars
- Trading and exchange of the LCFS Credit Token
- Two implementation alternatives
  1. Aggregated CP supply portfolio
  2. Microscopic, per transaction base

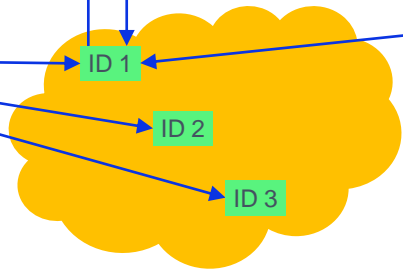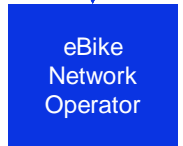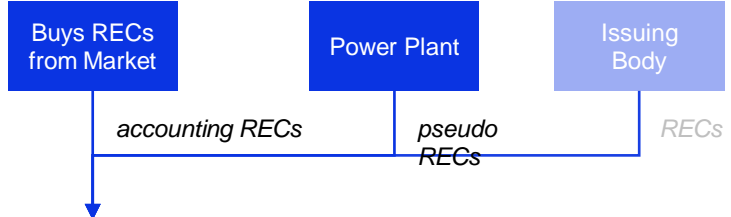# Example for Discussion: Set-up of a Decentral Settlement and REC Prototype

Seller/ Buyer

Charge Pole Operators

LCFS Credit Token

Blockchain DB, BigchainDB

ID	xxxxx
Master Data	yyyyy
TX Data	≡
Signatures	MRP, CEC

Energy Exchanges

Utilities

REC Token

California Energy Commission

Role of Issuing Body

Metering Responsible Party

API

Meter Data Gateway/DB

②

①

ID: xxxxx

- Tradable RECs must be issued and tracked by the Energy Commission tracking system
- Western Renewable Energy Generation Information System (WREGIS)
- Integration with existing WREGIS processes in dual mode of operations

CEC / WREGIS – Standards Process

- Renewable asset/meter registration
- Meter reading validation
- Digital *Guarantees of Origin* proof (REC) generated in WREGIS
- Maintenance of meter meta data registry

WREGIS - Blockchain REC Pilot Amendment (Dual Mode of Operations)

- CEC / WREGIS Meter Data Signing
  - Validation of the *API* Interface
  - Signing of meter data in blockchain database
- CEC / WREGIS Role in Prototype (optional)
  - Concept Co-creation
  - Plausibility check with energy market regulations

Green Certificate Bike Use Case

Vision

Circular Cloud

Verifiable Identity for Circular Things

Manufacturing Order
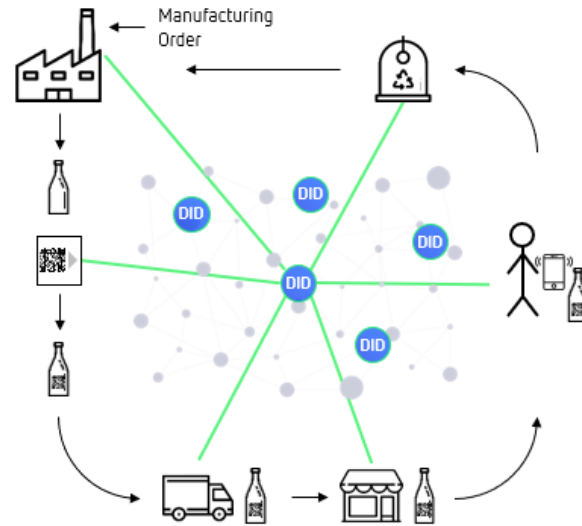
DID · Resolves to digital twin of the circular item which holds verifiable life-cycle credentials for back-to-birth track & trace

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

SPHERITY

Hyperledger Climate Action SIG

About Spherity's Decentralized Cloud-Edge Identity Solution

"Trust, but Verify"
September 2020

Contacts: Dr. Carsten Stöcker, +49 1520 8930 990, carsten.stoecker@spherity.com

Team Background – Spherity GmbH

In Spherity we bundle experience gained in 6 years of deep tech blockchain & identity technology development within enterprise environments

May 2015	●	Foundation of Machine Economy group at innogy Innovation Hub
Sept 2016	●	Membership World Economic Forum, Global Future Council on Blockchain & Identity
Jan 2017	●	Kick-off of project Twin of Things to focus on central Digital Twin business models
Nov 2017	●	Foundation of Spherity
Ongoing	●	Blockchain development of several Digital Twinning POCs for B2B partners
Q2 2019	●	Interoperable Digital Identity Wallet for NRW
Q3 2019	●	Mobile Identity Wallet with payment feature for Daimler Mobility
Q3 2019	●	**Fundraising with HTGF and Seed Capital Dortmund**
Ongoing	●	Enterprise Wallets for Third Party Risk Management with Novartis and PSCI
Q4 2019	●	SAP.io accelerator program
Ongoing	●	Enterprise Wallets for Drug Supply Chain Security Act (US) with SAP, Novartis, HDA

Trusted digital identity for authentication, authorization & agreements

Physical Wallet

Digital Identity Wallet

Cloud Identity Wallet
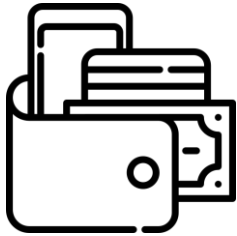
- Physical identity credentials
- Means of payment

- Human identity
- Digital identity credentials (KYC, drivers license, *e-prescriptions*)

- Cloud wallets for enterprises things and/or humans
- Verifiable data and data chains for auditable processes

# Secure Digital Identity for Citizens, Businesses & Governments

Features

1 Verifiable digital identities / twins

> » Citizens, Businesses, Government Entities
> » Vehicles, Products, Services, …

2 P2P trust through credential based verification

Verifiable Credentials

Trust Layer

3 Verifiable consent agreements & business transactions, payments

Consent agreements, business transactions

DocuSign on Steroids

4 Verifiable data chains & data provenance

Provenance for Industry 4.0
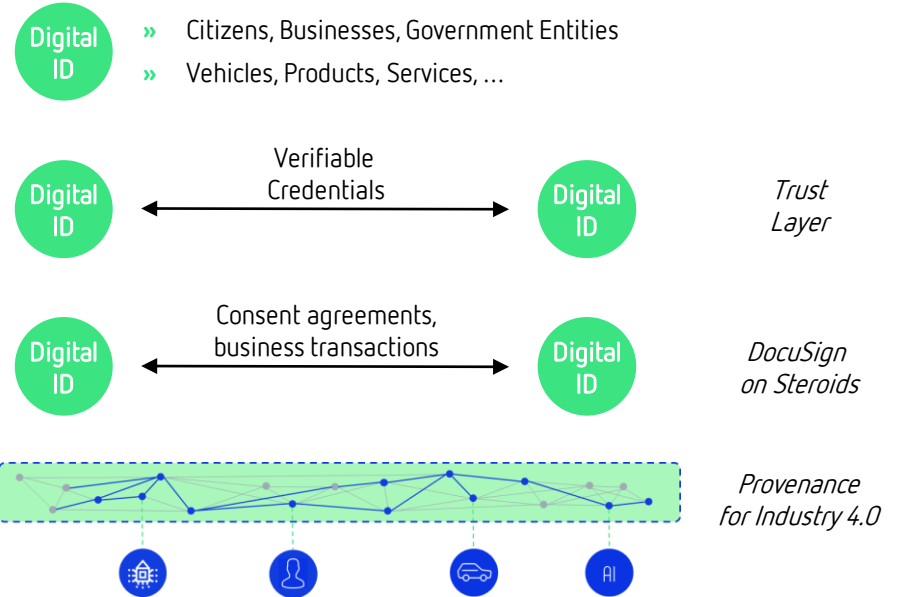
Combining unique Identifiers with Verifiable Credentials ...

Biological, Physical, Digital Entities
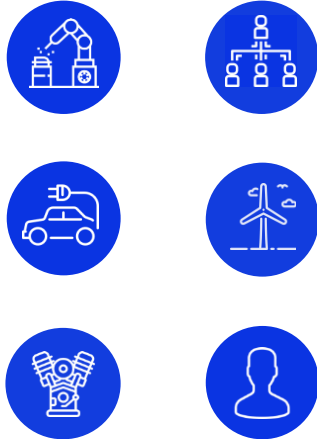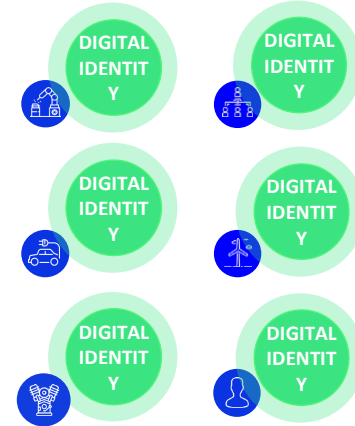
Digital Identity

+ **Decentralized Identifier (DID)**
"URL" or Service Endpoint for Identities

+ **Verifiable Credentials**
Digital verifiable set of data

DIGITAL IDENTITY

DIGITAL IDENTITY

DIGITAL IDENTITY

DIGITAL IDENTITY

DIGITAL IDENTITY

DIGITAL IDENTITY

... delivers an **unique and addressable representation** of everything.

SPHERITY

Identity Wallets built from Open Source libraries &Open Standards

Future-proof & No-lock in

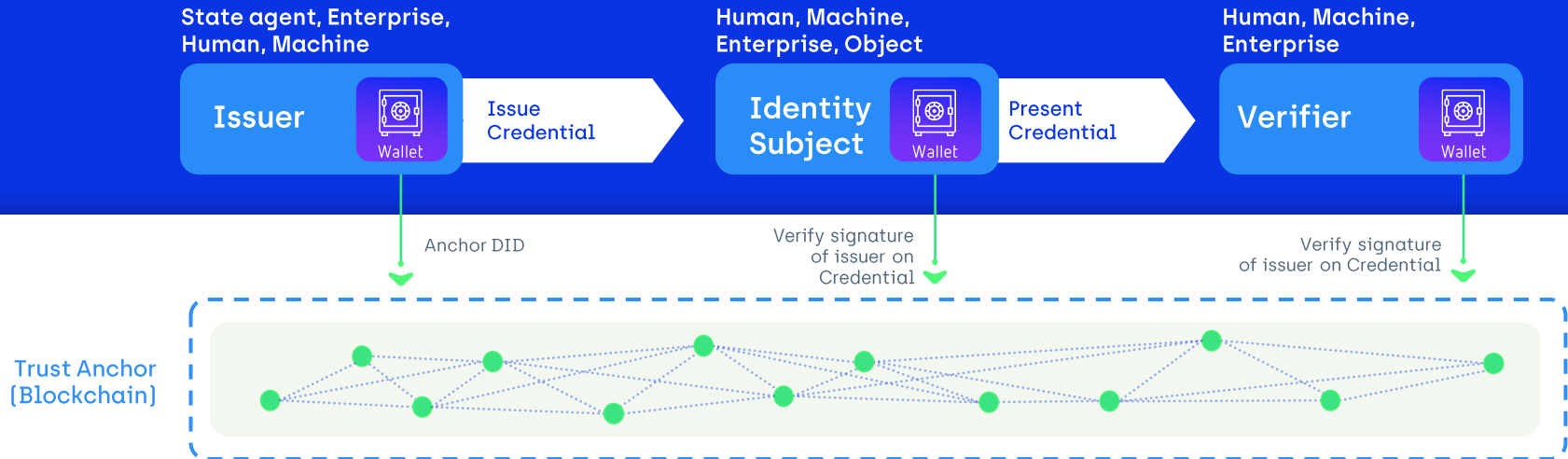|				
Blockchain agnostic	ethereum	☀ sovrin	HYPERLEDGER	HYPERLEDGER ARIES
Wallet agnostic [SaaS]	swisscom	evernym	SPHERITY	
Technology Ecosystem	DIF	W3C	r	imi innovative medicines initiative	PharmaLedger BLOCKCHAIN ENABLED HEALTHCARE
W3C Standard	DIDs	Verifiable Credentials	Wallet-to-Wallet Communications	

Real-time verification of Identity Subjects by proofing the issuer´s signature on credentials

State agent, Enterprise, Human, Machine

Human, Machine, Enterprise, Object

Human, Machine, Enterprise

Issuer | Wallet

Issue Credential

Identity Subject | Wallet

Present Credential

Verifier | Wallet

Anchor DID

Verify signature of issuer on Credential

Verify signature of issuer on Credential

Trust Anchor (Blockchain)

1. **Identity (DID)** of **Issuer** is registered on a Trust Anchor. **Issuer** delivers credentials to **Holders.**

2. **Subject** presents credential to Verifier.

3. **Requester verifies credentials** by proofing digital signature of issuer on Trust Fabric.

32

SPHERITY

Spherity Wallet: Verifiable data exchange & collaboration between digital entities

Integration
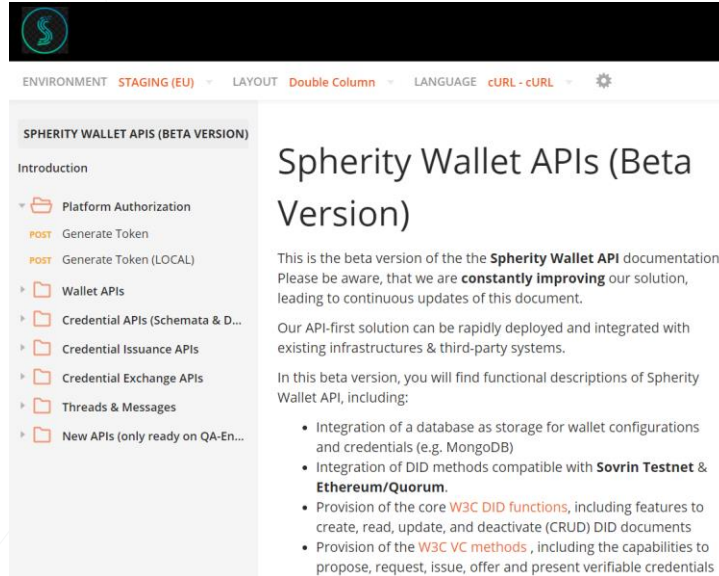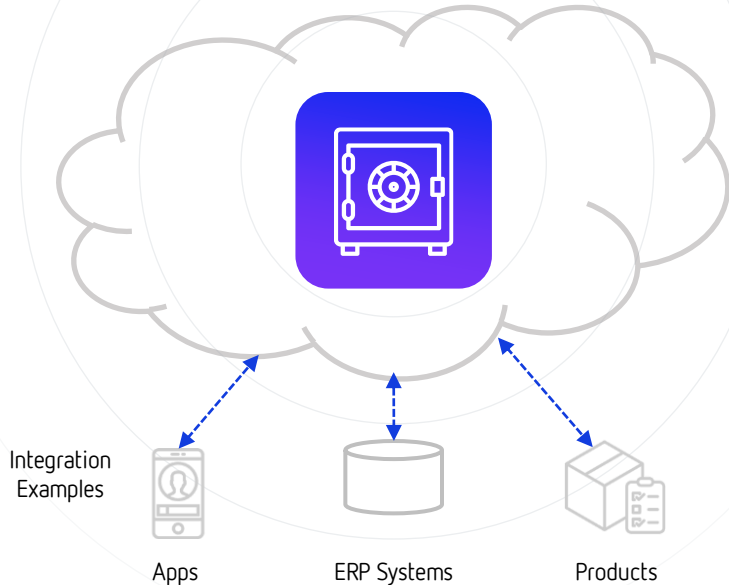Examples

Apps   ERP Systems   Products

What can you do with the Spherity Wallet?

» Configure digital verifiable identities of enterprises and products

» Issue, store, present and verify credentials

» Exchange credentialized data in a secure and temper-proof way

» Sign all transactions between digital identities to create an (off-chain) audit trail

» Anchor Decentralized Identifiers on a trust layer/ Blockchain

33

You can find our API documentation here

https://docu.spherity.com/

SaaS cloud wallet for idenitity in accordance to enterprise compliance and security requirements

Spherity Cloud DevSecOps Environment
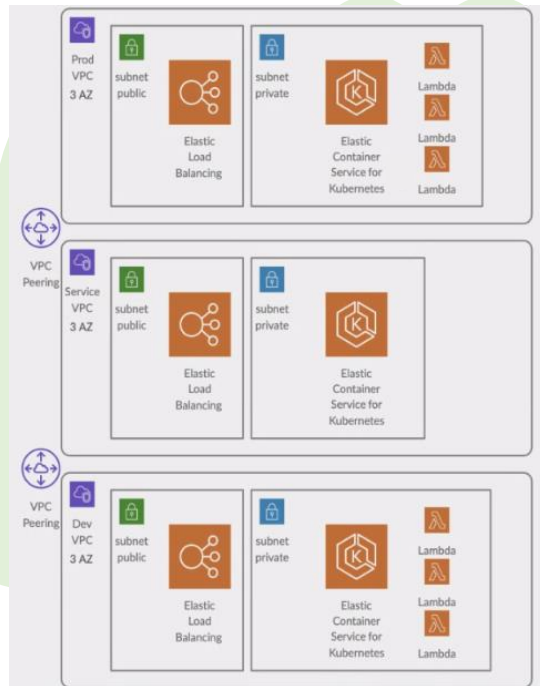
Spherity Focus on Security & Compliance

» Gitlab CD/CI development pipeline, test automation
» Clustered test, staging and development environments, SLAs, backup & recovery
» Cloud security, application firewall, IPS/IDP, DLP
» Cloud application monitoring, API call logging, resource usage tracking
» Universal resolver and blockchain integration of Ethereum, Evan Network, Indy (and R3 Corda in the future)
» Customer IAM integration (OpenID connect, oAuth 2.0, SAML 2.0)
» Wallet runs on any container manager (cloud or on-premise)
» Two tenancy options
  » Multi-tenant SaaS services
  » Isolated tenancy vault deployment
» Two options for key management
  » Custodial implementation (SW key stores, cloud HSMs, multi-party computation)
  » Non-custodial implementation (e.g. with MPC, customer HSM, smart phone edge, FIPS 140-2 Level 2 / 3 for Key Management)
» Multi-language support
» Application Security Testing
» ISO 27001 certification

Spherity offers out of the box cloud wallet capabilities

Spherity System Stack
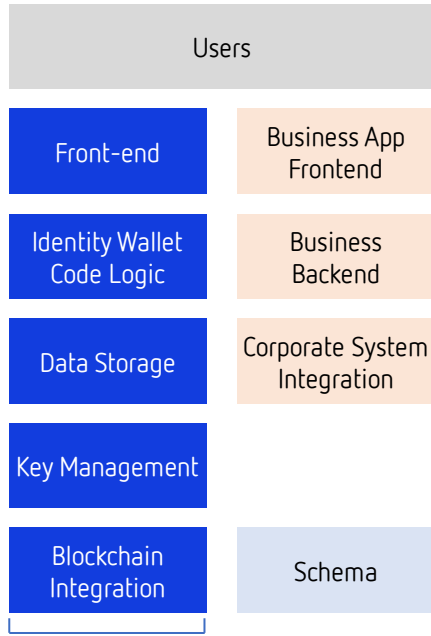
Architecture Overview
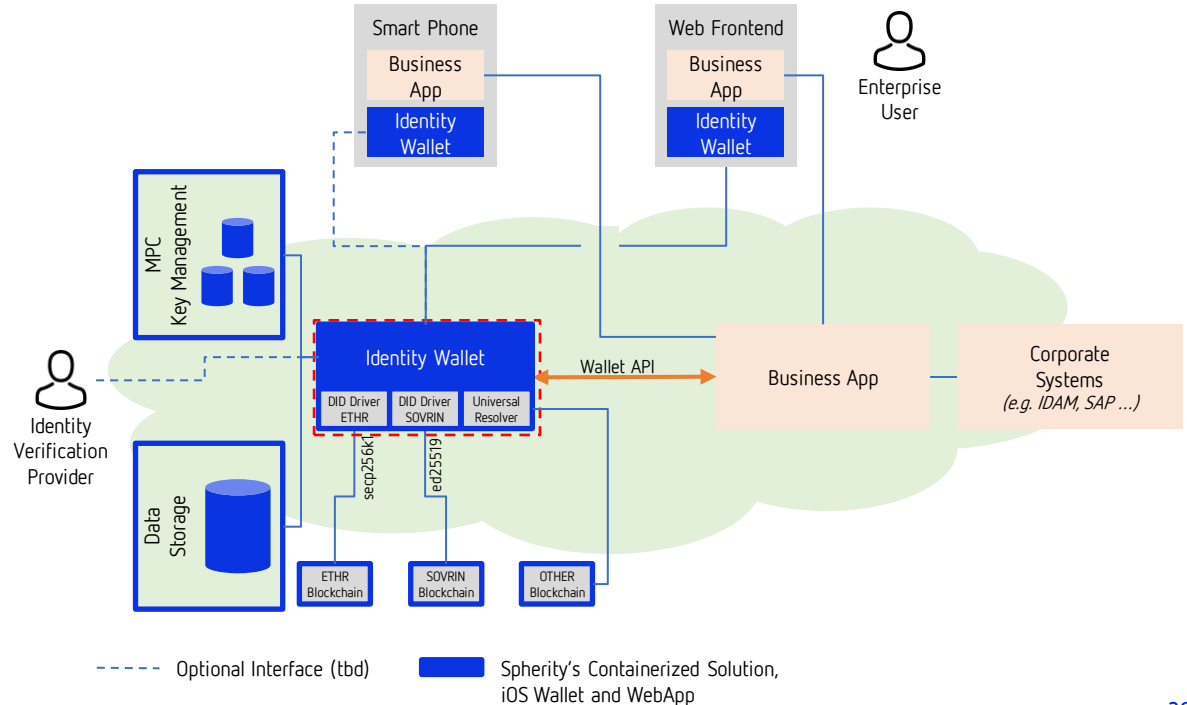
We engage with industry leaders on collaborative business and ecosystem innovation

Industry Leader
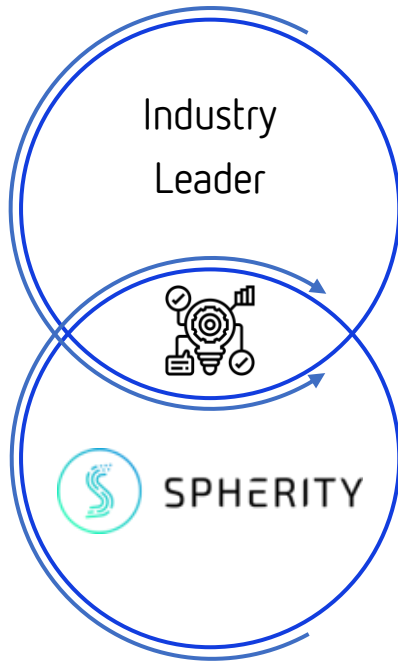
» Domain Knowledge
» Innovation Ecosystem
» Market reach

SPHERITY

» Decentralized identity and Verifiable Credentials technology
» Software as a Service
» Consulting

Realization
- Rollout
- Software as a Service
- Identity Management Service

Pilot & Field Test
- Implementation in Productive Environment
- Integration into existing systems
- Validation

Prototype
- Iteration-based prototyping of solution
- Use Case realization in test Environment
- Mobile or web application

Sprint Zero
- Problem Analysis
- Solution Concept
- Value Proposition

DIDs and DID Documents

Topic	Description	Structure

DID

1) A *permanent identifier* for individuals, organizations and things
   → It never needs to change over the lifecycle of an entity

2) A *resolvable identifier*, that is registered on a blockchain
   → You can look up its metadata in the respective DID document

3) A *cryptographically-verifiable identifier*
   → You van prove ownership and claims using cryptography

4) A *decentralized identifier*, created with public-private key pair
   → No central registration authority is required

DID Document

- DIDs resolve to DID Documents — simple documents that describe how to use that specific DID

- DIDs are *globally addressable*, as they can be resolved by any given actor by fetching the respective DID document from the blockchain

- By fetching a service endpoint (URL) from the DID document a DID could be understood as an *intelligent serial number* that provides access to a web service of any given DID subject

- Each DID Document typically contains at six things (see right hand side)

Structure

Creation   *Public Key* + *Private Key* —— **Cryptographic signature** to prove that I control the DID

Syntax   `did: ethr: 0xa22fdb2f2d2a3f901384673edc9b035d8f58432a`

Scheme   **Method**
How to read and write a DID (and its DID Document) on a specific Blockchain or decentral network

Method-Specific Identifier
Generated as defined by the DID Method specification

Key   DID
Decentralized Identifier

Value   DID-Document
Document describing the entity identified the DID

Standard elements of a DID Document

1. DID (for self-description)
2. Set of public keys (for verification)
3. Set of authentication methods (for authentication)
4. Set of service endpoints (for interaction) → URL to Interactive Web Service(s)
   • Wallet
   • Business Logic
5. Timestamp (for authentication history)
6. Signature (for integrity)

Source: https://w3c-ccg.github.io/did-spec/

Verifiable Credentials
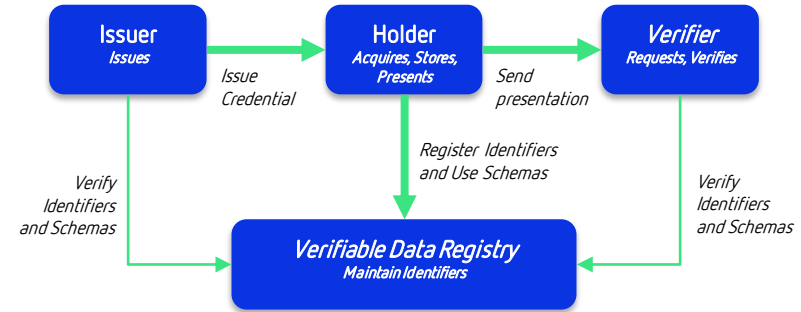
SPHERITY

Topic

Description

Structure

Verifiable Credentials

- A verifiable credential is a qualification, achievement, quality, or piece of information about an entity's background such as a name, government ID, quality report or birth certificate.
- Claims within a credential describe a quality or qualities, property or proper-ties of an entity which establish its existence and uniqueness.
- Goals of the W3C standards are standardization and interoperability of credentials with the goals of storing, transmitting, and receiving digitally verifiable proofs.

Issuer
Issues

Holder
Acquires, Stores, Presents

Verifier
Requests, Verifies

Issue Credential

Send presentation

Register Identifiers and Use Schemas

Verify Identifiers and Schemas

Verify Identifiers and Schemas

Verifiable Data Registry
Maintain Identifiers

Identity Wallet

- The place where the holder stores the verifiable credentials and the private key for signing with its identity is called a wallet. The wallet might have agent logic for requesting and storing credentials.
- Verifiable credentials are under control of the holder identity wallet.

Verifiable Presentation

- Verifiable Presentations is a W3C data format used to combine, sign and present credentials - that are stored in the wallet - to a 3rd party verifier.
- Prior presenting them Verifiable Presentations, they are signed by the holder.

Source: https://www.w3.org/TR/verifiable-claims-use-cases/