DSR
DOING SOFTWARE RIGHT

Hiero - ACA-Py plugin for Hedera ledger

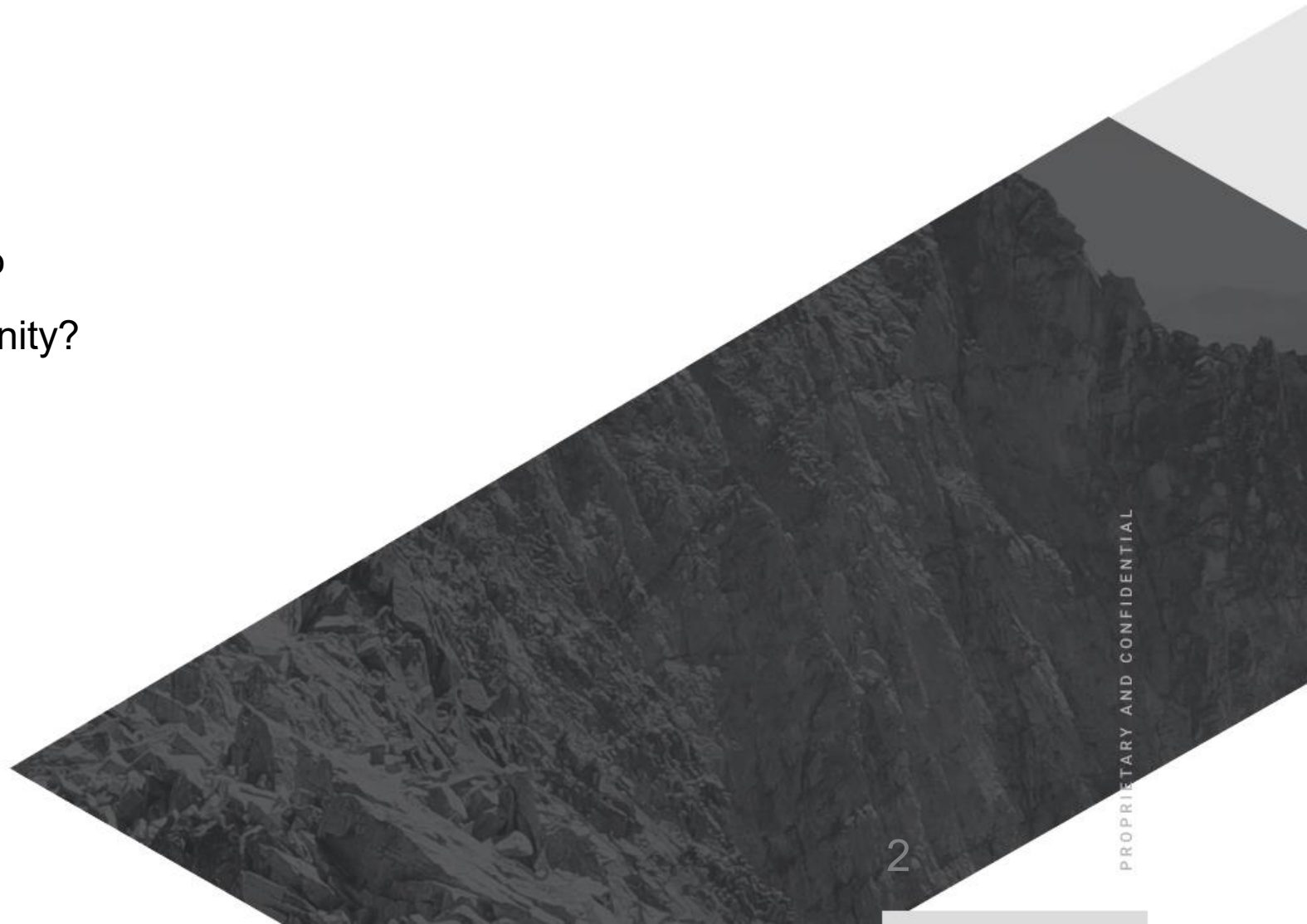
LFDT Webinar

Presented by
Alexander Shenshin – DSR Corporation
Keith Kowal – Hashgraph

06/18/2025

Agenda

- SSI overview
- About AnonCreds, benefits
- About ACA-Py, main advantages
- About Hiero and Hedera ledger
- Hedera ACA-Py plugin and demo
- What are the benefits for community?
- What’s next?
- Q&A

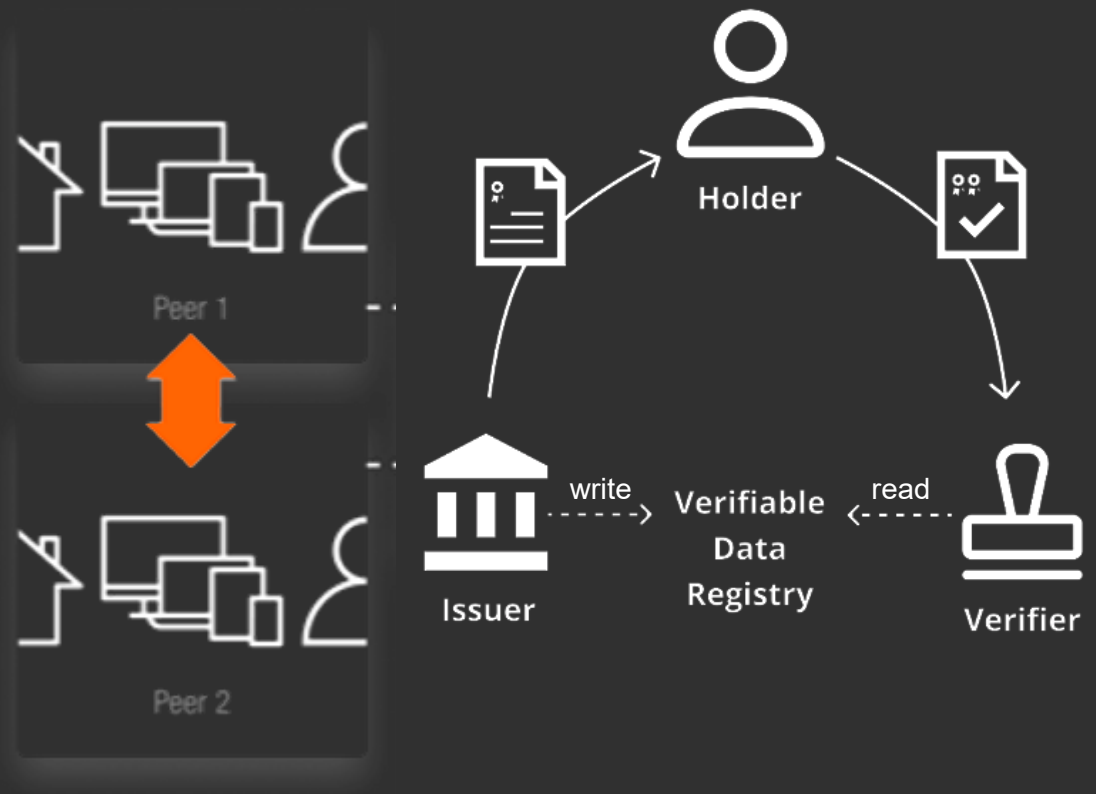


Digital Identity Models

#1: Siloed (Centralized) Identity

#2: Third-Party IDP (Federated) Identity

#3 Self-Sovereign Identity



Non-SSI vs SSI

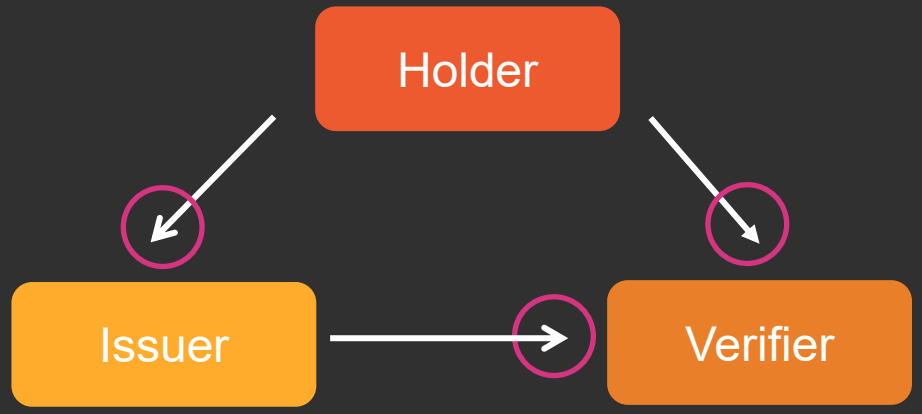
Self-sovereign Identity (SSI), or Decentralized Identity, is an approach to digital identity focusing on privacy and enabling individuals to maintain control over the information associated with their identity.

SSI is not tied to a specific framework or library; instead, it encompasses multiple specifications, standards, frameworks, and tools that implement SSI principles.

Key differences from Centralized and Federated:

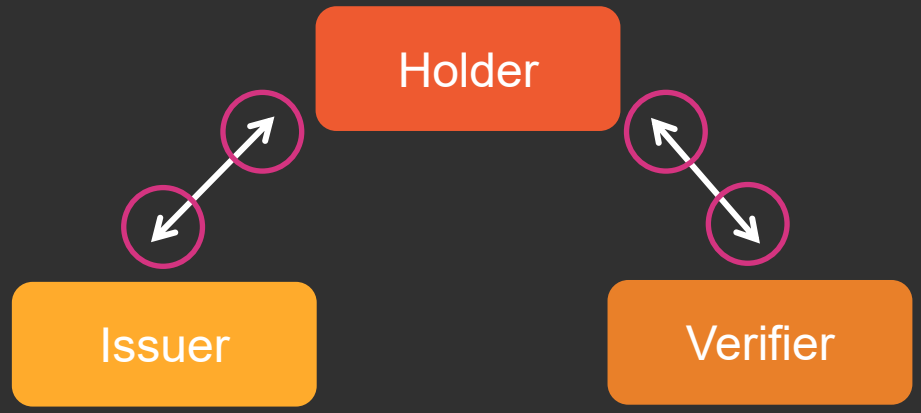
- peer-to-peer
- No need for centralized intermediaries
- No need for passwords
- Users (Data Holders) own their data and decide when and with whom (what Verifiers) they share it.

Federated vs SSI



Federated Identity (OAuth, OpenID)

Authorization-based credential exchange where the holder authorizes a verifier (client) to access information on her behalf.

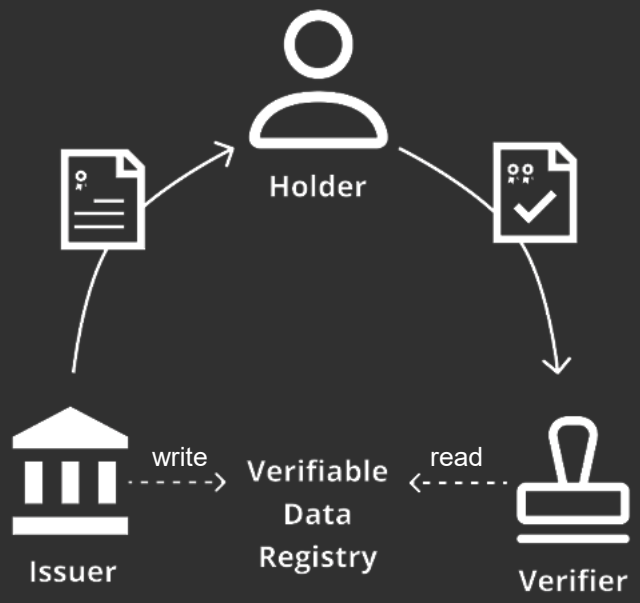


Self-sovereign Identity

Self-sovereign credential exchange where the holder can autonomously control the exchange of credentials with any verifier she wants.

SSI Use Case

1. Alice installs a certified Mobile Wallet application on her phone
2. Government issues a digital ID (passport or driver license) for Alice. The digital ID is stored in Alice's Mobile Wallet.
3. Alice is getting on an airplane, and need to present her ID. She presents her digital ID from the Mobile Wallet.

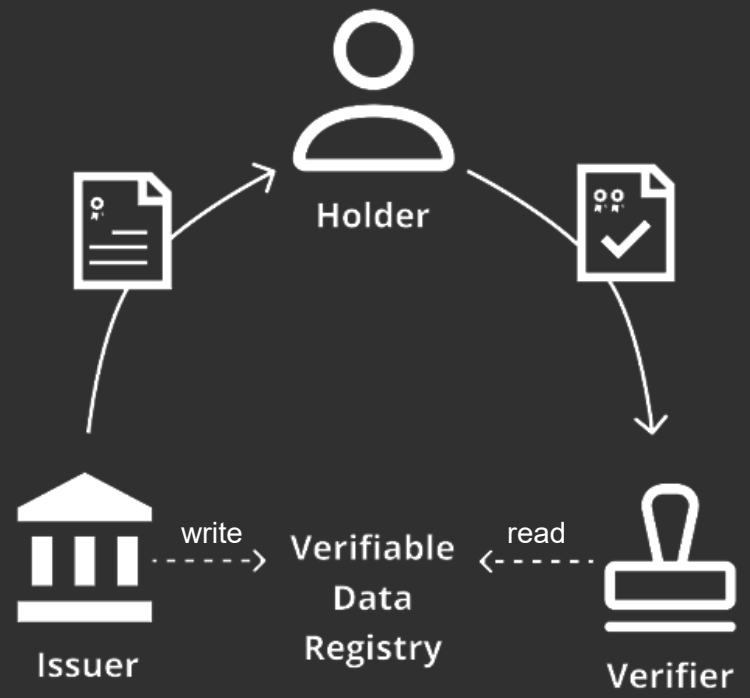


As we can see Alice is in control of her information and decides what parts of that information other entities can see

- Alice - Holder
- Government - Issuer
- Airport - Verifier

SSI Use Case

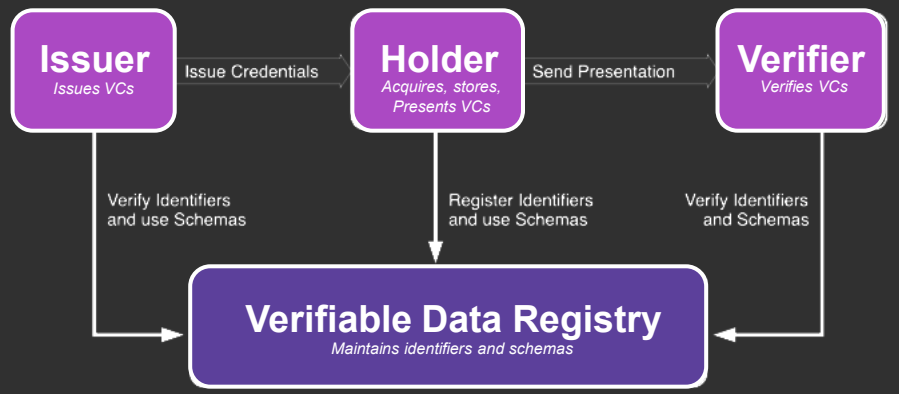
- Offline (proximity) and online
- Issuers: not only governments, but business as well
- Verifiers: governments, business, individuals
- Wallet: either provided by a state or a 3rd party one
- Wallets: Mobile, Cloud or Hybrid
- Issued credentials: almost anything. Digital ID, KYC, transport tickets, concerts, medical records, bank data, etc.
- Selective disclosure: disclose only part of the data, or even a predicate (over 21 years old)
- Root of trust (trusted lists): can be anything – X509, Blockchain, DLT, Web/DNS, etc.



SSI Technical Concepts

1. Verifiable Credentials (VC)

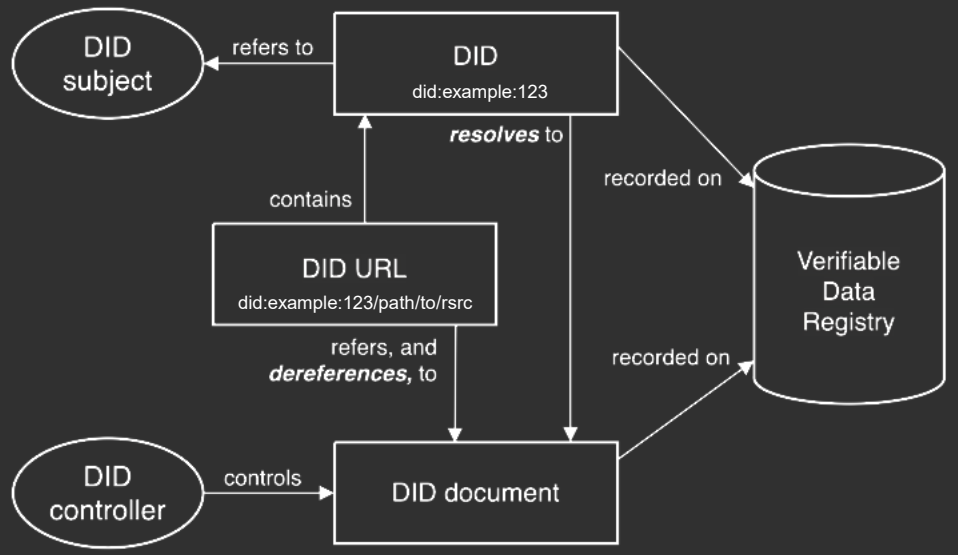
Verifiable Credentials Data Model v1.1,
W3C Recommendation 2022



From https://www.w3.org/TR/vc-data-model/

2. Decentralized Identifiers (DID)

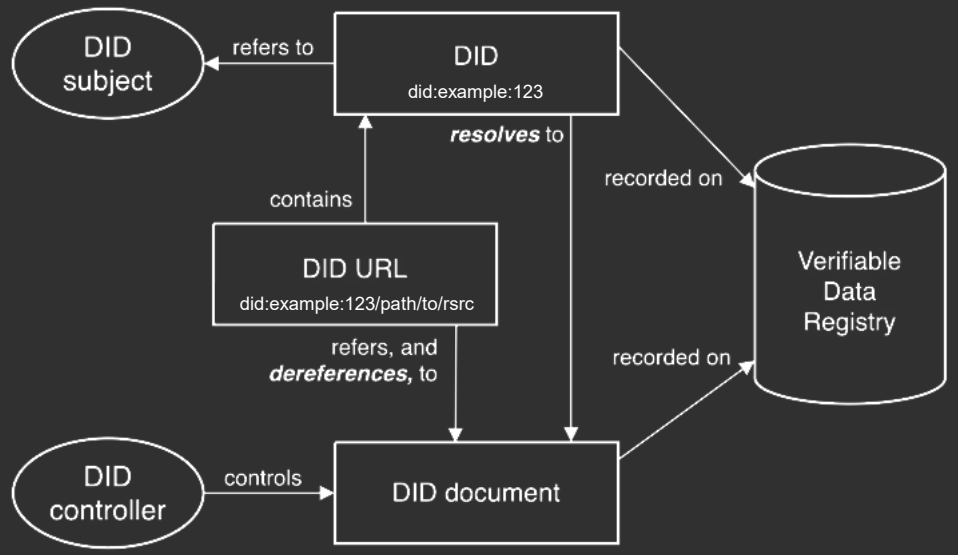
Decentralized Identifiers (DIDs) v1.0,
W3C Recommendation 2022



From https://www.w3.org/TR/did-core/

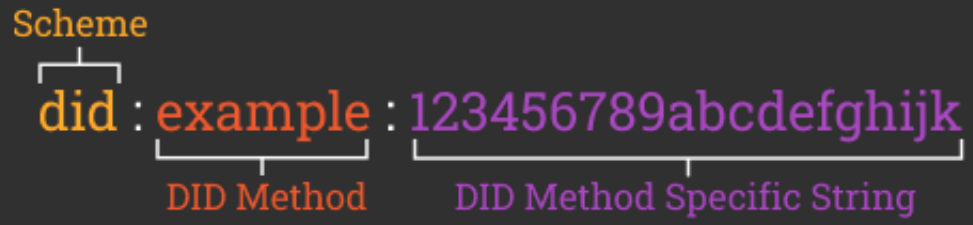
SSI Technical Concepts: DID

- A Decentralized Identifier (DID) refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.).
- In contrast to typical, federated identifiers, DIDs may be decoupled from centralized registries, identity providers, and certificate authorities.



From https://www.w3.org/TR/did-core/

Decentralized Identifiers (DIDs) v1.0, W3C Recommendation 2022



From https://www.w3.org/TR/did-core/

SSI Technical Concepts: DID and DID DOC

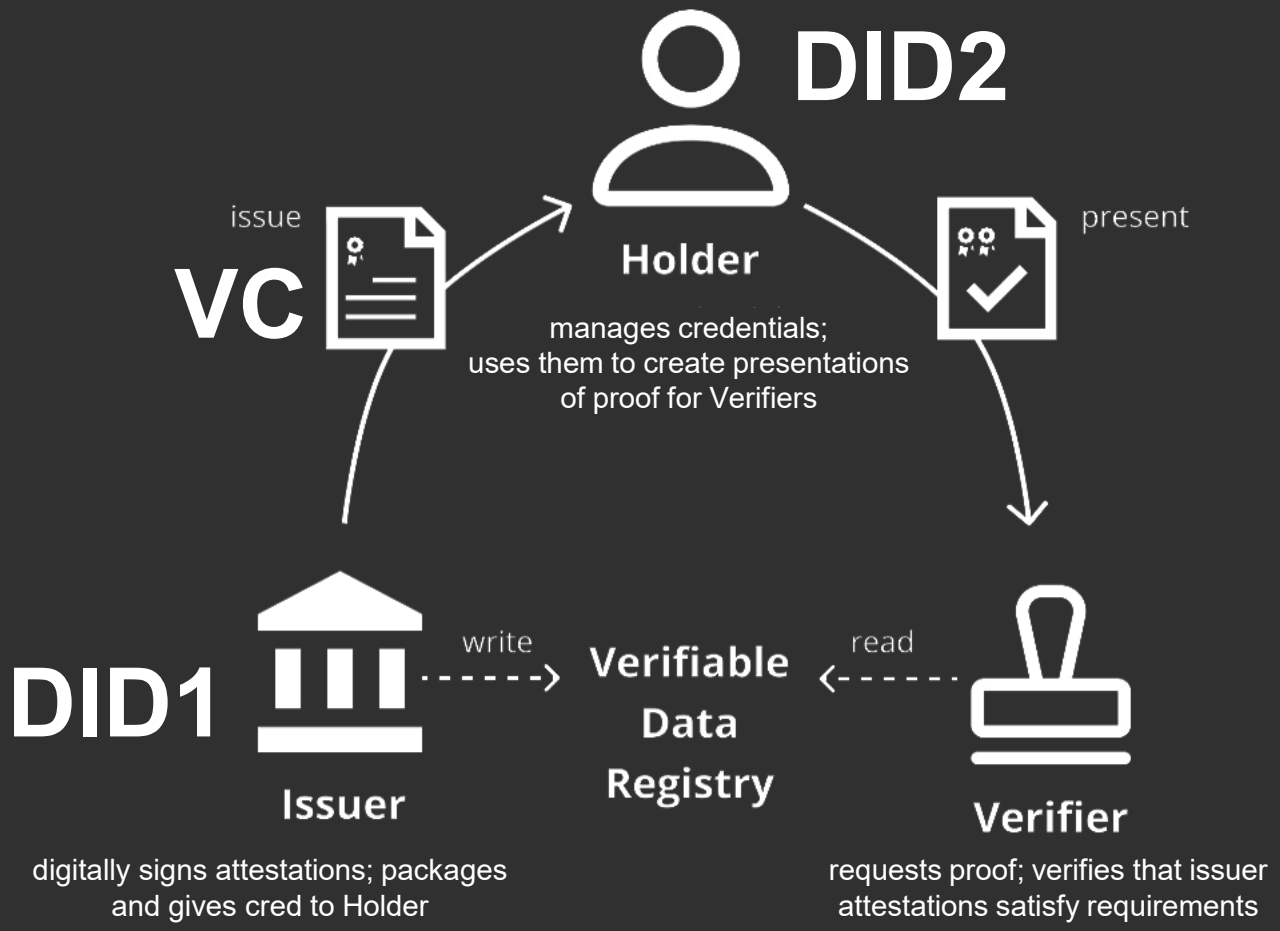
DSR

```
{
  "@context": ["https://www.w3.org/ns/did/v1","https://identity.foundation/.well-known/did-
  "id": "did:example:123",
  "verificationMethod": [{
    "id": "did:example:123#456",
    "type": "JsonWebKey2020",
    "controller": "did:example:123",
    "publicKeyJwk": {
      "kty": "OKP",
      "crv": "Ed25519",
      "x": "VCpo2LMLhn6iWku8MKvSLg2ZAoC-nlOyPVQaO3FxVeQ"
    }
  }],
  "service": [
    {
      "id":"did:example:123#foo",
      "type": "LinkedDomains",
      "serviceEndpoint": {
        "origins": ["https://foo.example.com", "https://identity.foundation"]
      }
    },
    {
      "id":"did:example:123#bar",
      "type": "LinkedDomains",
      "serviceEndpoint": "https://bar.example.com"
    }
  ]
}
```

Property	Required?
id	yes
alsoKnownAs	no
controller	no
verificationMethod	no
authentication	no
assertionMethod	no
keyAgreement	no
capabilityInvocation	no
capabilityDelegation	no
service	no

From https://www.w3.org/TR/did-core/

SSI Technical Concepts In Action



By Daniel Hardman licenced under CC BY-SA 4.0

- Issuer's DID and DIDDoc (Public Key)
  - Sign VC
  - Public, usually on a Blockchain or a trusted Web service (did:web, did:indy, did:hedera, etc.)
- Holder's DID
  - Associates a VC with a DID
  - Prove ownership (signature) of the Holder during presentation (unique DID2 for every Issued VC or even for every Verifier!)
  - Either Public or Private (did:key, did:peer, long form of did:ion, etc.)

About AnonCreds, benefits

AnonCreds (anonymous credentials) are a type of verifiable credential that supports advanced privacy-preserving capabilities through the use of zero-knowledge proof (ZKP) cryptography.

Benefits of AnonCreds:

- The use of ZKPs in the verifiable presentation process to enhance the privacy protections available to the holder in presenting data to verifiers, including
  - Blinding issuer signatures and use of unrevealed identifiers for holder
  - Support for predicate proofs to reduce the sharing of Personally Identifiable Information (PII)
  - A revocation mechanism that works without revealing correlatable identifiers
- Complete flows and defined data models for issuance and verification of VCs
- Fully defined applications of cryptographic primitives

About ACA-Py, main advantages

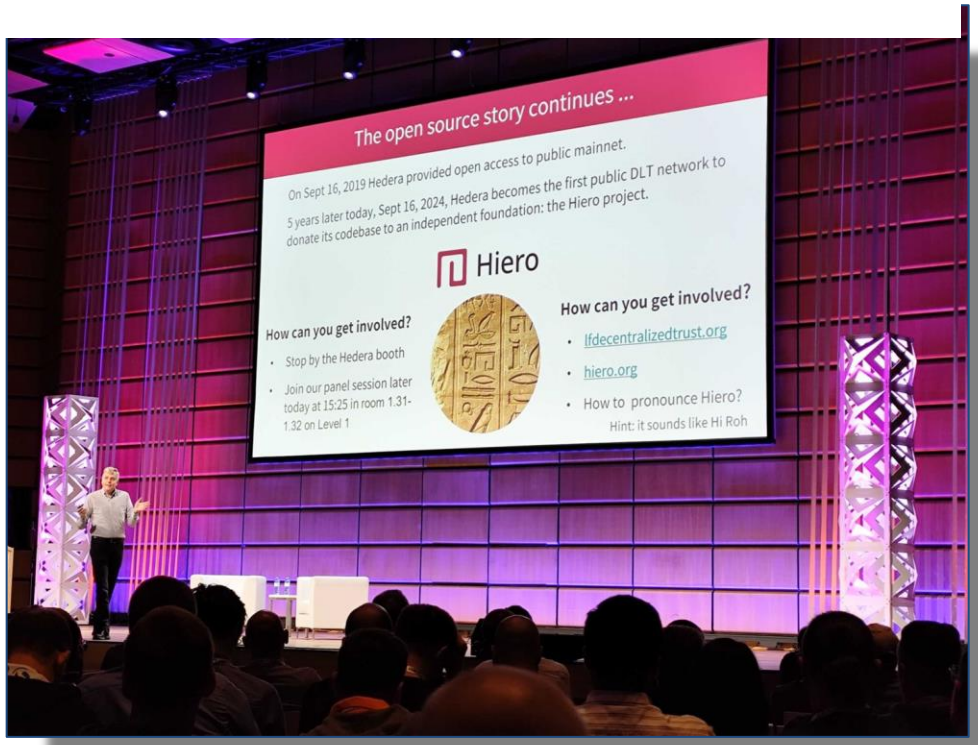
ACA-Py is a configurable and extensible non-mobile Aries agent that implements an easy way for developers to build decentralized identity services that use verifiable credentials.

Main advantages of ACA-Py:

- “Batteries included” and easy-to-use agent implementation
  - Supports all relevant protocols and standards (out-of-box or via plugins)
  - Used directly via HTTP API and designed to integrate with “controller” application that can be built with any language
  - Can be installed and run as a PyPi package
- Extensibility – supports plugins for adding new DID Methods, protocols and completely custom functionality
- Maturity and stability – extensively used in production environments

Hiero

Open Source Distributed Ledger Technology



“This contribution represents a historic moment in the evolution of decentralized networks and is setting a precedent for transparency and collaboration in the blockchain industry. By contributing our codebase to LF Decentralized Trust, as project Hiero, we are reaffirming our commitment to open governance and collaboration.

LF Decentralized Trust's mission to advance decentralized systems aligns perfectly with our own goals. We look forward to providing developers with unmatched access to tools and resources, creating an environment where decentralized applications can truly thrive.”

Charles Adkins

President, Hedera

What is Hiero?

Hiero, is now a Linux Foundation Decentralized Trust project, the first Layer 1 platform to be openly governed by an trusted independent foundation.

It is the open-source, vendor-neutral distributed ledger technology that is used to build the Hedera public ledger.

Why Linux Foundation?

- Trusted Brand
- Established Foundation of related projects including Besu
- Pathways to Cross-Chain Interoperability
- Expanding Hyperledger Foundation to Decentralized Trust

Hiero

Open Source Distributed Ledger Technology

LF DECENTRALIZED TRUST

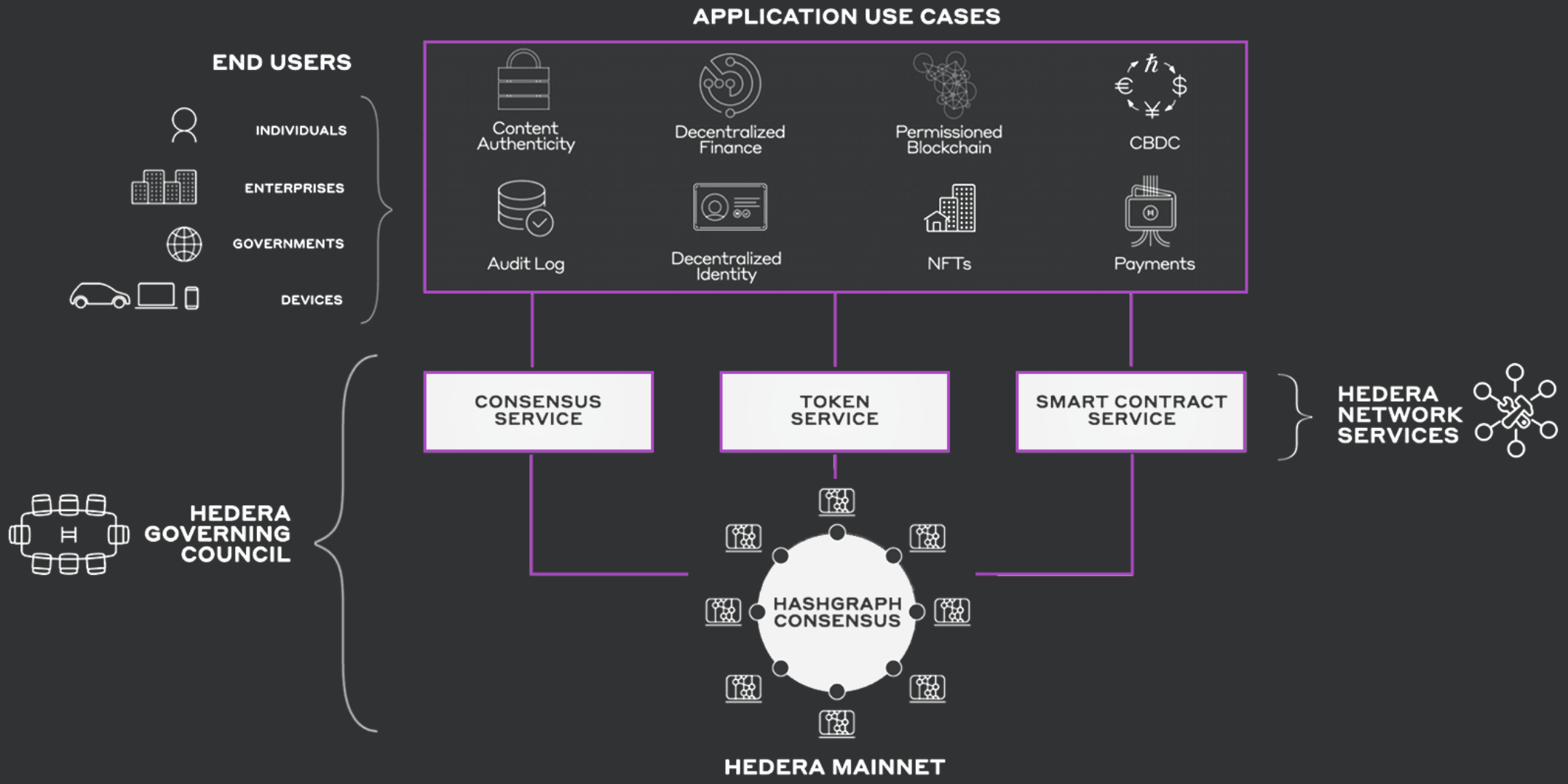
What is Hedera?

Hedera is a fully open source, proof-of-stake, public network and governing body for building and deploying decentralized applications.

Hedera is unique in that it is incredibly fast, energy-efficient (carbon negative), and secure — these advantages can be attributed to its underlying hashgraph consensus algorithm.

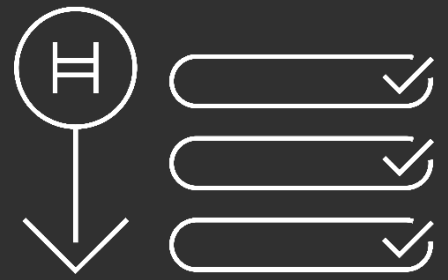
Open-source community around Hedera is very active, providing SDKs, other tools and applications that operate within Hedera ecosystem.

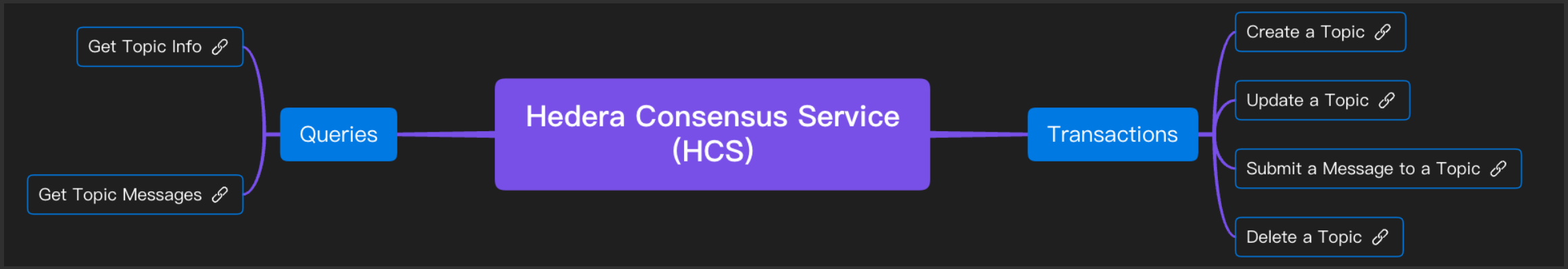
What is Hedera?



Hedera Consensus Service

- User can create topics and then publish messages to the topic
- Messages can contain any payload up to 1024 bytes
- High throughput, highly scalable, and low cost





Hedera ACA-Py plugin

ACA-Py plugin that provides components and integration of Hedera DID Method and AnonCreds registry in ACA-Py agent.

- Built on top of Hiero DID SDK that contains Python implementation of Hedera DID and AnonCreds methods
  - Identity objects (DID documents, AnonCreds resources) are stored on Hedera Consensus Service (HCS)
  - SDK focuses on providing high performance with special attention for read operations design and caching strategies
- Contributed to OWF ACA-Py plugins repo
  - Repo folder: https://github.com/openwallet-foundation/acapy-plugins/tree/main/hedera

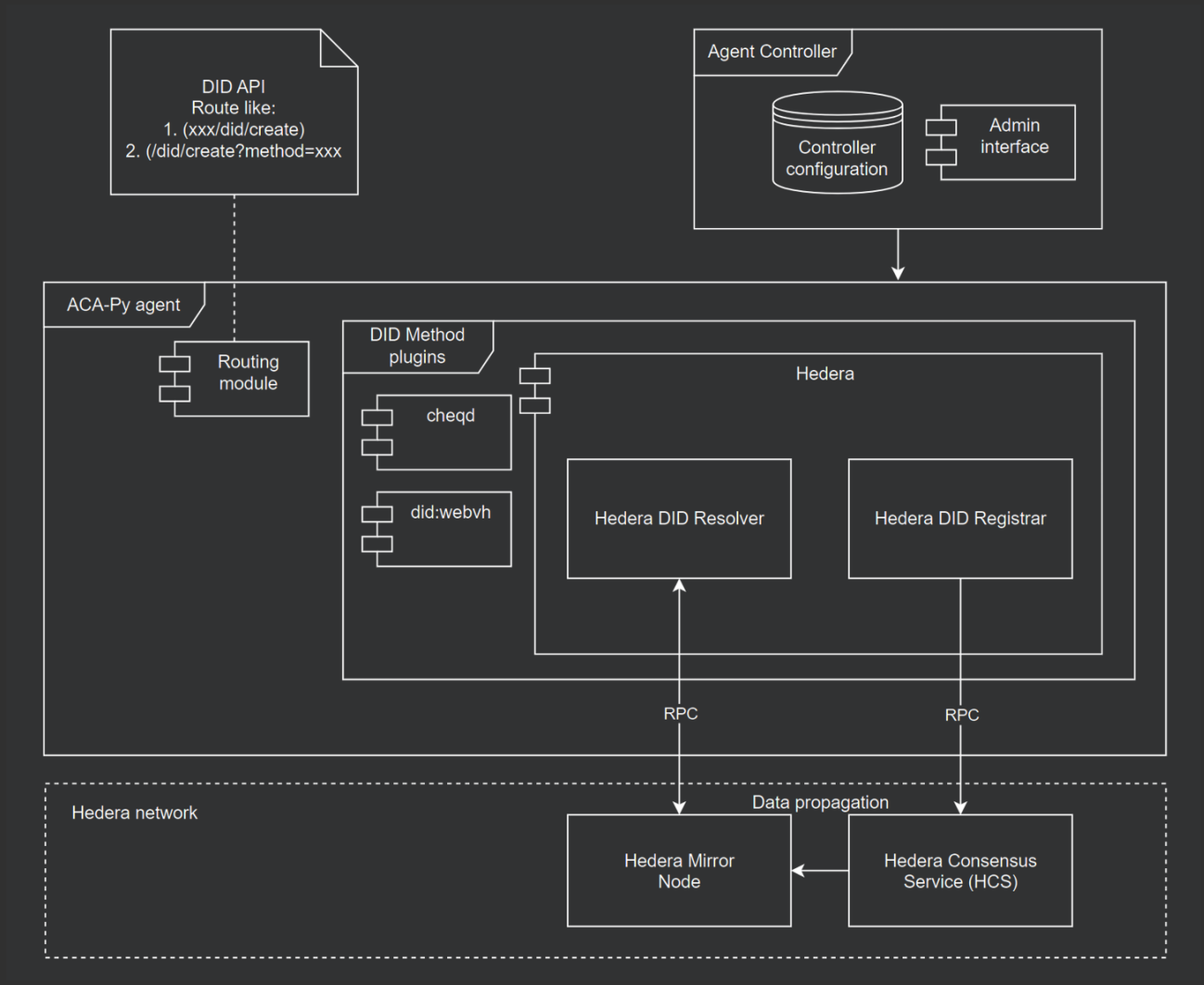
Hedera ACA-Py plugin

Internal plugin structure includes following components:

- Common
  - Plugin setup
    - Registers Hedera DID and AnonCreds implementations within ACA-Py instance
    - Registers custom endpoint for Hedera DID registration
  - Helpers for managing Hedera Client instances
- Hedera DID module
  - Implementation of ACA-Py interfaces (DID Resolver, DID Method class)
  - Custom implementation for Hedera DID registrar
- AnonCreds module
  - ACA-Py AnonCreds Registry interface implementation
  - AnonCreds-specific types mapping utilities

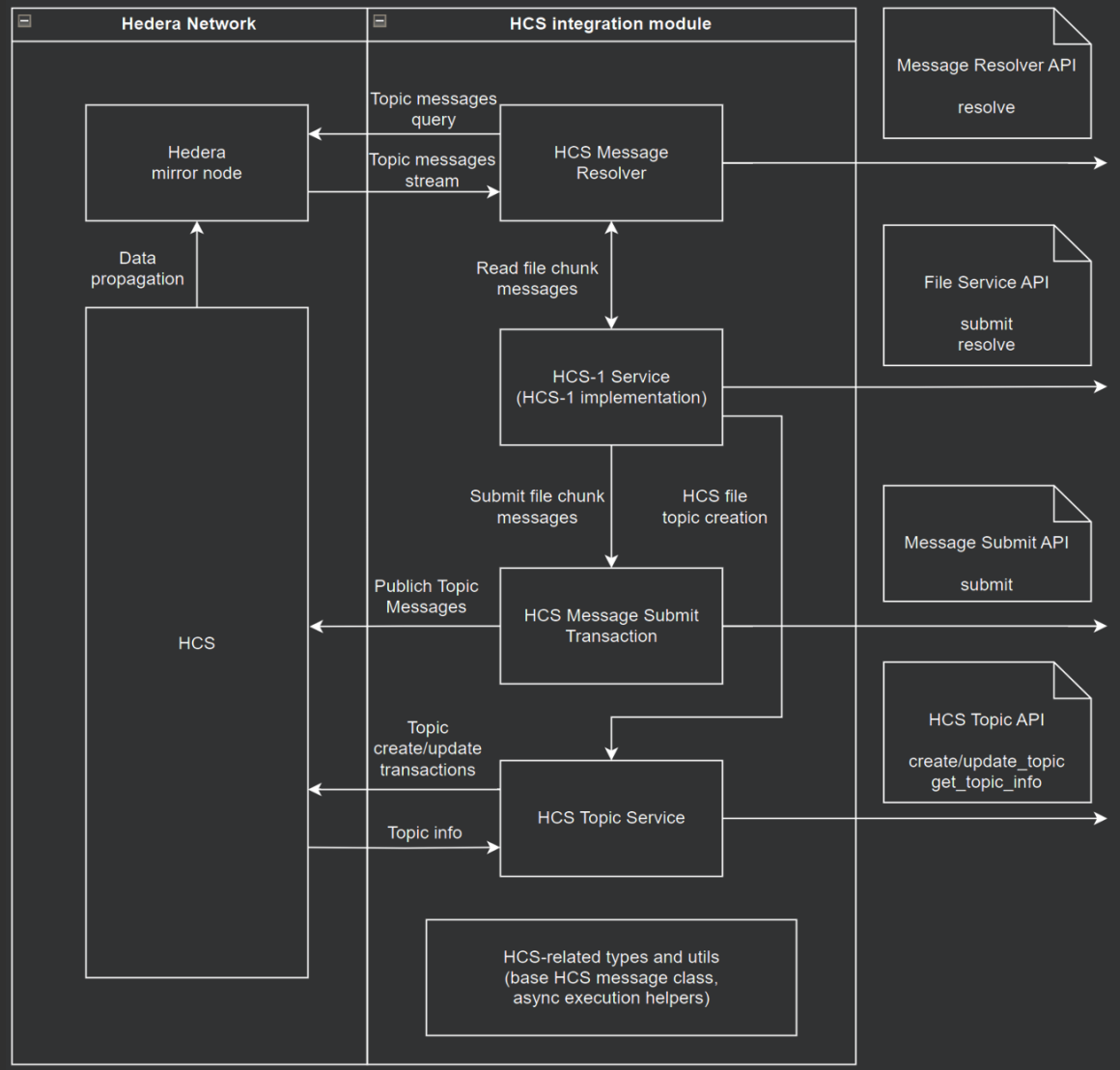
Plugins architecture

- ACA-Py plugins enable standardized extensibility without overloading the core ACA-Py code base – this feature is fully leveraged by Hedera plugin
- The diagram reflects integration of Hedera DID Method as an example



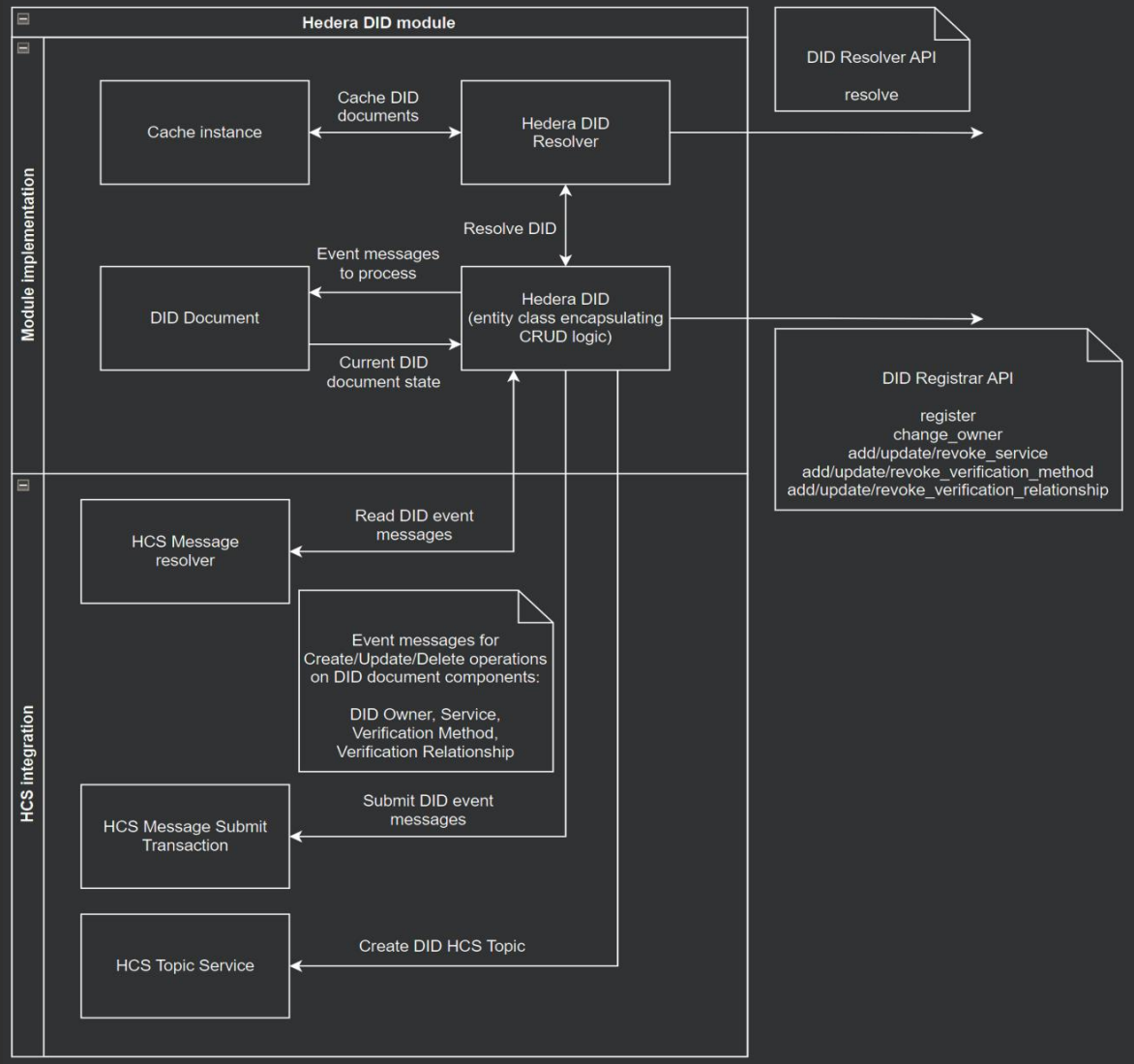
Integration with Hedera network

- Under-the-hood integration with Hedera network
- Main components/layers:
  - Hedera network
  - Hedera Consensus Service (HCS) integration module
  - HCS integration API (used by other modules)



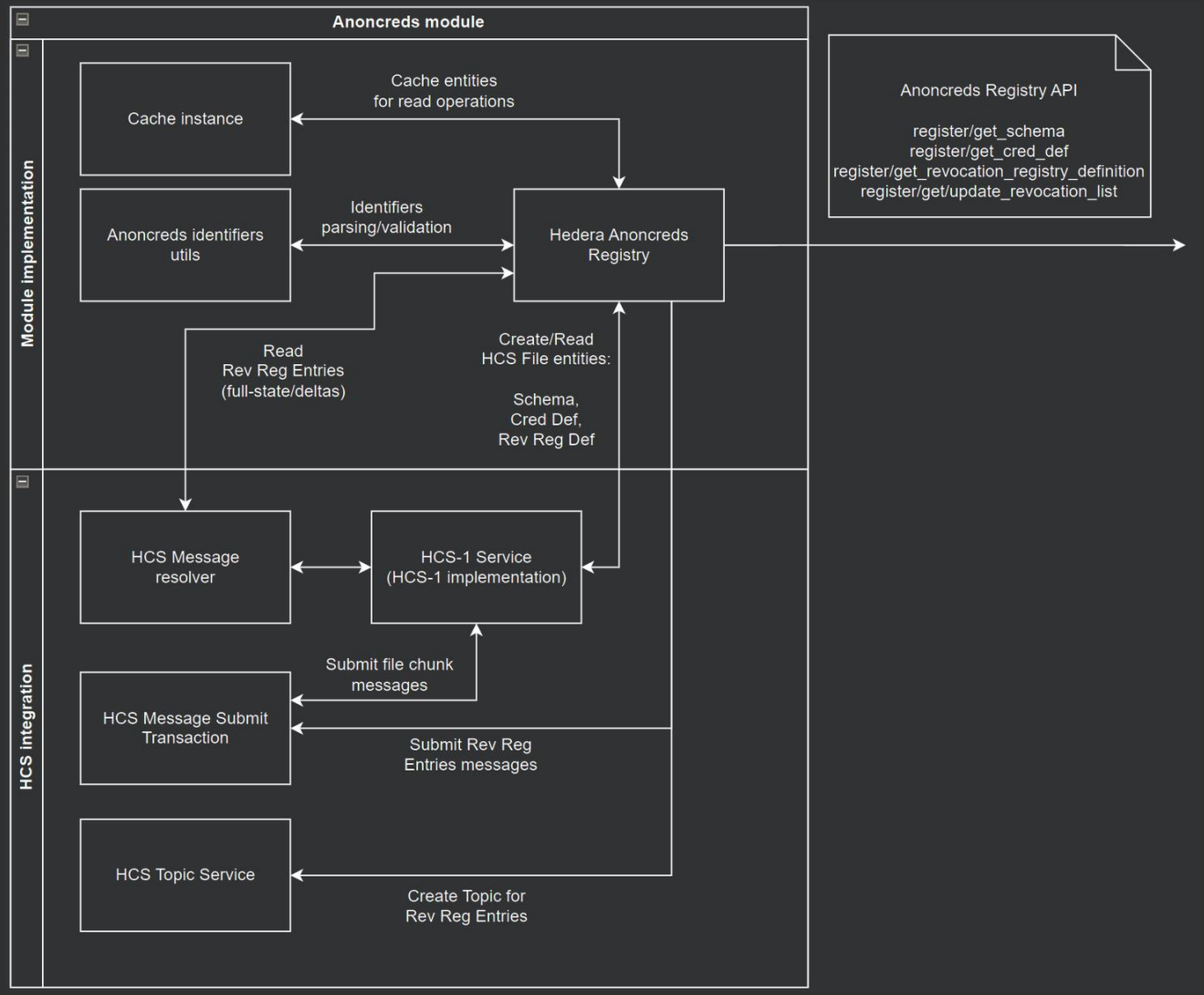
Integration with Hedera network

- Hedera DID management and integration with HCS
- Main components/layers:
  - Hedera Consensus Service (HCS) integration module
  - Hedera DID module
  - Hedera DID resolver and registrar APIs



Integration with Hedera network

- AnonCreds resources management and integration with HCS
- Main components/layers:
  - Hedera Consensus Service (HCS) integration module
  - AnonCreds module
  - AnonCreds registry API



Documentation

- ACA-Py plugin documentation consists from two parts:
  - README and dev tutorial
  - Demo guide
- All parts are markdown pages, stored in the repo

Demo

- Console app demo of ACA-Py + Hedera plugin (similar to existing ACA-Py demos)
- Enables full AnonCreds VC flow – issuance, verification and revocation
- The demo is a part of plugin codebase
  - Demo folder: https://github.com/openwallet-foundation/acapy-plugins/tree/main/hedera/demo

What are the benefits for community?

- Sovrin reached end of its service in March 2025 and there is a selection of identity applications and platforms that are looking for new trusted and stable ledger to use
  - Sovrin network was working without issues for 7 years, without significant devops support
- Many of these ecosystems also use ACA-Py in production or pre-production environments, so migrating to another ledger is much easier than moving to a completely new agent implementation and/or SDK
- Hedera ACA-Py plugin provides an option to use highly-performant Hedera network, bringing speed and low cost of operations to decentralized identity use cases
  - On part of reliability, Hedera is a large network that being trusted and successfully used for many use cases, while also having a large and active community
  - We expect it to be a great choice for both existing and new ACA-Py deployments

What's next?

- Development roadmap
  - Adding Hedera support to Credo framework
    - New Hiero DID SDK JS hosted under Hiero GitHub org
    - Hedera Credo plugin, to be contributed to OWF
  - Official Hedera AnonCreds method specification
  - Future adoption of relevant standards (AnonCreds 2.0 spec, Hedera DID spec updates)
- Upcoming event – presentation at Global Digital Collaboration conference in Geneva on July 2nd
  - Hedera x Ayra x DSR collaboration - demo of First Person Credentials project
  - GDC Day 2 agenda: https://globaldigitalcollaboration.org/agenda?day=2025-07-02
    - See «First Person Credentials and Trust in the Open Source Supply Chain» session at 4:20 PM

What's next?

- Join the community
  - LFDT Discord channel: https://discord.com/invite/hyperledger
    - See Hiero channel section and hiero-did-sdk-python channel
  - OWF Discord channel: https://discord.com/invite/yjvGPd5FCU
    - See aca-py channel (includes ACA-Py plugins discussions)

Technical resources

- GitHub organizations
  - Hiero: https://github.com/hiero-ledger
  - Hedera: https://github.com/hashgraph
- Repositories
  - Hiero Python SDK: https://github.com/hiero-ledger/hiero-sdk-python
  - Hiero DID SDK: https://github.com/hiero-ledger/hiero-did-sdk-python
    - For architecture/implementation details, please see design docs located in the repo
  - ACA-Py plugins: https://github.com/openwallet-foundation/acapy-plugins
- Hedera DID Method spec: https://github.com/hashgraph/did-method/blob/master/hedera-did-method-specification.md
- HCS-1 standard for storing immutable file data on Hedera Consensus Service: https://hashgraphonline.com/docs/standards/hcs-1/

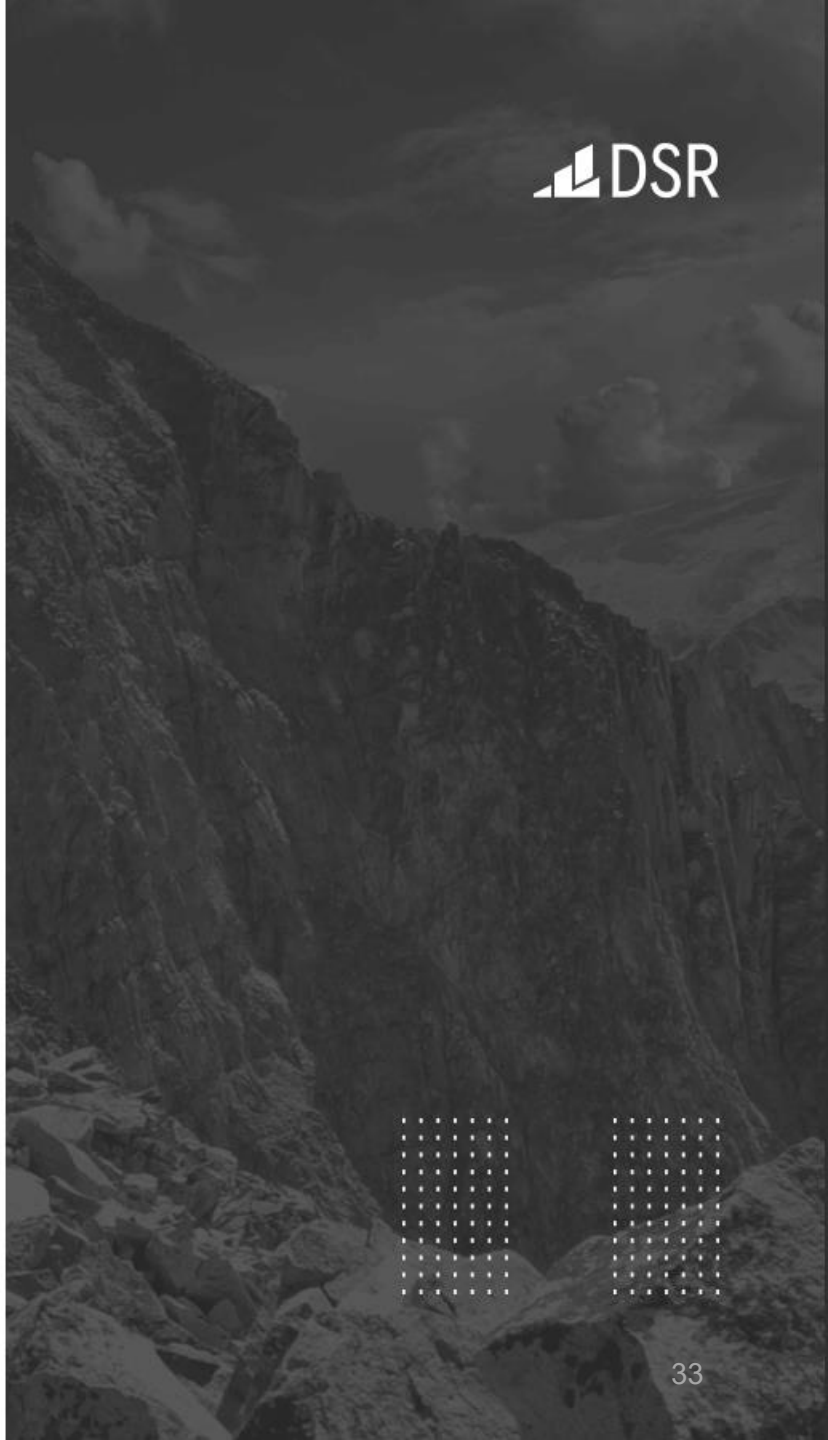
Contacts

- Alexander Shenshin
  - Email: alexander.shenshin@dsr-corporation.com
  - LFDT and OWF Discord: alexander.shenshin
- Keith Kowal
  - Email: keith.kowal@hashgraph.com

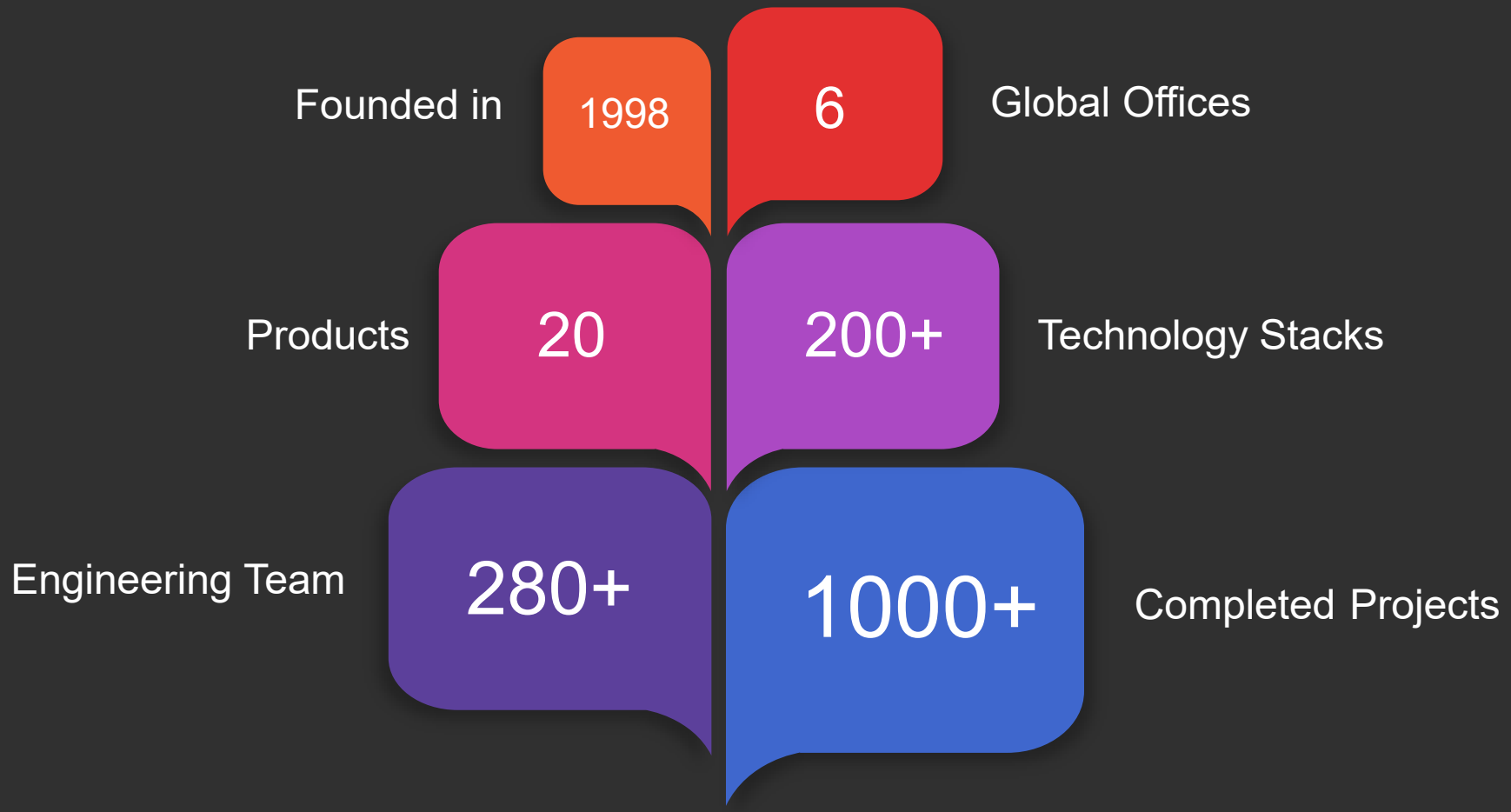
Q&A

- Any questions?

Appendix – About DSR

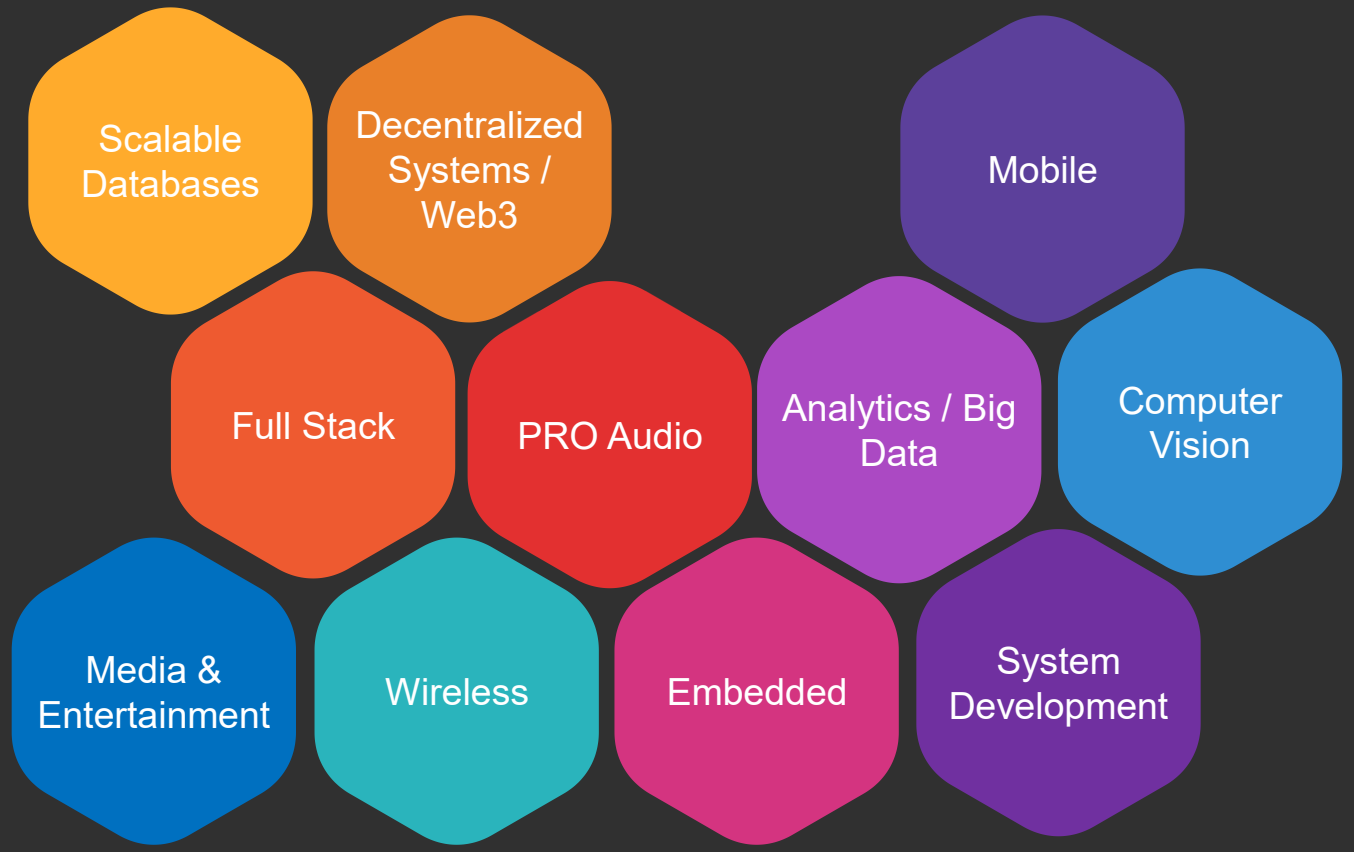


DSR Corporation



Privately-owned US company - custom, complex software development done right

DSR Capabilities



Industry Affiliations

DSR

Bluetooth SIG

CSA

Thread Group

Open Wallet Foundation

Hyperledger Foundation

iOS/Android Developer

MFi Licensee

Trust over IP Foundation

Decentralized Identity Foundation

The Linux Foundation

Industries Served

Media and Entertainment

IoT

Financial and Business Services

Marketing and Advertising

Consumer Electronics

Healthcare / Medical

Avionics

Automotive

Telecom

Server & Data Storage

Industries – Products & Services – Customers

Energy and Consumer Electronics

- Building access control system
- Home security monitoring system (Zigbee)
- Smart metering device
- Participation in development of the Smart Energy Zigbee standard

Transportation

- Toyota Prius 2014 infotainment system
- VW car component
- Aircraft configuration design system
- Wireless communication for highways (802.11p)
- Test suite for ARINC 653, DO-178C certifications

Data Processing

- Secure Document Storage SAAS
- Universal Laboratory Database web-based system
- Server farm infrastructure support system (80,000+ servers)

Web & Telecom Communication

- Dalet system support/maintenance
- Media Asset Management (MAM) web-based system
- Audio quality control system
- IMF format implementation for Netflix

Representative Clients

DSR

DOING SOFTWARE RIGHT

Full Stack Web | Embedded | Wireless

Analytics / Big Data | Scalable Databases | Digital Media

System Software | Mobile | Blockchain | CV / Machine Learning