Decentralized Identity in Supply Chain Context

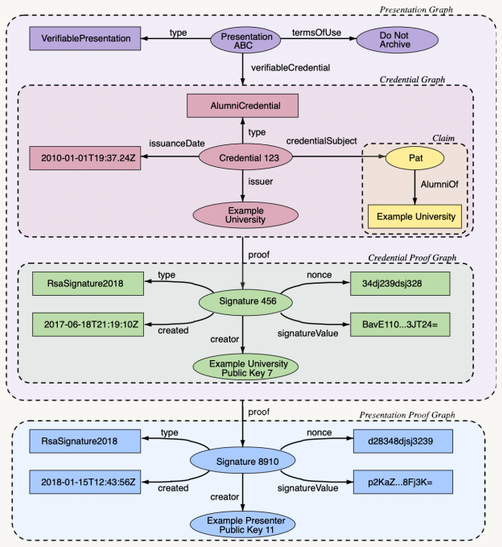
CSB/CSE Capstone Project 2022

Alex D'Alessandro, Emily Grandon, Alex Kline, Rafaela Mantoan Borges
Advisor: Professor Andrea Smith

Preserving Privacy While Managing Identites

Our goal was to create an abstraction layer that enables **Decentralized Identities (DIDs)** and **Verifiable Credentials (VCs)** in **Oracle Blockchain Platform (OBP)** to securely identify people and verify their credentials in a way that doesn't violate their privacy.

We demonstrate this functionality through a **demo application** that leverages the use of DIDs hosted on OBP and allows universities to issue VCs to their students who in turn can present those credentials to potential employers for verification.



What are DIDs?

- Unique digital identifiers
- Rely on asymmetric cryptography for authentication
- No central registration authority
- Provide anonymity
- Stored in a distributed ledger

What are VCs?

- Cryptographically-verifiable digital credentials
- Packaged into a Verifiable Presentation
- Signed by the private key of the issuer's DID
- Countersigned by the holder's DID private key
- Tamper-resistant and easily verified
- Enable selective disclosure

Motivation

In today's world, **identity** is primarily managed by **centralized service providers** and an organization verifying a user's credentials often entails **extensive and invasive background checks** that can share information the user never intended to.

That is why the **principal philosophy** behind this technology is to

- Give **individual control** of identity
- **Eliminate** or reduce trust of **central service providers**
- **Verify identify** while **preserving** individual **privacy**
- Provide **user control** over data sharing

We hope that this demo application highlights the potential of this emerging technology and works as a **proof-of-concept** leading to further applications in

- Licenses
- Medical records
- Financial records

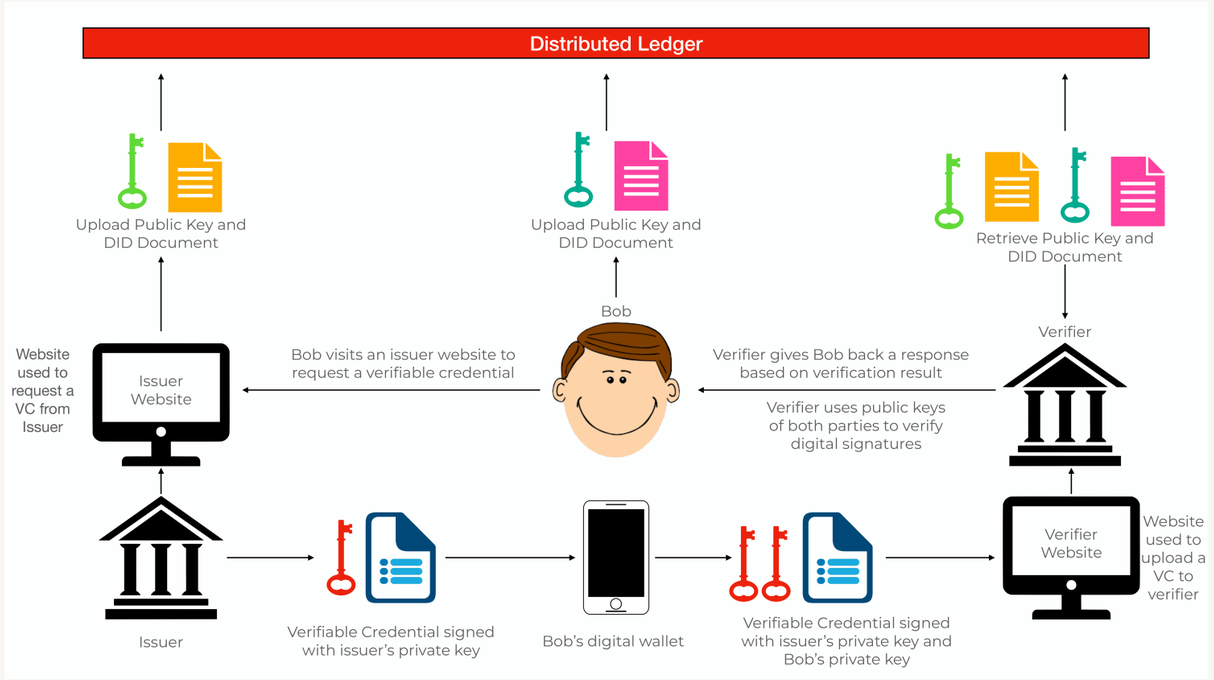
Solution

DID Management

- **Manage** DIDs throughout an OBP-deployed smart contract
- User **creates** an account through Oracle, then creates a private/public key pair associated with a DID
- Any third party can **view** a DID stored **on chain** through a resolve DID method
- With proper MSP ID authentication, a user can **perform updates** on or **remove** a DID

VC Management

- VCs are stored **off-chain** in a user's digital **wallet**
- After DID creation, a user can **store** a VC linked with their DID
- To attain a VC, a user must **request** one from an issuer website
- VCs contain a **proof section** which can be decrypted with corresponding public keys
- A verifier must **retrieve** the public keys associated with the DID of both the issuer and receiver to complete digital signature **decryption**
- If the digital signatures decrypt, a **verifier** can be **positive** that the digital diploma has not been tampered with



Contributions

Implemented DIDs and VCs in OBP allowing it to:

- Give control back to users **(self-sovereign identity)**
- **Eliminate central location** storing user id
- **Increase** trust, **reduce** fraud
- Ensure **transparency**
- **Speed up** verification

Future Work

Full integration with other **Oracle** and **Hyperledger Fabric** products