Finance Use Case

An individual applying for a loan online from a traditional banking system is obligated to present a government-issued citizen ID and proof of employment. This is because the know-your-customer process for being granted a loan needs the applicant to comply with federal regulations.

However, the process would be much simpler (and identity of the applicant better protected) if a Decentralized Identity Network or a Consortium Identity Network were to be instead. The participants in a Decentralized Identity Network would be the applicant, the government, the applicant's employer, the applicant's bank, and the public permissioned network.

Digital Identity Network

The ensuing process can be understood as follows: ...

Step 1

Rayan acquires a government-issued citizen ID

Step 2

Rayan uses it to secure employment

Step 3

Rayan receives proof of employment from his employer

Step 4

Rayan leverages his citizen ID and proof of employment to apply for a loan

Step 5

The bank verifies Rayan and grant him the loan that had been applied for

Decentralized Identity Network actions:

Examine > Issue > Hold > Present > Verify

Tasks such as vetting, due diligence, regulatory compliance are mandatory for participants to validate claims about identity traits. The information collected for these purposes are generally in hard copies, and the liability of the claims made lies squarely on the entity executing the vetting process. The applicant had to satisfy the vetting criteria to obtain a government-issued citizen ID wherein the government attests his name, date of birth, address, citizenship, and more.

Examine > **Issue >** Hold > Present > Verify

Once the government and the applicant's employer have satisfactorily examined the applicant a cryptographically-signed verifiable credential is generated and delivered. This credential encompasses a set of claims that follow a predefined schema. This credential and each issuer's decentralized identifier (DID) are then published on the public, permissioned ledger for any verifier to assess.

Examine > Issue > **Hold>** Present > Verify

Following the vetting process, the applicant establishes a link with the government's issuer service using his digital wallet. His government-issued citizen ID and peer-to-peer relationship with his employer in the form of verifiable credentials are stored it in this digital wallet. Along with these, he also stores his verifiable credential version of a proof of employment certificate here.

Examine > Issue > Hold > **Present >** Verify

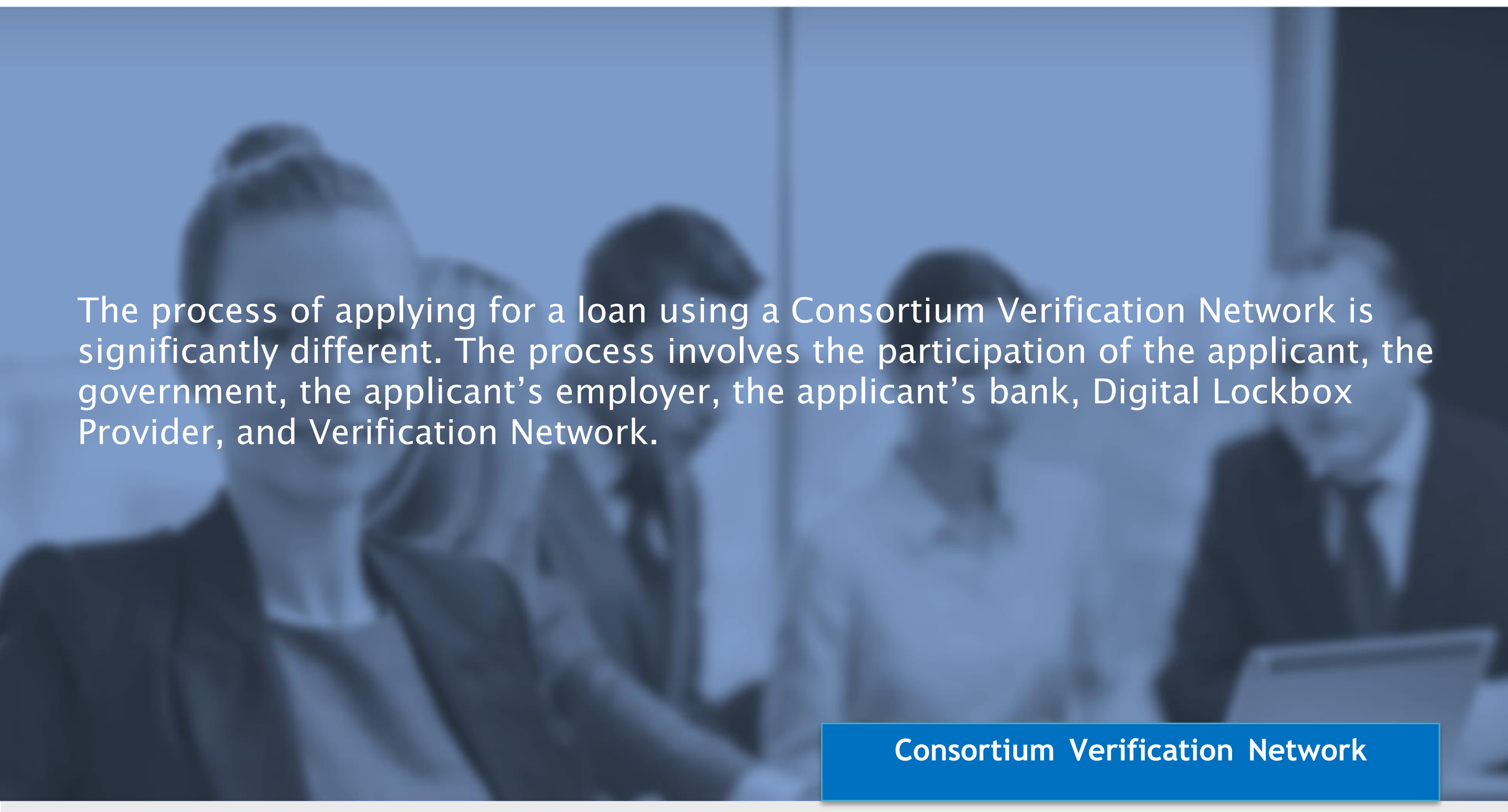
The user then furnishes the required number of credentials to an entity as a validation of identity. When the applicant uses his digital wallet to provide his verifiable credentials to his employer, he is given a proof request reflecting the employer's verification process. He selectively discloses the identity traits required to send a proof response uses his citizen ID verifiable credential in his digital wallet.

Similarly, the applicant also uses his digital wallet to provide his verifiable credentials to the bank and selectively disclose the identity traits required for a proof response

Examine > Issue > Hold > Present > **Verify**

The applicant sends in a request for a loan and is subsequently required to furnish traits that have been attested by trusted issuers on the network. In accordance with the bank's process and policy, it requires the applicant to provide his citizen ID and employer information, as part of the proof request. The bank turns to the decentralized identifier (DID) that is publicly visible and cryptographically verifiable to procure the required information attested by the government and the employer.

Continue to Consortium Verification Networkonnext page



The process of applying for a loan using a Consortium Verification Network is significantly different. The process involves the participation of the applicant, the government, the applicant's employer, the applicant's bank, Digital Lockbox Provider, and Verification Network.

Consortium Verification Network

...and they would take following steps:

Step 1

The applicant gets to pick his Digital Lockbox Provider, who is a founding member of the Verification Network.

Step 2

The applicant confirms his identity traits using his Verification Network application.

Step 3

The Verification Network is used by the applicant's employer to verify the government's claims about the applicant

Step 4

The Verification Network is then used by the bank to verify the government's and employer's claims about the applicant.

The Consortium Verification Actions Include:

Examine > Hold > Present > Verify

Required vetting is performed to conform to regulatory compliance accompanied by other tasks required to make a claim about an identity trait reliable. Once again, the documentations are in hard copies and the liability of the claims made rests on the entity performing the vetting process. The applicant is registered based on the vetting policies of the Digital Lockbox Provider and the Verification Network, and he is given an identity token. This identity token will be used to interact with the network via the Digital Lockbox Provider.

Issue

A credential consisting of a set of claims that is in accordance with certain predefined schema is generated and delivered.

Examine > **Hold >** Present > Verify

Individual or organization hold a credential, and systems of record about relationships Digital Asset Providers have with individuals such as the applicant are maintained by them.

Examine > Hold > **Present >** Verify

The user presents one or more credentials to an entity as proof of identity. The applicant uses the mobile app to give consent to the Digital Asset Providers in the Verification Network before the employer and bank performing verification transaction requests as Digital Asset Consumers.

Examine > Hold > Present > **Verify**

Validate authenticity of issuer and holder then consume data.

During David’s life experience, he graduated from a university and applied for a job. When applying for work, his employer challenges David to present his identity traits attested to by known and trusted issuers. The employer uses the Verification Network to verify the data known by Digital Asset Providers and validated by David.

The Bank receives David’s request to apply for a loan and challenges him to prove identity traits attested by trusted and known issuers on the network. The Bank uses the Verification Network verify the data known Digital Asset Providers and validated by David.