Finance Use Case

David Vincent wants to apply for a loan online. His bank's know-your-customer process for obtaining a loan needs to be compliant with federal regulations. As such, David is required to present a government-issued citizen ID and proof of employment.

Let's compare how David could use a Decentralized Identity Network or a Consortium Identity Network to make the process easier and more secure for him, seamlessly protecting his identity.

In a Decentralized Identity Network, the participants would be...

David | The government | David's employer | David's bank | Public permissioned network

Decentralized Identity Network

...and they would take following steps:

Step 1
David obtains a government-issued citizen ID

Step 2
David uses that government-issued citizen ID to apply for a job

Step 3
David receives proof of employment from his employer

Step 4
David leverages his citizen ID and proof of employment to apply for a loan

Step 5
The bank verifies David and issues him a loan

Decentralized Identity Network actions:

Examine > | Issue > | Hold > | Present > | Verify

Participants perform required vetting, due diligence, regulatory compliance and other tasks needed to establish confidence in making a claim about an identity trait. The documentation required for this process is typically not in digital form. The entity performing the vetting process takes on all liability about the claims they make.

In order for David to have obtained his government issued citizen ID, he had to meet the examination/vetting criteria for the issuance of a verifiable credential. Upon completion of the vetting process the government felt confident in making attestations (claims) about his name, date of birth, address, citizenship, and more.

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

Generate and deliver a Credential comprised of a set of Claims in accordance with some predefined schema.

The government and David's employer have done their due diligence in examining David and issue cryptographically-signed verifiable credentials attesting to David's citizenship and employment, respectively. These verifiable credentials are based off claim schemas, consisting of attested attributes each issuer and their digital signatures. Claim schemas for the government-issued citizen ID and a proof of employment certificate are published on the public, permissioned ledger along with each issuer's decentralized identifier (DID) for any verifier to resolve. Exchanges of these verifiable credentials are done point to point, directly with David, specific to each relationship he has. In this case, point-to-point with the government and his employer.

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

Individual or organization holds a credential.

- Upon completion of his vetting experience with the government, David uses his digital wallet to connect with the government's issuer service. Through this interaction he obtains his government-issued citizen ID in the form of a verifiable credential and stores it in his digital wallet.
- David uses his digital wallet to establish a personal (peer-to-peer) relationship with his employer. He requests a verifiable credential version of a proof of employment certificate from his employer's issuing service. David stores this new credential in his digital wallet along with a private decentralized identifier (DID) unique to his relationship with his employer.

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

User presents one or more credentials to an entity as proof of identity.

- When David interacts with his employer, he uses his digital wallet to share his verifiable credentials issued by the government. He accepts a proof request coinciding with the employer's verification process and uses the corpus of his citizen ID verifiable credential in his digital wallet to selectively disclose the required identity traits necessary to send a proof response.
- When interacting with his bank, David also uses his digital wallet to share his verifiable credentials issued by the government and his employer. He accepts a proof request coinciding with the bank's verification process and uses the corpus of his citizen ID and proof of employment certificate verifiable credential in his digital wallet to selectively disclose the required identity traits necessary to send a proof response.

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

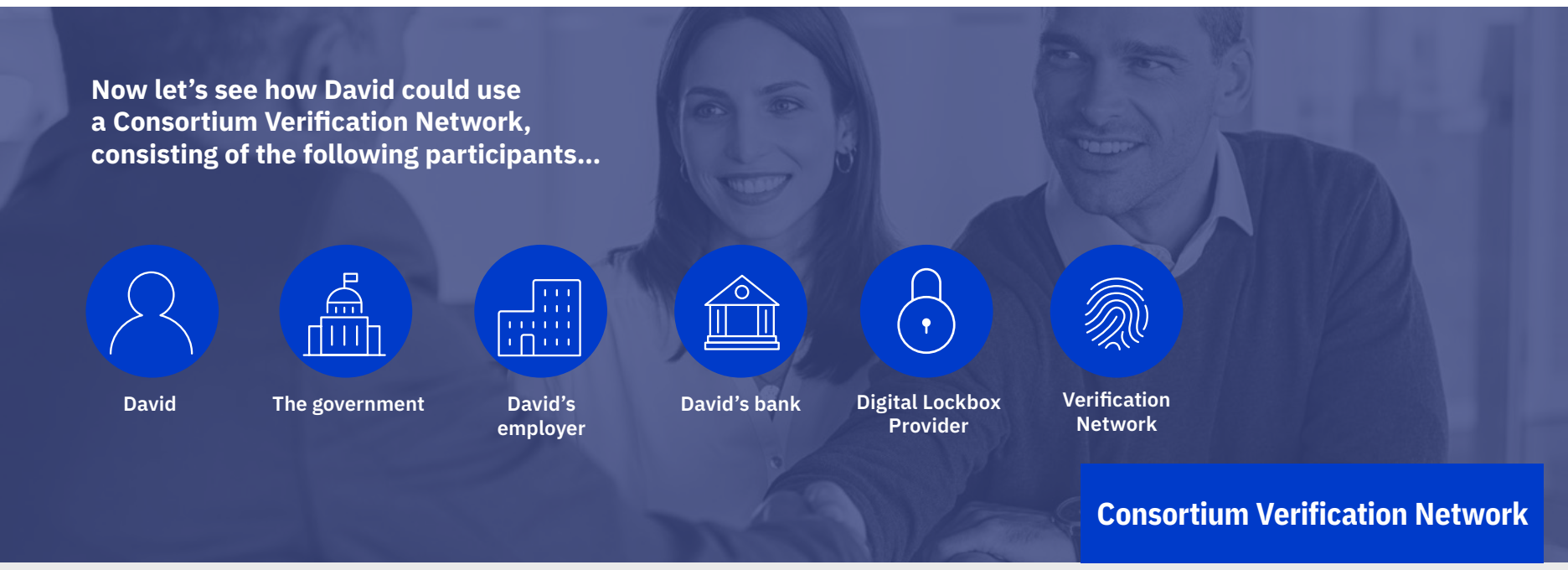
Validate authenticity of issuer and holder then consume data.

During David's life experience, he graduated from a university and applied for a job. When applying for work, his employer challenges David with a proof request for identity traits attested to by known and trusted issuers in accordance with his employer's process and policy. The employer uses the public, permissioned ledger to establish trust in the government because their decentralized identifier (DID) is publicly visible and cryptographically verifiable.

The bank receives David's request to apply for a loan and challenges his to prove identity traits attested by trusted and known issuers on the network. As part of the proof request, the bank requires David to present his citizen ID from the government and employer information for the employer. This proof request is in accordance with the bank's process and policy. The bank uses the public, permissioned ledger to establish trust with the government and employer because their decentralized identifier (DID) is publicly visible and cryptographically verifiable.

Continue to Consortium Verification Network on next page

IBM **Blockchain** Trusted Identity™



Now let's see how David could use a Consortium Verification Network, consisting of the following participants...

David | The government | David's employer | David's bank | Digital Lockbox Provider | Verification Network

Consortium Verification Network

...and they would take following steps:

Step 1

David choses his Digital Lockbox Provider, who is a founding member of the Verification Network

Step 2

David uses his Verification Network application to confirm identity traits known by identity providers in the Verification Network

Step 3

David's employer uses the Verification Network to verify the government's claims about David

Step 4

The bank uses the Verification Network to verify the government's and employer's claims about David

Consortium Verification Network actions:

Note: The "Issue" action is not used in this network. See below for further details.

Examine > | Hold > | Present > | Verify

Perform required vetting, due diligence, regulatory compliance and other tasks needed to establish confidence in making a claim about an identity trait. The documentation required for this process is typically not in digital form. The entity performing the vetting process takes on all liability about the claims they make.

Registers David based on the vetting policies of the Digital Lockbox Provider and the Verification Network. David is required to download a mobile app, Verified.Me, and is given an identity token to interact with the network via the Digital Lockbox Provider. David is required to use the provided identity token in every transaction.

Issue

Generate and deliver a Credential comprised of a set of Claims in accordance with some predefined schema.

There is no concept of the issuing of credentials in a Consortium Verification Network. David's Identity Traits are known by the Verification Network, are confirmed by him and used by the Digital Asset Providers to respond to verification transaction requests by Digital Asset Consumers.

Digital Asset Providers in this scenario could be the government and employer, while Digital Asset Consumers in this scenario could be the employer and bank.

Examine > | **Hold >** | Present > | Verify

Individual or organization holds a credential.

Digital Asset Providers maintain systems of record about relationships they have with individuals like David.

Examine > | Hold > | **Present >** | Verify

User presents one or more credentials to an entity as proof of identity.

Prior to the employer and bank performing verification transaction requests as Digital Asset Consumers, David uses his mobile app to provide consent to the Digital Asset Providers in the Verification Network.

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.