IBM **Blockchain** Trusted Identity™

Healthcare Use Case

Alice Garcia needs to get bloodwork done after her most recent physical exam. Her doctor has given her a bloodwork order to take to a local clinic.

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

Alice arrives at the clinic and needs to provide the order, her proof of insurance and her driver's license. In a Decentralized Identity Network, the participants would be...

- Alice
- Her doctor's office
- The clinic
- Her healthcare insurance company
- The Department of Motor Vehicles (DMV)

Decentralized Identity Network

...and they would take following steps:

Step 1

Alice has her insurance and driver's license credentials in her digital wallet, issued by the Insurance company and DMV

Step 2

After her physical, Alice's doctor's office issues a bloodwork order digital credential

Step 3

Alice visits the clinic for her bloodwork, providing her insurance, driver's license and bloodwork order credentials

Step 4

The clinic verifies Alice's credentials and performs blood work

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 Alice to have obtained her driver's license, she had to meet examination/vetting criteria for the issuance of a verifiable credential. Upon completion of the vetting process the DMV felt confident in making attestations (claims) about her name, date of birth, address, citizenship and more.

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

Paritcipants generate and deliver a credential comprised of a set of claims in accordance with some predefined schema. As a note, no PII resides on the public ledger.

The DMV, Alice's health insurance company and her doctor's office have done their due diligence in examining Alice and issues cryptographically-signed verifiable credentials attesting, respectively, to her driver's license, insurance coverage and bloodwork order. These verifiable credentials are based off a claim schema consisting of attested attributes from each issuer and their digital signatures. Claim schemas for her driver's license, insurance coverage and bloodwork 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 Alice, specific to each relationship Alice has. In this case, point to point with the DMV, Insurance company, and her doctor.

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

Individual or organization holds a credential.

- After Alice has completed vetting with the DMV, insurance company and doctor's office, each of these known and trusted entities issue verifiable credentials for Alice to store in her digital wallet.
- Each contains a private, pair-wise decentralized identifier (DID) with each relationship she has: the DMW, her insurance company and her doctor's office.

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

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

Alice uses her digital wallet when interacting with the clinic to share her verifiable credentials. Alice accepts a proof request from the clinic that coincides with their verification process and uses the corpus of her driver's license, insurance and bloodwork order verifiable credentials in her digital wallet to selectively disclose the required identity traits necessary to send a proof response.

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

Participants validate authenticity of issuer and holder, then consume data as defined through their verification process which can be verified through a web of trust rooted in the public ledger.

Alice has built relationships with her insurance provider and doctor. Over time, she leverages her digital wallet to present verifiable credentials accepted by her insurance company and her doctor through challenging Alice with proof requests for identity traits attested to by known and trusted issuers. This proof request is in accordance with processes and policies of the insurance company and doctor's office. The insurance company and doctor's office use the public, permissioned ledger to establish trust with other known and trusted issuers because their individual decentralized identifier (DID) is publicly visible and cryptographically verifiable.

Once Alice arrives at the clinic, Alice identifies herself through a point to point exchange with a device. The device challenges Alice with a proof request to present her driver's license, insurance and bloodwork credentials issued by the DMV, insurance company and doctor's office, respectively. This proof request is in accordance with the clinic's process and policy. The clinic uses the public, permissioned ledger to establish trust with the DMV, insurance company and doctor's office because their individual decentralized identifier (DID) is publicly visible and cryptographically verifiable.

Continue to Consortium Verification Network on next page

IBM **Blockchain** Trusted Identity™

IBM

Now let's see how Alice would use a Consortium Verification Network, which would consist of the following participants...

- Alice
- Her doctor's office
- The clinic
- Her healthcare insurance company
- The Department of Motor Vehicles (DMV)
- Digital Lockbox Provider
- Verification Network

Consortium Verification Network

...and they would take following steps:

Step 1

Alice chooses her Digital Lockbox Provider — a founding member of the Verification Network

Step 2

Alice uses her Verification Network application to confirm identity traits known by identity providers in the Verification Network including the DMV, her insurance company and her doctor

Step 3

The insurance company and doctor's office use the Verification Network to verify claims about Alice

Step 4

At the clinic, Alice uses the Verification Network to verify claims about her from the DMV, her insurance company and her doctor's office

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 Alice based on the vetting policies of the Digital Lockbox Provider and the Verification Network. Alice downloads the mobile app Verified.Me and is given an identity token to interact with the network via the Digital Lockbox Provider. Alice must use the provided identity token in every transaction.

Issue

Participants generate and deliver a credential comprised of a set of claims in accordance with some predefined schema.

Unlike a Decentralized Identity Network, **credentials are not issued in a Consortium Verification Network**. Alice's identity traits are known by the Verification Network are confirmed by her and used by Digital Asset Providers to respond to verification transaction requests by Digital Asset Consumers.

Digital Asset Providers in this scenario could be the DMV, Alice's insurance company and her doctor's office, while Digital Asset Consumers could be her health insurance company, doctor's office and the clinic.

Examine > **Hold >** Present > Verify

Individual or organization holds a credential.

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

Examine > Hold > **Present >** Verify

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

Prior to her insurance company, doctor's office and clinic performing a verification transaction request as Digital Asset Consumers, Alice uses her mobile app to provide consent to Digital Asset Providers in the Verification Network. This presentment requires Alice to be online to provide consent of sharing her identity.

Examine > Hold > Present > **Verify**

Validate authenticity of issuer and holder, then consume data.

When Alice selected an insurance provider and doctor, they challenged Alice to present identity traits attested to by known and trusted issuers. The insurance company and doctor's office use the Verification Network to verify data known by Digital Asset Providers and validated by Alice.

The clinic receives Alice's request to get her bloodwork done and challenges her to prove identity traits attested by trusted and known issuers on the network. The clinic uses the Verification Network to verify the data known by the DMV, her insurance company and her doctor's office, and validated by Alice.