Government Use Case

The applicant is a fresh graduate from college and has landed her first job. Now, she has decided to lease a car and insure it. The applicant needs to furnish proof of employment and driver's license to both the car dealer and the insurance company. After a few weeks of using the new car, the police pulls her over for a traffic violation. She is asked by the officer to show her driver's license, proof of auto registration and insurance. Now we will draw a comparison on how the applicant could make the process more secure (such as protecting her identity) and easy by using a Decentralized Identity Network or a Consortium Identity Network.

The participants in a Decentralized Identity Network, would be…

- **The applicant**
- **The Department of Motor Vehicles (DMV)**
- **The applicant's employer**
- **The Insurance Company**
- **The Car Dealer**
- **The Leasing Company**
- **Public Permissioned Network**
- **The Police Officer**

Digital Identity Network

The process will require the following steps:

Step 1
The applicant gets a driver's license

Step 2
She acquires the proof of her employment from the employer

Step 3
She gets approval for an auto lease by using the driver's license and proof of employment

Step 4
She gets auto insurance by using her driver's license and proof of employment

Step 5
Using her driver's license she registers the new car

Step 6
Using the applicant's digital credentials the car dealer finalizes the sale

Step 7
The applicant furnishes her driver's license, insurance and auto registration to the police officer

DECENTRALIZED IDENTITY NETWORK ACTIONS

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

Accomplish the necessary tasks such as checking, due diligence, regulatory compliance and the others that are required to confirm a claim related to an identity trait. The documents needed for the completion of the process is usually not digital. Hence the liability of all the claims made falls upon the individual/organization involved with the vetting process.

To acquire a driver's license the applicant had to fulfill the criteria of examination or vetting so that the verifiable credential could be issued. The completion of the vetting process gave the government confidence to make attestations (claims) about the applicant's name, address, date of birth, citizenship, and other necessary details.

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

Produce and deliver a Credential that comprises of a set of Claims in compliance with some predefined plan.

By issuing cryptographically signed verifiable credentials that attests to her proof of employment, lease agreement, vehicle insurance and registration and driver's license the applicant's employer, auto leasing company, insurance company and the DMV have done their part in confirming the credentials provided by her. These verifiable credentials are based on a claim scheme that consists of confirmed traits from every issuer along with their digital signatures. Claim schemes related to the applicant's employment proof, lease agreement, vehicle insurance documents, driver's license and vehicle registration are published on the public and permissioned ledger. It also has each of the issuer's decentralized identifier (DID) for any kind of verification. Any kind of exchange related to these verifiable credentials are done point to point, directly with the applicant. In this specific case, point to point with the applicant's employer, leasing company, insurance company and the DMV. After completion of the car sale the applicant is handed the keys of her car and she is also provided with a digital bill as proof of the auto sale. By issuing cryptographically signed verifiable credential confirming the bill of the new auto sale, the car dealer completes the business process. This specific verifiable credential is centered on a claim scheme that comprises confirmed attributes from the car dealer that are digitally signed. The claim scheme for the auto sale bill is issued on the ledger linked with the car dealer's decentralized identifier (DID) for any further verification.

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

The credential is held by an individual or organization

- After the inspection experience with the Government is complete, the applicant makes use of her digital wallet so that she can connect with the issuer service of the Government. The applicant is able to acquire her present identity characteristics, as a verifiable credential, and store it in her digital wallet, through this interaction.
- Using her digital wallet, the applicant is able to create personal/peer to peer relationships with specific individuals/organizations. She gets a new credential in her digital wallet and a private decentralized identifier (DID) through this interaction. The new credential issues is exclusive proof to her relationship with the particular individual/organization.
  - **Employer:** She asks for a verifiable credential version of employment proof from her employer's issuing service.
  - **Leasing company:** The car dealer delivers the applicant a point-of-sale device. This device initiates a proof request from the issuing service of the leasing company. This process needs the applicant to show her driver's license and employment proof.
  - **Insurance company:** The applicant is provided with a point-of-sale device by the car dealer which initiates a request for proof from issuing service of the insurance company. This process needs the applicant her to show her driver's license and employment proof. service requiring her to present her driver's license.
  - **DMV:** The applicant is provided with a point-of-sale device by the car dealer that initiates a request for proof from the issuing service of government's vehicle registration. The process needs her to show her driver's license.

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

As proof of identity the user furnishes one or more credentials to an individual/organization

The applicant (Person to Organization)
The applicant needs to create peer-to-peer identity relationships with individuals/organizations (employer, leasing company, insurance company, DMV and car dealer) that dispense her verifiable credentials. She makes use of her digital wallet when she interacts with her identity relationships. By accepting a proof request that matches with the individual/organization's verification process, the applicant establishes a connection with each of the identity relationships. Along with that, she uses the corpus of her verifiable credentials in her digital wallet to disclose selectively the needed identity characteristics that is required to deliver a proof response.

The Applicant (Person to Person)
The applicant is needed to create peer to peer identity relationships with the police officer. Using the officer's smartphone she addresses an identity challenge or proof request. The interaction that she has with the officer can be online. In case there is no internet access the sharing of verifiable credentials can be done offline as well. The applicant acknowledges the proof request using the corpus of her verifiable credentials using her digital wallet. This allows her to selectively reveal the necessary identity characteristics required to send a proof response.

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

The authenticity of issuer and holder is validated by the participants and the data is consumed as defined via the verification process. It can be validated with the help of a web of trust that can be found in the public ledger.

The Applicant (Person to Organization)
Before issuing a verifiable credential to the applicant, the individual/organization (employer, leasing company, and insurance company, DMV and car dealer) needs to validate the content in the proof response. After that the information needs to be processed in compliance with the policies of the organization related to the credentials issuing process. The public and permissioned ledger is used by the organization to create trust in the organization that digitally signed each and every identity traits available in the proof response. They use the ledger because the decentralized identifier (DID) of each issuer is visible publicly and can be verified cryptographically.

The Applicant (Person to Person)
It is very essential that the police officer is able to establish trust in authenticity of the information provided by the applicant as the information represents the claims about her. The content received in a proof response must be verified by the officer. Then it needs to be processed in compliance with government policies related to traffic rules. The public and permissioned ledger is used to establish trust in the issuing organizations that signed each of the identity traits provided in the proof response digitally. The ledger is put to use because each of the issuer's decentralized identifier (DID) is visible

publicly visible and can be verified cryptographically.

.

Continue to Consortium Verification Network on next page

HC **Blockchain** Digital Identity™

Consortium Verification Network

This requires one to follow the following steps:

Step 1
The applicant choses her Digital Lockbox Provider, which is a founding member of the Verification Network

Step 2
The applicant makes use of her Verification Network application to approve identity traits that are known by the identity providers in the Verification Network

Step 3
The Verification Network is used by the leasing company to validate the claims that are made regarding the applicant by the government and her employer before the lease agreement is approved

Step 4
The insurance company uses the Verification Network so that they can validate the claims that are made about the applicant by the government and her employer before the insurance policy is approved

Step 5
The DMV uses the Verification Network so that they can validate the claims made about the applicant by the government before the car is registered

Step 6
The car dealer completes the sale of the new car to the applicant

Step 7
The police officer uses the Verification Network to verify the information presented in paper by the applicant

CONSORTIUM VERIFICATION NETWORK ACTIONS:

Examine > | Hold > | Present > | Verify

Accomplish the necessary tasks such as checking, due diligence, regulatory compliance and the others that are required to confirm a claim related to an identity trait. The documents needed for the completion of the process is usually not digital. Hence the liability of all the claims made falls upon the individual/organization involved with the vetting process.

The applicant gets registered basing on the vetting policies used by the digital lockbox provider along with Verification Network. She will have to download an application. After that she will be given an identity token to interact with the network using the digital lockbox provider. The applicant needs to provide identity token in every transaction that she performs.

Issue

Produce and deliver a Credential that comprises of a set of Claims in compliance with some predefined plan

There is no concept related to the issuing of credentials in a Consortium Verification Network. The applicant's identity traits are known by the Verification Network and they are confirmed by her as well as by the Digital Asset Providers to respond to verification transaction requests by Digital Asset Consumers. Digital Asset Providers in this case involves the DMV, the applicant's employer, insurance company and the car leasing company. The Digital Asset Consumers in this case are the car dealer and the police officer.

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

Credential is held by an Individual or organization

Comprised of Digital Asset Providers who maintain systems of record about relationship they have with the applicants.

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

The credential is held by the Individual or organization

The user furnishes one or more credentials to an individual/organization as an identity proof.
Before her employer and bank performs the required verification transaction requests as Digital Asset Consumers, the applicant will use her mobile app to consent to the Digital Asset Providers in the Verification Network.

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

Consume data after verifying the credibility of the issuer and holder

There are multiple verification checks that needs to be performed by the salesman to complete the sale. All that has to be in compliance with the business workflow processes of the car dealer. Based on the verbal information given by the applicant, the salesman will perform multiple proof requests to the Verification Network to verify the data known by Digital Asset Provider:

- Driver's License data is verified by the DMV
- The income and employment status of the applicant is verified by the employer. The applicant's policy data is verified by the insurance company
- The lease agreement is approved by the leasing company after successfully verifying the applicant's income and employment status

· The applicant furnishes the police officer with physical documents that represents her driver's license, auto registration and insurance. The police officer using a device in the patrol car obtains the identity traits of the applicant by scanning the barcodes on the documents. The officer then makes use of the same device to submit a proof request to the Verification Network to validate the data known by Digital Asset Providers (DMV, insurance company) and the one validated by the applicant.