Data Sharing Using Verifiable Credentials in the Agriculture Sector

Paul Ashley(✉)

Anonyome Labs, Gold Coast 4217, Australia
pashley@anonyome.com

Abstract. The agricultural sector faces new challenges. Consumers now expect that food they eat is good for them and good for the environment. Fear of climate change is driving more regulation and data compliance requirements. There are new global standards of data verification requiring agriculture to confirm to these standards for international export. This paper describes the technical implementation details of a Decentralized Agricultural Ecosystem aiming to share data in a secure way; an approach that will allow farmers and growers to capture, manage and share their data while also controlling and protecting it.

Keywords: Verifiable Credentials · Verifiable Data · Decentralized Identity

1 Introduction

Around the world expectations, requirements and standards in the agriculture industry are changing. Greater proof of provenance and or other environmental and marketing claims and practices, are being demanded by regulators as well as consumers mindful of the ethical, sustainable and environmental impacts of what they buy.

To support this new world, agricultural enterprises need to exchange verifiable data across the whole supply chain in a way that respects the ownership of the data. This involves agricultural related enterprises coming together to form an ecosystem for exchanging trusted data. This ecosystem includes, but is not limited to:

- Farms
- Banks
- Fertilizer Companies
- Meat producers
- Crop producers
- Milk producers
- Geo-Surveyors
- Wholesalers
- Government
- more

N. Dong et al. (Eds.): SDLT 2023, CCIS 1975, pp. 72–81, 2024.
https://doi.org/10.1007/978-981-97-0006-6_5

Each of these enterprises participates in the network by exchanging data in a trusted way.

This paper describes the technical implementation of a Decentralized Agricultural Ecosystem to satisfy the requirements of regulators and consumers. It takes a decentralized approach and is founded on the decentralized identity based verifiable credentials technology. It is implemented in a way to allow the data owners full control of their data and entities in the network can independently verify data they receive.

2 Implementation of a Decentralized Agricultural Ecosystem

To meet the requirements imposed on the agricultural industry a new data exchange system has been developed and implemented using decentralized identity (DI) based verifiable credentials. As shown in Fig. 1, the decentralized identity verifiable credential system involves three key parties:

- **Issuer:** This entity creates a verifiable credential holding key data and transfers it to the holder. An example of an issuer in the network would be a Green House Gas (GHG) emissions certifier.
- **Holder:** This entity requests, receives, stores, and presents the verifiable credential. A holder uses a decentralized identity wallet. An example of a holder is a farm owner.
- **Verifier:** This entity receives the verifiable credential (as a presentation proof) from the holder and is able to verify the identity of the issuer and integrity of the data. An example of a verifier is a Government department checking the GHG emissions of a farm.

Also shown is the ledger or blockchain that provides the *trust foundation* for the system.

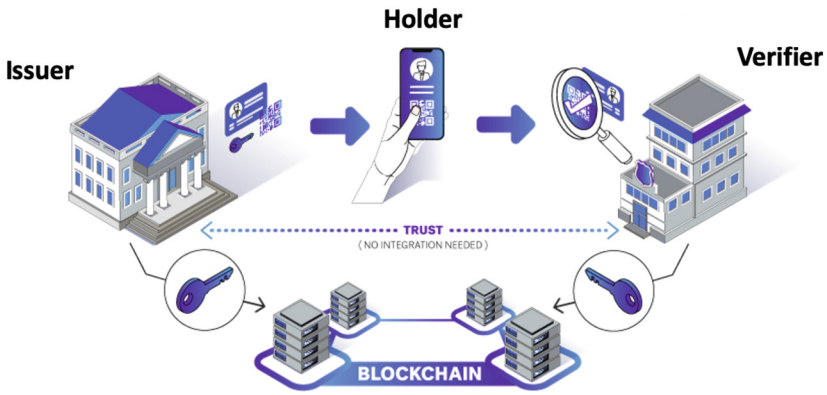

Fig. 1. The Verifiable Credential Data Exchange System

Figure 1 is also commonly called the *Triangle of Trust*. The holder (the farmer) wishes to receive a credential from the issuer (e.g. organic certifier), which they in turn present to the verifier (e.g. wholesaler).

To bootstrap the issuing of a verifiable credentials the issuer writes to the blockchain, in this case it is writing to the Hyperledger Indy network [1]. The issuer writes their Decentralized Identifier (DID) and associated information, the verifiable credential schema, and the verifiable credential definition.

The issuer is then in a position to issue verifiable credentials to the holders. The first step is to establish a DIDComm connection with the holder. Once a connection is established the issuer can present a credential issue offer to the holder. The holder then approves the offer, the verifiable credential is issued, and stored in the holder's wallet.

Once the holder has the credential it is in a position to accept a presentation proof request from a verifier. The holder (wallet) formulates the presentation proof (which could in fact be derived from multiple credentials) and delivers that to the verifier. The verifier can verify the proof by obtaining the issuer information from the blockchain. No communication is required back to the issuer.

2.1 Why Use a Decentralized Model?

Organizations want to protect their own data and share that data in a way that gives the organization more control.

Decentralization helps move the data under the stewardship of the organization to whom it belongs. Decentralization stops the direct integration between third parties. The organization is the integration point. They choose what data to share, with whom and where they want to share it, and how much of their data they want to share. That lets the organization perform the integration by following standard decentralized identity protocols.

In the Agricultural Ecosystem project the organization's data (farm data) is shared using verifiable credentials. In the issuing process the farm can receive a verifiable credential. The farm can then present that verifiable credential (presentation proof) to a relying party (verifier). There is no direct integration between issuer and relying party.

2.2 Verifiable Data Registry

The Verifiable Data Registry (VDR) is the technical term for blockchain/distributed ledger used as the *Trust Layer* for the network. The purpose of the VDR is to provide an immutable storage of information such as DIDs, public keys, service endpoints, credential schemas and so on.

The Agricultural Ecosystem uses Hyperledger Indy as its Trust Foundation. It is a project within the Linux Foundation. Hyperledger Indy's characteristics are shown in Table 1.

2.3 Verifiable Credential

Verifiable credentials are digitally signed documents that carry claims (attributes) about the subject (usually a person or organization) of the credential. For example, a plastic driver license can be re-created in a digital form as a verifiable credential. Almost any document or identity card can be made into a verifiable credential.

Table 1. Hyperledger Indy Ledger Characteristics

KEY AREA	DESCRIPTION
PUBLIC LEDGER	All data written to the ledger is open to be read by anyone
PERMISSIONED NETWORK	To write to the ledger an entity must be an approved endorser. An endorser is approved by the organization overseeing the ledger e.g. Sovrin Foundation. The endorser must agree to certain terms e.g. will not write Personally Identifiable Information (PII) to the ledger. In the Agricultural Ecosystem project each issuer is configured as an endorser. In addition, in comparison to permission-less networks, only approved validator nodes can be added to the ledger network
CONSENSUS ALGORITHM	Validator nodes on the ledger must come to agreement (consensus) before anything is written to the ledger. The Redundant Byzantine Fault Tolerance (RBFT) consensus algorithm is implemented. The size of the Hyperledger Indy network is restricted to around 24 validator nodes
GOVERNANCE	Governance is implemented in an offline and centralized way. Any changes to the governing rules is voted on through offline method, for example, by signing paper documents, rather than using on-ledger governance methods
ECONOMIC MODEL	The organization that supervises the running of the ledger e.g. Sovrin Foundation, charges for writes to the network (usually by charging an annual fee for unlimited writes)

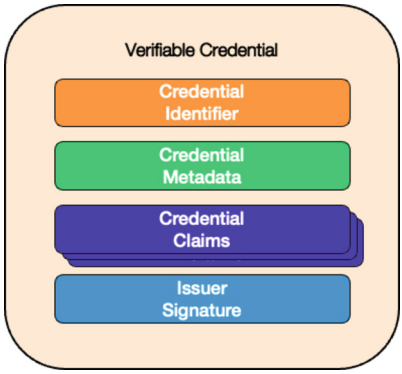

Fig. 2. Verifiable Credential Data Structure

Figure 2 shows the general form of a verifiable credential. There is an identifier and some metadata. It also holds claims that the issuer is asserting about the subject (user or organization). The issuer adds a signature to the verifiable credential so that a verifier can prove the credential's integrity.

There are significant advantages of verifiable credentials for user privacy. When the user (holder) is asked to present the credential (presentation proof) the user has control over what information is presented to the verifier. This is called selective disclosure. In addition, a Zero Knowledge Proof (ZKP) might be used which proves that a claim has a certain characteristic without revealing the claim itself. Also there is no communication between the verifier and issuer needed for the verifier to verify the credential.

The credential schema for one of the Agricultural Ecosystem credentials is shown in Fig. 3. In this case the purpose of the credential is to provide geo-spatial boundary coordinates of a farm.


```
{
  "txn": {
    "data": {
      "data": {
        "attr_names": [
          "organisation_address",
          "organisation_id",
          "satellite_image_url",
          "representative_id",
          "shape_geo_json",
          "boundary_id",
          "shape_file_url"
        ],
        "name": "Boundary_ID",
        "version": "1.0"
      }
    },
    "metadata": {
      "digest": "cbaf5ecda443ce52b66a6dd8c3b60939dfa9b39ec4b886e47ba67a898a92f653",
      "from": "QNetK7HNqt4mdmWRKGxzrZ",
      "payloadDigest": "ac7a6fe5a506103fd1cb4b7f8305453415b983b53bb4b5b13d6edddd915fe820",
      "reqId": 1686744132940649200,
      "taaAcceptance": {
        "mechanism": "wallet_agreement",
        "taaDigest": "c965dd01fec099ea95babaea3031bc09905432d3d7f1519bc0b99971aece8592",
        "time": 1686700800
      }
    },
    "protocolVersion": 2,
    "type": "101",
    "typeName": "SCHEMA"
  },
  "txnMetadata": {
    "seqNo": 45461,
    "txnId": "QNetK7HNqt4mdmWRKGxzrZ:2:Boundary_ID:1.0",
    "txnTime": "2023-06-14T12:02:12.000Z"
  }
}
```


Fig. 3. Boundary ID Credential Schema

2.4 AnonCreds vs W3C Credentials

There are two main types of verifiable credentials associated with the Agricultural Ecosystem project today.

The AnonCreds [2] or anonymous credentials specification created as part of the Hyperledger AnonCreds Project. AnonCreds are very commonly used for verifiable credentials projects. Some advantages of AnonCreds based credentials:

- Anonymity—The credential itself does not contain the identifier of the subject of the credential. A technology called link secret allows the holder of the credential to prove they were issued the credential without revealing their identity.
- Revocation—An issuer is able to revoke a credential in real time. The next time that (revoked) credential is presented to a verifier the verification will fail.
- Reduced PII exposure—Implementation of both selective disclosure and zero knowledge proofs assists in protecting the privacy of the credential subject.

An alternative credential type has been created by the World Wide Web Consortium (W3C). This new credential format has been defined in the Verifiable Credentials Data Model v1.1. [3]. This W3C recommendation is particularly of interest to government applications.

There are a few limitations in W3C credentials in comparison to AnonCreds:

- Anonymity—It is the normal practice with W3C credentials for the subject identifier (usually subject DID) to be placed within the credential itself.
- Revocation—The W3C data model does not specifically include a revocation process.
- Reduced PII exposure—To obtain the benefits of selective disclosure and ZKPs, a W3C credential has to be created in that way e.g. using the signature types that support it. It is not the default for W3C credentials.

The project has initially used AnonCreds as the credential standard. However, due to government regulation the use of W3C verifiable credentials is on the roadmap to potentially replace AnonCreds.

2.5 Connections, Issuing, Presentation Proof Protocols

The initial protocols implemented in the Agricultural Ecosystem follow the RFCs as part of the Aries Interop Protocol (AIP) 1.0 [4].

A holder (wallet) makes a DIDComm connection - the initial implementation follows Aries RFC 0160: Connection Protocol [5] - with the issuer.

The verifiable credential - the initial implementation follows Aries RFC 0036: Issue Credential Protocol 1.0 [6] - is sent over the connection and stored in the holder's wallet.

The holder in turn establishes a new DIDComm connection to the relying party (verifier). The verifier requests a proof presentation - the initial implementation uses Aries RFC 0037: Present Proof Protocol 1.0 [7] – and receives that from the holder.

As the project moves to use W3C credentials then the AIP 1.0 protocols will be replaced with the AIP 2.0 protocols (at least for issue and presentation proof) [8], a requirement for using the W3C credentials.

2.6 Governance

In a Decentralized Agriculture Ecosystem there is a centralized authority for making and enforcing the rules of the network. The participants therefore agree to follow a set rules for the network.

Some examples of the governance rules related to verifiable credentials:

- What is the list of trusted issuers in the network?
- What credentials are those trusted issuers allowed to issue?
- What is the list of trusted verifiers in the network?
- What credentials are the allowed to verify?

There are two main standards for enforcing governance within the network:

- Trust Registry [9]: When an event occurs, for example, a wallet receives a credential offer from an issuer, the wallet makes a call to a central server to query whether the offer is obeying the governance rules.
- Machine Readable Governance [10, 11]: In this case a JSON file is created that describes the rules and is distributed to every participant in the network. That is,the JSON file is distributed to all issuers, verifiers and holders (wallets).

Within the Agricultural Ecosystem, the decision was made to follow the Machine Readable Governance approach. The network coordinator creates a JSON file with the rules and this is distributed to each participant (Issuers, Holders, Verifiers) in the network.

2.7 Decentralized Identity Wallet

A decentralized identity wallet is an application that allows a person to receive, store and present verifiable credentials that relate to them. Examples of the type of credentials that a person might receive into their personal DI wallet are passport, vaccine certificates, club memberships, flight tickets and access credentials. The personal DI wallet allows secure connections to be established with verifiable credential issuers and verifiers, and for the requesting, receiving, storing and presenting of verifiable credentials and for secure communication. It also allows secure connections to be made with another user's personal DI wallet to allow for secure communication between the users.

There are a number of personal DI wallets in existence, such as created by Lissi, Trinsic, Indicio, and Anonyome Labs and they are typically mobile or desktop applications. They are relatively easy to install and use by normal users. In the Agricultural Ecosystem we have used the Anonyome Labs personal DI wallet as shown in Fig. 4. In the figure the wallet is shown with five of the credentials used in the project.

The farming credentials are not restricted to only text based claims. On the left of Fig. 5 is the credential for a Green House Gas (GHG) certificate for a farm. In this example a PDF link is included in the credential. The wallet is then able to present the PDF. On the right of Fig. 5 is another credential showing the geographic boundary of the farm. In this case the credential includes the coordinates of the farm as one of the claims. The wallet is then able to present the graphical image of the farm by interpreting those coordinates.

2.8 Personal vs Enterprise Decentralized Identity Wallets

In projects such as the Agricultural Ecosystem, the use of personal DI wallets are increasingly seen as too limited. This current generation of personal DI wallets do not provide

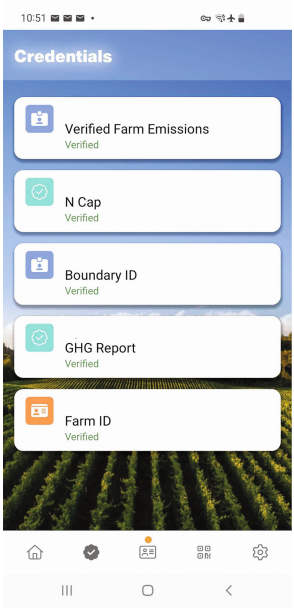

Fig. 4. Credentials from the Agricultural Ecosystem project

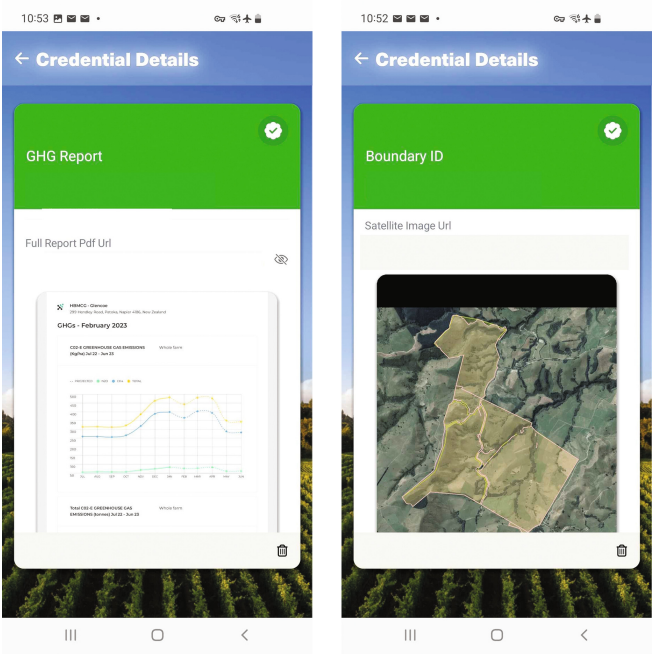

Fig. 5. Green House Gas Report and Boundary Credentials

sufficient capability for business or government use. In these settings a new type of wallet is required, that provides capabilities above and beyond a personal DI wallet.

To begin with, this new wallet (which we will call the enterprise DI wallet) does **NOT** hold verifiable credentials representing PII from an individual. Instead the enterprise DI wallet holds verifiable credentials that are representative of data related to the enterprise. For example, a verifiable credential in an enterprise DI wallet might represent a farm's GHG emission certificate. Or it might represent the organic status of a farm. The data may be sensitive from a privacy/business confidentiality point of view, but more importantly the integrity of data needs to be verifiable.

Another difference between a personal DI wallet and an enterprise DI wallet is that in the personal DI wallet, usually only the person (whose PII data is contained in the verifiable credentials in the wallet) accesses it. Whereas the enterprise DI wallet may need to be accessible by more than one authorized employee of the enterprise requiring a delegated authorization model to provide selective user access to the enterprise DI wallet.

Although the initial phase of the project used a personal DI wallet, the proposal is to replace this with an enterprise DI wallet.

3 Conclusions

The decentralized identity verifiable credential system provides an excellent foundation for providing a decentralized verifiable data exchange. This is possible because every part of the decentralized identity verifiable credentials system is standardized: DIDs, verifiable credentials, issuer-holder-verifier protocols, verifiable data registry and so on.

Participants in the Agricultural Ecosystem therefore choose roles of issuer, verifier or holder and can exchange data following these standards. It has also been possible to build this system with a consortium of different software vendors each following the standards. The network will need to evolve as the standards preferences change, such as the desire to move to W3C Credentials from AnonCreds.

Decentralized identity wallets typically are built for individual users and not for organizations. This has highlighted the need for an enterprise DI wallet, one that is built to share organizational data, and one that is accessible by multiple administrators of the organization.

References

1. Hyperledger Indy. https://www.hyperledger.org/projects/hyperledger-indy
2. AnonCreds Specification v1.0 Draft. https://hyperledger.github.io/anoncreds-spec/
3. Verifiable Credentials Data Model v1.1. https://www.w3.org/TR/vc-data-model/
4. Aries Interop Protocol 1.0. https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0302-aries-interop-profile/README.md#aries-interop-profile-version-10
5. Connection Protocol. https://github.com/hyperledger/aries-rfcs/tree/4d9775490359e234ab8d1c152bca6f534e92a38d/features/0160-connection-protocol
6. Issue Credential Protocol 1.0 Aries RFC0036. https://github.com/hyperledger/aries-rfcs/tree/bb42a6c35e0d5543718fb36dd099551ab192f7b0/features/0036-issue-credential

7. Presentation Proof Protocol 1.0 Aries RFC0037. https://github.com/hyperledger/aries-rfcs/tree/4fae574c03f9f1013db30bf2c0c676b1122f7149/features/0037-present-proof
8. Aries Interop Protocol 2.0. https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0302-aries-interop-profile/README.md#aries-interop-profile-version-20
9. ToIP Trust Registry Specification. https://wiki.trustoverip.org/display/HOME/ToIP+Trust+Registry+Protocol+Specification
10. Trust Establishment 1.0. https://identity.foundation/trust-establishment/
11. Credential Trust Establishment. https://identity.foundation/credential-trust-establishment/