

# Indicio

## Building **TRUSTED DIGITAL ECOSYSTEMS** with iProven™

Trevor Butterworth, Sam Curren, Heather Dahl, Ken  
Ebert, Mike Ebert, James Schulte

White paper v 1.0



# Contents

The Problem(s)	3	Types of Trusted Digital Ecosystems: Open and interoperable	23
The Struggle to Verify Identity and Data Online	4	Types of Trusted Digital Ecosystems: Constellation	24
Verifiable Credentials Will Change How We Interact Online	5	Global Deployments	25
Verifiable Credentials Allow Trust to be Triangulated	6	Solutions in Use Today	26
The Solution	8	Customer Example 1: Verifiable Credentials for Travel	27
The Components of a Trusted Digital Ecosystem	9	Customer Example 2: Canadian Financial Institution Using Verifiable Credentials for Account Holders	28
Decentralized Identifiers (DIDs) — A New Open Web Standard	10	Customer Example 3: Nonprofit using Verifiable Credentials for Climate Accounting	29
How DIDs Work	11	Customer Example 4: Bonifii Using Verifiable Credentials in the Metaverse	30
Schemas and Credential Definitions	12	Customer Example 5: Manufacturer Using Verifiable Credentials in Supply Chain	31
How to Revoke a Credential	12	Indicio Proven	33
Decentralized Ecosystem Governance	13	Proven Product Overview	34
Step 1: How to Create a Verifiable Credential	14	Proven Product Components	35
Step 2: How to Issue a Verifiable Credential	15	Conclusion: Prove Anything	36
Step 3: How to Accept a Verifiable Credential	16	Contact	37
Step 4: Presenting a Credential Using Privacy-Preserving Features	17		
Step 5: Verifying a Verifiable Credential	18		
Types of Trusted Digital Ecosystems	19		
Types of Trusted Digital Ecosystems: Closed	20		
Types of Trusted Digital Ecosystems: Open	21		



# The Problem

Fraud costs the global economy over US \$5.38 trillion each year<sup>1</sup>

The rate of identity fraud is increasing<sup>2</sup>

40% of those encountering fraud experience platform fraud<sup>3</sup>

Legal concerns for companies after GDPR court ruling<sup>4</sup>

Growing fears over data privacy for IoT adopters<sup>5</sup>

1. Crowe, The Financial Cost of Fraud 2021 ([link](#))

2. Onfido, Identity Fraud Report 2020 ([link](#))

3. PwC, Global Economic Crime and Fraud Survey 2022 ([link](#))

4. Wall Street Journal, August 10, 2022 ([link](#))

5. The Journey to IoT Maturity, Wi-Sun Alliance ([link](#))

# The Struggle to Verify Identity and Data Online

Traditional systems struggle with verifying digital identity because the internet was built without an “identity layer” for people, entities, and connected devices. At the time, this made sense: The internet — then called ARPANET — was, primarily, a way to connect a small number of geographically-distributed computers to communicate with each other and share limited memory resources. Communication protocols identified computers (IP addresses) but not the people using them; access was open; it was, as James Ball notes, “a trusted network.”<sup>1</sup>

As ARPANET became the internet, the openness of the network turned from a feature to a bug. Nodes, content, and users multiplied creating an information management and an information security problem. The management problem was solved by the creation of the World Wide Web, a combination of protocols that enabled web pages, web addresses, links, and web browsers. While this created an identity layer for resources online, users ended up, out of convenience, being identified by email addresses and passwords. Email was a leased identity; it came from a provider; and outside of institutional or work email, it required minimal to no identity assurance and, in turn, provided no legal proof of identity.

Email was the least frictional way to scale identity access and management on the web; and given the slow evolution of the internet and the inability to see what it would become, it’s difficult to see how things could have been different.

But the missing identity layer is now more of a monster than a bug. To assure email as an identity, web services and vendors require more and more personally identifiable information to be provided and stored for verification.

This made email and user accounts more valuable and more vulnerable. The inability to authenticate identity and the workarounds to try and solve this problem are a multi-dimensional privacy and security problem costing trillions of dollars. The problem will soon become exponentially worse as connected devices (IoT), digital objects, and even non-digital objects (in the Spatial Web) add billions of identities to our hybrid physical-digital existence. It sounds trivially true to say that the machines and robots of the very-near future need to be verifiable, but the reality is that they must. They must operate through an identity layer that is fundamentally different than the one we rely on now.





What to do? We cannot rip up the internet and start again. We need a solution that — to borrow a term from genetics — functions as a ‘killer-rescue construct.’ We need a technology that can be easily introduced into existing systems which then rescues them by adding an identity layer that delivers the verifiability, the privacy, and the security needed for all parties in online interactions to trust each other and the information they exchange. Such a solution would need to be open source and low cost to drive adoption, innovation, and scale.

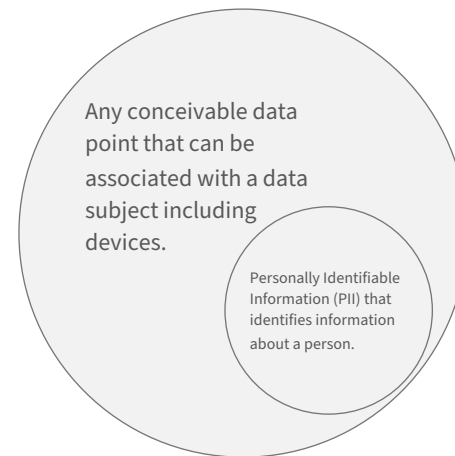
This solution exists. Broadly, it is called decentralized identity and sometimes more narrowly, self-sovereign identity. It is an identity layer for the internet *and* a privacy layer *and* a security layer. This is because its multiple components have multiple features. In an important way it returns us to the original, pre-web, open internet. Because identity is verifiable through a new ontology, it no longer needs to be locked into the defensive silos of centralized databases. And because the concept of identity pertains to information (and not just to the verified identity of a natural person), data becomes portable and immediately actionable. This has profound implications for the future of digital interaction.

But solutions are only solutions when they can be implemented successfully. This white paper is about Proven, the first complete open source product for rescuing the internet.

## Verifiable Credentials Will Change How We Interact Online

Over the past decade, the concept of decentralized identity, sometimes called “reusable identity” or “self-sovereign identity,” has emerged as a novel and powerful solution to the interconnected problems of verification, privacy, and security in online interaction.

Decentralized identity uses a combination of new technologies to establish the uniqueness, provenance, and integrity of a digital identity and the data associated with it through a verifiable credential. In this sense, “identity” goes beyond natural persons and their identity documents and covers the authenticity of any digital information issuable with a verifiable credential (*see figure opposite*).





## Verifiable Credentials Allow Trust to be Triangulated

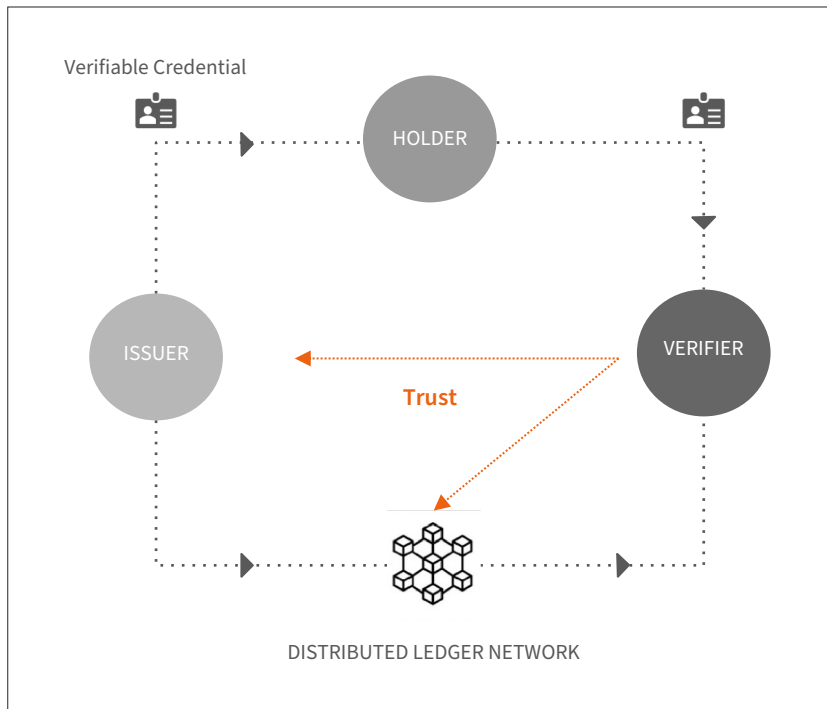
A verifiable credential can be verified without having to check in with the entity that created the credential. There is no need to “phone home” to the data originator through complex, direct system integrations. Similarly, the authenticity of a verifiable credential does not need to be cross checked against a third-party database by sharing information common to both.

This removes the need for centralized databases of personally identifiable information (PII), which has important implications for data privacy and security.

Decentralized identity enables positive and repeated verification of any given data point through the immutability of the blockchain ledger (*Figure 1*).

Using the [W3C Verifiable Credential Data Model](#), an **Issuer** of a credential attests to the credibility of the data contained in the verifiable credential.

Traditional KYC methods for determining the trustworthiness of the issuer will determine the acceptability of a credential for any given **Verifier**.



NO INDIVIDUAL CONTENT OR PII IS WRITTEN TO THE LEDGER

Figure 1

A key feature of verifiable credential technology is that PII or high-value data is *only* contained in the verifiable digital credential issued to the intended recipient; this information is not written to a blockchain or a distributed ledger.

It is the *form* of the verifiable credential that is written to a distributed ledger and the *form* that is verified. The integrity of the content in a verifiable credential is inseparable from the integrity of the form. This means that when you verify a verifiable credential, the content can be trusted.

This is a very high-level explanation of the power of verified credential technology; its mechanisms are more complex, involving decentralized identifiers (a new kind of URI), decentralized identifier communication protocols, revocation registries and cryptography. The “how?” will be explained in greater depth later in this paper.

One important point to note is that on July 19, 2022, decentralized identifiers (DIDs) were [recognized](#) by the World Wide Web Consortium (W3C) as an official web standard. If you are looking for a sign that the transformation is well under way, this is it.

As the holder of a verifiable credential holds their data, they can consent to share it; and as some verifiable credential types have powerful privacy-enabling features such as selective disclosure and zero-knowledge proofs, this information can be shared in ways that preserve privacy.

This addresses the many issues that data privacy law has been trying to solve in a simple, less burdensome way.

It can be difficult to see the multidimensional impact of verifiable credential technology all at once — or see how it will ultimately transform digital interaction. What happens when you have identity and data portability with seamless verification, data privacy law compliance, and uniquely encrypted peer-to-peer communication?

We see the original promise of the internet renewed in a way that benefits every sector and everyone.

How do we build this? By creating Trusted Digital Ecosystems using Proven™





# The Solution



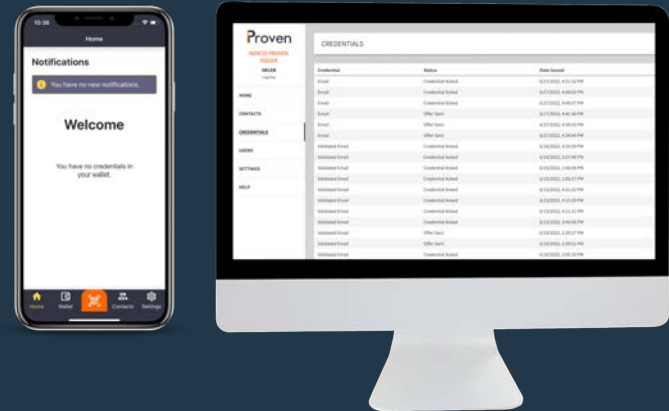
Trusted Digital Ecosystems built on open source decentralized identity technology for issuing, sharing, and verifying high value information

Proven™ is the easiest way to build, deploy, and scale a complete Trusted Digital Ecosystem

Proven is a complete, “off-the-shelf,” end-to-end system for decentralized verifiable credentials that can be quickly integrated with existing identity systems in a cost-effective way

Proven is designed to:

- a) deliver the benefits of open source technology without development teams having to master new codebases
- b) be fully open source. It's not just built on open source and open standards, it's delivered as a fully open source solution with no vendor lock-in
- c) be fully supported, so you get continuous upgrades and expert technical assistance when you need it and as soon as you need it





# The Components of a Trusted Digital Ecosystem



- **Issuers** — entities that issue verifiable credentials.
- **Holders** — those who are usually the subjects of the verifiable credentials and hold them on a mobile device (the Holder may also be a legal guardian of the subject, such as a caregiver or parent). Holders can also be digital objects or machines.
- **Verifiers** — those who need to verify the information contained within these credentials.
- **Software agents** — Each of the above roles has its own designated software, i.e., for issuing a credential, for holding and presenting a credential, and for verifying a credential. These are called “agents” because they manage the information flow between parties with each agent having a fiduciary responsibility to the party it represents.
- **Distributed Ledger Network** — Serves as a trust anchor for DIDs, Schemas, Credential Definitions, and Revocation Registries. The network can be public or private; multiple network nodes distributed in different geographic locations each support a copy of the ledger and provide resilience.

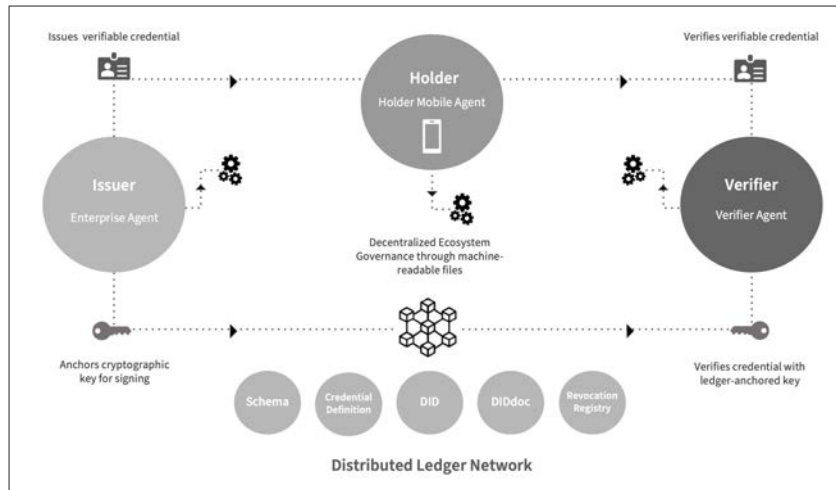


Figure 2

- Agents reference **Decentralized Ecosystem Governance** through machine-readable files to encode the governance decisions or rules normally made by humans. These files are an efficient and error-free way to choreograph information flows and to establish who is a trusted Issuer in an ecosystem without having the complexity, friction, and risk of going through a centralized trust registry.

See: [W3C Verifiable Credentials Data Model](#)

# Decentralized Identifiers (DIDs)— A New Open Web Standard



Software agents enable interaction within Indicio Proven by creating Decentralized Identifiers, or DIDs. DIDs are a new [open web standard](#) approved by the W3C to enable verifiable, decentralized identities.

Anyone can create a DID, hence they are neither dependent for their existence on, nor controlled by, a centralized organization. DID ownership can be cryptographically identified along with information that allows peer-to-peer communication with the owner.



As there are no limits on the number of DIDs that can be created, they do not need to be reused (and when representing persons, they should not be reused to prevent correlation).

When a software agent creates a DID for someone or something, it also creates a DID document (DIDdoc). This DIDdoc contains information about how to interact with the entity in control of the DID.

For example, if a bank issued a KYC credential, the DIDdoc would contain the mechanism by which the bank proves it created the DID for the credential and the information needed by the credential owner to connect with the bank to receive the credential.

Connection and verification occurs through public cryptographic keys paired with private keys. Parties connect with each other by using their private keys to encrypt the information they send. Paired with a public key, they enable peer-to-peer encrypted communication.

Issuers use public DIDs so that the cryptographic and related information needed to verify a credential can be found on a ledger. No personally identifiable information is written to the ledger for verifying a credential; personal data is sent directly to the Holder in a verifiable credential.

Mobile Agents can create unique, private DIDs for every communication channel. This prevents DIDs from a single entity being correlated, as there's a new, unique DID for every interaction.

DIDs have their own communications protocol called DIDComm. This can be accessed over any transport and allows for rich semantic interaction and offline verification directly between devices.



## How DIDs Work

Decentralized Identifiers on the ledger allow the issuer to prove control of the DID tied to a credential (Figure 3).

Cryptographic signature types that are attribute-specific allow provide the ability to parse the individual data points of a credential. This allows for privacy protection through selective disclosure.

The successful revelation of an attribute using signature keys is proof that the data has maintained its integrity and has arrived exactly as created by the Issuer.

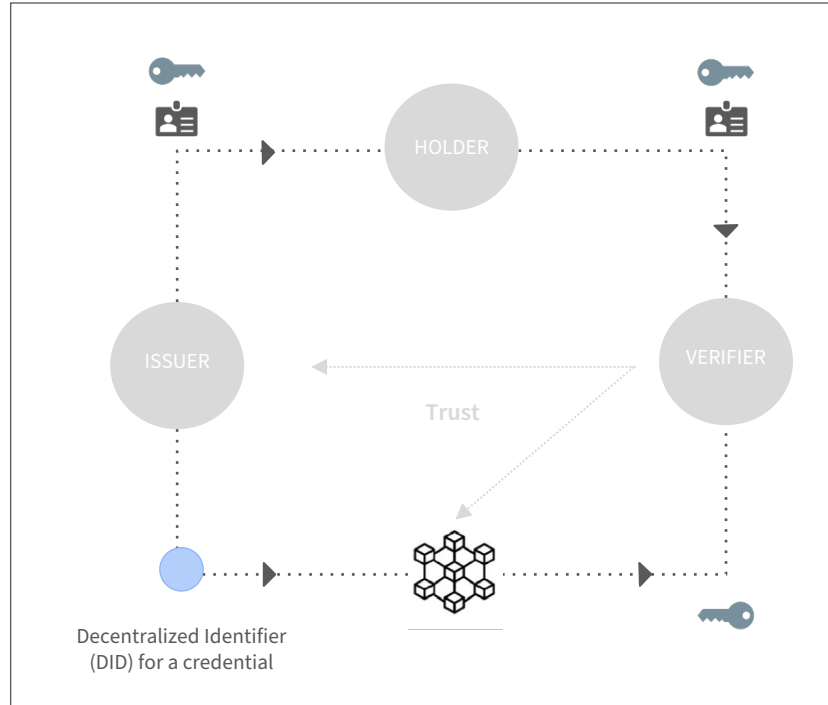


Figure 3

# Schemas and Credential Definitions



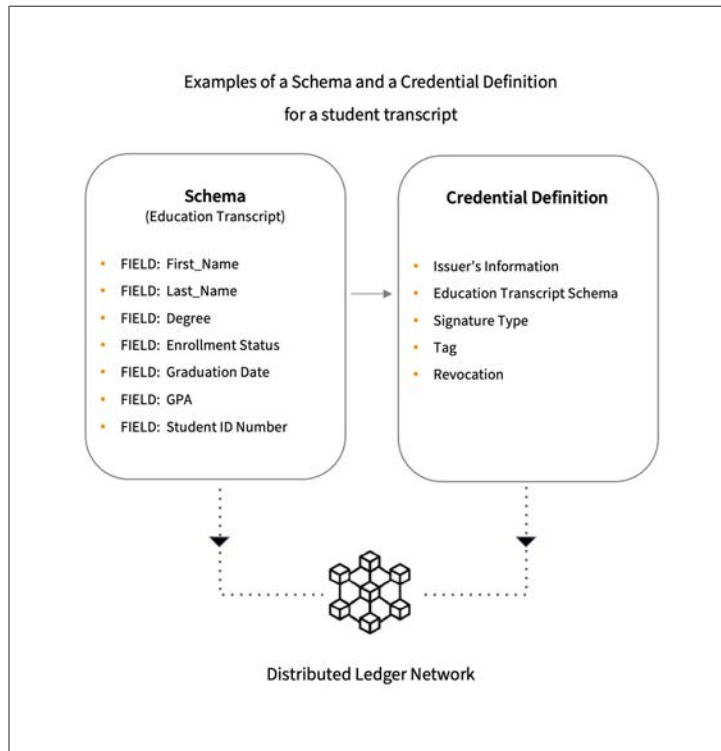
A **Schema** is a specification for verifiable credentials that defines and describes the data they contain (Figure 4). A **Credential Definition** describes the form of the credential, associates the Schema with a particular Issuer, contains the cryptographic material to support selective disclosure, and establishes an optional revocation mechanism (for listing the revoked credential in a decentralized registry).

## How to Revoke a Credential

Credentials can and must be revocable, whether due to errors in issuance, breach of user terms, or expiration of privileges. A **Revocation Registry** is a privacy-preserving way to list all the credentials that have been revoked in a Trusted Digital Ecosystem.

When presenting a credential for verification, each Holder provides a proof of non-revocation. Verifiers check the Revocation Registry to confirm non-revocation using complex computation methods to prevent the credential being correlated to the Holder by an outside observer.

A Revocation Registry is on the Indicio Proven development roadmap.



NO INDIVIDUAL CONTENT OR PII IS WRITTEN TO THE LEDGER

Figure 4

# Decentralized Ecosystem Governance



While the combination of DIDs, credential schemas and definitions, cryptographic calculation, and tamper-proof distributed ledgers creates immediately actionable, verifiable data, governance authorities must be able to make decisions about who can be trusted as an issuer of data and how data is to be acted on.

In Proven, this happens through Decentralized Ecosystem Governance, where a governance authority publishes a serialized, downloadable, machine-readable file containing all the information relevant to governing an ecosystem, which then propagates through the agent software in that ecosystem.

- No live calling of a trust registry is required, thereby improving the speed of verification.
- As governance files are cached, offline functionality is possible, mitigating connectivity issues.
- The rules and permissions for interaction in an ecosystem or jurisdiction can be efficiently choreographed in an error-free way
- Rules can be combined hierarchically, e.g., global > national > local
- There is no time lag waiting for third parties to update important rules as rapid changes can be quickly propagated to all parties in the ecosystem or jurisdiction

## Three reasons to avoid the service model of a trust registry

A trust registry as a service is often seen as the solution to the question, “which issuers of verifiable credentials can I trust?” This is because a trust registry is the traditional way such verification is accomplished.

But there is no need for a trust registry as a service when its functions can be decentralized and made machine-readable as a file.

1. In digital interaction, verification needs to be quick to be valuable. If every verification requires pinging a trust registry service for approval friction has been needlessly added to the system.
2. A centralized trust registry creates a dependence on real-time calling for verification when any system for verification needs to be able to function offline. With Decentralized Ecosystem Governance, the governance rules are cached in each participant's software, eliminating real-time dependence.
3. Trust registries as services create additional operational costs, which can then be passed on to the participants in a system as a toll. To implement governance rules, a trust registry needs additional governance to ensure that it operates effectively and fairly.

All this operational inefficiency and cost is eliminated by organizing a trust registry in a machine-readable governance file cached by software agents

## Step 1: How to Create a Verifiable Credential in a Trusted Digital Ecosystem



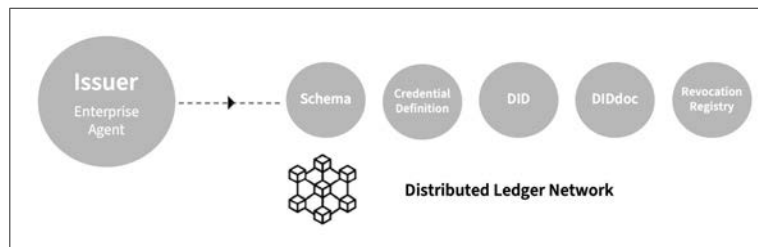
An Issuer uses an **Enterprise Agent** to write a public **DID** to a **Decentralized Ledger Network** (a Hyperledger Indy Network) announcing themselves as an Issuer (*Figure 5*).

This enables a person's software agent to establish contact with the Issuer to receive a credential.

The Issuer adds a **Credential Schema** and a **Credential Definition** to the ledger.

This describes the form of the credential — which allows all relevant parties to know what to expect in terms of the structure and content of information inside a credential.

The **Credential Definition** associates the **Schema** with a particular Issuer, and it establishes an **expiry date** or **revocation mechanism** (for listing the revoked credential in a registry if terms of use are violated).



NO INDIVIDUAL CONTENT OR PII IS WRITTEN TO THE LEDGER

Figure 5

## Step 2: How to Issue a Verifiable Credential in a Trusted Digital Ecosystem



The Issuer emails or displays an **invitation** to a person so they can connect and receive the credential (Figure 6).

If accepted, the Issuer will generate a unique **public DID** to directly communicate with the person via their application.

If accepted, the Holder will also generate a **unique DID** to communicate with the Issuer.

Public and private keys are generated within this connection for verifying identity and for the encryption and decryption of communications.

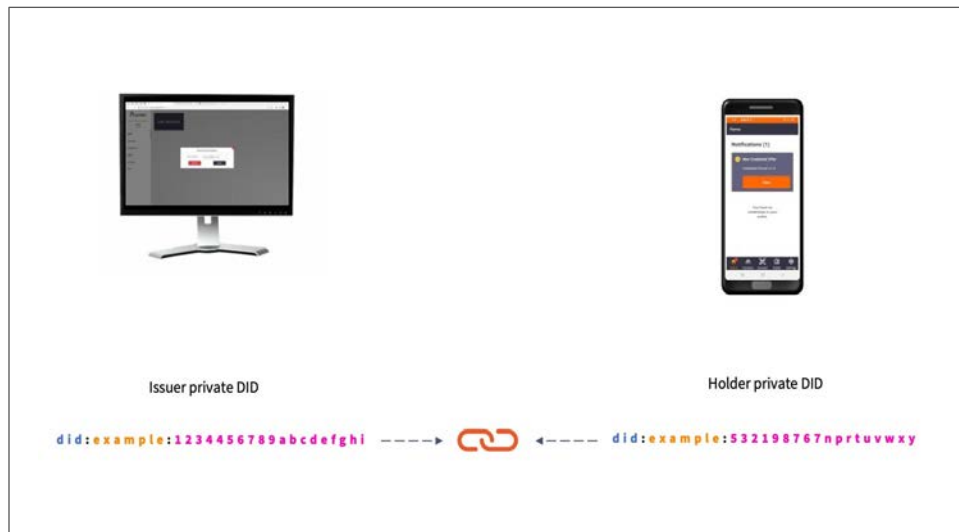


Figure 6

NO INDIVIDUAL CONTENT OR PII IS WRITTEN TO THE LEDGER



### Step 3: How to Accept a Verifiable Credential in a Trusted Digital Ecosystem



The person accepts the credential (*Figure 7*), checks that the information is correct (there is a step to correct any errors). There are two ways to store a credential. It can be stored in a **cloud agent** or in a **mobile agent** on a mobile device. The mobile agent can be standalone or integrated into an existing app.

Choosing which of these routes will depend on the use case and the preferred user experience.

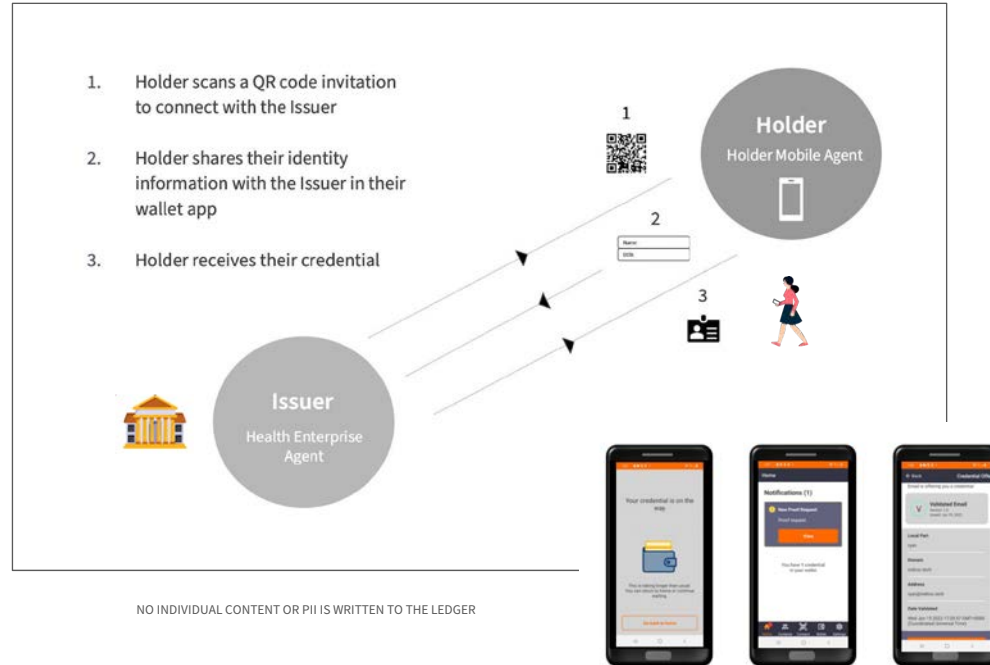


Figure 7

## Step 4: Presenting a Credential Using Privacy-Preserving Features



There are two ways to use the credential depending on the privacy required (Figure 8). Either a person can present a proof of the credential so that their identity or a fact related to their identity can be verified without the need to share any specific information or the person can respond to requests for specific information.

In this second case they also have the option of sharing some specific information in a privacy-preserving way, using **selective disclosure** and predicate proofs powered by **zero-knowledge credential** technology.

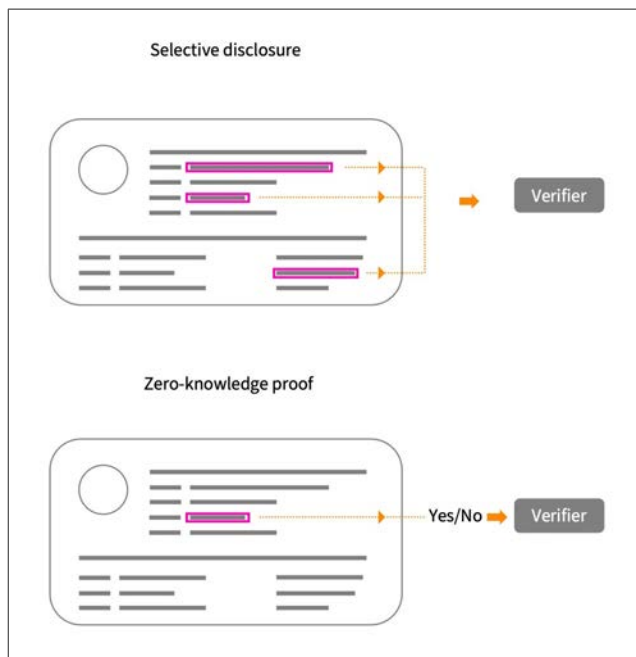


Figure 8

## Step 5: Verifying a Verifiable Credential in a Trusted Digital Ecosystem



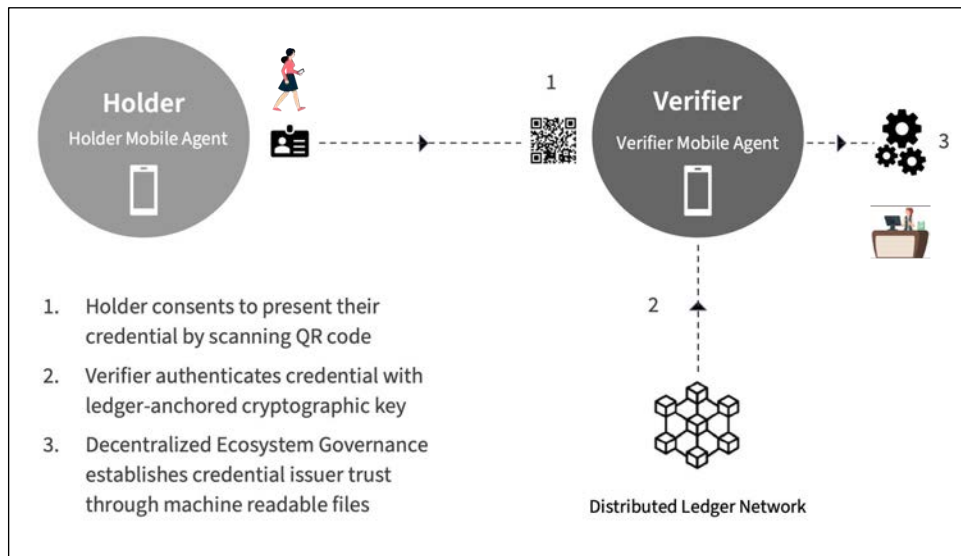
The Verifier checks the authenticity of the credential and its ownership by looking up the Issuer's **public key** and **DID** on the network and validating the credential (*Figure 9*). This means the issuing authority doesn't have to be consulted to prove the authenticity of the credential.

This also removes the need for a third party to facilitate verification by using PII stored for cross checking — or the need for a direct integration between the verifying organization and the issuing organization.

Each interaction in a Trusted Digital Ecosystem information flow is a **uniquely encrypted, non-correlatable, non-reusable, peer-to-peer** interaction.

When combined with the privacy-preserving features of a credential (**selective disclosure** and **zero-knowledge proofs**), Indicio Proven provides a new, multi-dimensional level of security for data sharing and verification.

When combined with **Decentralized Ecosystem Governance**, dynamic rulesets based on geography, regulations, and data type can be applied to further facilitate secure and private data sharing.



NO INDIVIDUAL CONTENT OR PII IS WRITTEN TO THE LEDGER

Figure 9

# Types of Trusted Digital Ecosystems



Closed, Open, and Constellation

Start by issuing and verifying, then expand to other verifiers, issuers, and multiple networks

## Types of Trusted Digital Ecosystems: Closed



In a **Closed** Trusted Digital Ecosystem, the entity issuing the verifiable credential is also the entity verifying the credential (Figure 10).

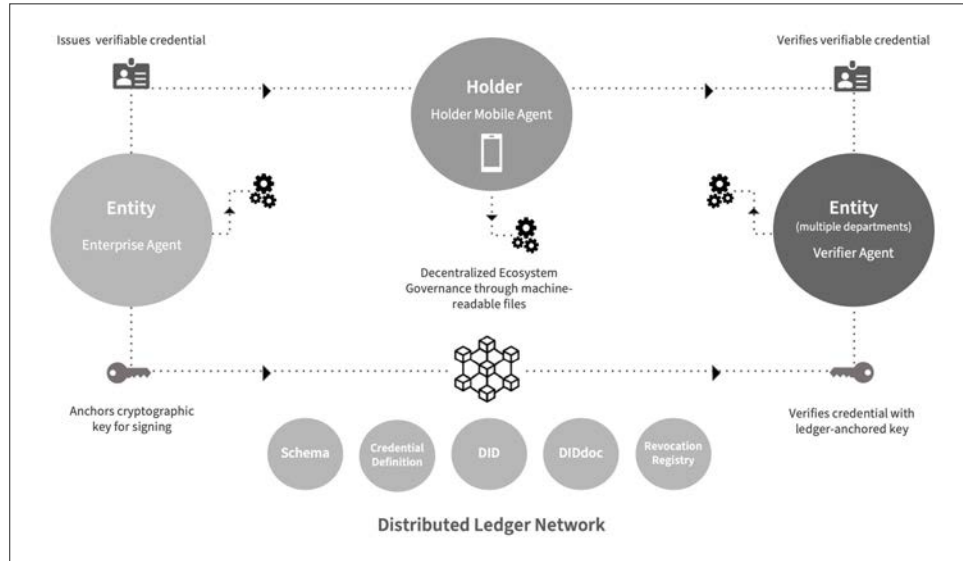


Figure 10

## Types of Trusted Digital Ecosystems: Closed



**Closed** ecosystems can also manage more complex information flows, for example, a company managing employee benefits through a secondary organization (Figure 11).

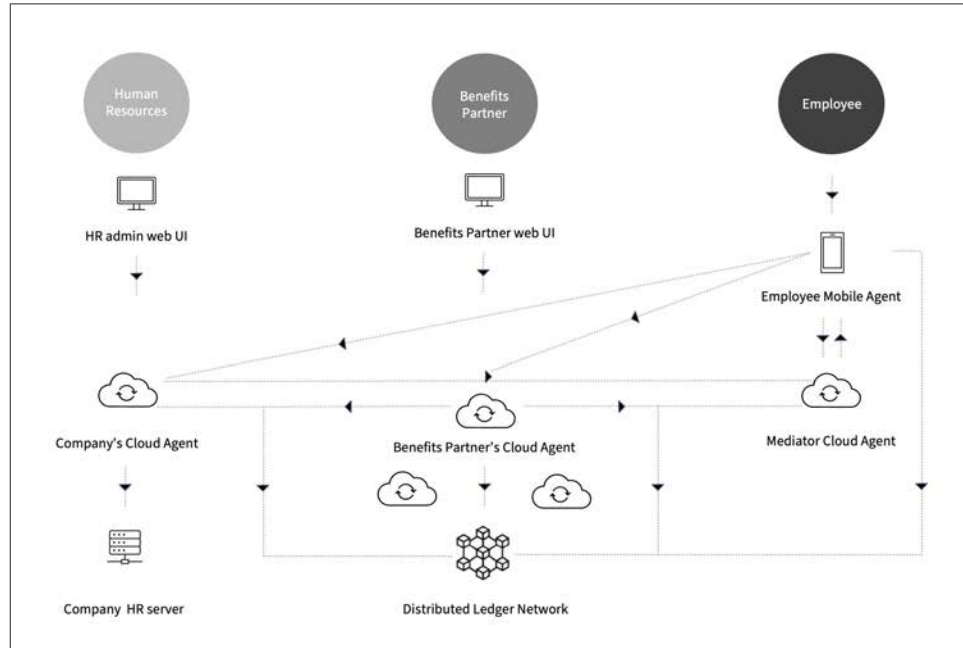


Figure 11

NO INDIVIDUAL CONTENT OR PII IS WRITTEN TO THE LEDGER

## Types of Trusted Digital Ecosystems: Open



In an **Open** Trusted Digital Ecosystem, the Verifier is a third party. In the application illustrated in the diagram, a bank uses an employer-issued credential as part of its KYC process (Figure 12).

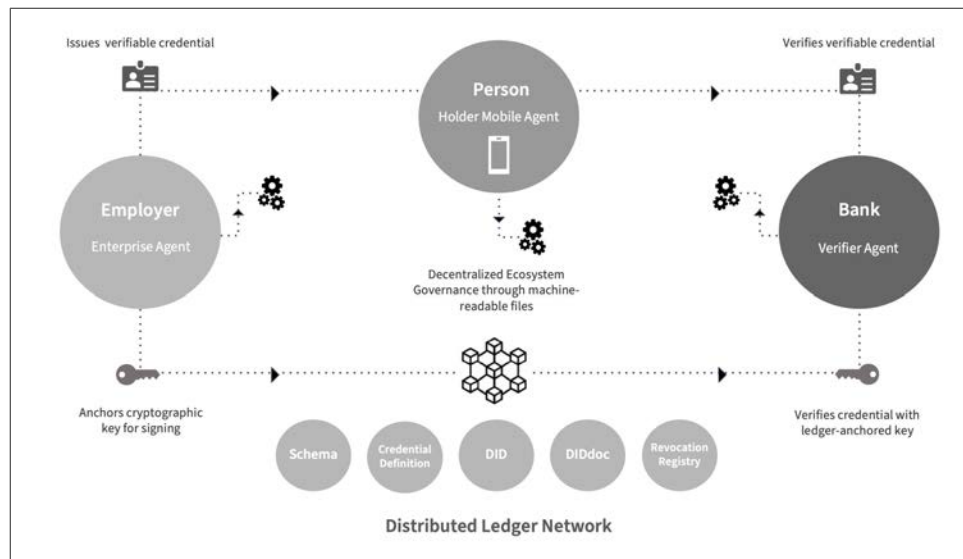


Figure 12

NO INDIVIDUAL CONTENT OR PII IS WRITTEN TO THE LEDGER



## Types of Trusted Digital Ecosystems: Open and interoperable



As Trusted Digital Ecosystems are designed to be interoperable and follow open standards, an open ecosystem can extend beyond additional Verifiers to additional Issuers and Holders (Figure 13).

The **did:indy Method** enables credentials issued on one Indy network to be verified on another.

**Decentralized Ecosystem Governance** establishes trust and choreographs information flows through machine-readable files.

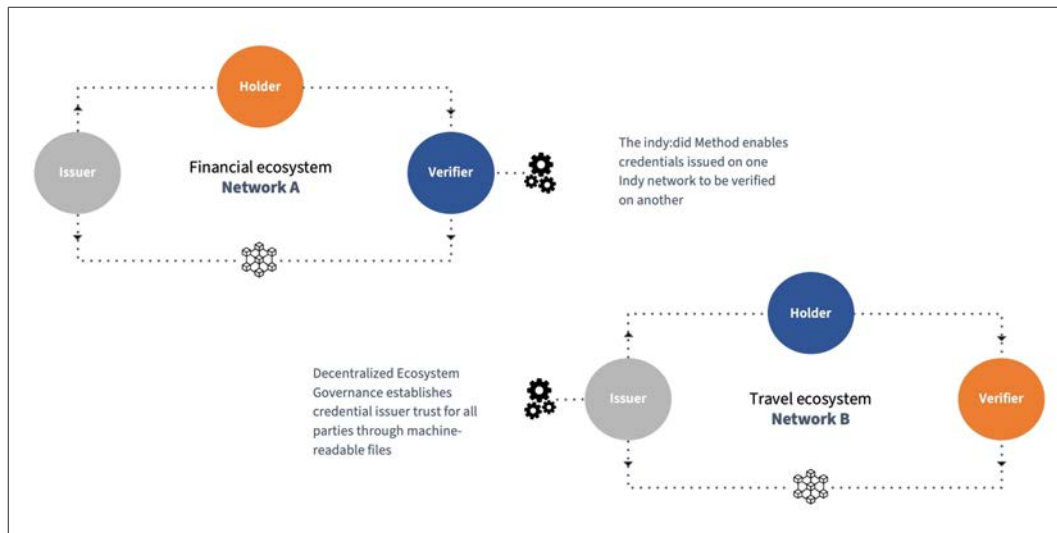


Figure 13

NO INDIVIDUAL CONTENT OR PII IS WRITTEN TO THE LEDGER

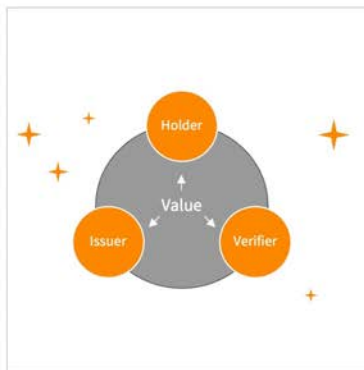
## Types of Trusted Digital Ecosystems: Constellation



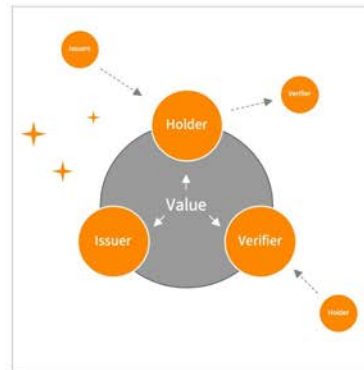
Finally, the combination of open source and interoperability drives innovation in new processes, products, and services based on immediately actionable, verified data.

The result is a **Constellation** of Trusted Digital Ecosystems — the organic growth and scale of interoperable verifiable digital credentials through network effects (*Figure 14*).

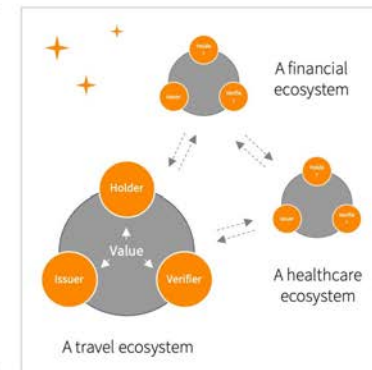
Figure 14



A single, closed ecosystem of Issuers, Holders, and Verifiers. The entity issuing the credential is the entity verifying the credential.



Interoperability opens the ecosystem to other verifiers, and then to other issuers and holders.



Verifiable credential ecosystems that show value drive links to other ecosystems, creating value for all.

# Global Deployments



Decentralized identity technology has rapidly matured over the past two years from working in theory to working in practice

Numerous global enterprise deployments

Indicio has built verifiable credential solutions for financial, healthcare, IAM, KYC, Metaverse, pharmaceutical, supply chain, and travel and hospitality applications

Indicio customers have won awards for their verifiable credential implementations

Indicio has been nominated for a Supernova Award by Constellation Research for its development of verifiable travel solutions



- Banking & Finance
- Travel, Events & Hospitality
- Identity Access Management
- Healthcare
- Supply chain
- Public Sector
- NGOs
- Secure documents
- Pharmaceutical
- Energy, Oil & Gas
- IoT devices
- Spatial Web



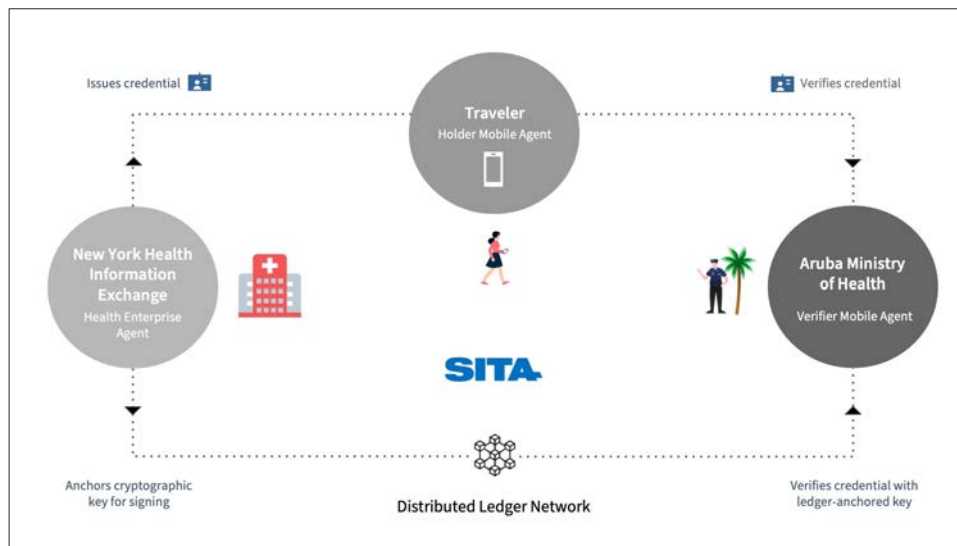
## Customer Example 1

### Verifiable Credentials for Travel

Indicio and SITA built a complete, open-sourced Trusted Digital Ecosystem for health and travel credentials



- SITA: World's largest aviation IT provider servicing over 90% of world's airports and airlines
- Uses verifiable credentials for cross-border travel
- Verifiable credentials prove passenger vaccine/test status
- Credentials are reusable throughout travel ribbon
- Reduces airport wait times, speeds up passenger flow
- No complex database integrations needed



NO INDIVIDUAL CONTENT OR PII IS WRITTEN TO THE LEDGER

[Read the news report here](#)

Figure 15

## Customer Example 2

### Financial Institution Using Verifiable Credentials for Account Holders

Indicio is helping a financial institution build a Trusted Digital Ecosystem to improve UX, reduce fraud, and increase accessibility



- Uses verifiable credentials to speed up customer onboarding and verification
- Uses verifiable credentials to eliminate redundant KYC processes
- Creates an ecosystem of organizations using interoperable systems
- Innovates with federal government to increase access to citizen and financial services
- Reduces financial crimes and fraud

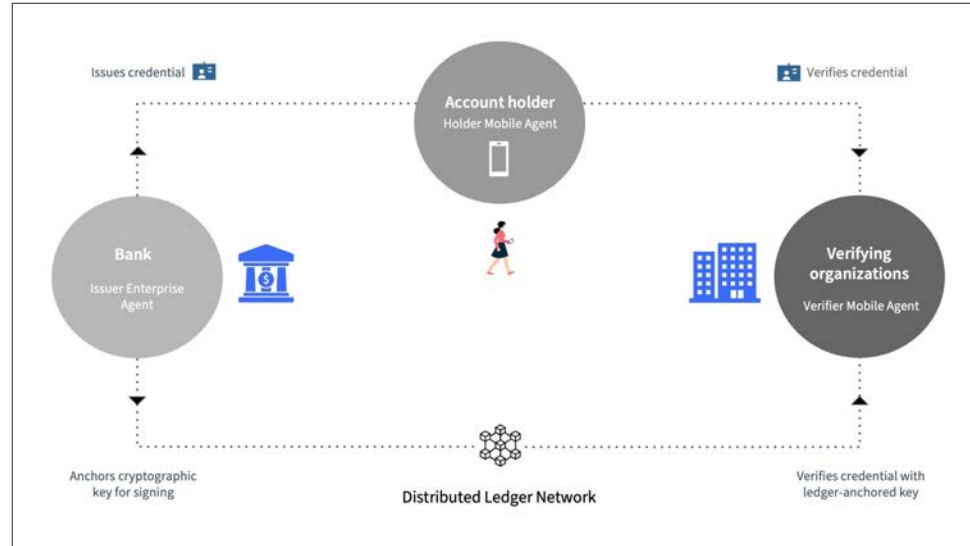


Figure 16

NO INDIVIDUAL CONTENT OR PII IS WRITTEN TO THE LEDGER

## Customer Example 3

### Nonprofit using Verifiable Credentials for Climate Accounting

Indicio has teamed up with a non-profit using a Trusted Digital Ecosystem to improve current, faulty climate accounting systems



- Verifiable credentials used to create trusted connections with verified data sources
- Measurement devices, people, and organizations use credentials for reporting access
- Verified sources can be relied on to produce high quality emissions data
- Verifiable credentials eliminate “double-counting” issue pervasive in existing climate accounting systems
- Reduces fraud and improves carbon credit attribution process
- Creates transparency and trust throughout ecosystem

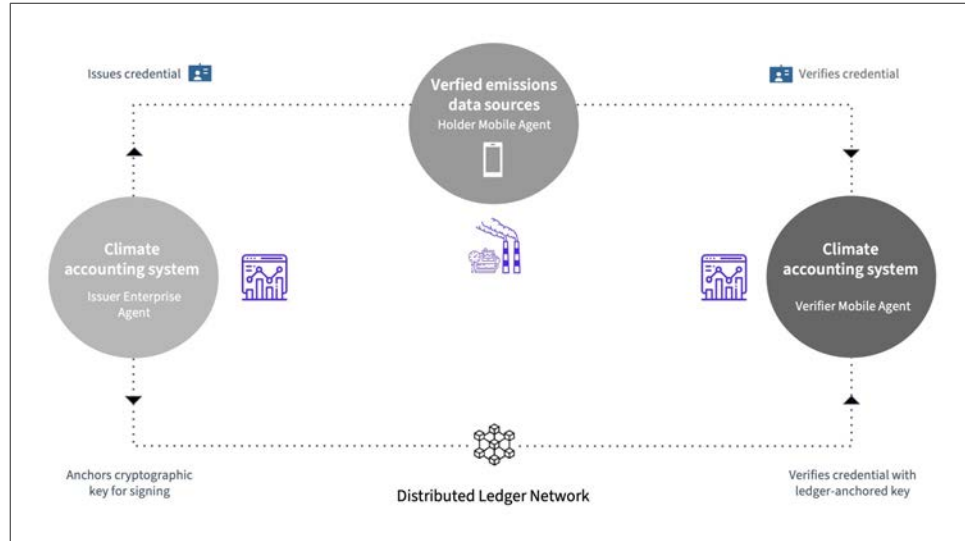


Figure 17

NO INDIVIDUAL CONTENT OR PII IS WRITTEN TO THE LEDGER



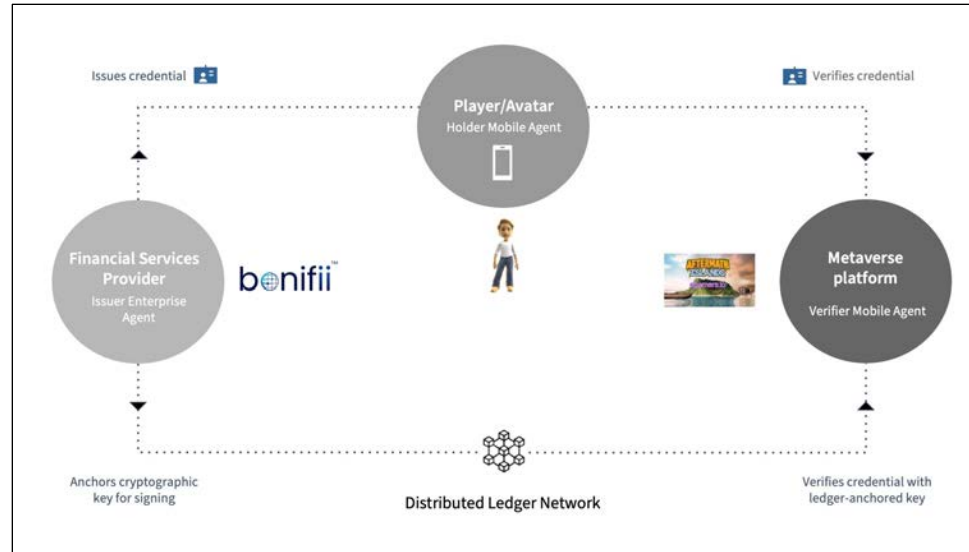
## Customer Example 4

### Bonifii Using Verifiable Credentials in the Metaverse

Bonifii, partnering with Indicio and Liquid Avatar, is using a Trusted Digital Ecosystem to enable secure financial transactions in the Metaverse



- Bonifii issues digital KYC credentials to enable privacy-preserving financial transactions in metaverse
- Maximizes privacy and security while providing end-to-end onboarding experience
- Opens opportunities for in-game payments, digital asset ownership, and cross-platform transactions



NO INDIVIDUAL CONTENT OR PII IS WRITTEN TO THE LEDGER

Figure 18

## Customer Example 5

### Manufacturer Using Verifiable Credentials in Supply Chain

An Indicio Node Operator is using a Trusted Digital Ecosystem to bring increased security measures to a Class 1 Dangerous Goods supply chain



- Uses verifiable credentials to ensure secure and authorized participation in dangerous goods supply chain
- Enables increased supply chain provenance and accountability
- Ensures regulatory compliance
- Creates tamper-proof digital shipping documents
- Prevents dangerous goods from ending up on black market
- Solves chain-of-custody identity challenges

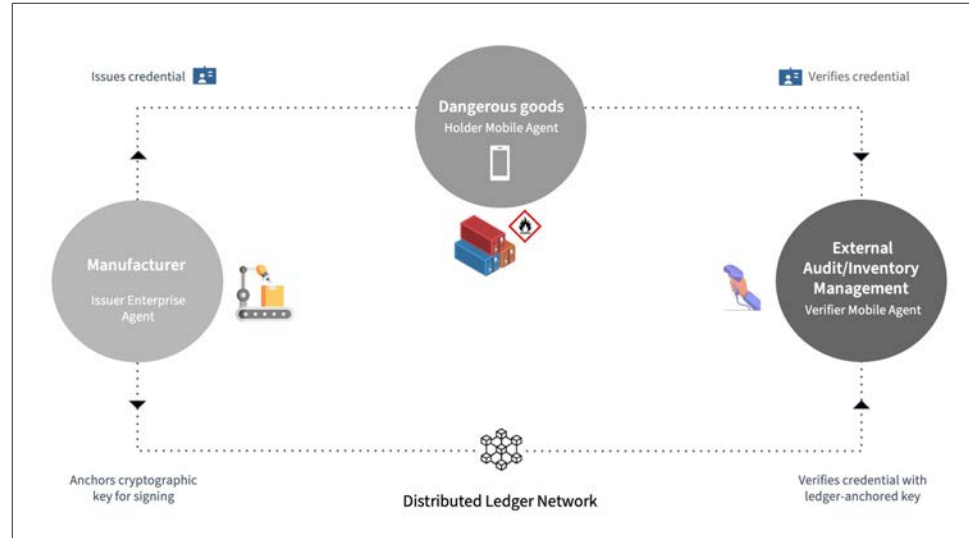


Figure 19

NO INDIVIDUAL CONTENT OR PII IS WRITTEN TO THE LEDGER



Introducing a simple and swift  
way to build and deploy  
**Trusted Digital Ecosystems**  
and take advantage of  
immediately actionable,  
trustworthy data...

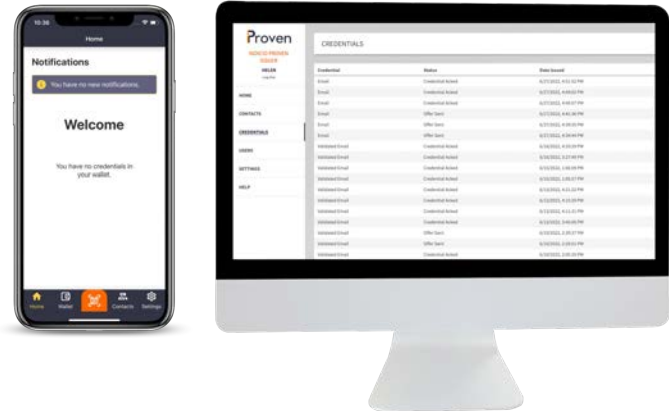
# Indicio iProven



Proven is a complete, fully open-source solution for implementing verifiable credentials and creating Trusted Digital Ecosystems

Proven is designed to make verifiable credential technology easy to integrate into existing systems, deploy, and scale

Proven is built on open source and open standards and delivered as a fully open source product with no vendor lock-in



# Proven Product Overview

Indicio Proven is built on open-source decentralized identity technology from the Hyperledger Indy, Aries, and Ursa project codebases. These form the most mature, functional protocol stack built specifically for decentralized Identity and verifiable credentials. Proven is fully open source, meaning there is no vendor lock-in to any component.

Proven follows specifications set out by the World Wide Web Consortium (W3C) and is compliant with the recommended technical standards advocated by organizations such as the Trust over IP Foundation (ToIP). This makes Proven interoperable with a large and growing ecosystem of W3C verifiable credential issuers and verifiers.

Proven is designed to make using decentralized identity technology simple by providing all the components needed to get up and running fast. It solves the problem of having to find and combine components from multiple vendors. It is also designed to flatten the open source learning curve so that development teams unfamiliar with the codebases can get straight to integration and implementation.

By combining privacy- and security-by-design features, non-correlatable peer-to-peer communications through DIDComm, consent-based sharing with automated governance, and familiar UI and UX, Indicio Proven is the most frictionless way to achieve fraud resistance, comply with data privacy regulations, implement Zero Trust security, and create actionable data.



# Proven Product Components



**Verifiable Credential Schema:** A flexible template hosted in the cloud for creating a verifiable credential using open source and interoperable standards.

**Issuer and Verifier Agents:** Simple software hosted in the cloud to connect, issue, and verify credentials; integration APIs available.

**Mobile App and Mediator:** Software hosted in the cloud to enable users to download, store, and use a credential on mobile devices.

**Decentralized Ecosystem Governance:** Agent software hosted in the cloud to establish trusted Issuers and automate information flows via machine-readable governance files.

**Distributed Ledger Network:** Configuration and deployment on existing Indicio Networks or any Hyperledger Indy-based distributed ledger network or a custom, public or private network. DID : Method ensures interoperability with other Indy-based networks

**Support and Training:** Continuous customer support, field-leading training covering every aspect of Proven and Trusted Digital Ecosystems

**Maintenance and Updates:** Managed updates and comprehensive testing to ensure maximum performance

## Enterprise Agents

- W3C Issuer customer care
- W3C VC Issuance services

## Web UIs

- Customer care (portals)

## Cloud Agents

- W3C VC Cloud Wallet

## Mediator Agents

- Off-line interaction

## Mobile Holder

- Mobile Wallet Application
- Mobile Wallet SDK

## Mobile Verifier Agent

- Mobile Verifier Application
- W3C VC Mobile Verifier SDK

## Decentralized Ecosystem Governance

- Issuer & Verifier Trust Anchor

## Distributed Ledger Network

- Trust Anchor

All Proven components are built according to the following formalized standardization and open-source initiatives for decentralized identity and verifiable claims exchange. As these evolve, Indicio Proven will incorporate updates.

[Decentralized Identifiers \(DIDs\) v1.0](#) (W3C)

[Verifiable Credentials Data Model 1.0](#) (W3C)

[Verifiable Credentials Use Cases](#) (W3C)

[Decentralized Identity Foundation Homepage](#) (DIF)

[Hyperledger/Indy-Node](#) GitHub

[Hyperledger/Aries](#) GitHub

[Hyperledger/Ursa](#) GitHub

## Conclusion: Prove Anything

Open source, interoperable decentralized identity technology is the fastest, most effective, most cost-efficient way to create a verification layer for digital interaction that provides the privacy and security needed by consumers and enterprises alike.

The ability to integrate this technology into existing systems, avoid complex integrations, and orchestrate multiple applications radically simplifies infrastructural transformation, allowing flexible implementation and organic growth. Open source is critical to this process; but it is not enough to *just* be built with open source code and on open standards.

The key to a cycle of rapid adoption and innovation around decentralized identity technology is true open source, which is when enterprises *fully* own their implementations and can innovate at-will to meet new needs and create new products and services.

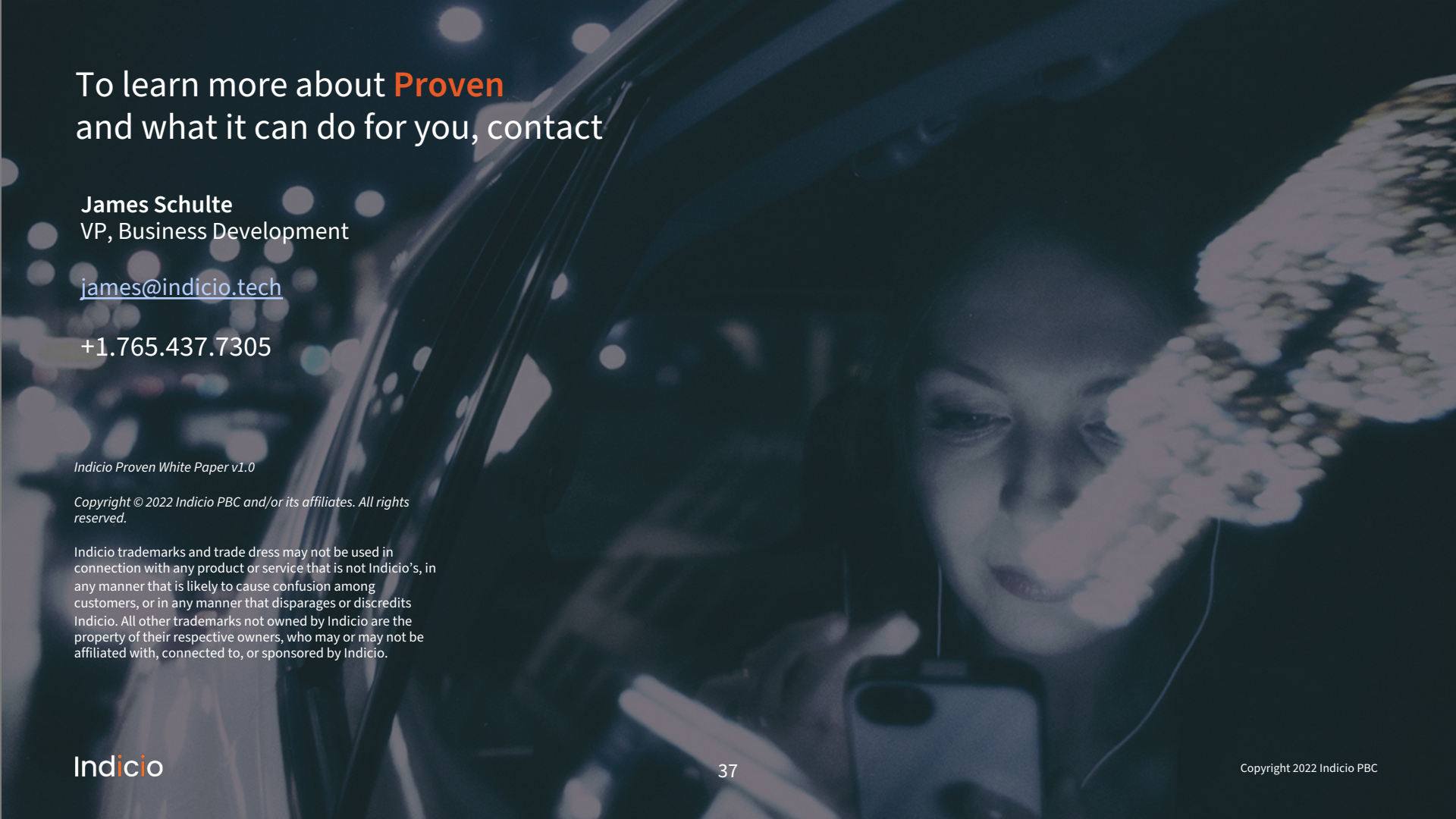
This understanding of open source is what drives Indicio, what has driven our success in the marketplace as a leading developer of solutions across multiple sectors, and what drove the creation of Proven.

If we want to transform digital interaction, create meaningful digital relationships, free data from its siloed bonds, and expand identity to incorporate digital and non digital devices — in short, fuel a new internet era through verified data — then we start by giving enterprises and organizations the power to build and fully own their own Trusted Digital Ecosystems. This is how open source becomes the force multiplier.

Build, control, interoperate, and innovate. You can do that because you own Proven, Proven doesn't own you.







To learn more about **Proven**  
and what it can do for you, contact

**James Schulte**  
VP, Business Development

[james@indicio.tech](mailto:james@indicio.tech)

+1.765.437.7305

*Indicio Proven White Paper v1.0*

*Copyright © 2022 Indicio PBC and/or its affiliates. All rights reserved.*

Indicio trademarks and trade dress may not be used in connection with any product or service that is not Indicio's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Indicio. All other trademarks not owned by Indicio are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Indicio.