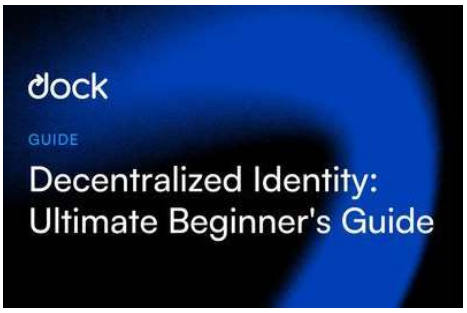
Decentralized Identity: The Ultimate Guide 2023



Published May 1, 2023 • 51 min read

Table of contents

Introduction

What is a Decentralized Ider

Key Benefits of Decentralize Solutions

Why Is Decentralized Identit Organizations?

Why Is Decentralized Identit Individuals?

Why Is Decentralized Identit Developers?

Issue Fraud-Proof Credentia

Decentralized Identity and S Identity: What's the differenc

Since 2017, Dock 's expert team has been building cutting-edge decentralized identity and Verifiable Credential technology. We created this complete guide on decentralized identity to explain what it is, how it works, and its many benefits to organizations, individuals, and developers.

TL;DR

- Certificate fraud, fake credentials, slow verification processes, and data breaches are just some of the problems associated with our current centralized digital identity systems that decentralized identity technology can solve.

- Decentralized identity is a type of identity management that has the following benefits for:

1) Organizations: Issuing organizations can provide fraud-proof credentials and verifying organizations can instantly check the authenticity of credentials.

2) Individuals: Fully own and control their digital identity and credentials without relying on any third party to prove their claims.

3) Developers: Build user-centric apps that eliminate the need for passwords and inefficient authentication processes.

- A decentralized identity system is made up of 3 pillars: blockchain, Verifiable Credentials (VCs), and decentralized identifiers (DIDs).
- Decentralized identity technology can be applied to a growing number of use cases including supply chain traceability, issuing fraud-proof certifications, and managing employee IDs.

Try Dock's Decentralized Identify Platform for Free

Introduction

Not-so-fun facts:

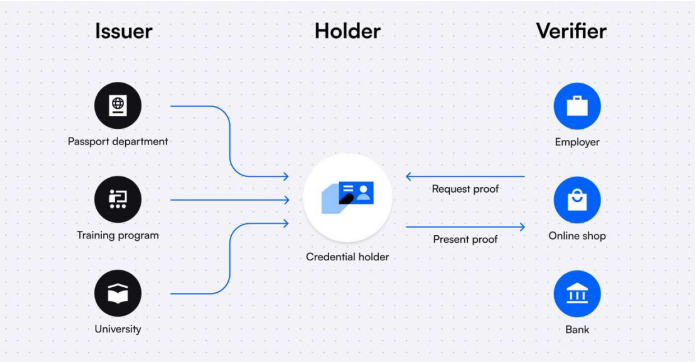
- In 2021, almost 1 in 10 qualified nurses who were issued new licenses last year waited six months or longer before they could start working. More than a third of

these 226,000 registered nurses and licensed practical nurses waited at least three months.

- Supply chain fraud is an increasingly global business risk for organizations. The Association of Certified Fraud Examiners say that 83.5% of fraud cases it surveyed in 2016 featured asset misappropriation schemes including fraudulent billing and disbursements.
- 71.1 million people fall victim to cyber crimes every year and individuals lose an average of US$4,476.
- 96% of baby boomers, 94% of Gen X, and 93% of Gen Z don't trust social media platforms to protect their data.

But don't get too down because there's hope! As decentralized identity technology gains more adoption, people and organizations will be able to share data securely.

What is a Decentralized Identity?



In a decentralized identity system, there is an issuer, holder, and verifier

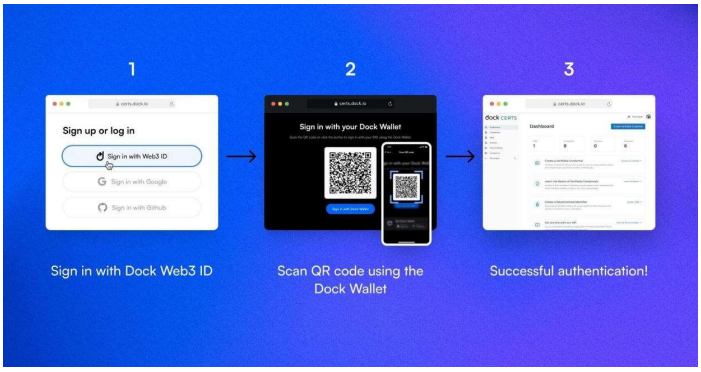
Decentralized identity is a type of identity management that allows people to control their own digital identity without depending on a specific service provider.

A digital identity is the body of information about an individual, organization, or electronic device that exists online. Data that form a digital identity include:

- User names and passwords
- Search history
- Social security number
- Buying history

A verifiable proof of existence is often needed for us to exercise our right as citizens to access essential services like healthcare, banking, and education. Unfortunately, 1 billion people in the world don't have an official proof of identity. With decentralized identity systems, all you need is an internet connection and a smart device which are becoming more accessible in emerging economies.

Key Benefits of Decentralized Identity Solutions



You can sign in securely without a password for platforms that use Web3 ID technology.

These are the key advantages of decentralized identity for:

Organizations: Issue and verify fraud-proof credentials and documents instantly and reduce the risk of data breaches by storing less user information

Individuals: Own and control your digital identity with more privacy

Developers: Secure authentication sign-in for app users that eliminates the need for passwords and privacy-preserving user verification is used

Why Is Decentralized Identity Important for Organizations?

Decentralized identity solutions come with many advantages for organizations including:

- **Allows organizations to verify information in seconds** without having to contact the issuing party, like a driver's licensing organization or university for

example, to ensure that IDs, certificates, or documents are valid. Traditional, manual verification processes take weeks to months which slows down recruitment and processing times while using a lot of financial and human resources. Imagine being able to instantly verify someone's credentials in seconds by scanning a QR code or running it through a user-friendly credential verifier tool

- **Prevents certificate fraud**
- **Improved data security** with public-key cryptography to encrypt and decrypt information safely
- **Reduces the risk of being targeted for cyber attacks** by storing less user data

Being able to verify credentials instantly is beneficial for a variety of use cases including speeding up the hiring process and reducing the risk of hiring someone without the appropriate credentials.

Many organizations around the world must follow regulations on how they collect, store, and use user data. If they don't follow the regulations, they can face penalties and sanctions for breaking the rules or data breaches.

The impact of data breaches on organizations:

- The average cost of a data breach for a small business is US$108,000 a year
- The average time to identify a data breach inside an organization is 206 days and another 73 days to fix it

- Small businesses are the victims of 43% of data breaches
- For large corporations, the average cost of a data breach is US$204 per employee while for SMBs it costs an average of US$3,533 per employee

Why Is Decentralized Identity Important for Individuals?

Decentralized identities enable people to:

- Fully own and control their data
- Prove their claims without depending on any party
- Prevent device and data tracking as they browse websites
- Choose who they want to share their relevant information to
- No entity can take away their decentralized identity once they are stored on their mobile digital identity wallets
- Prevent the spread of their data without their knowledge

A decentralized digital wallet can be used on a phone to securely store your digital identity and credentials with encryption. This approach conceals data which greatly reduces the risk of credential tracking, hacks, and gaining unauthorized access to steal or monetize people's data. With a decentralized identity, someone has to give authorization to share information when it is requested.

Verizon's email hacking statistics show that phishing attempts are responsible for 80% of malware infections and almost 95% of all espionage attacks. Also, Facebook has had many data breaches since it was launched. In one instance, 540 million records were exposed in a Facebook data leak, which included Facebook IDs, passwords, Facebook friends, photos, and check-ins. This data is a gold mine for hackers planning phishing scams and social engineering attacks.

With a decentralized identity, passwords don't exist. Rather cryptographic keys are used to authenticate users when they sign in. You could sign into a website with your Decentralized Identifier data instead of a user name. Basically, you only need to share the information that's relevant and necessary to access each service.

Why Is Decentralized Identity Important for Developers?

Decentralized identity solutions help developers by:

- Creating opportunities to build user-centric apps that eliminate the need for passwords and an inefficient authentication process that will enhance the user experience
- Being able to safely request data directly from users while maintaining their privacy

Imagine shopping on sites that don't need to build up and store personal details including credit card information. Instead, your verified payment and shipping information is securely transmitted from your decentralized identity wallet.

Or if someone wants to apply for a loan application, instead of finding all the paperwork, they can give permission to the bank to instantly receive all of the relevant information to show that they are eligible for a loan, including their salary, address, and name.

Issue Fraud-Proof Credentials Efficiently

If an organization like a university or training program is issuing credentials, they can do so securely by making credentials fraud proof. Fake diplomas are a billion-dollar industry and it's very easy for people to forge a certificate. This creates many risks for companies and impacts people's safety as many people who get fake credentials work in health care or more risky field work operating heavy machinery. Even back in the 80s, there were approximately 5,000 fake doctors in the US and it is now believed that there will be many more.

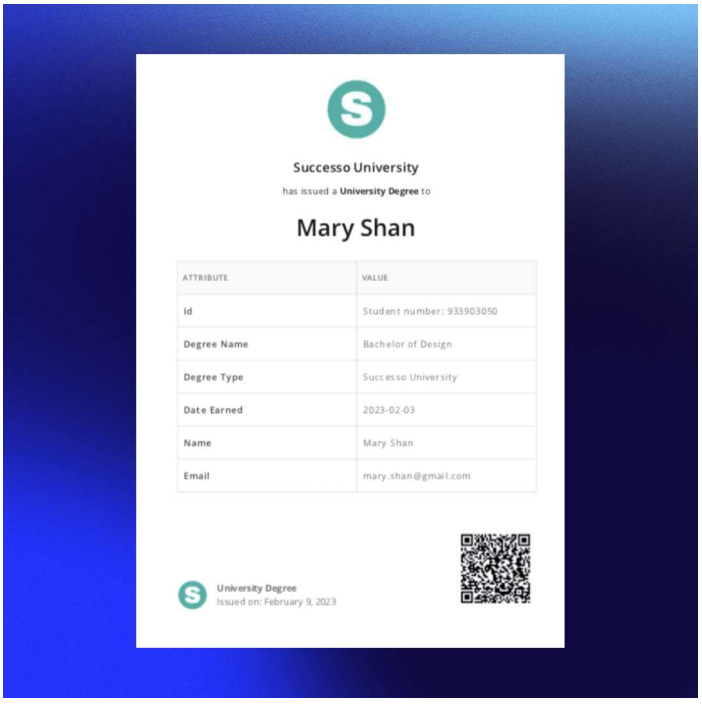
By using decentralized identity technology, organizations help prevent fraud to ensure that you are hiring qualified people with authentic credentials. Let's say a company is

looking for a project manager and they have a practice of hiring efficiently to get the best candidates. Many organizations take a long time to recruit and verify the credentials of candidates resulting in them losing out on great prospects as high-quality applicants often get multiple offers.

Here is how the company leverages decentralized identity technology to hire efficiently:

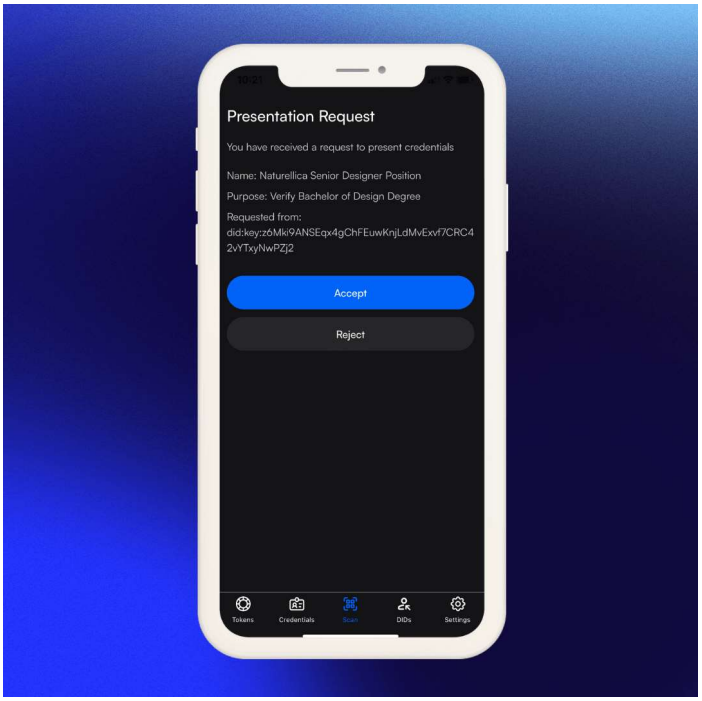
1. Mary, the job applicant, manages her decentralized identity and Verifiable Credentials on her phone with a Dock Wallet and wants to apply for the company Naturellica looking for a Senior Graphic Designer.

2. Mary's University issues her Bachelor of Design as a Verifiable Credential that she stores on her digital wallet and this credential can't be faked.

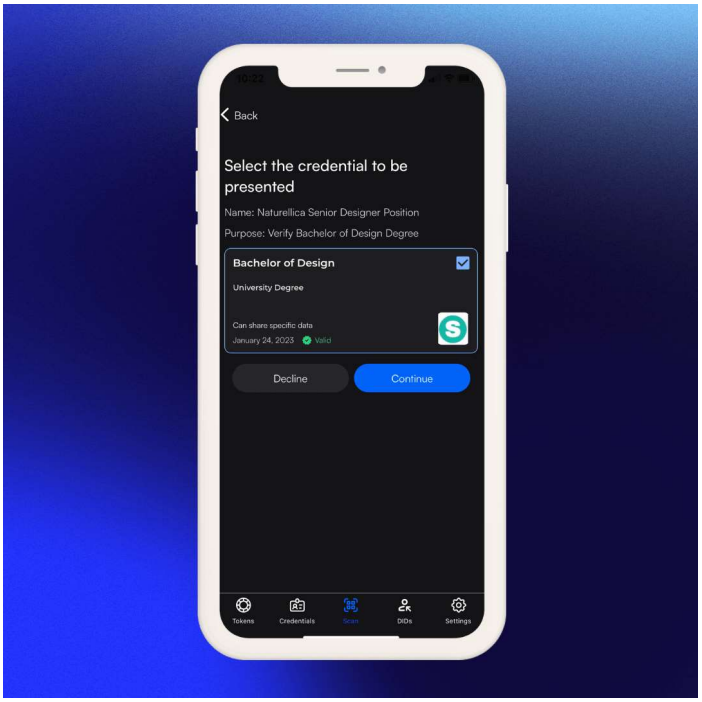


3. The company makes a job offer and they just need to check that her certificate is authentic. HR requests to view Mary's credentials and starts the verification process with this QR code that Mary can scan:

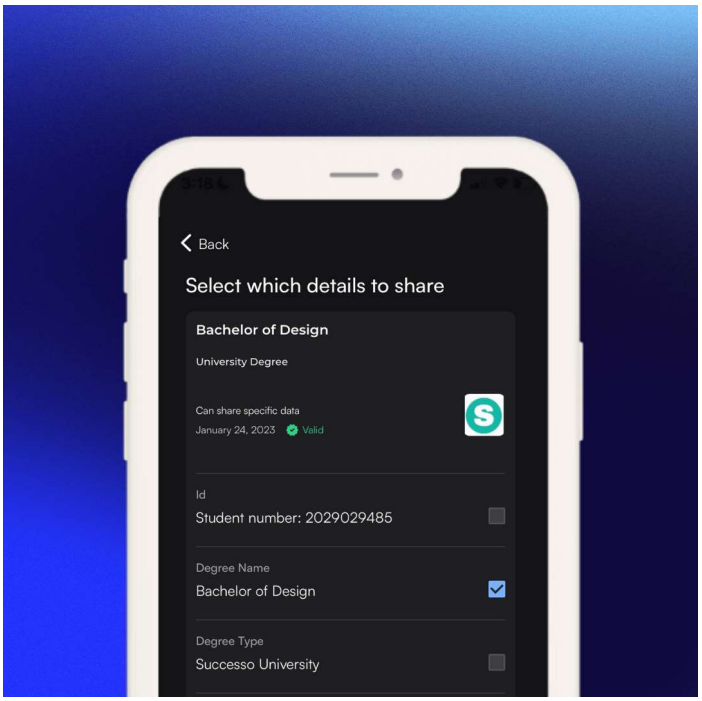
4. Mary scans the company's QR code to start the verification process.



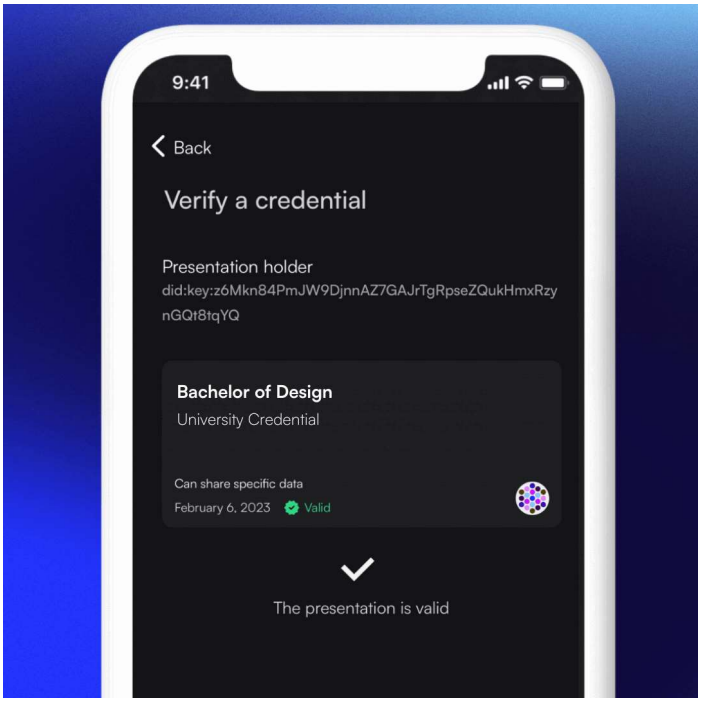
5. Mary selects the relevant credential to verify.



6. Mary can select which parts of her credential she wants to share rather than showing all of the details on the university degree to maintain privacy.

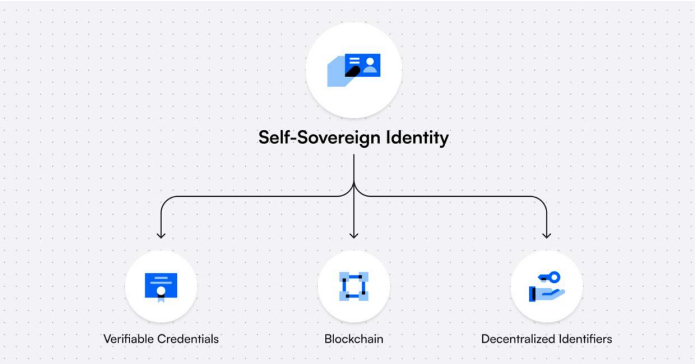


7. The company instantly sees that her credential is authentic and they offer Mary the job.



The traditional, manual verification process would normally take weeks to even months.

Decentralized Identity and Self-Sovereign Identity: What's the difference?

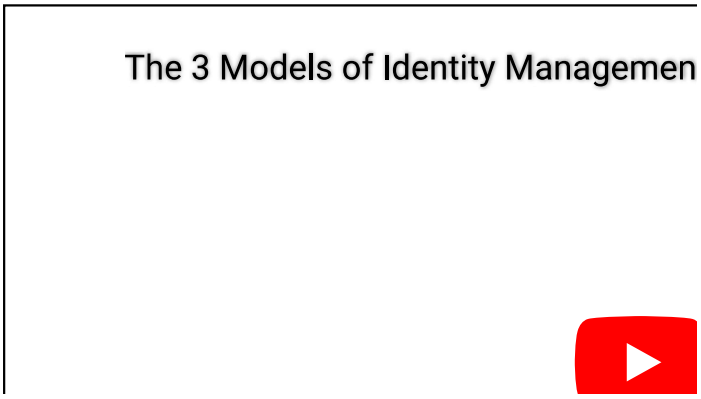


The term “decentralized identity” is used interchangeably with Self-Sovereign Identity (SSI), which is an approach to digital identity that gives individuals control of their digital identities. The three pillars of Self-Sovereign Identity are:

- **Blockchain:** A decentralized database that is shared among computers in the blockchain network that records information in a way that makes it very difficult to change, hack, or cheat the system.
- **Verifiable Credentials (VCs):** Digital cryptographically-secure versions of both paper and digital credentials that people can present to organizations that need them for verification.
- **Decentralized Identifiers (DIDs):** Cryptographically verifiable identifiers created by the user, owned by the user, and independent of any organization. DIDs contain no personally identifiable information.

A growing number of organizations in government and in the private sector around the world are leveraging decentralized identity technology, including the EU. As the world moves more and more towards Web3, which is the next evolution of the internet, an increasing number of people will take back control of their data through decentralization and blockchain.

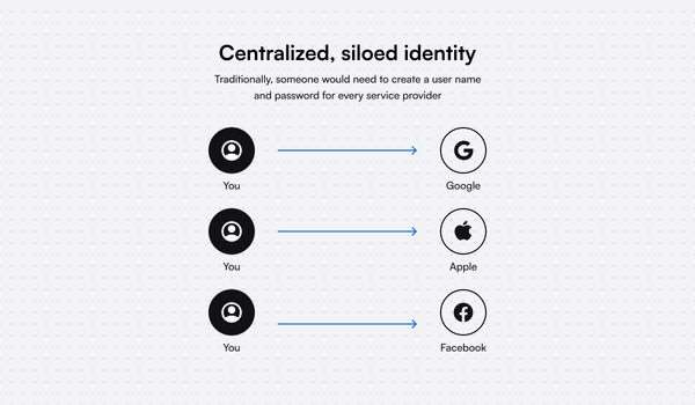
Problems and Risks With Centralized and Federated Digital Identity Systems



Centralized Identity Management: Administrative Control by a Single Authority or Hierarchy

Almost all of our digital identities are connected through services, devices, and apps.

Our personal information like our credit card, name, and address is being stored and shared on an increasing number of websites while our data is often used by websites to track people to display targeted content and advertise. As people access more websites and apps, the more accounts they have to create and manage, which creates a bad user experience.



Centralized systems often make digital identities vulnerable to cyber attacks and privacy breaches, including identity theft. Because so much user data is stored in one place, hackers could access a large amount of confidential information.

Federated Identity Management

Because of the problems that resulted from the centralized digital identity model, federated identity was developed. A federated identity allows authorized users to access multiple applications and domains with a single set of credentials like when people can use their Google or Facebook to sign into websites or apps. Signing in this way is also referred to as "single sign-on" tools.

While this method of signing in is more convenient for people because they don't have to create a whole new account, the main downside is that if your password gets stolen, all of the other sites you used with that single sign-on account could be exposed. You would have to trust both companies that offer single sign-on to protect your privacy and security as well as all of the third-party websites that offer these options to implement them correctly. In recent years, there have been several cases of Facebook and Google misusing information, including Facebook user data to manipulate people's moods and Google employees leveraging their positions to steal, leak, or abuse data they may have access to.

More aspects of our lives require verification of our identities in order to apply for a mortgage, buy a car, or sign up for a new

service. People have little to no choice but to surrender their privacy to use the things they want.

Thankfully, decentralized identity solutions can effectively solve many of these privacy and data breach problems. Decentralized identity gives people full ownership and control of their personal information and credentials.

Decentralized Identity Management vs. Centralized Identity Management

Decentralized identity management is a way of managing your online identity where you, the user, have control over your own personal information, rather than having it controlled by a central organization or company. This is different from centralized identity management, where a central organization or company holds and controls all of your personal information.

One of the main benefits of decentralized identity management is that it gives users more control over their personal information. With centralized identity management, users have to trust that the central organization or company will keep their personal information safe and not misuse it. With decentralized identity management, users have the ability to control who has access to their personal

information, and can easily revoke access if necessary.

Another benefit of decentralized identity management is that it is more secure. With centralized identity management, if the central organization or company's security is compromised, all of the personal information of all of its users is at risk. With decentralized identity management, each user's personal information is spread out and not centralized in one place, so even if one user's information is compromised, it does not affect the personal information of other users.

Also, decentralized identity management is more private. With centralized identity management, users often have to give out a lot of personal information to the central organization or company, which can be used for targeted advertising or other purposes that the user may not be comfortable with. With decentralized identity management, users only have to share the personal information that they want to, and can keep the rest private.

Centralized Identity Management	**Decentralized Identity Management**
Increased risk of data breaches from storing data in a centralized system	Data is decentralized and stored by users in their wallets, which reduces the risk of large scale data breaches
Data may be collected, stored, and shared with other parties without your knowledge	Data is only shared when you give authorization

Centralized Identity Management	Decentralized Identity Management
Data is owned and controlled by organizations, apps, and services	Data is fully owned and controlled by the user

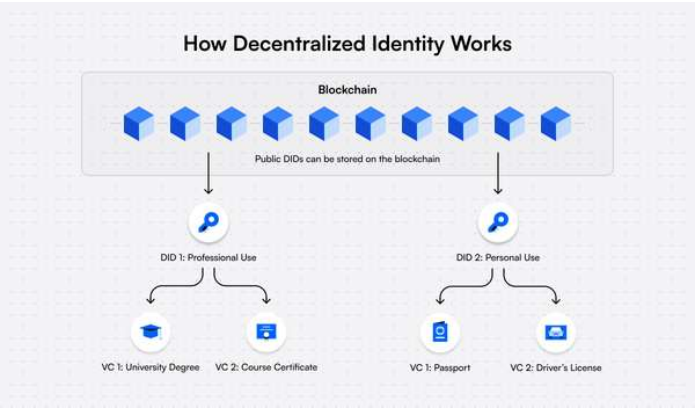
Establishing Standards for Decentralized Identity

There are many organizations working to standardize and shape the field of decentralized identity. These are the key organizations:

- Decentralized Identity Foundation (DIF): An engineering-driven organization focused on developing the foundational elements necessary to establish an open ecosystem for decentralized identity and ensure interoperability between all participants.
- World Wide Web Consortium (W3C): The mission of the W3C Digital Identity Community Group is to identify and resolve real world identity issues, to explore and build a more secure trusted digital identity ecosystem on the internet for people, organizations, and things. Their work focuses on the ecosystem's scalability, interoperability, mobility, security, and privacy.
- Internet Engineering Task Force (IETF): An open international community of network

designers, operators, vendors, and researchers working on the evolution of the Internet architecture and the smooth operation of the Internet.

How Decentralized Identity Works

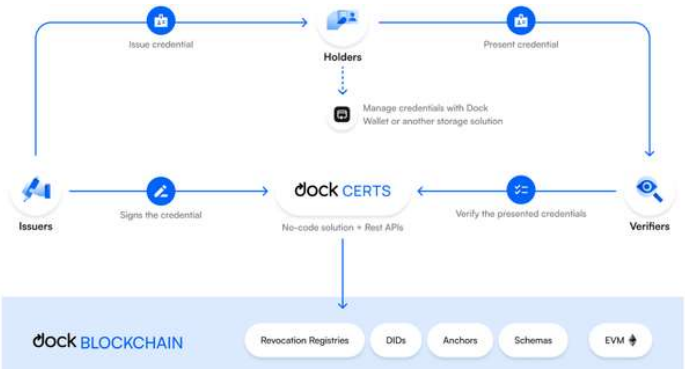


A decentralized identity system has these main elements:

1. **Blockchain:** A decentralized database that is shared among computers in the blockchain network that records information in a way that makes it very difficult to change, hack, or cheat the system.
2. **Decentralized Identity Wallet:** An app that allows users to create their decentralized identifiers and manage their Verifiable Credentials.
3. **Decentralized Identifier (DID):** A unique identifier on the blockchain made up of a string of letters and numbers that contains details like the public key and verification information.

4. **Verifiable Credential (VC):** A digital, cryptographically secured version of both paper and digital credentials that people can present to organizations that need them for verification. These are the main parties in the VC system:

- **Holder:** A user who creates their decentralized identifier with a digital wallet app and receives the Verifiable Credential.
- **Issuer:** The organization that signs a Verifiable Credential with their private key and issues it to the holder.
- **Verifier:** A party that checks the credentials and can read the issuer's public DID on the blockchain to verify if the Verifiable Credential the holder shared was signed by the issuer's DID.



The main parties in the Verifiable Credentials system are the holders, issuers, and verifiers.

Let's go into more detail about how each of these elements works individually and then how they all work together.

Decentralized Identity Using

Blockchain

A blockchain is a digital database that records transactions across a network of computers. It is called a "blockchain" because it is made up of a chain of blocks that contain information about the transactions. Each block contains a list of transactions, and once it is added to the chain, the information in it cannot be altered (or it's extremely difficult to alter). This makes the blockchain secure and transparent, and it is often used for things like cryptocurrency and online voting.

With Dock, only DIDs are registered on the blockchain, but no Verifiable Credential data is ever put on the blockchain for security and privacy.

<h3>Key Features of a Blockchain</h3>

Security: Blockchain uses cryptography to ensure that once a block is added to the chain, it's extremely difficult to alter, making the information stored in it secure.

Tamper-resistance: The blocks in a blockchain are linked together using a cryptographic function, making it difficult for any malicious actors to tamper with or alter the data stored in the blocks. Once data is written on blockchain it is almost impossible to change, tamper or delete, providing trust and security to the data.

Decentralized: A blockchain is a decentralized system, meaning that it is not controlled by any one central authority or organization. This allows for a more democratic and transparent system.

Transparency: All the transactions are recorded in a public ledger, which can be viewed by anyone on the network, promoting transparency and accountability.

Trustless: Blockchain enables trustless transactions by using consensus algorithms, smart contracts and digital signatures, which eliminates the need for third party intermediaries.

<h3>How Blockchain Is Used</h3>

Here is how each party uses the blockchain in a decentralized identity system:

- **Holder:** Owner of the Verifiable Credential (e.g. driver's license) has their public DID on the blockchain.
- **Issuer:** The issuer's public DID and associated public key is on the blockchain. When an issuer, like a licensing organization, provides a credential to a holder like a driver's license, the issuer signs the credential with their private key.
- **Verifier:** A verifier like an on-demand driving company can check the blockchain to ensure that the licensing department that they trust did in fact issue the license and who it was issued to.

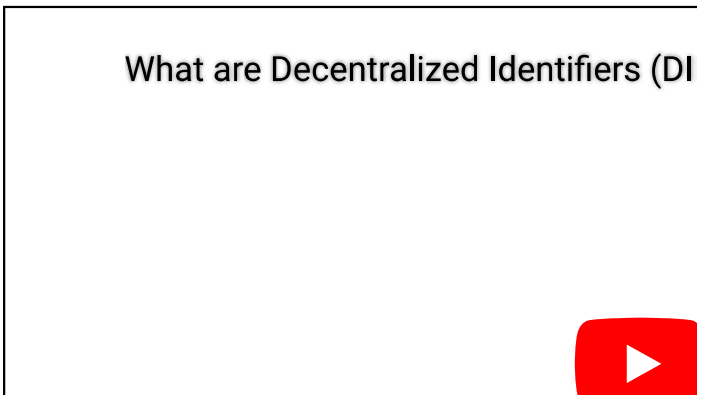
The blockchain allows everyone in the network to have the same source of truth about which credentials are valid and who authenticated the validity of the data inside the credentials. The blockchain establishes a basis of trust by maintaining a verifiable registry (or records) of:

- All DIDs

- Proof of credentials issued (if the credential is anchored to demonstrate proof of existence and authenticity)
- Public cryptographic keys (codes used to encrypt and decrypt information)
- Revocation registries

The identity information is not stored on the blockchain but rather on the holder's digital wallet. The credentials issued using the Dock blockchain are stored off-chain, usually in someone's decentralized digital wallet app.

What Are Decentralized Identifiers (DIDs)?

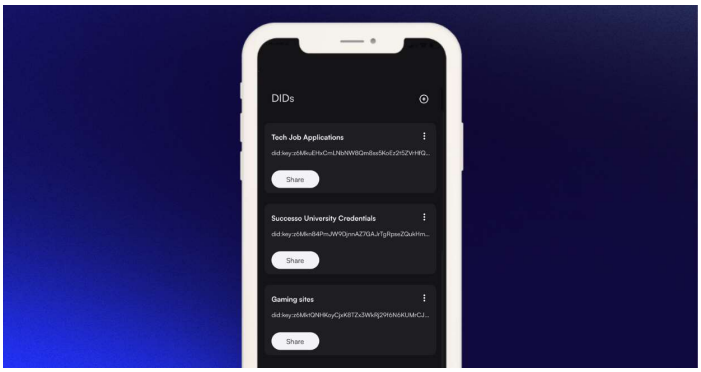


Dock's Solutions Architect Mike Parkhill explains how decentralized identifiers (DIDs) work and their importance.

A decentralized identifier (DID) is a way to identify yourself or something online without relying on a centralized company or organization. Imagine a phone number is like a centralized identifier because it is assigned

to you by a phone company, and they keep track of who it belongs to.

A DID is like a personal phone number that you create, own, and control. You can use it to prove who you are online without having to rely on a third party. It's like having a digital passport that you can use on the internet, and it's not controlled by any one company or organization. It's simple to understand like a phone number you own and control.



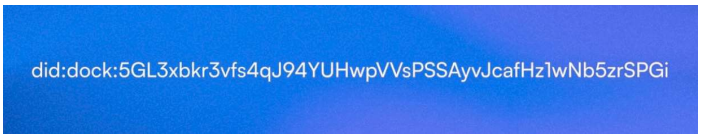
Right now, most of us use centralized identifiers like emails, passwords, and user names to access websites, apps, and services. But these identifiers have often resulted in:

- Our personal information being hacked
- Identity theft
- Our data being shared with other parties without our knowledge
- Making it harder for someone to manage all of the logins
- Being at the mercy of service providers who can revoke these identifiers at any time

But DIDs solve many of these problems. A Decentralized Identifier (DID):

- Is a globally unique identifier made up of a string of letters and numbers that is like an identifying address on the blockchain and independent of any organization
- Enables a universally accepted standard for exchanging and verifying digital credentials
- Allows the owner to prove cryptographic control over them
- Comes with one or many private key and public key pairs
- Doesn't contain personal data or wallet information
- Enables private and secure connections between two parties and can be verified anywhere at any time

Here is a decentralized identifier example that can be managed in a Dock wallet:



A party, either an individual or organization, can make as many DIDs as they want for different relationships. DIDs are like different personas that people can create.

Right now, many people use LinkedIn to show their professional experience and information. But because they don't want employers to see their personal photos and interests, they make a separate Facebook

profile. A DID is similar in that you can make different profiles for different purposes.

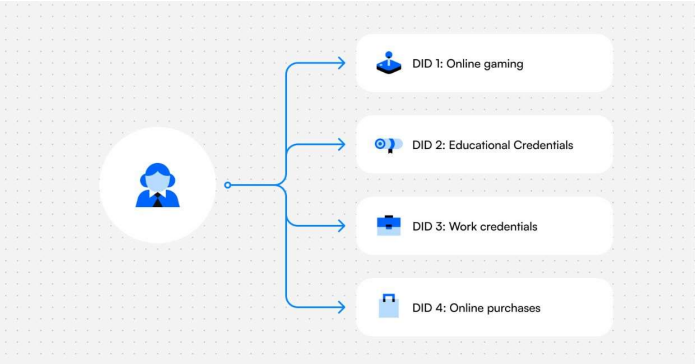
For example, you can have a DID for:

- Your personal interests like signing in to shopping websites or showing you are of legal age to buy alcohol
- Professional purposes where you can use this DID to show educational or professional credentials to an employer
- Accessing different cryptocurrency-related apps and services that need to verify your identity for your trading and investment activities

Right now, many people use LinkedIn to show their professional experience and information. But because they don't want employers to see their personal photos and interests, they make a separate Facebook profile. A DID is similar in that you can make different profiles for different purposes.

For example, you can have a DID for:

- Your personal interests like signing in to shopping websites or showing you are of legal age to buy alcohol
- Professional purposes where you can use this DID to show educational or professional credentials to an employer
- Accessing different cryptocurrency-related apps and services that need to verify your identity for your trading and investment activities



Decentralized Identity Solutions: Dock's Tools

Dock's decentralized identity solutions enable organizations and people, to completely create, own, and manage their digital identity.

Dock Certs: User-friendly, No Code Platform for Organizations

Enables users to easily create and manage their decentralized identity as well as issuing, verifying, and revoking Verifiable Credentials. With Dock Certs, organizations can issue fraud-proof certificates that will protect the value of their credential and enhance their reputation among their stakeholders.

Dock Wallet: Individuals and Organizations

People can conveniently take their DIDs and associated Verifiable Credentials anywhere by storing them securely on their Dock Wallet. The wallet enables people to easily create, edit, and manage their decentralized

identifiers and no party can take away these identifiers.

Certs API: Developers and Organizations

Dock's Certs API enables users to conveniently issue, verify and revoke Verifiable Credentials (VCs), manage decentralized identifiers (DIDs), and interact with the Dock blockchain. We have open-source software on GitHub that can be used with the API.

Certs API Benefits:

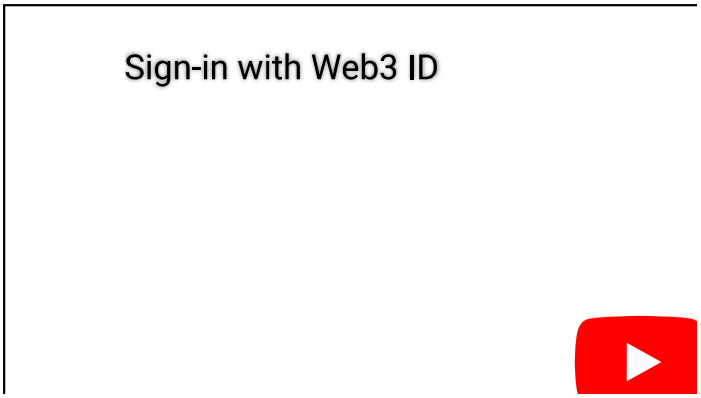
- Easy to integrate with other systems.
- Users can issue Verifiable Credentials with one call
- Dock takes care of key and token management for the customers
- Interoperable as Dock follows the international standards of the World Wide Web Consortium for DIDs and Verifiable Credentials

Web3 ID: Developers and Organizations (Open-Source and Free)

Web3 ID is an authentication and sign-in system that enables:

- Verification of private user data from their identity wallets. Always with the users' consent
- Passwordless login and prevents user tracking
- Security of user data with the use of cryptography

- Easy integration of OAuth, a standard protocol that enables people to provide secure access to applications without needing to share login details

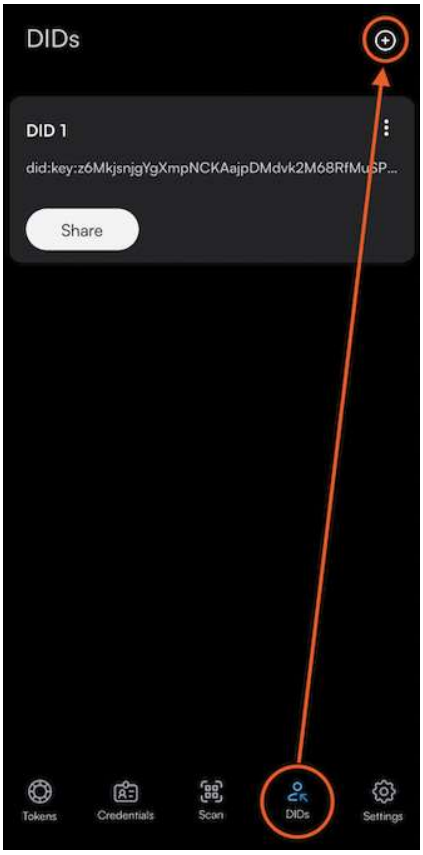


How Do You Create a Decentralized Identity With the Dock Wallet?

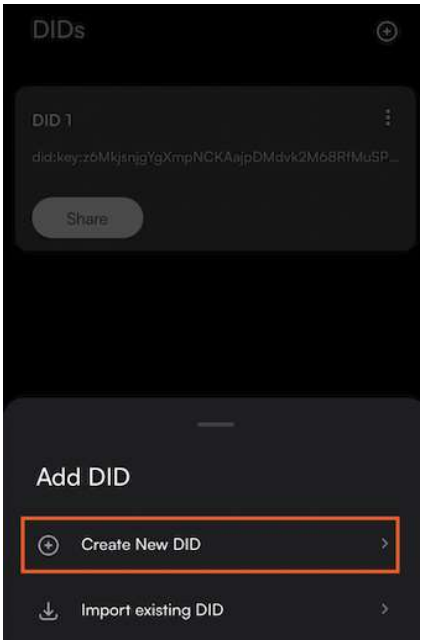
It's easy to start creating your decentralized identity with the Dock Wallet app, a wallet that allows users to fully own and control their decentralized identifiers. Verifiable Credentials are associated with DIDs.

Just follow these steps to create a DID:

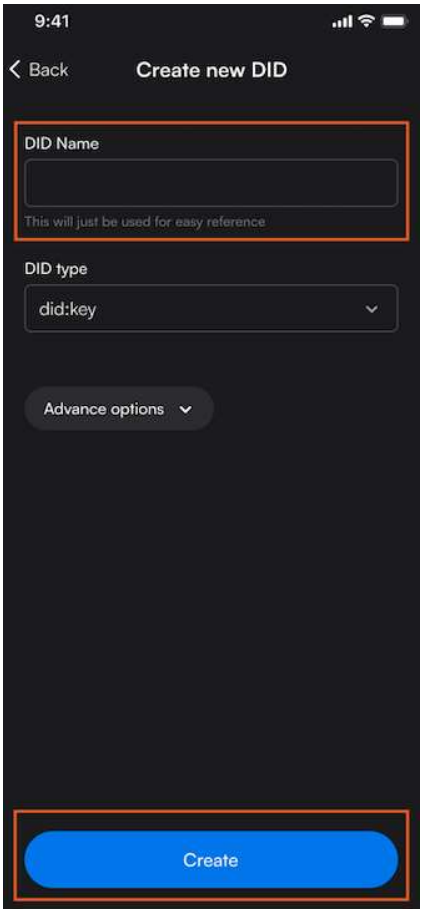
1. Select **DIDs** at the bottom of your wallet and click on the **+** sign on the top right of the screen.



2. Select **Create New DID**.

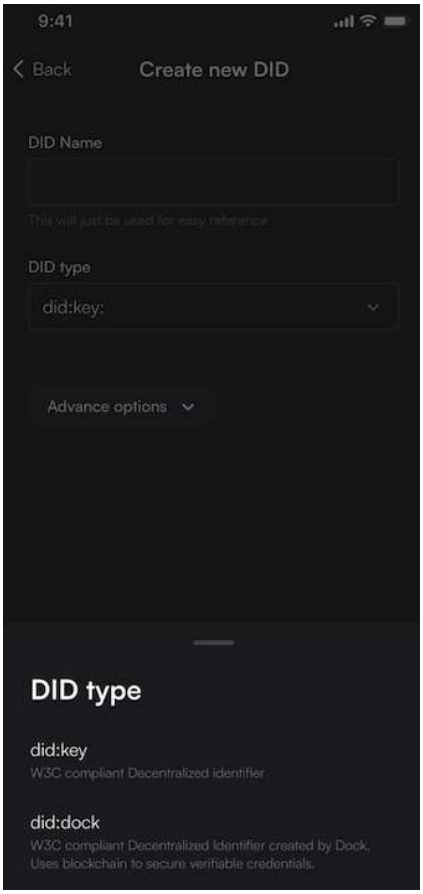


3. Name your DID like educational credentials, NFTs, IDs etc. and select **Create**.

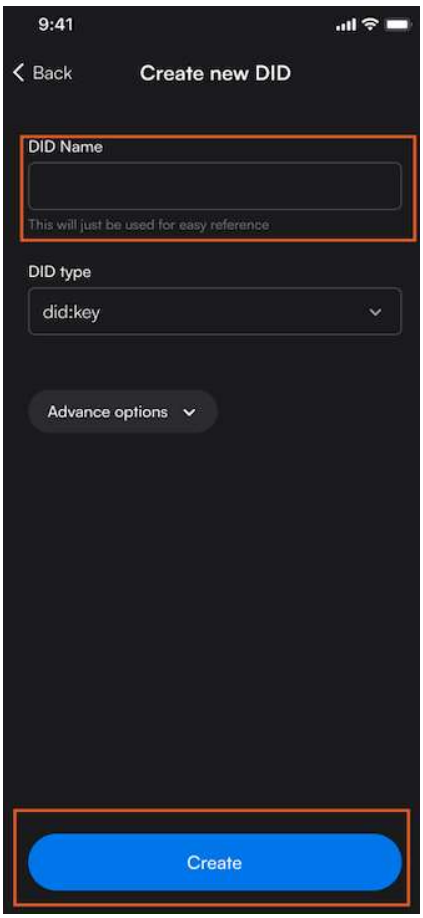


4. Choose a DID type. Difference between the two keys:

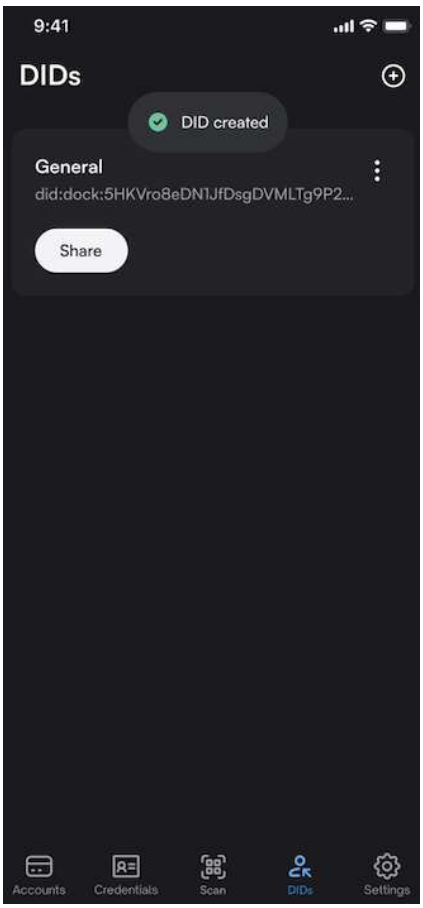
did:key	did:dock
Free to create this type of DID	Costs tokens to create this type of DID
DID isn't stored anywhere	DID is stored on the blockchain
	Will later have the capability to support several key pairs so you can choose which key pair to apply such as using different keys for different applications while still using the same DID.



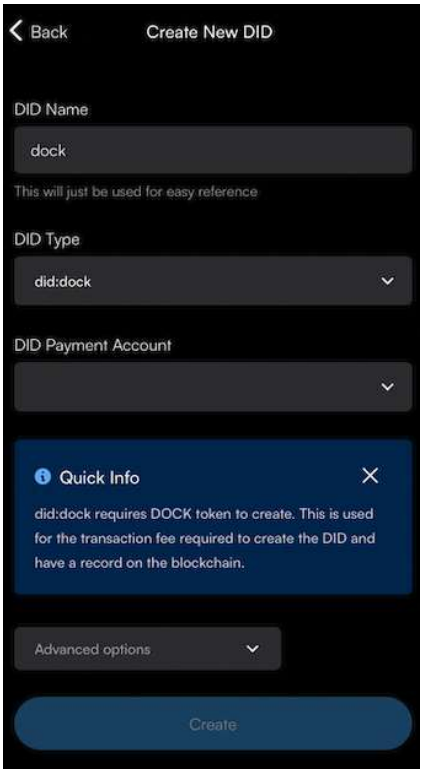
5. Select **Create** after selecting did:key for example and naming it.



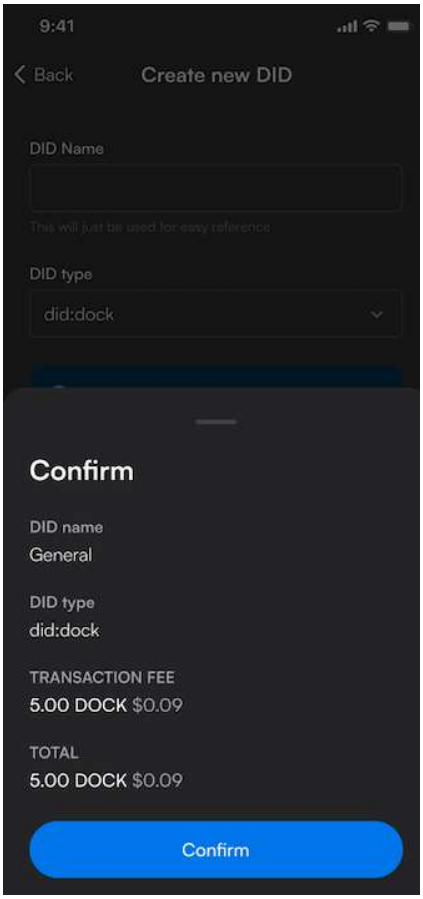
6. did:key is created.



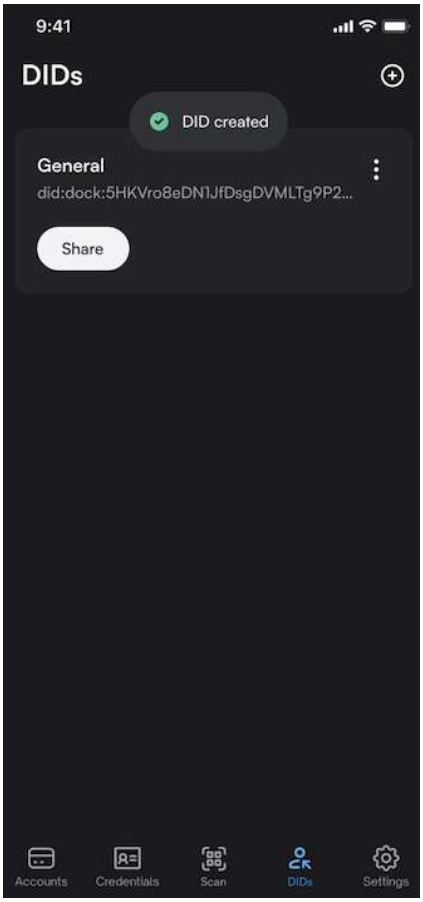
7. This is the next step if you select did:dock. Name your DID and select the DID Payment Account. If you have multiple accounts, you will see an extra field on this screen for you to choose which account to use to pay for the DID.



8. Select **Confirm**.

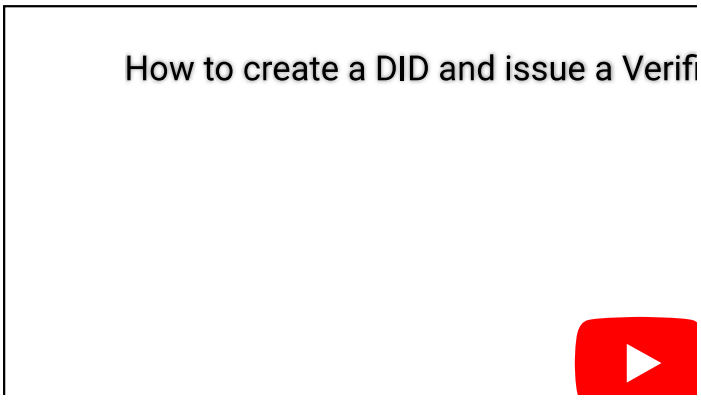


9. You now have a new DID!



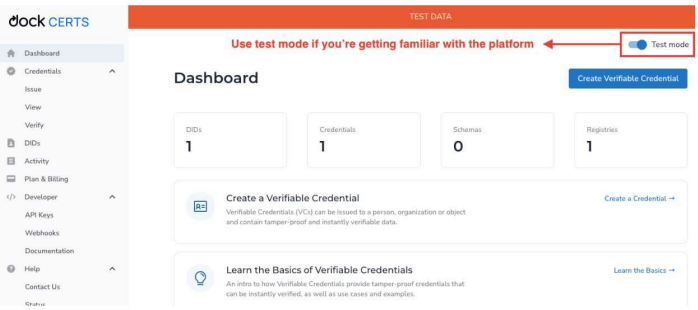
Click here to learn more about how to manage DIDs in your Dock Wallet.

How Do You Create Decentralized Identity With Dock Certs?



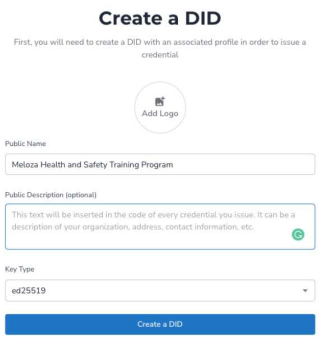
With a Dock Wallet and Dock Certs, you can create a DID by following these steps:

1. Create an account on Dock Certs and login. If you're just getting familiar with the platform, you can use **Test mode**.

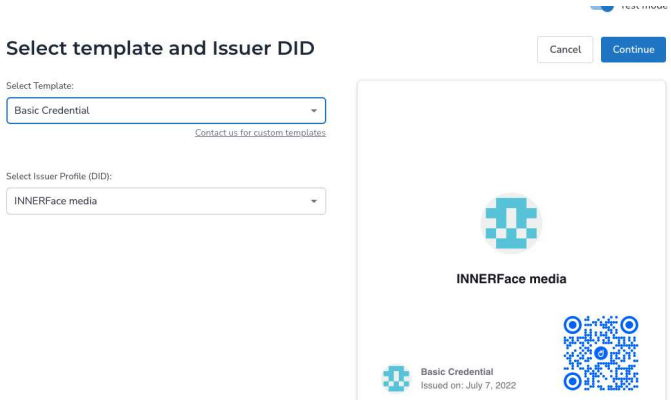


2. Click **Create Verifiable Credential** on the top right.

3. Create the issuer profile (a university for example) and you can leave the Key Type to the default setting. Then select **Create a DID.**

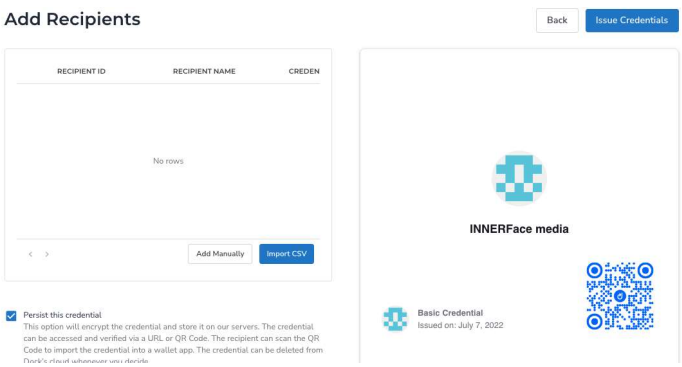


4. Choose among the basic template options, select the DID, click **Continue** on the top right.



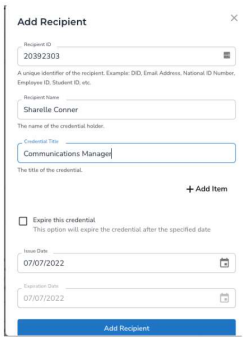
Issuing a Verifiable Credential in a Decentralized Identity System

1. You can add credential recipients manually one by one or in bulk with the **Import CSV option**.

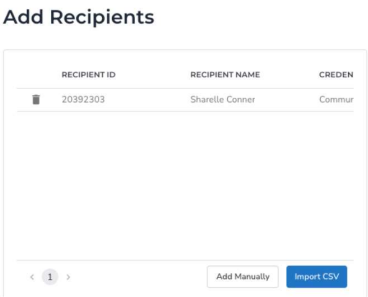


2. If you add someone manually, you will enter details like this example below where

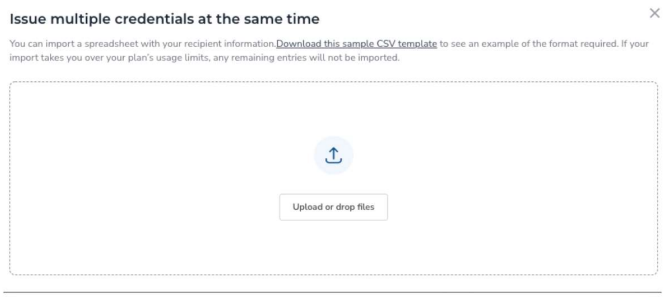
we are identifying someone by their employee number. Once you fill in all of the details, click **Add Recipient.**



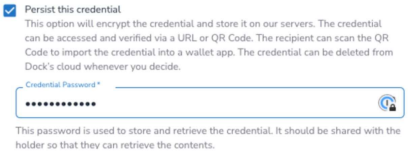
3. The information will appear like this:



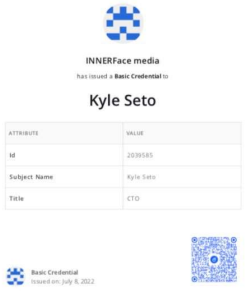
4. If you want to do bulk issuance, you can also import a CSV file. Download the sample template, fill it in, and upload it.



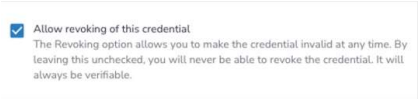
5. The next option is to **Persist the credential** which means that Dock will securely store the credential on our database (but NOT on the blockchain).



If you persist the credential, there will be a QR code that shows up on the PDF where the recipient can simply scan the QR code with their Dock Wallet app to import the credential in their wallet.

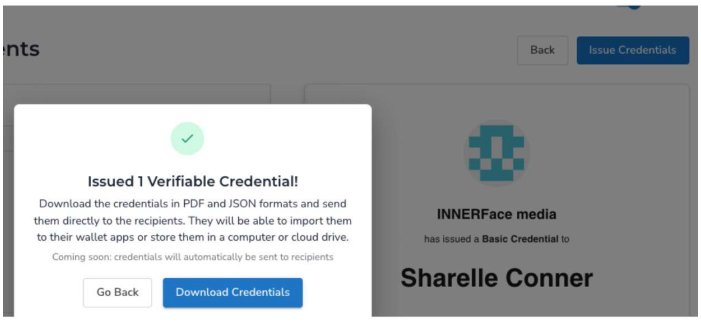


6. There is an option to add a registry (record) on the blockchain allowing this credential to be revoked.

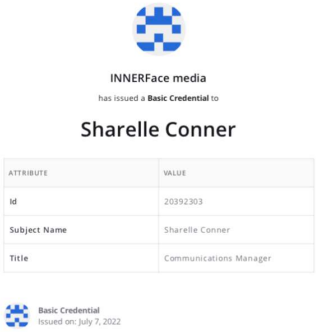


7. You can anchor the credential which will add a hash of the credential (like a digital fingerprint) you issue on the Dock blockchain. This allows someone to verify when and who created it.

8. Next click **Issue Credentials** on the top right and you will be able to download the credentials in JSON and PDF formats. A JSON file is a file that stores simple data structures and objects in JavaScript Object Notation (JSON) format, which is a standard data interchange format.



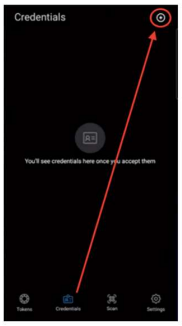
The Basic PDF credential will look like this:



It's important to know that if you don't persist or download the credential, you can't get it back.

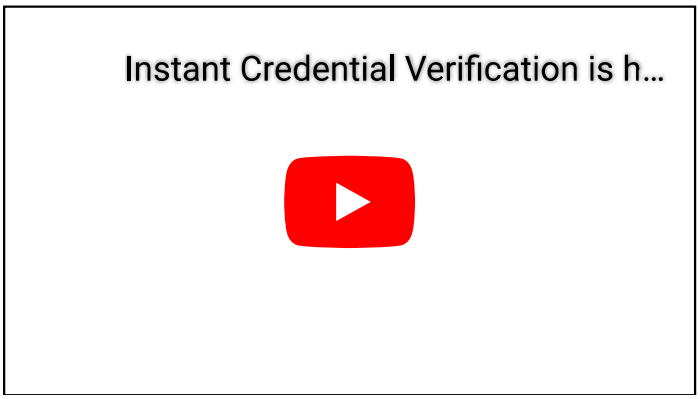
9. The issuer can email the PDF and JSON files to the recipient. Soon we will be releasing the Relay Service to automatically send the credential to the recipient's wallet.

10. If there is no QR code on the PDF file (because the credential wasn't persisted), then the recipient has to download and import the JSON file. To do this select **Credentials**, click on the + sign on the top right corner, and select the JSON file.



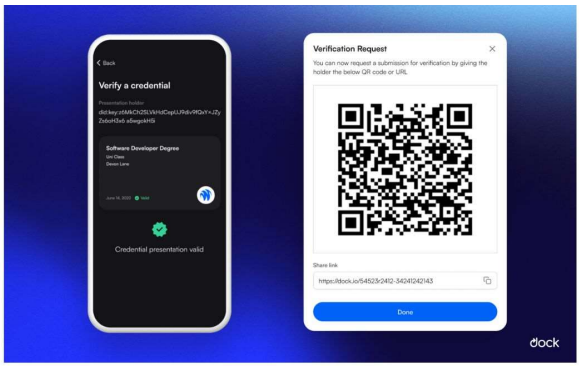
11. The credential will immediately appear in the Dock Wallet.

Decentralized Identity Verification



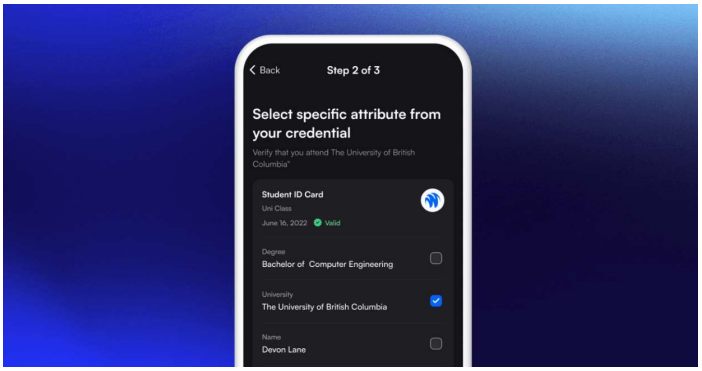
Organizations can quickly verify users' digital credentials in seconds using Dock Certs and the Dock Wallet on a phone or computer. The verification process is powered by blockchain technology, making it fast and reliable. Because Dock's tools detect fraudulent credentials, verifiers can be assured that the information presented is accurate. Organizations can verify documents with the web or wallet-to-wallet (online or in person).

Benefits of Instant Credential Verification for Organizations



- Quickly authenticate a Verifiable Credential in seconds instead of the conventional verification methods that can be time-consuming and take several weeks to months.
- Stop document fraud.
- Streamline the verification process to save time and reduce expenses by avoiding manual, time-intensive, and unproductive methods.
- Comply with data protection regulations.
- Boost operational effectiveness.
- Minimize the possibility of liabilities, fines, legal actions and catastrophic incidents by guaranteeing that only suitable candidates are hired.

Benefits of Instant Credential Verification for Individuals



With the Dock Wallet, individuals:

- Have greater control and protection over their personal data as they have the ability to selectively share parts of their credentials with a verifier. For example, they can opt to share only their degree

name and keep sensitive information such as their date of birth private.

- Effortlessly share their credentials directly from their phone.
- Reduce the risk of unauthorized data access by sharing only the required information with a verifier while keeping complete control over who has access to their information.

Complete Verification Guide for Dock Certs and the Dock Wallet

Click here for the complete guide on how to verify credentials.

Difference Between Public Key and Private Key Cryptography With an Example

Each DID comes with one or many private and public keys:

- **Private key:** Made up of a long string of letters and numbers that allows people to prove ownership, give consent to share selected data, and sign documents. It is used to both encrypt and decrypt the data. As an analogy, a private key is like a master key that can access all of your information and the owner should never share their private key with anyone.
- **Public key:** Made up of a long string of letters and numbers that can safely be shared with anyone you choose to give specific information to.

You can have multiple private-public key pairs, and it's good practice to generate new public keys when sharing information with a different party. This can be compared to using the same password for 10 different websites. It's not safe to do this for security reasons. It's better to have different and long complex passwords for all sites. Similarly, it's better to generate a new public key for each party you share information with.

Example of how private and public keys would be used

Let's say there's a health and safety training organization that provides certification for construction safety and this course is a requirement for workers to get a job with a construction company. Here is how decentralized identity helps prevent fraud and enables organizations to save a lot of time and resources issuing and verifying credentials:

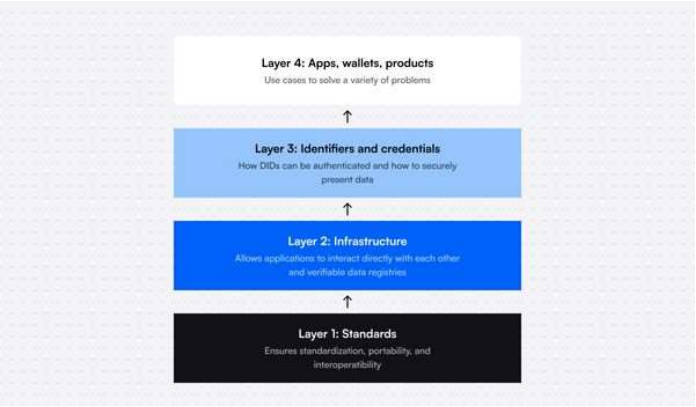
1. Carl finishes the program and the training organization requests to connect with his

digital identity wallet

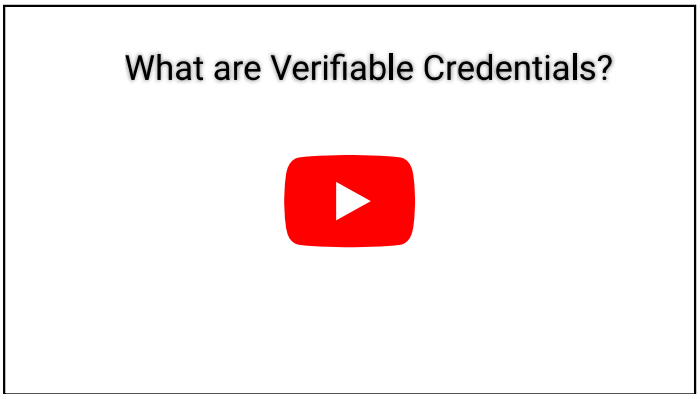
2. When Carl authorizes the training organization to connect, the wallet shares his public DID in order for them to issue the credential.
3. The training organization signs the digital certificate of completion with their **private key** and issues the credential. Their **public key** is stored on the blockchain. The organization can easily and efficiently issue many credentials at the same time with a decentralized identity platform like Dock.
4. Carl would hold his credential on a digital wallet on his phone that he can bring everywhere.
5. Carl gives the construction company authorization to see his credentials without showing any unnecessary information about himself like his address and date of birth.
6. The company instantly verifies the authenticity of his credentials by scanning a QR code and not having to contact the issuer at all because the training organization's **public key** is on the blockchain.

Traditional certification verification processes would normally take a few weeks before he can start working because the construction company would have to manually contact the issuer. The previous verification process would be time-consuming and expensive.

Layers in the Decentralized Identity Ecosystem



Verifiable Credentials

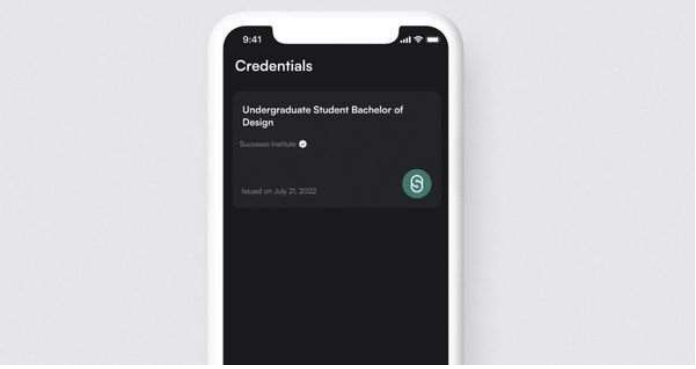


Verifiable Credentials are a digital, cryptographically secured version of both paper and digital credentials that people can present to organizations that need them for verification. A few of many examples of information that can be issued as Verifiable Credentials:

- Driver's licenses
- Passports
- Professional certifications

- Employee status

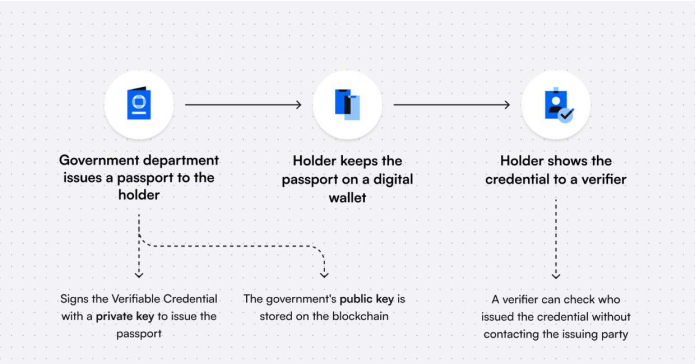
When digital credentials conform to the Verifiable Credentials Data Model 1.0, which is a standard established by World Wide Web Consortium (W3C), they can be referred to as Verifiable Credentials.



An example of a university degree issued as a Verifiable Credential that is stored on a Dock wallet.

Examples of Decentralized Identity Verification

Maintaining privacy is a major benefit of Verifiable Credentials. Let's say there's an on-demand food delivery company that requires applicants to have a valid driver's license. The company can instantly check the Verifiable Credential to confirm that an applicant has a valid driver's license. A verifiable presentation would allow an applicant, the holder, to show their license number without sharing unnecessary information like their full name or address.



In another example, a club's staff member can scan the QR code of the holder's Verifiable Credential to ensure they are at least 18 years old. The public DID of the government's licensing department is on the blockchain which allows the club to verify the authenticity of the Verifiable Credential because the club trusts the department that issued the credential. The Verifiable Credentials create trust between the parties and guarantee the authenticity of the data and claims without actually storing data on the blockchain.

In another situation, Sofia just moved to Canada without a physical copy of her university degree and she needs to prove her field of study to receive a job offer. Her university then issues her a Verifiable Credential, which is the degree, that is associated with her DID and she can store this in her digital wallet. Sofia then presents the credential to the employer who can instantly verify its authenticity.

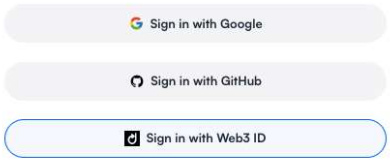
Decentralized Identity Wallet

A decentralized identity wallet enables people to securely store, manage, and share DIDs and Verifiable Credentials. It's comparable to a physical wallet that holds various IDs and claims about yourself like service cards, bank cards, and licenses. The decentralized identity wallet will store verified credential details like citizenship, employment, name, and address to prove eligibility, identity, or complete a transaction.

A mobile identity wallet stores information on the phone rather than a browser's storage or cloud. The digital wallet allows people to access apps and services without revealing personal information. DIDs also prevent your devices from being tracked and correlated (data may be traced back to someone's identity or online behavior). Verifiers can connect to the user's identity wallet and request data while the user always chooses when to give permission to share data.

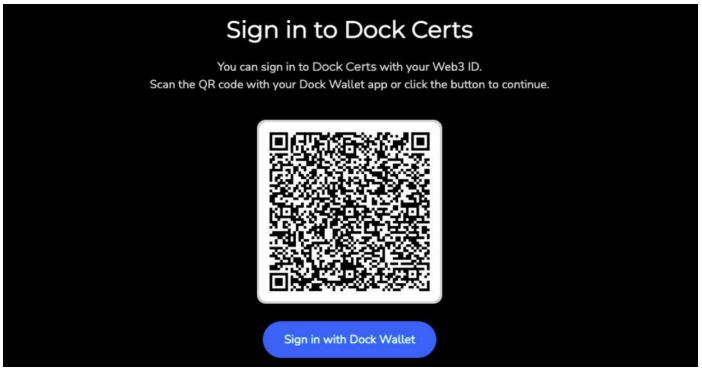
Let's say Anna wants to sign in with Dock Certs using her DID.

1. Dock Certs allow people to login with their DID using Dock's Web3 ID. This allows users to sign into the platform in a way that preserves their privacy.

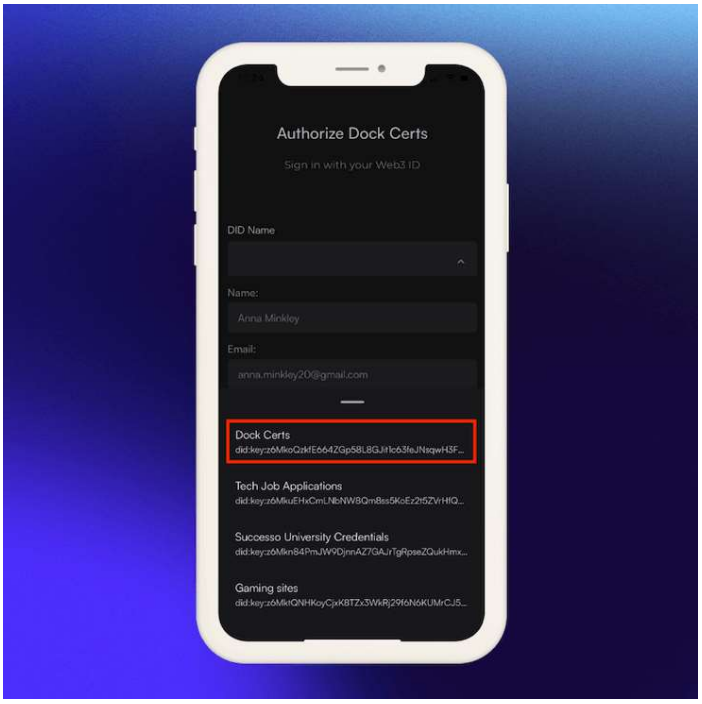


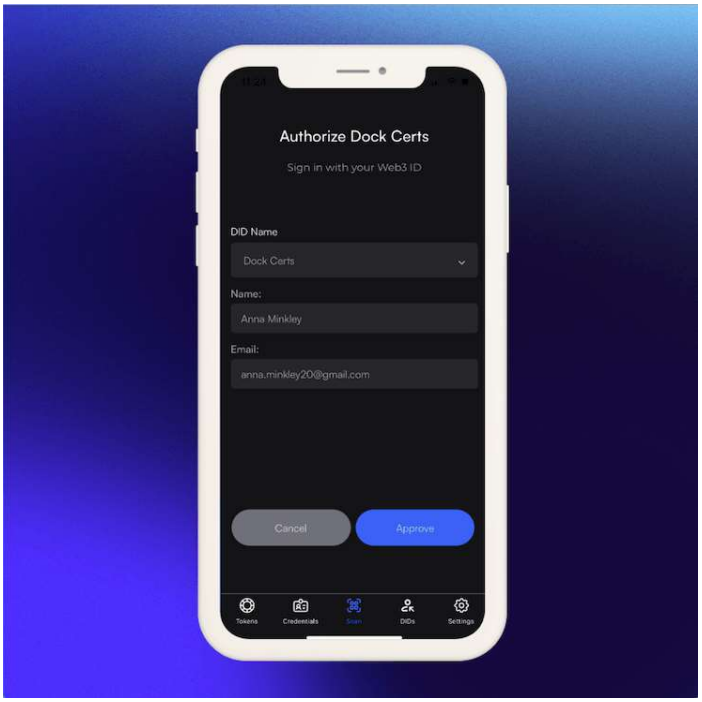
2. Anna scans the QR code with her Dock Wallet and authorizes the website to instantly

verify her credential.

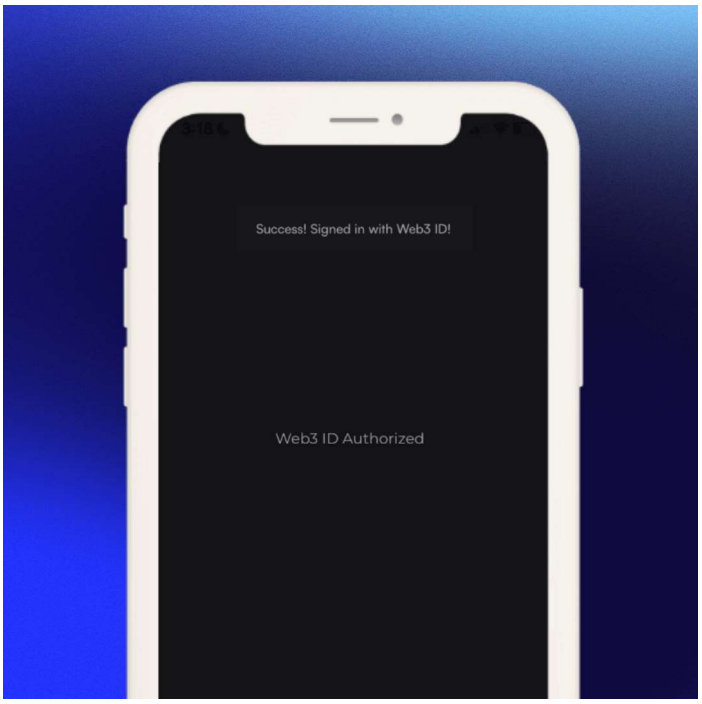


3. She selects the DID that she created for Dock Certs then clicks **Approve**.

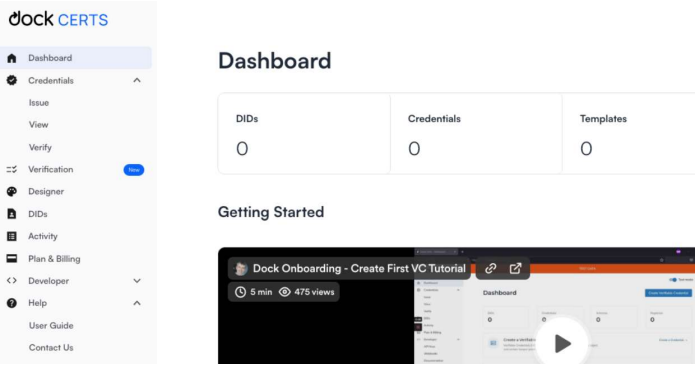




4. Anna successfully signs into Web3 ID



5. Anna accesses the Dock Certs platform.



Decentralized Identity Use Cases

Here are just a few of many examples of how decentralized identity technology can solve many problems that result from traditional verification processes and centralized identity management systems in a variety of industries.

Industry	Traditional Process	Problems/Risks	Verifiable Credentials Solution
Supply chain	Relies on physical IDs and documents to demonstrate compliance, which creates inefficiencies.	Documents can be easily forged and difficult to authenticate. Manual verification process is slow and prone to errors. An importer can bring unapproved, non-compliant medical supplies into a market putting public health at risk.	Verifiable Credentials can't be forged and they can be verified within seconds without contacting the issuing party, saving a tremendous amount of time and money.
Finance	To access financial	Individuals have no control over	The data provided in the

Industry	Traditional Process	Problems/Risks	Verifiable Credentials Solution
	services, someone has to go through compliance screening by submitting personal details in physical form that is stored in a large database and shared with one or more third parties that conduct know your customer (KYC) and credit checks.	how their data is secured, shared, and accessed by third parties.	credentials is cryptographically secured, tamper-proof, and can be verified.
Healthcare	Employers use manual processes to verify paper-based licenses and certificates for healthcare providers.	Traditional verification takes weeks if not months, which creates delays in filling much-needed health care roles.	Organizations that provide and regulate medical licenses for the healthcare workforce can issue licenses in the form of digital credentials. The recipients of these licenses can then easily share them for instant verification by any hospital, clinic, or medical department where they would like to work.

Summary of Key Terms

Blockchain: A decentralized database that is shared among computers in the blockchain network that records information in a way that makes it very difficult to change, hack, or cheat the system.

Centralized identity management: Administrative control by a single authority or Hierarchy.

Decentralized digital identity wallet: Enables people to securely store, manage, and share DIDs and Verifiable Credentials.

Decentralized Identifiers (DIDs): Cryptographically verifiable identifiers created by the user, owned by the user, and independent of any organization. DIDs contain no personally identifiable information.

Decentralized identity: A type of identity management that allows people to control their own digital identity without depending on a specific service provider.

Digital identity: The body of information about an individual, organization, or electronic device that exists online, including search history and user names.

Federated identity management: Allows authorized users to access multiple applications and domains with a single set of credentials like when people can use their Google or Facebook to sign into websites or apps.

Holder: A user who creates their decentralized identifier with a digital wallet app and receives the Verifiable Credential.

Issuer: The organization that signs a Verifiable Credential with their private key and issues it to the holder.

Private key: Made up of a long string of letters and numbers that allows people to prove ownership, give consent to share selected data, and sign documents. It is used to both encrypt and decrypt the data. As an analogy, a private key is like a master key that can access all of your information and the owner should never share their private key with anyone.

Public key: Made up of a long string of letters and numbers that can safely be shared with anyone you choose to give specific information to.

Self-Sovereign Identity (SSI): A model that gives individuals full ownership and control of their digital identities without relying on a third party. This term is often used interchangeably with the term “decentralized identity.”

Verifiable Credentials (VCs): Digital cryptographically-secure versions of both paper and digital credentials that people can present to organizations that need them for verification.

Verifier: A party that checks the credentials and can read the issuer’s public DID on the blockchain to verify if the Verifiable

Credential the holder shared was signed by the issuer's DID.

Conclusion

Decentralized identity is a type of identity management that allows people to own, and control their own digital identity without depending on a specific service provider. Decentralized identity technology is solving many of the problems resulting from centralized and federated identity management systems, including widespread certificate fraud, slow and expensive verification processes, and risks of data breaches.

Decentralized Technology Benefits

Industry	Traditional Process	Problems/Risks	Verifiable Credentials Solution
Supply chain	Relies on physical IDs and documents to demonstrate compliance, which creates inefficiencies.	Documents can be easily forged and difficult to authenticate. Manual verification process is slow and prone to errors. An importer can bring unapproved, non-compliant medical supplies into a market putting public health at risk.	Verifiable Credentials can't be forged and they can be verified within seconds without contacting the issuing party, saving a tremendous amount of time and money.
Finance	To access financial	Individuals have no control over	The data provided in the

Industry	Traditional Process	Problems/Risks	Verifiable Credentials Solution
	services, someone has to go through compliance screening by submitting personal details in physical form that is stored in a large database and shared with one or more third parties that conduct know your customer (KYC) and credit checks.	how their data is secured, shared, and accessed by third parties.	credentials is cryptographically secured, tamper-proof, and can be verified.
Healthcare	Employers use manual processes to verify paper-based licenses and certificates for healthcare providers.	Traditional verification takes weeks if not months, which creates delays in filling much-needed health care roles.	Organizations that provide and regulate medical licenses for the healthcare workforce can issue licenses in the form of digital credentials. The recipients of these licenses can then easily share them for instant verification by any hospital, clinic, or medical department where they would like to work.

Learn More

- How to Prevent Supply Chain Fraud
- Blockchain and Health Care: BurstIQ Use Cases
- Verifiable Credentials
- Decentralized Identifiers (DIDs)
- Blockchain Identity Management
- Data Compliance
- Digital Credentials

About Dock

Dock is a Verifiable Credentials company that provides Dock Certs, a user-friendly, no-code platform, and developer solutions that enable organizations to issue, manage and verify fraud-proof credentials efficiently and securely. Dock enables organizations and individuals to create and share verified data.

Share

Start issuing Verifiable Credentials today

Dock Certs is an all-in-one suite of Verifiable Credential (VC) tools built for organizations to issue digital credentials and certificates that are automatically and instantly verifiable, fraud-proof and auditable.

Schedule a demo

Sign up for free

"We've looked at a lot of the systems that allow you to issue DIDs and VCs and generally what we've found is that Dock is far easier to use than many of the existing tools out there. It can deploy very quickly and it will be very easy for our developers to use the tool."

Amber Hartley

Chief Strategy Officer, BurstIQ

Ready to get started?

Sign up for Dock Certs

Contact us

Company

About us

Roadmap

Brand Assets

Pricing

Contact us

Talk to sales

Solutions

Certs

Web3 ID

Wallet

Token

DOCK token

Get Started Guide

Community

Explorer

Governance

Validators

Developers

Docs

Github

Grants Program

API Documentation

Mobile Wallet SDK

Status

Industries

Healthcare

Supply Chain

Workforce

Finance

Education

Identity and Access Management

Metaverse

Resources

Blog

Roadmap

Videos

Technology

Terms

Privacy

Copyright © 2023 Dock Labs AG