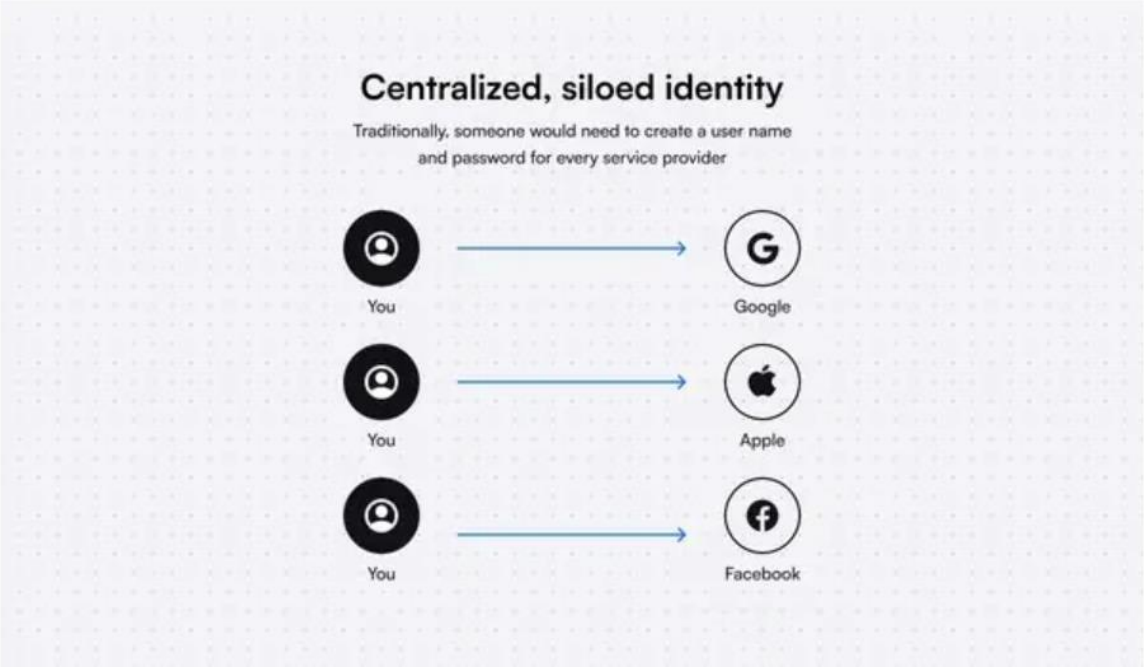
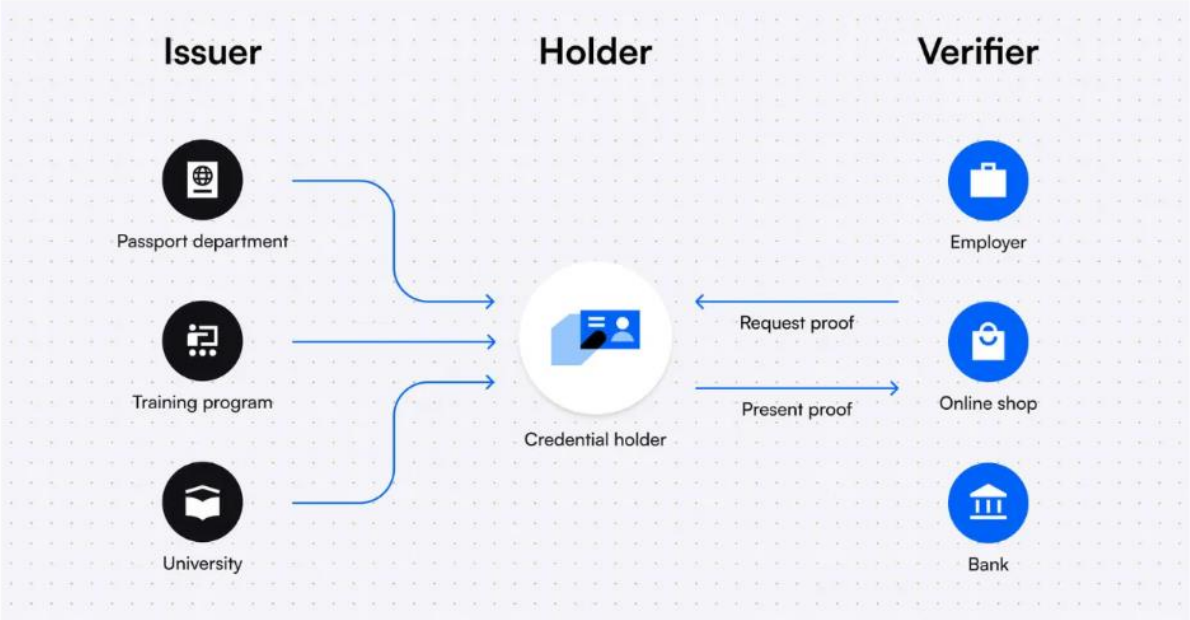
Decentralized identity is a type of identity management that helps issuing organizations create fraud-proof credentials and empowers verifying organizations to instantly check the authenticity of those credentials. Individuals fully own and control their digital identity and credentials without relying on any third party to prove their claims.

A decentralized identity system is made up of 3 pillars: blockchain, Verifiable Credentials (VCs), and decentralized identifiers (DIDs).





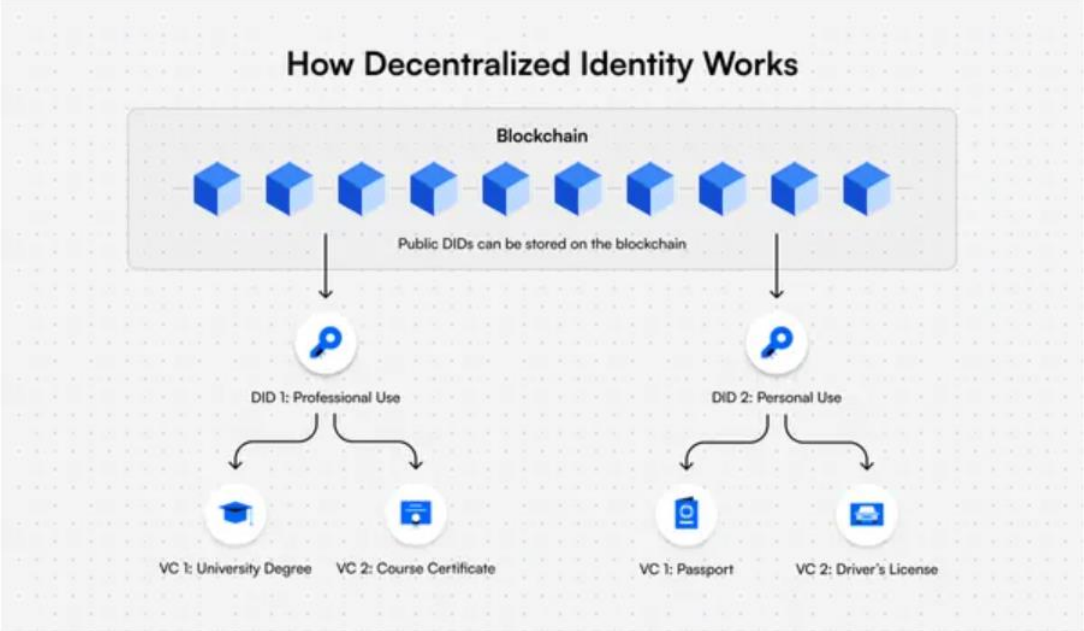
Decentralized identity is a type of identity management that allows people to control their own digital identity without depending on a specific service provider.

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

Why Is Decentralized Identity Important ?

- **Allows organizations to verify information in seconds**
- **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
- People 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

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.

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
Data is owned and controlled by organizations, apps, and services	Data is fully owned and controlled by the user