Decentralized Identity: The future of digital Identity management

Okta

September 28, 2024

Decentralized Identity is a methodology that allows individuals to securely control their digital Identity without relying on a central authority.

The need for decentralized Identity

Traditional Identity models do not protect user interests and can leave personal information vulnerable. Decentralized Identity helps close the gap on a growing list of digital Identity concerns:

- **Data breaches:** Organizations often collect sensitive personal data for authentication in a centralized location, exposing users to increasing risks from frequent and sophisticated data breaches.

their Identity, leaving them unable to participate fully in essential services and technological advancements.

- **Increasing regulatory pressure:** Stringent data protection laws like GDPR and CCP have further highlighted the need for more privacy-centric Identity solutions.

How decentralized Identity works

Decentralized Identity (DCI) allows individuals to verify and manage their digital identities and protect their personally identifiable information (PII).

Core components:

- **Credentials:** Information that uniquely identifies and describes an individual or entity
- **Digital wallets:** Secure software repositories where users store and manage their credentials and identifiers
- **Issuers:** Trusted entities that create and provide verifiable credentials to users, similar to an Identity or OpenID provider
- **Verifiers**: Parties that authenticate the validity of presented credentials
- **Blockchain or distributed ledger technology:** Decentralized, tamper-resistant systems that underpin many decentralized Identity solutions
- **Decentralized identifiers (DIDs):** Unique, user-controlled identifiers for verifiable, decentralized digital Identity management
- **Verifiable credentials (VCs):** Cryptographically secure digital credentials

Like with any Identity and access management (IAM) structure, these

1. Users (or *holders)* receive credentials from various issuers (e.g., government, educational institutions, employers)
2. A secure digital wallet stores the credentials
3. Users present their credentials to verifiers who need to confirm the user's claims or attributes
4. Verification occurs through blockchain-based ledgers or other decentralized systems
5. Cryptographic proofs ensure the authenticity and integrity of credentials without revealing unnecessary information

Blockchain's role in decentralized Identity

How blockchain technology functions in many decentralized Identity systems:

- **Immutability:** Blockchain provides an unalterable record of transactions and Identity-related data
- **Decentralization:** It eliminates the need for a central authority to manage identities
- **Privacy:** Zero-knowledge proofs and other cryptographic methods enable selective disclosure of information
- **Interoperability:** Blockchain can serve as a common infrastructure for different Identity systems to interact

How decentralization democratizes data and access

People typically need documented proof of existence to engage in financial,

Removing the barriers to access

Decentralized Identity systems significantly ease users' access to information. Online, blockchain-based cryptography systems enable anyone to establish digital wallets and access their digital Identity. Individuals need only an **internet connection** and a **smart device** to participate, tools becoming increasingly common in emerging economies as we bridge the digital divide. Decentralization projects offer a promising philanthropic approach to providing widespread digital identities and service access.

Enhancing user independence

User autonomy is another area where decentralized Identity promotes democratization. When registering for new online services, users traditionally have to provide an array of personal data, which organizations may process, share, or sell to third parties. In a decentralized system, users instead receive DIDs to verify their identities with each service provider. Users secure these credentials via private encryption, known only to themselves, and can verify them with each service provider.

This model accomplishes two things:

- It lets users share only the information that's relevant and necessary to access each service
- It helps to ensure that organizations can access a person's data only for authentication.

By default, users have access to a greater degree of privacy and control over their data.

Here's an example:

1. Jane has just migrated to the U.S. without a physical copy of her university diploma. She needs to prove her field of study to receive a confirmed job offer.

Benefits of decentralized Identity

Decentralized Identity restructures how data is stored and secured to the advantage of users, organizations, and developers.

Benefits to users:

- **Secure credential storage:** Digital wallets are a protected repository using encryption and biometrics.
- **Enhanced privacy:** The system requests informed consent for credential sharing and conceals metadata to prevent tracking.
- **Improved security:** Encrypted, decentralized storage systems like blockchain reduce the risk of unauthorized access and data theft.
- **Greater control:** Users manage their identities and decide what information to share and who they share it with.

Benefits to organizations:

- **Reduced liability:** Collecting and storing less data minimizes the risk of regulatory violations and cyberattacks.
- **Simplified compliance:** Organizations face fewer regulatory hurdles with reduced data storage responsibilities.
- **Increased trust:** Requesting only necessary credentials and obtaining user consent fosters transparency with users.
- **Enhanced security:** Decentralized systems reduce the risk of large-scale data breaches.

Benefits to developers:

- **Improved app design:** Decentralized Identity enables the creation of more user-friendly applications.

across different platforms and services.

Centralized vs. decentralized Identity management

Centralized Identity:

Centralized digital Identity management relies on storing and controlling user data in one environment.

In this model:

- Organizations collect and manage various data attributes that form a user's digital Identity, such as date of birth, social security numbers, usernames, and passwords.
- IAM systems encompass policies, services, and technologies that allow organizations to verify user identities and manage access levels.
- Users typically have limited control over storing, using, or sharing personal data.

Decentralized Identity:

In contrast, decentralized Identity shifts control to individuals.

Features include:

- Users control which data they share with organizations and can revoke access.
- Digital wallets store Identity and credential information that certified issuers

Authentication	Single Sign-On (SSO) for all applications	Separate aut
Environment	All IAM happens in one environment	IAM is sprea
Control	Consolidated control	Distributed c
Point of Failure	Potential single point of failure	No single poi
User Experience	Simpler user experience	More comple
Data Storage	Data stored in a central location	Data distribu
Privacy	Less user control over data	More user co
Security Risk	Higher risk of large-scale data breaches	Lower risk of

Addressing the risks of centralized and federated digital Identity systems

Federated Identity links a user's Identity across Identity management systems, providing convenience and security.

However, federated and centralized digital Identity systems can introduce vulnerabilities, including:

- Single points of failure that can compromise large amounts of personal data
- Potential for unauthorized access and misuse of personal information
- Lack of user control over how personal data is stored and shared

Decentralized Identity systems address these issues. By reducing reliance on central authorities, decentralized systems mitigate many risks associated with traditional Identity management approaches.

Identity (SSI) have subtle differences. SSI emphasizes the individual's absolute control over their Identity, while decentralized Identity focuses on the distributed nature of the Identity infrastructure. Both concepts share foundational elements but differ in their approach to controlling and managing Identity information.

Decentralized Identity use cases

Decentralized Identity has the potential to enhance privacy, security, and user control across many industries. These include:

E-commerce and retail

- Passwordless logins for online shopping
- Age verification for restricted products
- Loyalty programs with enhanced privacy

Education

- Verifiable digital diplomas and certificates
- Lifelong learning records
- Simplified student transfers between institutions

Finance

- Streamlined Know Your Customer (KYC) processes
- Simplified cross-border transactions
- Enhanced fraud prevention in digital banking

Government services

- Secure sharing of medical records between providers
- Patient-controlled health data management
- Streamlined insurance claims processing

Internet of Things (IoT):

- Identity management for connected devices
- Secure machine-to-machine communications
- Privacy-preserving smart home systems

Travel and hospitality:

- Seamless airport check-ins and border controls
- Contactless hotel check-ins
- Secure sharing of travel documents

Workforce management:

- Decentralized employee credentials
- Simplified background checks
- Secure access control for physical and digital assets

Current challenges and developments in decentralized Identity

users

- **Interoperability:** Ongoing work on standards like W3C's DIDs and VCs to ensure cross-platform compatibility

The future of decentralized Identity

Identity is at the core of how decentralized architectures will develop. It is increasingly important as a defense against AI-enabled cyberattacks and Identity fraud.

According to a recent survey in Security Magazine, more organizations are implementing **decentralized Identity strategies**, with a 13% increase from the previous year.

Organizations shaping decentralized Identity

While decentralized Identity is still evolving, some world-leading organizations have proven its potential to increase trust and democratization.

In the background, numerous organizations are working to standardize and structure decentralized Identity. Key players include:

- **Decentralized Identity Foundation (DIF):** DIF is the hub for all development, discussion, and management of initiatives to create an open, standards-based decentralized Identity ecosystem.

- **Hyperledger:** The Linux Foundation's Hyperledger community develops frameworks, tools, and libraries for deploying decentralized ledgers and blockchains.

FAQ:

Q: What is a decentralized identifier?

A: As outlined by the **W3C**, DIDs are identifiers that facilitate verifiable, decentralized digital identities. The term signifies any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID.

Q: What is decentralized Identity in blockchain?

A: In blockchain systems, decentralization shifts power away from single points of authority. Instead of relying on a central entity to make decisions and manage operations, decentralized systems distribute these responsibilities across a network of participants. This approach spreads control and decision-making authority among many nodes.

Q: What is an example of a centralized Identity?

A: A typical example of a centralized Identity system is an organization's internal network or employee management system. These systems rely on a central database to store all employee Identity information.

In this scenario, employees typically use a single set of credentials to access various company resources and applications. The IT department manages the system, handling tasks from account creation to deprovisioning.

okta

Elevate customer Identity protection with Okta

Learn how Okta **Customer Identity** solutions can safeguard every click, empower your teams, and grow your organization

Tags

decentralized identity, self-sovereign identity, IAM, Workforce

By **Sean Frazier**
Four days before the second inauguration of President Donald Trump, his predecessor President Joe Biden issued an executive order that aimed to create a...

Read now

Company

About Us

Our Customers

Leadership

Investors

Careers

Events

Press Room

Partners

Responsibility

Okta for Good

Diversity, Inclusion & Belonging

Customer Identity Cloud

Workforce Identity Cloud

Free Trial

Pricing

Contact Sales

Trust

Accessibility

Help & Support

Help and Support

Frequently Asked Questions

Contact Us

Customer Identity Cloud Status

Workforce Identity Cloud Status

To connect with a product expert today,
use our chat box, email us, or call
+1-800-425-1267.

okta

Legal Privacy Policy Site Terms Security Sitemap Cookies Settings

Your Privacy Choices ✓✕

United States