

The Road to Decentralized Identity: The Techniques, Promises, and Challenges of Tomorrow's Digital Identity

Mark Campbell , EVOTEK

As society increasingly relies on digital services, identity management becomes increasingly vital. Decentralized identity offers a novel approach to address today's identity challenges, putting users in control of their own digital identities and personal data.

Digital Object Identifier 10.1109/MC.2023.3263020
Date of current version: 31 May 2023

As society increasingly relies on digital services, secure and reliable identity management becomes increasingly vital. Traditional centralized identity (CID) systems have been plagued by data breaches, identity theft and loosely controlled usage of users' personal information. Decentralized identity (DID) offers a novel approach to address these challenges by putting users in control of their own digital identities.

DIGITAL SERVICES AND DIGITAL IDENTITY

Online transactions via digital services have become ubiquitous and virtually invisible in today's online world, at least until they fail or are misused by bad actors. To securely complete a digital transaction, a user (that is, a person, system, application, or device) and the service provider must complete an intricate handshake to verify user identity and digital service permission.



At the core of this interaction is the digital identity, which ideally must be¹:

- › **Convenient:** It must be easy to use, easy to remember, portable between devices, and frictionless to the user.
- › **Private:** Identity information must be kept private from parties outside the transaction.
- › **Secure:** Identity verification must be secure from eavesdropping, breaches, spoofing, and unauthorized replication, and leave no transaction traces for bad actors to exploit.
- › **Scalable:** Identity verification must be fast and highly scalable.

A digital identity can be verified by something we²:

- › know (for example, password, mother's maiden name)
- › have (for example, physical key, mobile device)
- › are (for example, our fingerprint, other biometrics)
- › are temporarily granted (for example, expiring one-time passcode).

The username-password model is today's most common identity verification technique, but it's often augmented with other technologies, such as single sign on (SSO), one-time passcode, multifactor authentication, and passwordless techniques, to reduce user friction and increase security.

CID

Today's standard form of identity management is CID, in which digital services are controlled by a single central service provider platform. A user registers their identity (for example, username) and proof (for example, password) with the service provider, who maps them to the services they are allowed to execute.³ When a user application requests a

service from the service provider, they assert their digital identity and provide proof of this assertion. The service provider authenticates the identity with the proof and verifies if the requested service use is authorized. If so, the service provider executes the service and provides the results back to the user application (Figure 1).

CID frameworks have existed since the early days of digital computation but have evolved over the decades.

Federated identity

Multiple service providers can form a "federation" of trust by linking their authentication systems to allow users to access multiple services with a single set of login credentials, thus eliminating multiple usernames and passwords.¹ This "federated identity" is often built on a hub-and-spoke model with a central identity hub (for example, Google, Meta, Microsoft) responsible for identity authentication, and other "spoke" federation members maintaining their own authorization maps. A big advantage is that new federation members need only plug into the existing hub via a published application programming interface (API) to join a federation.⁴

Passkeys

A "passkey" system, formally called a *fast identity online* or *FIDO* multidevice credential and built on the FIDO2 *webauthn* standard, is a cryptographic entity—invisible to the user—and used in place of a password.⁵ A passkey uses a public key registered with the service provider and a private key held only by the user. Using industry-standard public key infrastructure (PKI), users get a seamless identity verification process on multiple devices much more securely than traditional passwords. Passkeys can be stored and verified by a central federated identity hub like those hosted by Apple, Google, and Microsoft.⁶

ID as a service

An ID as a service (IDaaS) has a central identity server manage and verify identities of subscribing service providers. IDaaS solutions are commonly hosted as a multitenant framework in a public cloud.

A CID example: India's unified payments interface

Launched in 2016, India's unified payments interface (UPI) merges traditional payment applications and paper

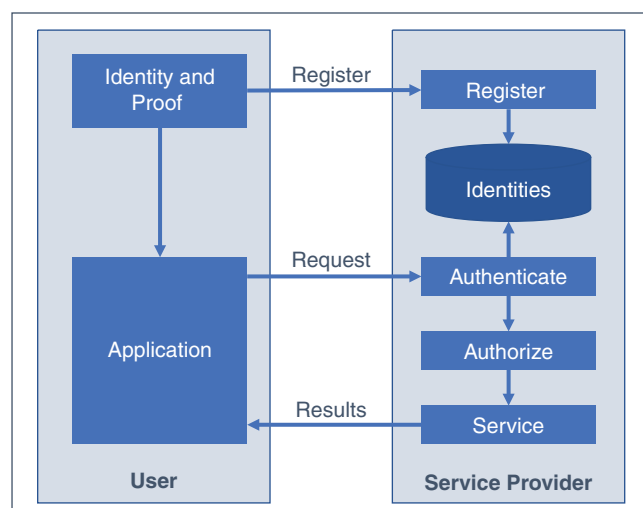


FIGURE 1. CID

processes into a single platform. The UPI system integrates banks, payment systems, and merchants, allowing users to access a wide range of payment services with a single interface. Easy integrating with UPI has spurred 50% digital payment volume growth per year for the past 5 years.⁷ UPI is based on a collection of uniquely Indian innovations, including:

- › *The India Stack*: This is a collection of open APIs allowing institutions to integrate with UPI systems.
- › *No-frills accounts*: Introduced in 2005 by the Reserve Bank of India, these basic bank accounts charge no fees for most transactions and require no minimum balance, thereby granting financial access to low-income populations.⁸
- › *Aadhaar*: Hindi for *foundation*, Aadhaar is a free unique 12-digit random number issued by the Unique Identification Authority of India. Residents need only minimal demographic and biometric information to receive their Aadhaar, which, once coupled with their bank, enables payment transactions anywhere from stock markets to street stalls.^{1,9}

Rapid growth of the UPI system has raised concerns about security, privacy,

and fraud, with reports of phishing attacks, unauthorized transactions, and data breaches.¹⁰

CID shortcomings

While CID solutions have been deployed for decades and handle nearly all current digital transactions, they have several inherent shortcomings:

- › *Trust and data breaches*: Users must trust the central service provider's availability, integrity, and confidential treatment of personal information.³ Unfortunately, most CID platforms (for example, Facebook, Google) have been victims of serious data breaches, rendering their best security intentions moot.¹¹
- › *Privacy and fraud*: CID approaches require users to surrender aspects of their privacy.¹¹ Should this information be divulged through a data breach, internal bad actor, or accidental disclosure, the user's privacy is forfeit. On the user side, credentials can be stolen, replicated, or phished by fraudsters.
- › *Convenience*: CID systems require users to authenticate identity for each accessed service provider. While passkeys, federation, and SSO solutions ease user friction,

multiple identity credential must be created and remembered for each identity federation accessed.¹²

Passkeys, federated identity, IDaaS, passwordless, and SSO techniques are continually advancing to ensure the longevity of CID solutions. However, CIDs' shortcomings have prompted many to seek alternative DID platforms.

DID

DID is a user-centric identity management approach where individuals control their identity data and disclose only select information to specific service providers. The user registers personal information (for example, name, age, credit card number) along with proof (for example, private key) with an independent issuer. The issuer records this personal information in a distributed ledger (for example, blockchain) and returns a signed credential to the user to store in a digital wallet. When the user's application requests a service from the service provider, it passes the appropriate signed credential for only the identity items the service requires (for example, credit card number but not age). The service provider then verifies the credential with the distributed ledger, verifies the identity is authorized to use the service, and returns service results to the user (Figure 2).

Two central components of DID are the *digital wallet* and *distributed ledger*. The digital wallet stores user information (for example, name, age, address, citizenship, credit card number) in an unphishable cryptographic credential created and signed by the issuer.¹² The distributed ledger is most commonly built on blockchain, but increasingly other frameworks, like distributed file systems and hashgraphs. Emerging distributed ledger technology (DLT) solutions include Microsoft ION, Hyperledger Indy, and the Tangle Identity framework.³ Today's thriving DID community includes Bitnation, Civic, EverID, IDchainZ, LifeID, SelfKey, ShoCard, Sovrin, THEKey, and uPort.¹³

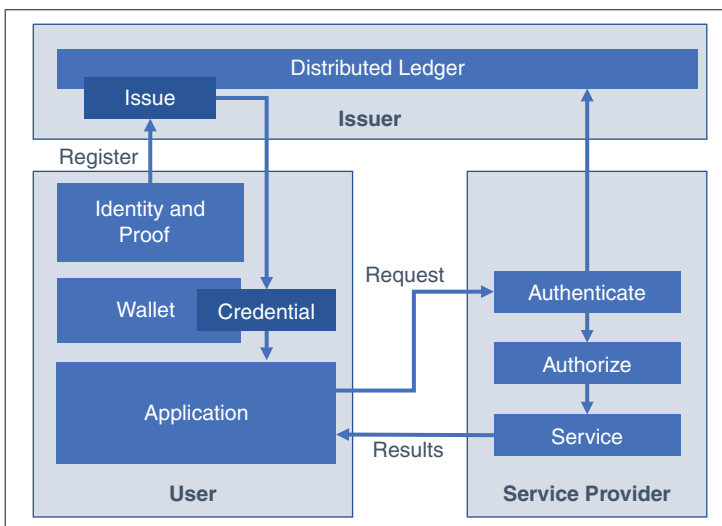


FIGURE 2. DID

Several international organizations, such as the World Wide Web Consortium, Decentralized Identity Foundation, and European Digital Identity are striving to establish a new DID ecosystem through published standards and frameworks.³

Self-sovereign identity (SSI) is often used in connection with DID. Each describes similar but not equivalent identity perspectives. DID details identity management without relying on a centralized verification authority,¹⁴ while SSI focuses on users retaining control over their identity and digital footprint, with or without DID.

DID benefits

DID can overcome major shortcomings of CID, such as:

- › *Trust and data breaches:* DID eliminates the single point of compromise found in CID's central or federated service provider.³ Should a DID service provider be breached, little to no personally identifiable data can be exploited. A growing number of users trust global distributed ledgers more than a service provider's assurance that proper security is in place.
- › *Privacy and fraud:* Because only pertinent identity items are used for each transaction, user data privacy is more easily controlled and secured. With total control of their identity items, users can grant or revoke access to service providers as needed and minimize identity theft.
- › *Convenience:* A user only registers identity items once, then grants access to service providers as needed, eliminating multiple identity registrations, usernames, and passwords.

DID challenges

Despite the technical solutions and promising characteristics of DID, widespread adoption faces significant challenges:

- › *Interoperability:* The DID ecosystem is built on a common issuer

and secure digital wallet. Today's proliferation of DID frameworks makes integration by service providers an arduous task.¹² In the coming years, consortiums and standards will coalesce into a common DID ecosystem much like India's UPI in the CID space.

- › *Scalability:* Supporting a global population of identity credentials, service requests, and verifications requires a gargantuan underlying DLT. It's not certain if current DLT technologies can achieve this scale performantly and cost effectively.¹³
- › *Governance:* Identity governance programs, like the European Union's General Data Protection Regulation (GDPR) are built on CID assumptions. DID will require many regulations be overhauled. For instance, GDPR regulates the user's "right to be forgotten," mandating service providers delete user data and identity on request. This is simply not possible or applicable to service providers in a DID regime.²
- › *Service provider resistance:* Today's global service providers (for example, Meta, Google, Amazon, Microsoft) operate platforms dependent on direct user data or indirect user behavior. DID removes this asymmetric control and greatly restricts user data monetization, making global services providers resistive towards DID.

Like any disruptive technology, there is initial resistance to change. There will undoubtedly be security vulnerabilities, performance bottlenecks, scaling issues, fear, uncertainty, and doubt encountered with DID adoption. However, user benefits, technical advancement, deployment framework maturation, and societal pressure will make DID more palatable.

TOMORROW'S DIGITAL IDENTITY

Traditional CID remains the default identity approach and newer CID techniques,


like passkeys, will continue to develop. However, DID and SSI solutions will soon mature, proliferate, and become the standard identity framework.

Beyond adopting DID platforms, other techniques and features will be developed to augment digital identity, including:

- › *Zero-knowledge proofs (ZKP):* This cryptographic technique proves digital identity without the user revealing private information. When coupled with a DID approach, ZKP offers a novel alternative to passwords and maintains user control over private data.¹⁵ Initial use cases are being explored in finance, health care, commerce, education, smart city, and travel industries.¹
- › *Nonrepudiation:* This technique encrypts a transaction so neither the sender nor recipient of a message can deny its creation, transmission, or receipt. However, in practice, nonrepudiation is left up to the DLT used by the issuer. DID implementations will increasingly build nonrepudiation into their digital transaction lifecycle.
- › *Fault tolerance:* It's difficult for today's DID solutions to recover from breakdowns in the middle of a transaction. Future frameworks will be more resistant to mid-transaction failures and automate the continuation, reconstruction, or rollback of transactions interrupted in flight.
- › *Multisource identity:* Future identity systems will incorporate multiple indirect user sources (for example, cell phone mast data, behavior patterns, digital idiosyncrasies) to more accurately verify identity and lower user friction.²
- › *Quantum safe:* Today's DID platforms are built on PKI. However, quantum computing advancements could render PKI-based solutions readily

transparent to decryption. Other encryption techniques—like lattice-based encryption, code-based encryption, multivariate polynomial cryptography, and hash-based signatures—are much more resistant to quantum computing.¹⁶ These “postquantum” or “quantum-safe” techniques will replace PKI in DID solutions.

- **Regulations and governance:** Regulations lag greatly compared to technical advancements, but DID and SSI techniques will require governance bodies to rethink and redraft policies and regulations.

DID solutions can fundamentally transform how users interact with digital services. By offering enhanced security, privacy preservation, and self-sovereignty, DIDs can address many limitations inherent in traditional centralized identity systems. As DID technology matures and gains wider acceptance, it will have far-reaching implications across industries as it streamlines processes, increases security, and improves trust. 

REFERENCES

1. M. Bajaj, private communications, Jan. 19, 2023.
2. M. Kennedy, private communications, Jan. 19, 2023.
3. Š. Čučko and M. Turkanović, “Decentralized and self-sovereign identity: Systematic mapping study,” *IEEE Access*, vol. 9, pp. 139,009–139,027, Oct. 2021, doi: 10.1109/ACCESS.2021.3117588 [Online]. Available: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9558805>
4. R. Broeckelmann, “Authentication vs. Federation vs. SSO,” *Medium*, Sep. 2017. [Online]. Available: <https://medium.com/@robert.broeckelmann/authentication-vs-federation-vs-ss-9586b06b1380>
5. V. Bertocci, “Our take on passkeys,” Auth0. Accessed: Mar. 16, 2023. [Online]. Available: <https://auth0.com/blog/our-take-on-passkeys/>
6. B. Collins, “Why passkeys from Apple, Google, Microsoft may soon replace your passwords,” *CNBC*, Feb. 2023. [Online]. Available: <https://www.cnb.com/2023/02/11/why-apple-google-microsoft-passkey-should-replace-your-own-password.html>
7. J. Kearns and A. Mathew, “Explained: How India is outpacing the world in digital payments,” *Int. Monetary Fund*, Oct. 2022. [Online]. Available: <https://www.imf.org/en/News/Articles/2022/10/26/cf-how-indias-central-bank-helped-spur-a-digital-payments-boom>
8. “What is no-frills account – Its eligibility, documents required and how to apply,” Navi. Accessed: Mar. 16, 2023. [Online]. Available: <https://navi.com/blog/no-frills-account/#:~:text=No%20Frills%20Account%20is%20a,who%20have%20low%20income%20backgrounds>
9. “About your Aadhaar,” Government of India. Accessed: Mar. 16, 2023. [Online]. Available: <https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar.html>
10. A. Mukherjee, “A little epoxy can unglue India’s welfare system,” *Bloomberg*, Jun. 2022. [Online]. Available: https://www.bloomberg.com/opinion/articles/2022-06-23/india-s-aadhaar-id-system-delivers-benefits-but-is-at-risk-of-widespread-fraud?lead_source=verify%20wall
11. C. Schram, “A future built on decentralized identity,” *Bloom*, Dec. 2021. [Online]. Available: <https://bloom.co/blog/a-future-built-on-decentralized-identity/>
12. D. Shou, “How decentralized identity is reshaping privacy for digital identities,” *Forbes*, Dec. 2021. [Online]. Available: <https://www.forbes.com/sites/forbestechcouncil/2021/12/10/how-decentralized-identity-is-reshaping-privacy-for-digital-identities/?sh=2893b82c3226>
13. O. Dib and K. Toumi, “Decentralized identity systems: Architecture, challenges, solutions and future directions,” *Ann. Emerg. Technol. Comput.*, vol. 4, no. 5, pp. 19–40, Dec. 2020, doi: 10.33166/AETiC.2020.05.002. [Online]. Available: https://www.researchgate.net/publication/347753956_Decentralized_Identity_Systems_Architecture_Challenges_Solutions_and_Future_Directions
14. G. Weston, “Self sovereign identity & decentralized identity – An unlimited guide,” *101 Blockchains*, Jul. 2022. [Online]. Available: <https://101blockchains.com/self-sovereign-identity-and-decentralized-identity/>
15. “Zero knowledge identity proof,” Identity Management Institute, Chatsworth, CA, USA, 2023. [Online]. Available: <https://identitymanagementinstitute.org/zero-knowledge-identity-proof/>
16. “Quantum computing and post-quantum cryptography,” National Security Agency, Washington, DC, USA, Aug. 2021. [Online]. Available: https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF
17. A. Sidana, private communications, Jan. 17, 2023.
18. C. Hughes, “IDaaS explained: How it compares to IAM,” *CSO*, May 2022. [Online]. Available: <https://www.csoonline.com/article/3660554/idaas-explained-how-it-compares-to-iam.html>
19. J. S. Savariraj and S. De Simone, “An introduction to post-quantum public key cryptography,” *InfoQ*, Feb. 2022. [Online]. Available: <https://www.infoq.com/articles/post-quantum-cryptography-introduction/>

MARK CAMPBELL is the chief innovation officer at EVOTEK, San Diego, CA 92121 USA. Contact him at mark@evotek.com.