coinbase INSTITUTE

INSIGHTS

The Future of Digital Identity: The Role of Decentralised ID in the UK

Decentralised Identity represents a model for identity management in which individuals, rather than central authorities or major platforms, control their verified credentials. Enabled by cryptographic proofs and decentralised ledgers, decentralised ID (DID) promises increased privacy, portability, and security while reducing dependence on large data-holding intermediaries. While there is well-founded, broader political debate on the merits and challenges of introducing a digital ID system, if the UK Government chooses to pursue digital ID, blockchain technology can address the challenges raised and should be considered as part of the design. **As part of the Government's upcoming consultation on the delivery of digital ID, it should consider decentralised technology (i.e., blockchain) to address the range of privacy, security, single point of failure, and other legitimate concerns raised by digital ID.**

Privacy and Control: Users store credentials in their own digital wallets and decide exactly what information to share and when. Personal data never sits in third-party databases, eliminating the potential for unauthorized access by intermediaries.

Interoperable: Standardized blockchain credentials work across borders, platforms, and service providers without creating vendor lock-in. One verified identity replaces countless siloed accounts, enabling seamless access to banking, healthcare, and government services.

Data Security: Decentralized storage eliminates centralized "honeypots" that attract hackers, while blockchain encryption makes credentials tamper-resistant. Identity theft payoff plummets when personal data isn't aggregated in vulnerable corporate databases.

Trust: Verification happens through cryptographic proof on public blockchains rather than faith in institutions. Users can instantly verify credentials without relying on potentially compromised central authorities.

Consent: Every data-sharing transaction requires explicit user approval through their digital wallet, creating a transparent audit trail. Unlike traditional systems where consent is buried in terms of service, blockchain-based consent is cryptographically recorded and revocable.

History of Identification and the Rise of Digital ID

Forms of identification have evolved over time, from official papers verified by watermarks to personal ID numbers and photo identification. With the advent of the internet in the 1990s came the rise of digital IDs. These IDs are often in the form of a username and password that provide entry to a particular website, thus granting access to critical information like your bank account or healthcare information. Digital IDs can also be used offline, such as in the form of a digital driver's license.

Digital IDs are convenient because they can be authenticated online, and therefore make it possible to access services remotely. But simply digitizing a business process or physical ID does little to improve user privacy or security, and in many instances introduces additional risks from hacking and cybercrime. This is true whether digital IDs are stored and managed in discrete "silos" by different organizations, or stored and managed by a "federated" cloud service.

Siloed: Under the initial "siloed" digital ID approach, each website or organization issues its own ID to users in the form of username/password combinations. This approach requires users to remember many unique usernames and passwords. It also leads to extensive data duplication across multiple websites and databases, all of which are prime targets for hacking and identity theft.

Federated: In response to shortcomings from the siloed model, organizations developed a "federated" approach, where big tech companies like Google and Facebook issue digital ID credentials that work across a variety of websites and services. This model makes online identity verification more convenient. But it puts even more personal data in the hands of central authorities that operate the federated entry point, raising additional concerns about privacy and security.

Services that issue a federated digital ID can compromise privacy through their need to collect, store, and share large amounts of user data. Some data is collected directly from the user, like name, birthdate, address, and sensitive answers to security questions. Other information, like geolocation data and browsing history, is tracked and collected by the organization, often without the user's knowledge. All of this data is ultimately stored and replicated hundreds of times in different databases, one for each website or service where a user has registered. Even more, this data can be shared with other companies for profit, without the user's consent.

Both the siloed and federated approaches raise serious security concerns. Storing personal information in countless different silos inherently increases vulnerability to hacking and cybertheft. Different websites have varying password and authentication requirements, and as security and identity protocols change over time, it's nearly impossible to consistently update disparate identity silos in unison, thereby increasing security risks.

Decentralised ID

Decentralised ID offers a new form of identity management that relies on blockchain technology to solve the security, privacy, and consent issues presented by paper and digital IDs. DID gives individuals control over their identity, rather than outsourcing identity management to a single centralized authority like the government or big tech.

DID works by relying on trusted third parties, called "issuers," to verify key identifiers. These issuers could include government agencies, universities, employers, and banks. The process of creating a DID begins when an issuer distributes an identifying credential, such as a digital birth certificate or proof of employment. That credential is stored on a blockchain and the user's digital wallet. When a third party needs to request identifying information, like proof of good credit in the context of making a major purchase, the user presents the credential to the requester by accessing the information stored on the blockchain. This proof can be generated in a number of easily accessible ways, including as a QR code on the user's phone.

Because the credential is stored on the blockchain and the user's wallet, and controlled by the user, there is no need for the government, merchants, employers, or others to keep a record of that credential in their own, siloed databases. There is also no need for tech companies to provide federated login solutions. DID therefore shifts the source and management of verification from centralized institutions to a decentralised ledger, while ensuring that identifying information stays fully within the control of the individual, stored securely on his or her digital wallet.

Key Terms

Blockchain: a software system that records and verifies transactions on a distributed network secured by cryptography. Blockchains operate like an open, append-only ledger, meaning data can only be added, not removed or altered. Transactions on the blockchain are recorded according to a predetermined set of rules known as a "consensus mechanism."

Verifiable credentials: digital credentials that represent physical documents such as a driver's license or passport, or attributes such as ownership of a car or house. They are tamper-resistant and instantaneously verifiable on the blockchain.

Zero-Knowledge Proof: a method by which one party can prove to another that a given statement is true, without needing to convey any additional information.

Potential Benefits of DID

Privacy and Control. Users control their own identifying data because they store it in their own digital wallet. They determine when to share their data and with whom. Consent is never an issue. Further, users can selectively share necessary information without disclosing personal details, and can revoke access to specific data at any time.

Convenience. Individuals can use their standardized credentials for many different transactions without the need for different usernames and passwords. For example, DID can greatly simplify compliance with financial regulations: once Hal is a verified user of one financial institution, he can show proof of that verification to other banks or exchanges. This reduces sign-up times and eliminates data duplication throughout multiple databases.

Portability. Individuals can take their ID and data with them when they move to a new state or switch to a new service provider, whether it be a social media platform, bank, or doctor's office. Because data

is portable, it reduces "lock-in effects,"[1] or the tendency to keep using certain services simply because the website manages your data or controls your login information.

Security. Because DID relies on the encryption of decentralised ledgers, it greatly increases data security. Not only is encryption incredibly resistant to tampering, but identifying information that is easily linked to the individual is no longer stored *en masse* in large databases, reducing the payoff for would-be hackers. DID can also reduce fraud by helping create online communities that are "free of fake accounts." Such communities could require users to verify their identity using a blockchain-based identity system that would reduce the number of bots.

Expanded Access. The World Bank estimates that over one billion people worldwide lack any formal identification, limiting their access to health care, finance, and other key services. In particular, many migrants and refugees lack IDs, which can easily become lost or invalidated in times of war or natural disaster. DID would allow anyone with a phone or access to a computer to provide proof of her name, birthdate, work experience, and more, quickly facilitating access to employment and education.

Institutional Benefits. With DID, entities no longer need to maintain large repositories of login and identifying data; instead, they can access necessary information from a user's wallet and verify it on the blockchain. Many organizations are subject to strict regulations governing the collection and storage of user data. By maintaining less data, they can simplify their compliance responsibilities and lessen their exposure to cyberattacks. Further, the ability to quickly verify credentials can significantly reduce the time and costs of everyday processes like employee onboarding.

DID Today

DID technology is growing rapidly, with public and private innovations poised to integrate DID into our everyday lives. For example, the Ethereum Name Service (ENS) provides the convenience of current cloud-based login services, while letting users retain total control over the information they share with other websites. ENS makes it easy to read and share crypto addresses by mapping an easily recognizable name, such as "hal.eth," onto a machine-readable identifier like an ENS address, which is a 40-character string of numbers and letters. ENS has many potential uses in the onchain economy. For example, start-ups have developed a "sign in with Ethereum'' feature that people can use to access multiple web-based services using their Ethereum wallet address.

Governments are also starting to embrace DID. A project sponsored by the European Commission is developing interoperable DID solutions that would facilitate faster and more reliable security checks for EU citizens.[2] And as part of its national blockchain strategy, India is building a decentralised, digital platform that will host IDs and documents related to education, healthcare, and agriculture.

[1] INATBA Report at 11.
[2] The selective sharing capability of DID is especially useful for federated governments like the EU, United States, and others, where personal information is often stored by multiple countries or states with varying security infrastructures.