

# Digital identity – The big shift



Welcome to the new web. It's not like the old web and it demands a new approach to identity. Data structures and commercial relationships will be markedly different in the Web3 era, requiring verification methods that are more streamlined, secure, and trustworthy to support them.

Existing online identity mechanisms are a poor adaptation of physical ones. All too often, companies use scanned copies of sensitive ID documents such as passports, sent over unsecured channels such as email, which is an inefficient and often times dangerous practice. Documents can be forged, and identity credentials are usually still centrally held and vulnerable to misuse or theft. Stolen identity information litters the dark web.

The time is right for a new type of identification, created with digital channels in mind. Built for Web3, it will be irrefutable, immutable, and controlled entirely by the person that owns it.

We explore the new frontier for digital identity in the first of this article series.



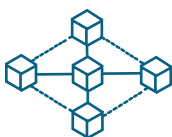
## What is Web3?

Web3 is the latest iteration of a journey that began over 30 years ago when Tim Berners Lee turned on the first web server at [CERN](#). The early days of this environment, which we refer to as Web0, focused on simple information publishing. It needed little, if any, identity verification, relying instead on first-person cookies where it collected data.

Web1 changed everything by introducing e-commerce. Consumers began interacting more with online services in the mid-nineties as sites like the BBC, Wired, and the Economist ventured into this new space. Soon-to-be e-commerce giants like Amazon and eBay emerged around the same time. Password-protected accounts became the prevalent method of authentication.

The rise of social networking and other sites promoting user-generated content in the early 2000s ushered in the era of Web2. This sparked debates over whether people should be forced to use their real IDs versus fake accounts when posting.

At the same time, the continuing digitization of commerce and public services coincided with the rise of mobile computing. Two-factor authentication (2FA) became more prevalent as mobile devices became part of the process, even verifying users by collecting biometrics.



## Enter decentralization

These developmental stages of the web are intertwined, often overlapping each other and sharing one characteristic – relying on centralized services. As they evolved, they eventually held (and often legally owned) all of the users' data, from bank balances to personal pictures. Following the natural aggregation of market share and move to cloud computing, a relatively small number of big tech players control most users' assets and digital identity information.

Web3 will change that relationship, transitioning the creation and storage of assets and identity information to decentralized blockchain models that are often owned and managed by no single entity – the foundation for Web3's big shift.

That transition also changes the model of digital ownership. In Web3, individuals have full ownership and control of their digital creations and assets and the movement of assets is recorded on a blockchain instead of on a central company's servers.

For example, in-game digital assets like avatars or weapons that video game players buy are historically stored as a record in the gaming company's database.

The company controls them and restricts the use of these assets to a single game. Conversely, when a video game player buys those assets as non-fungible tokens (NFTs) on the blockchain, it prevents the gaming company from altering them or revoking ownership. It also gives these assets more utility because they could be used in other games and tradable on third-party platforms.



## How Web3 will change commerce?

Web3 isn't just about video games and digital collectibles. Like the other iterations of the web, it will complement and enhance previous online business models by streamlining them. It has the potential to remove friction for traditional commerce.

For example, blockchain technology could reduce the time required for verification of applicants for mortgages and other loans, which is currently a time-consuming manual process. A Web3-based digital identity system would enable applicants to quickly prove facts about themselves, such as their identity, employment, and income, by allowing a bank and other companies to scan their digital wallet so the applicant can access products and services faster.

This fast verification capability promises to unlock liquidity, save time and cost, and provide faster, more equitable access to public services including healthcare. But for any of that to happen, we must transform traditional concepts of online identity.



## Updating digital identity for Web3

As Web3 decentralizes commerce, identity must also decentralize. Web3 identity credentials will be stored securely on devices owned by users, and records of who signed them will be stored in public data repositories, including blockchains.

These identities will comprise facts about a person such as their name, age, and address, but could also include other information such as music streaming logs, memberships, and credit scores. The owners of that information can use their digital wallets to store their credentials and share them with whomever they choose. Third parties can set up rules for identity criteria based on their requirements.

## This decentralized identity model carries several key advantages:



### Sovereignty



### Security



### Immutable and Irrefutable

## Sovereignty

In a Web3 environment, people control their own identity information. They decide who sees it. They can grant that access at a more granular level, revealing facts about themselves on a need-to-know basis. In the old model, you might have to show your driver's license just to prove your age, giving the attendant at the liquor store or the bouncer at the bar access to your name and address. Decentralized identity aims to solve for this problem.

## Security

When using the old model, you could not be certain how an organization stored your identity credentials or who it shared them with. This led to countless privacy breaches. Decentralization puts you in full control of your identity credentials and makes it accessible on your terms. It also means there are no single points of failure, because instead of allowing third parties to store your data in a centralized server, a third-party would only get access to it for a set period of time.

## Immutable and irrefutable

Encrypted records of digital identity signatures stored on the blockchain make it impractical for a malicious party to tamper with identity information, making it highly trustworthy. A third party will not be able to alter someone's identity signature.

## A long journey ahead

Reimagining both the nature of the web and the concept of digital identity together is a challenging and complex task, involving many stakeholders. It will take some time, but this transition is already underway. Standards for digital identity, such as W3C, are in development and have received strong support from private and public sector institutions alike.

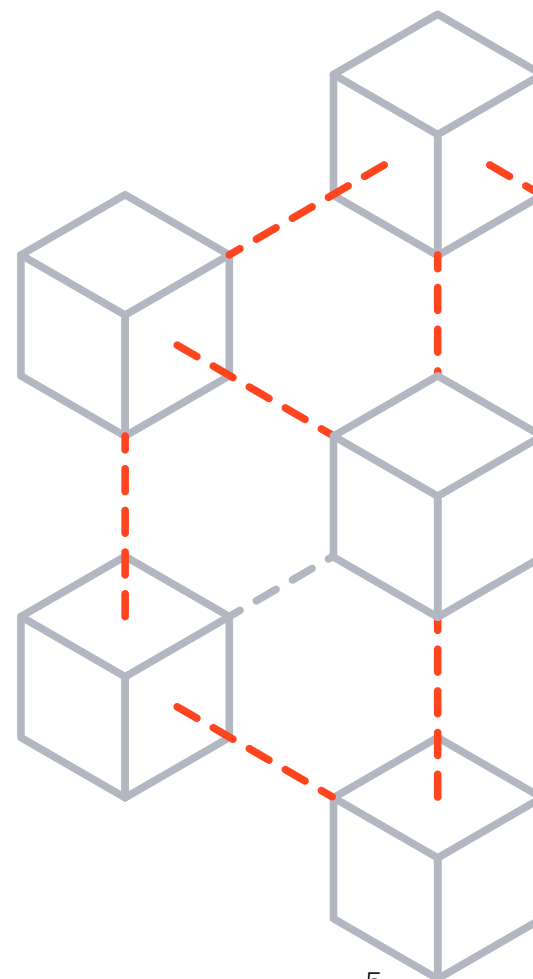
These standards will allow interoperability across a wide range of centralized and decentralized services. This ability to exist in both the old web space and the new one is key. Both usage models must coexist with each other in an environment as large, complex, and diverse as the web.

This article is part of a series on digital identity.

VISIT US AT [JPMORGAN.COM/DIGITAL-IDENTITY](https://jpmorgan.com/digital-identity) →

---

By Tyrone Lobban, Managing Director, Co-head of Kinexys by J.P. Morgan and George Kassis, Vice President, Digital Identity Lead, Kinexys Labs.



The information set forth herein has been obtained or derived from sources believed to be reliable. Neither the authors nor J.P. Morgan makes any representations or warranties as to the information's accuracy or completeness. The information contained herein has been provided solely for informational purposes and does not constitute an offer, solicitation, advice or recommendation, to make any investment decisions or purchase any financial instruments, and may not be construed as such. Offering of any product or service described herein will be subject to completion of development and internal review, as well as obtaining any regulatory approval which may be required. All expressions of opinion in the report are subject to change without notice and reflect the judgment of the authors as of the date of publication. No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof. Similarly, the material contained in this report does not constitute, and should not be relied on as, legal, regulatory, accounting, tax, investment, trading or other advice. Any financial, tax, or legal information contained in this report was so included for informational purposes only. You should consult with their financial adviser, tax adviser or legal counsel, as appropriate. Neither the authors nor J.P. Morgan are responsible for any error, omission or for the interpretation of any law or regulation. The opinions and recommendations herein do not take into account individual circumstances, objectives, or needs and are not intended as recommendations for the sale or purchase of particular securities, financial instruments or strategies. The recipient of this report must make its own independent decisions regarding the information mentioned herein. This report does not bind J.P. Morgan or the authors in any way. Additional disclosures and other information are available at: [www.jpmorgan.com/pages/disclosures](http://www.jpmorgan.com/pages/disclosures).

JPMorgan Chase Bank, N.A. Member FDIC. Deposits held in non-U.S. branches are not FDIC insured.

JPMorgan Chase Bank, N.A., organized under the laws of U.S.A. with limited liability.

© 2022 JPMorgan Chase & Co. All Rights Reserved.