# State of Authentication and Identity in Web3

An insights report by Civic | bd@civic.com

# Table of Contents

# Executive summary

01

The rapid growth of Web3 has generated intense excitement around decentralized applications (dApps) and digital ownership, yet the underlying authentication methods, which are critical to user security and experience, remain limited and often misunderstood. While wallet-based authentication has become the standard in Web3, it comes with a surprising set of challenges that may actually be hindering the decentralized ecosystem's potential to reach mainstream adoption.

This white paper is informed by insights from over 20 in-depth interviews with industry builders and experts, offering a grounded perspective on how authentication and identity systems are evolving to meet the needs of a decentralized world. Through these conversations, a clearer picture has emerged of the current limitations in Web3 authentication, including usability, security, and data management challenges, which alienate non-crypto-native users and stifle broader adoption.

Amid these challenges, the concept of decentralized identity emerges as a transformative approach. By placing control of identity directly in the hands of users, decentralized identity addresses key pain points of traditional systems. Unlike centralized databases, it allows individuals to securely manage and share their credentials through digital wallets, leveraging selective disclosure to protect sensitive information. These capabilities open up new possibilities for creating more user-friendly, privacy-preserving, and secure interactions in Web3.

We explore practical implementations of decentralized identity that enable multi-layered verification, hybrid Web2 and Web3 logins, and privacy-first design to solve today's pressing challenges. Decentralized identifiers (DIDs), combined with technologies like biometrics, passkeys, and non-transferable tokens (SBTs), address critical needs in applications requiring Sybil resistance, such as gaming and DeFi. Furthermore, these systems bridge the gap between Web2 and Web3 by offering familiar onboarding options, such as email or OAuth-compatible authentication.

Through real-world case studies and an analysis of the current limitations of decentralized identity implementation, this paper presents a fresh perspective on Web3's future. By adopting innovative approaches to authentication, developers and businesses can redefine user experience, enhance security, and drive broader engagement within a truly decentralized ecosystem.

# The Current State of Authentication

02

Web3 authentication is currently dominated by **wallet-based solutions**, particularly those that use “WalletConnect-like” methods. By linking cryptocurrency wallets like MetaMask, Coinbase Wallet, Phantom and others, users can interact with dApps without revealing personal information, preserving privacy and aligning with Web3’s decentralization ethos. However, this approach also presents multiple challenges in terms of usability, security, and scalability.

While wallet-based authentication is effective at protecting user privacy, it typically lacks advanced security features like two-factor authentication (2FA) or biometrics checks, which are ways to harden authentication in Web2 applications. This minimalist approach leaves users and platforms vulnerable to unauthorized access and fraud, as there's no verification of the individual behind the wallet. To address the limitations of wallet-based authentication, alternative approaches have emerged in Web3.

**Multi-factor authentication (MFA) and biometric verification** are paving the way for the future of secure digital identity. These technologies add critical layers of protection beyond traditional methods like wallet connections, incorporating advanced features such as biometrics and liveness checks to ensure that each account is tied to a unique human.

This approach is particularly valuable for applications that demand Sybil resistance—ensuring one person corresponds to one wallet—such as gaming and decentralized finance (DeFi). Additionally, interoperability across multiple blockchain ecosystems is becoming a fundamental requirement, and solutions that integrate seamlessly with diverse environments empower developers to build robust, scalable systems. As the need for secure, flexible, and user-friendly identity verification grows, MFA and biometric technologies are shaping the standards for the next generation of decentralized applications.

# Limitations of Current Authentication Methods

Despite advancements in Web3 authentication, several limitations impact both usability and security:

**Complex Wallet Integration**

Wallet integration requires significant development effort to support multiple blockchain networks and wallet types, resulting in inconsistent login experiences across applications. Interoperability across wallet types remains a major challenge for developers, leading to a fragmented user experience.

**Transaction Fees as a Barrier to Entry (i.e. Gas Fees)**

New users coming into blockchain applications have to deal with the fact that their wallets are often empty and each transaction requires a small fee to pay for network costs. This is often an added friction to them adopting the app and engaging with the desired tasks.

**Lack of Advanced Security Features**

Many Web3 platforms rely solely on a wallet connection to create user accounts, bypassing additional security measures like 2FA and biometric verification. This approach sacrifices security by not verifying the individual behind the wallet, leaving users and platforms more vulnerable to unauthorized access and fraud.

**Data Management and Synchronization Challenges**

Web3 applications often use both on- and off-chain data, but synchronizing these identity states is technically challenging.

When identity states (e.g., active or revoked) are not updated consistently, users may encounter issues with data expiration, impacting both security and usability. The solution is storing identity states exclusively on-chain, which eliminates the need for synchronization between on- and off-chain systems. This ensures that updates, such as changes to user status, are accurate and accessible in real-time.

# User Pain Points and Industry Concerns

### User Frustration with Complex Processes

A common pain point is the difficulty of explaining wallets and seed phrases to non-crypto-native users. As one interviewee pointed out:

> "It'd be nice if you could verify the person who brings them in, and then you just log in with Gmail. Almost everything in the world works that way. Instead, I have to explain wallets and seed phrases to people who don't know anything about this stuff—and then they have to verify themselves. It feels like the process should be reversed."

This challenge is not hypothetical—real-world examples prove its impact. When a decentralized finance protocol attempted to introduce wallet-based authentication, it received serious community pushback because of the complexity of the process. Users unfamiliar with wallets found it cumbersome, and the project ultimately removed the feature.

In another case, a decentralized trading platform faced extreme challenges with cross-chain asset swaps due to the complexity of managing identity across multiple chains. Yet, many people unfamiliar with Web3 still use wallets in some form:

### KYC Compliance and Process Simplification

Traditional Know Your Customer (KYC) processes are expensive and time-consuming, requiring repeated verifications with cumbersome manual tasks that discourage users. Reusable KYC solutions simplify this process by allowing users to verify their identity once and reuse it across multiple platforms. This helps Web3 projects comply with regulatory requirements without compromising user experience.

### Interoperability with Web2 Identity Standards

To achieve wider adoption, Web3 must bridge the gap with Web2 identity methods by offering options like email or OAuth authentication methods alongside a cryptocurrency wallet connection. However, relying on existing large-scale providers comes with its own challenges. As one expert noted, “These systems are superficial and friendly up to a point. But then you get lost—there’s no documentation, and you can never get to speak to a human.” This lack of support and transparency can leave developers and businesses frustrated when attempting to integrate or troubleshoot these solutions. At the same time, a hybrid approach can make onboarding smoother for users transitioning from Web2. Ideally, builders should be able to offer both Web3-native verification and Web2-compatible solutions that integrate with mobile and web platforms.

> It'd be nice if you could verify the person who brings them in, and then you just log in with Gmail. Almost everything in the world works that way. Instead, I have to explain wallets and seed phrases to people who don't know anything about this stuff—and then they have to verify themselves. It feels like the process should be reversed.

INTERVIEWEE

There is a clear need for more advanced and user-friendly authentication and verification solutions in Web3. Innovations like multi-layered verification and biometrics, and authentication tools with flexible onboarding options, address many of the challenges users and developers face today, as we will show in the next sections.

# Benefits and Practical Applications of Centralized vs. Decentralized Identity

03

It’s easy to think that decentralized identity, with all its promises of privacy, autonomy, and user control, should completely take over centralized systems across every industry. But the truth is more complex. While decentralized identity fits perfectly with Web3’s vision of putting power back into the hands of users, it’s not always practical—or even the best option—in every situation.

Centralized solutions still play a vital role in many areas, and hybrid models often strike the right balance between meeting compliance requirements and embracing decentralization. Let's dive into these trade-offs and explore how to pick the best identity management approach for Web3 applications.

# When Decentralized Identity Makes Sense

Gaming platforms face significant challenges in maintaining identity integrity. Fake accounts and bots frequently disrupt in-game economies, exploit rewards, and undermine the balance of play-to-earn ecosystems. Traditional solutions rely on centralized identity systems that often require players to share personal data, a notable drawback for a demographic that highly values anonymity.

Contrary to initial assumptions that stronger identity systems might compromise privacy, decentralized identity offers a privacy-preserving alternative. Through biometric checks or zero-knowledge proofs, gaming platforms can verify user uniqueness without retaining sensitive data. As one interviewee noted, "One of the advantages is it's reusable. If you launch it for the whole launchpad, then if somebody gets verified once and taps into one project, they can tap into the other projects as well and continue sharing their identity with the...verified individual." This reusability simplifies verification processes across multiple projects, reducing friction for users.

Proof of verification can be anchored on-chain, ensuring tamper-proof integrity while maintaining user anonymity. Another interviewee emphasized the importance of preventing Sybil attacks, highlighting the need to “keep one person, one wallet enforced.” By ensuring that each verified identity corresponds to a single user, decentralized identity systems address critical fairness and bot-prevention issues in gaming platforms.

This approach is transformative, as it separates the act of verification from the sharing of personal data. Decentralized identity not only addresses Sybil attack issues but also ensures fairness and fosters trust among users, aligning with the principles of privacy and autonomy that are central to Web3.

### DAO Governance and Secure Voting

DAOs rely on fair and transparent voting systems, and decisions must reflect the input of unique, verified members. Centralized solutions fall short when it comes to protecting voter privacy, a cornerstone of decentralized governance.

Decentralized identity systems solve this by ensuring one-person-one-vote participation without exposing sensitive personal data. Cryptographic verifications tied to decentralized credentials make it possible to prevent vote manipulation while maintaining voter anonymity. Unlike centralized systems, which require storing sensitive information, decentralized solutions enable DAOs to verify participants without undermining the principles of decentralization and transparency.

### Privacy-Preserving Verification for Airdrops and Crypto Faucets

Similarly, decentralized identity shines in crypto projects like airdrops or faucets, where bots often exploit vulnerabilities to claim rewards. Centralized CAPTCHA or email verification could handle such issues, but these methods can be easily circumvented or fail to respect user privacy.

Decentralized identity solves this by enabling quick and privacy-preserving verification. For example, a user might prove their uniqueness or eligibility using biometrics or CAPTCHA-like mechanisms, with the result anchored on-chain. As one interviewee noted,

> “This is good because this would avoid bot users or people signing up, making fake accounts”

By decoupling verification from personal data, such systems prevent abuse while maintaining the privacy and autonomy of participants.

# When Centralized Identity is More Feasible

Despite its appeal, decentralized identity is not a catch-all solution. In industries with stringent regulatory requirements, such as finance, centralized systems remain the more realistic choice. This is also a reflection of the current regulatory landscape, which demands transparency and auditability that decentralized systems struggle to provide.

### KYC/AML in Financial Services

The early expectations that decentralized identity could revolutionize KYC (Know Your Customer) and AML (Anti-Money Laundering) processes hit a wall, as regulators more often than not require financial institutions to not only verify users but also retain and audit their information.

Decentralized systems, which excel at avoiding the storage of personal data, are inherently at odds with these compliance requirements. For example, verifying a user's identity while ensuring that their information remains private might satisfy the individual, but it fails to meet the needs of auditors or regulators.

Critics of full decentralization argue that regulatory requirements cannot be ignored. Without centralized control over user data, financial institutions risk failing audits or violating AML standards. As one interviewee explained,

> “Decentralization advocates tend to focus on projects that don't require KYC for investors. But when it comes to collateral and actual financing, financial institutions need to know where the money is going and who it's going to, because there is a whole plethora of legal documents that need to be signed in the real world for this to work.”

As such, centralized identity systems remain indispensable for compliance-heavy sectors, ensuring that user data can be retained, audited, and shared when required.

# The Role of Hybrid Models

Hybrid models offer a compelling way to combine the strengths of both approaches. By using centralized systems for compliance-critical tasks and decentralized credentials for privacy-preserving interactions, hybrid models address both regulatory needs and user empowerment.

### How Hybrid Models Work

Hybrid models integrate centralized components for storing and managing sensitive information, such as KYC or government-issued IDs, with decentralized credentials for user-controlled interactions. For instance:

- A user undergoes centralized KYC verification to meet compliance requirements.

- Once verified, they receive a decentralized credential that can be stored in their wallet or use account.

- This credential is reusable across multiple platforms, allowing the user to access on-chain services like DeFi lending or DAO governance without repeatedly sharing sensitive information.

By separating compliance tasks from everyday interactions, hybrid systems reduce data exposure while maintaining the transparency and auditability required by regulators. As one industry expert noted about integrating decentralized identity solutions into existing systems:

> "We're going to set aside some of our development work, keep parts of our infrastructure, and plug in some of theirs. It's all going to come together and work out nicely."

This reflects a growing trend toward modular, flexible identity systems that integrate decentralized components without requiring a complete overhaul of existing infrastructure.

> We're going to set aside some of our development work, keep parts of our infrastructure, and plug in some of theirs. It's all going to come together and work out nicely.

INTERVIEWEE

# Examples of Hybrid Identity Systems

**Gaming Platforms**

In gaming, hybrid systems can pair centralized identity checks for legal compliance (e.g., age verification) with decentralized credentials for in-game activities. This ensures that players meet regulatory requirements while protecting their personal information.

**DeFi Protocols**

DeFi platforms often require centralized KYC for fiat on-ramps and off-ramps, but they can use decentralized credentials for staking, lending, or other on-chain interactions. This hybrid approach ensures compliance without compromising user privacy during on-chain activity.

**Crypto Wallets**

Wallet solutions are exploring ways to abstract key management for mainstream adoption. For example, some hybrid models tie private keys to passkeys or familiar login methods (e.g., email or social media), combining the convenience of centralized authentication with the control of decentralized wallets.

# Key Benefits of Hybrid Models

- Hybrid models ensure businesses meet regulatory obligations without unnecessarily exposing user data.

- By abstracting wallet complexity and simplifying identity verification, these systems appeal to both crypto-savvy users and newcomers.

- Hybrid systems adapt to diverse applications, from gaming and DeFi to identity-gated rewards and governance.

# Challenges to Adoption

Despite their promise, hybrid models face several hurdles:

- The lack of unified standards for decentralized credentials limits interoperability. Competing solutions often result in fragmented ecosystems.

- User experience is another issue that needs to be addressed. While hybrid systems simplify some processes, managing wallets and credentials remains challenging for mainstream users. Abstractions like passkeys and social logins are essential to drive adoption.

### Key Considerations for Choosing the Right Identity System

When deciding between centralized, decentralized, or hybrid identity solutions, builders should consider:

| | |
|---|---|
| **Application Goals** | What matters most—privacy and user control (gaming, DAOs) or compliance and auditability (finance)? |
| **User Base** | Are users crypto-savvy, or will they need simplified experiences (e.g., social logins)? |
| **Technical Feasibility** | Does your team have the expertise and resources to implement decentralized or hybrid systems? |
| **Regulatory Context** | What level of data retention and auditability do regulations in your industry require? |

# Striking the Right Balance

The debate between centralized and decentralized identity is less about which system is superior and more about choosing the right tool for the job. Decentralized identity offers transformative potential for privacy-first applications like gaming, DAOs, and crypto-native use cases. Meanwhile, centralized systems remain indispensable in compliance-heavy industries like finance.

Hybrid models, bridging the strengths of both, emerge as a practical solution, balancing regulatory requirements with user empowerment. By aligning identity systems with application goals and regulatory realities, builders can unlock Web3's potential without sacrificing practicality or trust.

# Trends in Authentication and Identity for Web3

04

The rapid advancement of Web3 technology has brought identity and authentication systems among its most pressing challenges and opportunities. As decentralized ecosystems grow, there is increasing pressure to meet user expectations for privacy, interoperability, and ease of use, all while navigating the demands of regulatory compliance and technical development. This complex environment has become a catalyst for innovation, spurring advancements in areas such as

streamlined onboarding for non-crypto users and privacy-preserving interactions that do not compromise regulatory obligations.

Based on insights gathered from over 20 interviews with industry builders and experts, the following trends illustrate how Web3 identity systems are evolving to address these challenges and shape the future of decentralized applications.

# 1. Authentication Methods That Bridge Web2 and Web3

One major trend in Web3 is the integration of Web2 authentication methods, such as Google and email logins, with blockchain-based wallets. This hybrid approach reduces friction during onboarding, particularly for users who are unfamiliar with private key management or Web3 technologies. As one industry expert highlighted:

> "Getting users to verify through something in crypto means they're already somewhat of a crypto user. It's really hard because you have to explain so many steps—it's just not fun."

This underscores the importance of user-friendliness and intuitive onboarding processes, a key trend in simplifying Web3 authentication. Web2 methods are widely trusted and familiar, allowing users to log in with credentials they already use, such as social media accounts or email.

> Getting users to verify through something in crypto means they're already somewhat of a crypto user. It's really hard because you have to explain so many steps—it's just not fun.

INTERVIEWEE

Recently, passwordless methods, such as passkeys, have started to gain attention as a replacement for traditional passwords. Passkeys store cryptographic keys on a user's device, which improves security by eliminating risks associated with password breaches. Although still an emerging concept in Web3, passkeys represent a broader industry shift toward user-friendly and secure authentication methods that align well with decentralized applications.

# 2. Wallet and Private Key Abstraction

Like the integration of Web2 authentication, wallet abstraction also aims to make Web3 more accessible to mainstream users. Instead of allowing users to log in with familiar methods, wallet abstraction tackles the complexity of Web3 itself.

Traditional wallets require users to manage private keys or seed phrases, which many find intimidating or confusing. Wallet abstraction solves this by embedding wallets directly into applications, hiding the underlying mechanics such as private key management. Using SDKs and APIs, wallet abstraction allows wallets to function seamlessly in the background, enabling a smoother and more familiar experience for users accustomed to Web2 interfaces. By removing the complicated parts of crypto, wallet abstraction ensures that users can interact with blockchain applications without needing to understand their technical underpinnings.

# 3. Biometric Authentication

Biometric authentication is emerging as a popular method for verifying user identity in Web3. By using tools like video selfies, these systems link wallets to real people, addressing challenges such as bot-driven account creation, Sybil attacks, and other forms of fraud.

Biometrics not only enhances security but also improves the user experience by making verification fast and frictionless. They are particularly valuable in gaming, DAOs, and airdrop distribution, where uniqueness and fraud prevention are extremely important. For instance, video-based facial recognition can verify human presence without requiring traditional identity documents, which enables privacy-preserving user verification. If these systems gain enough traction, biometrics could successfully address any current concern about long-term scalability and privacy.

# 4. Simplified Integration

There is a growing need for identity systems that are easy to integrate and manage. End-to-end solutions that handle everything from authentication to verification reduce the need for custom-built infrastructure, simplifying implementation and operations.

Developers often face challenges when aggregating multiple identity providers or replicating identity data across various sources. These fragmented approaches lead to increased complexity and strain on resources. One industry expert highlighted the pressing need for simplified, unified solutions that reduce duplication and streamline integration:

> “One of the friction points we encountered was the inability to directly integrate identity pools or credentials from different providers. We often had to replicate identities as proof during our flow and then submit them on-chain.”

To address this, API-based systems that streamline integration have emerged as the solution of choice. By reducing fragmentation and freeing up development resources, these systems enable businesses to implement identity solutions more efficiently and adapt to the rapid pace of Web3 innovation....

# 5. Tailored Solutions for Specific Verticals

As Web3 matures, identity systems are moving away from one-size-fits-all approaches toward tailored solutions designed to meet the unique requirements of specific industries. This shift reflects a deeper understanding of the specialized needs of Web3 users. For example, gaming platforms, DAOs, and DeFi applications demand solutions that balance privacy, security, and compliance in different ways, as discussed earlier.

> One of the friction points we encountered was the inability to directly integrate identity pools or credentials from different providers. We often had to replicate identities as proof during our flow and then submit them on-chain.

INTERVIEWEE

This trend demonstrates the importance of specialization in Web3 identity systems, enabling businesses to address the distinct challenges of their user base while focusing on their core offerings. By prioritizing tailored solutions, identity providers could help the authentication systems evolve following the needs of diverse Web3 applications.

# 6. Cross-Chain Interoperability

Many Web3 users are engaging with multiple blockchains and platforms, a fragmentation that usually creates a poor user experience. Managing separate wallets and identities across chains adds complexity and friction, especially for those who might want a consistent identity and reputation across platforms.

Cross-chain interoperability is emerging as a solution to this problem. By enabling identity systems to work seamlessly across multiple chains, users can interact with various platforms without starting over each time or juggling multiple wallets. This trend is particularly important in gaming, where users may interact with games operating on different chains, as well as in DeFi, where cross-chain compatibility is critical for accessing diverse financial services.

Creating a cohesive Web3 experience across chains requires solutions that abstract away these complexities, ensuring that users can navigate the ecosystem without unnecessary barriers. As one industry expert noted,

> “The general OAuth system is literally always going to be under attack. Disastrous, to say the least. You can roll your own technically, but keeping the dependencies up to date is much more aggressive. It’s just easier to outsource it to a big provider.”

In a fragmented, multi-chain environment, this makes a strong case for leveraging trusted identity solutions that simplify integration and reduce the burden on developers.

# 7. Privacy and Data Control

Privacy and data control are central to the evolution of Web3 identity systems. Users increasingly expect privacy-preserving solutions that minimize data collection and enable selective disclosure, giving them greater control over their personal information.

For example, some systems allow users to store verified credentials locally in an encrypted state, ensuring only they hold the decryption key. This approach reduces the risks of centralized data breaches while empowering users to manage their data. Selective disclosure mechanisms further enhance privacy by allowing users to share only the specific information required for an interaction, such as proving age or uniqueness, without exposing additional personal details.

At the same time, compliance requirements like KYC and AML present challenges for businesses operating in regulated industries. Balancing privacy with regulatory obligations will require continued innovation and user education to help participants understand the need for verification in some contexts.

# Conclusion

06

This report, shaped by insights from over 20 industry builders and experts, has explored the current limitations in Web3 authentication and highlighted emerging trends. It also showcased how Civic is addressing these challenges with innovative products like Civic Auth and Civic Pass. By providing tools that prioritize privacy, security, and seamless user experiences, Civic enables developers and businesses to build trusted, compliant applications that can reach a wider audience.

Decentralized identity solutions like Civic's are reshaping the landscape by returning control over personal data to users and aligning with Web3's core principles of privacy and data sovereignty. As the lines between Web2 and Web3 continue to blur, the convergence of authentication methods, the adoption of new technologies like biometrics and passkeys, and the growing demand for seamless user experiences are shaping the future of digital identity.

Civic's focus on multi-chain support, wallet agnosticism, and privacy-preserving features makes it a powerful partner for developers and businesses looking to build the next generation of Web3 applications. Through new technologies and staying ahead of industry trends, Civic is well-positioned to lead the evolution of Web3 authentication and identity management.

To learn more about Civic and its solutions, and to explore how its innovative approach can help you build secure, compliant, and user-friendly Web3 applications, visit the Civic website or reach out to the team.