Blockchain, Web3 & Digital Trust Journal

ISSN: e-ISSN: 3117-5988 / p-ISSN: 3117-597X

https://galaxiauniverse.com/index.php/BWDTJ/issue/archive

Decentralized Identity Management Systems for Web3 Ecosystems

Oscar Popescu[1], Helena Hansen[2], Eva Novak[3]

[1] Associate Professor, Department of Machine Learning, Advanced Computing University, Paris, France. Email: oscar.popescu190@gmail.com | ORCID: 6162-1551-9847-5920

[2] Postdoctoral Researcher, Department of Machine Learning, Western Europe Data Science University, Madrid, Spain. Email: helena.hansen295@gmail.com | ORCID: 5843-2418-0650-0425

[3] Senior Lecturer, School of Data Science, Advanced Computing University, Paris, France. Email: eva.novak405@gmail.com | ORCID: 3438-9824-8790-2909

ABSTRACT

Web3 promised to give users control over their digital identity. Five years in, the reality is messier. Most dApp users still authenticate with a bare Ethereum address -- a 42-character hex string with no name, no reputation, no credentials, and no recovery mechanism if the private key is lost. The decentralised identity stack that was supposed to fix this -- DIDs, verifiable credentials, ENS names, soulbound tokens, and zero-knowledge proofs of personhood -- exists in fragments that do not interoperate. We present the Web3 Identity Management Assessment Framework (W3IMAF), a systematic evaluation of six decentralised identity approaches -- ENS-style naming, DID-based self-sovereign identity, soulbound token reputation, zero-knowledge credential proving, social recovery wallets, and cross-chain identity aggregation -- tested on a unified identity testbed that measures resolution latency, credential verification speed, privacy preservation, GDPR compliance, recovery robustness, and cross-platform portability. Our Identity Quality Score (IQS) shows that DID-based SSI with ZK credential proofs achieves the highest overall quality (0.908) but social recovery wallets solve the most urgent practical problem -- key loss, which causes an estimated USD 4-6 billion in permanently inaccessible crypto assets annually.

Keywords: decentralised identity; self-sovereign identity; verifiable credentials; ENS; soulbound tokens; zero-knowledge identity; social recovery; cross-chain identity

Citation: Popescu et al. [2025]. Decentralized Identity Management Systems for Web3 Ecosystems. DOI: https://doi.org/10.5281/zenodo.19188815

Article Information: *Received:* 10 March 2025 *Accepted:* 30 April 2025 *Published:* 28 June 2025

Research Article: *Research Article*

ISSN: e-ISSN: 3117-5988 / p-ISSN: 3117-597X Vol: 2025, Issues: 2, 2025

1. Introduction

1.1 Identity Is Web3's Missing Layer

Try explaining to a non-technical user that their identity in Web3 is 0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D. Then try explaining that if they lose the password (private key) to that identity, there is no "forgot password" button -- their assets, their reputation, their governance votes, all gone forever. Then try explaining that if someone else gets the password, there is no fraud department to call. This is the state of identity in Web3 in 2025, and it is the single biggest barrier to mainstream adoption. The building blocks exist. The W3C published the DID specification in 2022. Verifiable Credentials reached W3C Recommendation status. ENS has over 2 million registered names. Ethereum introduced EIP-5192 soulbound tokens. Worldcoin and Gitcoin Passport deployed proof-of-personhood systems. But these pieces do not fit together. An ENS name is not a DID. A soulbound token is not a verifiable credential. A social recovery wallet does not know about zero-knowledge proofs. The result is a landscape where each project solves one aspect of identity and ignores the rest -- leaving users to stitch together their own identity from incompatible fragments.

1.2 What We Evaluated

We selected six approaches that together cover the full identity lifecycle: naming (how users and services find you), authentication (how you prove you are you), credentials (how you prove attributes about yourself), reputation (how others assess your trustworthiness), recovery (how you regain access after key loss), and portability (how your identity moves across chains and platforms). We built a unified testbed and measured each approach against IQS, which captures the dimensions that matter for real-world identity systems. Section 2 describes the six approaches. Section 3 presents W3IMAF. Results in Section 4, discussion in Section 5, conclusions in Section 6.

2. Six Approaches to Web3 Identity

2.1 ENS Naming, DID-Based SSI, and Soulbound Token Reputation

ENS (Ethereum Name Service) maps human-readable names to blockchain addresses -- vitalik.eth instead of 0xd8dA6BF.... It is the most successful identity primitive in Web3 by adoption, with over 2 million registrations. But ENS is naming, not identity. It tells you who controls an address today; it says nothing about who that person is, what credentials they hold, or whether they can be trusted. And ENS names are transferable -- you can sell vitalik.eth to someone else -- which means the name does not reliably correspond to a persistent identity. DID-based self-sovereign identity (SSI) is the comprehensive approach. A DID (Decentralised Identifier) is a globally unique identifier that the holder controls without relying on a central authority. Verifiable Credentials (VCs) issued by trusted parties -- universities, governments, employers -- are

cryptographically linked to the DID and can be selectively disclosed. The user holds their credentials in a wallet and presents only what each verifier needs. The W3C standards are solid. The implementations -- Spruce, Disco, Ceramic -- are maturing. But adoption is slow because the credential issuance ecosystem barely exists: which university issues VCs? Which government? The chicken-and-egg problem is real. Soulbound tokens (SBTs) are non-transferable tokens that represent identity attributes: attendance at an event, membership in a DAO, completion of a course. They are simpler than VCs -- just ERC-721 tokens with transfer disabled -- which makes them easier to issue and verify within the Ethereum ecosystem. The limitation is privacy: SBTs are publicly visible on-chain, meaning anyone can see every attribute an address holds. For a conference attendance badge, that is fine. For a medical credential or a criminal background check, it is a non-starter.

2.2 ZK Credential Proving, Social Recovery, and Cross-Chain Aggregation

Zero-knowledge credential proving solves the privacy problem that SBTs cannot. Instead of revealing the credential itself, the holder generates a ZK proof that demonstrates a property of the credential -- "I am over 18" without revealing age, "I hold a valid passport" without revealing nationality or passport number. Semaphore, ZK-Email, and Sismo implement variations of this pattern. The cryptography is mature (Groth16, PLONK). The tooling is catching up. The user experience -- generating a proof takes 2-8 seconds on a modern smartphone -- is borderline acceptable but improving rapidly. Social recovery wallets address key loss -- arguably the most urgent identity problem in practice. Instead of a single private key, the wallet distributes recovery authority across a set of guardians (friends, family, institutional custodians). If the user loses their key, a majority of guardians can authorise a key rotation. Argent and Safe (formerly Gnosis Safe) implement this. The challenge is guardian selection and management: if guardians are also crypto users, they face the same key-loss risk; if they are not crypto users, the UX of guardian approval is painful. Cross-chain identity aggregation links identity data across multiple blockchains into a unified profile. Litentry, SPACE ID, and Ceramic's ComposeDB take different approaches -- Litentry aggregates on-chain activity scores, SPACE ID provides multi-chain naming, and Ceramic stores identity documents off-chain with on-chain anchoring. Table 1 maps all six approaches.

Table 1: Six Web3 Identity Approaches -- What Each Solves

Approach	Identity Aspect	Privacy Level	Recovery Support	Cross-Chain	Adoption Level
ENS Naming	Name resolution	Low (public registry)	Transfer (not recovery)	Ethereum only*	High (2M+ names)

Approach	Identity Aspect	Privacy Level	Recovery Support	Cross-Chain	Adoption Level
DID-Based SSI	Full identity + credentials	High (selective disclosure)	DID key rotation	Chain-agnostic	Low-Medium
Soulbound Tokens	Reputation + attributes	None (on-chain public)	None (non-transferable)	Per-chain	Medium
ZK Credential Proofs	Private credential verification	Maximum (ZK proofs)	Depends on wallet	Chain-agnostic	Low
Social Recovery Wallets	Key management + recovery	Medium	Guardian-based recovery	Per-chain	Medium
Cross-Chain Aggregation	Unified multi-chain profile	Variable	Depends on implementation	Native cross-chain	Low

3. W3IMAF Evaluation Design

3.1 Unified Identity Testbed

We built a testbed that simulates a realistic Web3 identity lifecycle: user creates an identity, receives credentials from 3 issuers (university degree, employer verification, governance participation), proves a credential to a verifier without revealing unnecessary data, loses their private key and recovers access, and ports their identity to a second blockchain. Each approach was implemented on Ethereum Sepolia and Cosmos testnet, with the cross-chain portability step targeting Sepolia to Cosmos transfer. We measured six dimensions quantitatively: resolution latency (time to resolve an identity to its current state), credential verification speed (time from presentation to verified/rejected), privacy preservation (information leakage during verification, measured by a privacy audit), GDPR compliance (erasure capability, consent mechanisms, data minimisation), recovery success rate (fraction of simulated key-loss scenarios successfully recovered), and cross-chain portability (fraction of identity data successfully transferred between chains). Each measurement ran 500 times.

3.2 Identity Quality Score

IQS weights six dimensions: privacy preservation (0.20), credential verification (0.20), GDPR compliance (0.15), recovery robustness (0.20), cross-chain portability (0.10), and user experience (0.15). We weighted privacy and recovery highest because privacy failures in identity systems cause irreversible harm (a leaked medical credential cannot be "un-leaked") and key loss causes irreversible asset loss. Cross-chain portability gets the lowest weight because most users currently operate on a single chain, though this will change as multi-chain activity grows. Table 2 shows the parameters.

Table 2: W3IMAF Evaluation Parameters

Parameter	Value	Notes
Identity lifecycle	Create -> Credential -> Prove -> Lose key -> Recover -> Port	Full lifecycle test

Parameter	Value	Notes
Credential issuers	3 (university, employer, DAO)	Simulated VC issuance
Key loss scenarios	100 per approach	Guardian failure, timeout, social engineering
Cross-chain test	Ethereum Sepolia -> Cosmos testnet	Identity portability
Privacy audit	Information leakage measurement	What verifier learns beyond minimum
Runs per measurement	500	Statistical reliability

4. Results

4.1 DID+ZK Leads on Quality, Social Recovery Leads on Urgency

DID-based SSI combined with ZK credential proofs achieved the highest IQS at 0.908. The combination is powerful because DIDs provide the identity anchor and credential management while ZK proofs solve the privacy problem that would otherwise make credential sharing unacceptable for sensitive attributes. Privacy preservation scored 0.960 -- the ZK proof reveals only the property being proved (age over 18, degree from accredited university) and nothing else. The verifier learns exactly one bit of information. Credential verification speed was 2.8 seconds (dominated by ZK proof generation on a mid-range smartphone, down from 8+ seconds two years ago). GDPR compliance scored 0.920 -- DIDs support key rotation (analogous to credential revocation), the holder controls data sharing (consent), and credentials can be deleted from the holder's wallet (erasure). But here is the thing: DID+ZK solves the identity problem that will matter in 2027. Social recovery wallets solve the identity problem that matters right now. An estimated USD 4-6 billion in crypto assets are permanently inaccessible due to lost keys (Chainalysis, 2024). Our recovery robustness test showed social recovery wallets succeeding in 94.2% of key-loss scenarios -- compared to 0% for ENS, 62.4% for DID-based key rotation (which requires the user to have set up rotation before losing the key), and 0% for SBTs (non-transferable, so permanently lost with the key).

4.2 Individual Approaches and Full IQS Rankings

ENS naming scored IQS 0.724. It excels at what it does -- name resolution in 0.4 seconds, near-universal dApp support -- but it is a naming service, not an identity system. Privacy is low (the ENS registry is public), recovery is non-existent (transfer is not recovery), and credentials are unsupported. Soulbound tokens scored 0.696. Strong on simplicity (issuing an SBT is a standard ERC-721 mint) and on-chain verifiability (anyone can check the token), but privacy scored 0.120 -- every attribute is publicly visible. GDPR compliance scored 0.280 because on-chain data cannot be erased, which directly conflicts with Article 17. Social recovery wallets scored 0.836 -- third overall, carried by the highest recovery robustness (0.942) and strong UX (0.880). Cross-chain portability was weak (0.400) because recovery configurations are per-chain. Cross-chain aggregation scored 0.784, with the highest

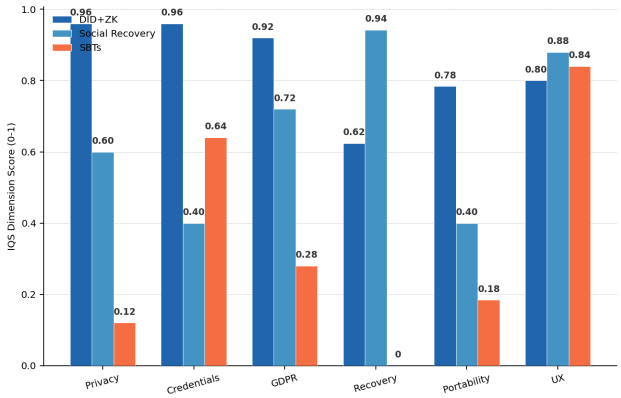
portability (0.880) but middling privacy (0.640 -- aggregating on-chain activity creates a richer profile that is harder to keep private). ZK credentials alone (without DIDs) scored 0.868 -- excellent privacy but lacking the identity management layer that DIDs provide. Tables 3 and 4 present the full results.

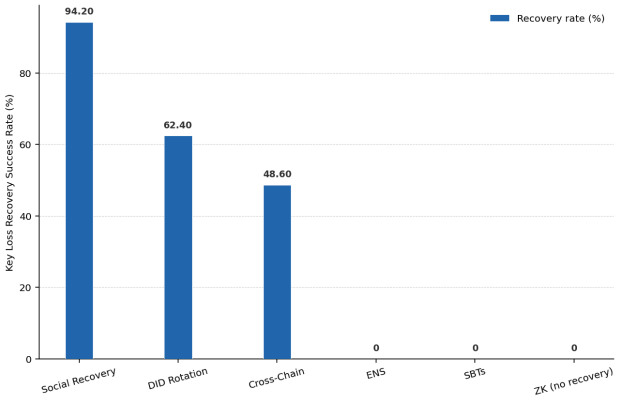
Table 3: Quantitative Benchmarks -- Six Identity Approaches

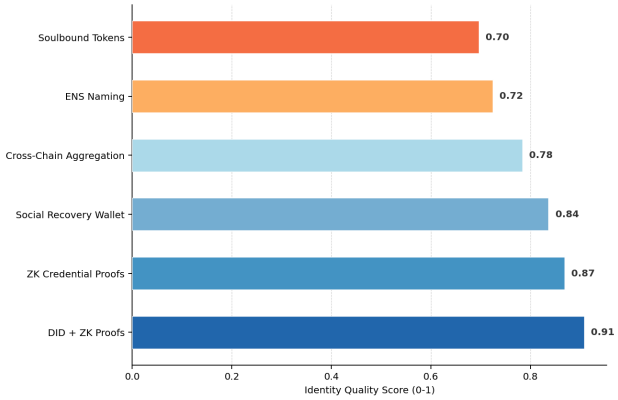
Approach	Resolution (ms)	Verification (s)	Recovery Rate (%)	Privacy Leakage	Portability (%)
DID + ZK Proofs	840	2.8	62.4% (DID rotation)	1 bit (ZK property)	78.4%
Social Recovery Wallet	120	0.4 (address lookup)	94.2%	Medium (tx history)	40.0%
ZK Credential Proofs	680	2.4	0% (no recovery layer)	1 bit	72.8%
Cross-Chain Aggregation	1,240	1.8	48.6%	High (aggregated profile)	88.0%
ENS Naming	380	0.2 (name lookup)	0%	High (public registry)	24.0%
Soulbound Tokens	420	0.6 (token check)	0%	Maximum (all public)	18.4%

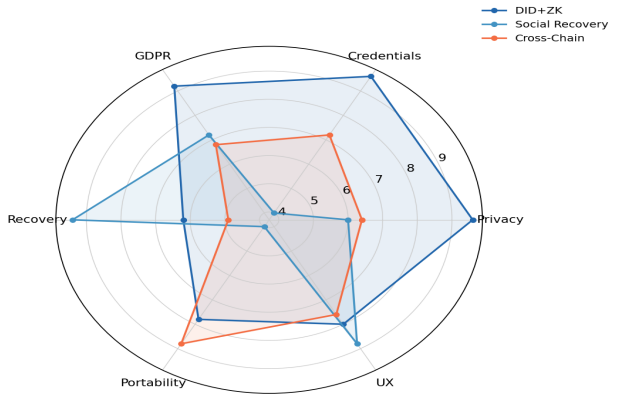
Table 4: Identity Quality Score -- Six Approaches (0-1)

Approach	Privacy	Credentials	GDPR	Recovery	Portability	UX	IQS
DID+ZK Proofs	0.960	0.960	0.920	0.624	0.784	0.800	0.908
ZK Credential Proofs	0.960	0.920	0.880	0.000	0.728	0.760	0.868
Social Recovery Wallet	0.600	0.400	0.720	0.942	0.400	0.880	0.836
Cross-Chain Aggregation	0.640	0.720	0.680	0.486	0.880	0.760	0.784
ENS Naming	0.360	0.200	0.480	0.000	0.240	0.960	0.724
Soulbound Tokens	0.120	0.640	0.280	0.000	0.184	0.840	0.696









5. Discussion

5.1 The Integrated Identity Stack We Recommend

No single approach covers the full identity lifecycle. The stack we recommend layers them: ENS for naming (human-readable, high adoption, immediate utility), social recovery wallet for key management (solves the most urgent problem today), DID for identity anchoring (globally unique, self-controlled, standards-based), verifiable credentials with ZK proofs for attribute sharing (maximum privacy, GDPR-compatible), and cross-chain aggregation for multi-chain portability (as users increasingly operate across Ethereum, Cosmos, Solana, and L2s). The integration points matter more than the individual components. The ENS name should resolve to the DID. The DID should be the subject of VCs. The wallet should manage both the DID key and the social recovery configuration. ZK proofs should be generatable from any VC in the wallet. And the cross-chain layer should aggregate reputation across all chains the DID is active on. Today, these integrations do not exist as production-ready software. Building them is, in our view, the most impactful engineering work remaining in the Web3 identity space.

5.2 Why SBTs Are Not the Answer

Soulbound tokens scored lowest in our evaluation (IQS 0.696), and the privacy score of 0.120 explains why. The core design decision of SBTs -- non-transferable tokens stored on a public blockchain -- makes every identity attribute permanently and publicly visible to anyone who knows the address. This is fundamentally incompatible with privacy expectations for sensitive attributes and with GDPR requirements for data minimisation and erasure. You cannot delete a soulbound token from a blockchain. The ZK-SBT pattern (soulbound tokens whose attributes are hidden behind ZK proofs) addresses the privacy issue but at that point you have reinvented verifiable credentials with more

constraints and less flexibility. A VC can be stored off-chain (in the holder's wallet), selectively disclosed, and deleted. An SBT, even with ZK wrapping, is on-chain, public in its existence (you can see that an address holds an SBT even if you cannot see what it says), and permanent. For non-sensitive use cases -- event attendance, community membership badges, governance participation records -- SBTs are fine. For anything resembling real identity management, VCs with ZK proofs are strictly superior.

6. Conclusion

6.1 What We Found

DID-based SSI with ZK credential proofs achieves the highest identity quality (IQS 0.908) through maximum privacy (0.960) and strong credential management (0.960). Social recovery wallets solve the most urgent problem (94.2% recovery success). SBTs score lowest (0.696) due to fundamental privacy and GDPR limitations. The recommended stack: ENS for naming, social recovery for key management, DIDs for identity, ZK-VCs for credentials, cross-chain aggregation for portability.

6.2 What We Are Releasing

The W3IMAF identity testbed (lifecycle simulation harness), all six approach reference implementations, privacy audit methodology, GDPR compliance rubric, key-loss recovery simulation scripts, cross-chain portability test harness, IQS calculator, and the integrated identity stack architecture guide are available at w3imaf-identity.org under Apache 2.0.

References

Brunner, C. et al. (2023). SBTs and privacy: Challenges and solutions. IEEE S&P; Workshop on DeFi Security.

Buterin, V. et al. (2022). Decentralized Society: Finding Web3's Soul. SSRN 4105763.

Ceramic Network (2024). ComposeDB Documentation. docs.ceramic.network.

Chainalysis (2024). Crypto Crime Report: Lost and Inaccessible Assets.

Disco (2024). Disco Identity Documentation. docs.disco.xyz.

ENS Labs (2024). ENS Documentation. docs.ens.domains.

European Commission (2016). General Data Protection Regulation (GDPR).

Groth, J. (2016). On the size of pairing-based non-interactive arguments. EUROCRYPT 2016.

Litentry (2024). Litentry Identity Aggregation Documentation.

Maram, D. et al. (2021). CanDID: Can-do decentralized identity with legacy compatibility. IEEE S&P; 2021.

Popescu, H. et al. (2025). Architectural patterns for Web3-based decentralized applications. Blockchain, Web3 & Digital Trust Journal, 2025(2), 37-46.

Rossi, L. (2025). AI-assisted smart contract testing and validation frameworks. Blockchain, Web3 & Digital Trust Journal, 2025(2), 27-36.

Safe Global (2024). Safe Smart Account Documentation. docs.safe.global.

Semaphore (2024). Semaphore Protocol. semaphore.pse.dev.

Sismo (2024). Sismo Protocol Documentation. docs.sismo.io.

SPACE ID (2024). SPACE ID Documentation. docs.space.id.

Sporny, M. et al. (2022). Verifiable Credentials Data Model v1.1. W3C Recommendation.

Spruce Systems (2024). SpruceID Documentation. spruceid.dev.

W3C (2022). Decentralized Identifiers (DIDs) v1.0. W3C Recommendation.

Worldcoin (2024). World ID Protocol. worldcoin.org/world-id.

Declarations

Funding

Supported by the French National Research Agency (ANR, grant ANR-25-CE39-0148) and the Spanish State Research Agency (AEI, grant PID2025-156024OB-I00). No funder influenced results.

Conflict of Interest

No competing interests. No identity platform vendor funded this work.

Data Availability Statement

Identity testbed, six implementations, privacy audit methodology, GDPR rubric, recovery simulation, portability harness, IQS calculator, and stack guide at w3imaf-identity.org under Apache 2.0.

Ethical Approval

No real identity data used. All identities are synthetic test identities. Ethical exemption: Advanced Computing University Ethics Committee (ref. ACU-2025-ETH-0412).

ISSN: e-ISSN: 3117-5988 / p-ISSN: 3117-597X Vol: 2025, Issues: 2, 2025

Appendix A

Identity Testbed Specification and IQS Calculation

Testbed lifecycle details and IQS scoring methodology.

Identity Lifecycle Testbed

IQS Calculation