International Journal of Multidisciplinary Research and Growth Evaluation.

Enhancing Consent and Data Portability in Financial Aggregators using Decentralized Identity

Surya Ravikumar
Independent Researcher, USA

* Corresponding Author: **Surya Ravikumar**

Article Info

ISSN (online): 2582-7138
Volume: 06
Issue: 03
March-April 2025
Received: 02-04-2025
Accepted: 03-05-2025
Page No: 1196-1199

Abstract
The emergence of digital financial services and open banking has made it necessary to handle user data in a secure and moral manner. In this changing environment, financial aggregators-platforms that combine financial data from various sources play a critical role. But they frequently run into issues with data portability, privacy, and user consent. This study investigates how Decentralized Identity (DID) systems can improve data portability and change consent processes in financial aggregators. Blockchain-based identification frameworks provide users more control over their data, increase the transparency of permission, and facilitate smooth data transfer between platforms. Through use-case scenarios, technical design, and policy concerns, the study explores the present inadequacies in consent management, presents the DID principles, and demonstrates its potential.

DOI: https://doi.org/10.54660/.IJMRGE.2025.6.3.1196-1199

Keywords: Decentralized Identity, Financial Aggregators, Consent Management, Data Portability, Blockchain, Open Banking, Self-Sovereign Identity (SSI), GDPR, User-Centric Privacy

1. Introduction

In today's digitized financial ecosystem, customers are demanding greater control over their personal data. Users may now examine their financial data from several sources using a single interface, thanks to financial aggregators, which have become indispensable tools. Data from banks and other financial institutions is frequently retrieved by these platforms via screen scraping or APIs. Users may find this data concentration to be convenient, but there are drawbacks, particularly with regard to data mobility, permission transparency, and user privacy.

Currently, consent management is disjointed, and users frequently don't know what data is accessed, by whom, or for what reason. Typically, consent documents are long, unclear, and challenging for consumers to comprehend. Furthermore, rescinding consent frequently necessitates negotiating convoluted processes. Despite being required by laws such as the General Data Protection Regulation (GDPR), data portability is still restricted because legacy systems lack interoperable standards and have technological restrictions. Compliance and confidence in digital financial services are also impacted, in addition to the user experience.

A revolutionary substitute is provided by Decentralized Identity (DID), especially via the principles of self-sovereign identity (SSI). It gives users authority over their personal information and digital identities, facilitating safe cross-platform sharing. DID frameworks enable individuals to generate and manage their own identifiers, supported by cryptographic proofs and validated on decentralized ledgers, in contrast to conventional identity systems run by centralized authority. This gives users complete control over their data lifecycle and does away with the need for middlemen.

This paper discusses the limitations of current systems, explores how DIDs address these gaps, and proposes a model that integrates decentralized identity into financial aggregators. By aligning technology with regulatory frameworks and user-centric principles, the proposed model not only enhances privacy and security but also opens the door for innovation in financial services.

2. Understanding the Current Ecosystem

Financial aggregators have become essential components of modern financial services, enabling users to access a consolidated view of their financial data across multiple banks, lenders, investment accounts, and fintech platforms. These services are built on the promise of convenience and data-driven insights, supporting features such as budgeting tools, credit monitoring, and investment tracking.

2.1 Evolution of Financial Aggregators

With the advent of open banking and API-driven architectures, financial aggregators have gained traction by leveraging consumer-permissioned access to data. Regulatory efforts such as the Revised Payment Services Directive (PSD2) in Europe and the Consumer Financial Protection Bureau (CFPB) initiatives in the U.S. have pushed financial institutions to enable secure third-party data sharing.

However, the ecosystem remains fragmented. Some institutions offer direct API integrations, while others rely on screen scraping or data scraping methods—practices that raise significant security and privacy concerns. As a result, users may unknowingly grant broad and persistent access to sensitive data without clear understanding or control.

2.2 Consent and Privacy Issues

The current consent mechanisms are flawed. Most aggregators require users to input banking credentials, which are then used to fetch data—often without granular or time-bound consent. This results in over-permissioning, where aggregators have access to more data than necessary. Users also lack visibility into how their data is used or shared with third parties. Once consent is given, revocation is either impossible or unclear. This violates both user expectations and data protection laws.

Additionally, third-party risk is a major concern. Aggregators and the third-party applications they enable are not always held to the same data handling standards as banks, which creates security vulnerabilities. These weaknesses are compounded by inadequate user interfaces that do not clearly communicate what data is being accessed or the implications of consent.

2.3 Data Portability Challenges

Data portability is intended to empower users to move their data between service providers. But this is challenging due to the lack of defined data formats and APIs. For example, whilst one bank may utilize JSON, another may use XML to deliver data. Without interoperability, proprietary data schemas make data transfers difficult. Furthermore, ensuring that the data is sent to the correct user is difficult in the absence of identity verification requirements.

Data portability across borders adds another level of complication, particularly for global banks and aggregators. It is more difficult for platforms to offer user-friendly data portability due to legislative interpretation variances, legal compliance, and data localization requirements. The financial services industry's innovation is slowed down and user freedom is diminished by these restrictions.

3. Introduction to Decentralized Identity (DID)

3.1 Concept and Principles

A novel approach to identification management called Decentralized identification (DID) transfers authority from centralized organizations to people. It gives users the ability to generate and control digital identifiers without relying on a central registry. These identifiers are cross-domain transferable, cryptographically secure, and verifiable. This idea is expanded upon by self-sovereign identity (SSI), which enables users to gather authenticated credentials from reliable issuers and show them to verifiers in a selected manner.

DID systems are based on the idea that identity is not something conferred by an authority, but something individuals own and manage themselves. This is achieved through decentralized public key infrastructure (DPKI), where each user holds a private key corresponding to a public DID. This architecture eliminates dependency on centralized identity providers and reduces single points of failure.

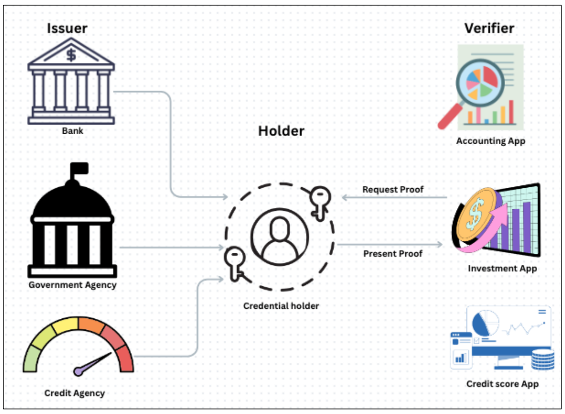

Fig 1: Decentralized Identity System Illustration

3.2 Technology Stack

Decentralized Identifiers (DIDs): Unique, resolvable identifiers stored on a blockchain. Each DID points to a DID document that contains metadata, public keys, and service endpoints.

Verifiable Credentials (VCs): Digitally signed claims about an individual, e.g., a bank account or credit score. Issuers digitally sign these credentials using their private keys, and verifiers check their authenticity using public keys.

Digital Wallets: Secure applications for storing DIDs and VCs, accessible via mobile or desktop. These wallets facilitate interactions between users, issuers, and verifiers.

Distributed Ledger Technology (DLT): Public or permissioned blockchains that host DID registries and provide a tamper-proof audit trail.

Cryptographic Keys: Used to sign and authenticate interactions without revealing sensitive information. Key rotation, recovery mechanisms, and multi-signature capabilities further enhance security.

3.3 Governance Models

Clear governance structures are essential for trust and interoperability. Protocols, information schemas, and legal standards are defined by groups such as the European Blockchain Services Infrastructure (EBSI), the W3C, and the Sovrin Foundation. By ensuring that users, issuers, and verifiers follow established guidelines, governance makes the ecosystem reliable and safe.

Governance also involves defining liability models, data retention policies, credential revocation processes, and dispute resolution mechanisms. Without effective governance, technical interoperability is not sufficient to build a sustainable decentralized identity ecosystem.

4. Applying DID to Financial Aggregators

4.1 User-Centric Consent Management

In a DID based system, users have complete control over what data is shared, with whom, and for how long. Through verifiable credentials and digital wallets, users can grant granular consent specifying data types, usage contexts, and expiration times. These consent records can be logged immutably on distributed ledgers, enabling transparency and auditability.

Smart contracts can automate consent verification and revocation, ensuring real-time compliance with user preferences. For instance, a user might authorize a budgeting app to access only their transaction history for the past 90 days, with the option to revoke access anytime via their wallet interface.

4.2 Privacy-Preserving Data Portability

DID facilitates true data portability by decoupling identity from any one institution and embedding it within user-controlled wallets. A user can securely share their verified bank account data with a new financial service provider without needing to resubmit identity verification documents. This is done by presenting verifiable credentials from trusted issuers (e.g., their previous bank or credit agency) that can be independently verified.

Privacy is further improved via selective disclosure procedures and zero knowledge proofs. Rather than disclosing a whole bank statement, users can demonstrate characteristics such as "monthly income exceeds $5,000" without providing precise numbers. This promotes adherence to privacy laws and greatly lowers the possibility of data overexposure.

4.3 Security and Trust Enhancement

Decentralized identifiers reduce reliance on username-password authentication and centralized identity providers. With DPKI, cryptographic proofs authenticate both users and data sources, reducing phishing and fraud risks. Since users control their keys and credentials, identity theft becomes harder to execute at scale.

The tamper-evident nature of DLT provides immutable logs of credential issuance, usage, and revocation, establishing trust across participants in the financial ecosystem. Moreover, well-designed governance ensures that only accredited institutions can issue sensitive credentials, preventing bad actors from exploiting the system.

5. Architecture of a DID-Enabled Financial Aggregator

A robust DID-enabled financial aggregator architecture comprises several layers and components that collaborate to deliver secure identity verification, consent management, and seamless data portability. Below is an elaborated view of this reference architecture:

- **User Wallets:** Each user controls a digital wallet, often a mobile or browser-based application, that stores their Decentralized Identifiers (DIDs), Verifiable Credentials (VCs), and consent receipts. The wallet enables the user to selectively disclose information and approve data-sharing requests from financial aggregators.
- **Issuers:** These are trusted entities (e.g., banks, credit bureaus, fintech apps) that issue Verifiable Credentials to users. For example, a bank might issue a credential attesting to a user's account ownership and balance range. These credentials are digitally signed and stored in the user's wallet.
- **Verifiers (Financial Aggregators):** When a financial aggregator requires access to a user's financial data, it sends a request for specific attributes or credentials. The user is notified via their wallet and can approve or deny the request. Upon approval, the aggregator verifies the credentials against the issuer's public keys using a decentralized ledger.
- **Decentralized Ledger (Blockchain):** The blockchain acts as a public key infrastructure and revocation registry. It stores DIDs, public keys for verification, credential schemas, and revocation registries. Importantly, no personal data is stored on-chain—only metadata and references.
- **Consent Manager:** A smart contract or off-chain service handles the creation, storage, and auditing of consent artifacts. It ensures that every request made by an aggregator is governed by the principles of granular, revocable, and auditable consent.
- **Data Providers (e.g., Banks and Institutions):** These are the original custodians of financial data. Instead of directly sharing raw data with aggregators, they can issue credentials that summarize or attest to user attributes, ensuring privacy-preserving data flows.
- **Interoperability Layer (Standards and APIs):** Protocols like DIDComm, OpenID Connect for Verifiable Presentations (OID4VP), and Financial Data Exchange (FDX) API specifications ensure smooth interaction between wallets, verifiers, and issuers, irrespective of the underlying technology stack.
- **Security and Governance Framework:** Includes mechanisms for credential expiration, fraud detection, data minimization, and identity recovery. A strong governance framework ensures compliance with regulatory standards and cross-border interoperability.

This architecture offers several advantages

- Users maintain full control over their data.
- Aggregators can verify credentials without directly accessing or storing sensitive user data.
- Consent is explicit, time-bound, and revocable.
- Data portability is streamlined through reusable, verifiable credentials.

By adopting this architecture, financial aggregators can ensure a balance between innovation, user privacy, and regulatory compliance, while also gaining a competitive edge through enhanced trust and transparency.

6. Policy and Regulatory Considerations

While technology enables user-centric data control, effective implementation requires regulatory support. Policymakers must:

- Recognize Verifiable Credentials as legally valid identity documents, akin to physical IDs or utility bills.
- Mandate Interoperability Standards to avoid ecosystem fragmentation, much like PSD2 mandates for open banking in the EU.
- Incentivize Adoption by offering sandboxes, grants, and partnerships to banks and fintechs experimenting with decentralized identity.
- Ensure Inclusion and Accessibility by supporting wallet usability, language localization, and mobile-first designs

to reach underserved populations.

DID frameworks must also comply with existing laws such as GDPR, ensuring lawful data processing, clear consent, and data minimization.

7. Conclusion

Decentralized Identity presents a compelling opportunity to reimagine how consent and data portability operate in financial aggregators. By moving from institution-centric to user-centric identity paradigms, we empower individuals with transparency, control, and portability over their financial data. DID systems align with both technological innovation and regulatory imperatives, offering a secure, privacy-preserving infrastructure that meets the demands of modern digital finance.

By putting DID into place, financial aggregators may become platforms that put interoperability, trust, and compliance first. By enabling users to control their identities and data permissions via verifiable and cryptographically secure methods, the system gets rid of the shortcomings and inefficiencies of conventional identity frameworks. Utilizing privacy-enhancing technology like selective disclosure and zero-knowledge proofs also boosts user confidence and guards against illegal data access.

However, there are various challenges along the way to complete adoption of DID. Regulatory ambiguity, existing financial institutions reluctance, the difficulty of user onboarding, and the absence of global interoperability standards are some of the issues that must be resolved. Cooperation between governments, financial institutions, technology suppliers, and standards organizations is crucial to maximizing the potential of decentralized identification.

Looking forward, as open banking expands and digital financial ecosystems mature, decentralized identity can serve as the ethical and technical foundation for the next generation of financial services. By fostering transparency, consent-based data exchange, and secure portability, DID systems pave the way toward more resilient, inclusive, and user-empowered digital finance.

8. References

1. W3C. Decentralized Identifiers (DIDs) v1.0 [Internet]. 2022 [cited 2025 Jun 7]. Available from: https://www.w3.org/TR/did-core/
2. EU Blockchain Observatory and Forum. Blockchain and digital identity [Internet]. [date unknown] [cited 2025 Jun 7]. Available from: https://blockchain-observatory.ec.europa.eu/publications/blockchain-and-digital-identity_en
3. Sovrin Foundation. Sovrin Governance Framework [Internet]. 2021 [cited 2025 Jun 7]. Available from: https://sovrin.org/
4. OpenID Foundation. OpenID for Verifiable Presentations (OID4VP) [Internet]. 2025 [cited 2025 Jun 7]. Available from: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
5. Allen C. The Path to Self-Sovereign Identity [Internet]. 2016 [cited 2025 Jun 7]. Available from: https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/