HSLU Lucerne University of Applied Sciences and Arts

# Digital Wallets

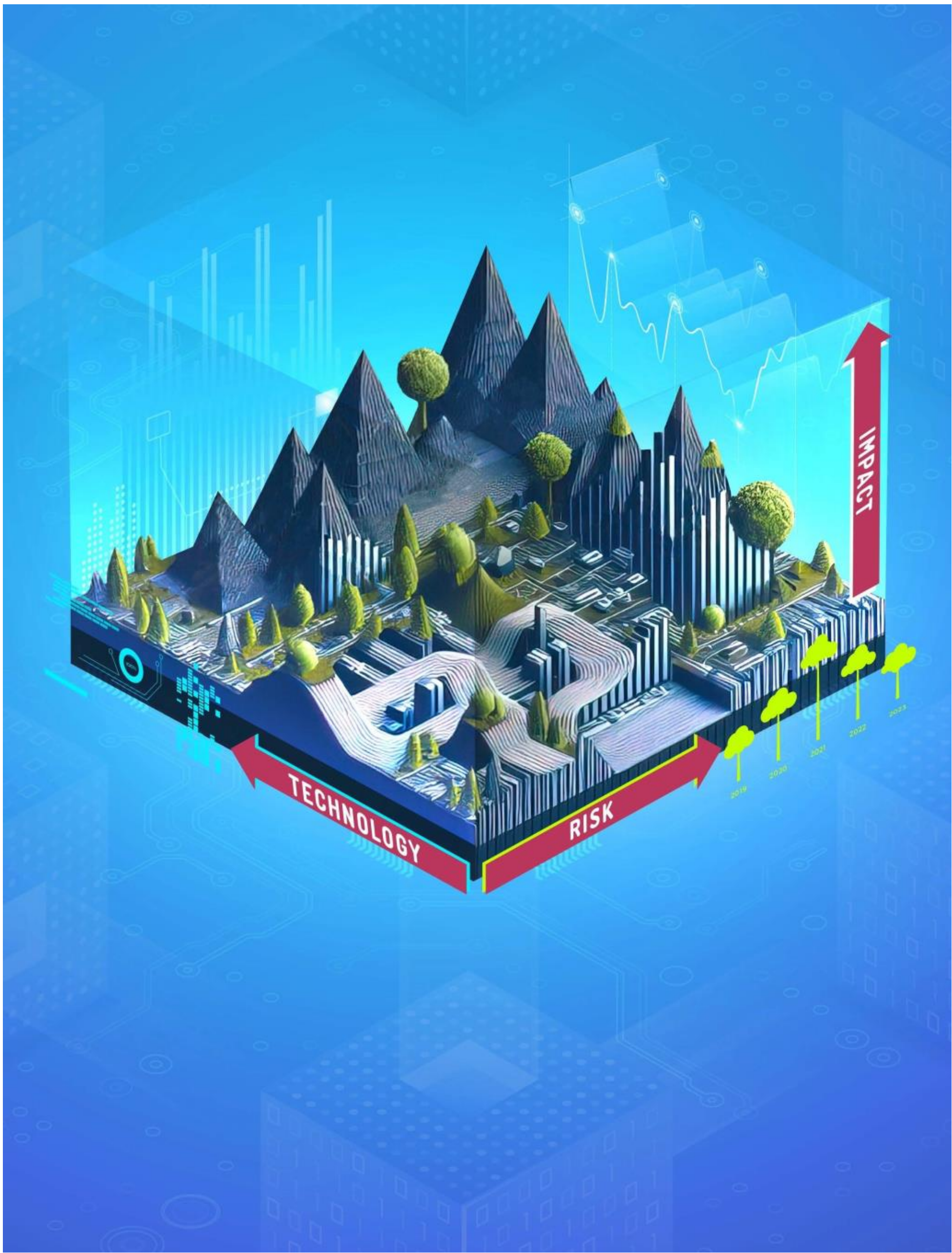
**Proposal for a Digital Wallets Taxonomy**

Institute of Financial Services Zug IFZ
www.hslu.ch/ifz

Swiss Banking

Swiss Stablecoin AG

ti&m



FH Zentralschweiz

# Contents

1 Introduction 2

2 Definition of Digital Wallets 3

3 Taxonomy and Service Architecture 5

4 Digital Wallets and Payments 8

5 Digital Wallets and Open Banking 11

6 Digital Wallets and DeFi 14

7 Digital Wallets and e-IDs 16

8 Regulation and Supervisory Framework Conditions 18

9 Conclusion and Outlook 20

References 22

# 1. Introduction

A few years ago, carrying a physical wallet or purse was an essential part of daily life, holding everything from cash and credit cards to identification documents and receipts. Today, however, mobile phones have increasingly taken over this role (and more), driven by the digital transformation of the economy. With the rise of digital wallets, many items that were once required in physical form can now be securely stored on a mobile device. This shift has not only changed how we manage our finances and personal information, but also how we interact with the digital economy at large. In Switzerland, this transition is exemplified by the emergence of mobile payments in comparison to cash transactions. A survey by the Swiss National Bank (2023) indicates a significant increase in payment transactions using mobile payment apps, often referred to as digital wallets for their role in managing payment instruments, much like traditional physical wallets, over recent years. Specifically, 68 percent of respondents were using such solutions in 2022, up from 48 percent in 2020 (Swiss National Bank, 2023). This shift towards digital wallets is part of a broader global trend. A study conducted across five countries (Brazil, France, Germany, the UK, and the US) found that nearly 90 percent of consumers are familiar with digital wallets (PYMNTS Intelligence, 2024).

The growing importance of digital wallets is driven by technological, social, and legal changes. For example, advances in open finance and open banking, i.e., the opening of interfaces by financial service providers, allow digital wallets to support services beyond their initially intended payment functions, such as investments, insurance, and pension funds. Moreover, digital wallets are becoming increasingly popular outside the area of banking and financial services. The rise of digital assets, both Distributed Ledger Technology (DLT)-based and those using traditional technologies, necessitates new solutions for their storage and management. Digital wallets can provide such solutions, storing digital data like event tickets, public transport tickets, certificates, and electronic identities whilst governing their use. Legal and regulatory requirements are crucial for the expansion of digital wallets, as they can either promote or hinder the growth and innovation of digital wallets. A notable Swiss example is the introduction of electronic identities (e-IDs) under the Federal Act on Electronic Identity Credentials and Other Electronic Credentials (E-ID Act). In September 2024, the Swiss Parliament made significant progress towards introducing a national e-ID, with both chambers approving the necessary legislation and funding, though differences remain regarding data protection and cyber security. The government-backed e-ID is now scheduled to launch in 2026 (The Swiss Parliament, 2024), along with a digital wallet issued by the federal government designed to securely store and manage the corresponding data for authentication.

The increasing adoption of digital wallets in everyday activities raises several questions, which this study seeks to explore: How do the various wallet types differ? Which use cases do wallet solutions promote? And ultimately: Will a single digital wallet dominate the market, or will we see an ecosystem of different wallet infrastructures evolve?

To answer these questions, a basic understanding of digital wallets and their designs is essential. Despite the increasingly important role of digital wallets, a unified and comprehensive framework remains absent. The taxonomy presented in this study seeks to bring clarity to an increasingly diverse and complex ecosystem. It aims to support users, developers, and regulators by providing a framework helping to understand and navigate the various wallet types, functionalities, and features more effectively.

We would like to thank our partners, the Swiss Bankers Association, Swiss Stablecoin AG, and ti&m AG, who have supported this condensed study financially, as well as in terms of content.

# 2. Definition of Digital Wallets

As stated in Chapter 1, digital wallets initially emerged as digital equivalents of physical wallets, designed primarily for storing and managing payment instruments in a mobile application. As such, the payment functionality to facilitate online and point-of-sale transactions lies at the core of a range of studies on the topic.[1] Since digital payments are linked to the market penetration of smartphones, the term “mobile wallets” is often used instead of digital wallets.[2] Alternatively, some studies also refer to the term “e-wallets” to reflect the nature of purely electronic transactions.[3] In the present report, the term “digital wallet” is consistently used as it encompasses the various forms of this emerging wallet type.

The design of digital wallets has evolved in response to technological advancements and the evolving requirements of the digital economy. Some solutions started incorporating (non-financial) features such as digital loyalty schemes, coupons, and tickets, transforming them into more comprehensive platforms that not only handle payment transactions but also consolidated additional services. Moreover, the opening of banking interfaces has created the opportunity to expand the range of services offered by digital wallets. This can, for example, enable a more fluid interaction with traditional banking systems and improve the user experience through the integration of banking services into their interfaces. In addition, digital wallets are playing an increasingly important role in wealth management as custody and brokerage solutions.

With the advent of the DLT, the scope of digital wallets has expanded further. In addition to traditional digital (financial) assets, digital wallets have extended their focus to the management of DLT-based tokens[4]. The term “crypto wallets” is typically used in this context, emphasising the cryptocurrency-related nature of such solutions.[5] However, since these wallets are designed not only for cryptocurrencies but can also support the tokenisation of a wide range of claims, assets, and rights, they should be viewed as more than just payment wallets. Instead, these crypto wallets function as digital vaults, capable of storing and managing a diverse array of DLT-based crypto assets. Digital wallets are especially crucial in the context of Decentralised Finance (DeFi) since users rely on these tools to interact directly with various DLT-based applications in the absence of intermediaries.

Another relevant development in this context is the discussion surrounding e-ID. An e-ID aims to provide a secure and verifiable way of representing a person’s identity online, potentially incorporating self-sovereign identity (SSI) principles. As governments and private entities increasingly move towards digital operations, the integration of e-IDs with digital wallets is seen as a further step in facilitating seamless and secure online interactions. Moreover, the inclusion of secure, legally recognised electronic signatures within digital wallets significantly enhances the value of these platforms.

As digital wallets continue to evolve in terms of their design and functionality, a universally accepted definition of the term has yet to be established. Given their expanding scope, recent reports have suggested broader, less functionally specific definitions of the term. One of these reports is provided by Mobey Forum (2024), whose definition of digital wallets has been adjusted slightly for the purpose of the present study, and reads as follows:

**A digital wallet is an interface to interact with and manage data and digitised assets securely.**

The definition thus neither limits itself to specific functionalities of digital wallets nor does it restrict the types of digital assets[6] it can manage, and thus does justice to the various developments related to digital wallets.

[1] See, e.g., the study on digital wallet features commissioned by the European Central Bank (Kantar Public, 2023).

[2] See, e.g., the mobile wallets report by Boku & Juniper Research (2021).

[3] See, e.g., the e-wallets report by PwC (2021).

[4] See Ankenbrand, Bieri, and Reichmuth (2024) for a discussion of different token and DLT types.

[5] See, e.g., the crypto assets study by Ankenbrand, Bieri, Kronenberger, et al. (2021).

[6] It should be noted that in this study, the term “digital assets” is used broadly to refer to digital resources managed within digital wallets. However, this may not always be entirely accurate in specific cases, such as payment instruments, identities, or credentials.

However, there is still a research gap identified in relation to the structured classification of the different possible (operational) digital wallet designs under the given definition. In both theoretical and practical discussions, this often leads to confusion regarding the various terminologies used and the general understanding of what digital wallets are, along with their attributes and functions. In the following chapter, a classification framework is proposed in order to establish a common understanding of the subject matter. This framework is detailed in Chapter 3 and discussed in the context of various developments, including payment systems (Chapter 4), open banking (Chapter 5), DeFi (Chapter 6), and e-IDs (Chapter 7).

# 3. Taxonomy and Service Architecture

In this chapter, a comprehensive taxonomy for digital wallets is proposed in order to categorise the vast array of existing and emerging solutions across a spectrum of attributes. A morphological box[1] is chosen as the methodological approach in order to be able to take the multidimensionality of the matter into account. The attributes selected for the taxonomy are based on a thorough analysis of existing reports and operational solutions, as well as practical considerations, aimed at covering the most relevant aspects of digital wallets. The chosen framework is inclusive and flexible, recognising that characteristics for certain attributes are not mutually exclusive, i.e., allowing a single digital wallet to embody multiple characteristics simultaneously. This approach ensures a comprehensive and adaptable framework that can accommodate the evolving nature of digital wallets.

Overall, the taxonomy, displayed in Table 3.1, delineates 18 main attributes of digital wallets, each broken down into possible characteristics. Since some of these attributes and characteristics are not intuitively clear, they are explained in more detail in the following:

**Issuer Governance**: Who provides the digital wallet?
- *Open-Source*: Provided by open-source developers.
- *Single Entity*: Provided by a single organisation.
- *Consortium*: Provided by a group of organisations.
- *Government*: Provided by a governmental body.

**Issuer Legal Status**: What is the issuer's legal classification in Switzerland (in descending order of regulatory oversight)?
- *FINMA-Supervised*: Issuer complies with banking regulation and is supervised by the Swiss Financial Market Supervisory Authority (FINMA).
- *SRO-Supervised*: Issuer only complies with AML-regulation and is supervised by a Self-Regulatory Organisation (SRO).
- *Swiss-Based*: Issuer has a sufficiently close connection to Switzerland for Swiss financial market law to apply (e.g., is legally incorporated).
- *Other*: Issuer operates without formal regulatory oversight in Switzerland.[2]

**Supported Content**: Which content is supported?
- *Transactional*: Assets or data used for regular transactions.
- *Investment*: Assets owned for investment purposes.
- *Utility*: Assets or data that serve a non-financial utility or function.
- *Credentials*: Data for identification and authentication purposes (ephemeral or permanent).

**Service Features**: Which services does the wallet offer?
- *Storage*: Only stores assets or data.
- *Transfer*: Supports transactions and exchange of assets or data between wallets.
- *Authentication*: Supports verification of user identity.
- *Other(s)*: Supports other functionalities.

**Transaction Handling**: How does the wallet manage assets or data during transactions?
- *Pass-Through*: Uses (tokenised) data to securely transmit transaction data without holding or storing assets.
- *Staged*: Manages transactions in two distinct phases, initially acquiring assets from a user's alternative accounts or sources, and then transferring those assets to the recipient.
- *Stored Value Account*: Maintains an asset balance and uses these to directly complete transactions with the receiving party.
- *Other*: Uses alternative methods for handling assets or data during transactions, or does not support transactions involving asset transfers.

**Content Range**: How diverse is the range of contents the wallet can manage?
- *Single*: Supports a single type of asset or data.
- *Multiple*: Supports multiple types of assets or data.

[1] A morphological box is a problem-solving tool that deconstructs a complex issue into its key components. By organising these components into a structured grid, it facilitates the exploration of all potential combinations and solutions.

[2] Note that this does not exclude the wallet from regulation in jurisdictions other than Switzerland. Wallets issued by a governmental body are also included in this category.

Table 3.1: Digital wallets' taxonomy

| Attribute | Option 1 | Option 2 | Option 3 | Option 4 | Option 5 |
|---|---|---|---|---|---|
| **Issuer Governance** | Open-Source | Single Entity | Consortium | Government | |
| **Issuer Legal Status** | FINMA-Supervised | SRO-Supervised | Swiss-Based | Other | |
| **Supported Content** | Transactional | Investment | Utility | Credentials | |
| **Service Features** | Storage | Transfer | Authentication | Other(s) | |
| **Transaction Handling** | Pass-Through | Staged | Stored Value Account | Other | |
| **Content Range** | Single | Multiple | | | |
| **Content Governance** | Self-Custody/SSI | Institutional Custody | SC-Governed | | |
| **Content Technology** | Centralised Database | Local Edge Storage | DLT | | |
| **Interoperability** | Monolithic Solution | Partner-Enabled | Ecosystem-Aligned | | |
| **Authentication** | Knowledge-Based | Possession-Based | Inherence-Based | Behavioural | Other(s) |
| **Signature Rights** | Single | Multi | Threshold | Hierarchical | Other(s) |
| **Privacy** | Data Minimisation | Opt-In Privacy | Shared Data Model | Public Data | |
| **Recovery** | Self-Service | Social | Institution-Assisted | Hardware-Based | No Recovery |
| **Wallet Type** | Mobile | Secured Mobile | Browser | Desktop | Hardware |
| **Programmability** | Non-Programmable | Basic Scripting or APIs | SC-Enabled | Fully Programmable | |
| **End-User Pricing** | Free | Subscription-Based | Service-Based | One-Time Fee | Mixed |
| **KYC Requirements** | No Information | Basic Credentials | Identity Verification | Tiered | |
| **Target Users** | B2B | B2C | B2B2C | | |

**Content Governance**: Who ultimately controls the assets or data held in the wallet?

- *Self-Custody/SSI*: Assets or data held by the user. User is in full control.
- *Institutional Custody*: Assets or data held by an institution. User needs intermediary approval for the transfer.
- *Smart Contract (SC)-Governed*: Assets or data held by a software. User does not have direct control and is subject to smart contract rules.

**Content Technology**: What technology controls the assets or data in the wallet?

- *Centralised Database*: Storage in a single, central repository controlled by a single entity.
- *Local Edge Storage*: Storage directly on the user's device.
- *DLT*: Storage distributed across a decentralised network.

**Interoperability**: Which external systems and services is the wallet designed to work with?

- *Monolithic Solution*: Standalone and non-communicative.
- *Partner-Enabled*: Integration with services from contractual partners.
- *Ecosystem-Aligned*: Compatible within a specific ecosystem.

**Authentication**: What method(s) does the wallet use to authenticate users?

- *Knowledge-Based*: Using information known by the user.
- *Possession-Based*: Using something the user possesses.
- *Inherence-Based*: Based on user's biometric data.
- *Behavioural*: Using behaviour patterns of the user.
- *Other(s)*: Other forms of authentication.

**Signature Rights**: Who can authorise actions?

- *Single*: Single user signature suffices.
- *Multi*: Multiple user signatures required.
- *Threshold*: A threshold of signatures needed for authorisation.
- *Hierarchical*: Signature rights are hierarchical.
- *Other(s)*: Other forms of signature rights.

**Privacy**: What privacy protection mechanisms are in place for users?

- *Data Minimisation*: Only necessary data is collected.
- *Opt-In Privacy*: Privacy options chosen by user.

- *Shared Data Model*: Data shared based on a predefined model.
- *Public Data*: Data is publicly available.

**Recovery**: What recovery options are available for users?

- *Self-Service*: Recovery without third-party involvement.
- *Social*: Recovery through social connections.
- *Institution-Assisted*: Recovery with institutional assistance.
- *Hardware-Based*: Recovery using hardware device.
- *No Recovery*: No recovery options available.

**Wallet Type**: What form does the wallet assume?

- *Mobile*: A wallet app on a mobile device.
- *Secured Mobile*: A wallet app on a mobile device that requires additional (hardware) security (e.g., cryptoprocessor).
- *Browser*: A wallet integrated and accessed through a web browser.
- *Desktop*: A wallet installed and run on a user's computer.
- *Hardware*: A physical device that stores assets, data, or corresponding keys.

**Programmability**: Can the wallet's functions be customised or automated?

- *Non-Programmable*: Not capable of running custom code.
- *Basic Scripting or APIs*: Supports basic scripting or APIs.
- *SC-Enabled*: Smart contract functionality.
- *Fully Programmable*: Full programming capabilities.

**End-User Pricing**: How is the wallet priced for end-users?

- *Free*: No cost for the end user.
- *Subscription-Based*: Regular payment required.
- *Service-Based*: Fees based on specific services used.
- *One-Time Fee*: A single payment required.
- *Mixed*: Different pricing levels.

**Know Your Customer (KYC) Requirements**: What level of KYC is required to onboard the wallet user?

- *No Information*: No KYC information required.
- *Basic Credentials*: Basic identification needed.
- *Identity Verification*: Full identity verification needed.
- *Tiered*: Different levels of KYC depending on functionalities used.

**Target Users**: What is the wallet's targeted user base?

- *B2B*: Wallet for businesses.
- *B2C*: Wallet for private individuals.
- *B2B2C*: Wallet for businesses to facilitate interaction with consumers.

In the following chapters, the practical applicability of the taxonomy is demonstrated through examples from four selected areas of digital wallet use, i.e., payments (see Chapter 4), open banking (see Chapter 5), decentralised finance (see Chapter 6), and electronic identities (see Chapter 7).

# 4. Digital Wallets and Payments

The rising popularity of digital payment systems, accelerated by the COVID-19 pandemic, has reduced the importance of cash (The Federal Council, 2022). This has also increased the importance of digital wallets, which, despite their constantly expanding range of functionalities, often retain the facilitation of payments as their central feature.[1] An example of a mobile payment wallet is Google Pay. This wallet is used as a classification example (see Table 4.1) in order to demonstrate the practicability of the taxonomy.

Google Pay is a digital wallet managed by Google (*Single Entity*), which oversees its operations and policies. The wallet functions internationally and with Google Switzerland GmbH, the provider has a legal entity present in Switzerland (*Swiss-Based*). Google Pay primarily supports payment methods. More precisely, users can register credit and debit payment instruments in the wallet, enabling them to make everyday payments (*Transactional*). Furthermore, selected features such as loyalty points and gift cards are also supported (*Utility*), indicating it covers a range of assets (*Multiple*). From a functional perspective, the wallet enables the safekeeping (*Storage*) and exchange (*Transfer*) of assets. Primarily, it facilitates payment transactions by passing encrypted information on the user's payment instrument between the issuer and the recipient (*Pass-Through*). Google Pay runs its own secure management system, but the actual financial assets are held in custody by third parties such as banks and credit card companies (*Institutional Custody*), rather than by Google Pay directly. While Google Pay manages transaction data and user information within its infrastructure (*Centralised Database*), the tokenised payment details are securely stored locally on the user's device (*Local Edge Storage*). Google Pay's services are enhanced through partnerships with various banks, financial institutions, and other contracting parties (*Partner-Enabled*). User authentication can be achieved through a PIN or password (*Knowledge-Based*), the possession of a specific device (*Possession-Based*), and/or biometric methods such as fingerprint recognition (*Inherence-Based*). The authorisation of transactions requires the signature of an individual user (*Single*). With regard to privacy, Google

[1] For an in-depth discussion of digital and mobile payment systems, see Stengel and Weber (2024).

Table 4.1: Classification of Google Pay

| Attribute | Option 1 | Option 2 | Option 3 | Option 4 | Option 5 |
|---|---|---|---|---|---|
| **Issuer Governance** | Open-Source | Single Entity | Consortium | Government | |
| **Issuer Legal Status** | FINMA-Supervised | SRO-Supervised | Swiss-Based | Other | |
| **Supported Content** | Transactional | Investment | Utility | Credentials | |
| **Service Features** | Storage | Transfer | Authentication | Other(s) | |
| **Transaction Handling** | Pass-Through | Staged | Stored Value Account | Other | |
| **Content Range** | Single | Multiple | | | |
| **Content Governance** | Self-Custody/SSI | Institutional Custody | SC-Governed | | |
| **Content Technology** | Centralised Database | Local Edge Storage | DLT | | |
| **Interoperability** | Monolithic Solution | Partner-Enabled | Ecosystem-Aligned | | |
| **Authentication** | Knowledge-Based | Possession-Based | Inherence-Based | Behavioural | Other(s) |
| **Signature Rights** | Single | Multi | Threshold | Hierarchical | Other(s) |
| **Privacy** | Data Minimisation | Opt-In Privacy | Shared Data Model | Public Data | |
| **Recovery** | Self-Service | Social | Institution-Assisted | Hardware-Based | No Recovery |
| **Wallet Type** | Mobile | Secured Mobile | Browser | Desktop | Hardware |
| **Programmability** | Non-Programmable | Basic Scripting or APIs | SC-Enabled | Fully Programmable | |
| **End-User Pricing** | Free | Subscription-Based | Service-Based | One-Time Fee | Mixed |
| **KYC Requirements** | No Information | Basic Credentials | Identity Verification | Tiered | |
| **Target Users** | B2B | B2C | B2B2C | | |

Pay only shares data needed to execute a transaction (*Data Minimisation*). However, the virtual credit and debit card numbers stored in the wallet are different from the user's actual credit card number provided, which is known as "tokenisation"[2]. Wallet access recovery can be accomplished by the user independently (*Self-Service*), such as through a password recovery process, or with assistance from the provider (*Institution-Assisted*). The wallet is available on smartphones (*Mobile*) and does not provide interfaces to customise its functions for the end-users (*Non-Programmable*). The use of the wallet is free of charge (*Free*) and the onboarding process only requires basic credentials, specifically a Google account (*Basic Credentials*). Google Pay's target clients are private individuals (*B2C*).

In Switzerland, TWINT is the leading mobile payment platform (Graf, Heim, Stadelmann, & Trütsch, 2024). However, in terms of its core functionality, TWINT operates more as an independent mobile-oriented payment system than as a digital wallet. Specifically, the TWINT app is typically linked directly to the user's bank account with the issuer, classifying it as a debit payment instrument rather than a digital wallet for payments in the stricter sense (Stengel & Weber, 2024). A less typical configuration is when the app is linked to a credit card instead of a bank account. In this case, TWINT can be considered a digital wallet. It is also a wallet for additional applications, such as loyalty schemes.

Given its relevance in Switzerland and widespread adoption, the TWINT app serves as a second example to demonstrate the applicability of the taxonomy for classifying digital wallets, though, as previously mentioned, not all of its functionalities strictly fit the definition of a digital payment wallet. The corresponding classification is presented in Table 4.2.[3]

TWINT, managed by TWINT AG (*Single Entity*), is a member of the "Verein zur Qualitätssicherung von Finanzdienstleistungen (VQF)" SRO, in accordance with the Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA) in the financial sector (*SRO-Supervised*). Using TWINT's digital wallet, users can conduct payment transactions through the direct integration of a partner bank account via a prepaid account top-up for each transaction executed by the

[2] Not to be confused with tokenisation of assets in the context of DLT.

[3] Note that this is a simplified representation, as there is not a single TWINT app. Instead, each issuer, i.e., bank, provides its own application alongside the standalone prepaid app offered directly by TWINT.

Table 4.2: Classification of TWINT

| Attribute | Option 1 | Option 2 | Option 3 | Option 4 | Option 5 |
|---|---|---|---|---|---|
| Issuer Governance | Open-Source | [✓ Single Entity] | Consortium | Government | |
| Issuer Legal Status | FINMA-Supervised | [✓ SRO-Supervised] | Swiss-Based | Other | |
| Supported Content | [✓ Transactional] | Investment | [✓ Utility] | Credentials | |
| Service Features | [✓ Storage] | [✓ Transfer] | Authentication | Other(s) | |
| Transaction Handling | Pass-Through | [✓ Staged] | [✓ Stored Value Account] | [✓ Other] | |
| Content Range | Single | [✓ Multiple] | | | |
| Content Governance | Self-Custody/SSI | [✓ Institutional Custody] | SC-Governed | | |
| Content Technology | [✓ Centralised Database] | Local Edge Storage | DLT | | |
| Interoperability | Monolithic Solution | [✓ Partner-Enabled] | Ecosystem-Aligned | | |
| Authentication | [✓ Knowledge-Based] | [✓ Possession-Based] | [✓ Inherence-Based] | Behavioural | Other(s) |
| Signature Rights | [✓ Single] | Multi | Threshold | Hierarchical | Other(s) |
| Privacy | Data Minimisation | [✓ Opt-In Privacy] | Shared Data Model | Public Data | |
| Recovery | [✓ Self-Service] | Social | [✓ Institution-Assisted] | Hardware-Based | No Recovery |
| Wallet Type | [✓ Mobile] | Secured Mobile | Browser | Desktop | Hardware |
| Programmability | [✓ Non-Programmable] | Basic Scripting or APIs | SC-Enabled | Fully Programmable | |
| End-User Pricing | Free | Subscription-Based | Service-Based | One-Time Fee | [✓ Mixed] |
| KYC Requirements | No Information | Basic Credentials | [✓ Identity Verification] | Tiered | |
| Target Users | B2B | [✓ B2C] | B2B2C | | |

app (*Transactional*), offering flexible options for managing their finances. Beyond transactions, TWINT provides access to specific services such as digital parking payment (*Utility*). This diverse asset range (*Multiple*), encompassing both transactional and utility assets, underscores TWINT's comprehensive approach to enhancing user convenience and (financial) asset management. If a credit card is linked to TWINT, the app functions as a staged wallet (*Staged*). If the prepaid service is used, the wallet acts as a stored value account (*Stored Value Account*). However, the app can also be directly linked to the user's bank account (*Other*), which makes it a debit payment instrument rather than a digital wallet (Stengel & Weber, 2024). TWINT offers the functionality of secure storage through its prepaid service (*Storage*) and facilitates the transfer of assets (*Transfer*), with intermediary control over the assets (*Institutional Custody*) using its own centralised database system (*Centralised Database*). The wallet's functionality is enhanced through integrations with contracting parties like the Swiss Federal Railways and merchants (*Partner-Enabled*). User authentication is multi-faceted, necessitating either a PIN (*Knowledge-Based*), the possession of a device (*Possession-Based*), or a biometric authentication method such as facial recognition (*Inherence-Based*). Transactions are authorised by the individual user (*Single*), ensuring personal control over the process. TWINT allows users to consent to data sharing with third parties (*Opt-In Privacy*). In the case of issues with wallet access, users can reset their access data independently (*Self-Service*) or rely on assistance from TWINT AG for recovery (*Institution-Assisted*). The wallet is designed for mobile use (*Mobile*) and does not offer customisation possibilities for the user (*Non-Programmable*). The fees for TWINT are free for private individuals for payment transactions or are based on the partner functions purchased (*Mixed*). Identity verification is required for compliance with KYC regulations (*Identity Verification*) and the primary targeted users are individual consumers (*B2C*).

In summary. the classification of two digital wallets primarily relevant in payments, Google Pay and TWINT, demonstrates that the proposed taxonomy effectively encompasses the fundamental aspects of digital wallets in the payment sector. This structured framework can serve as a robust basis for comparison when analysing alternative offerings. A comparison of the two classified exemplary wallets shows, for example, that although there is a similarity in terms of the services offered and the types of assets supported, they differ in certain aspects such as, for example, the legal status of the issuer and KYC requirements. Looking ahead, digital wallets are evolving into comprehensive service platforms, incorporating functions such as identification, ticketing, and support for DLT-based assets. This shift is driven by technological progress and changing consumer demands, with enhanced security measures like encryption and biometric authentication improving the user experience. As a result of these developments, digital wallets are expected to play an increasingly significant role in the global economy, reshaping the way we manage assets and conduct transactions.

# 5. Digital Wallets and Open Banking

Digital wallets have evolved significantly from their origin as payment tools to becoming integral components of the broader open finance ecosystem. The advent of open banking regulations (e.g., PSD2 in the European Union) further accelerated this evolution, allowing digital wallets to aggregate financial data from multiple sources, providing users with comprehensive financial management tools. In this context, digital wallets offer a seamless interface for managing various financial services beyond payments, including savings and investments, thereby transforming themselves into multifunctional hubs that give users more control and visibility over their financial activities. This shift reflects a broader trend towards open finance, where interoperability and data sharing create a more inclusive and transparent financial landscape.

A visualisation of the concept of digital wallets in a general framework of financial ecosystems[1] can be found in Figure 5.1. The architecture of open financial ecosystems is composed of several interconnected layers, facilitated by Application Programming Interfaces (APIs). At the top of the architecture is the customer seeking financial services. The *User Interface & Service Provider* layer serves as the interface for interaction and links the user with the providers of financial services. In open financial ecosystems, this function can be performed through digital wallets, which can include various services and products, potentially from different providers. The *Execution & Custody* layer handles the actual execution of services and asset custody. At this layer, a distinction can be made between different forms of open financial ecosystems. More precisely, in open banking, the banks are responsible for the execution of financial services and the custody of assets and provide the balance sheet. In open finance, insurance companies, other financial service providers, and alternative platforms like crowdfunding can assume this role, while in Decentralised Finance (DeFi), the execution and custody are handled via Distributed Ledger Technology (DLT).[2] An interface to the end customer is required, regardless of which entity or technology provides the financial service and custody. This interface can be a digital wallet.

[1] Note that an in-depth discussion of an initial version of the architecture for open financial ecosystems is provided in Ankenbrand, Bieri, Frigg, Grau, and Lötscher (2021).

[2] Note that the role of digital wallets in DeFi is discussed in more depth in Chapter 6.

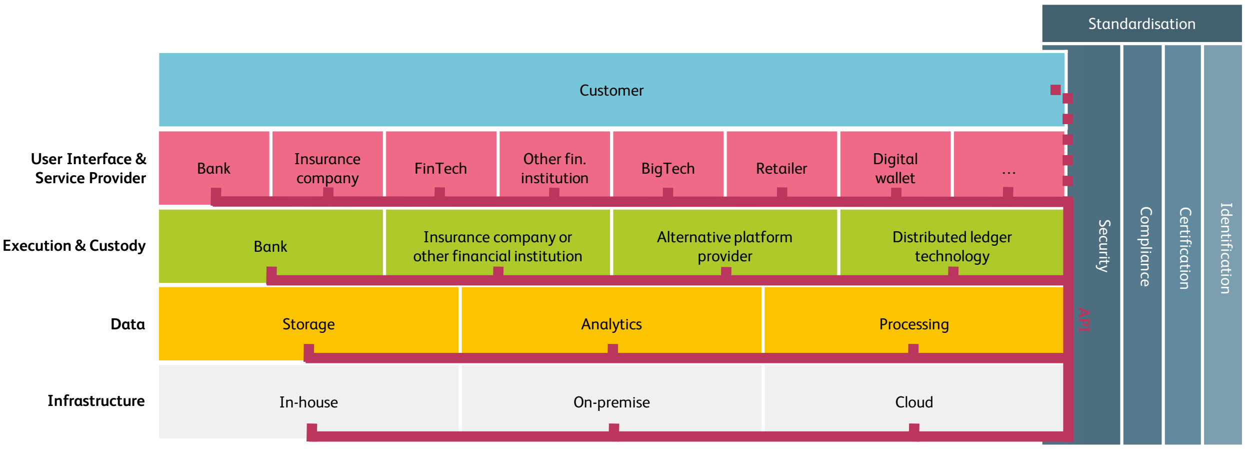


Figure 5.1: Digital wallets in a generalist financial ecosystem framework

Table 5.1: Classification of Revolut

| Attribute | Option 1 | Option 2 | Option 3 | Option 4 | Option 5 |
|---|---|---|---|---|---|
| Issuer Governance | Open-Source | Single Entity | Consortium | Government | |
| Issuer Legal Status | FINMA-Supervised | SRO-Supervised | Swiss-Based | Other | |
| Supported Content | Transactional | Investment | Utility | Credentials | |
| Service Features | Storage | Transfer | Authentication | Other(s) | |
| Transaction Handling | Pass-Through | Staged | Stored Value Account | Other | |
| Content Range | Single | Multiple | | | |
| Content Governance | Self-Custody/SSI | Institutional Custody | SC-Governed | | |
| Content Technology | Centralised Database | Local Edge Storage | DLT | | |
| Interoperability | Monolithic Solution | Partner-Enabled | Ecosystem-Aligned | | |
| Authentication | Knowledge-Based | Possession-Based | Inherence-Based | Behavioural | Other(s) |
| Signature Rights | Single | Multi | Threshold | Hierarchical | Other(s) |
| Privacy | Data Minimisation | Opt-In Privacy | Shared Data Model | Public Data | |
| Recovery | Self-Service | Social | Institution-Assisted | Hardware-Based | No Recovery |
| Wallet Type | Mobile | Secured Mobile | Browser | Desktop | Hardware |
| Programmability | Non-Programmable | Basic Scripting or APIs | SC-Enabled | Fully Programmable | |
| End-User Pricing | Free | Subscription-Based | Service-Based | One-Time Fee | Mixed |
| KYC Requirements | No Information | Basic Credentials | Identity Verification | Tiered | |
| Target Users | B2B | B2C | B2B2C | | |

An operational example of a digital wallet in the context of open financial ecosystems is Revolut, which allows users to link their accounts from various banks, facilitated through APIs. Revolut is a globally operating company (*Single Entity*) offering various financial services. The company is regulated by several authorities globally and, with Revolut (Switzerland) AG, has a legal representation in Switzerland (*Swiss-Based*). The wallet supports a broad array of assets, including fiat money, crypto assets, stocks, commodities, airline miles, and Revolut's own points programme "RevPoints" (*Transactional*, *Investment*, and *Utility*). This wide range of assets indicates the wallet's ability to manage multiple assets (*Multiple*). From a functional standpoint, Revolut provides users with the ability to store (*Storage*) and transact assets (*Transfer*). The wallet enables transactions via the user's Revolut bank account (*Other*), with the assets ultimately held in Revolut accounts under the institution's direct custody (*Institutional Custody*). The wallet infrastructure is centralised, meaning that all data and asset management are handled within Revolut's systems (*Centralised Database*). Revolut has partnerships with banks and third-party providers to extend its services beyond its internal ecosystem (*Partner-Enabled*). User authentication with Revolut is multi-layered, requiring knowledge of, for example, a PIN or passcode (*Knowledge-Based*), possession of the user's device for access (*Possession-Based*), and allowing additional biometric verification (*Inherence-Based*). Authorisations for payments and other actions are done through single-user approval (*Single*). Based on public information, Revolut collects the necessary user data to provide its services, while sharing data with selected third parties (*Shared Data Model*) in accordance with its privacy policy (Revolut, online). For account recovery, users can either use self-service options, such as verifying their identity with a selfie (*Self-Service*), or seek assistance from Revolut's customer support team to regain access to their account (*Institution-Assisted*). The wallet is accessible both through a mobile app (*Mobile*) and web browser (*Browser*). While Revolut provides APIs for partner integration, the wallet itself is not programmable for end-users (*Non-Programmable*). Revolut offers mixed pricing for its services, with free accounts available alongside premium and metal subscription plans (*Mixed*). Identity verification is required for all users, with full KYC processes in place to comply with financial regulations (*Identity Verification*). Revolut's main user base is private individuals (*B2C*), although it also provides services for businesses.

In summary, digital wallets have evolved significantly from their original role as payment tools to become integral components of the broader open financial ecosystem. Open banking has accelerated this shift, enabling digital wallets to consolidate financial data from various sources and offer users a more holistic financial management platform. Revolut illustrates how the proposed taxonomy can categorise these multifunctional digital wallets, which provide access to a range of assets and services. As this trend towards open financial ecosystems continues, digital wallets are set to play an increasingly central role, giving users greater control and visibility over their financial activities and futures.

# 6. Digital Wallets and DeFi

Decentralised Finance (DeFi) employs public DLT networks and smart contracts to build open, transparent, composable, and non-custodial financial protocols (Schär, 2021). It enables peer-to-peer transactions and financial services such as lending, borrowing, trading, and earning interest through smart contracts on decentralised platforms. Digital wallets are essential tools in DeFi as they allow users to store, manage, and transact securely with their crypto assets. These wallets provide the interface for interacting with DeFi applications, enabling users to participate in the decentralised financial ecosystem.

MetaMask is one of the most widely adopted digital (crypto) wallets. It therefore serves as a further exemplary subject for demonstrating the practicability of the taxonomy presented in Chapter 3. The classification of MetaMask across the taxonomy's 18 attributes is detailed in Table 6.1.

MetaMask is a digital wallet with an open-source code base, developed and issued by ConsenSys Software Inc. (*Single Entity*). With ConsenSys AG, the company is also legally represented in Switzerland (*Swiss-Based*). The digital wallet supports a variety of assets, including cryptocurrencies used for payments (*Transactional*), assets held for investment purposes (*Investment*), and assets that provide access to specific services within the blockchain ecosystem (*Utility*). This diverse asset range (*Multiple*) highlights MetaMask's versatility in supporting various types of crypto assets. MetaMask provides essential functionalities such as the secure storage of crypto assets, or, more precisely, corresponding private keys, (*Storage*) and the capability to transfer these assets between users (*Transfer*). By securing users' private keys, the wallet enables them to control and manage their crypto asset balances on the blockchain (*Stored Value Account*). The wallet supports self-custody, allowing users to have direct control over their assets (*Self-Custody/SSI*) without relying on third parties, using DLT for secure and transparent ownership and transaction recording (*DLT*). MetaMask is designed to align with the broader blockchain ecosystem (*Ecosystem-Aligned*), ensuring compatibility with a range of applications and services. User authentication in MetaMask is knowledge-based, using passwords (*Knowledge-Based*) to secure access to the wallet. Trans-

Table 6.1: Classification of MetaMask

| Attribute | Option 1 | Option 2 | Option 3 | Option 4 | Option 5 |
|---|---|---|---|---|---|
| **Issuer Governance** | Open-Source | [✓ Single Entity] | Consortium | Government | |
| **Issuer Legal Status** | FINMA-Supervised | SRO-Supervised | [✓ Swiss-Based] | Other | |
| **Supported Content** | [✓ Transactional] | [✓ Investment] | [✓ Utility] | Credentials | |
| **Service Features** | [✓ Storage] | [✓ Transfer] | Authentication | Other(s) | |
| **Transaction Handling** | Pass-Through | Staged | [✓ Stored Value Account] | Other | |
| **Content Range** | Single | [✓ Multiple] | | | |
| **Content Governance** | [✓ Self-Custody/SSI] | Institutional Custody | SC-Governed | | |
| **Content Technology** | Centralised Database | Local Edge Storage | [✓ DLT] | | |
| **Interoperability** | Monolithic Solution | Partner-Enabled | [✓ Ecosystem-Aligned] | | |
| **Authentication** | [✓ Knowledge-Based] | Possession-Based | Inherence-Based | Behavioural | Other(s) |
| **Signature Rights** | [✓ Single] | Multi | Threshold | Hierarchical | Other(s) |
| **Privacy** | [✓ Data Minimisation] | Opt-In Privacy | Shared Data Model | Public Data | |
| **Recovery** | [✓ Self-Service] | Social | Institution-Assisted | Hardware-Based | No Recovery |
| **Wallet Type** | [✓ Mobile] | Secured Mobile | [✓ Browser] | Desktop | Hardware |
| **Programmability** | Non-Programmable | Basic Scripting or APIs | [✓ SC-Enabled] | [✓ Fully Programmable] | |
| **End-User Pricing** | [✓ Free] | Subscription-Based | Service-Based | One-Time Fee | Mixed |
| **KYC Requirements** | [✓ No Information] | Basic Credentials | Identity Verification | Tiered | |
| **Target Users** | B2B | [✓ B2C] | B2B2C | | |

actions are authorised by the individual user (*Single*), ensuring personal control over the process. MetaMask follows data minimisation principles, collecting only the necessary amount of personal user data required for its operations (*Data Minimisation*).[1] In case of issues with wallet access, users can independently reset their access data using their seed phrase (*Self-Service*). The wallet is available as both a mobile application (*Mobile*) and a browser extension (*Browser*), providing access on smartphones and web browsers. MetaMask supports complex programmable transactions and interactions within the blockchain through smart contracts (*SC-Enabled*) and ensures full programmability due to its open-source code base (*Fully Programmable*). MetaMask is free to use, with no charges for basic wallet functionalities (*Free*), and does not require KYC information, allowing users to operate without providing identity verification (*No Information*). The primary target users for MetaMask are individual consumers (*B2C*).

In summary, digital wallets play an essential role in DeFi by facilitating secure, efficient, and user-controlled access to decentralised financial services. As DeFi platforms, at least conceptually, remove the need for traditional intermediaries, digital wallets act as the critical interface that allows users to interact with these systems. MetaMask, exemplifying the practicality of the proposed taxonomy in this chapter, demonstrates the multiple functions of digital wallets, including secure storage, asset transfer, and programmability through smart contracts.

[1] Note that on a public address level, which is a cryptic identifier, all activities can be viewed transparently in the system.

# 7. Digital Wallets and e-IDs

Electronic identity (e-ID) has become an essential component in the digital landscape, offering a secure and efficient way for individuals to verify their identities in both online and offline environments. This allows for easy access to services and secure authentication in a variety of settings. Digital wallets are increasingly integrating e-IDs, enhancing their role by combining identity verification and digital storage in one platform. Self-sovereign identity (SSI) further transforms the digital identity landscape by granting individuals full control over their own identities. Unlike traditional e-IDs, which are typically managed by centralised authorities, SSI enables users to independently create, manage, and share their identity credentials. This decentralised approach enhances privacy and security by allowing individuals to selectively disclose information, thereby reducing the risk of data breaches. When integrated within digital wallets, SSI offers a seamless and secure experience, combining the security of e-IDs with the autonomy and flexibility inherent in self-sovereign identity.

Estonia is a global leader in digital identity innovation, with 99 percent of its population using the national physical ID card. This card, supporting both contact and contactless systems, forms the foundation of Estonia's e-ID system. It enables citizens to fully participate in the digital economy and governance, offering access to key e-services like online voting, digital signatures, banking, healthcare, and tax submissions (e-Estonia, online-a). Estonia also offers the "Mobile-ID" and "Smart-ID" solutions, which enable authentication via mobile devices. The latter, an app that can be used for authentication like the ID card, has the highest level of recognition in the European Union and enables users to digitally sign documents that are legally recognised in all EU member states (e-Estonia, online-b).

A solution for electronic identities is also being considered in Switzerland, with plans for its implementation set for 2026 (EJPD, 2024). The technological roadmap and current developments of the Swiss Confederation's e-ID programme are transparently recorded by the federal government in a GitHub repository.[1] The primary objective is to meet the demands for strong privacy protection and in-

[1] The repository can be found here.

Table 7.1: Classification of the wallet described in the Swiss E-ID Program

| Attribute | Option 1 | Option 2 | Option 3 | Option 4 | Option 5 |
|---|---|---|---|---|---|
| Issuer Governance | Open-Source | Single Entity | Consortium | [✓ Government] | |
| Issuer Legal Status | FINMA-Supervised | SRO-Supervised | Incorporated | [✓ Other] | |
| Supported Content | Transactional | Investment | Utility | [✓ Credentials] | |
| Service Features | Storage | Transfer | [✓ Authentication] | Other(s) | |
| Transaction Handling | Pass-Through | Staged | Stored Value Account | [✓ Other] | |
| Content Range | [✓ Single] | Multiple | | | |
| Content Governance | [✓ Self-Custody/SSI] | Institutional Custody | SC-Governed | | |
| Content Technology | Centralised Database | [✓ Local Edge Storage] | DLT | | |
| Interoperability | Monolithic Solution | Partner-Enabled | [✓ Ecosystem-Aligned] | | |
| Authentication | Knowledge-Based | [✓ Possession-Based] | Inherence-Based | Behavioural | Other(s) |
| Signature Rights | [✓ Single] | Multi | Threshold | Hierarchical | Other(s) |
| Privacy | [✓ Data Minimisation] | Opt-In Privacy | Shared Data Model | Public Data | |
| Recovery | [✓ Self-Service] | Social | Institution-Assisted | Hardware-Based | No Recovery |
| Wallet Type | Mobile | [✓ Secured Mobile] | Browser | Desktop | Hardware |
| Programmability | [✓ Non-Programmable] | Basic Scripting or APIs | SC-Enabled | Fully Programmable | |
| End-User Pricing | [✓ Free] | Subscription-Based | Service-Based | One-Time Fee | Mixed |
| KYC Requirements | [✓ No Information] | Basic Credentials | Identity Verification | Tiered | |
| Target Users | B2B | [✓ B2C] | B2B2C | | |

ternational interoperability. However, as no single technology currently meets both requirements, the Swiss Federal Department of Justice and Police (EJPD) is considering a strategy that supports multiple technologies simultaneously and plans to propose a concrete plan, including initial formats and cryptographic standards for the e-ID, to the Federal Council by the end of the year.

One of the most discussed aspects in this regard is the so-called “holder binding”, i.e., the method by which an e-ID is securely linked to its rightful owner. Holder binding ensures that the electronic identity is not only issued to the correct individual, but also that it can only be used by that specific person. This is crucial for preventing identity theft and unauthorised access to sensitive information. The current proposal accomplishes this by using a cryptoprocessor, meaning e-IDs are only issued to mobile devices that have the federal wallet installed and are equipped with the necessary hardware capabilities.

Based on the information sourced from the tech roadmap on GitHub as of the end of August 2024, as well as the official website of the Swiss e-ID programme[2], the planned design for the e-ID wallet is classified in Table 7.1, using the taxonomy introduced. It is important to note that the precision of information regarding the assessed attributes varies. Therefore, the classification is partially derived from the most intuitive interpretation of the available data.

The wallet outlined in the Swiss government’s e-ID programme is issued by the government (*Government*), ensuring compliance with national identity management regulations and standards. As such, the issuer’s legal status can be defined as a sovereign entity (*Other*). The wallet supports credential assets (*Credentials*) exclusively (*Single*), focusing solely on authenticating user identities (*Authentication*) without facilitating any asset transactions (*Other*). With regard to the governance of the credentials, a self-sovereign identity approach is pursued (*Self-Custody/SSI*), enabled by the decentralised data storage on the individual user’s device (*Local Edge Storage*). The wallet is intended to be generally compatible with European Union systems and other digital identity frameworks (*Ecosystem-Aligned*). However, the decision on how to balance interoperability with the goal of preserving unlinkability has not been finalised. The e-ID can only be used by owning the linked, secured mobile device (*Possession-Based*), presumably in combination with other, as of yet unspecified authentication methods. The wallet is specifically designed to serve individual users (*Single*) and the data minimisation principle underscores the commitment to data privacy (*Data Minimisation*), ensuring that only the necessary user data is processed. The e-ID can only be recovered if the device to which it was issued is still available, meaning the corresponding keys are still present to the user (*Self-Service*). Otherwise, a new e-ID must be requested. The wallet is mobile-based but requires a device with a cryptoprocessor for enhanced security (*Secured Mobile*), and it does not support any customisation options (*Non-Programmable*). It is offered free of charge to encourage widespread adoption (*Free*). Finally, users are not required to provide information in order to access the federal wallet (*No Information*), as the wallet can also be used without an e-ID for various other credentials, and specifically targets private individuals (*B2C*).

In summary, the integration of digital wallets and e-ID systems is a significant step in enhancing secure identity verification. Estonia’s established e-ID system demonstrates the benefits of a comprehensive digital identity framework. Meanwhile, Switzerland’s planned e-ID aims to balance privacy, security, and interoperability. While challenges remain, the development of these systems highlights the growing importance of secure, user-centric identity solutions in the digital age. The classification of the corresponding federal wallet shows that the taxonomy presented in this study can also cover such wallet designs.

[2] See https://www.eid.admin.ch/.

# 8. Regulation and Supervisory Framework Conditions

The regulation applicable to a digital wallet depends largely on its design and functionality. In Switzerland, digital wallets offering payment services (see Chapter 4) may be subject to various regulations, although there is no specific law for digital payment systems. Instead, the regulatory framework is based on various legislation, such as the Financial Market Infrastructure Act (FinMIA)[1], the Banking Act (BA)[2], and the Anti-Money Laundering Act (AMLA)[3]. These have been amended several times in recent years in order to take technological developments into account.

Under the FinMIA, payment systems are not required to obtain a licence unless they are classified as systemically important and are not operated by a bank. Future revisions could introduce specific authorisation thresholds. The Swiss BA stipulates that wallets accepting deposits may need to obtain a banking licence if public deposits exceed CHF 100 million. If public deposits are below this threshold, a FinTech licence may suffice. Hence, if a wallet handles assets directly or holds balances (i.e., a staged wallet or a stored value account), it may be subject to the BA. In addition, wallet providers may also need to comply with the AMLA, which imposes due diligence obligations, including the identification of contracting parties and verification of ownership of external wallets before processing transactions.

Digital wallets that offer services beyond payment transactions may be subject to alternative regulations. Within open financial ecosystems, the range of services provided by these wallets has expanded (see Chapter 5). In this context, Switzerland pursues a market-driven approach without specific regulation for open banking being imposed by the authorities. Initiatives such as OpenBankingProject.ch[4], Common API[5], or OpenWealth[6] have been established in order to promote this development towards open financial ecosystems. Associations such as SwissBanking and Swiss FinTech Innovations (SFTI) have recognised the potential of this trend and taken a stance on the topic. However, digital wallets in Switzerland may still fall under existing regulations, such as the FinMIA, BA, or AMLA, depending on the services they provide. This market-driven approach contrasts, for example, with the approach pursued by the EU which enforces the opening of bank interfaces, particularly for payment information, with the Payment Services Directive 2[7].

When it comes to digital wallets for managing crypto assets (see Chapter 6), further regulations might become relevant for corresponding providers in Switzerland. The so-called “DLT Act”[8] came into force in 2021, establishing a legal framework for blockchain and DLT-based financial services. This framework aims to provide legal certainty for tokenised assets and introduces a new licence for DLT trading facilities. It also includes amendments to existing laws, such as enabling the segregation of crypto assets in bankruptcy proceedings, which may be particularly relevant for digital wallet providers. The EU adopts a distinct approach to the regulation of crypto assets and related services. Through the Markets in Crypto-Assets Regulation (MiCAR), formalised under Regulation (EU) 2023/1114[9], the EU has established a comprehensive and coordinated regulatory framework for crypto assets and service providers, including those offering custody and administration services on behalf of clients, and therefore may also affect wallet providers. It aims to achieve four key objectives: create legal certainty, enhance consumer and investor protection, foster innovation and fair competition, and address risks to financial stability.

As can already be observed in other countries, the introduction of e-IDs is also progressing in Switzerland (see Chapter 7), with a corresponding regulatory framework being created. The Federal Act on Electronic Identity Credentials and Other Electronic Credentials (E-ID Act)[10] sets the legal framework for issuing e-IDs and establishes the trust infrastructure necessary for their operation. Under this framework, the Swiss government oversees the issuance of e-IDs and provides a corresponding federal dig-

[1] See FinMIA.

[2] See BA.

[3] See AMLA.

[4] See https://www.openbankingproject.ch/.

[5] See https://swissfintechinnovations.ch/projects/common-api/.

[6] See https://openwealth.ch/.

[7] See PSD2.

[8] See DLT Act.

[9] See MiCAR.

[10] See E-ID Act.

ital wallet, while access for third-party wallets remains a topic of discussion.

While the e-ID can be used for authentication, Switzerland also has a legal framework for certification services in the form of the Federal Act on Electronic Signature (ZertES)[11]. This framework is crucial for the development and integration of digital wallets, as they can benefit from the secure and legally recognised electronic signatures enabled by ZertES. By using certified digital signatures, digital wallets in Switzerland offer a secure and convenient method for users to authenticate transactions, sign documents, and access services, thereby enhancing the digital ecosystem. Furthermore, as digital wallets may handle personal data, compliance with the Federal Act on Data Protection (FADP)[12] is required. Compliance with FADP ensures that personal information is protected, mandating digital wallet providers to implement robust data security measures, provide transparency regarding data use, and secure user consent.

In addition to the laws that have been passed, FINMA circulars and guidelines offer further clarity on regulatory requirements for digital wallets. These include, for example, the FINMA Circular 2016/7[13] on video and online identification, which outlines the regulatory framework and guidelines for the remote identification of clients using digital tools, whilst ensuring compliance with anti-money laundering regulations.

Looking ahead, significant legal reforms are on the horizon which are relevant for digital wallet providers in Switzerland. The State Secretariat for International Finance (SIF) is actively working on amendments to financial market legislation aimed at refining the regulatory landscape for innovative business models, particularly those used by FinTech companies and crypto asset providers. A key aspect of this initiative is the review of the “FinTech licence” under Article 1b of the Banking Act, with potential adjustments to better accommodate payment service providers, including stablecoin operators. The reforms will also align with recent international developments in DLT. A consultation bill is expected in 2025, addressing these evolving challenges and building on the initiatives outlined in the “2022+ Digital Finance Report”. The goal is to ensure a robust and progressive regulatory framework that aligns with technological advancements (SIF, 2024). These upcoming amendments are particularly relevant for digital wallets, as they aim to provide a clearer, more supportive regulatory framework for the growing use of digital payment solutions and crypto assets. By modernising the laws surrounding these technologies, the reforms will help ensure that digital wallets can operate securely and efficiently within Switzerland’s financial system.

To summarise, in Switzerland, regulations for digital wallets depend on their specific design and functionality. There are key legal frameworks, along with further clarifying documents provided by FINMA, that guide their operation. As digital wallets evolve, compliance with these diverse regulatory conditions becomes essential for their successful and secure integration into the broader (non-) financial ecosystem. Moreover, upcoming legal reforms, including amendments to financial market legislation, are expected to offer a clearer and more supportive regulatory framework for digital wallet providers in Switzerland (SIF, 2024).

[11] See ZertES.

[12] See FADP.

[13] See FINMA Circular 2016/7.

# 9. Conclusion and Outlook

The key findings of the “Digital Wallets” study can be condensed into the subsequent conclusions and hypotheses. These not only encapsulate the study but also provide an outlook on potential future developments.

**The wide range of digital wallets is complex and difficult to navigate.** The evolution of digital wallets from simple payment solutions to multifunctional product and service platforms has resulted in increasingly complex and diverse designs, making it challenging to maintain an overview of these solutions. The taxonomy proposed in this study, which is based on 18 main attributes, aims to provide a framework for categorising digital wallets in a structured manner. In this way, discussions and analyses of corresponding solutions can be carried out on a uniform basis with uniform terminology. In the study, the taxonomy is applied to selected digital wallets, which emphasises its practicability and added value as a navigation aid.

**Digital wallets are evolving from payment solutions into broader service platforms.** The evolution of digital wallets represents a convergence of technological innovation and changing consumer preferences. From their early beginnings as online payment tools, digital wallets have transformed into sophisticated platforms that play a vital role in the modern financial landscape and everyday life. As technology continues to evolve, digital wallets are poised to further optimise the way we conduct financial transactions, thereby fostering greater convenience, security, and inclusion in the global economy. However, applications are not limited to financial transactions but also include others such as identification or ticketing, and increasingly integrate (DLT-based) assets and services from the digital economy.

**New entrants are breaking up the financial services value chain.** Digital wallets present both an opportunity and a threat to incumbents in the financial services industry. On the one hand, they offer a new touchpoint for customers, facilitating convenient and seamless access to banking services while also creating potential revenue streams. On the other hand, banks face the risk of losing direct control over this touchpoint as third-party providers, such as FinTech or BigTech companies, increasingly mediate interactions between customers and financial services. This shift could not only reduce customer loyalty but also make it easier for customers to switch to alternative financial providers, potentially threatening traditional banking models. Thus, banks must strategically navigate this evolving landscape in order to maintain their relevance and leverage digital wallets for their competitive advantage.

**No wallet to rule them all in sight.** However, users are unlikely to adopt many digital wallets. Instead, they will likely focus on a select few that integrate a range of products and services. The popularity of a wallet will be driven by its convenience, functionality, availability, and cost-effectiveness, among other considerations. Adoption rates will clearly reflect customer preferences, signalling which features and experiences resonate most. For providers, it is crucial to closely monitor market trends, user behaviour, and feedback in order to adapt their services to meet customer demands. Therefore, listening to their users will be key to long-term success in the dynamic market for digital wallets. Furthermore, in Switzerland’s relatively small and saturated market, especially with regard to payment transactions, new entrants in the digital wallets space must carefully assess whether to build stand-alone solutions or integrate with existing platforms to leverage network effects. In an ideal open finance environment, this integration would be built on open standards, promoting interoperability and improving user convenience.

**Regulation is particularly well-established for payment purposes.** Regulations for digital wallets in Switzerland depend on their specific design and functionality. There are key legal frameworks that guide digital wallets’ operations. As digital wallets evolve, compliance with these diverse regulatory conditions becomes essential for their successful and secure integration into the broader (non-) financial ecosystem. Looking ahead, anticipated legal reforms, including updates to financial market legislation, aim to provide further clarity and support for digital wallets, especially in areas related to crypto assets and innovative FinTech solutions (SIF, 2024).

# Authors

This condensed study was prepared in collaboration with the following individuals who contributed in the form of text, discussion, document reviews, and other forms of feedback (in alphabetical order):

## Authors HSLU

**Thomas Ankenbrand**
Head Competence Center Investments

**Denis Bieri**
Lecturer

**Angelo Gattlen**
Research Associate

## Guest Authors

**Andrea Luca Aerni**
Policy Advisor Digital Finance
Swiss Bankers Association

**Christian Bieri**
Chief Executive Officer
Swiss Stablecoin AG

**Johannes Hoehener**
Board Member
ti&m AG

## Contact

For more information about this study, please contact us at:

**Thomas Ankenbrand**
Head Competence Center Investments
Lucerne University of Applied Sciences and Arts
thomas.ankenbrand@hslu.ch

**Nirmala Alther**
Specialist Corporate Communications & Media Relations
Swiss Bankers Association
nirmala.alther@sba.ch

**Pascal Steinmann**
Head Marketing
ti&m AG
pascal.steinmann@ti8m.ch

**Marc Wink**
Head Operations & HR
Swiss Stablecoin AG
marc.wink@swissstablecoin.ch

**Disclaimer**
This document has been prepared to provide general information. Nothing in this document constitutes a recommendation for the purchase or sale of any financial instrument or a commitment by Hochschule Luzern. In addition, this document includes information obtained from sources believed to be reliable, but Hochschule Luzern does not warrant its completeness or accuracy. This also includes the outputs of AI tools, like ChatGPT or DeepL, which were situationally used in the preparation of this document.

# References

Ankenbrand, T., Bieri, D., Frigg, M., Grau, M., & Lötscher, D. (2021). *IFZ FinTech Study 2021. An Overview of Swiss FinTech.* Retrieved 12/01/2022, from https://zenodo.org/records/5109653

Ankenbrand, T., Bieri, D., Kronenberger, T., Lötscher, D., Sardon, A., Schüpbach, C., & Vincenz, D. (2021). *Crypto Assets Study 2021.* Retrieved 30/04/2024, from https://blog.hslu.ch/retailbanking/files/2021/12/IFZ-Crypto-Assets-Study-2021.pdf

Ankenbrand, T., Bieri, D., & Reichmuth, L. (2024). *Crypto Assets Study 2024.* Retrieved 25/09/2024, from https://hub.hslu.ch/retailbanking/wp-content/uploads/sites/7/2024/08/Crypto_Assets_Study_2024.pdf

Boku & Juniper Research. (2021). *Mobile Wallets Report 2021.* Retrieved 29/04/2024, from https://wp-boku-2020.s3.eu-west-2.amazonaws.com/media/2021/09/18175330/2021-Mobile-Wallets-Report.pdf

e-Estonia. (online-a). *e-Identity.* Retrieved 09/09/2024, from https://e-estonia.com/solutions/estonian-e-identity/id-card/

e-Estonia. (online-b). *enter e-estonia.* Retrieved 09/09/2024, from https://e-estonia.com/wp-content/uploads/e-estonia_presentation_pdf.pdf

EJPD. (2024). *E-ID: Further clarifications on technical implementation.* Retrieved 27/08/2024, from https://www.ejpd.admin.ch/ejpd/en/home/latest-news/mm.msg-id-101414.html

Graf, S., Heim, N., Stadelmann, M., & Trütsch, T. (2024). *Swiss Payment Monitor 2024.* Retrieved 05/06/2024, from https://www.zhaw.ch/storage/hochschule/medien/news/2024/Bericht_Swiss_Payment_Monitor_2024-1.pdf

Kantar Public. (2023). *Study on Digital Wallet Features.* Retrieved 29/04/2024, from https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr230424_1_annex~93abdb80da.en.pdf

Mobey Forum. (2024). *Beyond Payments: Navigating the NEXT Generation of Digital Wallets.* Retrieved 29/04/2024, from https://mobeyforum.org/wp-content/uploads/2024/04/Beyond-Payments-Navigating-The-Next-Generation-of-Digital-Wallets.pdf

PwC. (2021). *E-wallets: Accelerating the journey to financial inclusion.* Retrieved 29/04/2024, from https://www.pwc.com/my/en/assets/publications/2021/pwc-e-wallet-accelerating-the-journey-to-financial-inclusion.pdf

PYMNTS Intelligence. (2024). *Digital Wallets Beyond Transactions.* Retrieved 02/10/2024, from https://www.pymnts.com/wp-content/uploads/2024/09/PYMNTS-Digital-Wallets-Beyond-Financial-Transactions-September-2024.pdf

Revolut. (online). *Customer Privacy Notice.* Retrieved 02/10/2024, from https://www.revolut.com/legal/privacy/

Schär, F. (2021). *Decentralized Finance: On Blockchain- and Smart Contract-based Financial Markets.* Retrieved 24/09/2024, from https://www.uni.lu/wp-content/uploads/sites/3/2024/08/Schar-Fabian.pdf

SIF. (2024). *Amendment of financial market legislation with regard to innovative business models of financial institutions.* Retrieved 04/10/2024, from https://www.sif.admin.ch/en/financial-market-legislation-innovative-business-models-financial-institutions

Stengel, C., & Weber, T. (2024). *Digitale und mobile Zahlungssysteme: Kredit- und Debitkarten, Wallets, virtuelle Währungen und Kryptowerte.* Schulthess.

Swiss National Bank. (2023). *Payment Methods Survey of Private Individuals in Switzerland 2022.* Retrieved 26/03/2024, from https://www.snb.ch/dam/jcr:ca671e5a-d0ff-48ca-bf08-f4c5cc57c9d8/paytrans_survey_report_2022.en.pdf

The Federal Council. (2022). *Federal Council adopts report on acceptance of cash in Switzerland*. Retrieved 04/10/2024, from https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-92124.html

The Swiss Parliament. (2024). *Parlament ist sich über Ausgestaltung der E-ID im Grundsatz einig.* Retrieved 11/09/2024, from https://www.parlament.ch/de/services/news/Seiten/2024/20240910100146714194158159026_bsd059.aspx

**Lucerne School of Business**
Institute of Financial
Services Zug IFZ
Campus Zug-Rotkreuz
Suurstoffi 1
6343 Rotkreuz

T +41 41 757 67 67
ifz@hslu.ch
hslu.ch/ifz

**A study conducted by**

HSLU Lucerne University
of Applied Sciences
and Arts

ISBN-Number
978-3-907379-31-8