



The
Big Whale



The Big Whale Report

The future of wallets

WITH THE SUPPORT OF



Dfns

EDITORIAL

THE GATEWAY TO A NEW FINANCIAL WORLD

It's a small digital door that we open with the tips of our fingers, a virtual key capable of projecting us into a universe of innovations. This first contact, often fleeting, with the world of cryptocurrencies happens through a discreet but fundamental object: the wallet. But this wallet, or crypto wallet, is not a simple container; it is the gateway to a thriving ecosystem. In this future where central banks are experimenting with digital currencies and where investing in cryptocurrencies is becoming a mainstream topic, the wallet presents itself as the indispensable pillar of digital and financial life.

But behind this door, what really lies hidden? There is no single model: each wallet is based on a technological approach and user experience that reflect radically different visions of cryptography and decentralization. Between custodial wallets, where the access key remains in the hands of a centralized entity, and non-custodial wallets, where the user alone is master of their assets, a range of choices opens up, offering as many ways to conceive digital ownership and manage interactions with the blockchain.

Added to this is the emergence of «smart wallets», true concentrates of decentralized intelligence, integrating advanced automation and security features that are already redefining the contours of this sector.

As a result, fintechs that intend to offer wallets to their clients find themselves faced with difficult choices: which wallet technology should they rely on to offer an effective, secure product that complies with emerging regulations? The issue is important, because between the United States, Europe, and Asia, legal frameworks are emerging to regulate the use of these digital wallets. However, the path is still strewn with uncertainties: gray areas persist, and debates around privacy, governance, and the storage of private keys are intensifying.

But what we must remember is that behind these innovations lies a colossal market. These wallets have become hubs for exchanges, payments, staking, and investment for millions of users worldwide. From tech giants to startups, players are rushing to impose their solution and capture an audience in search of simplicity, security, and freedom. This sector, which sits at the crossroads of finance and technology, is fueling considerable financial ambitions.

Thus, in the pages that follow, we will explore the possible trajectories of this near future where the crypto wallet, like a modern sesame, will continue to redraw the contours of our relationship with money, data, and trust.

GRÉGORY RAYMOND
Head of Research,
The Big Whale



01 DIFFERENT STORAGE TECHNOLOGIES

02 **CLARISSE HAGÈGE** DFNS « The concept of non-custodial wallet is partly an illusion »

03

WHAT FEATURES FOR
THE WALLET OF THE FUTURE?

table of contents

04 THE ARCHITECTURE OF THE WALLET OF THE FUTURE ACCORDING TO JESSE POLLAK

05 WHICH BUSINESS MODELS?



06 MAPPING THE WALLET ECOSYSTEM

07

PIERRE D'ORMESSON
DLA PIPER

« The distinction is clear:
holding private keys means
being regulated »

08

CLAIRE BALVA DEBLOCK

« The inevitable alliance
of wallets with banks »

09

THE BEST
SMART
WALLETS

10

NICOLAS BACCA

« Passkeys, biometrics, and
MPC technologies contribute
to simplifying the experience »

11

ACKNOWLEDGEMENTS

01

Standards

DIFFERENT STORAGE TECHNOLOGIES



DIFFERENT STORAGE TECHNOLOGIES

01 HARDWARE WALLETS

ADVANTAGES

- Maximum security against online attacks
- Private keys stored offline
- Multi-currency support

Hardware wallets, or physical wallets, are devices specifically designed to store private keys offline, making them highly resistant to cyber attacks. They are considered one of the safest solutions because they are not connected to the Internet.

This means that to sign a transaction, the user must physically connect the device to a computer or smartphone.

DISADVANTAGES

- Less convenient for frequent transactions
- Requires having a physical device with you
- Not well-suited for institutional use

EXAMPLES



LEDGER

KEYSTONE



DIFFERENT STORAGE TECHNOLOGIES

02 HSM WALLETS

ADVANTAGES

- Enterprise-level security, compliant with strict standards (FIPS)
- Total sovereignty of the private key for the company
- Excellent resilience against physical and software attacks
- Relevant for companies and institutions managing large volumes of assets

HSMs (Hardware Security Modules) are specialized hardware devices designed to generate, store, and manage cryptographic keys in an ultra-secure manner. Often used by financial institutions and businesses, they comply with rigorous security standards.

Although they may resemble hardware wallets, HSMs are typically used in more complex and centralized environments, often as part of cloud or enterprise solutions.

DISADVANTAGES

- High installation cost

EXAMPLES



LEDGER
ENTERPRISE



TAURUS

DIFFERENT STORAGE TECHNOLOGIES

03 MPC WALLETS

ADVANTAGES

- Enhanced security through private key division
- More convenient and flexible than hardware wallets and HSM
- Can be suitable for financial institutions and individual users
- More competitive costs than hardware wallets and HSMs

MPC (Multi-Party Computation) wallets are a more recent technology that distributes the management of private keys among multiple parties or devices. No single party possesses the entire key, and to sign a transaction, coordination between the different parties is required.

This model enhances security by making key theft more difficult, while maintaining a certain level of flexibility.

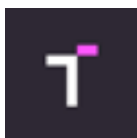
DISADVANTAGES

- Still relatively new technology
- Increased technical complexity
- Regulatory risk: the wallet provider could be recognized as a custodian (as they hold part of the key)

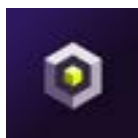
EXAMPLES



FIREBLOCKS



TAURUS



DFNS

FOR
BUSINESSES



ZENGO

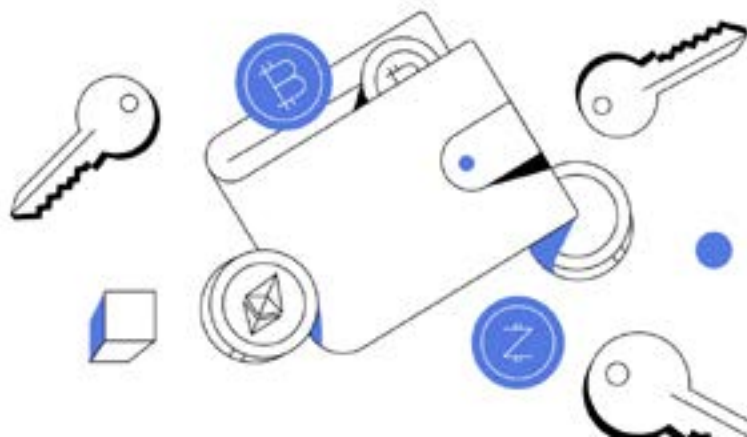


SWISSBORG



DEBLOCK

FOR
INDIVIDUALS



DIFFERENT STORAGE TECHNOLOGIES

04 SMART WALLETS

Smart wallets rely on smart contracts to automate and add advanced features.

Unlike traditional wallets, they allow for automatic interactions with decentralized applications (dApps) and can include functions such as key recovery, spending limits, or scheduled payments.

ADVANTAGES

- Advanced functions like key recovery or multi-signature protection
- Suitable for companies that don't handle many transactions and for individuals
- Can automate certain tasks via smart contracts

DISADVANTAGES

- Often limited to certain blockchains like Ethereum
- Unsuitable for financial institutions that operate numerous flows

EXAMPLES

FOR
INDIVIDUALS



COINBASE
SMART
WALLET

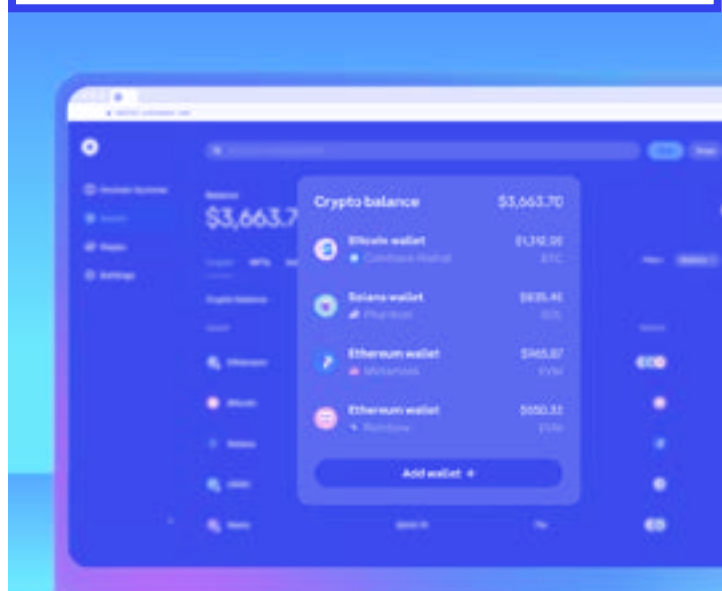


ARGENT
WALLET

FOR CERTAIN COMPANIES
OR DAOs



SAFE



DIFFERENT STORAGE TECHNOLOGIES

05 HOT WALLETS

Hot wallets are online wallets, accessible via web browsers or mobile applications, which are always connected to the Internet.

They are the most convenient for daily use and frequent transactions. However, this constant connection to the Internet makes them more vulnerable to attacks and hacking.

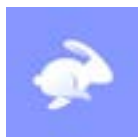
ADVANTAGES

- Ease of use, quick for transactions
- Ideal for interacting with dApps and DeFi
- Multi-currency support

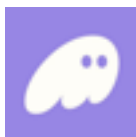
DISADVANTAGES

- High risks of hacking due to permanent Internet connection
- Less secure than hardware wallets (but you can improve the security of a hot wallet by linking it to a hardware wallet)
- Unsuitable for businesses

EXAMPLES



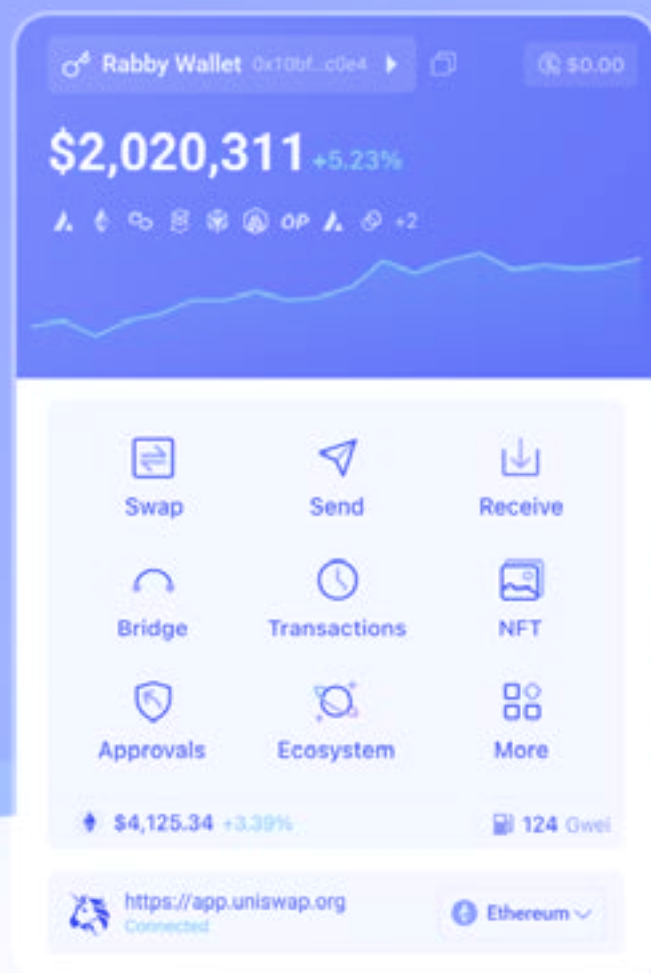
RABBY



PHANTOM



METAMASK



02

Interview

CLARISSE HAGÈGE

« THE CONCEPT OF NON-CUSTODIAL
WALLETS IS PARTLY AN ILLUSION »



ENG
IN



12:43
22-01-2022

CLARISSE HAGÈGE

DFNS

CLARISSE HAGÈGE, CEO OF DFNS, DISCUSSES HER AMBITIONS TO TRANSFORM CUSTODY INFRASTRUCTURE. SHE ALSO ADDRESSES SECURITY ISSUES, REGULATORY CHALLENGES, AND SHARES HER VISION FOR THE WALLET OF THE FUTURE—A SECURE, MODULAR, AND INTEROPERABLE TOOL DESIGNED FOR TOMORROW'S FINANCIAL INSTITUTIONS.

« The concept of non-custodial wallets is partly an illusion »

COULD YOU BRIEFLY TELL US ABOUT THE HISTORY OF DFNS?

Dfns has its roots in my personal journey. I spent a decade in the banking sector, working at Goldman Sachs, Bank of America, and Crédit Agricole from 2008 to 2018, gaining expertise in finance and asset management. During an incubation program at Village by CA in Paris, I met the team at IOV (now Starname), a project similar to the Ethereum Name Service (ENS) but based on Cosmos. I helped them structure their ICO over the summer, but I encountered a recurring issue: crypto adoption by traditional investors was hampered by technical barriers. Many investors were put off by the idea of buying a Ledger Nano and managing cryptographic keys to access their assets, in this case, IOV tokens. Although business meetings were positive, about 90% of discussions stalled when it came to handling hardware wallets and assuming security risks. I noticed a lack of suitable infrastructure for institutional investors who weren't seasoned security engineers or DeFi traders. At the same time, I explored custody solutions based on HSM (Ledger, Anchorage, BitGo) and MPC-based companies (Fireblocks, Curv, Sepior, Unbound). These tools had two major drawbacks: they were exclusively B2C- or B2B-oriented, whereas I believed finance would require a B2B2X solution focused on APIs. Secondly, their key deployment scheme exposed client-users to excessively high security risks. Convinced that blockchain would ultimately transform the financial sector, I decided to focus on creating a modular infrastructure

that would enable fintech developers, startups, and established financial institutions to launch their projects quickly and operate on multiple blockchains without delaying time-to-market, relying on proven technology capable of supporting their growth seamlessly. Dfns was officially founded in Paris in August 2020, following an exploration phase that began in 2019.

WHAT IS THE VOLUME OF ASSETS YOU CURRENTLY MANAGE AND SECURE?

We don't disclose AUM (Assets Under Management) to prevent competitors from drawing strategic insights. However, we are transparent about our monthly transaction volume, which currently exceeds \$980 million. This trend is recent, as until July 2024, we handled around \$150 million per month. This increase is due to new clients, the boom in stablecoin payments worldwide, and the growing adoption of our infrastructure by companies and banks seeking to automate and secure their operations at scale.

HOW DO YOU DIFFERENTIATE YOURSELF FROM COMPETITORS LIKE FIREBLOCKS?

Our distinction lies in our API-centric programmable approach. From the outset, we bet on a model similar to Algolia or Stripe, providing developers with tools to build blockchain applications easily and quickly. In contrast, Fireblocks initially developed a user interface for traders and funds that needed a manual wallet experience.

CLARISSE HAGÈGE

DFNS

They only introduced APIs later, and these remain significantly limited compared to ours. At Dfns, every feature is available via API, enabling teams to develop large-scale services with automation and configurability. For example, our "Wallet Entitlement Management (WEM)" system for wallet and transaction rights management is fully automatable. It allows setting permissions and access controls based on roles (auditor, approver, trader, account manager, etc.), transactional rules and variables (amount limits, frequency, anti-siphoning rules, whitelisting, etc.), as well as webhook-based conditions (e.g., if an address receives 100,000 USDC, the wallet is locked from any further fund outflows). We are the only provider offering this level of programmatic customization, a real asset at a time when regulation is tightening, and risks associated with cryptocurrencies are increasing along with their value. Our infrastructure is also gaining recognition for its high modularity. We allow clients to deploy their own instances on public clouds like AWS, private clouds, and connect their Thales or IBM HSMs to our blockchain transaction management system. This facilitates compliance with security departments, financial market authorities, and local regulators. Blockchain is not meant to overturn financial institutions or challenge decades of best practices in security and logic. It aims to improve existing processes. At Dfns, we are careful to understand the needs of financial players we work with, as their business logic is valuable. Our goal is to interface with these processes to streamline back-office and middle-office work. Lastly, we have adopted a usage-based pricing model, similar to AWS, rather than transaction volume or AUM-based fees, making our solutions better suited to the actual needs of financial institutions, payment solutions, token issuance platforms, and trading applications that rely on such solutions as a revenue source.

« At Dfns, every feature is available via API, allowing teams to develop scalable services with automation and configurability. We are the only provider offering such programmatic customization on the market »

HOW DOES MPC TECHNOLOGY WORK AT DFNS? WHAT ARE ITS ADVANTAGES?

Multi-Party Computation (MPC) is at the core of our key management solution offered as SaaS. This technology divides a key into several fragments, generated and stored in distinct locations. These fragments enable the creation of partial signatures without ever reconstructing the full key. Thus, even if some fragments are compromised or lost, the system can continue functioning using a validation threshold, for example, 2 out of 3 fragments. This reduces the risk of contagious human error and enhances security against internal or external attacks. MPC also ensures a higher level of service availability by fragmenting and providing contingency for sensitive assets like private wallet keys.

GIVEN THAT MPC FRAGMENTS A PRIVATE KEY INTO MULTIPLE PIECES AND THAT YOU KEEP ONE, HOW DO YOU SEE THE RISK OF BEING REGARDED AS A CUSTODIAN?

To answer in detail whether Dfns's key management solution could be seen as a financial custody service, it's crucial to clarify the legal criteria around custody, which vary by jurisdiction.

CLARISSE HAGÈGE

DFNS

In France and the European Union, the concept of digital asset custody has evolved through legislative debates, notably to exclude certain players like Ledger. Initially, the regulation included storing cryptographic private keys within the custody definition, but the French Parliament adjusted this definition to no longer equate simple key storage with a financial custody service. In a 2020 document, the AMF specifies that custody now includes not only physical possession of keys but also “control of access means” to assets under a contractual relationship. The AMF adds that an API could be seen as an access means if it provides effective control over the client’s assets. Therefore, although in some configurations, Dfns may host certain key fragments or even all fragments in its storage environments, the company neither has the ability to use these fragments independently to execute transactions nor the contractual right to do so. These two points are essential to distinguish Dfns from a qualified custodian of digital assets. Dfns is primarily a cybersecurity

company subject to rigorous audits by external controllers such as Deloitte or KPMG to verify our claims about internal processes and technology. We are obligated to describe precisely how Dfns operates and to meet hundreds of controls as part of recognized certifications, such as SOC 2, DORA, ISO 27001, ISO 27017, and ISO 27018. Our security relies notably on requiring each employee to cryptographically sign in using a Yubikey to access certain services and perform sensitive actions, often with additional approvals from separate individuals. If an employee were to make an error or commit a malicious act, this would not only be detected thanks to audit logs and monitoring systems, but legal action would also be taken to identify and prosecute the perpetrator in collaboration with law enforcement. Additionally, our insurance policies help cover potential damages. That said, the aspects I have discussed are related to the technical and legal security of a key management solution, which Dfns sometimes administers entirely or partially (or which Dfns delegates to the client when they choose to manage the keys themselves, which is mandatory in the UAE or Hong Kong, for example). However, the strategic and financial management of digital assets remains strictly the responsibility of a qualified custodian, a role distinct from Dfns’s role.

HOW DO YOU RESPOND TO CRITIQUES REGARDING THE LACK OF MATURITY IN THIS TECHNOLOGY?

All technologies, even the most mature, have vulnerabilities. Hardware solutions, even FIPS-certified ones, are regularly hacked and exposed as flawed at cybersecurity conferences (e.g., CVE-2023-3470 is a vulnerability discovered in 2023 in some F5 BIG-IP platforms equipped with Cavium Nitrox FIPS HSM cards). However, the cryptography behind MPC relies on several decades of research, and we are actively involved in its standardization.



CLARISSE HAGÈGE

DFNS

We have been members of the MPC Alliance board for three years and are working with the National Institute of Standards and Technology (NIST) on threshold signature standards. Three of the five papers selected by NIST in 2023 for their MPC workshops came from our research teams. While secure multi-party computation (MPC) is still being adopted in traditional finance, it is already widely used in crypto finance, with over 2,000 companies and millions of users benefiting from this technology to protect their digital assets. We believe it's only a matter of time before MPC becomes a universal standard, especially in combination with secure enclaves (TEE) and hardware security modules (HSM). However, if a client tells us that they don't want or can't use MPC for key security, often for regulatory or compliance reasons, it's not our role to defend this technology at all costs. We fully respect that choice. On the contrary, we are pleased to work closely with Thales (with whom we are incubated at Station F), IBM, Securosys, Yubico, and other HSM providers, as we are partners and resellers.

WHAT TYPES OF CLIENTS AND USE CASES DO YOU TARGET?

Our infrastructure operates in various fields of digital finance and blockchain. In the banking and regulated digital asset custody sector (or "qualified custody"), we provide wallet infrastructure to major players like Zodia Custody (the crypto subsidiary of British bank Standard Chartered), Tungsten Custody (the crypto subsidiary of Abu Dhabi's sovereign wealth fund, ADQ) in the UAE, ABN AMRO, Fidelity International, and Eastern Point Trust in the United States, which handles fund administration for Amazon, British Petroleum, or General Motors. We are also very active in the payments sector, where many companies are innovating around stablecoins. We provide wallets and blockchain connectivity for players like Bridge (recently acquired by Stripe), Triple-A (Grab's crypto

payment service), Sphere (behind Helium), and Vita, which allows over 500,000 users in South America to make crypto payments at low cost. These collaborations support the development of cross-border and stablecoin-based payment solutions. Tokenization is another important area of our business, where we work with specialized companies like Tokeny, Bitbond, Nomyx, Zoniq, Assetblocks, and others to tokenize financial assets. In trading and exchanges, we are proud to provide the technological infrastructure of Canada's largest exchange, NDAX, and a decentralized exchange (DEX) in Singapore called GRVT, based on the ZkSync blockchain. Finally, we are also entering the emerging integrated wallet market, providing "non-custodial" wallet infrastructure to players like Socios, Billy, and FIFA to integrate wallets directly into their platforms.



WHAT IS YOUR POSITION ON WALLET EVOLUTION AND ACCOUNT ABSTRACTION?

We have closely followed account abstraction developments since EIP 4337 was released in the summer of 2023. Although we are not smart contract developers, we work with players like ZeroDev, Biconomy, and Safe, and have integrated our digital signature services into their smart contracts to allow our clients to experiment with

CLARISSE HAGÈGE

DFNS

« Rather than focusing on the ideological battles of the blockchain industry, we should think about how to encourage broader adoption by addressing concrete commercial and utility needs. »

these new features exclusive to Ethereum and EVMs. It's now clear that Account Abstraction via ERC 4337 has not achieved the expected success, with recent usage and revenue figures (cf. Dune Analytics and BundleBear Review) being particularly disappointing. Many clients return from this experiment frustrated, often concluding, "not everything can be on-chain." Currently, it's too costly, slow, and risky, but this may change in the coming years. That's why we remain vigilant and closely monitor upcoming technical advances. Another major argument against using blockchain for all operations is the need for confidentiality. A bank cannot consider making its collateral movements public in real-time, as this would not be allowed by financial regulatory authorities and could even pose a significant risk to global financial stability. There are initiatives like the Canton Network, aimed at providing a public and confidential network, but there is still much work to be done before we see a consensus-building project emerge. In any case, in the future, wallets will need to be fast, interoperable, and compliant with local regulations, while integrating advanced features to ensure transaction security and fluidity.

This will be done off-chain if it cannot be done on-chain. By the way, we believe that the ideological debates and political quarrels that sometimes clutter the blockchain industry detract from its real commercial potential and practical utility for the masses. Instead of dwelling on them, we should all consider how to encourage broader adoption of this technology.

WHAT ARE YOUR THOUGHTS ON NON-CUSTODIAL WALLETS IN TODAY'S REGULATORY CONTEXT?

Unfortunately, we inherit more than a decade of language misuse that blurs understanding of the underlying technical realities, making it harder to clearly grasp security and operational issues related to "custodial" and "non-custodial wallets." Adding to these terms are expressions like "self-custodial," "co-custodial," "cold storage," "hot wallets," and other temperature-based designations. This proliferation of terms makes it difficult for regulators, legislators, and financial players who try to navigate an industry that uses words freely, often without understanding, to describe realities that may not be. That's why we oppose many of these terms, practices, and those who promote them. Above all, we believe it is crucial (and urgent) to distinguish technical aspects from legal aspects. The crypto industry tends to equate the term "custodial" with simply holding the private key. But what does "owning the key" really mean? Some would say it's simple: the key is mine as long as I can find it on my Metamask wallet. However, this private key often resides in the user's browser, be it Chrome or Safari, which belongs to Google and Apple, with potential access for their employees. How can we talk about "ownership" if the only criterion is technical access to the data? The truth is, we can't define it satisfactorily. That's why the term "custodial" must first be understood and defined from a contractual and regulatory perspective, as this is the only way that allows owners to seek justice when a dispute arises or an error is made.

CLARISSE HAGÈGE

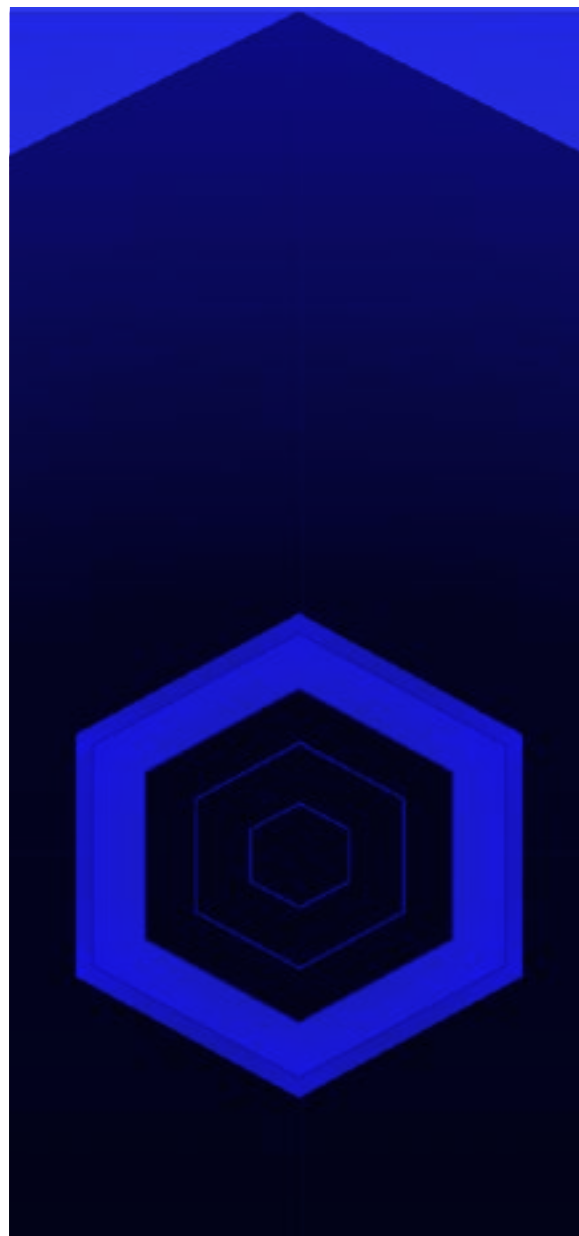
DFNS

Let's not for a second think that blockchain's purpose is to end the rule of law; that would be a major misjudgment in our view.

Sure, the technical aspects are important and far from being neglected, but at Dfns, we refer to the regulatory framework of each country to determine what is "custodial" or not. Instead, we prefer to talk about "user-controlled" or "organization-controlled" wallets.

WHAT WILL THE WALLET OF THE FUTURE LOOK LIKE?

The wallet of the future will not just be about who designs the best interface and will inevitably take many forms adapted to different sectors and regulatory situations. The needs of interbank payments differ widely from those of microtransactions in gaming or the remuneration of freelancers internationally. Wallets will need to be interoperable, fast, and low-cost. They will also need to comply with local laws and integrate with existing systems, including private banks, transfer agencies, clearinghouses, central banks, and governments. Finally, we believe that the future of wallets rests on a complex and intelligent aggregation of services where each component (KYT, market data, key storage, governance, smart contracts, exchanges, RPC node, etc.) plays a critical role in the end-to-end management and security of financial transactions across different blockchains.



03

Features

WHAT FEATURES
WILL THE WALLET
OF THE FUTURE
OFFER?



WHAT FEATURES WILL THE WALLET OF THE FUTURE OFFER?

ACCOUNT ABSTRACTION

Simplifying signatures

Current wallet users often need to manually sign each transaction, which can be tedious. With account abstraction, the need for manual signatures on every transaction will be eliminated.

This feature allows many actions to be automated, making the user experience smoother and less technical. Users can set rules or automatic authorizations, enabling the wallet to perform certain operations without requiring a signature for each transaction. This makes the wallet more intuitive, especially for frequent interactions with smart contracts.

PASSKEYS

Simplified security

Passkeys offer a futuristic replacement for passwords and private keys, combining simplicity and security. Instead of storing a complex private key, passkeys allow the use of biometric authentication methods (fingerprint, facial recognition) or secure tokens to access the wallet. This technology can make wallet management much simpler while enhancing security. No more forgotten passwords or lost keys—users will be able to access their wallets quickly and securely.

SOCIAL RECOVERY

A trusted network for recovery

Social recovery offers a solution to the problem of irrecoverable wallets in case of private key loss. With this system, users can designate trusted contacts, like friends or family members, to help them regain access to their wallet if they lose access. Instead of relying solely on personal security, the wallet could be restored through validation by a predefined social network. This feature adds a layer of resilience in case of loss or compromise of access methods.



WHAT FEATURES WILL THE WALLET OF THE FUTURE OFFER?

GAS FEE SPONSORSHIP

Reducing friction for users

Blockchain transactions require gas fees, which can sometimes be a barrier for users. In the wallet of the future, certain applications may sponsor these fees, eliminating the need for users to constantly manage their native token balances to pay these fees. For example, a decentralized finance (DeFi) application could cover transaction costs to offer users a smoother experience. This would encourage broader adoption, particularly among users unfamiliar with blockchain mechanics.

ABSTRACTION OF DIFFERENT BLOCKCHAINS

In the future, wallets will need to be able to mask the complexity of underlying blockchains. Users should not have to worry about which blockchain a transaction is conducted on (Ethereum, Solana, etc.). The wallet of the future would incorporate seamless interoperability between different blockchains, providing a unified experience where users can send funds or interact with decentralized applications without needing to consider the specific blockchain used. This blockchain abstraction would foster better Web3 adoption, as users would face fewer technical obstacles.

CLEAR TRANSACTION STATEMENTS FOR TAX ADMINISTRATION

Today's users often need to navigate complex interfaces to obtain transaction statements they can submit to tax authorities. The wallet of the future will provide simple, accessible, and detailed statements, automatically formatted for tax filing. This would include clear summaries of gains, losses, and fees, making it easier for users to comply with tax obligations. Such a feature would enhance transparency and offer users better administrative management of their crypto portfolios.



04

Perspectives

THE ARCHITECTURE OF THE WALLET OF THE FUTURE

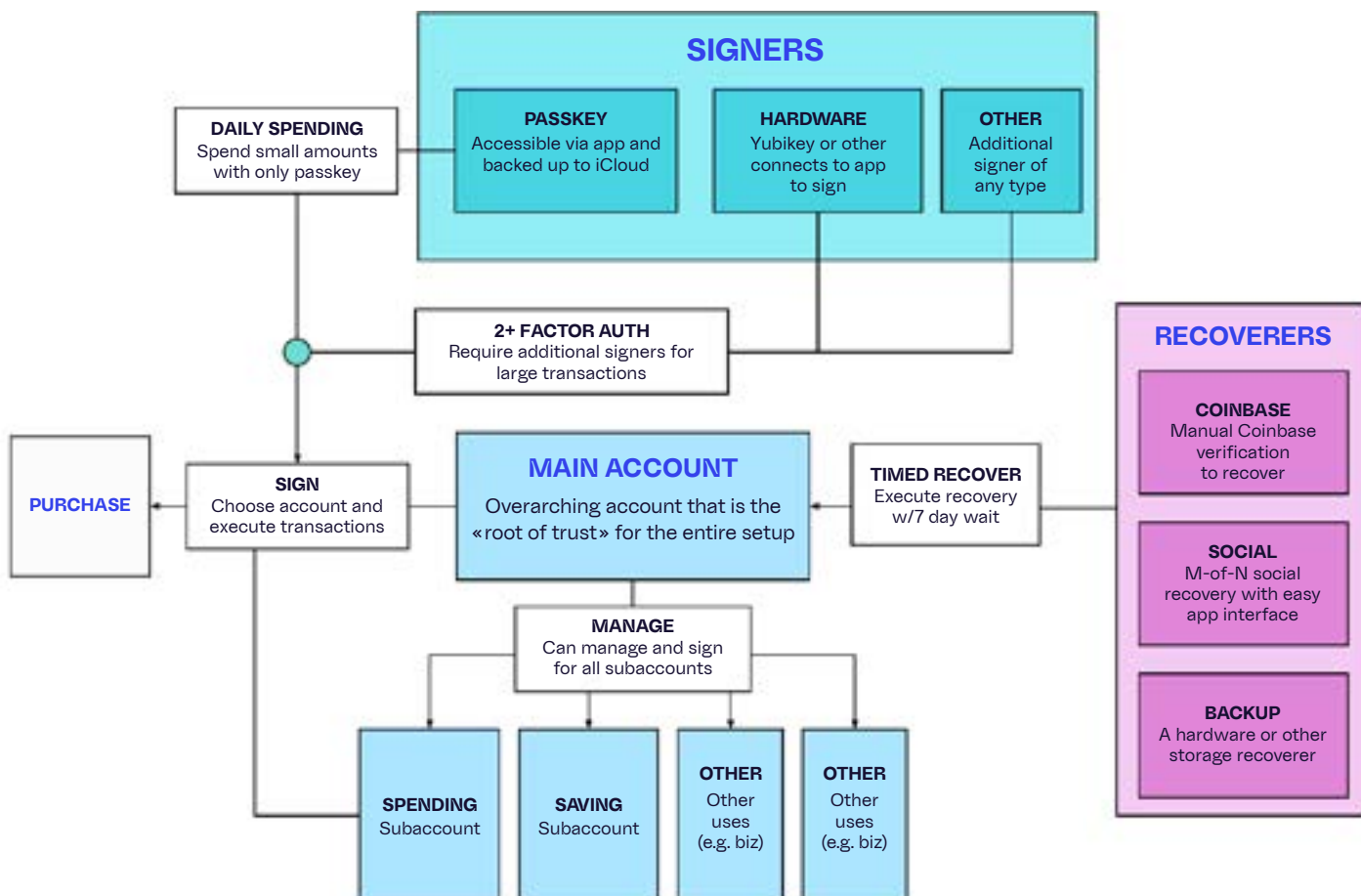
ACCORDING TO
JESSE POLLAK



THE ARCHITECTURE OF THE WALLET OF THE FUTURE ACCORDING TO JESSE POLLAK

JESSE POLLAK IS THE CREATOR OF BASE, COINBASE'S LAYER 2 BLOCKCHAIN. HE IS ALSO IN CHARGE OF THE ENTIRE WALLET DIVISION FOR THE AMERICAN GIANT. ON AUGUST 13, 2024, HE SHARED ON TWITTER WHAT HE ENVISIONS AS HIS "DREAM WALLET."

« I sketched out my «dream wallet» that would be 10x better than anything in web2 or onchain today. Need to solve a bunch of hard challenges, but i think we can get there in the next 6-12 months »



05

Business

WHAT BUSINESS MODELS FOR WALLET PROVIDERS?

WHAT BUSINESS MODELS FOR WALLET PROVIDERS?

Wallets like Metamask and Rabby have become essential gateways to Web3, facilitating interaction with dApps and capitalizing on the growth of DeFi and NFTs. Their success largely rests on an aggressive user acquisition strategy: free solutions integrated with Web3 ecosystems have attracted millions of users without economic barriers. However, with a solid user base established, these wallets are now shifting toward monetization by subtly adding fees to profit from their large audience without compromising their initial growth. Rather than imposing subscriptions or traditional usage fees, these wallets have gradually implemented discreet fees, often perceived as “invisible” by the average user.

1 FEES ON SWAPS

Token swaps directly within wallets through integrated swap services have become a key service for many users. Metamask, for instance, charges a 0.875% fee on each swap transaction made by its users, while Rabby charges 0.25%. For users who prioritize convenience, these fees often go unnoticed, but they represent a significant revenue source for wallets.

Wallets like Metamask and Rabby have become essential gateways to Web3, facilitating interaction with dApps and capitalizing on the growth of DeFi and NFTs.



WHAT BUSINESS MODELS FOR WALLET PROVIDERS?

2_FEEES ON ON/OFF-RAMP SERVICES

As more people look to convert fiat currency to crypto directly from their wallet, hot wallets have introduced on/off-ramp solutions—partner services that allow buying or selling crypto in fiat currency without leaving the app. These services also present an opportunity for wallets to charge additional fees on each transaction. These fees can vary depending on the provider and payment method, adding another layer of revenue for the companies behind the wallets.

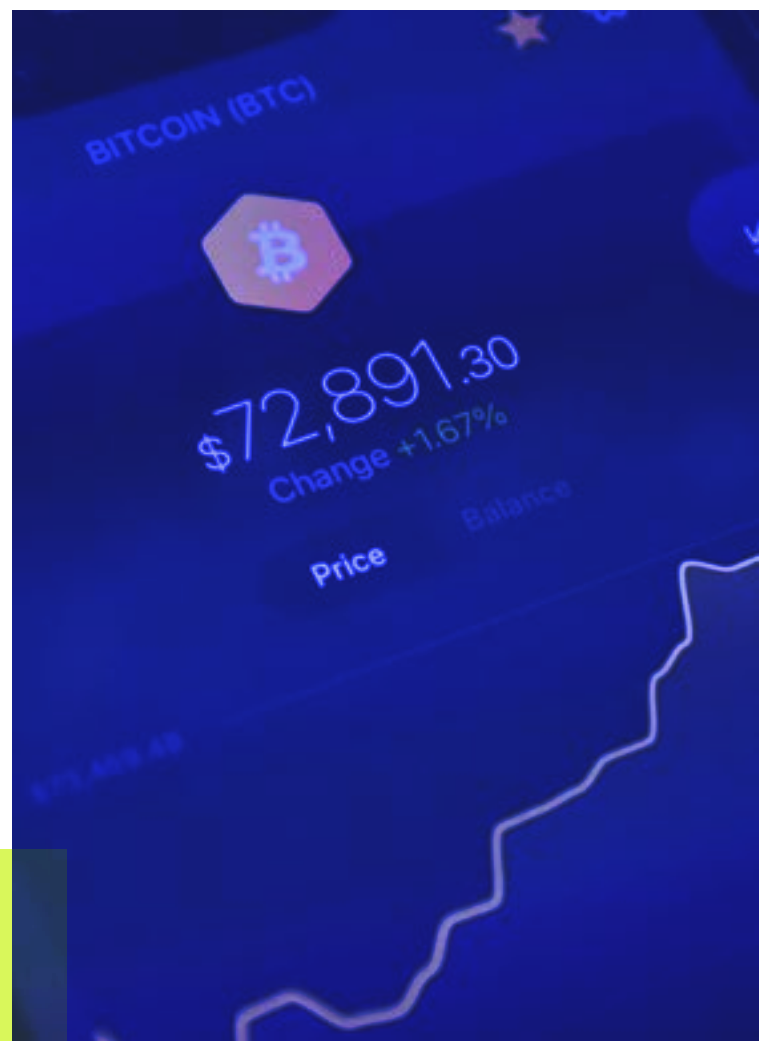
3_FEEES ON PAYMENT CARDS

More wallets are exploring the idea of introducing payment cards linked to crypto wallets, allowing users to spend their crypto directly in traditional stores. This approach aims to build user loyalty while capturing fees from transactions made with these cards. In this setup, wallets act as business referrers for card issuers, who then return a portion of the commissions to them. A notable example is the Argent wallet, which works with Kulipa and Mastercard. Though often modest, these multiple fees can add up to generate significant revenue streams, allowing these companies to monetize their audience effectively without imposing direct costs for basic wallet use.

WALLET TOKENS: AN UNCERTAIN STRATEGY

In parallel with this discreet monetization strategy, some wallets like Rabby are considering launching their own native tokens. This approach aligns with a trend in Web3, where many platforms have issued tokens to boost community engagement and create economic incentives for users.

However, this strategy is not without risks. Tokens issued by wallets can be a double-edged sword. On one hand, they offer benefits such as decentralized governance, fee discounts for token holders, and staking programs that help retain part of the audience. On the other, token volatility and dependence on crypto market cycles can make this strategy risky. Many projects that have launched tokens have faced significant price fluctuations, which can compromise their business model or long-term appeal.



06

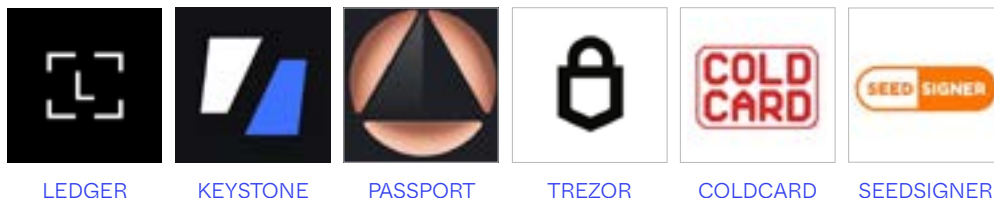
Mapping

MAPPING THE WALLET ECOSYSTEM

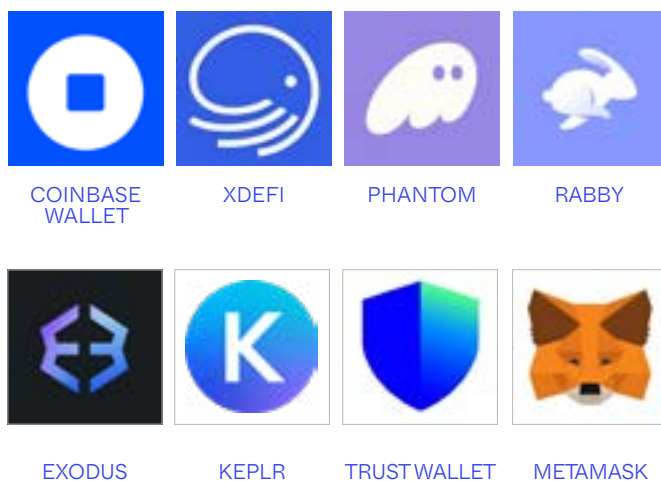


MAPPING THE WALLET ECOSYSTEM

Hardware wallets



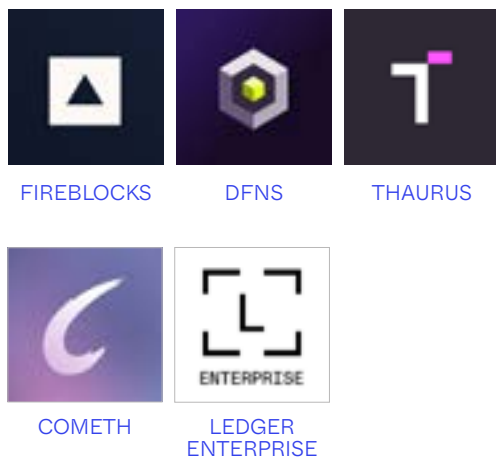
Hot wallet [browser extension]



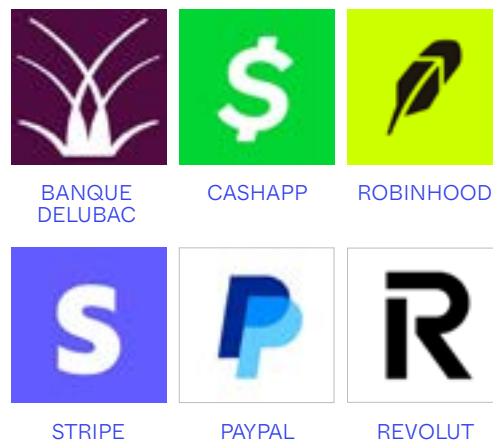
Mobile wallets MPC



Wallet-as-a-Service Providers



Banks/Fintechs Offering Wallets



MAPPING THE WALLET ECOSYSTEM

Non-Custodial Mobile Wallets



EXODUS

COINBASE
WALLET

XDEFI

RABBY



PHANTOM

KEPLR

TRUSTWALLET

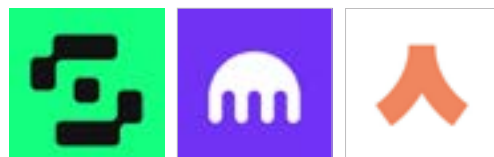
METAMASK

Smart wallets



CLAVE

INFINEX

COINBASE
SMART WALLET

SAFE

KRAKEN
WALLETARGENT
WALLET

Custodians institutionnels



ANCHORAGE

KOMAINU
(AVEC LEDGER
ENTERPRISE)

XAPO

BANQUE
DELUBAC

BITGO

CACEIS

COINBASE
CUSTODY

SG FORGE

Privacy-Focused Wallets

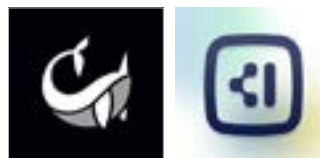


BRUME

WASABI

ASHIGARU
(FORK
SAMOURAI)

Wallet Services



NARVAL

ADAMIK

07

Interview

PIERRE D'ORMESSON

« THE DISTINCTION IS CLEAR:
HOLDING PRIVATE KEYS MEANS
BEING REGULATED »



PIERRE D'ORMESSON

DLA PIPER

LAWYER PIERRE D'ORMESSON BREAKS DOWN THE LEGAL ISSUES SURROUNDING CRYPTO WALLET REGULATION, HIGHLIGHTING THE DIFFERENCES BETWEEN CUSTODIAL AND SELF-HOSTED WALLETS, AS WELL AS THE IMPACT OF THE MICA REGULATION.

WHAT IS THE CURRENT STATE OF CRYPTO WALLET REGULATION?

To address this topic, there are two main perspectives. First, that of service providers. Current regulations primarily aim to regulate crypto-asset service providers, whether licensed or registered. Once regulated, they must comply with a set of rules, including anti-money laundering (AML) and counter-terrorism financing (CTF) under the supervision of a regulatory authority. Specifically, if a provider offers crypto custody services or private key management for third parties in France, they are subject to strict obligations. With MiCA regulations coming into effect soon, these providers will need to obtain a formal license, similar to that of investment firms, and implement internal processes to comply with risk control, AML, and transparency rules. Then, there's the user perspective. Those who use self-hosted wallets are not subject to the same rules as long as they avoid regulated platforms. But once they engage with a service provider (like a centralized exchange), that provider must comply with obligations like identity verification, fund traceability (especially via the travel rule), and transaction monitoring. These rules largely come from the Transfer of Funds Regulation (TFR), which imposes additional checks for any transfer over €1,000 involving a non-custodial wallet.

ARE THESE PROVISIONS ALREADY IN FORCE OR STILL IN DEVELOPMENT?

Some of these provisions are already in effect, especially the PSAN regime (soon to be replaced by MiCA), which initially introduced anti-money

« The distinction is clear: holding private keys means being regulated »

laundering rules for providers. However, others, such as MiCA and TFR, will not be fully implemented until December 30, 2024. While MiCA is already adopted, there remains a grace period before full implementation (providers currently operating under PSAN rules can continue under these regulations for a maximum of 18 months, until July 1, 2026). Established providers still have time to comply with the new rules, but most AML requirements are already in force.

ARE THERE ANY LEGAL OBLIGATIONS FOR TECHNOLOGY PROVIDERS OF WALLETS?

Manufacturers of hardware wallets, like Ledger, are not subject to legal obligations as custodians since they do not hold private keys for their users. A hardware wallet like Ledger is simply a tool, and the user maintains full control over their assets. Hardware wallet distributors are thus not registered or licensed as digital asset service providers under current regulations, as they do not provide regulated services. Self-hosted wallets, like MetaMask, are often associated with greater freedom and direct control for the user.

HOW DO REGULATORS INTEND TO BALANCE THIS WITH ANTI-FRAUD AND ANTI-MONEY LAUNDERING EFFORTS?

Indeed, self-hosted wallets offer more freedom to the user. However, as long as they stay outside regulated platforms, users are not held to the same compliance obligations. Regulators cannot directly oversee these users or their transactions unless

PIERRE D'ORMESSON

DLA PIPER

they use a regulated service, like an exchange or a service provider. Once a user goes through a regulated platform, that platform is obligated to apply anti-money laundering rules, such as identity verification, transaction monitoring, and origin-of-funds reporting. In short, regulators only intervene when a provider is involved, leaving self-hosted users a certain degree of freedom as long as they avoid these services.

« If a provider holds a user's private keys, they are considered as providing a digital asset custody service and must be regulated as such. »

WHAT LEGALLY DEFINES A SELF-HOSTED WALLET COMPARED TO A CUSTODIAL WALLET?

This is a key question. The main difference lies in who holds the private keys. A self-hosted wallet means that the user fully holds and controls their private keys, allowing them to manage their assets without a third party. In a custodial wallet, the service provider holds the private keys on behalf of the user and manages the assets for them. If a provider holds a user's private keys, they are deemed to be offering a digital asset custody service and must be regulated as such.

WHAT ARE THE LEGAL OBLIGATIONS FOR COMPANIES OFFERING CUSTODIAL WALLET?

MiCA and TFR regulations will significantly impact providers holding crypto assets for third parties. They will need to obtain a license and

comply with new rules. This includes implementing internal control policies, managing conflicts of interest, outsourcing procedures, and asset segregation to ensure fund security, in addition to AML and market abuse prevention obligations. Furthermore, MiCA and TFR will introduce new requirements for transparency and reporting to regulators, meaning providers will not only need to verify user identities but also monitor transactions for any suspicious activity.

HOW COULD MULTI-PARTY COMPUTATION (MPC) TECHNOLOGY IMPACT WALLET REGULATION?

MPC technology, which allows a private key to be split into multiple fragments distributed across different parties, raises an interesting question from a regulatory perspective. If a provider holds only a fragment of the private key, can they still be considered a custodian? Currently, there's no clear answer to this question in France's regulatory framework, and it would likely require clarification from regulators or relevant authorities.

THERE IS DEBATE AROUND REGULATING NON-CUSTODIAL WALLET; WHAT IS YOUR POSITION ON THIS?

It's an intriguing and forward-looking question. It's possible that in the future, regulators might require identity verification (KYC) even for transactions between non-custodial wallets. Currently, these wallets are not subject to such requirements, but this could change if regulators believe there's an increased risk of money laundering or terrorism



PIERRE D'ORMESSON

DLA PIPER

financing. For now, Metamask and similar wallets do not directly conduct KYC, as they primarily function as interface software for self-hosted wallets. They rely on third-party partners like MoonPay or Ramp for crypto-to-fiat conversions, who perform the necessary KYC checks. As long as these intermediaries meet their compliance obligations, Metamask doesn't need to be directly involved in these processes.

However, if no KYC verification is performed in the transaction chain, this anonymity could become problematic, and regulators might then require Metamask to intervene. For now, regulators do not engage with these actors, and legislators seem satisfied with the situation as long as some part of the chain handles identity verification and transaction traceability.

WHAT ARE THE COSTS OF COMPLIANCE?

Complying with MiCA poses significant challenges for a provider. Transitioning from a simple PSAN registration (digital asset service provider) to full licensing is complex. Under MiCA, this includes prudential capitalization requirements, internal governance, and compliance procedures far beyond the current AMF (Autorité des Marchés Financiers) registration rules in France. Providers will need, for instance, to establish whistleblower policies, enhanced cybersecurity, and stricter risk management. They will also be subject to continuous oversight from regulators, such as the AMF or ACPR, with regular reporting obligations. In terms of cost, compliance can quickly become expensive. While the license itself isn't paid, the legal support to obtain it, operational costs to meet requirements, and hiring a dedicated team for compliance and cybersecurity can represent several hundred thousand euros. For large organizations, the cost of obtaining MiCA licensing can reach around €500,000, including initial expenses and ongoing management and supervision costs.

DOES WALLET REGULATION VARY SIGNIFICANTLY BETWEEN REGIONS, FOR EXAMPLE, BETWEEN THE UNITED STATES, EUROPE, AND ASIA?

Yes, there are notable differences by region. In Europe, regulation tends to be harmonized through MiCA, which will introduce a uniform framework for the entire European Union. This allows companies to know precisely what obligations they will be subject to, whether they operate in France, Germany, or Spain. This is a very structured approach, with clear rules on asset custody, risk management, and the ability to provide services in other EU countries. In the United States, however, regulation is much more fragmented.

« In the U.S., regulation is much more fragmented, relying largely on court rulings and regulations specific to each state or federal regulator, meaning rules may vary by jurisdiction. »

It largely relies on court decisions and regulations specific to each state or federal regulator, such as the SEC or CFTC, meaning rules can vary by jurisdiction. In Asia, the situation is even more diverse. Some countries, like Singapore and Japan, have adopted clear regulatory frameworks for digital assets, while others, like China, reject this asset class, and others are drafting their own rules. Each region takes a different approach based on its priorities regarding security, innovation, and risk management.

08

Opinion

CLAIRE BALVA

« THE INEVITABLE ALLIANCE
BETWEEN WALLETES AND BANKS »



CLAIRE BALVA DEBLOCK

IN THE FACE OF A GROWING TREND OF ALLIANCES BETWEEN BANKS AND CRYPTO PLATFORMS, WALLETS STILL REPRESENT PURISTS, EVEN REBELS. BUT PERHAPS NOT FOR LONG, SUGGESTS CLAIRE BALVA, VP STRATEGY AT THE FINTECH DEBLOCK.

Observers of the publicized partnerships between centralized crypto players and traditional finance, many wallets now offer on/off-ramp solutions to convert crypto into fiat currency. These solutions, mainly dependent on regulated partners, remain imperfect. Users face numerous limitations, especially in selling crypto, with capped amounts, complex or delayed identity verification (KYC) processes, and even bank rejections after paying high fees. Many wallets are thus seriously considering the optional introduction of IBANs for their users. This addition could make wallet use more accessible to a broader audience and further democratize access to crypto. However, it remains a delicate subject, especially for wallets focused on Bitcoin or layer 2 (L2) solutions, whose communities value privacy. Adding services like fiat payment accounts often runs counter to this philosophy, imposing strict regulatory requirements, such as customer identification (KYC), which makes privacy impossible.

« The inevitable alliance between wallets and banks »

A FERTILE GROUND FOR REGULATORS

While KYC might only be required when creating an IBAN within the wallet, the impact could, in time, become much broader. This small step towards a regulated service opens the door for greater oversight by regulators, giving them a way to monitor activities previously seen as outside the system. Until now, authorities have preferred exchanges over wallets, which they couldn't supervise. Past regulatory attempts, like certain amendments to the MiCA regulation, sought to curb the appeal of self-custody by discouraging users from withdrawing their crypto from the regulated system. Adding banking services within wallets, even if optional, could change the game: it would allow authorities to monitor capital flows more closely by identifying the users behind wallets. Crypto flows wouldn't be censored, but they would become even more traceable. The arrival of traditional finance into wallets is thus a boon for regulators, letting them extend their reach over self-custody in a "soft" manner without additional legislation.



CLAIRE BALVA

DEBLOCK

WALLETS AS THE NEW CENTRAL POINT OF USER EXPERIENCE

While some maximalists might cry scandal, it's likely that commercial interest will be the guiding compass for most wallets. There is strong demand to centralize the user experience within a single tool, or at least to limit the number of different applications. Having both an IBAN and a wallet in the same place has real value for convenience and financial management, as shown by Deblock's success in just a few months. In response to the demand for an "all-in-one" user experience, wallets will likely have three main options. The first would be to refuse any regulatory entry into their application, which will probably be the choice of the most committed players, but could hinder the scaling of their service. Wallets could, on the contrary, undertake the steps themselves to obtain the necessary licenses to offer banking services. However, being directly under regulatory oversight would mean high compliance costs.

The third option would be to partner with specialized, already regulated providers in a Banking-as-a-Service (BaaS) model, holding an EMI or PSP license in Europe. This option is likely the most realistic, as it allows wallets to stay focused on their core business while expanding their financial services base safely. Integrations between banking services and wallets herald deep transformations and particularly lucrative revenue sources for these players. These opportunities, combined with the sector's growing consolidation, hint at future mergers between wallets, fintech, and banking players. While acquisitions of exchanges are already on the table, will banks soon turn to wallets to gain a foothold in crypto?



09

Innovation

SMART WALLET: THE FUTURE FOR INDIVIDUALS?



SMART WALLET: THE FUTURE FOR INDIVIDUALS?

Ethereum offers two types of accounts: externally owned accounts (EOAs), controlled by a private key, and smart contract accounts, managed through blockchain code. Unlike traditional wallets like MetaMask, limited to private key management, smart wallets utilize smart contracts that offer advanced features (social recovery, spending limits, multi-signature approvals). While classic wallets rely on the user's responsibility to secure assets, smart wallets provide greater flexibility and security through programmable functions, making access to digital assets simpler and safer for everyone.

ADVANTAGES

Enhanced and optimized security

Smart wallets offer enhanced security with advanced account recovery options, such as social recovery, and multi-signature features. These measures not only protect users from accidental loss of access but also add extra protection against hacking attempts.

Customization and automation

Thanks to programmable features, smart wallets enable customized and automated transactions. They can carry out complex tasks autonomously, allowing users to set, for example, spending limits, automate recurring payments, or establish specific authorization conditions. Consequently, these wallets facilitate process automation, enabling transactions without manual intervention at every step, which simplifies and improves digital asset management.

Cost reduction

Smart wallets can reduce gas fees by bundling multiple operations into a single transaction. In some cases, fees can even be entirely waived through the use of paymasters. These third-party entities cover transaction fees on behalf of users, enabling operations on the blockchain without the need to hold crypto for gas payments.

This functionality makes blockchain usage both more affordable and smoother.

Improved user experience

Smart wallets significantly simplify the user experience by eliminating the need to manage private keys or recovery phrases. By replacing traditional key management with modern methods like biometric authentication or passkeys, they make the user experience smoother and more accessible, reducing barriers for new users. This approach facilitates new user onboarding.

EASIER ACCESS: PASKEYS, GOOGLE AND APPLE ACCOUNTS, AND BIOMETRIC AUTHENTICATION

Smart wallets transform access to crypto by eliminating the need for each user to manage a private key. Using smart contract accounts, these wallets offer simplified recovery options, including Google and Apple accounts, passkeys, and biometric authentication options like Face ID. This changes how users interact with the blockchain. The management of private keys has long been a barrier to crypto wallet and Web3 adoption. With multiple authentication options, smart wallets make blockchain accessible to a broader audience, including those less familiar with technology.

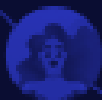
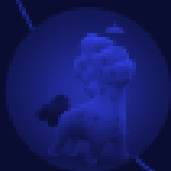
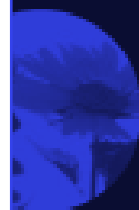
SMART WALLETS: THE FUTURE FOR INDIVIDUALS?

TOP SMART WALLETS

COINBASE SMART WALLET

On June 5, 2024, Coinbase launched its Smart Wallet, a crypto wallet designed to simplify the blockchain user experience. Currently in testnet, it offers a quick and direct signup via browser, without extensions or external applications. Users connect and sign transactions with passkeys, local security keys saved via iCloud or Google Password Manager, eliminating the complexity of recovery phrases. Access is easily managed through biometric options like fingerprint authentication. The Smart Wallet is compatible with eight EVM blockchains, including Ethereum, Polygon, and Base, providing smooth access to decentralized applications. With Coinbase's "paymaster" feature, certain dApps can cover transaction fees, offering a gas-free experience.


Through a unified account system, the Smart Wallet enables seamless connection to all on-chain applications with a single address, and its MagicSpend function allows direct spending from Coinbase accounts. Built on the ERC-4337 standard, the Smart Wallet supports bundled and sponsored transactions, optimizing interactions with dApps. Coinbase's smart contracts are regularly audited, ensuring enhanced security for each transaction.



SMART WALLETS: THE FUTURE FOR INDIVIDUALS?

TOP SMART WALLETS

INFINEX



Launched in May 2024, the Infinex Smart Wallet, known as the Infinex Account, aims to provide a seamless and secure DeFi experience. Developed by Kain Warwick, founder of Synthetix, this non-custodial wallet utilizes smart contracts and passkeys, giving users full control over their assets without intermediaries. Quick, extension-free signup is achieved through passkeys, generated and stored locally, with biometric login options like Face ID or fingerprint authentication. Infinex Account is compatible with six blockchains (not limited to EVM chains), including Ethereum, Solana, and Arbitrum, facilitating access to numerous DeFi applications with a single wallet. It also offers social recovery via Google or Apple

authentication, providing extra security in case of access loss. Infinex has also implemented a recovery mechanism allowing users to regain access to their Smart Wallet in case of lost passkeys, using social authentication methods such as Google or Apple accounts, while maintaining asset security.

SMART WALLETS: THE FUTURE FOR INDIVIDUALS?

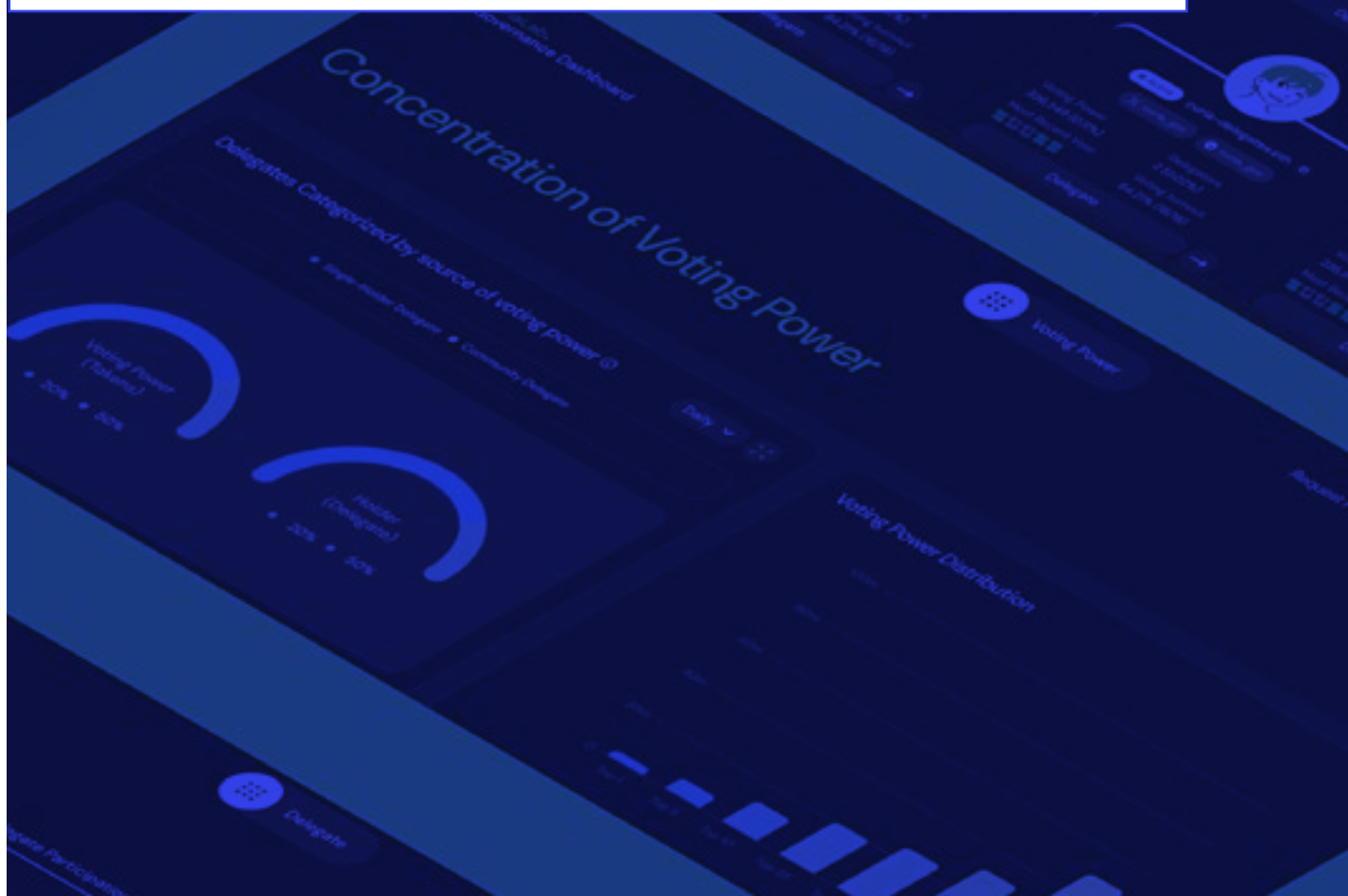
TOP SMART WALLETS

SAFE

Safe, formerly known as Gnosis Safe, is a benchmark smart wallet offering enhanced security through the setup of a minimum number of approvals for each transaction (a feature highly valued by organizations managing funds, like DAOs). Users set a quorum and a list of authorized accounts, ensuring the protection of their digital assets.

With over \$100 billion secured and 97 million transactions conducted, Safe operates on an open-source protocol and is compatible with over 15 networks, including Ethereum and Arbitrum.

It offers advanced features like transaction bundling, account recovery, and spending policies while integrating with more than 130 DeFi applications like Uniswap and AAVE. Safe's governance is managed by SafeDAO, allowing SAFE token holders to participate in strategic decisions. The decentralized model and SAFE token enable active community involvement in the platform's evolution.



SMART WALLET: THE FUTURE FOR INDIVIDUALS?

TOP SMART WALLET

ARGENT



Launched in 2018 and based in London, Argent is recognized as the first non-custodial smart wallet, designed to make DeFi and NFTs accessible on Ethereum and primarily on Starknet. Supported by major investors and with over two million users, Argent provides a smooth, intuitive experience for buying, staking, and investing in crypto with reduced fees. Argent stands out for its simple interface, account abstraction architecture allowing for transaction bundling, and advanced security features like Argent Shield, an email protection against hacking.

The wallet is open-source, offering transparency and customization by the community. Available on mobile and as a browser extension, Argent is compatible with DeFi applications like Ekubo and Nostra Finance, supporting account recovery features and spending policies.

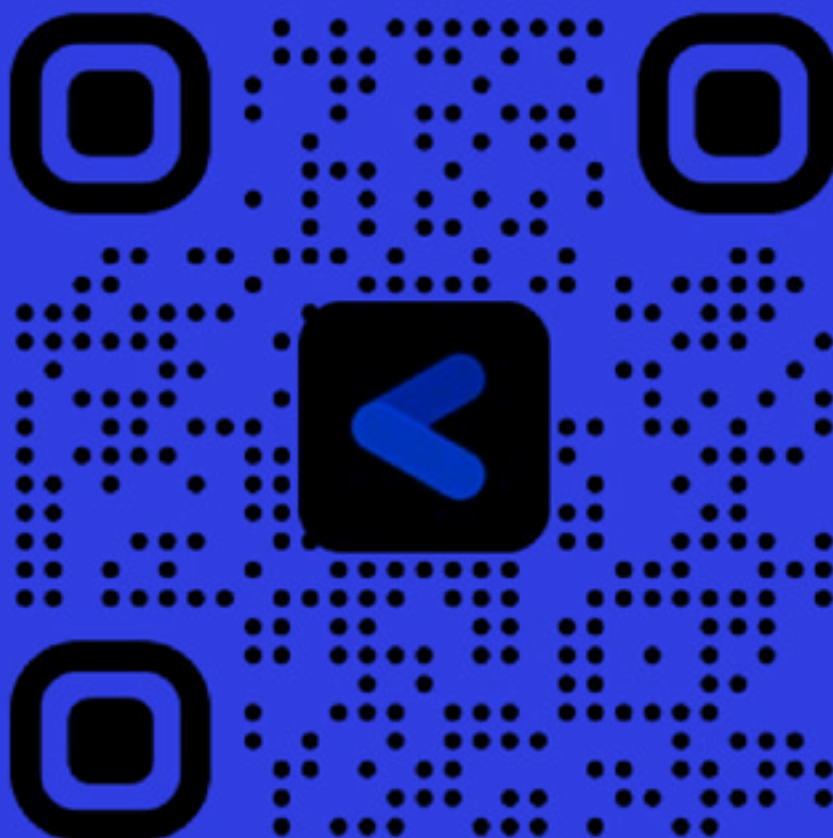
SMART WALLET: THE FUTURE FOR INDIVIDUALS?

TOP SMART WALLET

CLAVE

Launched in 2024, Clave Wallet is a non-custodial wallet that simplifies the Web3 and DeFi experience by integrating security and accessibility. With account abstraction, users can pay transaction fees with any token, making on-chain interactions more straightforward. Currently supporting only the ZkSync network, users can receive assets from other blockchains (with Clave bridging them to ZkSync).

Clave offers a key management system with social and passkey recovery, ensuring security and control over assets. Users also enjoy free usernames via ENS, making transactions more intuitive. Available on Android and iOS, the app allows simplified deposits, token swaps with no network fees, and staking and referral options.



10

Interview

NICOLAS BACCA

« PASSKEYS, BIOMETRICS,
AND MPC TECHNOLOGIES SIMPLIFY
THE USER EXPERIENCE »



NICOLAS BACCA

CO-FOUNDER AND FORMER CTO OF LEDGER, NICOLAS BACCA DISCUSSES THE INTEGRATION OF NEW STANDARDS IN CRYPTO WALLETS, BALANCING USER EXPERIENCE IMPROVEMENTS WITH NEW SECURITY CHALLENGES.

MORE WALLETS TODAY ARE ADOPTING BIOMETRIC IDENTIFICATION FOR LOGIN OR TRANSACTION VALIDATION. HOW DOES THIS WORK?

In fact, biometric identification doesn't directly sign transactions. It serves as an extra layer of security to access the private key or a fragment of it. Biometrics don't replace cryptographic signatures; instead, they act as a lock protecting access to the key, which itself signs the transactions, similar to a traditional signature. For example, with Face ID or a fingerprint, it's not the biometric data itself that validates the transaction, but rather it authorizes access to the private key. Access to this key is restricted until the biometric data is verified. Once the fingerprint or face is recognized, the device unlocks access to the key, which is then used to sign the transaction.

MOST OF THE TIME, IT'S THANKS TO "PASSKEYS" THAT ONE CAN VALIDATE TRANSACTIONS WITH FACE ID OR A FINGERPRINT, RIGHT?

Yes, that's correct. This standard allows transactions to be validated with a fingerprint or Face ID in a Web2 environment. When using a passkey on a compatible website or app, biometric authentication unlocks the private key to validate the operation.

CAN YOU EXPLAIN HOW PASSKEYS WORK?

A passkey is a Web2 standard intended to replace traditional passwords, which are often security risks. The basic idea is simple: instead of a password that the user has to remember, a passkey relies on a pair of cryptographic keys.

« Passkeys, biometrics, and MPC technologies simplify the user experience »

When a user creates an account with a passkey, a public key and a private key are generated. The public key is stored on the site or service, while the private key remains secure on the user's device, locked by biometrics, PIN, or other verification. The benefit is that for each login, the service sends a "challenge" that the user signs with their private key, proving their identity. This system is much more secure than passwords because the private key is never shared and remains protected by a cryptographic mechanism. Passkeys resist phishing and interception attacks, as there's no password to steal or reuse. In crypto wallets, the passkey standard is "repurposed" to serve as an authentication method for signing on-chain transactions. When a user signs a transaction with a passkey, the process is similar to MetaMask: a transaction is hashed, then signed by the private key before being sent to the network. The passkey thus serves as a bridge between Web2 and blockchain, allowing users to access services without worrying about passwords.

IN SMART WALLETS, WHO EXACTLY STORES THE PRIVATE KEYS IF THEY'RE INVISIBLE TO THE USER?

In smart wallets, key management varies based on technology and custody models. For passkeys, the key is always stored by the user but is often automatically synchronized across devices. For instance, if you use Face ID on an iPhone, the key is on the phone but also backed up via iCloud for easy recovery and multi-device use.

NICOLAS BACCA

Although the key is “invisible” to the user, it remains stored and controlled by them. In other models, such as those using Threshold Signature Scheme (TSS) or Multi-Party Computation (MPC), the key is split into fragments. One fragment is kept by the user, another by a trusted third party, and sometimes an additional fragment is independently secured. To sign a transaction, the fragments are combined through advanced cryptographic techniques, but each party holds a fragment and, theoretically, can influence access.

WHICH SMART WALLETS MEET YOUR HIGHEST SECURITY STANDARDS?

I think of wallets like Argent and Bravos on Starknet, designed for user autonomy. They use smart contracts for fund management and provide secure key management directly on the blockchain, without a trusted third party. In this model, everything is transparent and traceable on-chain, allowing users to retain full control over their assets. On Ethereum, another similar wallet is Clave. Although Clave is not yet fully web-based, it offers smart contract authentication, where access to funds is managed in a decentralized way by a smart contract rather than by a server that could block access. This solution enables purely blockchain-based authentication, enhancing security and transparency. Another important example is Coinbase Wallet in its “smart wallet” version. This one is notable because Coinbase built an on-chain validation infrastructure, closely aligning with the blockchain philosophy: the user controls their funds without relying on external servers. It's a good wallet model that respects user autonomy while offering modern security features.

IS THIS TYPE OF WALLET ONLY FOR ETHEREUM?

No, these solutions are not exclusive to Ethereum. Smart contract logic can be deployed on any programmable blockchain that supports smart contracts. Ethereum is ahead in terms of wallet standards and technology, but blockchains like

Starknet, Polygon, Binance Smart Chain, and others can also support smart wallets. Ethereum is often favored for these developments due to its robust standards for critical aspects like transaction fee payment (gas), transaction bundling, or gas sponsorship, which enhance the user experience. But the model is replicable on other programmable blockchains.

« Biometric identification doesn't directly sign transactions; it acts as a lock that protects access to the key, which is then used to sign the transaction. »

ARE PASSWORDS AND PRIVATE KEY STORAGE BY USERS DESTINED TO DISAPPEAR?

No, I don't think passwords and private keys will disappear entirely. Their use will likely become increasingly limited to critical operations, like account recovery or changing a wallet's security settings. For low-value transactions or frequent operations, simpler and automated solutions like biometrics or passkeys will gradually become the norm. However, for significant transactions or changes, holding the private key remains the safest and most direct approach. This is why wallets will probably always retain the option to use a private key in certain cases.

DOES THIS ADDED COMPLEXITY INCREASE RISKS, LIKE LOSING ACCESS TO ONE'S WALLET?

Absolutely, complexity introduces new risks. With smart wallets, authentication is programmable, enabling different recovery or security methods.

NICOLAS BACCA

For instance, if a user chooses a passkey without a recovery solution, they're vulnerable. If they lose their passkey, they could lose access to their wallet. This risk is especially present when the user relies on solutions like passkey synchronization through Google or Apple. If this synchronization is compromised, for instance, if an account is deactivated, the user could lose their passkey and thus access to their wallet. It's crucial for users to understand the recovery options provided by the wallet.

However, smart wallets help mitigate some risks. For example, one can set up recovery with another wallet, like MetaMask, or use solutions like Argent, which allows users to transfer wallet control if needed. But these options require user awareness to avoid being "locked out."

Choosing a good wallet also means selecting one that offers clear, flexible recovery methods and security options.

CAN APPLE OR GOOGLE ACCESS MY PRIVATE KEY WHEN USING WALLETS LIKE COINBASE WALLET OR ARGENT, WHICH RELY ON FACIAL RECOGNITION?

In theory, no, Apple and Google don't have direct access to the private key itself, especially if it's stored in a secure enclave, as with passkeys. The key is stored encrypted in a Hardware Security Module (HSM) or secure enclave, which isolates the private key from the rest of the system and applications, so even Apple or Google services can't access the raw key. However, an important point

is that when passkeys are synchronized, a layer of trust is placed in the company's infrastructure. This means that although the key itself remains inaccessible, a synchronization protocol depends on Apple or Google for secure transfer between devices. If these services are compromised, for example, if a hacker intercepts synchronized data or the user's account is hacked, it could affect access to passkeys.

ARE THESE NEW SYSTEMS THE KEY TO DEMOCRATIZING CRYPTO WALLETS FOR THE PUBLIC?

Yes, absolutely. For crypto wallets to gain broader adoption, some current obstacles, especially those related to user interface complexity and security, must be overcome. Passkeys, biometrics, and Multi-Party Computation (MPC) technologies simplify the experience, which is essential for the general public. Imagine if we could combine several open-source technologies, like passkeys, email authentication, and TSS (Threshold Signature Scheme) or MPC. This would enable the creation of modular and secure solutions accessible to everyone, without requiring advanced cryptographic knowledge. The goal is to reach a user experience similar to Web2 applications, with simple and secure logins, without users needing to manage their private keys directly.



NICOLAS BACCA

HOW CAN LEDGER FIT INTO THIS NEW DYNAMIC, WHICH IS CHANGING HABITS AND COULD POTENTIALLY IMPACT ITS CORE BUSINESS?

Ledger is already part of this dynamic in several ways. For instance, we've highlighted the external passkey feature. By offering a hardware wallet like Ledger to store a passkey, we add a layer of security for passkey users while giving them increased control over their private key. This feature allows users to authenticate with a passkey while ensuring their key is stored independently from any cloud or server. Furthermore, Ledger has already begun positioning itself as a tool for critical operations on smart wallets. With a hardware wallet like Ledger, users can consider performing advanced security operations, like changing a smart wallet's custody settings or modifying recovery policies. These actions require high security levels because they can directly impact fund management, and the hardware wallet provides the security assurance that few other solutions offer. In other words, while the hardware wallet may be used less frequently, it becomes an essential tool for critical operations.

This change strengthens Ledger's position, transforming the hardware wallet from merely a key storage tool to a security control device for transactions and important parameter updates. This is why we continue to improve the user interface and simplify interactions with the hardware wallet, enabling users to utilize this solution easily for critical actions without compromising security.

WHAT WILL THE WALLET OF THE FUTURE LOOK LIKE? WHAT WOULD BE ITS KEY FEATURES?

The wallet of the future will be versatile, modular, and ultra-secure. Jesse Pollak from Base has even created an excellent infographic describing this concept, called the "Dream Wallet." The idea is to combine multiple features to offer maximum flexibility while maintaining robust security.

« The wallet of the future will be versatile, modular, and ultra-secure, with modular recovery options like social recovery or Zero-Knowledge proofs, optimizing access without compromising security. »

First, a key element will be the ability to use different security levels for signatures, depending on the transaction's importance. For instance, a light signature could suffice for a small payment, while a more significant transaction would require more complex authentication. This flexibility will allow users to manage their funds more easily while ensuring reinforced security for critical transactions. Next, the future wallet will incorporate highly modular recovery options. This might include social recovery, where trusted contacts can help recover access in case of loss, or Zero-Knowledge proof (ZK) recovery, where a passport or other ID verifies the user's identity without revealing sensitive data. Projects like zkPassport allow a user to present their passport to regain access to their wallet, a significant advancement in convenience and security. Additionally, the future wallet will also offer features like gas sponsorship and solutions to optimize transaction costs. This will ease constraints for users, making gas fee payments more seamless and reducing obstacles to interacting with the blockchain. This vision of a modular and programmable wallet would provide an intuitive interface with institutional-level security, often lacking in current solutions. The industry is moving in this direction, integrating new technologies and standards to further democratize smart wallets.



The Big Whale

ACKNOWLEDGMENTS

NICOLAS BACCA

Cybersecurity Expert,
Co-founder of Ledger

CLAIRE BALVA

VP Strategy, Deblock

**CHRISTOPHER
GRILHAULT
DES FONTAINES**

Co-founder, Dfns

CHARLES GUILLEMET

CTO, Ledger

CLARISSE HAGÈGE

Co-founder, Dfns

ITAMAR LESUISSE

CEO, Argent

PIERRE D'ORMESSON

Partner, DLA Piper

JESSE POLLAK

Head of Base and Coinbase
Wallet, Coinbase

CÔME PROST-BOUCLE

Country Manager, Coinbase

JÉRÔME DE TYCHEY

CEO, Cometh

This report was produced by **The Big Whale**
Research Team under the direction
of **Grégory Raymond**.

www.thebigwhale.io

Contact us: contact@thebigwhale.io

9 rue des Colonnes, 75002 Paris, FRANCE

