The Big Whale

The Big Whale Report

Le futur **des wallets**

AVEC LE SOUTIEN DE

Dfns

ÉDITO

LA PORTE D'ENTRÉE VERS UN **NOUVEAU MONDE FINANCIER**

C'est une petite porte numérique que l'on ouvre du bout des doigts, une clé virtuelle capable de nous projeter dans un univers d'innovations. Ce premier contact, souvent furtif, avec le monde des cryptos se fait au travers d'un objet discret mais fondamental : le wallet. Mais ce wallet, ou portefeuille crypto, n'est pas un simple contenant ; il est la passerelle vers un écosystème foisonnant. Dans ce futur où les banques centrales expérimentent des monnaies numériques et où l'investissement dans les cryptos devient un sujet grand public, le wallet se présente comme le pilier indispensable de la vie numérique et financière.

Mais derrière cette porte, que se cache-t-il vraiment ? Il n'existe pas de modèle unique : chaque wallet repose sur un parti pris technologique et une expérience utilisateur qui traduisent des visions radicalement différentes de la cryptographie et de la décentralisation. Entre wallets custodial, où la clé d'accès reste entre les mains d'une entité centralisée, et wallets non-custodial, où l'utilisateur seul est maître de ses actifs, un éventail de choix s'ouvre, offrant autant de façons de concevoir la propriété numérique et de gérer les interactions avec la blockchain.

À cela s'ajoute l'émergence des "smart wallets", véritables concentrés d'intelligence décentralisée, intégrant des fonctionnalités avancées d'automatisation et de sécurité qui redéfinissent déjà les contours de ce secteur.

GRÉGORY RAYMOND_
Head of Research,
The Big Whale

Dès lors, les fintechs qui entendent proposer des wallets à leurs clients se retrouvent face à des choix cornéliens : sur quelle technologie de wallet faut-il s'appuyer pour proposer un produit efficace, sécurisé et conforme à la réglementation naissante ? Le sujet est important, car entre les États-Unis, l'Europe et l'Asie, des cadres juridiques émergent pour encadrer l'utilisation de ces portefeuilles numériques. Toutefois, le chemin est encore parsemé d'incertitudes : des zones grises persistent, et les débats autour de la confidentialité, de la gouvernance et de la conservation des clés privées s'intensifient.

Mais ce qu'il faut retenir, c'est que derrière ces innovations se dessine un marché colossal. Ces wallets sont devenus des carrefours d'échanges, de paiements, de staking et d'investissement pour des millions d'utilisateurs dans le monde entier. Des géants de la tech aux jeunes pousses, les acteurs se pressent pour imposer leur solution et capter un public en quête de simplicité, de sécurité et de liberté. Ce secteur, qui s'inscrit à la croisée de la finance et de la technologie, attise des ambitions financières considérables.

Ainsi, dans les pages qui suivent, nous explorerons les trajectoires possibles de ce futur proche où le wallet crypto, tel un sésame moderne, continuera de redessiner les contours de notre rapport à l'argent, aux données et à la confiance.

.sommaire

01

Standards

LES DIFFÉRENTES TECHNOLOGIES DE CONSERVATION

LES DIFFÉRENTES TECHNOLOGIES DE CONSERVATION_

01 HARDWARE WALLETS

Les hardware wallets, ou portefeuilles physiques, sont des dispositifs spécialement conçus pour stocker les clés privées hors ligne, ce qui les rend très résistants aux cyberattaques. Ils sont considérés comme l'une des solutions les plus sûres, car ils ne sont pas connectés à Internet.

Cela signifie que pour signer une transaction, l'utilisateur doit connecter physiquement l'appareil à un ordinateur ou à un smartphone.

AVANTAGES

- Sécurité maximale contre les attaques en ligne
- Clés privées stockées hors ligne
- Support multi-devises

INCONVÉNIENTS

- Moins pratique pour des transactions fréquentes
- Nécessite d'avoir un appareil physique avec soi
- Peu adapté à un usage institutionnel

EXEMPLES

LEDGER KEYSTONE

LES DIFFÉRENTES TECHNOLOGIES DE CONSERVATION_

02 HSM WALLETS

Les HSM (Hardware Security Modules) sont des dispositifs matériels spécialisés conçus pour générer, stocker et gérer les clés cryptographiques de manière ultra sécurisée. Souvent utilisés par des institutions financières et des entreprises, ils sont conformes à des normes de sécurité rigoureuses.

Bien qu'ils puissent ressembler à des hardware wallets, les HSM sont généralement utilisés dans des environnements plus complexes et centralisés, souvent dans le cadre de solutions cloud ou en entreprise.

AVANTAGES

- Sécurité de niveau entreprise, conforme aux standards stricts (FIPS)
- Souveraineté totale de la clé privée pour l'entreprise
- Excellente résilience contre les attaques physiques et logicielles
- Pertinent pour les entreprises et les institutions qui gèrent de gros volumes d'actifs

INCONVÉNIENTS

- Coût d'installation élevé

EXEMPLES

LEDGER ENTERPRISE

TAURUS

LES DIFFÉRENTES TECHNOLOGIES DE CONSERVATION_

03 MPC WALLETS

Les portefeuilles MPC (Multi-Party Computation) sont une technologie plus récente qui répartit la gestion des clés privées entre plusieurs parties ou appareils.
Aucune partie ne possède la clé entière, et pour signer une transaction, une coordination entre les différentes parties est requise.

Ce modèle améliore la sécurité en rendant le vol des clés plus difficile, tout en gardant une certaine flexibilité.

AVANTAGES

. Sécurité renforcée via la division de la clé privée

. Plus pratique et flexible que les hardware wallets et le HSM

. Peut convenir aux institutions financières et aux utilisateurs individuels

. Coûts plus compétitifs que les hardware wallets et les HSM

INCONVÉNIENTS

. Technologie encore relativement nouvelle

. Complexité technique accrue

. Risque réglementaire : le fournisseur de wallets pourrait être reconnu comme custodian (car il conserve une partie de la clé)

EXEMPLES

POUR LES ENTREPRISES

FIREBLOCKS TAURUS DFNS

POUR LES PARTICULIERS

ZENGO SWISSBORG DEBLOCK

LES DIFFÉRENTES TECHNOLOGIES DE CONSERVATION_

04 SMART WALLETS

Les smart wallets s'appuient sur des smart contracts pour automatiser et ajouter des fonctionnalités avancées.

Contrairement aux portefeuilles traditionnels, ils permettent des interactions automatiques avec des applications décentralisées (dApps) et peuvent inclure des fonctions telles que la récupération de clés, des limites de dépenses, ou encore des paiements programmés.

AVANTAGES

- Fonctions avancées comme la récupération de clés ou la protection multi-signature
- Adapté aux entreprises qui ne gèrent pas beaucoup detransactions et aux particuliers
- Peut automatiser certaines tâches via des smart contracts

INCONVÉNIENTS

- Souvent limités à certaines blockchains comme Ethereum
- Inadapté aux institutions financières qui opèrent de très nombreux flux

EXEMPLES

POUR LES PARTICULIERS

COINBASE SMART WALLET

ARGENT WALLET

POUR CERTAINES ENTREPRISES OU DAO

SAFE

LES DIFFÉRENTES TECHNOLOGIES DE CONSERVATION_

05 HOT WALLETS

Les hot wallets sont des portefeuilles en ligne, accessibles via des navigateurs web ou des applications mobiles, qui sont toujours connectés à Internet.

Ils sont les plus pratiques pour une utilisation quotidienne et des transactions fréquentes. Toutefois, cette connexion constante à Internet les rend plus vulnérables aux attaques et aux piratages.

AVANTAGES

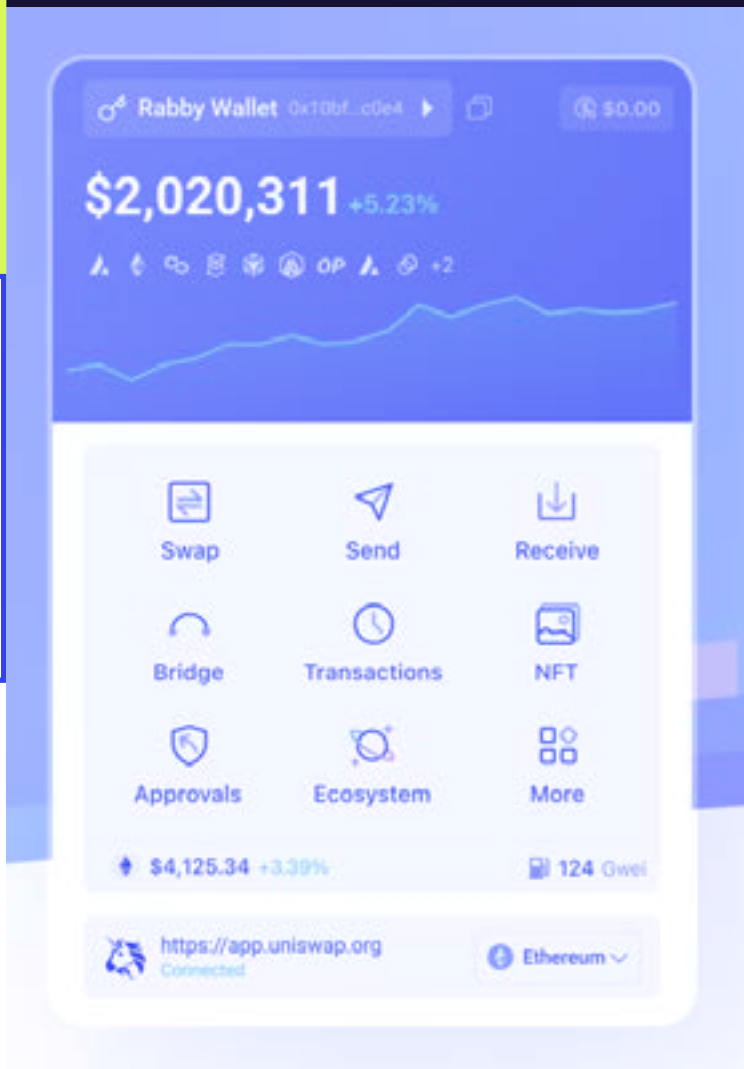
- Facilité d'utilisation, rapide pour les transactions
- Idéal pour interagir avec les dApps et DeFi
- Support multi-devises

INCONVÉNIENTS

- Risques élevés de piratage en raison de la connexion permanente à Internet
- Moins sécurisé que les hardware wallets (mais on peut améliorer la sécurité d'un hot wallet en le liant à un hardware wallet)
- Inadapté aux entreprises

EXEMPLES

RABBY PHANTOM METAMASK



02

Entretien

CLARISSE HAGÈGE

« LE CONCEPT DE WALLET NON-CUSTODIAL EST EN PARTIE UNE ILLUSION »

CLARISSE HAGÈGE
DFNS_

CLARISSE HAGÈGE, CEO DE DFNS, REVIENT SUR SES AMBITIONS POUR TRANSFORMER L'INFRASTRUCTURE DE LA CUSTODY. ELLE ABORDE ÉGALEMENT LES ENJEUX DE SÉCURITÉ, LES DÉFIS RÉGLEMENTAIRES ET LIVRE SA VISION DU WALLET DU FUTUR, UN OUTIL SÉCURISÉ, MODULAIRE ET INTEROPÉRABLE, PENSÉ POUR LES INSTITUTIONS FINANCIÈRES DE DEMAIN.

> **« Le concept de wallet non-custodial est en partie une illusion »**

POUVEZ-VOUS REVENIR RAPIDEMENT SUR L'HISTOIRE DE DFNS ?

Dfns a pris racine dans mon parcours, car j'ai passé une décennie dans le secteur bancaire. De 2008 à 2018, j'ai travaillé chez Goldman Sachs, Bank of America et Crédit Agricole, où j'ai acquis une expertise en finance et en gestion d'actifs. Lors d'un programme d'incubation au Village by CA à Paris, j'ai ensuite rencontré l'équipe de IOV (aujourd'hui Starname), un projet similaire à l'Ethereum Name Service (ENS) mais basé sur Cosmos. Je les ai aidés à structurer leur ICO pendant l'été, mais je suis tombé sur un problème récurrent : l'adoption de la crypto par les investisseurs traditionnels était freinée par des barrières techniques. De nombreux investisseurs étaient rebutés à l'idée d'acquérir un Ledger Nano et de gérer eux-mêmes les clés cryptographiques donnant accès à leurs actifs, en l'occurrence des jetons IOV. Bien que les réunions commerciales aient été positives, environ 90 % des discussions s'arrêtaient lorsqu'il s'agissait de manipuler des hardware wallets et d'assumer les risques de sécurité. J'ai alors constaté un manque d'infrastructure appropriée, adaptée aux investisseurs institutionnels qui n'étaient pas des ingénieurs aguerris en sécurité ou des traders dans la DeFi. En parallèle, j'ai exploré les solutions de custody basées sur des HSM (Ledger, Anchorage, BitGo) et des entreprises en vogue basées sur le MPC (Fireblocks, Curv, Sepior, Unbound), mais ces outils présentaient deux défauts majeurs : d'une part, ils étaient exclusivement orientés vers des cibles B2C ou B2B, alors que j'étais convaincue que la finance nécessiterait une solution B2B2X, centrée sur les API. D'autre part, leur schéma de déploiement des clés exposait les clients-utilisateurs à des risques de sécurité trop élevés. Convaincue que la blockchain transformerait à terme le secteur financier, j'ai donc décidé de me concentrer sur la création d'une infrastructure modulable, permettant aux développeurs de fintechs, aux startups et aux institutions financières établies de lancer leurs projets rapidement et d'opérer sur plusieurs blockchains sans retarder leur mise sur le marché, tout en s'appuyant sur une technologie éprouvée, capable de soutenir leur montée en puissance sans difficulté. Dfns a été officiellement fondée à Paris en août 2020, après une période d'exploration entamée dès 2019.

QUEL EST LE VOLUME DES ACTIFS QUE VOUS GÉREZ ET SÉCURISEZ AUJOURD'HUI ?

Nous ne communiquons pas l'AUM (Assets Under Management) pour éviter que nos concurrents puissent tirer des conclusions stratégiques. Cependant, nous sommes transparents sur notre volume mensuel de transactions, qui atteint actuellement plus de 980 millions de dollars. Cette tendance est récente, car jusqu'en juillet 2024, nous traitions environ 150 millions de dollars par mois. Cette augmentation est liée à l'arrivée de nouveaux clients, au boom des paiements en stablecoins à travers le monde et à une adoption accrue de notre infrastructure par des entreprises et des banques souhaitant automatiser et sécuriser leurs opérations à l'échelle.

CLARISSE HAGÈGE
DFNS_

COMMENT VOUS DISTINGUEZ-VOUS DE SOLUTIONS CONCURRENTES COMME FIREBLOCKS ?

Nous nous distinguons par notre approche programmable centrée sur l'API. Dès le début, nous avons parié sur un modèle similaire à celui d'Algolia ou Stripe, en fournissant des outils aux développeurs pour qu'ils puissent créer simplement et rapidement des applications blockchain. À l'inverse, Fireblocks a conçu une interface utilisateur pour des traders et des fonds qui avaient besoin d'une expérience manuelle avec les wallets. Par conséquent, ils ont introduit des API plus tard, et elles demeurent encore aujourd'hui très limitées par rapport aux nôtres. Chez Dfns, chaque fonctionnalité est disponible par API, permettant aux équipes de développer des services à grande échelle avec automatisation et configurabilité.

« Chez Dfns, chaque fonctionnalité est disponible par API, permettant aux équipes de développer des services à grande échelle avec automatisation et configurabilité. Nous sommes les seuls sur le marché à offrir un tel niveau de personnalisation programmatique. »

Par exemple, notre système de gestion des droits sur les wallets et les transactions, appelé "Wallet Entitlement Management (WEM)", est entièrement automatisable. Il permet de définir des autorisations et des contrôles d'accès basés sur les rôles (auditeur, approbateur, trader, gestionnaire de compte, etc.), des règles et variables transactionnelles (limites de montant, fréquence, règles anti-siphonnage, whitelisting, etc.) ainsi que des conditions basées sur des webhooks (par exemple : si une adresse reçoit 100 000 USDC, le wallet est bloqué pour toute nouvelle sortie de fonds). Nous sommes les seuls sur le marché à offrir un tel niveau de personnalisation programmatique, un véritable atout à l'heure où la réglementation se durcit et où les risques liés aux cryptomonnaies augmentent avec la hausse de leur valeur. Notre infrastructure est aussi de plus en plus reconnue pour sa grande modularité. Nous permettons à nos clients de déployer leurs propres instances sur des clouds publics comme AWS, des clouds privés, et de connecter leurs HSM Thales ou IBM à notre système de gestion des transactions blockchain. Cela facilite la conformité avec les départements de sécurité, les autorités de marchés financiers et les régulateurs locaux. La blockchain n'a pas pour vocation de bouleverser les institutions financières ou de remettre en question des décennies de bonnes pratiques en matière de sécurité et de logique. Elle vise à améliorer les processus existants. Chez Dfns, nous prenons soin de bien comprendre les besoins des acteurs financiers avec qui nous travaillons, car leurs logiques métier sont précieuses. Notre objectif est de nous interfacer avec ces processus pour faciliter le travail du back-office et du middle-office. Enfin, nous avons adopté un modèle de tarification basé sur l'usage, à l'image d'AWS, plutôt que des commissions sur le volume des transactions ou sur l'AUM, ce qui rend nos solutions plus adaptées aux besoins réels des institutions financières, des solutions de paiement, des plateformes d'émission de jetons et des applications de trading dont c'est la source de revenu.

CLARISSE HAGÈGE
DFNS_

COMMENT FONCTIONNE LA TECHNOLOGIE MPC CHEZ DFNS ? QUELS SONT SES AVANTAGES ?

La Multi-Party Computation (MPC) est au cœur de notre solution de gestion de clé offerte en SaaS. Cette technologie répartit une clé en plusieurs fragments, générés et stockés dans des lieux distincts. Ces fragments permettent de créer des signatures partielles sans jamais reconstituer la clé entière. Ainsi, même si certains fragments sont compromis ou perdus, le système peut continuer à fonctionner en utilisant un seuil de validation, par exemple 2 sur 3 fragments. Cela réduit les risques d'erreurs humaines contagieuses et renforce la sécurité contre les attaques internes ou externes. C'est aussi une technologie qui garantit un plus haut niveau de disponibilité des services grâce à la fragmentation et à la contingence qu'elle apporte au matériel sensible que sont les clés privées des wallets.

COMPTE TENU DU FAIT QUE LE MPC FRAGMENTE UNE CLÉ PRIVÉE EN PLUSIEURS MORCEAUX ET QUE VOUS EN GARDEZ UN, COMMENT ENVISAGEZ-VOUS LE RISQUE D'ÊTRE ASSIMILÉ À UN CUSTODIAN ?

Pour répondre en détail à la question de savoir si la solution de gestion de clés de Dfns pourrait être perçue comme un service de conservation financière, il est crucial de clarifier les critères juridiques relatifs à la conservation, qui varient d'une juridiction à l'autre. En France et dans l'Union européenne, la notion de conservation des actifs numériques a évolué au fil des débats législatifs, notamment pour exclure certains acteurs tels que Ledger. Initialement, la réglementation incluait le stockage des clés privées cryptographiques dans la définition de la conservation, mais le Parlement français a ajusté cette définition pour ne plus assimiler le simple stockage des clés à un service de conservation financière.

Dans un document de 2020, l'AMF précise que la conservation inclut désormais non seulement la possession physique de clés, mais également le « contrôle des moyens d'accès » aux actifs en vertu d'une relation contractuelle. L'AMF ajoute qu'une API pourrait être perçue comme un moyen d'accès si elle confère un contrôle effectif sur les actifs du client.

Par conséquent, bien que dans certaines configurations, Dfns puisse héberger certains fragments de clé ou même tous les fragments dans ses environnements de stockage, l'entreprise n'a ni la capacité d'utiliser ces fragments de manière autonome pour exécuter des transactions, ni le droit contractuel de le faire. Ces deux éléments sont essentiels pour distinguer Dfns d'un conservateur qualifié de biens numériques. Dfns est avant tout une entreprise de cybersécurité soumise à des audits rigoureux par des contrôleurs externes tels que Deloitte ou KPMG, afin de vérifier nos déclarations relatives

CLARISSE HAGÈGE
DFNS_

aux processus internes et à notre technologie. Nous avons l'obligation de décrire avec précision le fonctionnement de Dfns et de répondre à des centaines de contrôles dans le cadre de certifications reconnues, telles que SOC 2, DORA, ISO 27001, ISO 27017 et ISO 27018. Notre sécurité repose notamment sur l'obligation pour chaque employé de signer cryptographiquement via une Yubikey pour accéder à certains services et exécuter des actions sensibles, souvent avec des approbations supplémentaires de personnes distinctes. Si un employé devait commettre une erreur ou un acte malveillant, non seulement cet acte serait détecté grâce aux journaux d'audit et aux systèmes de surveillance, mais des actions légales seraient engagées pour identifier et poursuivre l'auteur, en collaboration avec les forces de l'ordre. Par ailleurs, les polices d'assurance que nous avons en place contribuent à couvrir les éventuels dommages. Cela étant dit, les aspects que je viens d'aborder relèvent de la sécurité technique et juridique d'une solution de gestion de clés, que Dfns administre parfois en totalité ou partiellement selon le cas (ou que Dfns délègue au client lorsque celui-ci choisit de gérer lui-même les clés, ce qui est obligatoire aux Émirats ou à Hong Kong, par exemple). En revanche, la gestion stratégique et financière des actifs numériques demeure strictement du ressort d'un conservateur qualifié, un rôle distinct de celui que joue Dfns.

COMMENT RÉPONDEZ-VOUS AUX CRITIQUES SUR LE MANQUE DE RECUL SUR CETTE TECHNOLOGIE ?

Toutes les technologies, même les plus matures, présentent des vulnérabilités. Les solutions hardware, même certifiées FIPS, sont régulièrement piratées et exposées comme défaillantes lors de conférences de cybersécurité (ex. : CVE-2023-3470 est une vulnérabilité qui a été découverte en 2023 dans certaines plateformes F5 BIG-IP équipées de cartes Cavium Nitrox FIPS HSM). Cependant, la cryptographie à l'origine du MPC repose sur plusieurs décennies de recherche, et nous participons activement à sa standardisation. Nous sommes membres du board de la MPC Alliance depuis trois ans et collaborons avec le National Institute of Standards and Technology (NIST) sur l'élaboration de standards pour les signatures à seuil. Trois des cinq papiers sélectionnés par le NIST en 2023 pour leurs workshops sur le MPC proviennent de nos équipes de recherche.

Bien que le calcul multipartite sécurisé (MPC) soit encore en phase d'adoption dans la finance traditionnelle, il est déjà largement répandu dans la crypto-finance, avec plus de 2 000 entreprises et des millions d'utilisateurs bénéficiant de cette technologie pour protéger leurs actifs numériques. Nous sommes convaincus que c'est une question de temps avant que le MPC devienne un standard universel, notamment en combinaison avec des enclaves sécurisées (TEE) et des modules matériels de sécurité (HSM). Toutefois, si un client nous indique qu'il ne veut pas ou ne peut pas, souvent pour des raisons réglementaires ou de conformité, utiliser le MPC pour sécuriser ses clés, notre rôle n'est pas de défendre cette technologie à tout prix. Nous respectons totalement ce choix.

CLARISSE HAGÈGE
DFNS_

Au contraire, nous sommes ravis de collaborer étroitement avec Thales (avec qui nous sommes incubés à Station F), IBM, Securosys, Yubico et d'autres fournisseurs de HSM, dont nous sommes partenaires et revendeurs.

QUELS TYPES DE CLIENTS ET CAS D'USAGE CIBLEZ-VOUS ?

Notre infrastructure opère dans divers domaines de la finance numérique et de la blockchain. Dans le secteur bancaire et de la conservation d'actifs numériques réglementée (ou "qualified custody"), nous fournissons l'infrastructure de wallets à des acteurs majeurs comme Zodia Custody (la filiale crypto de la banque britannique Standard Chartered), Tungsten Custody (la filiale crypto du fonds souverain d'Abu Dhabi, ADQ) aux Émirats arabes unis, ABN AMRO, Fidelity International ou encore Eastern Point Trust aux États-Unis, qui font de l'administration de fonds pour Amazon, British Petroleum ou General Motors. Nous sommes également très actifs dans le secteur des paiements, où de nombreuses entreprises innovent autour des stablecoins. Nous fournissons des wallets et assurons la connectivité aux blockchains pour des acteurs tels que Bridge (récemment acquis par Stripe), Triple-A (le service de paiement crypto de Grab), Sphere (derrière Helium), ainsi que Vita, qui permet à plus de 500 000 utilisateurs en Amérique du Sud de réaliser des paiements crypto à moindre coût. Ces collaborations soutiennent le développement de solutions de paiements transfrontaliers et basés sur les stablecoins. La tokenisation est un autre axe important de notre activité, où nous travaillons avec des entreprises spécialisées telles que Tokeny, Bitbond, Nomyx, Zoniqx, Assetblocks et d'autres pour la tokenisation d'actifs financiers. Dans le secteur du trading et des échanges, nous sommes fiers de fournir l'infrastructure technologique du plus grand exchange canadien, NDAX, ou encore d'un DEX (échange décentralisé) singapourien appelé GRVT basé sur la blockchain ZkSync. Enfin, nous nous positionnons aussi sur le marché émergent des portefeuilles intégrés, en fournissant l'infrastructure de wallets "non-custodial" à des acteurs comme Socios, Billy et FIFA pour intégrer des wallets directement dans leurs plateformes.

QUELLE EST VOTRE POSITION SUR L'ÉVOLUTION DES WALLETS ET L'ABSTRACTION DE COMPTE ?

Nous avons observé avec intérêt le développement de l'abstraction de compte depuis la sortie de l'EIP 4337 pendant l'été 2023. Bien que nous ne soyons pas des développeurs de smart contracts, nous collaborons avec des acteurs comme ZeroDev, Biconomy et Safe, et avons intégré nos services de signatures digitales à leurs smart contracts pour permettre à nos clients d'expérimenter ces nouvelles fonctionnalités exclusives à Ethereum et aux EVM. Il est désormais évident que l'Account Abstraction via l'ERC 4337 n'a pas rencontré le succès escompté, avec des chiffres récents (cf Dune Analytics et BundleBear Review), tant en termes d'usage que de revenus, particulièrement décevants.

« Plutôt que de se focaliser sur les querelles idéologiques de l'industrie de la blockchain, nous devrions réfléchir à la manière d'encourager une adoption plus large en répondant aux besoins commerciaux et utilitaires concrets. »

CLARISSE HAGÈGE
DFNS_

De nombreux clients reviennent de cette expérimentation frustrés, tirant souvent la même conclusion : “tout ne peut pas être onchain”. Actuellement, c’est trop coûteux, lent et risqué, mais cela pourrait évoluer dans les prochaines années. C’est pourquoi nous restons vigilants et suivons de près les avancées techniques à venir. L’autre argument majeur contre l’utilisation de la blockchain pour toutes les opérations est le besoin de confidentialité. Une banque ne peut en aucun cas envisager de rendre publics les mouvements de son collatéral en temps réel, car cela ne serait pas autorisé par les autorités de régulation financière et pourrait même représenter un risque considérable pour la stabilité financière mondiale.

Il existe des initiatives comme le Canton Network dont l’objectif est de fournir un réseau public et confidentiel, mais il y a encore beaucoup de chemin à parcourir avant de voir un projet émerger qui fasse consensus. Dans tous les cas, à l’avenir, les wallets devront être rapides, interopérables et conformes aux réglementations locales, tout en intégrant des fonctionnalités avancées pour garantir la sécurité et la fluidité des transactions. Cela va se faire offchain si ça ne peut pas se faire onchain.

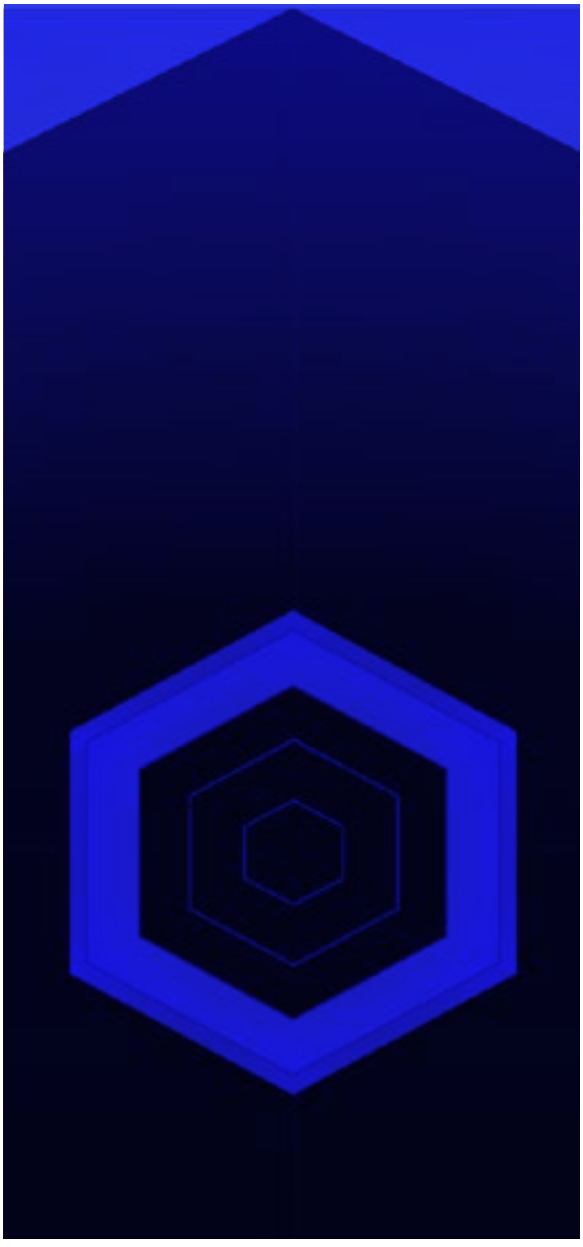
Soit dit en passant, nous pensons que les débats idéologiques et les querelles politiques, qui encombrent parfois l’industrie de la blockchain, détournent l’attention de son véritable potentiel commercial et de son utilité concrète pour le plus grand nombre. Plutôt que de s’y attarder, nous devrions tous réfléchir à la manière d’encourager une adoption plus large de cette technologie.

QUE PENSEZ-VOUS DES WALLETS NON-CUSTODIAL DANS LE CONTEXTE RÉGLEMENTAIRE ACTUEL ?

Nous héritons malheureusement de plus d’une décennie d’abus de langage qui brouille la compréhension des réalités techniques sous-jacentes, compliquant ainsi une appréhension claire des enjeux de sécurité et d’opérations liés aux concepts de “custodial” et “non-custodial wallets”. À ces termes s’ajoutent des expressions comme “self-custodial”, “co-custodial”, “cold storage”, “hot wallets”, et autres dénominations basées sur des températures. Cette prolifération de termes rend la tâche difficile aux régulateurs, législateurs et acteurs financiers qui tentent de s’orienter dans une industrie utilisant des mots à tout-va, souvent sans les comprendre, pour décrire des réalités qui n’en sont pas. C’est pourquoi nous nous opposons à bon nombre de ces termes, pratiques et à ceux qui les promeuvent. Avant tout, nous pensons qu’il est crucial (et urgent) de distinguer les aspects techniques des aspects juridiques. L’industrie crypto tend à confondre le terme “custodial” avec la simple possession de la clé privée. Mais que signifie vraiment “posséder la clé” ? Certains diront que c’est simple : la clé est mienne dès lors que je peux la retrouver sur mon wallet Metamask. Pourtant, cette clé privée réside souvent dans le navigateur de l’utilisateur, que ce soit Chrome ou Safari, lesquels appartiennent à Google et Apple, avec un accès potentiel pour leurs employés. Comment parler de “propriété” si le seul critère est un accès technique à la donnée ?

CLARISSE HAGÈGE
DFNS_

La vérité est qu'on ne peut pas définir cela de manière satisfaisante. C'est pourquoi le terme "custodial" doit être avant tout compris et défini sous l'angle contractuel et réglementaire, puisque c'est la seule manière qui permet aux propriétaires de recourir à la justice lorsqu'un désaccord a lieu ou une faute est commise. Ne pensons pas une seule seconde que le projet de la blockchain soit la fin de l'état de droit, ce serait une erreur d'appréciation très importante selon nous. Certes, les aspects techniques sont importants, et loin d'être négligés, mais chez Dfns, nous nous référons au cadre réglementaire de chaque pays pour déterminer ce qui est "custodial" ou non. Au lieu de cela, nous préférons parler de wallets "contrôlés par l'utilisateur" ou "contrôlés par l'organisation".



À QUOI LE WALLET DU FUTUR RESSEMBLERA-T-IL ?

Le wallet du futur ne se résume pas à qui fabriquera la plus belle interface, et il prendra forcément de nombreuses formes adaptées à différents secteurs et différentes situations réglementaires. Les besoins des paiements interbancaires diffèrent largement de ceux des microtransactions dans le gaming ou de la rémunération de freelances à l'international. Les wallets devront être interopérables, rapides et peu coûteux. Ils devront également être conformes aux lois locales et intégrés aux systèmes existants, notamment ceux des banques privées, des agences de transfert, des chambres de compensation, des banques centrales et des gouvernements. Enfin, nous pensons que l'avenir des wallets repose sur une agrégation complexe et intelligente de services où chaque composant (KYT, données de marché, stockage de la clé, gouvernance, smart contracts, échanges, noeud RPC, etc.) joue un rôle critique dans la gestion et la sécurisation de bout en bout des transactions financières sur les différentes blockchains.

03

Features

QUELLES FONCTIONNALITÉS POUR LE WALLET DU FUTUR ?

QUELLES FONCTIONNALITÉS POUR LE WALLET DU FUTUR ?_

ACCOUNT ABSTRACTION_
Simplification des signatures

Les utilisateurs de wallets actuels doivent souvent signer chaque transaction manuellement, ce qui peut être fastidieux. Avec l'account abstraction, les signatures manuelles pour chaque transaction seront éliminées. Cette fonctionnalité permet d'automatiser de nombreuses actions, rendant l'expérience utilisateur plus fluide et moins technique. Les utilisateurs peuvent définir des règles ou autorisations automatiques, permettant au wallet d'effectuer certaines opérations sans nécessiter une signature pour chaque transaction. Cela rend le wallet plus intuitif, notamment pour les interactions fréquentes avec des smart contracts.

PASSKEYS_
Sécurité simplifiée

Les passkeys sont un remplacement futuriste des mots de passe et des clés privées, combinant simplicité et sécurité. Plutôt que de stocker une clé privée complexe, les passkeys permettent d'utiliser des méthodes d'authentification biométrique (empreinte digitale, reconnaissance faciale) ou des tokens sécurisés pour accéder au wallet. Cette technologie peut rendre l'expérience de gestion des wallets beaucoup plus simple, tout en renforçant la sécurité. Finis les mots de passe oubliés ou les clés perdues : les utilisateurs pourront accéder à leurs wallets de manière rapide et sécurisée.

SOCIAL RECOVERY_
Réseau de confiance pour la récupération

La social recovery (récupération sociale) offre une solution au problème des wallets irrécupérables en cas de perte de clés privées. Grâce à ce système, les utilisateurs peuvent désigner des contacts de confiance, comme des amis ou des membres de la famille, pour les aider à récupérer l'accès à leur wallet en cas de perte d'accès. Plutôt que de dépendre uniquement de la sécurité personnelle, le wallet serait restauré via une validation par un réseau social pré-défini. Cette fonctionnalité ajoute une couche de résilience en cas de perte ou de compromission des moyens d'accès.

QUELLES FONCTIONNALITÉS POUR LE WALLET DU FUTUR ?_

SPONSORING DES FRAIS DE GAZ_

Moins de frictions pour l'utilisateur

Les transactions sur blockchain nécessitent des frais de gaz, ce qui peut parfois être un obstacle pour les utilisateurs. Dans le wallet du futur, certaines applications peuvent sponsoriser ces frais, éliminant ainsi la nécessité pour l'utilisateur de gérer constamment ses soldes en tokens natifs pour payer ces frais. Par exemple, une application de finance décentralisée (DeFi) pourrait couvrir les coûts de transaction pour offrir une expérience plus fluide à ses utilisateurs. Cela encouragerait une adoption plus large, en particulier chez les utilisateurs non familiers avec les mécanismes des blockchains.

ABSTRACTION DES DIFFÉRENTES BLOCKCHAINS_

Dans le futur, les wallets devront être capables de masquer la complexité des blockchains sous-jacentes. L'utilisateur ne devrait pas avoir à se soucier de savoir sur quelle blockchain une transaction est effectuée (Ethereum, Solana, etc.). Le wallet du futur intégrerait une interopérabilité transparente entre les différentes blockchains, offrant une expérience unifiée où les utilisateurs peuvent envoyer des fonds ou interagir avec des applications décentralisées sans se préoccuper de la blockchain spécifique utilisée. Cette abstraction des blockchains permettrait une meilleure adoption du Web3, car les utilisateurs seraient confrontés à moins de frictions techniques.

RELEVÉS DE TRANSACTIONS CLAIRS POUR L'ADMINISTRATION FISCALE_

Les utilisateurs actuels doivent souvent naviguer à travers des interfaces complexes pour obtenir des relevés de transactions qu'ils peuvent soumettre aux autorités fiscales. Le wallet du futur fournira des relevés simples, accessibles et détaillés, automatiquement formatés pour les déclarations fiscales. Cela inclurait des résumés clairs des gains, des pertes et des frais, facilitant ainsi la tâche aux utilisateurs lorsqu'il s'agit de se conformer aux obligations fiscales. Une telle fonctionnalité augmenterait la transparence et offrirait aux utilisateurs une meilleure gestion de leur portefeuille crypto au niveau administratif.

04

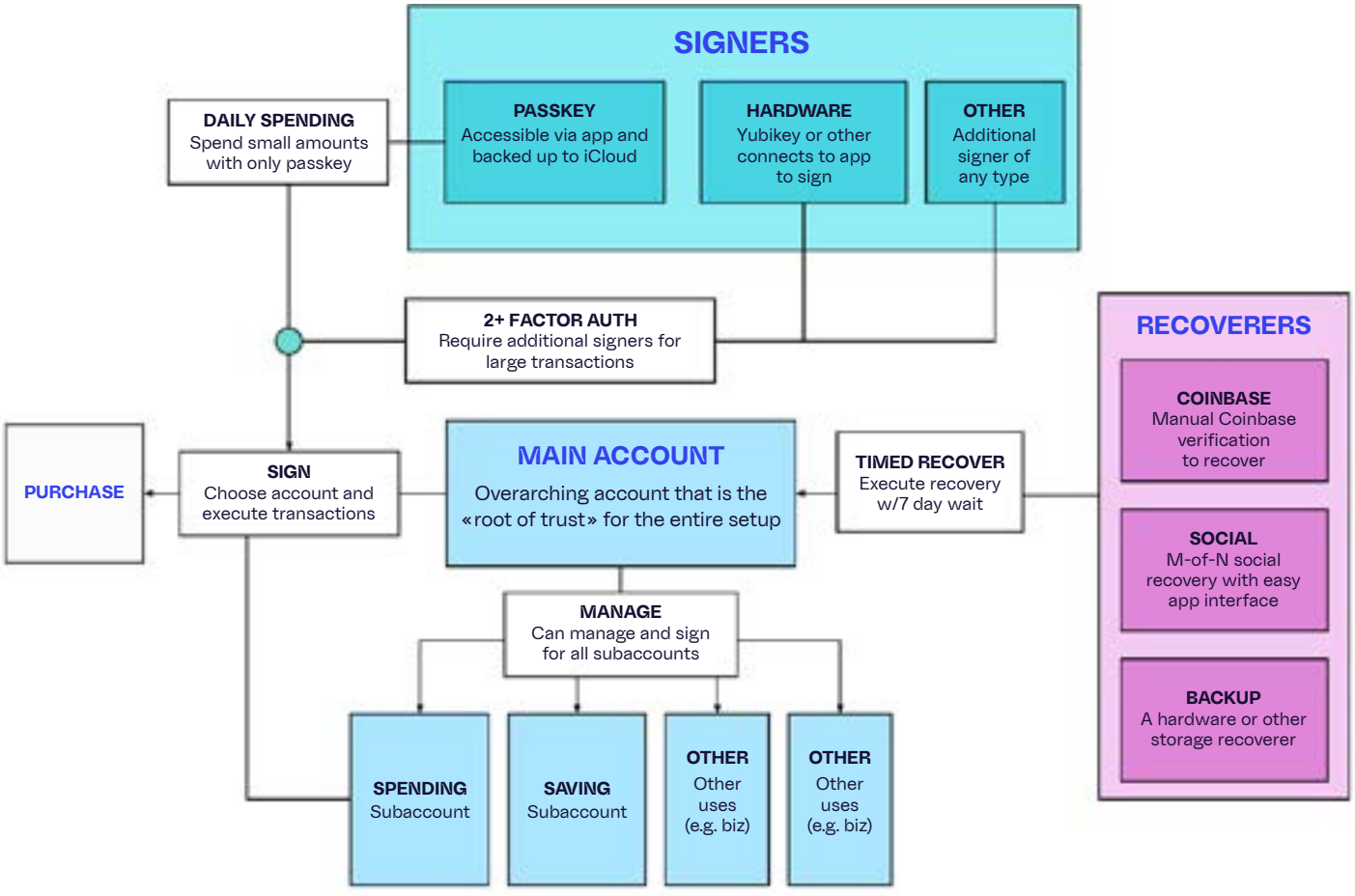
Perspectives

L'ARCHITECTURE DU WALLET DU FUTUR SELON JESSE POLLAK

L'ARCHITECTURE DU WALLET DU FUTUR, SELON JESSE POLLAK_

JESSE POLLAK EST LE CRÉATEUR DE BASE, LA BLOCKCHAIN L2 DE COINBASE.
IL EST ÉGALEMENT EN CHARGE DE LA TOUTE PARTIE WALLET POUR LE GÉANT AMÉRICAIN. IL PUBLIÉ LE 13 AOÛT 2024 SUR TWITTER CE QU'IL IMAGINE COMME "DREAM WALLET".

« J'ai esquissé mon wallet de rêve qui serait 10 fois meilleur que tout ce qui existe aujourd'hui sur le Web2 ou sur blockchain. Il faut résoudre un tas de défis difficiles, mais je pense que nous pouvons y arriver dans les 6 à 12 prochains mois. »



05

Business

QUELS MODÈLES ÉCONOMIQUES POUR LES FOURNISSEURS DE WALLETS ?

QUELS MODÈLES ÉCONOMIQUES POUR LES FOURNISSEURS DE WALLETS ?_

Les wallets comme Metamask et Rabby sont devenus des portes d'entrée incontournables vers le Web3 en facilitant l'interaction avec les dApps, profitant de l'essor de la DeFi et des NFT. Leur succès repose en grande partie sur une stratégie d'acquisition d'utilisateurs agressive : des solutions gratuites et intégrées aux écosystèmes Web3 ont attiré des millions d'utilisateurs, sans barrières économiques.

Cependant, avec une base solide d'utilisateurs, ces wallets orientent désormais leur modèle vers la monétisation, en ajoutant discrètement des frais pour tirer profit de cette large audience sans compromettre leur croissance initiale. Mais plutôt que d'imposer des abonnements ou des frais d'utilisation traditionnels, ces wallets ont progressivement mis en place des frais discrets, souvent perçus comme "invisibles" par l'utilisateur moyen.

1_FRAIS SUR LES SWAPS

Les échanges de tokens directement dans les wallets via des services intégrés de swap sont devenus un service clé pour de nombreux utilisateurs. Metamask, par exemple, facture des frais de 0,875 % sur chaque transaction de swap effectuée par ses utilisateurs. Rabby prélève quant à lui 0,25%. Pour les utilisateurs qui préfèrent la facilité, ces frais passent souvent inaperçus, mais ils constituent une source de revenus majeure pour les wallets.

Les wallets comme Metamask et Rabby sont devenus des portes d'entrée incontournables vers le Web3 en facilitant l'interaction avec les dApps, profitant de l'essor de la DeFi et des NFT.

QUELS MODÈLES ÉCONOMIQUES POUR LES FOURNISSEURS DE WALLETS ?_

2_FRAIS SUR LES SERVICES D'ON/OFF-RAMP

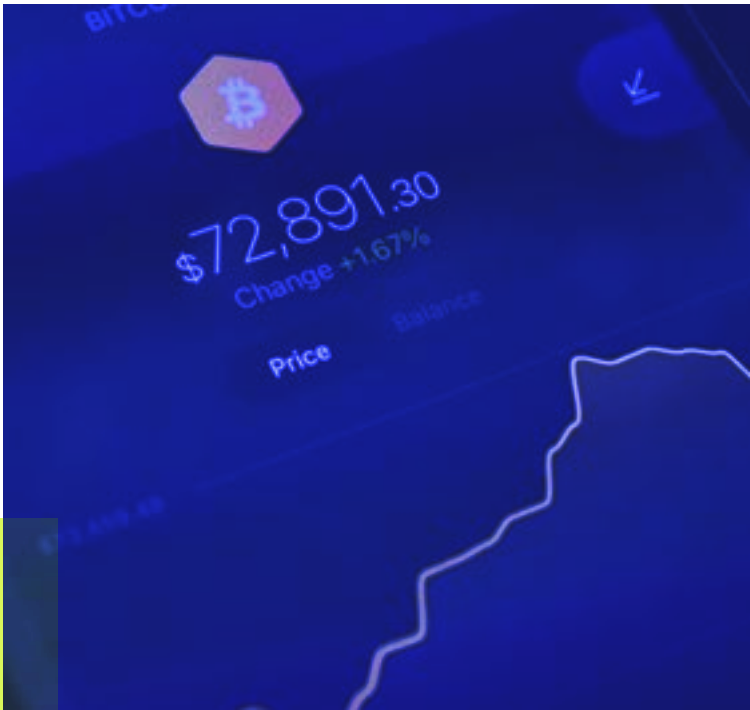
Alors que de plus en plus de personnes souhaitent convertir leurs devises fiat contre crypto directement depuis leur wallet, les hot wallets ont introduit des solutions d'on/off-ramp, c'est-à-dire des services partenaires permettant d'acheter ou vendre des cryptos en monnaie fiat sans quitter l'application. Ces services sont également l'occasion pour les wallets de facturer des frais supplémentaires sur chaque transaction. Ces frais peuvent varier selon les prestataires et les moyens de paiement, mais ils ajoutent une autre couche de revenus pour les entreprises derrière les wallets.

3_FRAIS SUR LES CARTES DE PAIEMENT

De plus en plus de wallets explorent l'idée d'introduire des cartes de paiement liées aux wallets crypto, permettant aux utilisateurs de dépenser directement leurs cryptos dans les commerces traditionnels. Cette approche vise à fidéliser les utilisateurs tout en captant des frais sur les transactions effectuées avec ces cartes. Dans ce cadre, ils jouent le rôle d'apporteurs d'affaires auprès des émetteurs de cartes, qui leur rétrocèdent une partie des commissions. L'un des exemples à retenir est celui du wallet Argent, qui travaille avec Kulipa et Mastercard. Ces multiples frais, bien que souvent modestes, peuvent s'accumuler pour créer des flux de revenus importants. Ils permettent à ces entreprises de monétiser leur audience de manière efficace, sans imposer de coûts directs pour l'utilisation de base du wallet.

DES TOKENS DE WALLETS : UNE STRATÉGIE INCERTAINE

Parallèlement à cette stratégie de monétisation discrète, certains wallets comme Rabby envisagent de lancer leurs propres tokens natifs. Cette démarche s'inscrit dans une tendance observée dans le Web3, où de nombreuses plateformes ont émis leurs tokens pour dynamiser leur communauté et créer des incitations économiques pour les utilisateurs. Cependant, cette approche n'est pas sans risques. Les tokens émis par les wallets peuvent devenir un double tranchant. D'un côté, ils peuvent offrir des avantages : gouvernance décentralisée, réductions de frais pour les utilisateurs qui détiennent des tokens, ou encore programmes de staking permettant de fidéliser une partie de l'audience. De l'autre, la volatilité des tokens et leur dépendance aux cycles du marché crypto peuvent rendre cette stratégie hasardeuse. Beaucoup de projets ayant lancé des tokens se sont retrouvés confrontés à des fluctuations de prix importantes, compromettant ainsi leur modèle économique ou leur attractivité à long terme.



06

Mapping

LA CARTOGRAPHIE DE L'ÉCOSYSTÈME DES WALLETS

LA CARTOGRAPHIE DE L'ÉCOSYSTÈME DES WALLETS_

_Hardware wallets

LEDGER KEYSTONE PASSPORT TREZOR COLDCARD SEEDSIGNER

_Hot wallet [browser extension]

COINBASE WALLET XDEFI PHANTOM RABBY

EXODUS KEPLR TRUST WALLET METAMASK

_Mobile wallets MPC

ZENGO WEB 3 WALLET (BINANCE)

DEBLOCK

_Fournisseurs de solutions wallet-as-a-service

FIREBLOCKS DFNS THAURUS

COMETH LEDGER ENTERPRISE

_Banques/Fintech proposant des wallets

BANQUE DELUBAC CASHAPP ROBINHOOD

STRIPE PAYPAL REVOLUT

LA CARTOGRAPHIE DE L'ÉCOSYSTÈME DES WALLETS_

_Wallets mobile non-custodial


EXODUS


COINBASE WALLET


XDEFI


RABBY


PHANTOM


KEPLR


TRUST WALLET


METAMASK

_Smart wallets


CLAVE


INFINEX


COINBASE SMART WALLET


SAFE


KRAKEN WALLET


ARGENT WALLET

_Custodians institutionnels


ANCHORAGE


KOMAINU (AVEC LEDGER ENTERPRISE)


XAPO


BANQUE DELUBAC


BITGO

CACEIS


COINBASE CUSTODY


SG FORGE

_Wallets spécialisés dans la vie privée


BRUME


WASABI


ASHIGARU (FORK SAMOURAI)

_Services pour wallets


NARVAL


ADAMIK

07

Entretien

PIERRE D'ORMESSON

« LA DISTINCTION EST CLAIRE : DÉTENIR LES CLÉS PRIVÉES, C'EST ÊTRE RÉGULÉ »

PIERRE D'ORMESSON
DLA PIPER_

L'AVOCAT PIERRE D'ORMESSON DÉCRYPTE LES ENJEUX JURIDIQUES LIÉS À LA RÉGLEMENTATION DES WALLETS CRYPTOS, EN METTANT EN LUMIÈRE LES DISTINCTIONS ENTRE WALLETS CUSTODIAL ET AUTO-HÉBERGÉS, AINSI QUE LES IMPACTS DU RÈGLEMENT MICA.

> **« La distinction est claire : détenir les clés privées, c'est être régulé »**

QUEL EST L'ÉTAT DE LA RÉGLEMENTATION DES WALLETS CRYPTOS ?

Pour aborder ce sujet, il y a deux angles principaux. D'abord, celui des prestataires de services. La réglementation actuelle vise principalement à encadrer les prestataires de services sur crypto-actifs, qu'ils soient agréés ou enregistrés. Une fois régulés, ils doivent respecter un ensemble de règles, y compris celles de lutte contre le blanchiment d'argent (AML) et le financement du terrorisme, sous la supervision d'une autorité de contrôle. Concrètement, si un prestataire propose des services de conservation de cryptos ou de gestion de clés privées pour des tiers en France, il est soumis à des obligations strictes. Avec l'entrée en application du règlement MiCA prochainement, ces prestataires devront obtenir un agrément formel, similaire à celui des entreprises d'investissement, et mettre en place des processus internes pour se conformer aux règles de contrôle des risques, anti-blanchiment et de transparence. Ensuite, il y a l'angle utilisateur. Ceux qui utilisent des wallets auto-hébergés (self-hosted), tant qu'ils n'utilisent pas de plateformes régulées, ne sont pas soumis aux mêmes règles. Mais dès qu'ils passent par un prestataire de services (comme un exchange centralisé), ce prestataire doit respecter des obligations telles que la vérification d'identité, la traçabilité des fonds (notamment via la travel rule), et la surveillance des transactions. Ces règles proviennent en grande partie du règlement TFR (Transfer of Funds Regulation), qui impose des vérifications supplémentaires pour tout transfert de plus de 1 000 euros impliquant un wallet non custodial.

CES DISPOSITIONS SONT-ELLES DÉJÀ EN VIGUEUR OU EN PROJET ?

Certaines de ces dispositions sont déjà en vigueur, notamment le régime PSAN (bientôt remplacé par MiCA) a dès le départ introduit des règles de lutte contre le blanchiment pour les prestataires. Mais d'autres, comme MiCA et TFR, ne seront pleinement appliquées qu'à partir du 30 décembre 2024. Bien que MiCA soit déjà adopté, il reste un délai avant la mise en œuvre complète (les prestataires ayant fourni des services sous le régime PSAN peuvent continuer sous ces règles pour une période maximale de 18 mois, soit jusqu'au 1er juillet 2026). Les prestataires historiques disposent donc encore de temps pour se conformer aux nouvelles règles, mais pour l'AML, la plupart des exigences sont déjà en vigueur.

DU CÔTÉ DES FOURNISSEURS TECHNOLOGIQUES DE WALLETS, Y A-T-IL DES OBLIGATIONS LÉGALES ?

Les fabricants de hardware wallets, comme Ledger, ne sont pas soumis à des obligations légales en tant que custodians, car ils ne conservent pas les clés privées pour leurs utilisateurs. Un hardware wallet comme Ledger est un simple outil, et l'utilisateur garde le contrôle total de ses actifs. Les distributeurs de hardware wallets ne sont donc pas enregistrés ni agréés comme prestataires de services sur actifs numériques selon la réglementation actuelle, car ils ne fournissent pas de services régulés.

PIERRE D'ORMESSON
DLA PIPER_

Les wallets auto-hébergés, comme Metamask, sont souvent associés à une plus grande liberté et un contrôle direct pour l'utilisateur.

COMMENT LES RÉGULATEURS ENVISAGENT-ILS DE CONCILIER CELA AVEC LA LUTTE CONTRE LA FRAUDE ET LE BLANCHIMENT D'ARGENT ?

Effectivement, les wallets auto-hébergés offrent plus de liberté à l'utilisateur. Cependant, tant qu'ils restent en dehors des plateformes régulées, les utilisateurs ne sont pas tenus aux mêmes obligations de conformité. Les régulateurs ne peuvent pas directement encadrer ces utilisateurs ou leurs transactions, sauf s'ils utilisent un service régulé, comme un exchange ou un prestataire de services. Dès que l'utilisateur passe par une plateforme régulée, celle-ci a l'obligation d'appliquer les règles anti-blanchiment, comme la vérification d'identité, la surveillance des transactions et la déclaration des origines des fonds.

« Si un prestataire détient les clés privées d'un utilisateur, il est considéré comme fournissant un service de conservation d'actifs numériques et doit être régulé en tant que tel. »

En somme, les régulateurs interviennent uniquement lorsqu'un prestataire est impliqué, ce qui laisse une certaine liberté aux utilisateurs auto-hébergés tant qu'ils restent en dehors de ces services.

QU'EST-CE QUI DÉFINIT JURIDIQUEMENT UN WALLET AUTO-HÉBERGÉ PAR RAPPORT À UN WALLET CUSTODIAL ?

C'est une question clé. La différence principale repose sur la détention des clés privées. Un wallet auto-hébergé signifie que l'utilisateur détient et contrôle entièrement ses clés privées, lui permettant de gérer ses actifs sans passer par un tiers. Dans un wallet custodial, le prestataire de services détient les clés privées au nom de l'utilisateur et gère les actifs pour son compte. Si un prestataire détient les clés privées d'un utilisateur, il est considéré comme offrant un service de conservation d'actifs numériques et doit être régulé en tant que tel.

CONCRÈTEMENT, QUELLES SONT LES OBLIGATIONS LÉGALES DES ENTREPRISES QUI PROPOSENT DES WALLETS CUSTODIAL ?

Les règlements MiCA et TFR auront un impact significatif sur les fournisseurs de wallets conservant des crypto-actifs pour des tiers. Ils devront obtenir un agrément et se conformer à de nouvelles règles. Cela comprend la mise en place de politiques de contrôle interne, de gestion des conflits d'intérêts, d'externalisation, ainsi que de ségrégation des actifs pour assurer la sécurité des fonds, en plus des obligations liées à l'AML et à la prévention des abus de marché. De plus, MiCA et TFR introduiront de nouvelles exigences en matière de transparence et de reporting aux régulateurs, ce qui signifie que les prestataires devront non seulement vérifier l'identité de leurs utilisateurs, mais aussi surveiller les transactions pour détecter toute activité suspecte.

PIERRE D'ORMESSON
DLA PIPER_

COMMENT LA TECHNOLOGIE MPC (MULTI-PARTY COMPUTATION) POURRAIT-ELLE IMPACTER LA RÉGULATION DES WALLETS ?

La technologie MPC, qui permet de diviser une clé privée en plusieurs fragments et de distribuer ces fragments entre plusieurs parties, pose une question intéressante d'un point de vue réglementaire. Si un prestataire détient seulement un fragment de la clé privée, peut-il encore être considéré comme un custodian ? Pour l'instant, il n'y a pas de réponse claire à cette question dans la réglementation actuelle en France, et cela nécessiterait probablement une clarification de la part des régulateurs ou des autorités compétentes.

IL EXISTE UN DÉBAT POUR RÉGULER LES WALLETS NON CUSTODIAL, QUELLE EST VOTRE POSITION SUR LE SUJET ?

C'est une question très intéressante et prospective. Il est possible qu'à l'avenir, les régulateurs imposent des obligations de vérification d'identité (KYC) même dans les transactions entre wallets non-custodiaux. Actuellement, ces wallets ne sont pas soumis à de telles obligations, mais cela pourrait évoluer si les régulateurs estiment qu'il y a un risque accru de blanchiment d'argent ou de financement du terrorisme. Pour l'instant, Metamask et des wallets similaires ne réalisent pas directement de KYC, car ils fonctionnent principalement comme un logiciel d'interface pour les wallets auto-hébergés. Ils dépendent de partenaires tiers comme MoonPay ou Ramp pour la conversion entre crypto et fiat, qui effectuent les vérifications KYC nécessaires. Tant que ces intermédiaires remplissent leurs obligations de conformité, Metamask n'a pas besoin de s'impliquer directement dans ces processus.

Cependant, si aucune vérification KYC n'est effectuée dans la chaîne de transaction, cet anonymat pourrait poser problème, et les régulateurs pourraient alors exiger que Metamask intervienne. Pour l'instant, les régulateurs n'interviennent pas auprès de ces acteurs, et les législateurs semblent se satisfaire de la situation tant qu'une partie de la chaîne prend en charge la vérification des identités et la traçabilité des transactions.

« Aux États-Unis, la réglementation est beaucoup plus fragmentée, reposant largement sur des décisions de justice et des régulations spécifiques à chaque État ou régulateur fédéral, ce qui signifie que les règles peuvent varier selon les juridictions. »

PIERRE D'ORMESSON
DLA PIPER_

QUELS SONT LES COÛTS DE CONFORMITÉ ?

Se conformer à MiCA représente plusieurs défis importants pour un prestataire. Passer d'un simple enregistrement PSAN (prestataire de services d'actifs numériques) à un agrément complet est complexe. Sous MiCA, cela inclut des exigences de capitalisation prudentielle, de gouvernance interne et de procédures de conformité allant bien au-delà des règles actuelles de l'enregistrement AMF (Autorité des marchés financiers) en France. Les prestataires devront, par exemple, mettre en place des politiques de signalement d'alerte, une cybersécurité renforcée et une gestion plus stricte des risques. Ils seront également soumis à une supervision continue par les régulateurs, comme l'AMF ou l'ACPR, avec des obligations de reporting régulières. En termes de coût, cette mise en conformité peut rapidement devenir onéreuse. Bien que l'agrément en tant que tel ne soit pas payant, l'accompagnement juridique pour l'obtenir, les coûts opérationnels pour répondre aux exigences et les coûts liés à l'embauche d'une équipe dédiée à la conformité et à la cybersécurité peuvent représenter plusieurs centaines de milliers d'euros. Pour les grandes structures, le coût d'obtention de l'agrément MiCA peut atteindre environ 500 000 euros, ce qui inclut les frais initiaux et les coûts continus de gestion et de supervision.

EST-CE QUE LA RÉGLEMENTATION DES WALLETS DIFFÈRE BEAUCOUP D'UNE RÉGION À L'AUTRE, PAR EXEMPLE ENTRE LES ÉTATS-UNIS, L'EUROPE ET L'ASIE ?

Oui, il existe des différences notables selon les régions. En Europe, la réglementation tend à s'harmoniser grâce à MiCA, qui introduira un cadre uniforme pour toute l'Union européenne. Cela permet aux entreprises de savoir précisément à quelles obligations elles seront soumises, qu'elles opèrent en France, en Allemagne ou en Espagne. C'est une approche très structurée, avec des règles claires sur la conservation d'actifs, la gestion des risques et les possibilités de fournir des services dans d'autres pays de l'UE. Aux États-Unis, en revanche, la réglementation est bien plus fragmentée. Elle repose largement sur des décisions de justice et des régulations spécifiques à chaque État ou à chaque régulateur fédéral, comme la SEC ou la CFTC, ce qui signifie que les règles peuvent varier selon les juridictions. En Asie, la situation est encore plus diversifiée. Certains pays, comme Singapour et le Japon, ont adopté des cadres réglementaires clairs pour les actifs numériques, tandis que d'autres pays, comme la Chine, refusent cette classe d'actifs, et d'autres encore élaborent leurs propres règles. Chaque région adopte une approche différente en fonction de ses priorités en matière de sécurité, d'innovation et de gestion des risques.

08

Tribune

CLAIRE BALVA

« L'INÉVITABLE ALLIANCE
DES WALLETS
AVEC LES BANQUES »

CLAIRE BALVA
DEBLOCK_

FACE À LA TENDANCE D'UNE ALLIANCE ENTRE BANQUES ET PLATEFORMES CRYPTO, LES WALLETS FONT ENCORE OFFICE DE PURISTES VOIRE DE PIRATES. PEUT-ÊTRE PLUS POUR LONGTEMPS, COMME L'ESTIME CLAIRE BALVA, VP STRATÉGIE DE LA FINTECH DEBLOCK.

> **« L'inévitable alliance des wallets avec les banques »**

Spectateurs de l'alliance médiatisée entre les acteurs centralisés crypto et le monde de la finance traditionnelle, de nombreux wallets offrent désormais des moyens de convertir ses cryptos en monnaie fiduciaire (l'on/offramp). Ces solutions, principalement dépendantes de partenaires régulés, demeurent néanmoins imparfaites. Les utilisateurs font face à de nombreuses limitations, particulièrement pour la vente de cryptos, avec des montants plafonnés, des processus de vérification d'identité (KYC) parfois complexes ou retardés, et des rejets bancaires après avoir payé des frais élevés. De nombreux wallets envisagent ainsi sérieusement l'IBAN-isation (optionnelle) de leurs utilisateurs. L'introduction de ce service pourrait par ailleurs simplifier l'utilisation des wallets pour un public plus large et démocratiser encore l'accès aux cryptos. Il s'agit néanmoins d'un sujet délicat, notamment pour les wallets axés sur Bitcoin ou les solutions de couche 2 (L2), dont les communautés prônent la confidentialité. Introduire des services comme l'ouverture de comptes de paiement fiat va souvent à l'encontre de cette philosophie : cela impose des contraintes réglementaires strictes, comme l'identification du client (KYC), rendant la confidentialité impossible.

UN TERRAIN FERTILE POUR LES RÉGULATEURS

Si le KYC ne serait probablement imposé qu'au moment de la création d'un IBAN dans le wallet, l'impact pourrait, à terme, être bien plus large. Ce simple pas vers un service régulé ouvre la voie à une supervision par les régulateurs, qui auront désormais une porte d'entrée pour surveiller de plus près les activités jusqu'ici considérées comme hors système. Jusqu'ici, les autorités préféraient largement les plateformes d'échange aux wallets, qu'elles ne pouvaient pas superviser. Les tentatives de régulation passées, telles que certains amendements au règlement MiCA, visaient justement à limiter l'attrait de la self-custody en dissuadant les utilisateurs de retirer leurs cryptos du système réglementé. L'ajout de services bancaires au sein des wallets, même s'ils sont optionnels, pourrait changer la donne : elle permettra aux autorités de suivre plus précisément les flux de capitaux, en étant capables d'identifier les utilisateurs derrière les wallets. Les flux crypto ne pourront pas être censurés, mais seront encore plus traçables. L'arrivée de la finance traditionnelle dans les wallets est donc une aubaine pour les régulateurs, en leur permettant d'étendre leur influence, de manière "douce" et sans législation supplémentaire, sur la self-custody.

CLAIRE BALVA
DEBLOCK_

LES WALLETS COMME NOUVEAU POINT CENTRAL DE L'UX

Si certains maximalistes crieront peut-être au scandale, il y a fort à parier que l'intérêt commercial sera la boussole de la plupart des wallets. La demande pour centraliser l'expérience utilisateur dans un même outil, ou en tout cas pour limiter le nombre d'applications différentes, est forte. Avoir au même endroit son IBAN et son wallet a une vraie valeur en termes de praticité et de gestion financière, comme en atteste le succès de Deblock en à peine quelques mois. Face à cette demande d'une expérience utilisateur "tout-en-un", les wallets auront essentiellement trois possibilités. La première consisterait à refuser toute entrée du système réglementé dans leur application. Ce sera probablement le choix des plus engagés. mais qui freinera le passage à l'échelle de leur service. Les portefeuilles pourraient, à l'inverse, entreprendre eux-mêmes les démarches pour obtenir les licences nécessaires afin d'offrir des services bancaires. Mais être dans le giron direct du régulateur signifierait un coût de mise en conformité élevé.

La troisième option serait de s'allier avec des prestataires spécialisés, déjà régulés, dans une logique de Banking-as-a-Service (BaaS), détenteurs en Europe d'une licence EMI ou PSP. Cette option est sans doute la plus réaliste, car elle permettra aux wallets de continuer à se concentrer sur leur cœur de métier en élargissant sereinement leur base de services financiers. Les intégrations entre services bancaires et wallets augurent de profondes transformations et des sources de revenus particulièrement lucratives pour ces acteurs. Ces opportunités, combinées à la concentration croissance du secteur, laissent entrevoir de futurs rapprochements entre wallets, fintech et acteurs bancaires. Alors que les acquisitions de plateformes d'échange sont déjà une possibilité assumée, les banques se tourneront-elles prochainement vers les wallets pour mettre un pied dans la crypto ?

09

Innovation

SMART WALLETS, LE FUTUR POUR LES PARTICULIERS ?

SMART WALLETS, LE FUTUR POUR LES PARTICULIERS ?_

Ethereum propose deux types de comptes : les comptes externes (EOA), contrôlés par une clé privée, et les comptes de smart contracts, gérés par du code blockchain. Contrairement aux wallets traditionnels comme MetaMask, limités à la gestion des clés privées, les smart wallets utilisent des smart contracts qui offrent des fonctionnalités avancées (récupération sociale, limites de dépenses, approbations multi-signatures). Alors que les wallets classiques reposent sur la responsabilité de l'utilisateur pour sécuriser ses actifs, les smart wallets offrent plus de flexibilité et de sécurité via des fonctions programmables, rendant l'accès aux actifs numériques plus simple et sûr pour tous.

LES AVANTAGES_

Sécurité renforcée et optimisée

Les smart wallets offrent une sécurité renforcée grâce à des options avancées de récupération de compte, telles que la récupération sociale, ainsi qu'à des fonctionnalités de multi-signature. Ces mesures permettent non seulement de protéger les utilisateurs contre la perte accidentelle d'accès, mais aussi d'ajouter des mesures de protection supplémentaires contre les tentatives de piratage.

Personnalisation et automatisation

Grâce à leur programmation, les smart wallets permettent des transactions personnalisées et automatisées. Ils peuvent exécuter des tâches complexes de manière autonome, ce qui permet aux utilisateurs de définir, par exemple, des limites de dépenses, d'automatiser des paiements récurrents ou d'établir des conditions d'autorisation spécifiques. Par conséquent, ces portefeuilles facilitent l'automatisation des processus, permettant des transactions sans nécessiter d'intervention manuelle à chaque étape, ce qui rend la gestion des actifs numériques plus simple et efficace.

Réduction des coûts

Les smart wallets permettent de réduire les frais de gaz en regroupant plusieurs opérations en une seule transaction. Dans certains cas, les frais peuvent même être entièrement annulés grâce à l'utilisation de paymasters. Ces entités tierces financent les frais de transaction pour le compte des utilisateurs, permettant ainsi d'effectuer des opérations sur la blockchain sans avoir à détenir de crypto pour payer les frais de gaz. Cette fonctionnalité rend l'utilisation de la blockchain à la fois plus abordable et plus fluide.

Amélioration de l'expérience utilisateur

Les smart wallets simplifient considérablement l'expérience utilisateur en supprimant la nécessité de gérer des clés privées ou des phrases de récupération. En remplaçant la gestion des clés traditionnelles par des méthodes modernes telles que l'authentification biométrique ou les passkeys, ils rendent l'utilisation plus fluide et accessible, réduisant ainsi les obstacles pour les nouveaux utilisateurs. Cette approche facilite l'intégration des nouveaux utilisateurs.

SIMPLIFIER L'ACCÈS : PASSKEYS, COMPTES GOOGLE ET APPLE, ET AUTHENTIFICATION BIOMÉTRIQUE_

Les smart wallets transforment l'accès aux crypto en éliminant la nécessité de gérer une clé privée pour chaque utilisateur. Grâce à des comptes de smart contracts, ces portefeuilles proposent des méthodes de récupération simplifiées, comme l'intégration de comptes Google et Apple, des passkeys et des options d'authentification biométrique telles que Face ID. Cela change la manière dont les utilisateurs interagissent avec la blockchain.

La gestion des clés privées a longtemps été un frein à l'adoption des wallets crypto et du Web3. Avec plusieurs options d'authentification, les smart wallets rendent la blockchain accessible à un public plus large, y compris ceux moins familiers avec la technologie.

SMART WALLETS, LE FUTUR POUR LES PARTICULIERS ?_

LES MEILLEURS SMART WALLETS_

COINBASE SMART WALLET

Le 5 juin 2024, Coinbase a lancé son Smart Wallet, un portefeuille crypto conçu pour simplifier l'expérience utilisateur sur la blockchain. Actuellement en testnet, il offre une inscription rapide et directe via navigateur, sans extension ni application externe. Les utilisateurs se connectent et signent des transactions grâce aux passkeys, des clés de sécurité locales sauvegardées via iCloud ou Google Password Manager, éliminant ainsi la complexité des phrases de récupération. L'accès se fait facilement via des options biométriques comme l'empreinte digitale. Le Smart Wallet est compatible avec 8 blockchains EVM, telles qu'Ethereum, Polygon et Base, et permet un accès fluide aux applications décentralisées.

Grâce à la fonctionnalité "paymaster" de Coinbase, certaines dApps peuvent prendre en charge les frais de transaction, rendant l'expérience sans frais de gaz. Avec son système de compte unifié, le Smart Wallet simplifie la connexion à toutes les applications onchain avec une seule adresse, et la fonction MagicSpend permet de dépenser des fonds directement depuis le compte Coinbase. Construit sur la norme ERC-4337, le Smart Wallet prend en charge les transactions groupées et sponsorisées, optimisant les interactions avec les dApps. Les smart contracts de Coinbase sont régulièrement audités, assurant ainsi une sécurité renforcée pour chaque transaction.

SMART WALLETS, LE FUTUR POUR LES PARTICULIERS ?_

LES MEILLEURS SMART WALLETS_

INFINEX

Lancé en mai 2024, le Smart Wallet d'Infinex, appelé Infinex Account, vise à offrir une expérience fluide et sécurisée dans la DeFi. Développé par Kain Warwick, fondateur de Synthetix, ce wallet non-custodial utilise des smart contracts et des passkeys, permettant aux utilisateurs de conserver un contrôle total sur leurs actifs sans intermédiaires.

L'inscription, rapide et sans extension, se fait via des passkeys, générées et stockées localement, avec des options de connexion biométriques comme Face ID ou empreinte digitale. Infinex Account est compatible avec six blockchains (et pas uniquement des EVM), dont Ethereum, Solana et Arbitrum, facilitant l'accès à de nombreuses applications DeFi avec un seul portefeuille.

Il propose également un mécanisme de récupération par authentification sociale via Google ou Apple, offrant une sécurité accrue en cas de perte d'accès. Infinex a également mis en place un mécanisme de récupération qui permet aux utilisateurs de regagner l'accès à leur Smart Wallet en cas de perte de passkey, en utilisant des méthodes d'authentification sociale telles que les comptes Google ou Apple, tout en maintenant la sécurité des actifs.

SMART WALLETS, LE FUTUR POUR LES PARTICULIERS ?_

LES MEILLEURS SMART WALLETS_

SAFE

Safe, anciennement Gnosis Safe, est un smart wallet de référence qui offre une sécurité accrue grâce à la configuration d'un nombre minimum d'approbations pour chaque transaction (une caractéristique très appréciée par les structures qui gèrent des fonds, comme les DAO). Les utilisateurs définissent un quorum et une liste de comptes autorisés, garantissant ainsi la protection de leurs actifs numériques. Avec plus de 100 milliards de dollars sécurisés et 97 millions de transactions réalisées, Safe fonctionne sur un protocole open-source et est compatible avec plus de 15 réseaux, dont Ethereum et Arbitrum. Il propose des fonctionnalités avancées, telles que le regroupement de transactions, la récupération de comptes et les politiques de dépense, tout en s'intégrant à plus de 130 applications DeFi, comme Uniswap et AAVE. La gouvernance de Safe est assurée par SafeDAO, permettant aux détenteurs de jetons SAFE de participer aux décisions stratégiques. Le modèle décentralisé et le token SAFE permettent une implication active de la communauté dans l'évolution de la plateforme.

SMART WALLETS, LE FUTUR POUR LES PARTICULIERS ?_

LES MEILLEURS SMART WALLETS_

ARGENT

Lancé en 2018 et basé à Londres, Argent est reconnu comme le premier smart wallet non-custodial, conçu pour rendre la DeFi et les NFTs accessibles sur Ethereum et surtout Starknet. Soutenu par des investisseurs majeurs et avec plus de 2 millions d'utilisateurs, Argent offre une expérience fluide et intuitive, permettant d'acheter, staker et investir en crypto avec des frais réduits. Argent se distingue par son interface simple, son architecture basée sur l'abstraction de compte qui permet de regrouper les transactions, et ses fonctionnalités de sécurité avancées, comme Argent Shield, une protection par email pour prévenir les piratages.

Le wallet est open-source, offrant transparence et possibilité de personnalisation par la communauté. Disponible sur mobile et en extension de navigateur, Argent est compatible avec des applications DeFi comme Ekubo et Nostra Finance, tout en prenant en charge des fonctionnalités de récupération de compte et des politiques de dépense.

SMART WALLETS, LE FUTUR POUR LES PARTICULIERS ?_

LES MEILLEURS SMART WALLETS_

CLAVE

Lancé en 2024, Clave Wallet est un portefeuille non-custodial qui simplifie l'expérience Web3 et DeFi en intégrant sécurité et accessibilité. Grâce à l'abstraction de compte, les utilisateurs peuvent payer les frais de transaction avec n'importe quel token, facilitant les interactions on-chain. Il supporte uniquement le réseau ZkSync pour le moment, mais on peut recevoir depuis d'autres blockchains (Clave s'occupe de les bridger sur ZkSync).

Clave propose un système de gestion des clés avec récupération sociale et par passkey, garantissant sécurité et contrôle sur les actifs. Les utilisateurs bénéficient aussi de noms d'utilisateur gratuits via ENS, rendant les transactions plus intuitives. Disponible sur Android et iOS, l'application permet des dépôts simplifiés, des échanges de tokens sans frais de réseau, et des options de staking et de parrainage.

10

Entretien

NICOLAS BACCA

« LES PASSKEYS, LA BIOMÉTRIE, ET LES TECHNOLOGIES DE MPC CONTRIBUENT À SIMPLIFIER L'EXPÉRIENCE »

NICOLAS BACCA_

COFONDATEUR ET EX-CTO DE LEDGER, NICOLAS BACCA REVIENT SUR L'INTÉGRATION DE NOUVEAUX STANDARDS DANS LES WALLETS CRYPTO, ENTRE SIMPLIFICATION DE L'EXPÉRIENCE UTILISATEUR ET NOUVEAUX DÉFIS DE SÉCURITÉ.

DE PLUS EN PLUS DE WALLETS ADOPTENT AUJOURD'HUI L'IDENTIFICATION BIOMÉTRIQUE POUR SE CONNECTER OU VALIDER DES TRANSACTIONS. COMMENT CELA FONCTIONNE-T-IL ?

En réalité, l'identification biométrique ne signe pas directement les transactions. Elle sert de couche de sécurité supplémentaire pour accéder à la clé privée ou à un fragment de celle-ci. La biométrie ne remplace donc pas la signature cryptographique : elle agit comme un verrou protégeant l'accès à la clé, qui elle-même signe les transactions, comme dans une signature classique. Par exemple, avec Face ID ou l'empreinte digitale, ce n'est pas l'empreinte qui valide directement la transaction, mais elle autorise l'accès à la clé privée. L'accès à cette clé est restreint tant que la biométrie n'est pas validée. Une fois l'empreinte ou le visage reconnu, l'appareil déverrouille l'accès à la clé, utilisée ensuite pour signer la transaction.

LA PLUPART DU TEMPS, C'EST GRÂCE AUX "PASSKEYS" QU'ON PEUT VALIDER DES TRANSACTIONS AVEC FACE ID OU UNE EMPREINTE DIGITALE, N'EST-CE PAS ?

Oui, c'est exact. Grâce à ce standard, on peut valider une transaction avec une empreinte digitale ou Face ID dans un environnement Web2. Lorsqu'on utilise une passkey sur un site ou une application compatible, le mécanisme d'authentification biométrique se charge de déverrouiller la clé privée pour valider l'opération.

> **« Les passkeys, la biométrie, et les technologies de MPC contribuent à simplifier l'expérience »**

POUVEZ-VOUS EXPLIQUER COMMENT FONCTIONNENT LES PASSKEYS ?

Une passkey est un standard issu du Web2, destiné à remplacer les mots de passe traditionnels souvent sources de problèmes de sécurité. L'idée de base est simple : au lieu d'un mot de passe que l'utilisateur doit mémoriser, une passkey repose sur une paire de clés cryptographiques. Lorsqu'un utilisateur crée un compte avec une passkey, une clé publique et une clé privée sont générées. La clé publique est stockée sur le site ou le service, tandis que la clé privée reste sécurisée sur l'appareil de l'utilisateur, verrouillée par biométrie, PIN ou autre vérification. L'avantage est que pour chaque connexion, le service envoie un "défi" que l'utilisateur signe avec sa clé privée, prouvant son identité. Ce système est bien plus sécurisé que les mots de passe, car la clé privée n'est jamais partagée et reste protégée par un mécanisme cryptographique. Les passkeys résistent ainsi aux attaques de type phishing ou interception, car il n'y a pas de mot de passe à voler ou réutiliser. Dans les wallets crypto, on "détourne" un peu le standard passkey pour l'utiliser comme méthode d'authentification pour signer des transactions on-chain. Lorsqu'un utilisateur signe une transaction avec une passkey, le processus est similaire à celui de Metamask : une transaction est hashée, puis signée par la clé privée avant d'être envoyée au réseau. La passkey devient donc un pont entre le Web2 et la blockchain, permettant aux utilisateurs d'accéder aux services sans se soucier des mots de passe.

NICOLAS BACCA_

DANS LES SMART WALLETS, QUI STOCKE EXACTEMENT LES CLÉS PRIVÉES SI ELLES DEVIENNENT INVISIBLES POUR L'UTILISATEUR ?

Dans les smart wallets, la gestion des clés varie selon les technologies et les modèles de custody. Pour les passkeys, la clé est toujours stockée par l'utilisateur mais souvent synchronisée automatiquement entre ses appareils. Par exemple, si vous utilisez Face ID sur un iPhone, la clé est sur le téléphone mais aussi sauvegardée via iCloud pour faciliter la récupération et l'utilisation sur plusieurs appareils. Bien que la clé soit "invisible" pour l'utilisateur, elle reste stockée et contrôlée par lui. Dans d'autres modèles, comme ceux utilisant le Threshold Signature Scheme (TSS) ou la Multi-Party Computation (MPC), la clé est divisée en fragments. Un fragment est conservé par l'utilisateur, un autre par un tiers de confiance, et parfois un autre est sécurisé indépendamment. Pour signer une transaction, les fragments se combinent via des techniques cryptographiques avancées, mais chaque partie détient un fragment et peut, en théorie, influencer l'accès.

QUELS SONT LES SMART WALLETS QUI RÉPONDENT À VOS STANDARDS DE SÉCURITÉ LES PLUS ÉLEVÉS ?

Je pense aux wallets comme Argent et Bravos sur Starknet, conçus pour l'autonomie de l'utilisateur : ils utilisent des smart contracts pour la gestion des fonds et permettent une gestion de clés sécurisée directement sur la blockchain, sans tiers de confiance. Dans ce modèle, tout est transparent et traçable on-chain, ce qui permet à l'utilisateur de garder le contrôle total sur ses actifs. Sur Ethereum, un autre wallet similaire est Clave. Bien que Clave ne soit pas encore entièrement web, il offre une authentification par smart contract, où l'accès aux fonds est géré de manière décentralisée par un contrat intelligent, plutôt que par un serveur susceptible de bloquer l'accès. Cette solution permet une authentification purement basée sur la blockchain, offrant ainsi une sécurité et une transparence accrues. Un autre exemple important est le Coinbase Wallet dans sa version "smart wallet". Celui-ci est remarquable, car Coinbase a construit une infrastructure utilisant une validation on-chain, ce qui se rapproche le plus de la philosophie de la blockchain : l'utilisateur contrôle ses fonds sans dépendre de serveurs externes. C'est un bon modèle de wallet, respectant l'autonomie de l'utilisateur tout en offrant des fonctionnalités de sécurité modernes.

« En réalité, l'identification biométrique ne signe pas directement les transactions : elle agit comme un verrou qui protège l'accès à la clé, qui est ensuite utilisée pour signer la transaction. »

EST-CE QUE CE TYPE DE WALLET EST RÉSERVÉ UNIQUEMENT À ETHEREUM ?

Non, ces solutions ne sont pas réservées à Ethereum. La logique de smart contract peut être déployée sur toute blockchain programmable prenant en charge les contrats intelligents. Ethereum a une longueur d'avance en matière de standards et de technologies de wallets, mais des blockchains comme Starknet, Polygon, Binance Smart Chain, et d'autres peuvent également accueillir des smart wallets. Ethereum est souvent privilégiée pour ces développements en raison de ses standards robustes pour des aspects critiques comme le paiement des frais de transaction (le gaz), le bundling des transactions ou le sponsoring du gaz, qui facilitent l'expérience utilisateur. Mais le modèle est réplicable sur d'autres blockchains programmables.

NICOLAS BACCA_

LES MOTS DE PASSE ET LE STOCKAGE DES CLÉS PRIVÉES PAR LES UTILISATEURS SONT-ILS VOUÉS À DISPARAÎTRE ?

Non, je ne pense pas que les mots de passe et les clés privées vont complètement disparaître. Leur usage sera probablement de plus en plus limité à des opérations critiques, comme la récupération d'un compte ou la modification des règles de sécurité d'un wallet. Pour des transactions de faible valeur ou des opérations fréquentes, des solutions plus simples et automatisées comme la biométrie ou les passkeys vont progressivement se généraliser. Cependant, pour des transactions ou des changements importants, la conservation de la clé privée reste l'approche la plus sûre et la plus directe. C'est pourquoi les wallets conserveront sans doute toujours la possibilité d'utiliser une clé privée pour certains cas.

EST-CE QUE CETTE COMPLEXITÉ ACCRUE AUGMENTE LES RISQUES, NOTAMMENT DE PERDRE L'ACCÈS À SON WALLET ?

Absolument, la complexité introduit de nouveaux risques. Avec les smart wallets, l'authentification est programmable, permettant différentes méthodes de récupération ou de sécurisation. Par exemple, si un utilisateur opte pour une passkey sans solution de récupération, il est vulnérable. En cas de perte de sa passkey, il pourrait perdre l'accès à son wallet. Ce risque est surtout présent lorsque l'utilisateur dépend de solutions comme la synchronisation des passkeys via Google ou Apple. Si cette synchronisation est compromise, par exemple si un compte est désactivé, l'utilisateur pourrait perdre sa passkey et donc l'accès à son wallet. Il est donc crucial pour l'utilisateur de bien comprendre les options de récupération proposées par le wallet. Les smart wallets permettent cependant d'éviter certains risques.

Par exemple, on peut prévoir une récupération avec un autre wallet, comme Metamask, ou utiliser des solutions comme Argent qui permettent de transférer le contrôle du wallet en cas de problème. Mais ces options nécessitent de la vigilance de la part de l'utilisateur pour éviter d'être "verrouillé". Choisir un bon wallet, c'est aussi choisir un wallet offrant des méthodes de récupération et des options de sécurité claires et flexibles.

APPLE OU GOOGLE PEUVENT-ILS, D'UNE MANIÈRE OU D'UNE AUTRE, ACCÉDER À MA CLÉ PRIVÉE LORSQUE J'UTILISE DES WALLETS COMME COINBASE WALLET OU ARGENT, QUI ONT RECOURS À LA RECONNAISSANCE FACIALE ?

En théorie, non, Apple et Google n'ont pas directement accès à la clé privée elle-même, surtout si elle est stockée dans une enclave sécurisée, comme c'est le cas pour les passkeys. La clé est sauvegardée de manière chiffrée dans un HSM (Hardware Security Module) ou une enclave sécurisée, qui isole la clé privée du reste du système et des applications, donc même les services Apple ou Google ne peuvent pas extraire la clé brute. Cependant, il y a un point important : lorsqu'on active la synchronisation des passkeys, une couche de confiance est placée dans l'infrastructure de l'entreprise. Cela signifie que même si la clé elle-même reste inaccessible, il existe un protocole de synchronisation dépendant d'Apple ou de Google pour le transfert sécurisé entre les appareils. Si ces services sont compromis, par exemple si un pirate intercepte les données synchronisées ou si le compte de l'utilisateur est piraté, cela pourrait affecter l'accès aux passkeys.

NICOLAS BACCA_

EST-CE QUE CES NOUVEAUX SYSTÈMES SONT LA CLÉ POUR DÉMOCRATISER LES WALLETS CRYPTOS AUPRÈS DU GRAND PUBLIC ?

Oui, absolument. Pour que les wallets cryptos soient adoptés par un public plus large, il faut surmonter certains obstacles actuels, notamment ceux liés à la complexité de l'interface utilisateur et à la sécurité. Les passkeys, la biométrie et les technologies de MPC (Multi-Party Computation) simplifient l'expérience, ce qui est essentiel pour le grand public. Imaginons que l'on puisse combiner plusieurs technologies en open source, comme les passkeys, les authentifications par e-mail et le TSS (Threshold Signature Scheme) ou le MPC. Cela permettrait de construire des solutions modulaires et sécurisées, accessibles à tous, sans connaissances avancées en cryptographie. L'objectif est d'arriver à une expérience utilisateur similaire à celle des applications Web2, avec des logins simples et sécurisés, sans que les utilisateurs aient à gérer directement leurs clés privées.

COMMENT LEDGER PEUT-IL S'INTÉGRER DANS CETTE NOUVELLE DYNAMIQUE QUI MODIFIE LES HABITUDES ET POURRAIT POTENTIELLEMENT AFFECTER LE CŒUR DE SON BUSINESS ?

Ledger s'intègre déjà dans cette dynamique, et cela de plusieurs manières. Par exemple, nous avons mis en avant la fonctionnalité de passkey externe. En proposant un hardware wallet comme Ledger pour stocker une passkey, nous ajoutons une couche de sécurité pour les utilisateurs de passkeys, tout en leur offrant un contrôle accru sur leur clé privée. Cette fonctionnalité permet aux utilisateurs de s'authentifier avec une passkey, tout en assurant que leur clé est stockée indépendamment d'un cloud ou d'un serveur. De plus, Ledger a déjà commencé à se positionner comme un outil pour des opérations critiques sur les smart wallets.

Avec un hardware wallet comme Ledger, on peut envisager d'effectuer des opérations de sécurité avancées, comme changer les paramètres de custody d'un smart wallet ou modifier les politiques de récupération. Ces opérations nécessitent un niveau de sécurité élevé, car elles peuvent impacter directement la gestion des fonds, et le hardware wallet offre cette assurance de sécurité que peu d'autres solutions proposent. En d'autres termes, même si le hardware wallet peut être moins utilisé au quotidien, il devient un outil essentiel pour les opérations critiques. Ce changement renforce la position de Ledger, en faisant du hardware wallet non seulement un outil de stockage de clés, mais aussi un dispositif de contrôle de sécurité pour les transactions et les mises à jour de paramètres importants. C'est pourquoi nous continuons d'améliorer l'interface utilisateur et de simplifier les interactions avec le hardware wallet, pour que les utilisateurs puissent utiliser cette solution facilement pour des actions critiques sans compromis sur la sécurité.

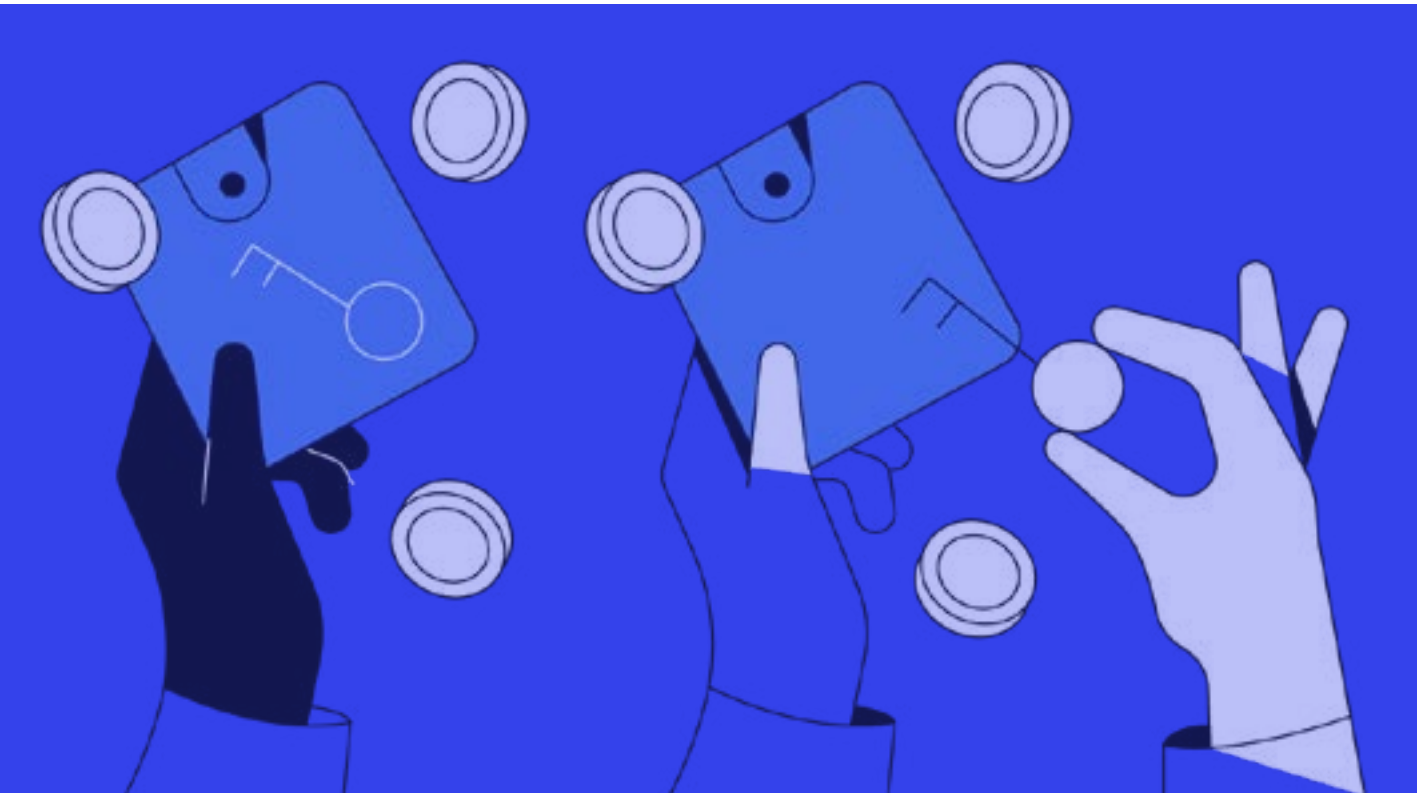
« Le wallet du futur sera à la fois polyvalent, modulaire et ultra-sécurisé, avec des options de recovery modulaires comme la récupération sociale ou par preuves Zero-Knowledge, optimisant l'accès sans compromettre la sécurité. »

NICOLAS BACCA_

À QUOI RESSEMBLERA LE WALLET DU FUTUR ? QUELS EN SERAIENT LES ÉLÉMENTS CLÉS ?

Le wallet du futur sera polyvalent, modulaire et ultra-sécurisé. Jesse Pollak de Base a d'ailleurs réalisé une excellente infographie décrivant ce concept, appelé le "Dream Wallet". L'idée est de combiner plusieurs caractéristiques pour offrir une flexibilité maximale tout en maintenant une sécurité robuste. Premièrement, un élément essentiel sera la capacité d'utiliser différents niveaux de sécurité pour les signatures, selon l'importance de la transaction. Par exemple, pour une petite dépense, une signature légère pourrait suffire, tandis qu'une transaction plus importante nécessiterait une authentification plus complexe. Cette flexibilité permettra à l'utilisateur de gérer ses fonds plus facilement, tout en assurant une sécurité renforcée pour les transactions critiques. Ensuite, le wallet du futur intégrera des options de recovery très modulaires.

Cela pourrait inclure la récupération sociale, où des contacts de confiance peuvent aider à récupérer l'accès en cas de perte, ou la récupération par preuves Zero-Knowledge (ZK), où un passeport ou autre pièce d'identité prouve l'identité de l'utilisateur sans révéler de données sensibles. Par exemple, des projets comme zkPassport permettent à un utilisateur de présenter son passeport pour récupérer son wallet, une avancée énorme en termes de praticité et de sécurité. En outre, le wallet du futur offrira aussi des fonctionnalités comme le sponsoring du gaz et des solutions pour optimiser les coûts de transaction. Cela allégera les contraintes pour les utilisateurs, rendant le paiement des frais de gaz plus fluide et limitant les obstacles pour interagir avec la blockchain. Cette vision de wallet modulaire et programmable permettrait une interface intuitive, avec une sécurité de niveau institutionnel, un élément souvent absent des solutions actuelles. L'industrie se dirige vers cette direction, intégrant de nouvelles technologies et standards pour démocratiser davantage les smart wallets.



REMERCIEMENTS

NICOLAS BACCA
Expert cybersécurité, cofondateur Ledger

CLAIRE BALVA
Deblock, VP Stratégie

CHRISTOPHER GRILHAULT DES FONTAINES
Dfns, cofondateur

CHARLES GUILLEMET
Ledger, CTO

CLARISSE HAGÈGE
Dfns, cofondatrice

ITAMAR LESUISSE
Argent, CEO

PIERRE D'ORMESSON
DLA Piper, Partner

JESSE POLLAK
Coinbase, Head of Base and Coinbase Wallet

CÔME PROST-BOUCLE
Coinbase, Country manager

JÉRÔME DE TYCHEY
Cometh, CEO

Ce rapport a été conçu par le service recherche de **The Big Whale** et sous la direction de **Grégory Raymond.**

www.thebigwhale.io

Nous contacter : contact@thebigwhale.io
9 rue des Colonnes, 75002 Paris, FRANCE