Livre Blanc de ChatWallet

Redéfinir l'Interaction Sociale et Financière dans le Web3

Version 1.2

Date : Juillet 2025

Résumé Exécutif (Abstract)

ChatWallet est une application décentralisée (dApp) de nouvelle génération conçue pour restaurer la souveraineté numérique en fusionnant un portefeuille de cryptomonnaies à auto-garde (self-custodial) avec un système de messagerie chiffré de bout en bout. Notre approche offre aux utilisateurs un contrôle absolu sur les trois piliers de leur vie numérique : leur identité, leurs actifs et leurs communications privées. Ceci est réalisé en intégrant des technologies fondamentales où chacune sert un objectif souverain : les Identifiants Décentralisés (DIDs) sécurisent la propriété de l'identité, les Adresses Furtives (Stealth Addresses) protègent la confidentialité financière, et un protocole chiffré garantit la liberté de communication. Ces composants créent un écosystème unifié où les interactions sociales et financières se renforcent mutuellement de manière native, privée et véritablement souveraine.

1. Introduction : La Fragmentation Actuelle Le paysage numérique d'aujourd'hui est brisé. La finance et la communication sociale opèrent dans des silos centralisés et déconnectés :

- **Portefeuilles Isolés :** Les portefeuilles de cryptomonnaies sont des outils transactionnels, dépourvus de contexte social ou communicatif. Un utilisateur doit copier-coller des adresses dans des applications de messagerie tierces (comme Telegram ou Discord) pour coordonner un paiement, s'exposant à des erreurs et des arnaques.
- **Messagerie Centralisée :** Les plateformes de chat populaires sont des jardins clos qui contrôlent les données des utilisateurs, monétisent leur attention et agissent comme des points uniques de défaillance et de censure.
- **Identité Fragmentée :** Les utilisateurs gèrent des dizaines d'identifiants, perdant le contrôle de leur propre identité numérique, qui appartient à des entreprises. ChatWallet est né pour résoudre ce triple problème, en offrant une expérience unifiée, souveraine et sécurisée.

2. La Solution : ChatWallet - Le Protocole Socio-Financier

ChatWallet n'est pas seulement un portefeuille avec une fonction de chat. C'est une plateforme intégrée où chaque conversation est une interaction économique potentielle, et chaque transaction peut avoir un contexte social. Notre vision est simple : *Si vous pouvez*

discuter avec quelqu'un, vous pouvez effectuer des transactions avec cette personne en toute sécurité et instantanément. Les fonctionnalités qui rendent cela possible sont :

- 💬 **Chat et Transactions Unifiés :** Envoyez et recevez des actifs directement dans la fenêtre de chat.
- 🛡️ **Confidentialité par Conception :** Communications chiffrées et historique des transactions privé.
- 👤 **Identité Souveraine :** Vous êtes le seul propriétaire de votre identité numérique.
- 🔗 **Interopérabilité Native :** Conçu dès le premier jour pour un avenir multichaîne.

3. Architecture et Composants Clés

ChatWallet est construit sur une pile de technologies Web3 de pointe, soigneusement sélectionnées pour garantir la décentralisation, la sécurité et la souveraineté de l'utilisateur.

3.1. Portefeuille à Auto-Garde (EVM & Multichaîne) La base de ChatWallet est un portefeuille de cryptomonnaies non-dépositaire. Le contrôle réside exclusivement chez l'utilisateur.

- **Norme BIP39 :** La génération du portefeuille est basée sur la norme BIP39, permettant aux utilisateurs de créer une phrase mnémonique de 12 ou 24 mots. Cette phrase est la seule clé pour accéder aux fonds et à l'identité et doit être conservée en lieu sûr par l'utilisateur.
- **Support EVM :** Au lancement, ChatWallet offre une compatibilité totale avec l'Ethereum Virtual Machine (EVM), prenant en charge l'ETH, les jetons ERC-20, les ERC-721 (NFTs) et l'interaction avec les dApps sur tous les réseaux L1 et L2 compatibles (ex. Polygon, Arbitrum, Optimism, Base).
- **Vision Multichaîne :** L'architecture est conçue pour être agnostique à la blockchain. L'intégration future de Solana et d'autres chaînes non-EVM est une priorité sur notre feuille de route.
- **Moteur :** Nous utilisons la bibliothèque robuste et éprouvée `ethers.js` pour toute la logique du portefeuille, garantissant la sécurité et la fiabilité des interactions avec la blockchain.

3.2. Identité Souveraine avec Ceramic Network et OrbisDB L'identité d'un utilisateur ne devrait pas dépendre d'un serveur central. Pour ce faire, nous intégrons un système d'Identifiants Décentralisés (DIDs).

- **DIDs (Identifiants Décentralisés) :** Chaque utilisateur de ChatWallet possède un DID qu'il contrôle avec ses clés cryptographiques. Ce DID est le point d'ancrage de son profil, de ses contacts et de sa réputation sociale.
- **Ceramic Network :** Nous utilisons Ceramic comme réseau décentralisé pour gérer les données composables liées aux DIDs. Cela permet aux données de profil (nom d'utilisateur, avatar, liens sociaux) d'être portables et vérifiables dans tout l'écosystème Web3.
- **OrbisDB :** Pour une gestion efficace et structurée des données sociales sur Ceramic, nous intégrons OrbisDB. Cela nous permet de gérer les relations sociales

(contacts, groupes), les paramètres et d'autres données de manière évolutive tout en maintenant la décentralisation. Les données sont stockées et sauvegardées sur IPFS.

3.3. Communication Sécurisée et Privée avec XMTP v3 La messagerie est au cœur de l'expérience sociale de ChatWallet. La confidentialité et la sécurité ne sont pas optionnelles.

- **Protocole Ouvert :** XMTP (Extensible Message Transport Protocol) est un réseau de messagerie décentralisé et open-source pour la communication de portefeuille à portefeuille.
- **Chiffrement de Bout en Bout :** Tous les messages sur ChatWallet sont chiffrés de bout en bout. Seuls l'expéditeur et le destinataire peuvent lire le contenu. Ni les nœuds XMTP, ni l'équipe de ChatWallet, ni personne d'autre ne peut accéder aux conversations.
- **Interopérabilité :** En utilisant XMTP, les utilisateurs de ChatWallet peuvent communiquer avec n'importe quel autre portefeuille utilisant ce protocole, créant un effet de réseau puissant et ouvert.

3.4. Confidentialité Financière Avancée : Le Protocole d'Adresses Furtives (Stealth Address) La transparence des registres publics est une arme à double tranchant ; si elle garantit l'auditabilité, elle compromet la vie privée des utilisateurs. Le pseudonymat standard (où les adresses ne sont pas directement liées à des noms réels) est insuffisant, car l'analyse du graphe des transactions peut facilement relier tout l'historique financier d'un utilisateur. Pour résoudre ce problème fondamental, ChatWallet met en œuvre un protocole robuste d'Adresses Furtives, inspiré de normes comme l'ERC-5564, et l'améliore avec une couche de communication interactive. Notre protocole fonctionne en deux modes : statique et interactif.

- **Le Modèle Statique (Paiements Asynchrones) :** Pour les cas d'utilisation non interactifs comme les adresses de dons publiques, un utilisateur peut publier une méta-adresse furtive sur son profil DID sur le Ceramic Network. Un expéditeur peut récupérer cette méta-adresse publique et l'utiliser pour dériver cryptographiquement une adresse de destination unique et à usage unique pour sa transaction. L'expéditeur publie également une clé publique éphémère comme "indice" on-chain, ce qui permet au portefeuille du destinataire de scanner la blockchain, de découvrir la transaction et de dériver la clé privée correspondante pour contrôler les fonds.
- **L'Innovation de ChatWallet : Le Modèle Interactif (Paiements Synchrones) :** C'est là que la conception intégrée de ChatWallet crée un modèle de confidentialité supérieur. Au lieu de s'appuyer sur une méta-adresse publiée publiquement, les utilisateurs peuvent échanger des informations de paiement de manière sécurisée et dynamique au sein d'un chat chiffré par XMTP. Le déroulement est le suivant :
    - **Canal Sécurisé :** L'expéditeur (Alice) et le destinataire (Bob) établissent une session chiffrée de bout en bout via le protocole XMTP.
    - **Requête Signée :** Le portefeuille d'Alice demande les détails de paiement à Bob dans le chat.
    - **Réponse Signée :** Le portefeuille de Bob génère ou récupère sa méta-adresse furtive et la fournit à Alice. Fait crucial, cette donnée est signée

cryptographiquement par la clé principale du portefeuille de Bob avant d'être envoyée.
    - **Vérification et Dérivation :** Le portefeuille d'Alice reçoit la méta-adresse signée et vérifie la signature. Cela garantit qu'elle interagit avec le propriétaire authentique du DID, empêchant toute attaque de l'homme du milieu (man-in-the-middle). Après une vérification réussie, son portefeuille procède à la génération standard de l'adresse furtive.
    - **Transaction Privée :** Alice envoie les fonds directement à la nouvelle adresse à usage unique.
- **Avantages du Modèle Interactif :**
    - **Aucune Empreinte Publique :** La méta-adresse de l'utilisateur n'est jamais exposée publiquement, empêchant les collecteurs de données et les sociétés d'analyse de chaîne de la lier à son DID.
    - **Sécurité Renforcée :** La signature cryptographique fournit une preuve d'authenticité plus forte que la récupération d'une adresse à partir d'une source modifiable comme une biographie sur les réseaux sociaux ou même un registre public.
    - **Confidentialité Contextuelle :** Les clés sont échangées dans un but spécifique et immédiat, en respectant le principe du moindre privilège.

En prenant en charge les deux modèles, ChatWallet offre une confidentialité financière complète pour pratiquement tous les cas d'utilisation, des dons anonymes au commerce conversationnel privé.

3.5. Vers l'Abstraction de Compte : SCAs Modulables L'avenir de l'utilisabilité du Web3 réside dans l'Abstraction de Compte (ERC-4337).

- **Comptes de Contrat Intelligent (SCAs) :** ChatWallet est conçu pour être compatible avec les SCAs. Cela permettra aux futures versions de mettre en œuvre des fonctionnalités avancées telles que :
    - **Transactions sans Gaz :** Sponsoriser les frais de gaz pour les nouveaux utilisateurs.
    - **Récupération Sociale :** Récupérer l'accès au compte via des contacts de confiance.
    - **Logique Personnalisée :** Autoriser des dépenses quotidiennes automatiques, fixer des limites, et plus encore.

3.6. Le Tissu Social : Attestations Souveraines Au-delà de l'identité et de la communication, ChatWallet est conçu pour construire un tissu social basé sur la confiance et l'honneur vérifiables. Ceci est réalisé grâce à un système natif d'Attestations Souveraines. Une attestation est une déclaration cryptographique qu'une identité (DID) fait à propos d'une autre. Ces déclarations peuvent être publiques ou privées, on-chain ou off-chain, mais elles sont toujours signées et vérifiables. Elles sont le fondement pour construire une réputation décentralisée et portable.

- **Normes Ouvertes :** Notre implémentation sera compatible avec des normes ouvertes comme l'Ethereum Attestation Service (EAS), garantissant une

interopérabilité maximale. Toute attestation créée dans ChatWallet pourra être reconnue dans tout l'écosystème Web3, et vice-versa.

- **Toile de Confiance (Web of Trust) :** Les attestations permettent aux utilisateurs de construire une toile de confiance. Avant d'effectuer une transaction importante, un utilisateur peut vérifier les attestations reçues par sa contrepartie directement dans le chat. Par exemple :
    - Une attestation "Travail Terminé" d'un client précédent.
    - Une attestation "Membre Vérifié" d'une DAO.
    - Une attestation "Ami de Confiance" d'un contact mutuel.
- **Construire l'Honneur :** Ce système transforme la réputation d'une métrique abstraite en un ensemble de preuves concrètes et vérifiables. Il encourage les interactions honorables, car les actions positives peuvent être enregistrées et les négatives (ou l'absence de positives) sont apparentes. C'est l'infrastructure d'une société numérique où la parole et les actes retrouvent leur valeur.

4. Philosophie et Fonctionnalités Supplémentaires

- **Permettre des Économies Libres (Monnaie Libre) :** ChatWallet est un outil d'échange P2P résistant à la censure. Son architecture décentralisée promeut la souveraineté économique et permet la création d'économies circulaires et de communautés basées sur la confiance et l'échange de valeur direct.
- **Soutenu par IPFS :** Les métadonnées de profil, les attestations et autres données importantes sont stockées sur l'InterPlanetary File System (IPFS), garantissant leur persistance et leur résistance à la censure.

5. Cas d'Utilisation

- **Freelances & Clients :** Un designer discute des détails d'un projet avec un client dans un chat chiffré et reçoit le paiement en USDC dans la même interface après avoir atteint une étape clé.
- **Communautés & DAOs :** Les membres d'une DAO discutent d'une proposition et, une fois le consensus atteint, le trésorier exécute le paiement depuis la même application, gardant tout le contexte au même endroit.
- **Amis & Dépenses :** Un groupe d'amis crée un chat de groupe pour planifier un voyage. Ils peuvent partager l'addition d'un dîner et régler leurs dettes instantanément dans le chat.
- **Artistes & Créateurs :** Un musicien peut discuter avec sa communauté de fans et leur vendre directement un nouveau NFT musical, sans intermédiaires.

6. Feuille de Route (Roadmap)

- **Phase 1 (Actuelle) :** Lancement sur les réseaux EVM. Fonctionnalités de base : Portefeuille, Chat (XMTP), DIDs (Ceramic), Adresses Furtives.
- **Phase 2 :** Intégration de Solana. Expansion de la fonctionnalité multichaîne. Implémentation des attestations.
- **Phase 3 :** Intégration des SCAs (Abstraction de Compte). Lancement de la récupération sociale et des transactions sans gaz.
- **Phase 4 :** API et SDK pour développeurs afin de permettre à d'autres dApps d'intégrer la couche socio-financière de ChatWallet.

7. Conclusion ChatWallet est plus qu'un outil ; c'est un changement de paradigme. En tissant la communication et la finance en une seule trame décentralisée, nous construisons l'infrastructure pour une nouvelle génération d'interactions numériques : plus humaines, plus sécurisées et fondamentalement plus libres. Nous invitons les développeurs, les investisseurs et les utilisateurs pionniers à nous rejoindre pour construire l'avenir du web social et financier.

Avis de non-responsabilité : Ce document est fourni à titre informatif uniquement. Il ne constitue ni une offre de vente de titres ni une sollicitation d'investissement. Les informations présentées ici sont susceptibles de changer à mesure que le projet évolue. La participation à des projets de cryptomonnaies comporte des risques importants.