Whitepaper de ChatWallet

Redefiniendo la Interacción Social y Financiera en la Web3

Version 1.2

Fecha: Julio 2025

Resumen Ejecutivo (Abstract)

ChatWallet es una aplicación descentralizada (dApp) de nueva generación diseñada para restaurar la soberanía digital al fusionar una billetera de criptomonedas de autocustodia con un sistema de mensajería cifrado de extremo a extremo. Nuestro enfoque proporciona a los usuarios un control absoluto sobre los tres pilares de su vida digital: su identidad, sus activos y sus comunicaciones privadas. Esto se logra integrando tecnologías fundamentales donde cada una cumple un propósito soberano: los Identificadores Descentralizados (DIDs) aseguran la propiedad de la identidad, las Direcciones Sigilosas (Stealth Addresses) protegen la privacidad financiera y un protocolo cifrado garantiza la libertad de comunicación. Estos componentes crean un ecosistema unificado donde las interacciones sociales y financieras se potencian mutuamente de forma nativa, privada y verdaderamente soberana.

1. Introducción: La Fragmentación Actual

El panorama digital actual está roto. Las finanzas y la comunicación social operan en silos centralizados y desconectados:

- **Billeteras Aisladas:** Las billeteras de criptomonedas son herramientas transaccionales que carecen de contexto social o comunicativo. Un usuario debe copiar y pegar direcciones en aplicaciones de mensajería de terceros (como Telegram o Discord) para coordinar un pago, exponiéndose a errores y estafas.
- **Mensajería Centralizada:** Las plataformas de chat populares son jardines vallados que controlan los datos del usuario, monetizan su atención y actúan como puntos únicos de fallo y censura.
- **Identidad Fragmentada:** Los usuarios gestionan docenas de inicios de sesión, perdiendo el control sobre su propia identidad digital, que es propiedad de las corporaciones. ChatWallet nació para resolver este triple problema, ofreciendo una experiencia unificada, soberana y segura.

2. La Solución: ChatWallet - El Protocolo Socio-Financiero

ChatWallet no es solo una billetera con una función de chat. Es una plataforma integrada donde cada conversación es una potencial interacción económica, y cada transacción puede tener un contexto social. Nuestra visión es simple: *Si puedes chatear con alguien, puedes realizar transacciones con esa persona de forma segura e instantánea.* Las características que hacen esto posible son:

- 💬 **Chat y Transacciones Unificadas:** Envía y recibe activos directamente dentro de la ventana de chat.
- 🛡️ **Privacidad por Diseño:** Comunicaciones cifradas y un historial de transacciones privado.
- 👤 **Identidad Soberana:** Eres el único propietario de tu identidad digital.
- 🔗 **Interoperabilidad Nativa:** Diseñado desde el primer día para un futuro multicadena.

3. Arquitectura y Componentes Clave

ChatWallet está construido sobre una pila de tecnologías Web3 de vanguardia, cuidadosamente seleccionadas para garantizar la descentralización, la seguridad y la soberanía del usuario.

3.1. Billetera de Autocustodia (EVM y Multicadena) La base de ChatWallet es una billetera de criptomonedas sin custodia. El control reside exclusivamente en el usuario.

- **Estándar BIP39:** La generación de la billetera se basa en el estándar BIP39, permitiendo a los usuarios crear una frase semilla de 12 o 24 palabras. Esta frase es la única clave para acceder a los fondos y la identidad, y debe ser salvaguardada por el usuario.
- **Soporte EVM:** En su lanzamiento, ChatWallet ofrece compatibilidad total con la Ethereum Virtual Machine (EVM), soportando ETH, tokens ERC-20, ERC-721 (NFTs) e interacción con dApps en todas las redes L1 y L2 compatibles (ej. Polygon, Arbitrum, Optimism, Base).
- **Visión Multicadena:** La arquitectura está diseñada para ser agnóstica a la blockchain. La futura integración de Solana y otras cadenas no-EVM es una prioridad en nuestro roadmap.
- **Motor:** Utilizamos la robusta y probada librería `ethers.js` para toda la lógica de la billetera, garantizando seguridad y fiabilidad en las interacciones con la blockchain.

3.2. Identidad Soberana con Ceramic Network y OrbisDB La identidad de un usuario no debe depender de un servidor central. Para lograrlo, integramos un sistema de Identificadores Descentralizados (DIDs).

- **DIDs (Identificadores Descentralizados):** Cada usuario de ChatWallet posee un DID que controla con sus claves criptográficas. Este DID es el ancla para su perfil, contactos y reputación social.
- **Ceramic Network:** Usamos Ceramic como la red descentralizada para gestionar datos componibles vinculados a los DIDs. Esto permite que los datos del perfil (nombre de usuario, avatar, enlaces sociales) sean portátiles y verificables en todo el ecosistema Web3.
- **OrbisDB:** Para una gestión de datos sociales eficiente y estructurada sobre Ceramic, integramos OrbisDB. Esto nos permite manejar relaciones sociales (contactos, grupos), configuraciones y otros datos de manera escalable, manteniendo la descentralización. Los datos se almacenan y respaldan en IPFS.

3.3. Comunicación Segura y Privada con XMTP v3 La mensajería es el corazón de la experiencia social de ChatWallet. La privacidad y la seguridad no son opcionales.

- **Protocolo Abierto:** XMTP (Extensible Message Transport Protocol) es una red de mensajería descentralizada y de código abierto para la comunicación de billetera a billetera.
- **Cifrado de Extremo a Extremo:** Todos los mensajes en ChatWallet están cifrados de extremo a extremo. Solo el emisor y el receptor pueden leer el contenido. Ni los nodos de XMTP, ni el equipo de ChatWallet, ni nadie más puede acceder a las conversaciones.
- **Interoperabilidad:** Al usar XMTP, los usuarios de ChatWallet pueden comunicarse con cualquier otra billetera que utilice este protocolo, creando un efecto de red potente y abierto.

3.4. Privacidad Financiera Avanzada: El Protocolo de Direcciones Sigilosas (Stealth Address) La transparencia de los registros públicos es un arma de doble filo; si bien garantiza la auditabilidad, compromete la privacidad del usuario. El seudonimato estándar (donde las direcciones no están directamente ligadas a nombres reales) es insuficiente, ya que el análisis del grafo de transacciones puede vincular fácilmente todo el historial financiero de un usuario. Para resolver este problema fundamental, ChatWallet implementa un robusto protocolo de Direcciones Sigilosas, inspirado en estándares como el ERC-5564, y lo mejora con una capa de comunicación interactiva. Nuestro protocolo opera en dos modos: estático e interactivo.

- **El Modelo Estático (Pagos Asíncronos):** Para casos de uso no interactivos como direcciones de donación públicas, un usuario puede publicar una meta-dirección sigilosa en su perfil DID en la Ceramic Network. Un remitente puede obtener esta meta-dirección pública y usarla para derivar criptográficamente una dirección de destino única y de un solo uso para su transacción. El remitente también publica una clave pública efímera como una "pista" on-chain, que permite a la billetera del destinatario escanear la blockchain, descubrir la transacción y derivar la clave privada correspondiente para controlar los fondos.
- **La Innovación de ChatWallet: El Modelo Interactivo (Pagos Síncronos):** Aquí es donde el diseño integrado de ChatWallet crea un modelo de privacidad superior. En lugar de depender de una meta-dirección publicada, los usuarios pueden intercambiar información de pago de forma segura y dinámica dentro de un chat cifrado con XMTP. El flujo es el siguiente:
    - **Canal Seguro:** El remitente (Alice) y el receptor (Bob) establecen una sesión cifrada de extremo a extremo a través del protocolo XMTP.
    - **Solicitud Firmada:** La billetera de Alice solicita los detalles de pago a Bob dentro del chat.
    - **Respuesta Firmada:** La billetera de Bob genera o recupera su meta-dirección sigilosa y se la proporciona a Alice. Crucialmente, estos datos son firmados criptográficamente por la clave principal de la billetera de Bob antes de ser enviados.
    - **Verificación y Derivación:** La billetera de Alice recibe la meta-dirección firmada y verifica la firma. Esto garantiza que está interactuando con el propietario auténtico del DID, previniendo ataques de intermediario (man-in-the-middle). Tras una verificación exitosa, su billetera procede con la generación estándar de la dirección sigilosa.

    - **Transacción Privada:** Alice envía los fondos directamente a la dirección de un solo uso recién generada.
- **Ventajas del Modelo Interactivo:**
    - **Cero Huella Pública:** La meta-dirección del usuario nunca se expone públicamente, evitando que los recolectores de datos y las empresas de análisis de cadena la vinculen a su DID.
    - **Seguridad Mejorada:** La firma criptográfica proporciona una prueba de autenticidad más fuerte que obtener una dirección de una fuente mutable como una biografía en redes sociales o incluso un registro público.
    - **Privacidad Contextual:** Las claves se intercambian para un propósito específico e inmediato, adhiriéndose al principio de mínimo privilegio.

Al soportar ambos modelos, ChatWallet proporciona una privacidad financiera integral para prácticamente cualquier caso de uso, desde donaciones anónimas hasta comercio conversacional privado.

3.5. Hacia la Abstracción de Cuentas: SCAs Conectables El futuro de la usabilidad en Web3 reside en la Abstracción de Cuentas (ERC-4337).

- **Cuentas de Contrato Inteligente (SCAs):** ChatWallet está diseñado para ser compatible con SCAs. Esto permitirá que futuras versiones implementen características avanzadas como:
    - **Transacciones sin Gas:** Patrocinar las comisiones de gas para nuevos usuarios.
    - **Recuperación Social:** Recuperar el acceso a la cuenta a través de contactos de confianza.
    - **Lógica Personalizada:** Autorizar gastos diarios automáticos, establecer límites y más.

3.6. El Tejido Social: Atestaciones Soberanas Más allá de la identidad y la comunicación, ChatWallet está diseñado para construir un tejido social basado en la confianza y el honor verificables. Esto se logra a través de un sistema nativo de Atestaciones Soberanas. Una atestación es una declaración criptográfica que una identidad (DID) hace sobre otra. Estas declaraciones pueden ser públicas o privadas, on-chain u off-chain, pero siempre están firmadas y son verificables. Son la base para construir una reputación descentralizada y portátil.

- **Estándares Abiertos:** Nuestra implementación será compatible con estándares abiertos como el Ethereum Attestation Service (EAS), asegurando la máxima interoperabilidad. Cualquier atestación creada en ChatWallet puede ser reconocida en todo el ecosistema Web3, y viceversa.
- **Red de Confianza (Web of Trust):** Las atestaciones permiten a los usuarios construir una red de confianza. Antes de realizar una transacción importante, un usuario puede verificar las atestaciones recibidas por su contraparte directamente en el chat. Por ejemplo:
    - Una atestación de "Trabajo Completado" de un cliente anterior.
    - Una atestación de "Miembro Verificado" de una DAO.
    - Una atestación de "Amigo de Confianza" de un contacto mutuo.

- **Construyendo el Honor:** Este sistema transforma la reputación de una métrica abstracta a un conjunto de pruebas concretas y verificables. Fomenta interacciones honorables, ya que las acciones positivas pueden registrarse y las negativas (o la ausencia de positivas) son evidentes. Es la infraestructura para una sociedad digital donde la palabra y los hechos de uno recuperan su valor.

4. Filosofía y Características Adicionales

- **Habilitando Economías Libres (Monnaie Libre):** ChatWallet es una herramienta para el intercambio P2P resistente a la censura. Su arquitectura descentralizada promueve la soberanía económica y permite la creación de economías circulares y comunidades basadas en la confianza y el intercambio directo de valor.
- **Respaldado por IPFS:** Los metadatos del perfil, las atestaciones y otros datos importantes se almacenan en el InterPlanetary File System (IPFS), asegurando su persistencia y resistencia a la censura.

5. Casos de Uso

- **Freelancers y Clientes:** Un diseñador discute los detalles del proyecto con un cliente en un chat cifrado y recibe el pago en USDC en la misma interfaz al alcanzar un hito.
- **Comunidades y DAOs:** Los miembros de una DAO discuten una propuesta y, una vez alcanzado el consenso, el tesorero ejecuta el pago desde la misma aplicación, manteniendo todo el contexto en un solo lugar.
- **Amigos y Gastos:** Un grupo de amigos crea un chat grupal para planificar un viaje. Pueden dividir la cuenta de una cena y saldar deudas al instante dentro del chat.
- **Artistas y Creadores:** Un músico puede chatear con su comunidad de fans y venderles un nuevo NFT musical directamente, sin intermediarios.

6. Hoja de Ruta (Roadmap)

- **Fase 1 (Actual):** Lanzamiento en redes EVM. Funciones principales: Billetera, Chat (XMTP), DIDs (Ceramic), Direcciones Sigilosas.
- **Fase 2:** Integración de Solana. Expansión de la funcionalidad multicadena. Implementación de atestaciones.
- **Fase 3:** Integración de SCA (Abstracción de Cuentas). Lanzamiento de la recuperación social y transacciones sin gas.
- **Fase 4:** API y SDK para desarrolladores para permitir que otras dApps integren la capa socio-financiera de ChatWallet.

7. Conclusión ChatWallet es más que una herramienta; es un cambio de paradigma. Al entrelazar la comunicación y las finanzas en un único tejido descentralizado, estamos construyendo la infraestructura para una nueva generación de interacciones digitales: más humanas, más seguras y fundamentalmente más libres. Invitamos a desarrolladores, inversores y usuarios pioneros a unirse a nosotros en la construcción del futuro de la web social y financiera.

Descargo de Responsabilidad: Este documento es solo para fines informativos. No constituye una oferta de venta de valores ni una solicitud de inversión. La información aquí

presentada está sujeta a cambios a medida que evoluciona el proyecto. La participación en proyectos de criptomonedas implica un riesgo significativo.