

Privacy & Confidentiality in Plasma Payments

English Explanation

This document explains how the Lava Payment project addresses privacy and confidentiality for stablecoin payments on the Plasma blockchain.

Plasma is a public blockchain, meaning transactions are transparent by design. Our goal is not to hide on-chain data, but to reduce unnecessary data exposure and limit the ability to link multiple payments together.

Privacy measures implemented:

- No user accounts, emails, or personal data are collected.
- No centralized backend is required to process payments.
- Payments are peer-to-peer wallet-to-wallet using USDT on Plasma.
- Payment history and metadata are stored locally in the browser only.

The application strongly encourages the use of a fresh receiving address for each invoice. Users are guided to create or switch to a new MetaMask account before generating a payment request. This significantly reduces on-chain linkability between payments.

Payment notes (memos) are never written on-chain. If used, they are stored locally and visible only to the receiver.

Explication en français

Ce document explique comment le projet Lava Payment traite les aspects de confidentialité et de protection de la vie privée pour les paiements en stablecoin sur la blockchain Plasma.

Plasma étant une blockchain publique, les transactions sont par nature transparentes. L'objectif du projet n'est pas de masquer les données on-chain, mais de réduire l'exposition inutile des informations et de limiter la corrélation entre paiements.

Mesures de confidentialité mises en place :

- Aucun compte utilisateur, email ou donnée personnelle n'est collecté.
- Aucun backend centralisé n'est nécessaire pour traiter les paiements.
- Les paiements sont effectués directement de wallet à wallet en USDT sur Plasma.
- L'historique et les métadonnées sont stockés uniquement en local dans le navigateur.

L'application recommande fortement l'utilisation d'une adresse de réception unique pour chaque facture. L'utilisateur est guidé afin de créer ou de basculer vers un nouveau compte MetaMask avant de générer la demande de paiement, réduisant ainsi la corrélation on-chain.

Les notes de paiement ne sont jamais écrites sur la blockchain. Elles restent locales et visibles uniquement par le receveur.