TS 2021.010-30

Paymail

fact sheet

Publication date: 12 July 2022

Authors: Andy Mee and Miguel Duarte

Area of interest

Wallets, Client Services, On-chain data

Categories & related standards

Wallets, Client Services, On-chain Data, Payments, Identity, Interoperability, Accessibility

Executive summary

Paymail provides an interoperability mechanism for users of Bitcoin applications to transact and interact with each other securely using a stable, human-readable aliases. The Paymail core offers a foundation for vendors to build cross-implementation applications and safely deliver new use cases whilst benefiting from the security and ease of use of Paymail itself.

Abstract

Paymail is a collection of protocols for Bitcoin SV wallets and applications that let users identify each other in a human-readable and secure way. Paymail aliases, similar to email addresses, allow for cross-application message and payment flows whilst hiding the complexity of legacy Bitcoin addresses and preventing common forms of malicious behaviour. Diverse implementations may exchange messages and funds via a standard protocol, whilst an ecosystem of extensions provide rich functionality for many different application flows.

Extensions offer cross-wallet flows for peer-to-peer payments, MultiSig fund security, mutual party authentication, confidential communication, user profile cards and more. Users of varying implementations may form collaborate and transact regardless of the software application selected by each party.

Benefits

- Ease of use – Paymail addresses work just like email addresses to provide a stable identity to an individual or business, whilst simultaneously providing mechanisms for privacy-preserving on-chain best practices such as using unique Bitcoin addresses for every transaction.
- Interoperability - complex flows previously restricted to a single software implementation, such as managing a MultiSig group, are enabled even when each party is using a different wallet implementation.
- Identity – Paymail facilitates adding identity to a BitcoinSV application or service.
- Security – Paymail's mutual party authentication and secure confidential message exchange provide a secure and private party-to-party application messaging framework, with checks to detect and defeat interception and impersonation.

Monitoring and review

The TSC keeps track of the standard implementation or to notify the TSC that this standard is due for review or has become obsolete, fill the appropriate form published in the Paymail Standard Webpage.