Bitcoin SV TECHNICAL STANDARDS

Roadmap 2021-2023

Wallets	Client services	On-chain data	Regulation and compliance	Mining

Area description

- Standardise wallets and other Bitcoin client tools to improve the usability, security and adoption of Bitcoin wallets.
- Standardise server side services and APIs for Bitcoin clients to consume.
- Implement and standardise tokenised digital assets on Bitcoin.
- Standards that drive compliance with regulatory requirements to help further the regulation of Bitcoin.
- Standards that assist miners commercialising services they can offer on Bitcoin.

Stream

- SPV client tools
- SPV client services
- Data and token interoperability
- FATF compliance
- Mining interoperability

Stream goals

- Standardise direct payment exchange between wallets.
- Standardise making payment requests between merchants and wallets.
- Standardise the process of payment verification by wallets and its successful confirmation.
- Encrypted data standard for payment metadata.
- Standardise a login protocol (Paymail Oauth will require a client service).
- Standardise offline and/or direct peer-to-peer communications between wallets.
- Standardise protections to prevent fraudulent transactions.
- Standardise fee/policy specification for transaction construction.
- Standardise callback interfaces for transaction event notifications (double spends, SPV proofs).
- Standardise service discovery for user-associated services.
- Standardise token protocol for token representation and exchange.
- Standardise token protocol extensions for future use-cases.
- Standardise wrapping of non-standard tokens to allow interoperability between token services.
- Standardisation of Metanet data structure.
- Adherence to Financial Action Task Force (FATF) Recommendation 16 for virtual assets and virtual asset service providers.
- Standardise the exchange of data between virtual asset service providers.
- Standardise the message flows between virtual asset service providers and/or identity services.
- Standardise API's for interacting with miners.
- Standardise the exchange of data between miners.

Standards in progress

- Transaction ancestors
- Direct payment protocol
- Wallet API specification
- Paymail
- Deferred fee allocation
- Envelope specification
- Travel rule

Prior art or proposals for consideration

- Accumulator multiSig
- Peer discovery and transport
- SPV channels
- mAPI
- Orphan notification
- Paymail ID extensions e.g. cell/ phone number
- Paymail transaction flow extensions
- Paymail group extensions
- Paymail threshold signatures extensions
- Paymail payment channels extensions
- Double-spend and SPV proof notifications
- Mining fee specs/ rate cards
- Nano-payment negotiation
- Protocol identifiers
- Data framing
- UTXO based token
- On-chain identity (KYC)
- Region codes
- Miner ID
- Authenticated channels