TS 2020.010-31

# Merkle proof standardised format

fact sheet


**Publication date:** 09-06-2021

**Authors:** Steve Shadders, nChain

**Licensing:** nChain Patent pledge



## Area of interest

Wallets, SPV client tools

## Categories & related standards

Categories:

- SPV client tools
- SPV client services

Related standards:

- TS 2021.012 Transaction Ancestors
- TS 2021.014 Invoice Based Payments

## Executive summary

This standard documents a JSON and binary data structure to share SPV merkle proofs between applications. This is a critically important data structure in bitcoin interactions that enables sharing of proof-of-inclusion of a transaction in the Bitcoin blockchain.

## Abstract

This document serves to provide a Merkle proof standard which will assist in application and wallet interoperability as services on the network transition toward the Simplified Payment Verification paradigm as described in Section 8 of the Bitcoin Whitepaper. The document provides standardisation around the JSON and binary data structures to be used to relay index and interior node values of the Merkle path for the relevant transactions as well as the algorithmic instruction for the execution of both simple and composite proofs. The standard also provides the particular flag values to indicate which data elements are included in the Merkle proof envelope and which element will be chosen as default in the instance of a null value for the flag.

## Benefits

- Easier interoperability between wallets for wallet-wallet interactions (e.g. negotiation payments)
- Provides a standard and well-known format for miners to provide merkle proofs to users through mAPI and other user to miner services.
- Will assist in the formation of graph structures from overlay networks and integrating their off-chain transaction trees with the main ledger.
- Will assist in the building and integration of individualised 'working blockchains' with the main ledger.
- Will assist in the efficient verification of novel graph structures which are themselves constituents of a new value-based internet.

## Monitoring and review

The TSC keeps track of the standard implementation. To record yours, visit the standard page in the TSC library. To notify the TSC that this standard is due for review or has become obsolete, email tsc@bitcoinassociation.net quoting the standard UID with a short supporting statement.