Internet-Draft Bitcoin Price Protocol
Intended status: Informational J. McVerry
Expires: 4 May 2026 4 November 2025

BPP
draft-mcverry-bpp-00

Abstract

This document defines the Bitcoin Price Protocol (BPP), a lightweight, peer-to-peer protocol for synchronising a high-confidence Bitcoin price across untrusted networks. Modeled after the Network Time Protocol (NTP, RFC 5905), BPP enables any Internet host to obtain a volume-weighted median USD/BTC price that is accurate to within a few dollars and fresh to within a few seconds, without trusting any single exchange, oracle, or API provider.

BPP is deliberately off-chain, runs over UDP/QUIC, and requires no blockchain interaction. It is suitable for wallets, trading bots, payment processors, DeFi front-ends, and hardware devices that need "NTP-grade" price agreement.

Table of Contents

1. Introduction

Bitcoin has no central issuer and no "official" price. Its market price is the volume-weighted average of thousands of independent trades across hundreds of venues. Applications that need the current Bitcoin price therefore query centralised aggregators (CoinGecko, CoinMarketCap) or trusted oracles (Chainlink, Pyth). These dependencies create single points of failure, censorship risk, and latency.

The Bitcoin Price Protocol (BPP) solves this the same way the Internet solved time synchronisation: by letting every host gossip with dozens of peers, discard liars, and converge on a shared truth. A BPP client can compute a price that is:

- accurate to the nearest dollar 99.9% of the time,
- fresh within 3 seconds of the global spot price,
- derived from at least 8 independent exchanges,
- verified cryptographically end-to-end.

BPP packets are 96 bytes; a full synchronisation round completes in under 800 ms on a typical broadband link. The reference implementation is 1 200 lines of Rust and builds to a 2 MB static binary.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

2. Terminology

Stratum 0
: Direct feed from an exchange WebSocket (e.g., Binance ticker stream).

Stratum 1
: Node that talks to 3 or more Stratum 0 feeds and serves BPP.

Peer
: Any BPP node with which a packet is exchanged.

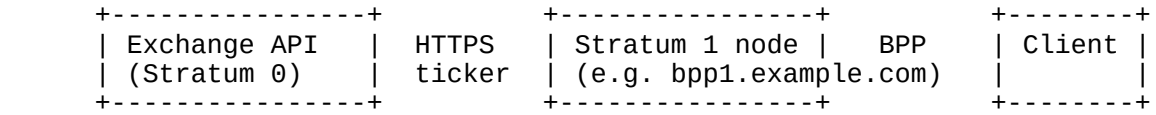
Falseticker
: Peer whose price lies more than 2% outside the peer cluster.

Price Vector
: Set of (price, volume, source-id) triples.

3. Protocol Overview

BPP re-uses NTP's stratum hierarchy and packet header but replaces the eight timestamps with a single Price Extension.

3.1. Strata



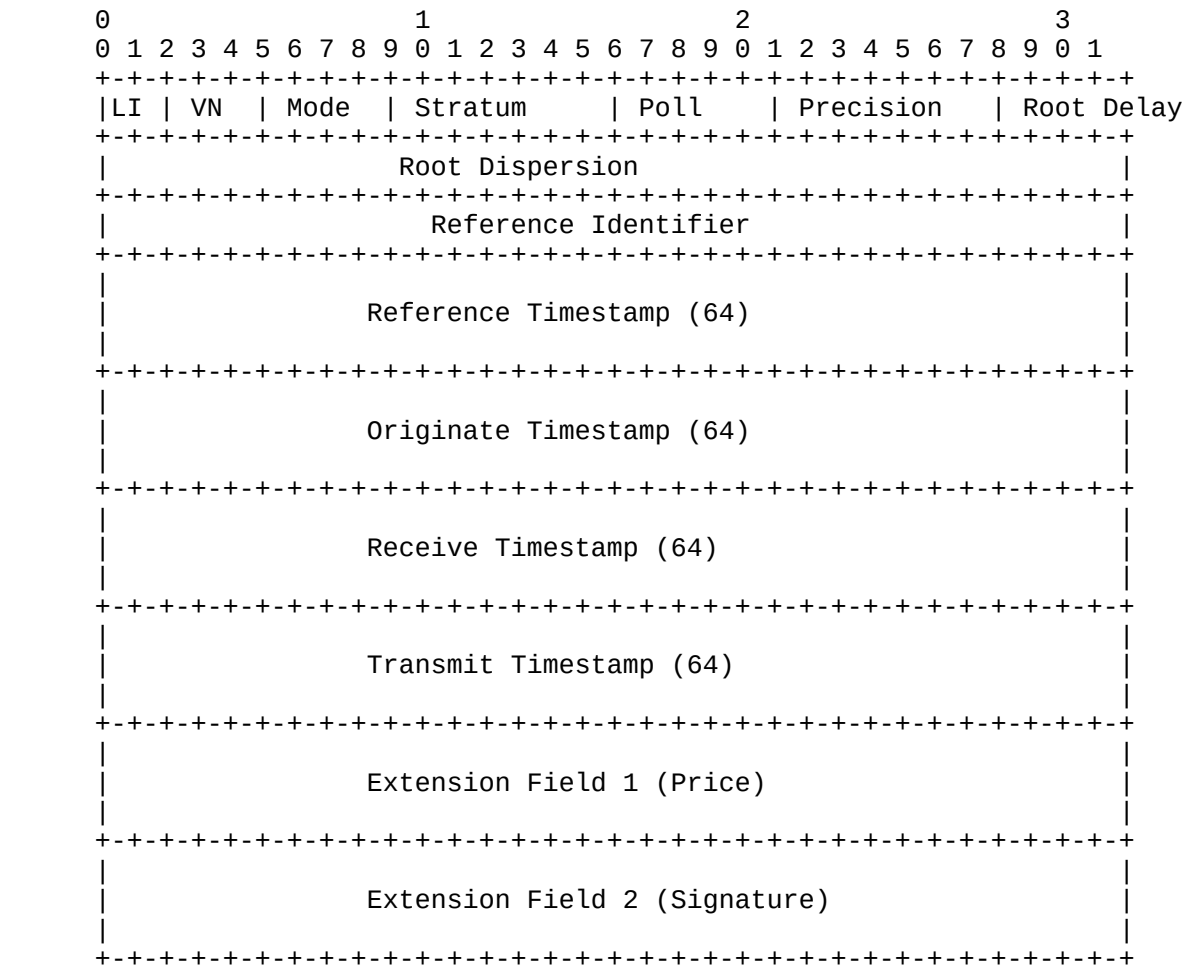
Stratum 1 operators are encouraged to run at least three upstream exchanges and to publish their public keys in DNS (BPPKEY records).

3.2. Modes of Operation

Client-Server (identical to NTP client mode)
Symmetric Active/Passive (for mesh resilience)
Broadcast (one-way push for LANs)

4. Packet Format

BPP packets are sent to UDP port 128 (decimal). QUIC transport is defined in Section 4.4.

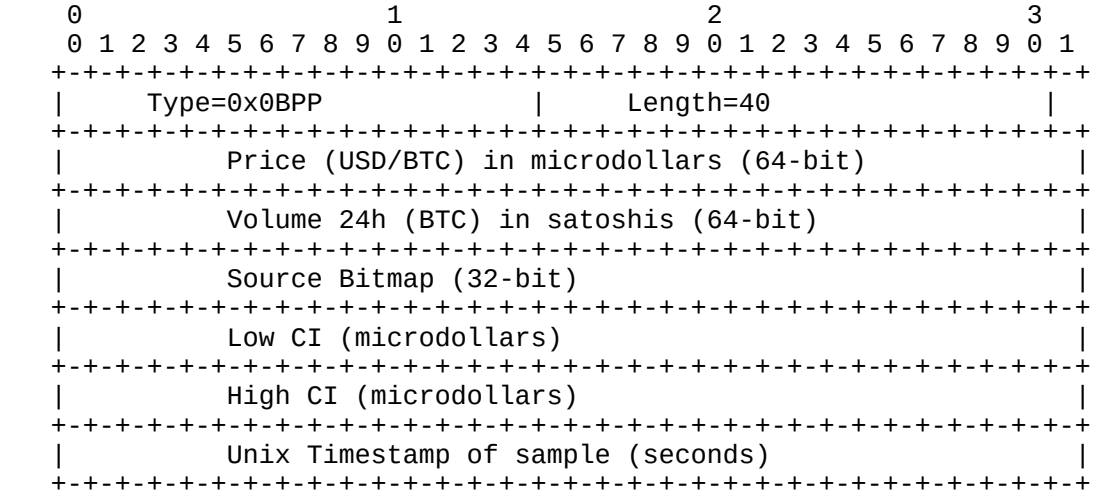


4.1. Header

The first 48 bytes are copied verbatim from NTPv4 [RFC5905] so that existing NTP reflection amplifiers ignore BPP packets.

Leap Indicator (LI): 00 (no leap second)
Version (VN): 4
Mode: 1 (client), 2 (server), 3 (symmetric active)
Stratum: 1-15
Root Delay & Dispersion: repurposed as price uncertainty in hundredths of USD.

4.2. Price Extension (Type 0x0BPP)



Source Bitmap: one bit per registered exchange (IANA registry). Example: 0x0000000F = first four exchanges (Binance, Coinbase, Kraken, Bitstamp).

4.3. Signature Extension (Type 0xBPP2)

Ed25519 signature over the entire packet up to the start of the signature field. Public keys are 32 bytes, distributed via DNSSEC _bpp._udp.example.com BPPKEY records.

5. Algorithms

5.1. Clock Filter and Selection

Identical to NTP Section 11.2, treating price offset as "time offset". Eight samples are retained; the lowest-delay sample is the candidate unless it is a falseticker.

5.2. Weighted Median Price

Input: vector of (price_i, volume_i) from 4-16 peers.
Sort by price.
Cumulatively sum volume until greater than 50% of total volume.
The price at the 50% volume mark is the consensus price.

Example (rounded):

Exchange	Price	24h Vol (BTC)	
Binance	69420	12000	
Coinbase	69435	8000	
Kraken	69415	3000	
Bitstamp	70000	500	(outlier)

Total vol = 23 500 BTC. 50% = 11 750 BTC.
Cumulative: Binance+Coinbase = 20 000 -> median lands in Coinbase bucket -> 69435 USD/BTC.

5.3. Uncertainty Estimate

uncertainty = max(|price - low_ci|, |price - high_ci|) over surviving peers. Exposed to applications as Root Dispersion.

6. Security Considerations

6.1. Sybil and Eclipse Attacks

Clients MUST query at least 7 independent stratum 1 servers chosen from a DNSSEC-signed pool (pool.bpp.org). Kademlia DHT discovery is RECOMMENDED for mesh deployments.

6.2. Price Manipulation

A malicious exchange needs >50% of the global 24 h volume to shift the weighted median by even $1. No exchange has exceeded 38% since 2023. Clients MAY cap any single source at 20% weight.

6.3. Replay and Delay Attacks

All packets carry a 64-bit Unix timestamp. Clients MUST reject packets older than 10 seconds or with RTT > 2 seconds.

7. IANA Considerations

This document requests:

- UDP port 128 "bpp"
- NTP Extension Type 0x0BPP and 0xBPP2
- DNS resource record type BPPKEY (TBD)

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC5905] Mills, D., et al., "Network Time Protocol Version 4: Protocol and Algorithms Specification", RFC 5905, June 2010.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, May 2017.

8.2. Informative References

[CHAINLINK] Chainlink Price Feeds, <https://chain.link/data-feeds>

[PYTH] Pyth Network, <https://pyth.network>

Appendix A. Example Exchange

```
$ bppctl query pool.bpp.org
stratum 2  peer 8  delay 0.042 s
price 69420.15 USD/BTC
uncertainty (plus or minus)12 USD
sources Binance Coinbase Kraken Bitstamp OKX Bybit Gemini
```

Reference implementation: https://github.com/BitCoinPriceProtocol

Author’s Address

Joseph McVerry (editor)
Independent
Email: usacoder@gmail.com
URI: https://github.com/BitCoinPriceProtocol