BitcoinPurple

A Peer-to-Peer Electronic Cash System

Ticker: **BTCP**

Founded by **Alym Wehrli**

Maintained by Davide Grilli, Maurito83

Originally launched: **4 August 2023**

May 2026

Website:	`bitcoinpurplechain.com`
Explorer:	`bitcoinpurple-explorer.store`
Community:	Telegram `t.me/+o3I0A1q1W29mMmQ0`

Contents

Abstract

BitcoinPurple (BTCP) is a decentralised peer-to-peer digital currency designed to enable fast, low-cost, censorship-resistant transactions without reliance on intermediaries or central authorities. Derived directly from the Bitcoin Core codebase, BitcoinPurple retains Bitcoin's battle-tested SHA-256d proof-of-work consensus, its UTXO model, and its full suite of modern script capabilities (SegWit, Taproot), while introducing three key refinements:

- **1-minute block interval** — ten times faster confirmations than Bitcoin.
- **120-block difficulty retarget** (≈2 h) — rapid hashrate-responsive adjustment with a 4× change ceiling per epoch.
- **Strict monetary cap of 1 000 000 BTCP** — all soft-forks (including Taproot) active from genesis; Lightning Network support built in from the start.

BitcoinPurple launched with no premine on 4 August 2023. The initial block reward is 1 BTCP, halving every 500 000 blocks, yielding an asymptotic supply of ≈1 000 000 BTCP. Infrastructure development is ongoing, with a dedicated Electrum SPV wallet and a Lightning Network node implementation on the near-term roadmap.

1 Introduction

Since the publication of the Bitcoin whitepaper in 2008, blockchain-based digital currencies have established that peer-to-peer electronic cash is not only theoretically sound but practically deployable at scale. Bitcoin remains the gold standard for security and decentralisation; however, its 10-minute block interval and comparatively slow difficulty adjustment make it sub-optimal for everyday micropayments and high-frequency retail use.

BitcoinPurple addresses this gap without sacrificing Bitcoin's proven security model. By shortening the block interval to 60 seconds and tightening the difficulty-adjustment window to 120 blocks (≈2 hours), the network achieves a user experience comparable to traditional payment processors while remaining fully permissionless and censorship-resistant.

The project was founded by **Alym Wehrli** and launched with a public genesis block on **4 August 2023**. It is currently maintained and developed by **Davide Grilli** and **Maurito83**. The codebase is a fork of Bitcoin Core, meaning that security improvements and protocol upgrades from the upstream Bitcoin ecosystem can be integrated with minimal friction. All modern Bitcoin soft-forks — SegWit, CSV, CLTV, and Taproot — are active from block 0, providing a clean slate for second-layer development.

1.1 Design Principles

1. **Bitcoin-compatible security** — SHA-256d PoW means BTCP is mineable with the same ASIC hardware as Bitcoin, lowering the barrier to participation.
2. **Speed** — 1-minute blocks reduce median confirmation latency from ≈5 minutes (Bitcoin) to ≈30 seconds.
3. **Scarcity** — a hard cap of 1 000 000 BTCP mirrors Bitcoin's deflationary model at a more accessible nominal unit price.
4. **Fairness** — no premine; distribution begins from the genesis coinbase.
5. **Futureproofing** — native Taproot and Lightning support enable privacy, smart contracts, and instant off-chain payments from day one.

2 Technical Architecture

2.1 Proof-of-Work Algorithm

BitcoinPurple uses **SHA-256d** (double SHA-256), identical to Bitcoin. This choice was deliberate:

- Existing SHA-256 ASIC miners can mine BTCP without hardware modification.
- The algorithm has been subject to over a decade of cryptanalysis with no known weaknesses at the current security margin.
- Mining pools and firmware developed for Bitcoin are compatible after a simple RPC endpoint change.

The mainnet PoW target (difficulty-1 limit) is:

```
00000ffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
```

2.2 Block Parameters

Table 1: Core consensus parameters

Parameter	Value	Note
Block interval (`nPowTargetSpacing`)	60 s	10× faster than Bitcoin
Difficulty retarget window	120 blocks	≈ 2 hours
PoW target timespan	7 200 s	120 × 60 s
Max adjustment per retarget	±4×	clamped to [1 800 s, 28 800 s]
Coinbase maturity	100 blocks	≈ 100 minutes
Rule-change activation threshold	108/120 blocks	90%
Protocol version	70016	Bitcoin Core-compatible

2.3 Difficulty Adjustment

BTCP retargets difficulty at every block height H where $H \bmod 120 = 0$. The algorithm is identical to Bitcoin's, but operating on a 120-block window rather than 2016 blocks:

$$T_{\text{new}} = T_{\text{old}} \times \frac{t_{\text{clamped}}}{7200}, \qquad t_{\text{clamped}} = \text{clamp}(\text{actual\_timespan},\ 1800,\ 28800)\ \text{s}$$

$$T_{\text{new}} = \min(T_{\text{new}},\ T_{\text{limit}})$$

This design means:

- Blocks produced faster than 60 s increase difficulty.
- Blocks produced slower than 60 s decrease difficulty.
- A single epoch can never move difficulty by more than a factor of 4.

The short retarget window provides rapid response to large hashrate changes — a critical property for a young network where mining participation may be volatile.

2.4 Emission Schedule

The total monetary supply is capped at **1 000 000 BTCP**. Emission follows a halving schedule anchored at every 500 000 blocks:

Table 2: Block reward schedule

Era	Block range	Reward	Era total	Cumulative
0	0 – 499 999	1.00000000 BTCP	500 000 BTCP	500 000 BTCP
1	500 000 – 999 999	0.50000000 BTCP	250 000 BTCP	750 000 BTCP
2	1 000 000 – 1 499 999	0.25000000 BTCP	125 000 BTCP	875 000 BTCP
3	1 500 000 – 1 999 999	0.12500000 BTCP	62 500 BTCP	937 500 BTCP
⋮	⋮	⋮	⋮	⋮
∞	—	$\to 0$	$\to 0$	$\approx$ 1 000 000 BTCP

Note on spendable supply: The genesis coinbase (1 BTCP) follows standard construction but, as in Bitcoin Core-derived chains, it is not spendable from the UTXO set. The maximum spendable subsidy therefore asymptotically approaches ≈999 999 BTCP.

2.5 Address Formats and Encoding

Table 3: Address encoding — Mainnet

Type	Prefix byte	Base58 prefix	Bech32 HRP
P2PKH (legacy)	56 (0x38)	P	—
P2SH	55 (0x37)	P	—
P2WPKH / P2WSH	—	—	btcp1...
P2TR (Taproot)	—	—	btcp1p...
WIF (private key)	183 (0xb7)	—	—

Table 4: HD key version bytes — Mainnet (BIP32 / SLIP-0132)

Script type	xpub prefix	xprv prefix	Base58 header
Standard (P2PKH)	0488B21E	0488ADE4	xpub / xprv
P2WPKH-P2SH (BIP49)	049D7CB2	049D7878	ypub / yprv
P2WPKH (BIP84)	04B24746	04B2430C	zpub / zprv
P2TR (BIP86)	0488B21E	0488ADE4	xpub / xprv + path

2.6 Soft-Fork Activation

All soft-forks are active from genesis (block 0), providing a clean protocol baseline with no legacy upgrade paths to maintain:

Table 5: Active soft-forks from genesis

BIP(s)	Feature	Activation height
BIP34	Block height in coinbase	0
BIP65	CHECKLOCKTIMEVERIFY	0
BIP66	Strict DER signatures	0
BIP68/112/113	CheckSequenceVerify (CSV)	0
BIP141/143/147	Segregated Witness (SegWit)	0
BIP340-342	Taproot / Schnorr / Tapscript	0 (ALWAYS_ACTIVE)

2.7 Genesis Block

Table 6: Genesis block parameters

Field	Value
Timestamp (UTC)	2023-08-04T05:27:12Z
Unix timestamp	1691126832
Hash (display)	`000003823fbf82ea...c015`
Merkle root	`b5f46757618a0aa2...0a05`
nBits	`1e0ffff0`
Nonce	1 302 816 (`0x13E120`)
Version	1
Coinbase message	*"Global transactions for everyone around the world"*
LN chain_hash (wire)	`15c04ef0bc1856d6...0000`

3 Network Infrastructure

3.1 Node Software

The BitcoinPurple full-node daemon is **`bitcoinpurpled`** (version 1.1.1), a Bitcoin Core fork with BTCP-specific consensus parameters. The companion CLI tool is `bitcoinpurple-cli`. Configuration is stored at `~/.bitcoinpurple/bitcoinpurple.conf`.

Table 7: Network ports

Service	Mainnet	Testnet	Signet	Regtest
P2P	13496	23496	33496	18444
RPC	13495	23495	33495	18443
ElectrumX TCP	50001	60001	—	—
ElectrumX SSL/TLS	50002	60002	—	—

Table 8: Network identity bytes

Parameter	Mainnet	Regtest
Magic bytes (P2P)	`fc 99 13 95`	`31 34 6a c9`
Bech32 / BOLT11 HRP	`btcp`	`rbtcp`

3.2 ElectrumX Server

BitcoinPurple ships a coin-definition patch for the ElectrumX indexing server. The patch adds a `BitcoinPurple` class to `electrumx/lib/coins.py`, enabling full UTXO-history indexing and the standard Electrum protocol (version 1.4.2).

Key ElectrumX parameters:

The ElectrumX node requires the full node to run with `txindex=1` and pruning disabled. SSL/TLS service on port 50002 is recommended for public deployments.

Table 9: ElectrumX coin parameters

Parameter	Value
COIN	BitcoinPurple
GENESIS_HASH	000003823fbf82ea...c015
SEGWIT_HRP	btcp
RPC_PORT	13495
REORG_LIMIT	1 200 blocks
MIN_REQUIRED_DAEMON_VERSION	1.1.1

4 Lightning Network

BitcoinPurple's 1-minute block time and native Taproot support make it technically well-suited for Lightning Network (LN) payment channels. An LN implementation for BTCP is on the project roadmap (see Section 7).

4.1 Chain Identification (BOLT1)

Every LN message that references a specific chain carries a `chain_hash` — the genesis block hash in wire byte order (little-endian):

Table 10: LN chain identification

Network	chain_hash (BOLT1 wire)
Mainnet	15c04ef0bc1856d6b1ec199ca25d0aa7e77c6114e2cb0649ea82bf3f82030000
Testnet	98d9f92e8867ee945d5aab422bd49896497f58cc6f8168d31a1c92c3fd020000

4.2 BOLT11 Invoice Prefix

Network	HRP	Example prefix
Mainnet	btcp	lnbtcp1...
Testnet	tbtcp	lntbtcp1...

4.3 Block-Time-Scaled Timeout Parameters

This is the most safety-critical aspect of LN on BTCP. Because BTCP has 1-minute blocks (vs Bitcoin's 10-minute blocks), all block-count-based LN timeouts *must* be scaled by a factor of ×10 to maintain the same real-world security windows:

Failure to scale these parameters would leave channel operators with a dangerously short penalty window — for example, Bitcoin's default `to_self_delay` of 144 blocks would grant only 2.4 hours to react to a cheating peer on BTCP, instead of the intended 24 hours.

Table 11: Recommended LN timeout parameters for BTCP

Parameter	Bitcoin	BTCP	Wall-clock
`to_self_delay` (justice window)	144 blocks	**1 440 blocks**	≈ 24 h
`cltv_expiry_delta` per hop	40 blocks	**400 blocks**	≈ 6.7 h
`min_final_cltv_expiry_delta`	9 blocks	**90 blocks**	≈ 90 min
Max remote `to_self_delay`	2 016 blocks	**20 160 blocks**	≈ 14 days
`max_cltv_expiry`	2 016 blocks	**20 160 blocks**	≈ 14 days
Channel funding confirmation target	3–6 blocks	**30–60 blocks**	≈ 30–60 min

5 Wallet Infrastructure

5.1 Current State

Users may currently interact with BitcoinPurple through:

- **Full node wallet** (`bitcoinpurpled` built-in wallet) — requires a fully synced node.
- **Block explorer** — bitcoinpurple-explorer.store for transaction and address lookup.

5.2 Electrum SPV Wallet (Roadmap)

A dedicated SPV wallet is under development as a fork of the Electrum client. The wallet will connect to ElectrumX servers over TCP port 50001 (plain) or 50002 (SSL/TLS) and will support all BTCP address formats:

Table 12: Electrum wallet `constants.py` key parameters

Parameter	Mainnet	Testnet
`NET_NAME`	`"bitcoinpurple"`	`"testnet"`
`ADDRTYPE_P2PKH`	56	56
`ADDRTYPE_P2SH`	55	55
`WIF_PREFIX`	0xb7 (183)	0xb7 (183)
`SEGWIT_HRP`	`btcp`	`tbtcp`
`BOLT11_HRP`	`btcp`	`tbtcp`
`POW_TARGET_SPACING`	60	60
`COINBASE_MATURITY`	100	100

Supported derivation paths:

BIP	Script type	Path
BIP44	P2PKH (legacy)	`m/44'/COIN_TYPE'/0'/...`
BIP49	P2WPKH-P2SH (wrapped SW)	`m/49'/COIN_TYPE'/0'/...`
BIP84	P2WPKH (native SegWit)	`m/84'/COIN_TYPE'/0'/...`
BIP86	P2TR (Taproot)	`m/86'/COIN_TYPE'/0'/...`

The BIP44 coin type for BTCP is not yet registered in SLIP-0044; a provisional value aligned with the BTCP P2P port (13496) is used internally until official registration.

5.3 Dust Thresholds

BTCP uses the same dust limits as Bitcoin, since script formats are identical:

Script type	Dust limit
P2PKH	546 sat
P2WPKH	294 sat
P2WSH	330 sat
P2TR (Taproot)	294 sat
`OP_RETURN`	0 (unspendable)

6 Use Cases

BitcoinPurple's combination of fast block times, low fees, and strong security makes it suitable for a broad range of payment scenarios:

1. **Retail payments** — 1-minute confirmations enable in-store payments where the customer can leave after a single on-chain confirmation.
2. **Remittances** — censorship-resistant international transfers with no correspondent-bank fees and near-Bitcoin security guarantees.
3. **Micropayments** — the low nominal unit price and Lightning-ready infrastructure support sub-cent micropayments for content, APIs, and IoT applications.
4. **Online purchases** — faster confirmation reduces cart-abandonment risk for e-commerce merchants compared to 10-minute-block chains.
5. **Cross-border transactions** — permissionless global reach with no restrictions based on jurisdiction, identity, or transaction size.
6. **Lightning Network instant payments (roadmap)** — once the LN layer is live, payments will settle in milliseconds with fees measured in fractions of a satoshi, enabling real-time streaming payments and machine-to-machine commerce.

7 Roadmap

Table 13: Development roadmap

Phase	Status	Deliverable
Genesis	**Complete**	Full-node launch (4 Aug 2023); mainnet, testnet, signet, regtest; SegWit + Taproot active from genesis.
Explorer	**Complete**	Public block explorer at `bitcoinpurple-explorer.store`.
ElectrumX	**Complete**	ElectrumX coin patch; public Electrum server infrastructure (ports 50001 / 50002).
Electrum Wallet	**In progress**	SPV wallet fork of Electrum supporting P2PKH, SegWit, Taproot, HD derivation (BIP44/49/84/86), and SLIP-0132 extended keys.
Lightning Network	**Planned**	LN node fork (CLN or LND) with BTCP chain parameters, scaled block-count timeouts (§7), BOLT11 `btcp` HRP, and DNS bootstrap seed infrastructure.
SLIP-0044 Registration	**Planned**	Official coin-type registration for BTCP to ensure wallet interoperability.
Exchange Listings	**Future**	Listing on cryptocurrency exchanges to provide market liquidity.

8 Team and Governance

8.1 Core Team

Name	Role
Alym Wehrli	Founder
Davide Grilli	Developer & Maintainer
Maurito83	Community Manager

8.2 Governance Model

BitcoinPurple follows a community-driven governance model in the spirit of open-source Bitcoin development. Protocol changes are discussed openly in the community Telegram group (t.me/+o3I0A1q1W29mMmQ0) and, once community consensus is reached, are implemented by the core developers and released under the project's open-source licence.

Key principles:

- **Transparency** — all code changes are published publicly on GitHub before activation.
- **Community input** — major protocol decisions are discussed in the Telegram community before any implementation begins.
- **Miner signalling** — soft-fork activations require 90% (108 / 120 blocks) miner signalling within the retarget window.
- **No premine / no ICO** — there are no founders' tokens, investor allocations, or pre-sold coins; every BTCP in existence was earned through mining.

9 Security Considerations

9.1 51% Attack Resistance

As a young SHA-256d network, BitcoinPurple shares its proof-of-work algorithm with Bitcoin. This is a deliberate security trade-off: ASIC hardware developed for Bitcoin can also mine BTCP, which expands the accessible miner base. However, as hashrate grows, the cost of a 51% attack increases proportionally. The project encourages mining participation to strengthen network security.

9.2 Short Block Interval and Orphan Rate

1-minute blocks produce a higher orphan rate than 10-minute blocks if network propagation latency is non-negligible relative to the block interval. Compact block relay (BIP152, inherited from Bitcoin Core) mitigates this by propagating only missing transactions after a block header is announced, reducing propagation time to well under one second on modern infrastructure.

9.3 Lightning Network Safety

As documented in Section 5.3, LN timeout parameters *must* be scaled for BTCP's 1-minute block cadence. Using unmodified Bitcoin LN defaults on BTCP would reduce the justice window from 24 hours to 2.4 hours — an unacceptable security degradation. The official BTCP LN fork will ship with correct scaled defaults.

9.4 Coinbase Maturity

Mining rewards require 100 blocks (≈100 minutes) before they can be spent. This provides protection against chain reorganisations invalidating recently mined rewards.

10 Conclusion

BitcoinPurple represents a carefully considered evolution of the Bitcoin protocol, optimised for the everyday payment use case without sacrificing the core properties — decentralisation, censorship-resistance, and verifiable scarcity — that give Bitcoin its value.

The key design decisions are mutually reinforcing:

- SHA-256d PoW preserves compatibility with the world's largest pool of dedicated mining hardware.
- 1-minute blocks dramatically reduce confirmation latency for end users.
- 120-block difficulty retarget keeps the network stable under volatile hashrate without compromising security.
- A hard cap of 1 000 000 BTCP, with no premine, ensures that no single party holds a structural advantage.
- Native Taproot and Lightning readiness from genesis position BTCP for a second-layer ecosystem without requiring a contentious soft-fork campaign later.

With the full-node software stable, an ElectrumX indexing layer deployed, and an Electrum SPV wallet and Lightning Network implementation actively in development, BitcoinPurple is progressing toward its vision of a fast, accessible, and secure global payment network.

The community is invited to participate in development discussions on Telegram (t.me/+o3I0A1q1W29mMmQ0), to run a full node, and to contribute to the open-source codebase.

"Global transactions for everyone around the world."
— BitcoinPurple genesis coinbase message

A Network Parameter Reference

A.1 Quick Reference

Table 14: Network parameters across all chain modes

Parameter	Mainnet	Testnet	Signet	Regtest
P2P port	13496	23496	33496	18444
RPC port	13495	23495	33495	18443
ElectrumX TCP	50001	60001	—	—
ElectrumX SSL	50002	60002	—	—
P2PKH prefix	56	56	56	56
P2SH prefix	55	55	55	55
WIF prefix	183	183	183	183
Bech32 HRP	`btcp`	`tbtcp`	`tbtcp`	`rbtcp`
Block time	60 s	60 s	60 s	instant
Halving interval	500 000	—	—	150

A.2 Magic Bytes

Network	Magic
Mainnet	`fc 99 13 95`
Testnet	`29 fb c5 fe`
Regtest	`31 34 6a c9`

A.3 Genesis Block Hashes

Network	Genesis hash (display)
Mainnet	`000003823fbf82ea4906cbe214617ce7a70a5da29c19ecb1d65618bcf04ec015`
Testnet	`000002fdc3921c1ad368816fcc587f499698d42b42ab5a5d94ee67882ef9d998`
Signet	`00000131aa3124412b7ba8473f137922692c88da8fe26042e250c6cd76b7b403`
Regtest	`6f6ffbda4cb789c69d885d4624ea4a28841d3689fbaf969262150ca45a1ae1df`

A.4 DNS Seeds

Host	Network
`node3.walletbuilders.com`	Mainnet

A.5 Full Node Default Values

Table 15: bitcoinpurpled compile-time defaults

Parameter	Default	Source
`dbcache`	450 MiB	`src/txdb.h:30`
`maxmempool`	300 MB	`src/kernel/mempool_options.h:20`
`mempoolexpiry`	336 h	`src/kernel/mempool_options.h:24`
`blockmaxweight`	3 996 000 wu	`src/policy/policy.h:23`
`rpcthreads`	4	`src/httpserver.h:12`
`rpcworkqueue`	16	`src/httpserver.h:13`
`rpcservertimeout`	30 s	`src/httpserver.h:14`
`maxconnections`	125	`src/net.h`

B Legal Disclaimer

This whitepaper has been prepared for informational purposes only and does not constitute an offer to sell, a solicitation of an offer to buy, or a recommendation regarding any security or other financial instrument. BitcoinPurple (BTCP) is a decentralised, open-source software project.

No guarantee of value. Participation in any cryptocurrency project involves significant risk, including the risk of total loss of any funds used to acquire tokens. The value of BTCP may fluctuate and could decline to zero.

No financial advice. Nothing in this document should be construed as investment, legal, tax, or financial advice. Readers should conduct their own research and consult qualified professionals before making any financial decisions.

Forward-looking statements. This document contains forward-looking statements regarding the project's roadmap and future development. Actual results may differ materially from those expressed or implied. The authors assume no obligation to update forward-looking statements.

Open-source software. The BitcoinPurple software is provided "as is", without warranty of any kind. Users run nodes and wallets at their own risk.