



Proof over Promise

The Bitcoin Swap whitepaper:
philosophy, architecture, token model and ecosystem
of the Bitcoin Swap chain (chain ID 482120)

- | | | | |
|---|------------------------------|----|-------------------|
| 1 | Abstract | 7 | Tokenomics |
| 2 | Philosophy: six principles | 8 | Ecosystem |
| 3 | Design rules | 9 | Operations |
| 4 | The network | 10 | Roadmap |
| 5 | Architecture | A | Contract registry |
| 6 | Assets and the RWA framework | B | References |

1 Abstract

Bitcoin Swap is an EVM chain (chain ID **482120**). It runs Hyperledger Besu with QBFT consensus, five-second blocks and immediate finality. Its native coin, **BTCw**, is quoted at the BTC/USD rate and pays for gas at a fraction of a cent per transaction.

The chain hosts three kinds of assets:

- **Bridged assets locked 1:1 on Arbitrum:** WBTCw (backed by WBTC) and USDC.e (backed by USDC).
- **USDw**, the chain's US-dollar unit of account.
- **321 oracle-priced tracker tokens** following crypto assets, US equities and ETFs.

Users trade them on several venues:

- two oracle market makers (BTCw and ETHw against USDw);
- two families of continuous-liquidity pools, 643 pools in all;
- a standard Uniswap V2 venue.

An ownerless router reaches any of these assets in one transaction.

This paper sets out the idea the system is built on: **every claim about value should be provable on-chain, by anyone, at any time**. We call it *proof over promise*. The paper then turns that idea into design rules, an architecture, a token model and an ecosystem plan.

2 Philosophy: six principles

Bitcoin showed that a monetary system can earn trust without asking for it. Any holder can check the whole supply and every rule. Bitcoin Swap takes that attitude and applies it to a fast, programmable EVM chain: users *check* rather than *believe*.

P1 **Proof over promise**

Each statement about backing, supply, volume or yield maps to an on-chain quantity that anyone can read with a public RPC call. Each published figure should mean exactly what it says. That is why *backed value* and *protocol inventory* are reported as separate numbers, rolling out in the Proof phase (section 10).

P2 **Backing comes from outside**

A backed token is backed by an asset the system cannot create.

- WBTCw is backed by WBTC, and USDC.e by USDC.
- Both are locked on another chain, under rules that no key can override.
- The native coin is never used to absorb redemptions of another token, so value cannot leak between assets in a loop.

P3 **Rewards come from revenue**

Rewards should be funded by income the protocol has already collected: swap fees, spreads and bridge fees. A reward that depends on continual top-ups does not last, while one funded from revenue grows with real use. From Earn v3 (Proof phase), each epoch's rewards are bounded by realised revenue.

P4 **Rules before discretion**

Order caps, oracle bounds, staleness halts and inventory limits are written into contracts before they are needed. Limits are not loosened in a hurry, because a rule that bends under pressure was never a rule.

P5 **Keys cannot move backed funds**

The WBTC and USDC.e bridge routes deployed in October 2026 are *sealed*, and every new route follows the same design. Their verification module and remote router are fixed at deployment. An administrator can pause a route or manage its allowlist, and can do nothing else. Losing a key therefore affects availability, not solvency.

P6 **Stability first, then decentralisation**

A new network is safest when one accountable operator runs it during launch. Bitcoin Swap is operated by its founding operator through the launch phase, until 22 December 2026, and then hands control out step by step on published milestones (section 10).

The test applied to every feature: *Can a user verify what they hold, and the rule that protects it, without asking anyone?*

3 Design rules

The principles turn into ten rules that guide the contracts, operations and roadmap. The last column shows the roadmap phase in which each rule is fully delivered (section 10).

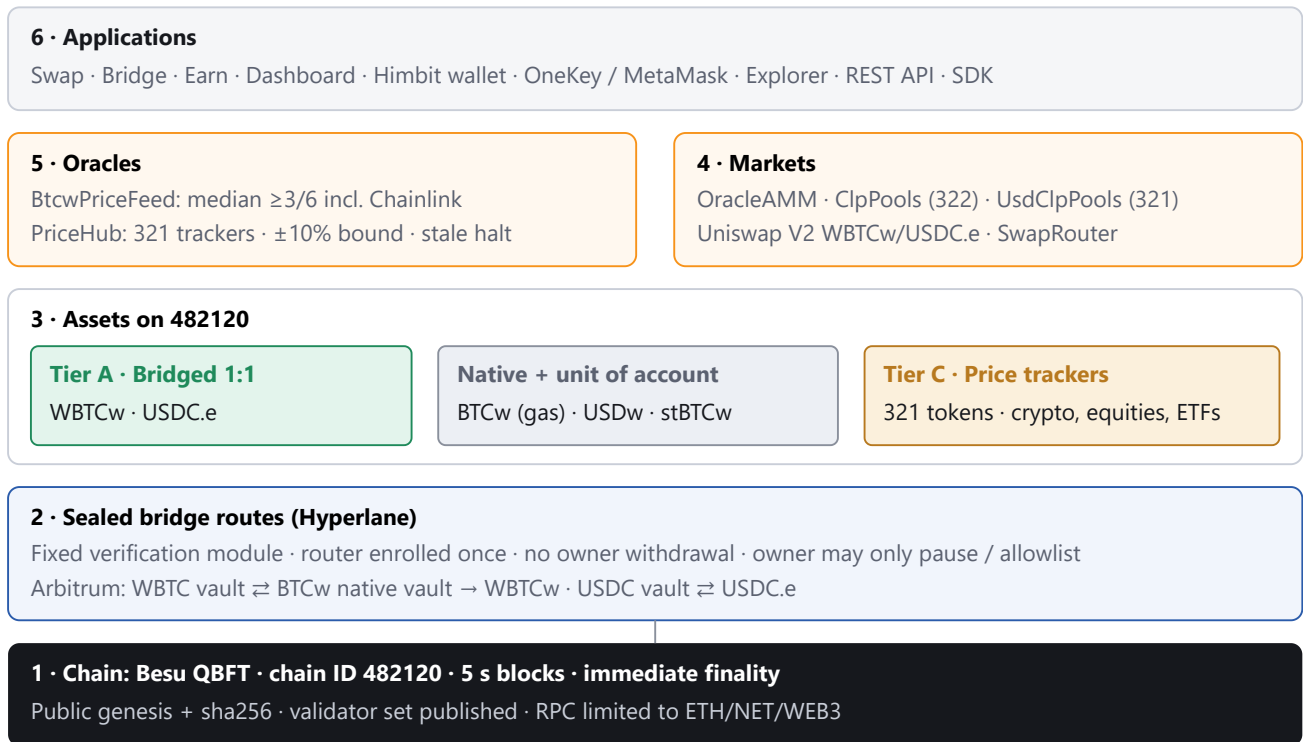
Rule	Topic	Statement	Phase
R1	External backing	Backed tokens are minted only when an external asset is locked: $WBTC_w \Leftarrow WBTC$, $USDC_e \Leftarrow USDC$. They have no owner mint function.	Launch
R2	Revenue-funded rewards	Rewards in each epoch are bounded by revenue realised in the epoch before. The reward budget and its source are published.	Proof
R3	Same-asset reserves	Reserves are held in the same asset as the claim, cover 100% of it, and are released by a holder's redemption message.	Launch (bridged) · Open (USDw)
R4	Breakers in code	Max order size, $\pm 10\%$ oracle jump bound, stale-price halt and per-token daily caps live in contracts. From the decentralisation phase, cap changes go through a timelock.	Launch · Open (timelock)
R5	Liquidity care	Liquidity moves in rehearsed slices, never in a way that thins a live venue. Pool depth is tracked against the largest holders.	Launch · Proof (depth tracking)
R6	Disclosed market makers	Every keeper and rebalancer has a published address and mandate (developer docs, Addresses page). Its volume is reported separately from user volume.	Launch
R7	Honest metrics	Usage counts only addresses outside the operator list. TVL is reported as backed value and protocol inventory, separately.	Proof
R8	Validator independence	Validators are added by count of distinct operators. QBFT is never run with exactly two validators.	Proof → Community
R9	Oracle discipline	A median of at least three sources, a jump bound and a staleness halt. Manual submissions carry a reason code. A tracker whose sources disagree is not priced from a single source: no price is written.	Launch · Proof (reason codes)
R10	Separated roles	Reserves sit in sealed contracts, market inventory in capped contracts, and the treasury in its own account. No single contract holds all three.	Proof

4 The network

Item	Value
Chain	Bitcoin Swap · chain ID 482120 (0x75b48) · native coin BTCw, 18 decimals
Client and consensus	Hyperledger Besu 26.2.0, QBFT, 5 s blocks, immediate finality, 30M gas per block, Shanghai + Cancun
Genesis	22 September 2026. Published at btcw.tech/genesis.json with its sha256 (686cc9ad...385fea) so anyone can check it. Block reward is zero
Fees	Base fee 0, minimum gas price 0.001 gwei. A typical pool swap (~80k gas, measured median 77,806) costs about 0.00000008 BTCw
Capacity	About 285 transactions per second measured at peak
Public endpoints	https://rpc.btcw.tech , wss://rpc.btcw.tech/ws , https://explorer.btcw.tech (Blockscout), REST API btcw.tech/api/v2 , JavaScript SDK
Operation	Run by the founding operator during the launch phase (until 22 December 2026). The validator set is listed on the transparency page
Wallets	Any EVM wallet. One-click network add through <code>wallet_addEthereumChain</code> (OneKey, MetaMask), plus the Himbit wallet

5 Architecture

The system has six layers. Each layer can be checked on its own.



External backing on Arbitrum One: WBTC and USDC locked in collateral routers

Figure 1. Layered architecture.

Sealed bridge routes

Each route has the following properties:

- The message-verification module is fixed as an immutable value at deployment.
- The remote router is enrolled exactly once.
- Hooks are fixed, fees are off, and the vault accepts no LP deposits or rebalancing.
- The owner can pause the route and manage its allowlist, and can do nothing else.

The routes enforce:

$$\text{supply}(\text{WBTCw}) \leq \text{WBTC locked on Arbitrum} \quad \cdot \quad \text{supply}(\text{USDC.e}) = \text{USDC locked on Arbitrum}$$

Both sides of each equation can be read from public RPC endpoints of the two chains.

Markets

- **Continuous Liquidity Pools.** The fee depends on slippage: output $y = x \cdot X \cdot \gamma / (x + X)^2$, with a 5 bps floor. Every pool pairs with a common base asset (BTCw or USDw), so any two assets swap in at most two hops.
- **OracleAMM.** Quotes at the oracle price ± 30 bps, with a 10 BTCw per-order cap and a 300-second staleness halt.

- **Uniswap V2** (official bytecode). Hosts the WBTCw / USDC.e reference pair that external indexers read. A disclosed keeper holds it at the Chainlink BTC/USD price: threshold 0.5%, at most 50 USDC.e per trade.
- **SwapRouter**. Ownerless. Chains up to four hops across venues in one transaction.

6 Assets and the RWA framework

Every asset sits in exactly one tier. From the Proof phase, the tier is shown in the token's metadata, the API and the explorer.

Tier	What the holder has	Issuance rule	On 482120
A • Bridged	A claim on an asset locked 1:1 on another chain, redeemable by message	Minted only by a verified bridge message. Supply can be checked against the remote vault at any time	WBTCw, USDC.e
B • Custodied RWA	A claim on an off-chain asset (treasury bills, gold, equities) held by a regulated custodian	Requires a named custodian and issuer, attestations at least monthly, an on-chain reserve feed and a redemption path	Roadmap (phase 3)
C • Price tracker	A token whose market price follows a reference price through the oracle and pool rebalancing	Provisioned by a capped rebalancer within daily and per-token limits. The token name states "Price Tracker"	321 tokens: 100 crypto, 201 US equities, 20 ETFs

Operating rules for Tier C

1. **Quorum or pause.** A price is written only when at least 3 sources agree within band. Crypto trackers need $\pm 2\%$ agreement on at least 4 exchanges. Without quorum, no price is written.
2. **Jump bound.** A move above 10% between writes is rejected. Genuine large moves, such as splits or post-weekend gaps, are submitted manually; reason codes for these submissions arrive in the Proof phase.
3. **Corporate-action calendar.** Splits, ticker changes and delistings are scheduled in advance, and pools pause across the event (Proof phase).
4. **Not collateral.** Tier C tokens are trading assets. They are not accepted as loan collateral.
5. **Inventory caps.** Daily and per-token rebalancer caps bound the effect of any single price error.

Tier B building blocks

The protocol side of custodied RWA is three pieces:

- A token standard without owner mint, which changes supply only through attested custodian messages.
- An on-chain attestation registry.
- A reserve page that shows custodian attestations beside on-chain supply.

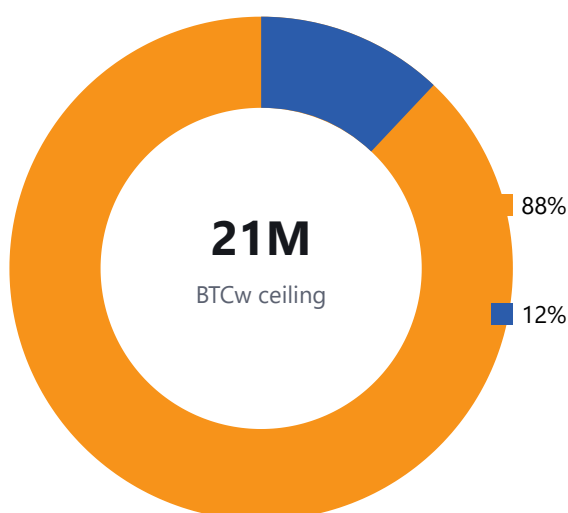
The first Tier B asset launches together with its named custodian and issuer.

7 Tokenomics

7.1 BTCw, the native coin

- **Ceiling:** 21,000,000 BTCw, created at genesis. Block reward is zero and no contract can create native BTCw, so the ceiling is permanent and checkable from block 0.
- **Price reference:** BTCw is quoted at the BTC/USD rate (ratio $R = 1$ on BtcwPriceFeed).
- **Uses:** gas for every transaction, and the base asset of 322 pools.
- **Circulation:** lock 1 WBTC on Arbitrum and 1 BTCw is released from the native vault. Bridge back, and the BTCw returns to the vault while the WBTC unlocks. The route is allowlisted during the launch phase and opens to every wallet in the Open phase.

7.2 Allocation of the 21,000,000 ceiling (proposed)



Bucket	BTCw	Rule
Bridge Reserve	18,480,000	Released only 1:1 against WBTC locked on Arbitrum.
sealed native vault	88%	Returns on bridge-out
Market Inventory	2,520,000	Lives only in market contracts and disclosed keepers. Hard cap; any excess returns to the Reserve
protocol-owned	12%	

Figure 2. Two buckets. There is no team, investor or presale allocation.

Under this allocation, the founding operator is funded from protocol revenue (7.5), not from a coin allocation. That keeps one statement simple enough to check: *every BTCw outside the two buckets is matched by WBTC on Arbitrum.*

7.3 Supply identity

$21,000,000 = \text{Vault reserve} + \text{Market inventory} + \text{Free float}$
Free float (including BTCw wrapped as WBTCw) $\leq$ WBTC locked on Arbitrum

Every term can be read on-chain. A Proof-of-Reserve page will display the identity live. Public bridge-out for WBTC opens once the page is live.

7.4 USDw, the unit of account

USDw quotes the 321 USDw-paired pools and makes up their inventory. Its design follows three rules:

- **Segregation.** USDw held by market contracts and disclosed keepers is inventory. USDw held by anyone else is float. The two are reported separately from the Proof phase.
- **StableReserve (roadmap).** A reserve contract that redeems float USDw 1:1 for USDC.e and enforces $\text{float} \leq \text{reserve on-chain}$.
- **No cross-asset loop.** No contract mints or sells BTCw to support USDw.

7.5 Revenue and rewards



Figure 3. Protocol revenue accrues to the project treasury, which funds rewards, security and grants.

Earn. Earn offers three products: flexible savings, fixed terms of 7 to 90 days, and BTCw staking with a 1:1 receipt token (stBTCw). Rewards are paid automatically to depositors' wallets.

The next version, Earn v3, follows rule R2:

- Each epoch's reward pool is a share of the previous epoch's revenue.
- Rewards are paid in USDC.e, or in WBTCw for BTC deposits.
- The displayed rate is a trailing figure computed from that pool.

8 Ecosystem

The ecosystem is organised into fourteen modules, each following the principles above. Section 10 shows when each module comes online.

#	Module	Components
1	Chain and validators	Besu QBFT; validator set grows by count of independent operators
2	Oracles	BtcwPriceFeed, PriceHub; multi-signer price writes with reason codes
3	Unit of account	USDw; StableReserve against USDC.e
4	Markets	OracleAMM, ClpPools, UsdClpPools, Uniswap V2, SwapRouter
5	Price trackers	321 tokens across crypto, US equities and ETFs
6	Earn	Flexible, fixed-term, staking; revenue-funded rewards (v3)
7	Bridges	Sealed Hyperlane routes for WBTC and USDC to Arbitrum
8	Multi-asset staking	stBTCw, then WBTCw and USDC.e staking
9	Wallets	Himbit, OneKey, MetaMask; one-click network add; token list
10	Payments	Payment links and a checkout SDK in USDC.e and WBTCw
11	Treasury and grants	Revenue splitter, ecosystem grants programme
12	Transparency and data	Proof-of-Reserve page, explorer labels, metrics API, listings (Chainlist, GeckoTerminal, CoinGecko)
13	Developer platform	RPC, REST API, SDK, docs, public test chain with faucet
14	Governance	Parameter proposals with timelock (decentralisation phase)

Participants

USERS

Swap between bridged assets, trackers and the native coin, with immediate finality and negligible gas. Check balances and backing on-chain.

ARBITRAGEURS

Keep the reference pool aligned with external markets. The disclosed keeper is deliberately small, so outside arbitrage is worth doing.

VALIDATORS

Collect gas fees and, from the decentralisation phase, a share of security revenue.

BUILDERS

Full EVM, source verification on the explorer, a public REST API and JS SDK with no API keys, a test chain, and grants.

Developer surface

- RPC: <https://rpc.btcw.tech>, <wss://rpc.btcw.tech/ws>

- Explorer and verification: <https://explorer.btcw.tech>
- API: [btcw.tech/api/v2/{stats, pools, history, swaps, swap/quote, usd-pools, earn}](https://btcw.tech/api/v2/{stats,pools,history,swaps,swap/quote,usd-pools,earn})
- SDK: btcw.tech/swap/sdk/btcw-swap.js
- Contract list: btcw.tech/developers/contracts.json

9 Operations

Change management

- Every on-chain change is rehearsed first. Rehearsals run on a fork of the live chain or on the test chain, with the same signing page and parameters.
- Irreversible steps (deployments, pool creation, liquidity moves) are signed one by one, from a page that shows the exact calldata.
- Services are built and tested locally, then deployed one at a time.

Automatic safeguards

Condition	Automatic response
Oracle older than 300 s	OracleAMM stops quoting
Price move above 10%	Write rejected; a manual submission is required
Reference pool off by more than 0.5%	Keeper trades at most 50 USDC.e. It stands down if its reference is stale or more than 2% from the chain's own feed
Bridge supply out of line with the locked amount	Monitoring alert; the operator can pause the route

Key management

Roles use separate keys:

- the validator key;
- the owner key for sealed contracts;
- bridge verification keys;
- small-balance hot keys for the relayer and keepers.

Keys that guard bridged funds have backups held apart from their hosts.

10 Roadmap

Each phase ends when its checks pass on-chain.

Phase	Milestones
Launch to 22 Dec 2026	• Network run by the founding operator for stability • Public genesis and hash • Sealed WBTC and USDC routes • WBTCw / USDC.e reference pool at the Chainlink price • Earn • Chainlist and GeckoTerminal listings
Proof	• Proof-of-Reserve page with the supply identity • Reserve moved into the sealed native vault • Backed and inventory metrics on every dashboard • Earn v3 • Oracle reason codes and a corporate-action calendar • Three validators • Token list and wallet integrations
Open	• Bridge routes open to every wallet, with per-transaction and daily caps • StableReserve for USDw • Four or more validators, including independent operators • Multi-signer bridge verification • Timelocked cap changes • Independent smart-contract audit
Community	• Seven or more independent validators • Oracle signers run by independent parties • Parameter governance with a timelock • Grants programme • First Tier B asset with a named custodian

Closing

Bitcoin Swap makes a small number of claims. Each one can be checked with a public RPC call and a few lines of code. That is the whole philosophy: proof over promise.

A Contract registry

Addresses on chain 482120. The complete, machine-readable list is btcw.tech/developers/contracts.json.

Source code and verification status of each contract can be inspected on explorer.btcw.tech. The Uniswap V2 contracts use the official v2-core 1.0.1 and v2-periphery bytecode.

Contract	Address
WBTCw (WrappedBTCw) · Tier A	0xA7182E25e635108AD401E3be78f1c2A4593B8831
USDC.e · Tier A	0x7b56B7B06B8e586064787E7FfE466Ab6B78C31C7
USDw · unit of account	0x3b5BD179CA6Aab4DAF0f842829776843ABe6e727
BTCw native vault (WBTC route)	0x10Ecc6EF494D0Ec1A1446a30026951b0923F3606
OracleAMM	0xd953d53414a81eb6AC5a4edE73d13992181aF51E
ClpPools	0x557aDc3d900c471F3907cdDA3a9F5377d6F9E7e0
UsdClpPools	0x78aCB6Ec7aF4cc83BF9E698706de79c08D61C13f
SwapRouter	0x397E607eA05eF7909f84540077F3a716778031E4
BtcwPriceFeed	0x6E0687A5D5a5b98CC5fb05c4d8d742fBD75ba96c
PriceHub	0xE87FDdCC0b668564a20B23F3bE1EE108C805ecb4
Uniswap V2 Factory / Router02	0x453F946CB371a2039137453BAaFfB83FF4ccf9f7 0x436997135b9332B2dFa1B20e6B24f0987778a246
Uniswap V2 pair WBTCw / USDC.e	0xED2967B738d98B3e4D3e6780A08Dc161A55EF304
SimpleEarn / FixedEarn	0x353ffb50779e3A4d96CFaBA62810f0292fE41b7c 0x0a3fD8b35593fB4f82Da4C110C356745Dd7CDce2
StakedBTCw (stBTCw)	0xa4794DB9f26f489db1a6d8Cf6FC2Ab3106B1027e
TokenFactory · OracleRebalancer	0xa4860BdfaE9B2881B1B593aFFC8740d926eCC1d1 0x6c811003D301769575e9A8661B9197FAf2A32e69
Multicall3	0xA0093EA76633A983364cb2582959870eaffDdea0

B References

1. Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.
2. Hyperledger Besu documentation: QBFT consensus, permissioning, private networks (besu.hyperledger.org).
3. Hyperlane documentation: warp routes, collateral routers, interchain security modules (docs.hyperlane.xyz).
4. Adams, H., Zinsmeister, N., Robinson, D. "Uniswap v2 Core", 2020.
5. THORChain documentation: Continuous Liquidity Pools and slip-based fees.
6. Chainlink Data Feeds: AggregatorV3Interface.
7. EIP-1559, EIP-3085 (`wallet_addEthereumChain`), EIP-6963 (multi-wallet discovery), EIP-1167 (minimal proxy).
8. Uniswap Token Lists standard (tokenlists.org).