WIKIBUSINESS

W B I Z

Whitepaper — Version 1.0
September 2026

Independent proof-of-work blockchain
forked from Bitcoin Core — with staking rewards,
hardened pool custody, and optional privacy.

Contents

1. Abstract
2. Introduction & Vision
3. Technical Foundation
4. Supply & Economics
5. Staking — Lock to Earn
6. Pool Security
7. Privacy Roadmap
8. Mining
9. Wallets & Ecosystem
10. Exchange Strategy
11. Roadmap
12. Risks & Disclaimers

1. Abstract

Wikibusiness (WBIZ) is an independent proof-of-work blockchain forked from Bitcoin Core v31.1. It preserves Bitcoin's monetary policy and security model exactly — SHA-256d proof-of-work, ten-minute blocks, a 21,000,000-coin mining schedule with halvings every 210,000 blocks, and Bitcoin's market-based fee model — while adding three things Bitcoin does not have: a staking-rewards pool that pays holders for locking coins over a 100+ year horizon, a hardened tiered-custody system protecting that pool, and a roadmap to optional, Zcash-style shielded privacy where every sender chooses transparent or private transactions.

Total issuance is 21,420,000 WBIZ: the 21,000,000-coin mining schedule plus a one-time 420,000 WBIZ genesis premine dedicated exclusively to staking rewards. Mining is public and permissionless from genesis. This document describes the chain's design, economics, security architecture, roadmap, and risks — plainly, without promises about exchange listings or returns.

2. Introduction & Vision

Bitcoin proved that sound, permissionless digital money works. Wikibusiness starts from that proven foundation rather than reinventing it: the consensus engine is Bitcoin Core's, unchanged in every rule that matters.

The vision builds on that base in three directions:

1. Reward the holders. Long-term holders can lock WBIZ for years of their choosing and earn pro-rata rewards from a dedicated pool designed to pay for over a century.
2. Protect the pool. The staking pool is the system's most valuable key. It is guarded by tiered custody — an offline multisig vault for the bulk, a small online float for payouts, and a payout server that can only pay computed rewards and refuses everything else.
3. Offer privacy as a choice. The roadmap adds an optional shielded transaction pool, Zcash-style: every sender chooses per transaction whether it is transparent (Bitcoin-like) or shielded (private). Privacy is never mandatory and never hidden from the protocol's supply accounting.

What Wikibusiness does not do: it does not change Bitcoin's fee market, it does not redirect block rewards, and it does not call its lock-to-earn program "proof-of-stake" — consensus is and remains proof-of-work.

3. Technical Foundation

Wikibusiness Core v1.0.0 is a fork of Bitcoin Core v31.1. Consensus rules are Bitcoin's:

- Proof-of-work: SHA-256d, the same double-SHA-256 construction as Bitcoin.
- Block time: 10 minutes (difficulty retarget every 2,016 blocks, as in Bitcoin).
- Subsidy schedule: 50 WBIZ per block, halving every 210,000 blocks (~4 years), to a 21,000,000 WBIZ mined cap.
- Fees: unchanged from Bitcoin Core. Fees are market-based (satoshis per vbyte); there is no protocol tax, no fee redirect, and no mandatory pool fee. Relay policy, dust limits, and fee estimation are upstream defaults.

- Script and soft forks: on mainnet all soft-fork rules are active from chain start — BIP 34/65/66/CSV at height 1, SegWit from height 0, Taproot always active. There are no historical script exceptions.

Wikibusiness is a fully independent network. It cannot join or be confused with the Bitcoin network:

Parameter (mainnet)	Value
P2P port / RPC port	59333 / 59332
P2P message magic	`e3 62 69 7a`
Bech32 human-readable part	`wbiz`
P2PKH address version	73 (addresses start with `W`)
P2SH address version	135
WIF private-key version	197
BIP32 public / private versions	`0x046F2DC8` (`wbiz…`) / `0x0473E353` (`wprv…`)
PoW limit	`0x1d00ffff` (Bitcoin's original difficulty)
DNS / fixed seeds	none (operator-configured at launch)

The node software ships as `wikibusinessd` (full node daemon), `wikibusiness-cli` (RPC client), `wikibusiness-tx` (transaction utility), and `wikibusiness-qt` (desktop GUI wallet). Default data directory: `~/.wikibusiness`. The genesis block and its coinbase were independently reproduced in C and Python implementations that agree exactly, as a correctness cross-check.

4. Supply & Economics

4.1 Total issuance: 21,420,000 WBIZ

Component	Amount	Notes
Mined issuance	21,000,000 WBIZ	Bitcoin-identical subsidy schedule
Genesis staking premine	420,000 WBIZ	One-time; staking rewards only
Total	21,420,000 WBIZ	

The premine is additional issuance on top of the 21M mining schedule, not carved out of it. "21M cap" refers to the mining subsidy schedule, exactly as in Bitcoin.

4.2 Halving schedule

Identical to Bitcoin. Each era spans 210,000 blocks (~4 years at 10-minute blocks):

Era	Block range	Reward (WBIZ/block)	Issued in era (WBIZ)
0	0 – 209,999	50	10,500,000
1	210,000 – 419,999	25	5,250,000
2	420,000 – 629,999	12.5	2,625,000
3	630,000 – 839,999	6.25	1,312,500
4	840,000 – 1,049,999	3.125	656,250
5	1,050,000 – 1,259,999	1.5625	328,125

Era	Block range	Reward (WBIZ/block)	Issued in era (WBIZ)
…	…	…	… (continues to the 21M cap)

Figure 1 shows the complete schedule graphically — every era's block reward and the cumulative mined supply over the 200 years following genesis.

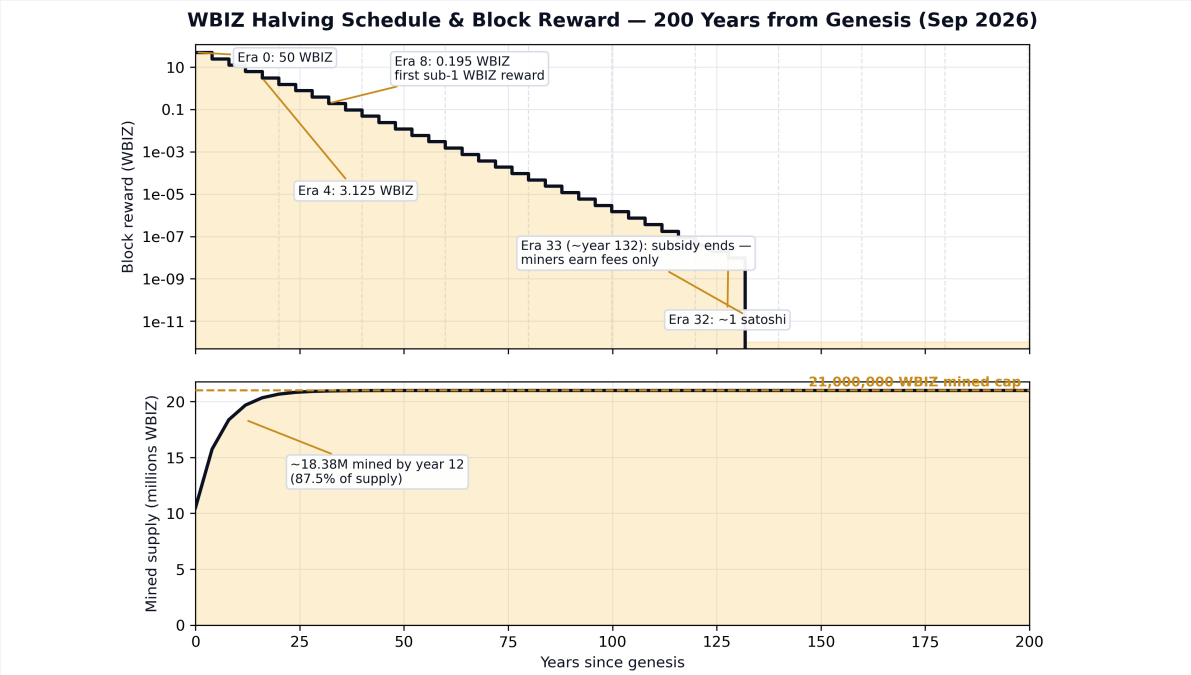

Figure 1 — WBIZ halving schedule and block reward over 200 years

4.3 Genesis block

The genesis coinbase carries two outputs:

- Output 0 — 50 WBIZ tribute. Paid to Bitcoin's historical genesis public key. It is a tribute and is unspendable: it is deliberately not seeded into the UTXO set.
- Output 1 — 420,000 WBIZ staking pool. Paid to the staking-pool address. This output is spendable: a deterministic bootstrap rule (`Chainstate::SeedGenesisOutputs()`) inserts it into the UTXO set on an empty chainstate. This is an initialization rule, not a change to block validation — proof-of-work checks, the subsidy schedule, and script rules are untouched.

Genesis block parameters: version 1, `nBits 0x1d00ffff`, timestamp "Wikibusiness Times 24/Sep/2026 Proof-of-work genesis with staking pool premine". The final proof-of-work nonce and block hash are published with the release software.

5. Staking — Lock to Earn

Wikibusiness rewards long-term holders through a lock-to-earn program funded by the 420,000 WBIZ genesis premine. An important clarification first: this is not proof-of-stake. Consensus is pure proof-of-work and is untouched by staking. Locking is a wallet/application-layer construct built on Bitcoin-native CLTV (CheckLockTimeVerify) timelocked outputs.

5.1 How it works

- A holder locks WBIZ in a timelocked vault for a duration of their choice, in whole years.
- Locked principal always returns to the holder when the lock expires. It is never at risk from the rewards program.
- Rewards accrue over time and are paid automatically from the staking pool.

5.2 Emission: designed to pay for 100+ years

Each year, 1% of the pool's remaining balance is distributed as rewards. Because it is a percentage of what remains rather than a fixed amount, the pool never runs dry:

- Year 1: 4,200 WBIZ distributed.
- After 100 years: roughly 154,000 WBIZ still in the pool, still paying about 1,540 WBIZ per year.
- After 200 years: still paying. The program is designed to outlive its founders.

5.3 Pro-rata distribution

Each staker's weight is coins locked × lock duration in years (coin-years). A staker's annual reward is:

> reward = annual emission × (staker's weight ÷ total weight of all stakers)

Longer locks earn proportionally more — automatically, with no manual tiers and no discretion.

Worked example. In year 1 the emission is 4,200 WBIZ. Alice locks 1,000 WBIZ for 5 years, giving her a weight of 5,000 coin-years. If the network's total weight is 500,000 coin-years, Alice earns 4,200 × 5,000 / 500,000 = 42 WBIZ that year — on top of her 1,000 WBIZ principal, which returns in full at lock expiry.

6. Pool Security

The 420,000 WBIZ staking pool is the single most valuable key in the system. If it is stolen or lost, the staking program dies with it. It is protected accordingly.

6.1 Tiered custody

The pool never sits in one online wallet:

- Cold vault (~99%+ of the pool). A 2-of-3 P2WSH native-segwit multisig vault. Keys are generated at a guided key ceremony on offline devices; the vault never touches the internet. Its sole job is periodic refills of the hot float via PSBTs signed offline by two participants.
- Hot float (~1% of the pool; 1,000–2,000 WBIZ in year one). A few months of payouts held on a dedicated payout server. If that server were fully compromised, the loss is capped at the float — the vault's 99% is untouched.

6.2 Policy-constrained payout signer

The payout server does not hold "a key and hope." Its payout pipeline refuses to sign unless a rewards ledger satisfies every policy rule:

1. Schedule — the ledger period must match the expected payout period.
2. Whitelist — every destination must be a valid chain address registered in the lock-vault registry (human-reviewed each period).

3. Per-staker cap — each payout within (dust, cap] (default cap: 50 WBIZ).
4. Period budget — total within the period budget (default: 350 WBIZ per month in year one).
5. Uniqueness — no destination paid twice in one ledger.
6. Fee cap — transaction fee within limits.

Even with a fully compromised rewards calculator, one period can move at most the budget, and only to registered stakers. Every payout runs through a dry-run review before signing.

6.3 Monitoring and transparency

- A watchdog snapshots the UTXO set of all pool addresses and diffs it continuously. Any movement not matching a logged, expected payout raises an immediate alert.
- Pool addresses are public, with a public dashboard of pool balance and payouts. Sunlight is the best watcher.

Honest framing: nothing is unhackable. The design forces an attacker to break several independent things at once — and makes any attempt instantly visible. Accepted residual risk (such as a coordinated compromise of two of three key holders) is documented in the full security plan.

7. Privacy Roadmap

Wikibusiness will offer optional privacy, Zcash-style: every transaction sender chooses, per transaction, whether it is transparent (Bitcoin-like) or shielded (private). Monero-style mandatory privacy (ring signatures) is excluded — it cannot be bolted onto a Bitcoin transaction model; it would require replacing the signature layer, i.e. building a different coin.

7.1 Technical approach

- Follow the Zcash recipe: keep transparent Bitcoin-style transactions working and add an optional shielded pool beside them, with per-pool value-balance ("turnstile") accounting so total supply stays bounded and auditable across pools even while amounts inside the shielded pool are hidden.
- Use the modern Halo 2 proving system (Orchard-style), which requires no trusted setup ceremony — eliminating the most operationally painful and trust-sensitive part of shielded protocols.
- Reuse audited cryptography, never reinvent it: integrate Zcash's audited Rust crates (`orchard`, `halo2_proofs`, and related libraries) via FFI, with a new thin integration layer for consensus, mempool, wallet, and RPC. Zcash's old C++ codebase (forked from Bitcoin Core 0.11.2, a decade of divergence) will not be ported.
- Transparent addresses remain the default everywhere (wallets, explorer, exchange documentation); shielding is an explicit user opt-in, with viewing-key export for voluntary disclosure.

7.2 Honest scope

This is a 12–18 month specialist program (applied cryptographers, Core consensus engineers, wallet engineers), on the order of low-seven-figures USD — a protocol R&D program, not a feature ticket. Independent audits of both the circuits and the implementation are mandatory before mainnet activation. The cautionary tale: in June 2026 a critical soundness bug was found in Zcash's own Orchard circuit — live for four years, missed by multiple professional audits, requiring

an emergency hard fork. It happened to the most experienced shielded-protocol team in the world, on audited code. That is why reuse of audited crates, turnstile accounting, and real audit time are non-negotiable.

7.3 Exchange considerations

Optional privacy is materially more listable than mandatory privacy: Coinbase lists ZEC, OKX relisted ZEC in November 2025, and in January 2026 the SEC closed a ~2-year investigation into the Zcash Foundation with no enforcement action. But "every exchange" still narrows to exchanges willing to list a privacy-capable coin, and exchanges that list such coins overwhelmingly support transparent deposits only. The product posture above — transparent by default, shielding as opt-in — is what keeps the transparent listing path clean.

8. Mining

Mining is public and permissionless from genesis. Anyone with the software can mine WBIZ under Bitcoin's rules — SHA-256d proof-of-work, difficulty retargeting every 2,016 blocks, block rewards per the halving schedule.

At mainnet launch the founder bootstraps the network: the first blocks are mined to a founder wallet whose keys are generated at launch and handed over securely for import into the desktop wallet. From there the network is open — once public, anyone can point hash power at the chain and earn their own block rewards, exactly as in Bitcoin's early days, when difficulty starts low and adjusts upward as miners join.

A mining guide is published with the release software so anyone can participate. A public mining pool is a possible later phase. There is no premine for miners beyond the staking pool described in §4–§6, and no portion of block rewards is redirected anywhere.

9. Wallets & Ecosystem

- Desktop — Wikibusiness Core. The reference wallet is the desktop GUI (`wikibusiness-qt`) for Windows, macOS, and Linux, alongside the full-node daemon for power users. Releases are PGP-signed.
- Mobile. A mobile wallet (balances, send/receive) follows after mainnet launch, built on an Electrum-server backend for the chain, with in-app staking UI added next — lock for years, rewards land automatically.
- Block explorer. A public explorer ships with the network so anyone can verify supply, blocks, transactions, and pool payouts independently.
- Trading. The founder's own trading exchange is a separate project; the mobile app will plug into it for in-app trading once live.
- Community. A community/holder view (holders, activity, leaderboard) completes the ecosystem.

Each phase builds on the live chain — nothing throwaway, everything integrated.

10. Exchange Strategy

Stated plainly: exchange listings cannot be created in code. A listing is a business process — an application to the exchange, listing fees where charged, demonstrated liquidity and trading

volume, and compliance review (including, where relevant, the considerations in §7.3 for a privacy-capable coin).

What the project does to be listable: ship correct, audited, PGP-signed software; run a stable public network with explorers and documentation; keep the transparent transaction path clean and default; and never promise a listing that has not been granted. Any claim about a specific exchange listing will only be made after it is confirmed by the exchange itself.

11. Roadmap

Phases run in order; each begins when its foundation is ready:

1. Chain launch — final genesis proof-of-work baked in, final binaries rebuilt, 1–2 always-on public seed nodes, PGP-signed desktop releases (Windows, macOS, Linux), founder wallet and pool key ceremonies, mining guide.
2. Explorer + app backend — public block explorer and the Electrum-server infrastructure the mobile app needs.
3. Mobile wallet — see coins, send/receive on iOS and Android.
4. In-app staking — lock-for-years UI with automatic pro-rata rewards from the pool.
5. Own exchange — the separate trading venue, then in-app trading.
6. Community features — holder/leaderboard views and social layers.

The optional shielded-privacy program (§7) runs as a parallel specialist track; its activation point (genesis vs. later network upgrade) is a founder decision with the trade-offs described in §7.2.

12. Risks & Disclaimers

- Not financial advice. This document is a technical description, not investment advice, and not an offer to sell anything. WBIZ has no established market or price.
- No guaranteed returns or listings. Staking rewards depend on participation and the published pro-rata rules; they are not interest and not guaranteed. Exchange listings are not guaranteed (§10).
- Regulatory uncertainty. Digital-asset regulation differs by jurisdiction and is evolving; privacy-capable coins face additional scrutiny and delisting risk in some venues (§7.3).
- Software risk. This is new software. Despite testing, cross-checked implementations, and planned audits, bugs are possible. Never hold more value in any wallet — including timelocked vaults — than you can afford to lose, and keep secure backups of every seed and key.
- Key loss. Lost keys mean lost coins; there is no recovery mechanism and no administrator who can reverse transactions.
- Network risk. Early in its life the network's hashrate is small; difficulty adjusts with participation, as in Bitcoin.

Wikibusiness (WBIZ) — Whitepaper v1.0, September 2026. This is a living document; substantive changes will be versioned.