XEB Token

Technical Whitepaper — August 2026

Contents

1. Architecture

XEB is an ERC-20 token designed for deployment on Base mainnet, inheriting OpenZeppelin's upgradeable contracts. The protocol uses a proxy pattern for future upgrades while maintaining immutability of core token logic. Contracts are written and tested — mainnet deployment is pending.

- Chain: Base (Layer-2 Ethereum)
- Standard: ERC-20 with EIP-2612 permits
- Upgradability: UUPS proxy pattern
- Block time: ~2 seconds
- Gas: Sub-cent transactions

2. Tokenomics

The fixed supply of 100,000,000 $XEB is allocated across five buckets designed to balance liquidity, community incentives, and long-term sustainability. All allocations vest according to on-chain schedules.

Bucket	Amount	Vesting
Staking Rewards	35M (35%)	4 years
Airdrop Pool	20M (20%)	Monthly
Liquidity	20M (20%)	6 months
Community	15M (15%)	3 years
Team	10M (10%)	12mo cliff, 36mo vest

3. Airdrop Mechanics

Monthly NFT art airdrops use an on-chain random selection process seeded from block data. Eligibility requires a minimum balance of 10,000 $XEB at the snapshot block. Staked positions receive multiplier weighting. A future upgrade path to Chainlink VRF is planned for stronger randomness guarantees as the protocol matures.

- Frequency: Monthly (1st of each month)
- Selection: On-chain block-seeded random (VRF upgrade planned)
- Min. balance: 10,000 $XEB
- Staking boost: 1.5x to 3x multiplier

- Recipients per drop: 50 to 200 random holders

4. Security

XEB is built on OpenZeppelin's audited upgradeable contract libraries and covered by an internal test suite of 49 tests. No third-party security audit has been completed yet — this is an early-stage protocol and should be treated accordingly. Contract upgrade authority will transition from a single deployer key to a multi-signature wallet as the protocol matures.

- Base contracts: OpenZeppelin (audited library)
- Test coverage: Internal Foundry test suite (49 tests)
- Third-party audit: Not yet completed
- Upgrade authority: Single key → multi-sig (planned)

5. Staking

Four staking tiers offer escalating APY rewards in exchange for lock-up commitment. Staked $XEB accrues rewards continuously and qualifies for airdrop multiplier weighting. Early unstaking incurs a 10% penalty redirected to the airdrop pool.

Tier	Lock-up	APY	Airdrop Boost
Flexible	None	8%	1.0x
30-day	30 days	15%	1.5x
90-day	90 days	25%	2x
365-day	365 days	35%	3x

6. Governance

On-chain governance allows $XEB holders to propose and vote on protocol parameters. Voting power is proportional to token holdings via ERC20Votes snapshot delegation.

- Proposal threshold: 1,000,000 $XEB
- Quorum: 10,000,000 $XEB
- Voting period: 72 hours
- Execution: Timelocked 48 hours
- Delegation: Supported via ERC20Votes

7. Browser Mining

XEB introduces browser-based proof-of-work mining, allowing anyone to mine $XEB tokens for free directly from their web browser. No special hardware, no electricity cost — just a Web Worker computing keccak256 hashes until a valid proof is found.

How It Works

The mining system uses a lightweight proof-of-work algorithm based on keccak256. Users run a Web Worker in their browser that hashes candidate nonces until finding one that produces a hash with the required number of leading zero bits. The hash preimage is:

```
keccak256(abi.encodePacked(chainId, contractAddress, miner, currentEpoch, epochChallenge, nonce))
```

Once a valid nonce is found, the user submits it on-chain via the XEBMining contract. The contract verifies the proof and transfers 10 $XEB to the miner. No new tokens are minted — rewards come from a pre-funded 2,000,000 $XEB mining reserve.

Mining Parameters

Parameter	Value
Reward per proof	10 $XEB
Daily wallet cap	30 $XEB (3 proofs)
Global daily cap	1,370 $XEB
Claim cooldown	10 minutes
Difficulty	22 bits (adjustable 18-28)
Mining reserve	2,000,000 $XEB
Epoch	24 hours (block.timestamp / 1 days)
Challenge	keccak256(blockhash(block.number-1), epochId)
Replay prevention	Per-hash usedProofs mapping

Difficulty Adjustment

The mining difficulty (number of leading zero bits required) is adjustable by the contract owner within the range of 18 to 28 bits. At 22 bits (default), miners must compute approximately 4,194,304 hashes on average to find a valid proof. At typical browser hash rates of 50,000-200,000 H/s, a proof can be found every 20-80 seconds.

Value Protection

The mining system is designed to distribute tokens without compromising value:

- Fixed supply: No minting — rewards come from the pre-funded reserve
- Controlled emission: Maximum 1,370 $XEB/day globally (0.00137% of supply)
- Per-wallet limits: 30 $XEB/day per wallet prevents farming
- Cooldown: 10-minute wait between claims
- Difficulty: Adjustable to control mining rate as network grows
- Finite reserve: 2M $XEB reserve lasts ~4 years at max emission

8. Smart Contract Source

The full source code for all XEB contracts is available at the XEB Token project. Contracts include XEBBToken.sol (ERC-20), XEBBStaking.sol (4-tier staking), XEBBArtNFT.sol (12 optical illusion types), XEBBAirdrop.sol (monthly drops), XEBBGovernance.sol (on-chain governance), and XEBBMining.sol (browser PoW mining). All contracts are written in Solidity 0.8.26, tested with Foundry (49/49 tests passing), and use OpenZeppelin libraries.