EliteXcoin

A 100% Proof-of-Stake Cryptocurrency

EXC · Whitepaper v1.0 · August 2026

Abstract

EliteXcoin (EXC) is a cryptocurrency secured entirely by Proof-of-Stake (PoS) consensus. Rather than relying on energy-intensive mining, network security and new coin issuance are both handled by holders who keep coins staked in their own non-custodial wallet. Stakers earn a transparent, consensus-enforced reward of 1.72% of their staked balance per month, computed deterministically from coin-age rather than a flat block subsidy. This document describes the consensus rules, reward mathematics, network parameters, and wallet architecture that make up the EliteXcoin protocol.

Introduction

Proof-of-Work blockchains secure themselves by having miners compete to solve a computational puzzle, consuming large amounts of electricity in the process. Proof-of-Stake systems replace that competition with economic weight: the right to produce the next block, and the reward for doing so, is proportional to how many coins a participant has staked and for how long. EliteXcoin builds on the PoS 3.0 design lineage pioneered by early proof-of-stake coins, with a coin-age-weighted reward formula chosen specifically to give every staker - regardless of when they started staking - the same effective 1.72% monthly rate.

Consensus Mechanism

EliteXcoin blocks are produced approximately every 64 seconds. A short Proof-of-Work bootstrap window (blocks 2 through 150) exists purely to let the genesis allocation and early participants reach coin maturity, since a brand-new chain has no existing stake to bootstrap from; from block 151 onward, 100% of blocks are produced via Proof-of-Stake. A stake input must be at least 8 hours old (the "minimum stake age") and confirmed at least 100 times ("coin maturity") before it is eligible to participate.

Staking Reward Formula

The reward for a stake is computed directly from the value being staked and how long it has been held, using 256-bit integer arithmetic (no floating point) to keep the result fully deterministic across every node on the network:

```
reward = floor( value x time_held x 172 / (2,629,800 x 10,000) )
```

Here, value is the staked amount, time_held is the coin-age in seconds, 2,629,800 is the number of seconds in an average month (365.25 days / 12), and 172 / 10,000 represents the 1.72% rate. Because the formula scales linearly with both value and time, a balance staked continuously for one average month earns exactly 1.72% of its value - regardless of when the staking started. Compounded simply (without re-staking gains), this works out to approximately 20.64% per year.

Why coin-age instead of a flat block subsidy?

A flat per-block subsidy pays the same reward to a stake regardless of its size or how long it has been held, which unfairly favors large, recently-moved balances that happen to find a block. Weighting by coin-age ties the reward directly to genuine economic commitment - the amount held, and for how long - which is the actual quantity the network wants to reward for securing itself.

Tokenomics

Ticker	EXC
Consensus	100% Proof-of-Stake (PoW bootstrap: blocks 2-150 only)
Genesis allocation	14,000,000,000 EXC, minted transparently in block 1
Ongoing emission	Exclusively via the public staking reward formula above
Staking reward	1.72% of staked value per month
Simple annual yield	approximately 20.64% per year
Minimum stake age	8 hours
Coin maturity	100 confirmations
Block time	64 seconds
Max supply	Uncapped (ongoing PoS emission after the one-time genesis allocation)

The 14 billion EXC genesis allocation is minted once, in block 1, and is fully visible on-chain to anyone running a node - it is not a hidden or ongoing emission. It exists to fund development, exchange listings, and ecosystem growth. Every EXC minted after block 1 comes exclusively from the staking reward formula described above; there is no additional mining subsidy or discretionary issuance.

Network Parameters

Address prefix	Legacy addresses start with "E"
Bech32 HRP	exc (mainnet), texc (testnet), excrt (regtest)
Minimum relay fee	0.0001 EXC / kB
Networks	Mainnet, Testnet, Signet, Regtest

Wallets

Desktop wallet

A full-node Qt wallet is available for Windows, macOS, and Linux, with staking, coin control, an address book, wallet encryption, and QR code support built in.

Web wallet

An installable Progressive Web App serves as the official mobile wallet - no app store required. Keys are generated and BIP39/BIP32-derived entirely on the user's device, then AES-256-GCM encrypted with a password-derived key (PBKDF2, 600,000 iterations) before being stored locally. Where supported, biometric or PIN unlock is available via WebAuthn's PRF extension, which derives the wallet's unlock key directly from the device's authenticator - no weaker fallback is offered if PRF isn't available. The backend server only ever relays already-signed transactions and answers balance/UTXO queries; it never receives a private key or mnemonic.

Security Considerations

- Non-custodial by design: private keys never leave the device that generated them, in either wallet.
- The genesis allocation is transparent and verifiable on-chain, not hidden or claimed as decentralized.
- All consensus code, both wallets, and this website are open source and publicly auditable.
- Reward math uses fixed-point 256-bit integer arithmetic - no floating-point rounding in consensus code.

Disclaimer

This document is a technical description of the EliteXcoin protocol, not an offer or solicitation of securities, and not financial, investment, or legal advice. Cryptocurrency involves risk, including the possible loss of value. Readers should conduct their own research and consult independent advisors before making any financial decisions.