FALQBIT

WHITEPAPER · VERSION 1.1

The token only quantum-safe accounts can hold.

FALQBIT is an Algorand Standard Asset that can only be held by accounts secured with Falcon-1024, a post-quantum signature scheme. The rule is enforced on-chain by an immutable contract.

4 November 2026 · falqbit.com · ASA ID 3760920399

1. The problem
2. The solution
3. How it works
4. Token facts
5. Supply and allocation
6. Rewards
7. Joining and trading
8. Security and limits
9. Roadmap and vision
10. Risks and legal notice

01 The problem

Almost every crypto wallet today is protected by elliptic-curve signatures such as Ed25519 or ECDSA. They are secure against today's computers. A large enough quantum computer running Shor's algorithm could derive a private key from a public key, and then sign transactions as the owner.

Nobody knows when such a machine will exist. But public keys stay on-chain forever, and standards bodies are already moving: NIST selected Falcon as a post-quantum signature standard, and governments have set migration deadlines for critical systems around 2030. Assets that cannot move to post-quantum keys will be the easiest to attack.

Algorand added Falcon-1024 accounts to its MainNet, and wallets such as Pera now let anyone create a **Quantum Account**. What was missing was a reason to use one.

02 The solution

FALQBIT is the first token that **only post-quantum accounts can hold**. A classic account cannot receive it, hold it or trade it: the network itself refuses the transfer.

- **For users**, it is a simple, practical reason to move to a Quantum Account, with rewards for doing it.
- **For Algorand**, it is a live, public showcase of post-quantum accounts being used every day.
- **For everyone**, the rules are code: no admin, no clawback, no way to change them later.

03 How it works

Frozen by default

FALQBIT was created with *default frozen* set. Every account that adds the token starts locked. The freeze role does not belong to a person: it belongs to the **gate contract** (application 3760919863). The token has no manager and no clawback, so these settings can never change.

Proving a Falcon key

An account is unlocked only if it proves that a Falcon-1024 key signs for it. Algorand derives a Quantum Account's address from its Falcon public key:

```
address = SHA512-256("PQA" || "f1" || salt || public_key)
```

The user sends the public key and salt to the gate. The contract recomputes the address, checks that it matches the account (or the account's current signer, if it was rekeyed), and then unfreezes the holding. The unlock page at falqbit.com/unlock does all of this in one approval in Pera Wallet. A small deposit (about 0.03 ALGO) pays for the record the contract keeps.

Going back to classic gets you locked again

If an unlocked account later rekeys to a classic key, **anyone** can call the contract's relock method. The holding is frozen again and the caller receives the account's deposit as a reward. The tokens stay with their owner and unlock again once the account returns to a Falcon key.

Pools and contracts

Pools and other smart contracts have no signing key. They can hold FALQBIT only if the program that controls them is on the gate's approved list. **Tinyman v2** is the only approved program, so any Tinyman v2 pool can hold FALQBIT. The approver role has been **renounced**: the list can never grow or shrink.

04 Token facts

ITEM	VALUE
Name / unit	FALQBIT / FALQBIT
Network	Algorand MainNet
Asset ID	`3760920399`
Total supply	10,000,000,000 (fixed, no minting)
Decimals	6
Manager / clawback	None / None
Freeze role	Gate contract, application `3760919863` (immutable)
Main pool	Tinyman v2 FALQBIT/ALGO, pool token `3760920578`
Launch	2 November 2026
Compiled gate (SHA-256)	`f14801163a468bc7e990531cd866dd21fe69a6f5d0b7bf0bd71cd8109e4f95a9`

05 Supply and allocation

The whole supply was minted once, at launch. Every allocation sits in a public account, so anyone can check the balances live on the supply section of the site or on any Algorand explorer.



ALLOCATION	SHARE	AMOUNT	PURPOSE
Liquidity pool	63%	6.3B	Paired with ALGO in the Tinyman pool: 5.5B at launch, more added since. Tokens bought by users leave the pool. Live amounts are on the site's supply dashboard.
Hold-to-earn	25%	2.5B	Monthly rewards for holders
Welcome drop	2%	200M	1M for each of the first 200 accounts. Accounts 201–1,000 are paid from the project reserve (see Rewards).
Project reserve	5%	500M	Welcome rounds 2–4 (270M), liquidity, contests and partners
Team	5%	500M	Held in a quantum account

Public accounts

ACCOUNT	ADDRESS
Project (creator, reserve, liquidity)	`OCAF6EHCGLZ3SJDE54SL2TBKNDLIQAUQDM6CAFQAFZ7LNLERA4SBY73YIU`
Rewards (hold-to-earn + welcome)	`V4J46SMHHEJHXRKXHA6MJKWFJMZIXQSMBPU5UC7W6BRUEYYB3SF7CPTC2Q`
Team	`XMKDQFY55TLREPRIUG3WLWPUPKFW33WPV7GZF6U22EWOXYWHLKTPGBDT7Q`
Tinyman v2 pool	`CEQH5WNK3VFUVGZ6WET7GO2JLZVYY7BDPCN74LGWEUWC5WCMPYU7M7VCIA`

All project accounts are Falcon-1024 Quantum Accounts. There was no presale, no private sale and no token sale other than the public Tinyman pool.

06 Rewards

Welcome drop

- A free drop for the first **1,000** quantum accounts that unlock. No purchase needed. The earlier you join, the more you get:

    - Accounts 1–200: **1,000,000 FALQBIT**
    - 201–600: **500,000**
    - 601–800: **250,000**
    - 801–1,000: **100,000**

  Accounts 201–1,000 (270M FALQBIT in total) are funded from the project reserve.
- One per person. The account must hold at least **2 ALGO** on payout day; accounts below that are skipped and can receive it in a later round.
- Paid in rounds from the Rewards account, with the note `FALQBIT welcome`. Accounts that look like duplicates of the same person may be excluded.

Hold-to-earn

- **0.5% a month** of each wallet's **lowest balance since the 1st** of the month, for wallets holding at least 1,000,000 FALQBIT.
- Paid on the **25th** of every month, with the note `FALQBIT hold YYYY-MM`.
- Maximum **500,000 FALQBIT** per wallet per month.
- The monthly pool is **15,000,000 FALQBIT**, shared by all holders. If everyone's 0.5% adds up to more, every payout shrinks in the same proportion.
- Launch month (November 2026): **1%** of the balance on the 25th, with the same cap and pool.
- No staking and nothing to claim. Tokens never leave the holder's wallet. Project accounts and pools are excluded.

YOU HOLD	YOU GET PER MONTH
1,000,000	5,000
10,000,000	50,000
100,000,000 or more	500,000 (max)

How long it lasts. The Hold-to-earn allocation is 2.5B FALQBIT. Even if the full 15M pool is paid every month, it lasts 166 months, nearly 14 years. Months that pay less make it last longer.

> **Important:** rewards are sent by the project from the public Rewards account. They are not enforced by a smart contract. Every payment is visible on-chain with its note, so anyone can check that the rules above were followed.

07 Joining and trading

1. **Create a Quantum Account** in Pera Wallet (Add account → Add Quantum Account), or rekey an existing account to a Falcon-1024 key.
2. **Unlock** it at falqbit.com/unlock. Adding the token and unlocking happen in one step.
3. **Buy, sell or hold** on falqbit.com/trade, in the FALQBIT app or on Tinyman. All three use the same Tinyman pool. Price and charts are on Vestige.
4. **Pay and get paid** with QR codes in the app. Every payment is approved in Pera; the app never holds keys.

Fees. A Falcon-1024 signature is larger than a classic one, so each transaction costs about three minimum fees, around 0.003 ALGO. Tinyman charges its usual 0.3% swap fee, which goes to liquidity providers.

From FALQBIT to local currency. Today: swap FALQBIT to ALGO on Tinyman, then ALGO to USDC. On falqbit.com/trade this takes one approval. Then send the USDC (or ALGO) to a regulated exchange that supports Algorand, sell it for your local currency (EUR, USD and others) and withdraw to your bank. The project itself never converts FALQBIT to fiat money.

Exchanges. Pools on DEXs other than Tinyman v2 cannot hold FALQBIT. Centralized exchanges can list it by holding it in quantum accounts and unlocking them like any user.

08 Security and limits

What the code guarantees

- **No clawback.** Nobody can take tokens out of an account, not even the creator.
- **No admin key.** The freeze role is a public contract.
- **Immutable.** The gate cannot be updated or deleted, the token has no manager, and the approver role is renounced.
- **Open source.** The gate is under 200 lines of Algorand Python, published with its compiled program and ABI. An independent automated review found no way for a classic account to unlock. There has been **no professional audit** yet.

What FALQBIT does not solve

- **Consensus.** Algorand's accounts can be post-quantum, but block voting still uses classical keys. Post-quantum consensus is on Algorand's own roadmap.
- **Relocking is after the fact.** An account that rekeys back to classic stays unlocked until someone calls relock.

- **Code-controlled addresses.** Pool and application addresses are hashes, not keys. Their long-term quantum safety depends on Algorand's protocol, not on this contract.
- **One DEX family.** The approved list is final: only Tinyman v2 pools can hold FALQBIT.

09 Roadmap and vision

FALQBIT starts as a token. The goal is to become a simple way to **use** post-quantum money every day. The phases below are plans, not promises, and have no fixed dates.

PHASE	GOAL
Done	TestNet rehearsal, MainNet launch, gate contract, Tinyman pool, unlock page, rewards live, deeper liquidity, this whitepaper, **verified ASA on Pera** (4 November 2026), **swaps with ALGO or USDC on falqbit.com/trade**, **FALQBIT app** (wallet, swaps and QR payments, installed from the browser).
Now	Logo on Tinyman and Vestige, listing in Algorand project directories, official community channels on Telegram.
Next	**Shop mode** in the app: prices shown in local currency, payments by QR, and shops able to receive USDC.
Later	First shops and services accepting FALQBIT. Listings on trackers such as CoinGecko, and more wallets and explorers.
Future	**Spend anywhere**: swap FALQBIT to USDC on falqbit.com, then use a crypto card from any **licensed** provider that accepts USDC. No partnership is needed, and FALQBIT never acts as a payment institution itself.

10 Risks and legal notice

FALQBIT is not an investment product. It gives no right to profits, dividends, interest, governance or redemption, and nothing in this document is financial advice or a promise of returns.

- **Price risk.** The price is set only by the market and can fall to zero. Liquidity is small and prices can move sharply.
- **Smart contract risk.** The gate is immutable and has not been professionally audited. A bug could not be fixed.
- **Reward risk.** Rewards depend on the project continuing to send them. They can shrink when many people hold.
- **Key risk.** Losing a recovery phrase means losing the tokens. Nobody can recover them.
- **Technology risk.** Post-quantum cryptography and Algorand's Falcon accounts are new. Wallet or protocol changes could affect how FALQBIT works.
- **Regulatory risk.** Crypto-asset rules, including the EU's MiCA regulation, keep changing and could affect how FALQBIT can be offered, listed or used in some countries.

Only acquire FALQBIT with money you can afford to lose. Always check the official asset ID **3760920399**: anyone can create a token with the same name.
