

VAULT PROGRAM · SOLANA MAINNET

Security Review

The BTCgold vesting vault, live and immutable since November 21, 2026

- **No way was found to take tokens out early, to pay more than the schedule, or to pay anyone other than the two fixed payout wallets.**

7,810	26,036	2126
ATTACKS TRIED ALL REFUSED	RANDOM TEST ACTIONS CHECKED STEP BY STEP	FULL SCHEDULE REPLAYED ON THE REAL VAULT

Internal review, not a third-party firm audit. Prepared for the BTCgold team with two AI review agents working separately: Claude Code (Anthropic) and OpenAI Codex. Every check is recorded so anyone can repeat it.

Program CGHrTU4xx1AZQkJFmXhVzRXCNrJGhYLJ7z5bwrmnx7Mk

Code sha256 b04c547c17ca34cfabd4f088aaafb4b49d40aac7679865b7ce01aabe1c41d178

1. Summary

The BTCgold vault is a Solana program that holds 15,744 BTCgold and releases them every ten minutes on a halving schedule until 2126, half to each of two fixed payout wallets. Its code can no longer be changed. This review checked the live program and its state on mainnet, rebuilt the code from source, read it line by line, and attacked it with thousands of automated tests on the exact code that runs on Solana.

Result: no way was found to steal from the vault, to pay early, to pay more than the schedule, or to pay anyone other than the two fixed wallets. Two findings are rated Medium. Both concern how the two payout wallets and the treasury wallets are kept, not a flaw that outsiders can use.

0	0	2	2	5
CRITICAL	HIGH*	MEDIUM	LOW	INFO

* OpenAI Codex rated BTCG-01 High because its block can be permanent. This report rates it Medium because only a payout wallet's own key can cause it and nobody gains tokens from it (page 4).

What holders and partners can rely on

Question	Answer, as verified on November 22, 2026
Can anyone take tokens out of the vault?	**No.** Only the payout instruction moves tokens, and only into the standard token accounts of the two fixed wallets.
Can the team take tokens out early?	**No.** There is no admin, withdraw or close instruction, and the code cannot be changed.
Can more BTCgold be created?	**No.** The mint authority is revoked. Supply is exactly 21,000.
Can anyone freeze wallets?	**No.** The freeze authority is revoked.
Can the program be changed?	**No.** Its upgrade authority is none. The code on chain matches the reviewed source byte for byte.
Does it depend on the website or the bot?	**No.** Anyone can send a payout; it can only pay the two fixed wallets.
What could go wrong?	A payout wallet could stop all payouts with its own key (BTCG-01). The 5,256 treasury tokens depend on how their wallet keys are kept (BTCG-02).

MAIN RECOMMENDATION

Keep the two payout wallets on hardware wallets, and never change the owner of, add a delegate to, or close their BTCgold token accounts. Move the treasury into a multisig and publish its addresses and rules.

2. Scope

Item	Value
Program	`CGHrTU4xx1AZQkJFmXhVzRXCNrJGhYLJ7z5bwrmnx7Mk` Upgrade authority: none (finalized 2026-11-21 18:57:43 UTC)
Source	Git tag `vault-review-2`, commit `5caba734b295027de4895e4d518876df2965a19f` Program: 338 lines of Rust. Schedule math: 193 lines
Deployed code	sha256 `b04c547c17ca34cfabd4f088aaafb4b49d40aac7679865b7ce01aabe1c41d178` (252,680 bytes)
Libraries	Anchor 0.31.3, SPL Token 7.0.0, SPL Associated Token Account 6.0.0
Token (mint)	`C3iRkiV2vpVk6jCEF4pgJeSpiqunnuUJ8s2hVjfvqKyU`
Vault record **Vault token account**	`3SMf3H9htj6PDKJEPRDpGcjgLeC2udpWQ8EcKxEW5EAP` `C17hNzFYuio3TLMXj3jHamFyHEffibXZ21eZ3KhH24RQ`
Payout wallet A **Payout wallet B**	`F1hWkNERZhXVsxJbJ4CpqHu1oPZ3VqzSqEKGSJ6YMiVC` `7FHzee7PAn2GMhBo5RwEQEtmvJ8hwMC1tdWrbt3bBr9f`
Mainnet snapshot	Slot 472,525,321, November 22, 2026
Also reviewed	The automatic payout bot, the website btc-gold.com, and where all 21,000 tokens are held

3. Method

- **On-chain checks:** every program, token, vault and payout account read from mainnet, plus their full history.
- **Rebuild:** the source tag built fresh in a separate folder and compared with the code on chain.
- **Code review:** every line, including the checks the Anchor framework actually generates.
- **Attack testing:** the exact deployed bytes run in a local Solana test machine (LiteSVM) with random attacks, edge cases and a replay of the real accounts to 2126.
- **Second reviewer:** OpenAI Codex, read-only, without being told the first reviewer's findings.
- **Libraries:** all 271 locked libraries checked against the public OSV advisory database.

Severity scale

CRITICAL	Anyone can steal or permanently lock funds.
HIGH	An outsider can cause loss or a lock under realistic conditions.
MEDIUM	Serious impact, but only through a trusted party or a stolen key.
LOW	Limited or temporary impact that is easy to undo.
INFO	No direct risk. Good to know or good practice.

4. Findings

The program is immutable, so no finding can be fixed in code. Where action is possible, it is about how wallets, the treasury and the website are run.

ID	Severity	Finding	Action
BTCG-01	MEDIUM	Either payout wallet can stop payouts to both wallets, possibly for good	Wallet rules (cannot be fixed in code)
BTCG-02	MEDIUM	Payout wallets and the 10 treasury wallets are single-key wallets	Hardware wallets; treasury multisig
BTCG-03	LOW	A delegate on, or a closed, payout token account pauses payouts	Easy to undo; nothing is lost
BTCG-04	LOW	Release times follow Solana's on-chain clock	By design
BTCG-05	INFO	Tokens sent straight to the vault stay there forever	By design
BTCG-06	INFO	Lookalike tokens can create their own vault from the same program	Always check the mint address
BTCG-07	INFO	5 library advisories, none in code the vault uses	None
BTCG-08	INFO	Website: old funding page still online; no anti-framing header	FIXED Nov 22, 2026
BTCG-09	INFO	The payout bot is a convenience, not a dependency	None

BTCG-01 Either payout wallet can stop payouts to both MEDIUM

HOW Each payout pays both wallets in one step. For each wallet, the program checks that the token account at the wallet's standard address is still owned by that wallet. The classic SPL Token program lets an owner hand a token account, including the standard one, to another address. If A or B does that, every payout fails and **neither** wallet is paid. The address is taken, so the account cannot be created again.

RECOVERY If the new owner hands the account back, everything owed is paid in the next payout. If it was handed to an address nobody controls, payouts stop for good and the rest of the vault stays locked forever. The tokens do not go to anyone.

WHO CAN Only payout wallet A or B, or someone who holds its private key. No outsider can.

EVIDENCE Confirmed in the generated Anchor check (anchor-syn 0.31.3) and in SPL Token's `SetAuthority`. Two dedicated tests reproduce the block and the recovery. OpenAI Codex found the same issue on its own.

RATING Medium in this report; High in Codex's review. The impact can be permanent, but only a payout wallet's own key can trigger it.

DO Payout wallets A and B must never transfer ownership of their BTCgold token account, never approve a delegate on it, and never close it. Keep both on hardware wallets with offline seed backups.

BTCG-02 Single-key payout and treasury wallets MEDIUM

WHAT A and B are fixed in the vault until 2126. Whoever controls one of their keys controls that wallet's payouts and can trigger BTCG-01. If a key is lost, payouts still arrive, but nobody can spend them. The 5,256 treasury tokens sit in 10 ordinary wallets of 525.6 each; whoever holds each key can move them at any time, and no program limits that.

DO Hardware wallets for A and B. Move the treasury into a multisig (for example Squads). Publish the treasury addresses and the rules for using them.

BTCG-03 Temporary pauses from a delegate or a closed account LOW

WHAT If A or B approves a delegate on its BTCgold account, payouts fail until the delegate is revoked. If A or B closes its account (possible only with a zero balance), payouts fail until the account is created again. Anyone can recreate it for about 0.002 SOL. The payout bot does not recreate accounts, so payouts pause until someone does. They then catch up in full.

EVIDENCE Covered by the random tests and a dedicated test: nothing is lost in either case.

BTCG-04 Releases follow Solana's on-chain clock LOW

WHAT Releases count ten-minute steps of Solana network time, not wall-clock time, so they can come slightly early or late if the network clock drifts. If the clock ever moved backwards, a payout attempt fails and nothing moves. At the end time, 2126-09-17 03:06:59 UTC, everything left becomes payable.

EVIDENCE Tested with the clock moved backwards to many earlier times, at exact ten-minute and halving edges, and at the largest possible time value. Every case paid exactly the schedule or refused cleanly.

BTCG-05 Tokens sent straight to the vault stay there INFO

WHAT Anyone can send BTCgold directly to the vault token account. It does not change the schedule, and after 2126 it stays there forever, because the vault has no way to send it out.

EVIDENCE Tested with 1,499 random deposits: payouts were unchanged, and only the deposits remained at the end.

NOTE ON OUTSIDERS

No finding lets an outsider block, redirect or speed up payouts. Every attempt by a third party, including closing, taking over or adding a delegate to the vault's or a payout wallet's token account, was refused in testing.

BTCG-06 Lookalike tokens can use the same vault program INFO

WHAT The funding instruction works for any token with 21,000 supply, 9 decimals and no mint or freeze authority. Someone could create a fake "BTCgold" with a real-looking vault from this same program. It cannot touch the real vault (tested), but it could confuse buyers.

DO Always state the real token address: `C3iRkiV2vpVk6jCEF4pgJeSpiqunnuUJ8s2hVjfvqKyU`.

BTCG-07 Library advisories INFO

WHAT All 271 locked libraries were checked against the OSV advisory database. Five advisories matched four libraries. None affects code the vault uses:

Library	Advisory	Why it does not matter
bincode 1.3.3	No longer maintained	Not used by the vault
libsecp256k1 0.6.0	No longer maintained	The vault uses no secp256k1
rand 0.7.3 (2 records)	Unsound with a custom logger	The vault uses no randomness
borsh 0.10.4	Unsound for zero-sized types	The vault stores no such types

Codex also checked the two 2026 Anchor advisories; they concern other versions or features and do not apply to Anchor 0.31.3 as used here.

BTCG-08 Website hardening INFO FIXED

WHAT At the time of review, the one-time funding page `btc-gold.com/fund/` was still online. Any new funding attempt failed because the vault exists, but a page that asks people to connect a wallet should not stay up after its job is done. The site also sent no header that stops other sites from showing it inside a frame.

FIXED On November 22, 2026, after this review: `/fund/` was removed and old links now go to the homepage, and every page now sends `X-Frame-Options: DENY` and `Content-Security-Policy: frame-ancestors 'none'`.

BTCG-09 The payout bot is optional INFO

WHAT The bot (a Cloudflare Worker) only sends the payout instruction, which can pay only A and B, so it can never redirect tokens. Its key holds only fee SOL: 0.0238 SOL at 0.0000058 SOL per payout covers about 4,100 daily payouts, roughly 11 years. If it stops, tokens keep vesting and anyone can send one payout that pays everything owed. The first mainnet payout used 18,725 of the bot's 40,000 compute units. The bot passed four Codex reviews before launch.

5. On-chain verification

Read directly from Solana mainnet on November 22, 2026 with a read-only script (`audit/check-mainnet.mjs`). Nothing was sent.

Result	Check
PASS	Program is executable, owned by the upgradeable loader, and its upgrade authority is none
PASS	Deployed code equals the reviewed build byte for byte (sha256 `b04c547c…d178`)
PASS	Only two transactions ever touched the program's code account: the deploy and the finalize
PASS	Token: classic SPL mint, supply exactly 21,000.000000000, 9 decimals, no mint authority, no freeze authority; name and logo record immutable
PASS	Vault record: owned by the program, correct type and addresses, start time 1795288019 (2026-11-21 19:06:59 UTC), the published A and B
PASS	Vault token account: right token, owned by the vault, no delegate, no close authority, not frozen
PASS	Vault balance plus everything paid out is exactly 15,744
PASS	Both vault accounts hold enough SOL that they can never be removed (rent-exempt)
PASS	A's and B's standard token accounts are owned by A and B, with no delegate, not frozen
PASS	The vault's whole history is two transactions: the funding and one payout

Where all 21,000 BTCgold are

Holder	BTCgold	Share
Vault (still locked, released on schedule)	15,742.875428538	74.97%
Treasury: 10 wallets of 525.6 each	5,256.000000000	25.03%
Paid out so far: A and B, 0.562285731 each	1.124571462	0.005%
Total	**21,000.000000000**	**100%**

Rebuilding the code

The source tag was copied fresh into a different folder and built with `cargo-build-sbf` 4.4.0 (platform-tools v1.57, Windows). The result was **identical to the code on Solana** (252,680 bytes):

`sha256 b04c547c17ca34cfabd4f088aaafb4b49d40aac7679865b7ce01aabe1c41d178`

The binary contains Windows-style relative paths, so a Linux or Docker build gives a different fingerprint; reproduce it with the same toolchain on Windows.

6. Testing

All tests ran on the exact program bytes downloaded from mainnet.

Test suite	Result
Schedule math in Rust, including a walk over all 5,250,000 intervals	PASS 8 of 8
Independent schedule check in Node: ends at 15,744 = 7,872 + 7,872	PASS 0 mismatches
Original end-to-end suite	PASS 21 of 21
New audit suite: random attacks, wallet actions, clock edges, mainnet replay	PASS 12 of 12

Random testing

250 seeded scenarios of 120 steps: 10,743 payouts at random times, 7,810 attacks, 1,499 direct deposits, 1,204 clock rollbacks, 901 double payouts in one transaction, and 3,879 payout-wallet actions. After every step the test checks that payouts match the schedule exactly, never run ahead of it, split 50/50 within one base unit, and that the vault balance, the supply and a second vault are correct. Each scenario then runs to 2126 and must end at exactly 7,872 + 7,872.

Mainnet replay

The real vault accounts from slot 472,525,321 were loaded and paid out at random times to the end of the schedule: 495 payouts. A and B each ended with exactly 7,872 BTCgold from the vault, and the vault was empty. Every attack on the real accounts failed and changed nothing.

Compute cost

A payout cost 18,725 compute units on mainnet, against the bot's limit of 40,000. The cost is fixed for the real wallets.

7. Independent second review

OpenAI Codex reviewed the code read-only, given only the scope and the on-chain facts. It independently found BTCG-01 (rating it High), the custody risk (BTCG-02), and the clock, deposit and bot points. It found no way to move tokens anywhere except A's and B's standard accounts, to pay early, to pay more, or to record a payout without the tokens moving.

8. Limits

- This review was done by AI review agents for the BTCgold team, not by a named third-party security firm. The team is seeking a review by an independent firm of the same source tag and code fingerprint.
- It assumes the Solana runtime and the SPL Token and Associated Token programs behave as their published source says.
- Tests show behavior across very many cases. They are not a formal mathematical proof.

Full working files, test logs and the second reviewer's report are kept with the source: `contract/audit/` and `contract/tests/audit.test.ts`. Contact: hello@btc-gold.com · btc-gold.com