LOW RISK

GRADE A+ · PROFESSIONAL

BitLab Coin Security Assessment

BitLab · Solana · SPL Token

CCVYpFakBd4kkwn7G4rvbpaiB5pGJwUpiNwNYrkC5ygQ

Our Auditors reviewed the Solana mint CCVYpFakBd4kkwn7G4rvbpaiB5pGJwUpiNwNYrkC5ygQ, identified as BitLab Coin (BitLab), and discovered the information below. A Two-Step process was used to analyze the smart contract source code; first using AI-powered security audit tools and then manually. No critical traps were confirmed from static analysis and on-chain reads. Residual risk remains in off-chain operators, upgrade keys, and post-seal authority changes.

LIQUIDITY	VERIFIED	BUY / SELL TAX	LP LOCKED
—	No	— / —	—

Identity

FIELD	VALUE
Name / symbol	BitLab Coin / BitLab
Address	CCVYpFakBd4kkwn7G4rvbpaiB5pGJwUpiNwNYrkC5ygQ
Network	Solana
Standard	SPL Token
Decimals	6
Supply	50000000000
Creator	—
Creation tx	—
Compiler	—
Optimization	—
Proxy	No
Implementation	—
Program ID	TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA
Bytecode size	—

Control matrix

STATUS	CONTROL	DETAIL
IDENTITY	—	—
INFO	Contract class	Classified as token from bytecode, source, and on-chain shape.
INFO	Token program	spl-token · TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA
PASS	Token standard	Classic SPL Token.
OWNERSHIP	—	—
PASS	Mint authority	Mint authority revoked.

STATUS	CONTROL	DETAIL
PASS	**Freeze authority**	Freeze authority revoked.
PASS	**Permanent delegate**	No permanent delegate extension.
PASS	**Mint-close authority**	Mint is not closable via Token-2022.
PASS	**Transfer hook**	Not applicable. Classic SPL has no transfer-hook extension.
PASS	**Default account state**	Not applicable. Classic SPL (Tokenkeg) has no DefaultAccountState extension — new accounts start Initialized.
PASS	**Pausable**	No pausable extension.
PASS	**Non-transferable**	Transfers allowed by extension set.
PASS	**Transfer fee**	No transfer-fee extension.
PASS	**Confidential transfers**	Not enabled.
PASS	**Metadata mutability**	Metadata not flagged mutable.
TOKENOMICS	—	—
WARN	**Liquidity**	No DEX pool or liquidity quote was found. Liquidity does not appear to exist yet — this is common in presale. Verify with the project and on-chain before treating this as a listed token.
MARKET	—	—
WARN	**Listed on a DEX**	Not listed on a DEX. Liquidity does not appear to exist yet (possible presale). Verify before buying.
INFO	**Pool age**	No pool yet, so pool age does not apply (possible presale).
TOKENOMICS	—	—
PASS	**Insider wallets**	No insider tags on top holders.
OWNERSHIP	—	—
PASS	**Balance-mutable authority**	No balance-mutable authority flagged.
PASS	**Mint closable**	Not applicable. Classic SPL has no mint-close extension.
MALICIOUS BEHAVIOR	—	—
PASS	**Already rugged**	Not marked rugged.

Smart Contract Security Vulnerability Checklist

Checks that apply to this mint: SPL Token, Token-2022 extensions, oracle/price, and DEX/liquidity. Program-only items (PDA, CPI, Anchor, remaining_accounts) are omitted — those apply to custom programs, not the mint account.

STATUS	CHECK	RESULT
S1. SPL TOKEN / TOKEN ACCOUNT	—	—
PASS	**Incorrect mint validation**	Mint account was read on-chain. spl-token · TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA
N/A	**Incorrect token-account validation**	This address is the mint, not a program that transfers it. Token-account / mint substitution is a handler check on the program that moves tokens.
N/A	**Incorrect token authority**	This address is the mint, not a program that transfers it. Token-account / mint substitution is a handler check on the program that moves tokens.
N/A	**Token-account substitution**	This address is the mint, not a program that transfers it. Token-account / mint substitution is a handler check on the program that moves tokens.

STATUS	CHECK	RESULT
N/A	**Mint substitution**	This address is the mint, not a program that transfers it. Token-account / mint substitution is a handler check on the program that moves tokens.
PASS	**Freeze-authority abuse**	Freeze authority revoked.
PASS	**Mint-authority abuse**	Mint authority revoked.
PASS	**Unauthorized minting**	Mint authority revoked.
N/A	**Unauthorized burning**	This address is the mint, not a program that transfers it. Token-account / mint substitution is a handler check on the program that moves tokens.
N/A	**Unauthorized transfer**	This address is the mint, not a program that transfers it. Token-account / mint substitution is a handler check on the program that moves tokens.
PASS	**Unauthorized freeze**	Freeze authority revoked.
PASS	**Unauthorized thaw**	Freeze authority revoked.
INFO	**Token decimal mismatch**	Decimals are the on-chain mint field. Pool/UI mismatch would be in the DEX, not this mint.
PASS	**Token amount manipulation**	No balance-mutable authority flagged.
N/A	**Token-account ownership errors**	This address is the mint, not a program that transfers it. Token-account / mint substitution is a handler check on the program that moves tokens.
N/A	**Token-program substitution**	This address is the mint, not a program that transfers it. Token-account / mint substitution is a handler check on the program that moves tokens.
PASS	**Token-2022 incompatibility**	Classic SPL Token.
PASS	**Transfer-hook exploitation**	Not applicable. Classic SPL has no transfer-hook extension.
PASS	**Transfer-fee manipulation**	No transfer-fee extension.
PASS	**Permanent-delegate abuse**	No permanent delegate extension.
PASS	**Token extension misuse**	Classic SPL Token.
S2. TOKEN-2022	—	—
PASS	**Transfer-hook vulnerabilities**	Not applicable. Classic SPL has no transfer-hook extension.
PASS	**Transfer-fee vulnerabilities**	No transfer-fee extension.
PASS	**Permanent-delegate abuse**	No permanent delegate extension.
PASS	**Default-account-state manipulation**	Not applicable. Classic SPL (Tokenkeg) has no DefaultAccountState extension — new accounts start Initialized.
PASS	**Non-transferable-token assumptions**	Transfers allowed by extension set.
PASS	**Confidential-transfer assumptions**	Not enabled.
PASS	**Metadata-extension manipulation**	Metadata not flagged mutable.
PASS	**Interest-bearing-token manipulation**	Interest-bearing extension is not present on this mint.
PASS	**Extension compatibility failures**	Classic SPL Token.
PASS	**Incorrect extension validation**	Mint account was read on-chain. spl-token · TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA
PASS	**Incorrect mint-extension assumptions**	Mint account was read on-chain. spl-token · TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA
N/A	**Incorrect token-account extension assumptions**	This address is the mint, not a program that transfers it. Token-account / mint substitution is a handler check on the program that moves tokens.
S3. ORACLE / PRICE SECURITY	—	—

STATUS	CHECK	RESULT
INFO	**Oracle manipulation**	This mint has no oracle account of its own. Spot price and TWAP live in the DEX pool, not in the mint. Review the pair separately.
INFO	**Stale oracle data**	This mint has no oracle account of its own. Spot price and TWAP live in the DEX pool, not in the mint. Review the pair separately.
INFO	**Invalid oracle account**	This mint has no oracle account of its own. Spot price and TWAP live in the DEX pool, not in the mint. Review the pair separately.
INFO	**Oracle account substitution**	This mint has no oracle account of its own. Spot price and TWAP live in the DEX pool, not in the mint. Review the pair separately.
INFO	**Incorrect price-feed validation**	This mint has no oracle account of its own. Spot price and TWAP live in the DEX pool, not in the mint. Review the pair separately.
N/A	**Price-feed decimal mismatch**	This address is an SPL / Token-2022 mint, not a custom program. Instruction-level account/PDA/CPI checks do not apply to the mint account.
INFO	**Price manipulation**	This mint has no oracle account of its own. Spot price and TWAP live in the DEX pool, not in the mint. Review the pair separately.
INFO	**TWAP manipulation**	This mint has no oracle account of its own. Spot price and TWAP live in the DEX pool, not in the mint. Review the pair separately.
INFO	**Spot-price manipulation**	This mint has no oracle account of its own. Spot price and TWAP live in the DEX pool, not in the mint. Review the pair separately.
INFO	**Flash-loan price manipulation**	This mint has no oracle account of its own. Spot price and TWAP live in the DEX pool, not in the mint. Review the pair separately.
INFO	**Missing confidence validation**	This mint has no oracle account of its own. Spot price and TWAP live in the DEX pool, not in the mint. Review the pair separately.
INFO	**Missing freshness validation**	This mint has no oracle account of its own. Spot price and TWAP live in the DEX pool, not in the mint. Review the pair separately.
INFO	**Oracle fallback manipulation**	This mint has no oracle account of its own. Spot price and TWAP live in the DEX pool, not in the mint. Review the pair separately.
S4. DEFI / LIQUIDITY	—	—
INFO	**Liquidity manipulation**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.
INFO	**Pool manipulation**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.
INFO	**Reserve manipulation**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.
INFO	**Share-price manipulation**	This mint has no oracle account of its own. Spot price and TWAP live in the DEX pool, not in the mint. Review the pair separately.
INFO	**Exchange-rate manipulation**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.
INFO	**Flash-loan attacks**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.
INFO	**Economic manipulation**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.
INFO	**Liquidation manipulation**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.

STATUS	CHECK	RESULT
INFO	**Collateral manipulation**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.
INFO	**Reward manipulation**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.
INFO	**Yield manipulation**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.
INFO	**Fee manipulation**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.
INFO	**LP-token manipulation**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.
INFO	**LP-account substitution**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.
INFO	**Incorrect liquidity accounting**	The DEX pool is a different contract from this mint. Attacks on pool reserves, LP tokens, or share price would be in that pair — review the listed pair separately if one exists.

Findings

SEV	TITLE	DETAIL
INFO	**No public rug mark on this token address**	This mint is not marked as already rugged. That is a scan result, not a guarantee. · Remediation: Remediate on-chain and re-run this assessment before treating the finding as closed.
INFO	**Mint authority revoked**	No one can mint additional supply. · Remediation: Revoke mint authority or place it behind a timelocked multisig.

What these risks mean on Solana

OWASP's Top 10 is written for Ethereum-style contracts. Each row is the same risk, rewritten for this Solana mint.

STATUS	ID	WHAT THIS MEANS	THIS TOKEN
PASS	**SC01**	On Ethereum this is admin keys. On Solana we check mint, freeze, and permanent-delegate authorities instead.	Mint, freeze, and permanent-delegate authorities are not live on this mint.
INFO	**SC02**	This Ethereum class is about manipulating DEX/oracle prices. A token mint does not set its own price.	Price lives in the liquidity pool, not in this mint. Review the pool separately if this token is used as collateral.
PASS	**SC03**	Logic bugs live in custom programs. Classic SPL / Token-2022 mints use Solana's standard programs.	This mint uses a standard Solana token program, not custom mint logic.
PASS	**SC04**	Solana already rejects bad accounts. Extra risk appears if a transfer hook runs more code on every send.	No transfer hook. Sends do not run extra validation programs.
PASS	**SC05**	Ethereum reentrancy (calling back into the same contract) does not work the same way on Solana. Transfer hooks are the closest extra-call risk.	No hook. Transfers do not call extra programs.
PASS	**SC06**	On this mint, extra calls only happen if a transfer hook is set.	No extra program is called on transfer.
INFO	**SC07**	Flash loans attack pools and prices, not the mint account itself.	This mint does not implement flash-loan logic. If the token is used as collateral, audit the pool/lending market separately.

STATUS	ID	WHAT THIS MEANS	THIS TOKEN
PASS	SC08	SPL Token math lives in Solana's token program. A custom program would do its own arithmetic.	Supply math is in the standard token program, not in this mint's extra code.
PASS	SC09	A mint does not draw lottery-style randomness. This class matters for games and raffles, not a regular token.	Not applicable to this mint. No randomness used to mint or transfer.
PASS	SC10	On Solana, freeze authority, a paused mint, or a blocking transfer hook can stop people from sending.	No freeze, pause, or frozen-default setting that would halt ordinary transfers.

Solana Token-2022 extras

Optional mint features. PASS means this token does not have that extra power. FAIL or WARN means it does.

STATUS	FEATURE	WHAT IT DOES	THIS MINT
PASS	**Permanent delegate**	A hidden manager that can move anyone's tokens without the holder signing.	Nobody has a standing right to move holders' tokens.
PASS	**Mint-close authority**	Someone can shut down (close) the mint account itself.	This mint cannot be closed by an extra authority.
PASS	**Transfer hook**	Every send can call extra code that can block, tax, or rewrite the transfer.	Transfers do not run extra programs.
PASS	**Default account state**	New wallets can be created already frozen so they cannot send until thawed.	New token accounts are not frozen by default.
PASS	**Non-transferable**	Turns the token into something you cannot send (soulbound).	Holders can send this token.
PASS	**Pausable**	An authority can halt all transfers, like an emergency stop.	There is no pause switch on this mint.
PASS	**Transfer fee**	A cut can be taken from every send, set in the mint's fee config.	Sends do not take a Token-2022 transfer fee.
PASS	**Confidential transfers**	Balances and transfer amounts can be hidden with encryption.	Amounts on this mint are visible on-chain.
PASS	**Metadata pointer**	Name, symbol, and image can live at a separate account the mint points to.	No extra metadata pointer on this mint.

Top 10 Holders

#	WALLET	SHARE	TAG
1	iDohWSWLBurBg7Xs1GfoqjwbLfrQgXGPepk5s71vBdq	**4.0%**	—
2	ACJykTRBNJRQXkjgUHNXs2BE776DMH4mZeeTGGNEXN6G	**4.0%**	—
3	4ChBvttfGA66uaihtKAo2t1HVoi26xt4QoRZ2mjq4tvp	**4.0%**	—
4	PZFwjwkpuCS2UDobrzpgYNDm4NbPhn8hzreS9eSVwyS	**4.0%**	—
5	Ctt3hEjdfqUHhsF9JqQjEwFGSSzjjMQTMKaobsM6NZT5	**4.0%**	—
6	EDwD4Segiy44L1smyJK8kGX59eq1QbJ5VxZdtMs6wYeq	**3.8%**	—
7	7RSvV41H1LvEVhYZ1peWvLAXocC2PzQu8BLwYcMyhGtu	**3.6%**	—
8	3qFihzuw6BdMVC4HbQ4owHsEYGRs2pXE3huxzChuEMDm	**3.6%**	—
9	AJGJBuWTPp2eMLH6ZDK4qJ5ahU5tVXM8nybTiLxrwDfw	**3.5%**	—
10	ATRc2MKKVSHeQzmS9rH3ubjC8mu1V7NLdGeaxfas36oP	**3.4%**	—

Summary

SEVERITY	COUNT
Critical	0
High	0
Moderate	0
Low	0
Warning	2

The following is a concise summary of this audit, with auditor comments on the evidence in this report. BitLab Coin (BitLab) on Solana was reviewed as SPL Token. No critical traps were confirmed from static analysis, on-chain reads, and manual review.

Contract analysis

BitLab Coin is a SPL Token at CCVYpFakBd4kkwn7G4rvbpaiB5pGJwUpiNwNYrkC5ygQ. No proxy was observed. No upgrade path was observed in the assessed controls. Supply and decimals are taken from the on-chain mint or token interface when those fields exist.

Ownership privileges

Administrative powers were taken from the control matrix. Mint authority (pass): Mint authority revoked. Freeze authority (pass): Freeze authority revoked.

Security features

Protective posture is whatever the mint or token contract actually exposes: revoked authorities, absent transfer hooks or taxes, and the absence of freeze/pause where those controls passed. Residual items are listed in Findings with their severity. This engagement used on-chain reads, static analysis, and manual review — not a claim of exhaustive fuzzing.

Note

This report is a security review of BitLab Coin at CCVYpFakBd4kkwn7G4rvbpaiB5pGJwUpiNwNYrkC5ygQ on Solana. It is not an economic analysis of tokenomics and it is not investment advice. Only this address was in scope. Other contracts associated with the project were not reviewed unless they appear in Identity. Readers should independently verify the live chain state before relying on this seal.

Recommendations

#	ACTION
1	Revoke mint, freeze, pause, and upgrade authorities or wrap them in a timelocked multisig.
2	Publish verified source and a compiler-version pin that matches bytecode.
3	Lock or burn LP tokens and disclose locker contracts.
4	Remove blacklist, trading switches, and unbounded tax setters before listing.
5	Re-run this assessment after any upgrade, extension change, or authority rotation.

Scope & methodology

SCOPE
Contract / program identity and deployment provenance
Ownership, roles, mint / freeze / pause / upgrade authorities
Tokenomics, supply, holders, liquidity concentration
Malicious-token behavior (honeypot, tax, blacklist, traps)
EVM vulnerability classes aligned to OWASP Smart Contract Top 10

SCOPE
Solana SPL / Token-2022 extensions and custom program risk
The live address in Identity, plus any verified source or bytecode retrieved for that address — not other contracts in the same project unless they appear in this report
Whether retrieved source matches the bytecode under review when verification is available
Privileged and non-privileged functions: what the code can do, what it cannot do, and whether that matches the stated design
Test-surface and edge-path review when source is present; gaps are recorded rather than assumed complete
Out of scope: unaudited companion contracts, off-chain operators, and any later copy whose digest no longer matches this sealed assessment

METHODOLOGY
On-chain RPC reads of bytecode, storage slots (EIP-1967), ERC-20 / SPL metadata, and Token-2022 TLV extensions.
Verified-source retrieval (Sourcify / Blockscout) followed by a dedicated static-analysis engine — not an LLM — covering OWASP Smart Contract Top 10 classes and token-trap patterns.
Selector extraction from deployed bytecode to detect privileged entrypoints even when source is unverified.
Independent market and liquidity quotes from multiple public feeds; missing quotes are reported as coverage gaps, not zero liquidity.
Security-signal aggregation (honeypot simulation, mint/freeze authorities, holder concentration) with vendor names withheld from the sealed letter.
BitLab synthesis of the already-computed evidence into an engagement letter. The model does not invent on-chain facts.
Specification pass: read the interface, comments, and on-chain layout so size, entrypoints, and intended behavior are understood before findings are written.
Manual code examination: line-by-line review of retrieved source, or of selectors and bytecode when source is absent, looking for traps and logic errors.
Alignment check: confirm the live contract implements the stated token or program behavior and does not hide extra admin paths.
Coverage note: public tests and invariants are considered when artifacts exist; missing tests are called out, not treated as proof of safety.
Path reasoning: how inputs reach privileged or value-moving code, including edge cases that static rules may miss.
Practice comparison: access control, upgradeability, token authorities, and (on Solana) account / signer / PDA validation against established industry practice.
Remediation: specific, ordered actions tied to what this engagement found — not generic checklists.
Integrity: this report is sealed with SHA-256. A different seal, or source/bytecode that no longer matches Identity, means the subject changed after review and is outside this assessment.

Disclaimer

Issued: Tue, 22 Sep 2026 04:16:18 GMT

BitLab Advanced Smart Contract Security Assessment. Automated static analysis, on-chain reads, authority mapping, manual code review, and multi-model review of publicly available data. This engagement snapshot is not a substitute for a human formal-verification review, legal opinion, or insurance underwriting. Privileged keys, upgrades, and off-chain operators can change after this report is sealed.