Predge External Verification Pilot

Verification summary prepared by Velmère

Artifact	pm-2169995-microstrategy-may31.pack.json
Pack ID	pm-2169995-v0
Artifact size	28,156 bytes
Artifact SHA256	ae5f24d6ccf62df01e05800042bc31e18a1f9a98162405d5c377657228cb40b8
Signed content hash	fed6d15eb50da0c8e08e4a1fd95b767f7d9ced13985e246ede843705454b1f64
Verification date	7 October 2026

Overall result

PASS WITH LIMITATIONS

The supplied Predge evidence pack matched the pinned artifact identity and passed the cryptographic integrity checks. The core public facts were independently corroborated. No contradictory evidence was identified. Several exact low level historical values remain outside the independently reproduced subset and are listed below.

Scope

The review covered the pinned JSON artifact supplied by Predge, its byte level identity, canonical payload, content hash, Ed25519 signature, internal timeline consistency, negative mutation tests and the eight findings included in the pack. External checks used public market, filing, resolution and rules evidence where available.

This review is not a security audit of Predge production systems, not a certification, and not a statement that the demo signing key represents Predge production identity.

Verification results

Check	Result	Notes
Exact artifact bytes	PASS	The file size and pinned SHA256 matched exactly.
Canonical payload	PASS	Recanonicalization reproduced the signed canonical string.
Content hash	PASS	SHA256 of the canonical payload matched the declared content hash.
Ed25519 signature	PASS	The signature verified under the supplied demo public key.
Negative tests	PASS	19 mutation cases were executed. None was accepted by the full pinned verification path.
External corroboration	PASS WITH LIMITATIONS	The core public facts were corroborated. Exact raw replay remained incomplete for selected historical values.
Contradictions	NONE	No conflicting fact was identified during the review.

Findings review

Finding	Status	Assessment
F1	SUPPORTED	The original market wording is event based and does not include a confirmation before deadline requirement.
F2	SUPPORTED	The SEC filing independently supports the sale of 32 BTC during 26 to 31 May 2026 and the later disclosure timing.
F3	PARTIAL	The official market record supports No, dispute, No, dispute and final No. Exact raw RPC dispute timestamps were not independently replayed.
F4	SUPPORTED	The two later bulletin updates, including the confirmation clause and their timing, were independently corroborated.
F5	PARTIAL	The final No resolution and approximately 98.6 percent support were corroborated. Exact raw vote aggregates and request linkage were not fully reconstructed.
F6	SUPPORTED	The June 30 and December 31 sibling markets were independently confirmed as resolving Yes.
F7	PARTIAL	The sharp price increase after the filing and collapse after the clarification were corroborated. The exact six historical ten minute samples were not independently refetched.
F8	PARTIAL	The two bulletin updates and contract mechanics were corroborated. The exact initializer versus poster getter result was not independently replayed.

Result by finding

4 supported. 4 partial. 0 contradicted.

Important trust boundary

The signature proves that the canonical payload is valid under the public key included in the file. It does not by itself prove that this key belongs to Predge. The artifact itself identifies the key as a prototype demo key. A production identity claim would require a separately trusted production key or trust anchor.

The whole file SHA256 is therefore an important part of this verification. It protects the complete envelope, including fields that are outside the signed canonical payload.

Remaining limitations

Polygon	Exact raw RPC reproduction of the two dispute timestamps and the bulletin getter result was not completed.
UMA	Exact reconstruction of 607 reveals, 19,433,398.3 UMA and the full L1 to L2 request linkage was not completed.
CLOB	The exact six historical ten minute price samples were not independently refetched.
Kalshi	The exact archived PDF hash and the zero listed contracts inventory check were not independently reproduced.

Conclusion

Velmère independently verified the pinned artifact bytes, canonical payload, content hash and demo key signature, and independently corroborated the core public market, filing, resolution and rule change facts. No contradictions were found. The remaining limitations are confined to selected exact historical raw source values and production key provenance.

Final case result: PASS WITH LIMITATIONS