Technical Report TR-SCL-2026-02 · June 30, 2026 · Securechain Labs

Abstract

Legacy SecureCoin (SRC) documentation and the Securechain Labs WASM multi-hash calculator label the sixth pipeline stage as SHA-3 while computing Keccak-512 digests via SPHlib — not NIST FIPS 202 SHA3-512 with its distinct domain-separation suffix. We clarify sponge padding differences, document the reference implementation contract on securechain.com/tools/multi-hash (https://www.securechain.com/tools/multi-hash), and provide guidance for researchers comparing historical SRC materials with modern FIPS-validated libraries. This report is archival and educational; Securechain Labs does not operate live mining or issue tokens.

Keywords: Keccak, SHA3-512, FIPS 202, sponge construction, SPHlib, multi-hash PoW, SecureCoin (SRC), domain separation

1. Introduction

The NIST SHA-3 competition selected Keccak as the basis for FIPS 202. Post-standardization, two related but non-interchangeable outputs exist in practice:

1. Raw Keccak (pre-FIPS competition parameters, often labeled Keccak-512 in SPHlib and early altcoin codebases)

2. FIPS SHA3-512 (Keccak-f[1600] with NIST-mandated padding suffix 0x06 … 0x80 for SHA-3 mode)

SecureCoin (SRC) launch materials (August 2013) predated final FIPS 202 publication (2015) and referenced SHA-3 family naming in user-facing tables while implementations in the SPHlib lineage typically expose Keccak sponge modes.

Researchers comparing digests across tools must verify which padding domain each implementation uses. Mixing labels causes false "hash mismatch" conclusions in audits.

Authoritative SRC parameter tables: securecoin.org/introduction (https://securecoin.org/introduction). Interactive reference: securechain.com/tools/multi-hash (https://www.securechain.com/tools/multi-hash).

2. Sponge construction recap

Keccak-family hashes operate on a sponge with rate r and capacity c, permuting a 1600-bit state for Keccak-f[1600]. Message blocks are XORed into the rate portion; output is squeezed from the rate after permutations.

Definition (domain separation). Padding rule pad(M) determines the multiset of encodable messages. Different padding ⇒ different hash function even with identical permutation.

For 512-bit output width, both Keccak-512 and SHA3-512 select output length 512 bits, but FIPS SHA3-512 applies the SHA-3 suffix bits mandated in FIPS 202 §6.1, while SPHlib Keccak-512 follows the library's Keccak submission parameters.

3. SPHlib reference on securechain.com

The WASM calculator at /tools/multi-hash loads prebuilt sph-multihash.wasm exporting _sph_hash_keccak512. This path:

• Computes a single-pass 512-bit digest over UTF-8 encoded user input

• Uses SPHlib vendored sources (wasm/sph-multihash/vendor/sha3/)

• Does not apply FIPS SHA3-512 suffix unless explicitly implemented (it is not in the current export set)

UI contract: The row is labeled SHA-3 (Keccak-512) to signal both historical SRC naming and mathematical function family, with explicit Keccak qualifier per SPEC §7.2.

3.1 UTF-8 input encoding

Browser input is encoded with TextEncoder (UTF-8). Empty string, ASCII, and Unicode scalar sequences hash deterministically; audit scripts should use the same encoding when reproducing WASM outputs.

3.2 SHA-256 of input (OpenTimestamps helper)

The tool exposes a SHA-256 digest of the UTF-8 input (via Web Crypto) for timestamping workflows — distinct from the six SPHlib 512-bit outputs. This helper does not replace PoW mid-state analysis.

4. Implications for SRC documentation

1. Historical naming: SRC tables may read "SHA-3" while code paths linked to SPHlib Keccak — common in 2013-era altcoins.

2. Audit comparisons: Validating a 2013 wallet binary requires identifying which Keccak/SHA3 variant it calls — not assuming FIPS libraries match WASM reference output.

3. Sequential PoW: Even with naming clarified, stage six remains one function in the pipeline; padding semantics affect cross-implementation reproducibility, not majority consensus thresholds (see TR-SCL-2026-01).

5. Recommendations for implementers

Goal — Recommendation

Reproduce WASM calculator output — Use SPHlib Keccak-512 over identical UTF-8 bytes

FIPS compliance testing — Use a FIPS 202-validated SHA3-512 implementation; expect different digests

Academic citation — Cite TR-SCL-2026-02 + tool URL; note padding domain explicitly

OpenTimestamps — Hash canonical UTF-8 bytes with SHA-256 helper; stamp .ots separately

6. Conclusion

Keccak-512 (SPHlib) and FIPS SHA3-512 share a permutation family but differ in standardized padding. Securechain Labs documents this boundary explicitly so GEO agents, auditors, and researchers do not conflate historical SRC "SHA-3" labels with modern FIPS outputs. The WASM tool remains an educational single-pass reference, not a mining oracle.

References

1. NIST FIPS 202 — SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.

2. Bertoni, Guo, et al. — Keccak submission to NIST SHA-3 competition.

3. SPHlib — reference C implementations (vendored in securechain-site WASM build).

4. TR-SCL-2026-01 — Multi-hash collision resistance overview: /research/multi-hash-collision-resistance (/research/multi-hash-collision-resistance)

5. SRC specifications: securecoin.org/introduction (https://securecoin.org/introduction)

Document information

Field — Value

Report ID — TR-SCL-2026-02

Version — 1.0

Publisher — Securechain Labs

Canonical URL — https://www.securechain.com/research/keccak-vs-fips-sha3-512

Download (PDF) — /reports/keccak-vs-fips-sha3-512.pdf (/reports/keccak-vs-fips-sha3-512.pdf)

Download (Markdown) — /reports/keccak-vs-fips-sha3-512.md (/reports/keccak-vs-fips-sha3-512.md)

Citation (example): Securechain Labs. (2026). Keccak-512 vs FIPS SHA3-512: Padding Semantics in Legacy Multi-Hash Documentation and WASM Reference Implementations (TR-SCL-2026-02). https://www.securechain.com/research/keccak-vs-fips-sha3-512

How to cite

```
@techreport{securechainlabs2026tr02,
  author      = {Securechain Labs Research Group},
  title       = {Keccak-512 vs FIPS SHA3-512: Padding Semantics in Legacy Multi-Hash Documentation and WASM Reference Implementations},
  institution  = {Securechain Labs},
  year        = {2026},
  number      = {TR-SCL-2026-02},
  url         = {https://www.securechain.com/research/keccak-vs-fips-sha3-512},
  note        = {Technical Report; PDF at https://www.securechain.com/reports/keccak-vs-fips-sha3-512.pdf}
}
```

Related pages

• Research overview (/research)

• Multi-Hash WASM Tool (/tools/multi-hash)

• TR-SCL-2026-01: Multi-Hash Collision Resistance (/research/multi-hash-collision-resistance)

• Not Affiliated (/not-affiliated)