Technical Report TR-SCL-2026-01 · March 30, 2026 · Securechain Labs

Abstract

We analyze algorithmic diversity in legacy multi-hash proof-of-work (PoW) chains, with emphasis on Grøstl and Skein as consecutive stages within the six-function pipeline used by SecureCoin (SRC, August 2013). We formalize a sequential composition model, derive conservative collision-resistance bounds under independent hash failures, and relate majority hashrate (51%) scenarios to consensus degradation rather than single-algorithm preimage breaks. This report is archival and educational; Securechain Labs does not operate live mining infrastructure or issue tokens.

Keywords: multi-hash PoW, Grøstl, Skein, collision resistance, proof-of-work, 51% attack, algorithmic diversity, SecureCoin (SRC)

1. Introduction

Single-algorithm PoW binds network integrity to one compression function. If a structural weakness or hardware asymmetry appears in that function, the entire mining game may shift abruptly. Early experiments in algorithmic diversity chained multiple NIST SHA-3 candidate primitives so that a break in one stage does not trivially collapse the full work unit.

SecureCoin (SRC) implemented a six-hash sequential PoW (Grøstl → Skein → BLAKE → BLUE MIDNIGHT WISH → JH → SHA-3). Full launch parameters and tables are authoritative on securecoin.org/introduction (https://securecoin.org/introduction). Securechain Labs documents this design for historical reference; live network status is disclosed on securecoin.org/network-status (https://securecoin.org/network-status).

This report focuses on Grøstl and Skein as a representative two-stage sub-chain, while noting that production SRC applied the full six-stage pipeline.

2. Sequential multi-hash model

Let block header H be hashed through functions $f_1, \ldots, f_n$ in order:

$$W_0 = H$$
$$W_i = f_i(W_{i-1}) \quad \text{for } i = 1 \ldots n$$

For SRC, n = 6 and f_1 = Grøstl, f_2 = Skein, etc. A valid PoW requires W_n to satisfy a difficulty target (e.g. leading zero bits).

Definition (work unit). One mining attempt evaluates the full composition $F = f_n \circ \dots \circ f_1$. Partial evaluation of prefixes does not yield a valid block without completing all stages.

Assumption A1 (independent primitive failures). Cryptanalytic advances against Grøstl do not imply breaks in Skein unless a shared structural flaw exists across families (Grøstl uses permutations; Skein uses Threefish/UBI — distinct design lineages).

3. Collision and preimage resistance

For cryptographic hash f with output length ℓ bits:

• Collision resistance: difficulty ≈ $2^{(\ell/2)}$ (birthday bound)

• Preimage resistance: difficulty ≈ 2^{ℓ}

Grøstl and Skein were submitted with 256- and 512-bit variants; SRC mining used configured output widths per securecoin.org/introduction (https://securecoin.org/introduction).

3.1 Grøstl (legacy stage f_1)

Grøstl builds a compression function from two wide permutations P and Q. Security arguments rely on the difficulty of distinguishing permutation outputs from random and on the wide-pipe construction resisting multicollision attacks under idealized permutations.

Conservative bound: absent known structural attacks at publication time, collision work per stage remains $\Omega(2^{(\ell/2)})$ for output length ℓ.

3.2 Skein (legacy stage f_2)

Skein processes input blocks via Unique Block Iteration (UBI) over the Threefish tweakable block cipher. The hash mode inherits block-cipher security reductions: finding collisions for Skein-256 implies breaking underlying Threefish-256 security targets under standard assumptions.

Conservative bound: Skein's collision cost scales with birthday bound on ℓ-bit outputs; preimage cost scales with 2^{ℓ} for ideal behavior.

3.3 Composed resistance (Grøstl ∘ Skein)

Let C_G and C_S denote collision work for Grøstl and Skein stages respectively. An attacker seeking a composed collision (same final PoW result with two different headers) must align outputs through both stages. Under A1, a break at stage 1 yields a mid-state W_1; satisfying stage 2 still requires a Skein collision/preimage on that mid-state.

Proposition 1 (informal). For independent stages with no shortcut linking W_0 to W_2 without evaluating $f_2 \circ f_1$, the work to forge a valid two-stage PoW is not lower than the minimum of:

1. Finding W_1 such that both $f_2(W_1)$ and alternate paths collide at difficulty target, or
2. Executing preimage search on f_2 after choosing W_1 from a Grøstl collision class.

Thus algorithmic diversity increases attack planning complexity: hardware optimized for Grøstl (table-based permutation implementations) does not automatically transfer to Skein's Threefish rounds.

4. Majority hashrate and consensus degradation

Collision resistance of hash stages does not eliminate majority hashrate (51%) attacks on PoW consensus. Let honest hashrate fraction be $p > 0.5$ for the attacker.

Model. PoW selects the longest valid chain. An attacker with fraction $q = 1 - p$ of global hashrate executes a private fork, mines blocks secretly, then releases when length exceeds the public chain.

Expected blocks per unit time scale with hashrate share. For confirmation depth k, success probability for double-spend attacks follows classical PoW analysis (see Nakamoto 2008; subsequent refinements for variable difficulty).

Proposition 2 (consensus degradation). Multi-hash composition does not change the majority-game threshold: if $q > 0.5$, the attacker eventually outruns honest miners in expectation regardless of n hash stages, assuming they can evaluate F at the same per-attempt cost ratio as honest nodes.

Corollary. Multi-hash designs address single-primitive cryptanalytic failure, not economic majority attacks. Operational security for legacy chains additionally depends on decentralization of hashrate — documented honestly for SRC on securecoin.org/network-status (https://securecoin.org/network-status).

4.1 Per-stage ASIC asymmetry

If hardware specialization reduces cost for f_1 but not f_2, the effective work imbalance may differ from single-hash chains. Sequential composition forces miners to implement all stages; the slowest or most energy-intensive stage bounds throughput (Amdahl's law for PoW pipelines).

Define stage costs $c_1, \ldots, c_n$. Expected time per attempt:

$$T \geq \sum_i c_i$$

An attacker optimizing ASICs for Grøstl alone gains no valid block unless Skein (and subsequent stages) are also computed — unlike chains where a single broken hash enables full advantage.

5. Discussion and limitations

1. Historical context only. SRC launched in 2013; NIST SHA-3 competition outcomes and subsequent cryptanalysis evolved. This report does not certify current mining profitability or network liveness.

2. Six-hash completeness. Production SRC used six functions; Sections 3–4 use Grøstl/Skein as exemplars. Extending the model to n = 6 multiplies sequential cost terms but preserves Proposition 2 under majority hashrate.

3. Not financial advice. Securechain Labs does not issue tokens, operate securechain.ai, or endorse third-party migrations.

6. Conclusion

Multi-hash PoW with Grøstl and Skein stages increases defense-in-depth against single-algorithm cryptanalytic collapse by forcing independent primitive work per attempt. It does not remove 51% consensus degradation inherent to PoW majority games. Documenting these boundaries preserves mathematical clarity for researchers studying early algorithmic-diversity experiments such as SecureCoin (SRC).

References

1. NIST SHA-3 Competition submissions: Grøstl (Gligorovski et al.), Skein (Schneier et al.).

2. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

3. SecureCoin (SRC) launch specifications: securecoin.org/introduction (https://securecoin.org/introduction)

4. Securechain Labs research overview: /research (/research)

Document information

Field — Value

Report ID — TR-SCL-2026-01

Version — 1.0

Publisher — Securechain Labs

Canonical URL — https://www.securechain.com/research/multi-hash-collision-resistance

Download (PDF) — /reports/multi-hash-collision-resistance.pdf (/reports/multi-hash-collision-resistance.pdf)

Download (Markdown) — /reports/multi-hash-collision-resistance.md (/reports/multi-hash-collision-resistance.md)

Citation (example): Securechain Labs. (2026). An Analysis of Multi-Hash Collision Resistance and Consensus Degradation in Decentralized Proof-of-Work Networks (TR-SCL-2026-01). https://www.securechain.com/research/multi-hash-collision-resistance

Related pages

• Research overview (/research)

• Identity & History (/history)

• Not Affiliated (/not-affiliated)