ASIC ULTRA BOOST™

Message scheduling optimisation for SHA256 ASICs

Patent: “Message Scheduling for Cryptographic Hashing” — US 2024/0405998 A1 (Application No. 18/696,073)

Technology overview for industry, partners, and investors

Efficiency is the primary axis of competition

Bitcoin mining hardware

1

J/TH is the scoreboard

Miners select hardware almost entirely on joules per terahash. Each generation's marketing claim rests on a small, hard-won efficiency delta.

2

SHA256 dominates the die

Three chained SHA256 instances ($SHA256_0$, $SHA256_1$, $SHA256_2$) are executed on every hash attempt — billions of times per second, per chip.

3

Small deltas compound

A few percentage points of switching-activity reduction, repeated across a fleet of millions of chips, becomes a material power and cost advantage.

Source: Bitcoin Block Header structure; SHA256 specification (FIPS 180-4)

The overlooked inefficiency: the message scheduler

Each SHA256 round requires an input value W[t], expanded from the message block by a message scheduler. Existing optimisations (e.g. “ASICBoost”, hardwired-constant designs) only reuse values that are fully invariant across hash attempts.

Standard approach

Recompute W[t] in full for every hash attempt

Prior art (ASICBoost)

Reuse only fully-invariant values — narrow applicability

ASIC Ultra Boost™

Partially compute once, store reusable values μ[t], complete only the variable remainder

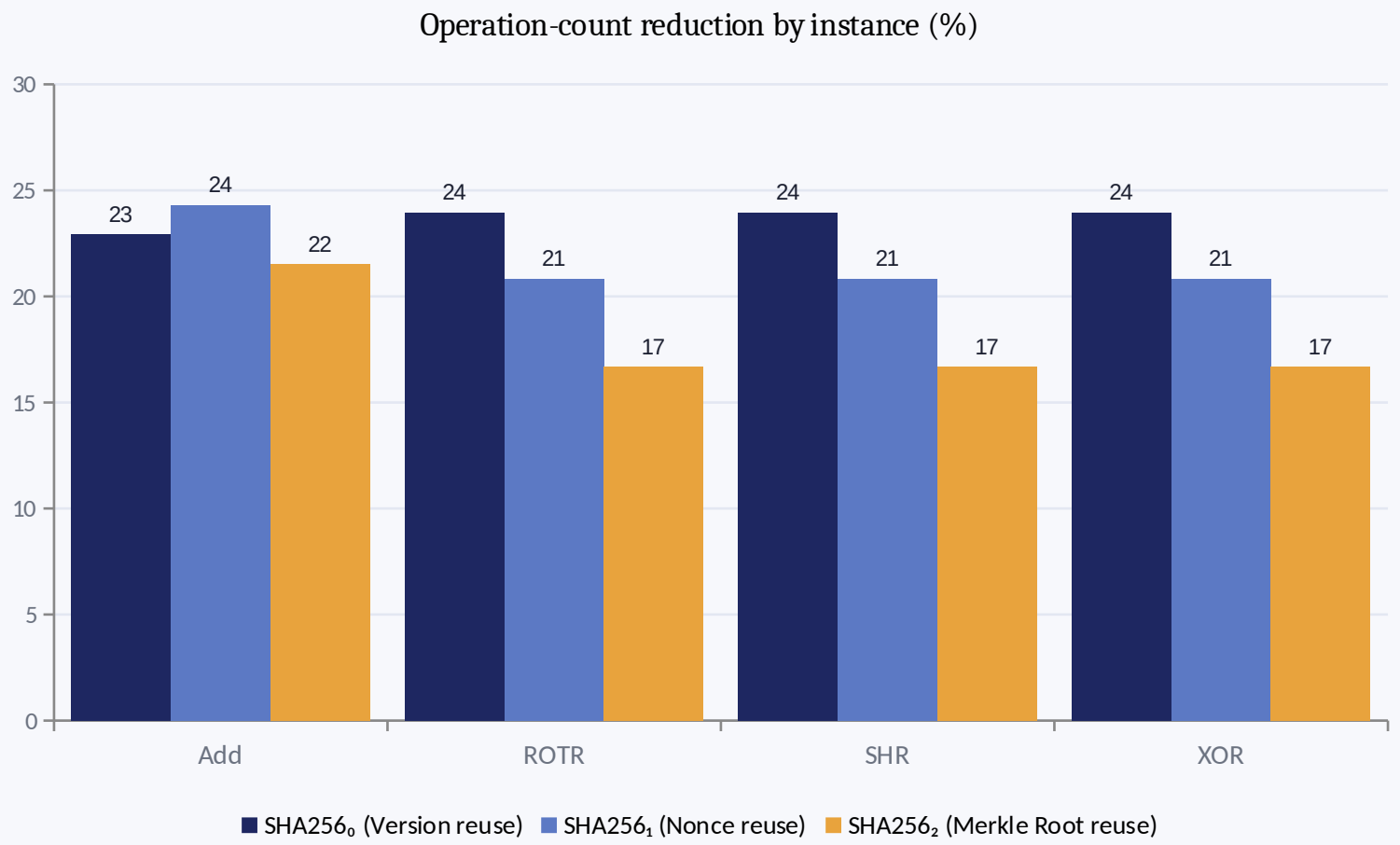
The result: fully-calculated scheduler inputs for subsequent hash attempts are built from cached partial results — not recomputed and not merely reused as-is — cutting the operation count needed each time a Nonce, Version, or Merkle Root value changes.

Granted claim scope (US 2024/0405998 A1)

“Calculate a set of partially-calculated input values using invariable portions of an initial input message … and, for each subsequent message, calculate a set of fully-calculated input values using the partially-calculated values together with the variable portions.” — Claim 1 (method) / Claim 20 (apparatus)

Quantified reduction in message-schedule operations

Per subsequent hash attempt, as disclosed in the patent specification



~20–24%

reduction in scheduler-level operations, consistently across all three SHA256 instances

SHA256₁ matters most

The Nonce field is incremented on nearly every hash attempt — this is the dominant, always-executing code path in mining.

Conservative framing

These figures describe the scheduler in isolation. Whole-chip impact depends on each manufacturer's specific architecture and is discussed next.

Source: US 2024/0405998 A1, ¶0081–¶0123 (message-schedule operation counts as disclosed)

From scheduler savings to whole-chip impact

An illustrative, conservative translation — actual gains depend on each manufacturer's architecture

Component	Share of critical-path operations	Addressed by this patent?
Message scheduler (per instance)	~30%	Yes — ~20–24% reduction
Compression function (64 rounds)	~70%	No — unaffected
Net effect on per-hash critical path ($SHA256_1$ + $SHA256_2$)	**—**	**Estimated ~5–8% operation-count reduction**

Indicative range: 2–5% net J/TH improvement at chip level

This range applies a further dilution for non-hashing overhead (I/O, control logic, clocking, voltage regulation) that does not shrink with this technique. It should be validated against each manufacturer's own synthesis results before being relied upon.

Why a modest efficiency gain is commercially meaningful

24/7

operation

Mining hardware runs continuously; small power savings compound daily over the life of the fleet.

millions

of units/year

Efficiency gains scale linearly with production volume across a manufacturer's product line.

J/TH

is the marketing claim

Each generation's headline efficiency number is the primary driver of purchase decisions by miners.

A deliberately conservative view

We are not presenting a specific royalty, revenue, or valuation figure in this document. Any commercial terms would need to reflect: (i) validated silicon-level power measurements against a manufacturer’s own design; (ii) freedom-to-operate analysis of existing or planned architectures; and (iii) mutually agreed licensing structure. Any such terms would be developed through a structured, professionally advised commercial process.

Intellectual property position

Commercial name	ASIC Ultra Boost™
Publication (original title)	US 2024/0405998 A1 (Application No. 18/696,073) — “Message Scheduling for Cryptographic Hashing”
Applicant / Assignee	Quantum Blockchain Technologies PLC (London, UK)
Inventor	Rahul Naik
Priority date	29 September 2021 (GB 2113962.1)
Route to grant	PCT/GB2022/052458 — US national phase entered 27 March 2024; Notice of Allowance received 23 July 2026
Claim scope	20 claims: independent method (claim 1) and apparatus (claim 20), with dependent claims specific to Bitcoin Block Header fields (Version, HashPrevBlock, HashMerkleRoot, Timestamp, Target, Nonce)

Differentiated from prior art

Distinguished in the specification from EP 3 095 044 A1 (“ASICBoost” — reuse of fully-invariant messages) and US 2018/0006808 A1 (hardwired invariant constants), by introducing an intermediate, partially-calculated value that is reusable even where portions of the input do vary.

Let’s discuss ASIC Ultra Boost™

get in touch

We welcome the opportunity to share further technical detail and explore whether ASIC Ultra Boost™ — the invention disclosed in US 2024/0405998 A1, “Message Scheduling for Cryptographic Hashing” — has a fit with your organisation's roadmap.

Quantum Blockchain Technologies plc

London, United Kingdom · AIM: QBT