Cryptix (CPAY)

Cryptix Network | https://Cryptix-Network.org | info@cryptix-network.org
2026-02-27

Cryptix OX8i Hash v3

Version: 3.0 (Codename: Iridium)

1. Introduction

OX8i is the **next-generation extension of the OX8 (v2) hash**, designed to provide a **robust, low-memory, and hardware-resistant proof-of-work** for decentralized networks.

The codename **Iridium** reflects its philosophy:

Iridium (Ir, atomic number 77) is one of the hardest and most resilient metals known.

Similarly, OX8i is engineered to be **resilient against FPGA, ASIC, and botnet attacks** while remaining CPU/GPU-accessible.

Key objectives:

1. Significantly increase hardware resistance compared to OX8 v2.
2. Maintain low memory usage (<10 KB per hash).
3. Introduce serial and chaotic operations that limit parallel acceleration.
4. Lay the groundwork for future experimental enhancements.

---

2. Already Integrated in OX8i (v3)

The current v3 hash includes several fully integrated mechanisms:

Feature	Description	Security Impact
LUT Chaos Burner	Multi-layer nested loops combining four 32-byte state arrays with millions of internal operations per round.	Exceeds FPGA LUT limits; full unrolling is infeasible. Forces serial execution, drastically limiting FPGA throughput.

Feature	Description	Security Impact
Chaos Mix Extra	Additional diffusion via dynamic swaps, bit rotations, grouped arithmetic, and state permuting.	Amplifies entropy, increases serial complexity, and prevents predictable GPU/bot pipelines.
ASIC Slow Mix	Carry chains, nested variable loops, dynamic rotations, and serial dependencies.	Makes ASIC design prohibitively expensive and slow. Forces multiple sequential cycles per byte.

Hardware Resistance Notes:

- **FPGAs:** Even high-end devices cannot achieve competitive hash rates. Benchmark tests with Vivado indicate that **full parallelization requires ~20× more LUTs than available on the strongest FPGA**.
- **ASICs:** Custom hardware would require tens of millions in development, with multiple sequential critical paths. Economically non-viable.
- **Botnets:** Serial dependencies, randomized memory access, and variable loops reduce efficiency. Bots still participate but cannot scale linearly.

Memory & Performance:

- Low-memory design (<10 KB).
- CPU/GPU mining remains feasible with moderate performance reduction relative to OX8 v2.
- Deterministic integer-based operations; no floats to ensure cross-platform consistency.

---

3. Planned / Experimental Features (Research Phase)

The following enhancements are **under development and not yet fully integrated**. They represent the potential **v3 final extension**:

Feature	Description	Expected Impact
Enhanced Octonion Chains	Multiple dynamic octonion multiplications with post-multiplication chaos injection.	Increases critical-path multiplier usage; deters FPGA/ASIC parallelization.
Extended Random Hash Chains	8–16 chained hash primitives selected dynamically based on input bytes.	Prevents precomputed pipelines; increases unpredictability for botnets and hardware miners.
Nested Variable Loops (v2)	Multi-layer loops with data-dependent iteration counts.	Creates unpredictable latency; GPU/FPGAs cannot pipeline effectively.

Feature	Description	Expected Impact
Extra Temporary States	5–10 additional 32-byte arrays mixed in final state.	Boosts register pressure; increases spill into LUTs/BRAM, complicating hardware mapping.

Note: These functions are experimental and may be refined or replaced during the final v3 rollout. They are designed to further **increase FPGA/ASIC costs and reduce botnet efficiency** without violating the low-memory principle.

---

4. Security & Hardware Resistance

4.1 FPGA Resistance

- **LUT-limited design:** Current integrated functions already exceed serial parallelization thresholds on commercial FPGAs.
- **Serial-only execution:** Even top-tier FPGAs cannot outperform a single high-end GPU.
- **Integer-only operations:** No floats; deterministic across platforms.

4.2 ASIC Resistance

- **High gate complexity:** Integrated and planned features increase DSP/multiplier/barrel shifter demands.
- **Economic deterrent:** Custom ASIC would cost tens of millions USD; sequential loops make pipeline gains marginal.
- **Dynamic primitives (planned):** Future extensions make fixed-function ASICs less viable.

4.3 Botnet Mitigation

- **Serial dependencies**: Each iteration depends on previous state.
- **Randomized memory access & loops**: Multiple bots cannot scale linearly.
- **Dynamic rotations & nested loops**: GPU optimizations are ineffective.

While botnets can still submit hashes, **cost per bot is significantly higher**, slowing potential abuse.

---

5. Performance

- **CPU/GPU Mining:** Moderate slowdown vs OX8 v2; fully feasible on modern desktop hardware.
- **Memory Footprint:** <10 KB per hash.

- **Expected Throughput:** v3 is designed to prioritize hardware deterrence over raw CPU/GPU hash speed, keeping the network accessible but preventing massive hardware advantage.

---

6. Conclusion

OX8i (v3, Iridium) is a strategic upgrade to OX8 v2:

- **Already integrated**: LUT Chaos Burner, Chaos Mix Extra, ASIC Slow Mix – provides strong baseline hardware resistance.
- **Planned extensions**: Enhanced octonions, extended hash chains, nested variable loops, extra states – will push FPGA/ASIC costs beyond practical limits.
- **Network Accessibility**: Low-memory design ensures CPUs and GPUs can still participate efficiently.
- **Botnet Mitigation**: Serial dependencies and chaotic memory access make mass bot operations inefficient.

OX8i is **robust, resilient, and engineered for a decentralized proof-of-work future**, living up to its Iridium namesake: hard to break, resistant to specialized hardware, and predictable only for legitimate network participants.