

Forensic Analysis: Circle Arc Architecture

Silicon Dependencies, Closed-Source Drivers & Vulnerability Mapping

Project Anchor — FluidCluster.pt

FluidCluster Forensic Audit Panel

Vanguard Cryptography & Hardware Security Division

September 2026

Forensic Audit Scope

Hardware Dependencies & Intel SGX SDK

Closed-Source Binaries & Driver Analysis

Vulnerability Surface Exploration

The Alternative: Photonic Math Sovereignty

The Silicon Roots: Hardware Component Mapping

The privacy architecture of Arc (*Arc Privacy*) is not cryptographic at the runtime layer; it is boundary-enforced by physical silicon.

Critical Hardware Requirements

- ▶ **Intel SGX (Software Guard Extensions):** Requires 3rd Gen Intel Xeon Scalable processors (Ice Lake) or newer with Flexible Launch Control (FLC).
- ▶ **AMD SEV-SNP:** Requires AMD EPYC processors (Milan/Genoa) with Secure Nested Paging enabled in the UEFI/BIOS layer.

The Architectural Risk

Validation nodes cannot run on commodity decentralized hardware. The network topology is strictly bound to specialized data-center tiers controlled by institutional cloud providers.

The Proprietary Blobs: libsgx_urts.so and DCAP

Forensic repository inspection of the arc-privacy subsystem reveals direct linking against closed-source Intel binary blobs.

The Untrusted Runtime Client

- ▶ `libsgx_urts.so`: Manages Ring 3 initialization of enclaves, ecalls, and ocalls.
- ▶ Operates as a black box within the compilation pipeline, blocking complete open-source reproducible builds.

DCAP Attestation Flow

- ▶ Uses Intel's Data Center Attestation Primitives (DCAP).
- ▶ Verification relies on Intel's ECDSA Provisioning Certification Service (PCS), introducing a centralized point of failure.

The Binary Compilation Pipeline Blindspot



Supply Chain Risk

Because the binary dependencies cannot be compiled from clean source, backdoor detection at the hardware-software boundary is mathematically unfeasible for external auditors.

Microarchitectural Side-Channels & Exploitation Vectors

The repository treats enclaves as static cryptographic boxes, ignoring known transient execution leakage vectors.

Cache-Timing Exploits: Malicious co-located hypervisor threads can observe enclave memory access patterns via L1d cache state disruptions (*e.g., Flush+Reload attacks*).

Speculative Leakage: Fault-driven speculative execution paths (*Downfall, Gather Data Sampling*) can force the internal CPU registers to dump unencrypted financial states into cleartext cache lines.

Retroactive Compromise: Unlike FHE/ZKP, if a single global Intel attestation private key is leaked or compromised via coercive national security mandates, **the entire historical archive of encrypted ledger states becomes decryptable.**

Dismantling the Silicon Dependency

The forensic panel concludes that the Circle Arc architecture introduces structural liabilities disguised as regulatory compliance frameworks.

FluidCluster Architectural Verdict

- ▶ **Arc's Flaw:** Privacy is treated as an isolation of hardware, creating vulnerable execution boundaries.
- ▶ **The Solution (fhEVM):** True privacy must be math-native. By computing directly over ciphertext, the hardware layer is neutralized.
- ▶ **Photonic Acceleration:** Modulating light beams to perform Lattice-LWE computations bypasses both the silicon clock speed constraints and the side-channel vulnerability surface.