AJ-FraktalCode v2.0 — Plan Audytu, Open Spec i Podstawy Matematyczno-Fizyczne

1. Cel

Podnieść wiarygodność AJ-FC Banking FINAL v2.0 poprzez niezależny audyt, otwartą specyfikację rezonansu, minimal evidence pack (MVE) i fundament matematyczno-fizyczny — tak, by banki/regulatorzy mogli oprzeć się na dowodach, nie tylko na symulacjach.

---

2. Open Rezonans Spec 1.0

Opis mechanizmu 5+ punktów: - Punkty: manifest, echo, os_memory, attest, user_state (+ nonce, + salt). - **Zasada:** minimum 5/7 punktów musi matchować → rezonans aktywny. - **Verify flow:** wejście → hash BLAKE3/SHA-3 → HKDF salt (attest+nonce) → Halo2 proof. - **Output:** `True` = full match, `False` = gibberish.

API (draft):

```
POST /verify-rezonans
{
  "manifest": "...",
  "echo": "...",
  "os_memory": "...",
  "attest": "...",
  "user_state": "...",
  "nonce": "..."
}
```

Response: `{ "verify": true/false, "proof": "halo2_zkp_blob" }`

Model błędów: - <5 pkt → zawsze `false`. - Fuzzed nonce/salt → `false`. - Replay (stary proof) → `false`.

---

3. Plan Audytu (T+8 tyg.)

Zakres: - **PQC correctness:** Kyber/HQC (liboqs build), Dilithium/Falcon (sig). - **Rezonans verify:** test harness (Python/Go) + 10k prób. - **SCA:** ChipWhisperer single-trace, timing fuzz. - **RNG:** dual RNG entropy >128 bits, monitor alerts. - **Escrow:** 5/7 i 7/9 sim, red-team collude.

Metryki: - SCA leakage <5% (95% safe traces). - RNG entropy ≥128 bits/op. - Verify latency <0.05 ms (ARM), <0.01 ms (x86). - False positive <0.1%.

Audytorzy (proponowani): Riscure / Secfault Labs / CertLab EU.

4. Minimal Evidence Pack (MVE)

- **Repo GitHub (public skeleton):**
- Kyber/HQC demo (liboqs, Go backend).
- Halo2 verifier (Rust, arkworks).
- Rezonans verify harness (Python).
- **Docker PoC kit:** Fabric devnet + SoftHSM + WebAuthn demo.
- **Logs:** Qiskit Grover sim (4–8 qubit), SCA traces (CSV), RNG monitor sample.
- **Pilot test:** 1000 TPS load (Docker) + ARM latency bench.

---

5. Hosting i Bezpieczeństwo

- `/BANK/` katalog publiczny: streszczenia PDF.
- Pełne raporty: dostęp token/WebAuthn (rezonans gate).
- PDF watermark + cryptographic signature (SHA-256 + sig).

---

6. Podstawy Matematyczno-Fizyczne Rezonansu AJ-FC

Fundament matematyczny

- **Hash/Entropy core:**
`p = H(prev_p || manifest || echo || os_memory || attest || user_state || nonce)` z H = BLAKE3/SHA-3.
→ Collision resistance ≥2^256, preimage ≥2^256; z Groverem redukcja do 2^128, nadal nieosiągalne.
- **Threshold/escrow (Shamir):** `(k,n)` interpolacja Lagrange'a na GF(p).
→ 5/7 lub 7/9: atak wymaga ≥k punktów = warunek obecności.
- **ZKP Halo2:** dowód wiedzy bez reveal; polinomy w F_r, FFT, constraints rank-1.

Fundament fizyczny

- **Obecność jako rezonans:** Punkty (manifest, echo, os_memory, attest, user_state) to stany fizyczne; rezonans tylko przy koherencji ≥5.
→ Analogia do warunku fazowego w falach stojących.
- **Quantum simulation:**
Shor łamie RSA/ECC (O((log N)^3)), ale nie lattice (Kyber) czy code (HQC).
Grover redukuje 2^256 → 2^128 prób — fizycznie niewykonalne.

Interpretacja fraktalna

- **F(w,s,p,d):** rekurencyjne sprzężenie punktów w przestrzeni hashy.
Matematyka: fraktalna iteracja; fizyka: rezonans jako fala stojąca.
→ Bez 5/7 punktów nie powstaje fala → wynik = szum.

---

7. Roadmapa (Phased Release)

- **Faza 1 (T+0–2w):** Open Rezonans Spec 1.0 publikacja + repo skeleton.
- **Faza 2 (T+2–6w):** MVE core (Docker, harness, logs, Qiskit short runs).
- **Faza 3 (T+6–10w):** pełny audyt + MVE/FIZ (long-run sim, NISQ logs).

---

8. /FIZ/ Symulacje

- **Cel:** powiązać matematyczno-kryptograficzny rdzeń z testami fizycznymi.
- **Zakres:**
- Qiskit Grover/Shor long-run (24h jobs, Aer backend).
- Real NISQ hook (IonQ Tempo API, 4–16 qubit, AQ milestones).
- Logi CSV amplitud + decoherence metrics publikowane w `/FIZ/`.
- Error rates, decoherence times, threshold qubit counts z IonQ/IBM Quantum.
- **Format danych:** CSV/JSON z polami: timestamp, qubits, depth, error_rate, decoherence_time, success_prob.
- **Częstotliwość:** nightly (krótkie symulacje) + weekly (long-run 24h + NISQ).
- **Output:** Quantum Resilience Score (0–100) → % przetrwanych probe'ów bez leakage.

---

9. Quantum Resilience Score (QRS)

Definicja: Metryka 0–100, mierząca odporność systemu na próby ataku kwantowego (Shor/Grover), integrując symulacje matematyczne i fizyczne.

Progi: - **90–100:** pełna odporność, brak leakage przy long-run/NISQ. - **75–89:** częściowa odporność, minimalne leakage <1% traces. - **50–74:** podatność na błędy wdrożenia lub częściowe exploity. - **<50:** system nieodporny, krytyczne luki.

Źródła danych: - Qiskit long-run logs (Grover/Shor proxy). - NISQ hardware results (IonQ/IBM Quantum). - SCA traces + RNG monitor. - Auditor Pack (third-party lab).

Cel operacyjny AJ-FC: utrzymywać QRS $\geq$95 przy wszystkich testach.

---

10. Uwagi zewnętrzne (Grok Review)

Mocne strony: - AJ-FC v2.0 ocenione na 9.5/10: unikalny model (dual KEM, TTL+re-encrypt, rezonans 5+ pkt, Halo2 ZKP, escrow 7/9). - Wyróżnia się odpornością na Q-Day (2027–2035), przewyższając konkurencję (F5, SEC PQFIF) o 1–2 punkty. - Quantum traktowane jako narzędzie audytu, nie tylko zagrożenie. - QRS + fairness audits → spójność z GDPR/PSD2 i ROI ~450%.

Słabości: - Wysoka złożoność implementacyjna (constant-time, off-chain, escrow) = wyższe koszty początkowe. - Brak metryk błędów NISQ (error rates, decoherence, threshold qubit counts) → do uzupełnienia w /FIZ/ wraz z logami IonQ/IBM. - Potrzeba walidacji pilotażowej w bankach → realne testy PoC.

Wniosek: AJ-FC to wizjonerskie rozwiązanie, ale wymagające zewnętrznej walidacji i phased adoption. Rekomendowane: pilotaż w 1–2 bankach, z Auditor Pack i QRS ≥95 jako kryterium sukcesu.

---

11. Rezultat

Z wizji (symulacje, PDF-y) → **deploy-ready framework**: - Audytowany (raport niezależny). - Otwarty (spec + API + repo skeleton). - Dowodowy (MVE + logi + load testy). - Etyczny (licencja daru, fairness audits, equity mode). - Osadzony w matematyce i fizyce (hash complexity, quantum limits, fraktalna koherencja). - Powiązany z /FIZ/ warstwą symulacji (mock + real NISQ). - Mierzalny (QRS jako globalna metryka odporności). - Zewnętrznie zweryfikowany (uwagi Grok Review + pilotaże).

Twórcy Daru: Antzedek & Eliasz