Foglio Progetto — Bitcoin Reforged (BTRF)

Versione: 1.0

Data: 2025-08-06

Responsabili proposti: 2–3 maintainer (firmatari build), security contact dedicato

Sintesi: Progetto di chain PoW, CPU-friendly (RandomX), senza premine, con cap 21.000.000 BTRF
Questo foglio incorpora le modifiche adeguate e la roadmap per avvio testnet pubblica e hardening.

---

1) Obiettivi e risultati attesi

- **Fair-launch** senza premine e senza owner, supply fissata a 21M.
- **Decentralizzazione del mining** via RandomX (CPU).
- **Time-to-use**: testnet pubblica stabile entro ~12–16 settimane da T0.
- **Sicurezza e governance minime**: release firmate, policy security, bug bounty.
- **Onboarding**: wallet GUI + documentazione + explorer + faucet.

KPI principali:

- Propagazione blocchi P50 < **2 s** su testnet; riorgani >1 blocco **rari**.
- 100+ nodi testnet e 1.000+ tx/settimana entro Fase 2.
- Copertura test consenso/P2P > **80%** entro Fase 3.

---

2) Modifiche approvate (adeguamenti chiave)

1. DAA: adozione LWMA v3, per-block.
   - Finestra **N = 144** blocchi (~6 h).
   - Clamp solve-time: **±7×T** con T=150 s.
   - Damping leggero (±0,2%) e **hard-limit ±100%** per step.
   - Uso di **Median Time Past** per robustezza timestamp.
2. Parametri rete: porte e magic bytes dedicati, DNS seed multipli.
3. Script & address: SegWit + Taproot abilitati; bech32m (HRP: btrf, tbtrf).
4. Mempool/policy: min relay fee 1 sat/vB, mempool 300 MB, RBF attivo.
5. Sicurezza & release: build riproducibili, binari firmati (2-of-3), SECURITY.md.
6. Branding: rimozione firma “Nakamoto, 2025”; manifesto firmato da team/comunità.
7. Tooling: wallet GUI desktop leggero e guide d’onboarding (Ubuntu/WSL/macOS/Win).

(Emissione rimane conforme alla bozza: 25 BTRF/blocco, halving 420.000 blocchi, cap 21M.)

---

3) Parametri di consenso — versione proposta

Timing & difficoltà

- Target spacing (T): **150 s** (2,5′).
- DAA: **LWMA v3, N=144**, clamp ±7T, damping ±0,2%, hard-limit ±100%, MTP.

- Future drift consentito: **+2 h** (validazione header).

Ricompense & emissione

- Ricompensa iniziale: **25 BTRF**.
- Halving: **420.000** blocchi (~2 anni).
- Cap: **21.000.000 BTRF**.
- Coinbase maturity: **100** blocchi.

Rete & P2P

- Magic bytes (mainnet/testnet): **da pubblicare** in `CONSENSUS.md`.
- Porte: mainnet **9433**, testnet **19433**.
- DNS seed: **≥3** domini indipendenti.
- User agent: `/BTRFCore:0.1.0/`.

Blocchi & mempool

- Peso massimo blocco: **4 MWU** (iniziale).
- Policy: allineata a Bitcoin Core v26; RBF **on**; min relay fee **1 sat/vB**; mempool **300 MB**.

Script & feature

- SegWit **on**, Taproot **on**.
- Address: **bech32m**, HRP `btrf` (mainnet), `tbtrf` (testnet).
- Soft fork policy: **BIP8(LOT=false)**; attivazione 6–12 mesi (mainnet), 3 mesi (testnet).

Sicurezza & governance

- Maintainers: **3** (PR review 2-of-3).
- Release: tag firmati **2-of-3**; build riproducibili; **SECURITY.md** con PGP keys.
- Bug bounty Fase 3.

---

4) DAA — nota di implementazione (alto livello)

Per ogni nuovo blocco:

1. T=150 s. Prendi ultimi N=144 solve-time (timestamp MTP) e clamp a [−7T, +7T].
2. Calcola LWMA = $\Sigma(w_i \cdot solve_i) / \Sigma(w_i)$ con pesi lineari crescenti.
3. next_diff = prev_diff · T / max(1, LWMA).
4. Applica damping e hard-limit.
5. Protezioni anti-timestamp: rigetta header troppo futuri (> +2 h).

(Patch C++/Rust disponibile su richiesta.)

---

5) Deliverable tecnici

- `CONSENSUS.md` (parametri finali)
- `DAA.md` (specifica LWMA e test vettori)
- `SECURITY.md` (policy, chiavi, disclosure)
- `ROADMAP.md` (milestone + KPI)
- `wallet-gui/` (client desktop leggero)

- **Explorer** minimale + **faucet** testnet
- Script di **seed node** e DNS seeder

---

6) Roadmap (T0 = data di kickoff)

Fase 0 — Freeze consenso (Settimane 0–2)

- Chiudere `CONSENSUS.md` + `DAA.md`.
- Tag `v0.1.0-testnet` compilabile.

KPI: build CI verdi su 3 OS.

Fase 1 — Testnet pubblica (Settimane 2–4)

- 2–3 seed DNS, explorer, faucet.

KPI: >50k blocchi, propagazione P50 <2 s, riorgani >1 rari.

Fase 2 — Tooling & UX (Settimane 4–8)

- Wallet GUI, guide, installer.

KPI: 100+ nodi e 1.000+ tx/sett in 10 gg.

Fase 3 — Hardening (Settimane 8–12)

- Fuzzing, property-based tests, benchmark RandomX, bug bounty.

KPI: copertura >80%, 0 crash noti, audit esterno avviato.

Fase 4 — Ecosistema minimo (Settimane 12–16)

- Integrazione Bisq (se rete stabile).

KPI: 10+ scambi/sett, P50 conferma <3 min.

---

7) Rischi critici & mitigazioni

- **Oscillazioni hash-rate** (CPU): DAA LWMA, finestra breve, damping.
- **Superficie d’attacco RandomX**: benchmark + audit esterno + hardening VM/JIT.
- **Concentrazione iniziale coinbase**: monitoraggio distribuzione, incentivi mining diffusi, comunicazione trasparente.
- **UX scarsa**: priorità a wallet GUI, guide, faucet.

---

8) Emissione — materiali allegati

Dati e grafico generati:

- `btrf_epoch_emission.csv` — emissione per epoca.
- `btrf_daily_emission_20y.csv` — emissione giornaliera (20 anni).
- `btrf_supply_curve.png` — curva della supply nel tempo.

---

9) Branding & comunicazione

- Manifesto firmato dal **team/comunità** (no riferimenti fuorvianti).

- Sito minimal con link a repo, explorer, faucet, wallet.
- Linee guida contributi e codice di condotta.

---

10) Prossimi passi operativi

- Approvazione di questo foglio (OK/Change Request).
- Kickoff (T0) e assegnazione owner per: consenso, rete/seed, wallet GUI, infra.
- Apertura issue tracker con milestone e KPI collegati.