CriptoEuro: Proposta di una criptovaluta bancaria ancorata all'Euro

Versione: 2.2
Data: 10 Aprile 2025

CriptoEuro: Proposta di una criptovaluta bancaria ancorata all'Euro

Versione 2.0 – Aprile 2025

---

1. Introduzione

La crescente diffusione delle criptovalute ha evidenziato la necessità di soluzioni digitali che uniscano la stabilità della moneta fiat alla sicurezza e trasparenza della tecnologia blockchain. CriptoEuro propone un sistema monetario digitale supportato da riserve bancarie reali, costruito su un protocollo decentralizzato basato su Litecoin e l'algoritmo Scrypt. Il sistema è progettato per emettere una valuta digitale coperta da euro reali depositati presso istituti bancari autorizzati.

Il presente documento descrive dettagliatamente l'architettura tecnica, le funzionalità, i meccanismi di sicurezza e governance, e le prospettive operative del progetto CriptoEuro, ispirandosi alla chiarezza e alla logica espositiva adottata nei whitepaper di riferimento come Bitcoin e Litecoin.

---

2. Obiettivi

Il sistema CriptoEuro si propone di raggiungere i seguenti obiettivi fondamentali:

- **Stabilità**: offrire una criptovaluta ancorata 1:1 all'euro tramite riserve bancarie reali e verificabili.
- **Affidabilità istituzionale**: demandare l'emissione esclusivamente a banche autorizzate e soggette a controllo tra pari.
- **Decentralizzazione della governance**: introdurre un meccanismo di approvazione distribuito per l'accesso delle banche al sistema.
- **Trasparenza**: garantire auditabilità completa di ogni emissione, transazione e riconversione tramite blockchain pubblica.
- **Interoperabilità**: costruire un sistema compatibile con l'infrastruttura finanziaria esistente, facilitando l'integrazione con conti correnti bancari e circuiti di pagamento nazionali.

---

3. Architettura del Sistema

3.1 Banche

Le banche rappresentano l'unica entità autorizzata a creare nuovi CriptoEuro. Ogni emissione è effettuata a fronte di un deposito equivalente in euro, vincolato e verificabile. Le banche utilizzano firme digitali avanzate (multi-sig) per autorizzare le operazioni, inclusa la proposta e approvazione di nuove banche.

3.2 Wallet

Ogni wallet è collegato in modo univoco a un conto corrente presso una banca partecipante. Questa relazione è fondamentale per garantire la tracciabilità e l'identificazione dell'utente, nonché per abilitare funzionalità di conversione Payout. I wallet supportano transazioni P2P, ricezione di CriptoEuro, e richieste di riconversione.

3.3 Blockchain e Miners

La rete CriptoEuro è strutturata su una blockchain pubblica e immutabile, alimentata dal meccanismo di consenso **Proof-of-Work** basato sull'algoritmo **Scrypt**, come Litecoin. I miner hanno il compito di validare le transazioni, creare blocchi, garantire la sicurezza della rete, e sono ricompensati con le commissioni di transazione.

---

4. Emissione dei CriptoEuro

4.1 Simulazione di Flusso Emissione e Utilizzo

Caso d'uso: Mario vuole acquistare beni digitali utilizzando CriptoEuro

Step 1 – Emissione:

1. Mario deposita 1.000 € nel suo conto corrente presso Banca X.
2. Banca X genera una MintRequest firmata, specificando l'importo e il wallet di Mario.
3. La richiesta viene propagata sulla blockchain e validata da miner.
4. 1.000 CriptoEuro vengono creati e accreditati nel wallet di Mario.

Step 2 – Transazione tra utenti:

1. Mario vuole pagare 100 CriptoEuro a Luca per un servizio.
2. Mario invia una TransferTx al wallet di Luca.
3. La transazione è firmata, propagata e validata.
4. Luca riceve 100 CriptoEuro.

Step 3 – Riconversione Payout:

1. Luca richiede un Payout alla sua banca, Banca Y, per 100 CriptoEuro.

2. Banca Y verifica e firma la PayoutRequest entro 24 ore.
3. I 100 CriptoEuro vengono bruciati.
4. Banca Y trasferisce 100 € sul conto di Luca.

4.2 Diagramma di flusso (descrizione testuale)

[Utente] --> [Deposito € presso banca] --> [Banca emette MintRequest]

--> [Blockchain valida] --> [Wallet riceve CriptoEuro]

--> [Transazione P2P tra wallet]

--> [Richiesta Payout alla banca]

--> [Firma banca] --> [CriptoEuro bruciati]

--> [Trasferimento € a utente]

Questo flusso simula in modo completo l'interazione tra sistema bancario, utenti e blockchain. Mostra il ciclo completo di vita di un CriptoEuro: dalla creazione alla transazione fino alla riconversione in euro fiat.

L'emissione dei CriptoEuro avviene secondo un processo rigoroso e verificabile:

1. **Deposito in euro**: l'utente deposita una somma in euro presso una banca partecipante.
2. **Generazione richiesta**: la banca crea una transazione di tipo MintRequest, firmata digitalmente, che specifica l'importo, il wallet di destinazione, e il riferimento bancario.
3. **Registrazione su blockchain**: la transazione è trasmessa alla rete e validata dai miner, venendo registrata pubblicamente.
4. **Emissione**: i CriptoEuro vengono generati e accreditati sul wallet dell'utente.

Questo meccanismo garantisce che ogni CriptoEuro esistente sia effettivamente coperto da euro in deposito, rendendo l'intero sistema trasparente e auditabile.

---

5. Transazioni Wallet-Wallet

Le transazioni tra wallet si svolgono secondo un protocollo standardizzato e sicuro:

- Il mittente genera una transazione contenente l'indirizzo del destinatario, l'importo e una firma digitale.

- La rete propaga la transazione ai nodi.
- I miner validano la transazione e la includono in un blocco.
- Il destinatario vede accreditati i CriptoEuro nel proprio wallet.

Ogni transazione è irreversibile, visibile pubblicamente, e sottoposta al consenso distribuito della rete.

---

6. Meccanismo di Payout

La funzione Payout consente agli utenti di riconvertire i CriptoEuro in euro reali:

1. L'utente invia una PayoutRequest alla propria banca, specificando importo e coordinate bancarie per l'accredito.
2. La banca ha un intervallo massimo di tempo pari a 24 ore (espresso in blocchi) per firmare la transazione.
3. In caso di firma, i CriptoEuro vengono **bruciati (burn)** e la banca accredita l'equivalente in euro all'utente.
4. In caso di mancata firma entro il tempo limite, la richiesta è automaticamente **annullata** e i fondi rimangono nel wallet.

Tale sistema evita l'accumulo eccessivo di liquidità in CriptoEuro e garantisce un canale sicuro di uscita.

---

7. Onboarding di Nuove Banche

L'aggiunta di una nuova banca segue un meccanismo di approvazione distribuito:

- Una banca attiva crea una proposta NewBankProposal contenente i dati dell'istituto candidato.
- Le altre banche possono firmare in modo asincrono tramite transazioni BankApprovalSignature.
- Al raggiungimento della soglia richiesta (es. maggioranza assoluta), viene generata una NewBankActivation.

Il processo assicura una governance collaborativa e resistente a tentativi di centralizzazione.

---

8. Sicurezza e Auditabilità

8.1 Struttura del Blocco

Ogni blocco CriptoEuro contiene:

- BlockHeader: hash del blocco precedente, timestamp, nonce, Merkle root
- TxList: lista delle transazioni (TransferTx, MintRequest, PayoutRequest, BankApproval)
- BlockHash: firma del miner valida con PoW (Scrypt)

8.2 Formato delle Transazioni (esempio JSON semplificato)

```
{
  "type": "TransferTx",
  "from": "wallet_A",
  "to": "wallet_B",
  "amount": 150,
  "signature": "hex_firma",
  "timestamp": 1712740000
}
{
  "type": "MintRequest",
  "bank": "Bank_X",
  "to": "wallet_M",
  "amount": 1000,
  "euro_reference": "DEP20250410",
  "signature": "hex_firma_banca"
}
```

8.3 Sicurezza lato utente: gestione wallet

Il wallet per PC sarà un'applicazione equivalente al wallet Litecoin ufficiale, con piena gestione delle chiavi private, seed di ripristino, e firma delle transazioni.

Sarà previsto anche un **wallet mobile leggero**, tecnicamente definito in fase 2 del progetto, simile all'app **Guarda Wallet** (Android/iOS), che permetterà:

- Invio/ricezione CriptoEuro
- Integrazione con dispositivi biometrici
- Connessione semplificata ai conti bancari

Entrambi i wallet useranno protocolli sicuri di crittografia locale e consentiranno backup cifrati.

8.4 Conformità normativa

CriptoEuro è progettato per essere conforme ai principi del regolamento europeo **MiCA**, nonché compatibile con i requisiti di **KYC/AML** grazie alla connessione dei wallet a conti correnti reali.

È inoltre integrabile con l'infrastruttura esistente attraverso **API bancarie PSD2** e protocolli standard di open banking.

CriptoEuro è progettato per garantire elevati standard di sicurezza:

- **Multi-sig bancario**: ogni operazione critica richiede firme multiple da parte della banca emittente.
- **Blockchain pubblica**: tutte le transazioni sono visibili e consultabili in tempo reale.
- **Validazione decentralizzata**: nessuna entità può censurare o modificare i dati senza il consenso della rete.
- **Controllo sull'emissione**: ogni CriptoEuro è legato ad un deposito reale, facilmente verificabile da enti terzi o regolatori.

---

9. Confronto con altri Stablecoin

Caratteristica	CriptoEuro	EURC (Circle)	EURCV (SG)	EURM (Monei)
Emittente	Banche multiple	Circle	Société Générale	Monei (Spagna)
Copertura 1:1	Sì	Sì	Sì	Sì
Blockchain pubblica	Sì	Sì	Limitata	Sì
Meccanismo di consenso	PoW (Scrypt)	Varia	N/A	Varia
Governance distribuita	Sì	No	No	No

CriptoEuro si distingue per la trasparenza on-chain, la partecipazione di più istituti, e l'accesso vincolato ad autorizzazioni bancarie distribuite.

---

10. Roadmap Tecnica

Fase 1 – Architettura e Testnet (Q3–Q4 2025)

- Costruzione blockchain PoW Scrypt dedicata
- Implementazione transazioni base (mint, transfer, payout)
- Validazione testnet e wallet desktop

Fase 2 – Integrazione bancaria (Q1 2026)

- Integrazione primi istituti (Banca Pilota)
- Connessione conti correnti, creazione seed wallet bancari
- App mobile prototipo simile a Guarda Wallet

Fase 3 – Audit & Regolazione (Q2 2026)

- Audit indipendente su codice e sicurezza
- Adeguamento a MiCA, normativa anti-riciclaggio
- Protocolli per riconoscimento bancario ufficiale

Fase 4 – Lancio pubblico (Q3 2026)

- Avvio rete principale (mainnet)
- Distribuzione wallet ufficiali
- Collaborazioni pubbliche per uso istituzionale

---

11. Conclusione

CriptoEuro fornisce una soluzione ibrida che unisce la stabilità bancaria alla trasparenza della blockchain. Ogni unità digitale è garantita da euro reali depositati presso banche partecipanti, e tutte le operazioni sono pubbliche e verificabili.

Grazie alla governance distribuita, al meccanismo di riconversione e al supporto di wallet collegati a conti correnti bancari, CriptoEuro offre uno strumento robusto per l'economia digitale europea.

Le prossime evoluzioni prevedono:

- Supporto a smart contract regolamentati

- Integrazione con sistemi bancari e di pagamento
- Interfacce per utenti privati e istituzionali
- Collaborazioni con enti pubblici per l'uso di CriptoEuro in servizi e sussidi

CriptoEuro è la base per un'economia digitale trasparente, sicura e ancorata a valori tangibili.