CriptoEuro: Proposal for a Bank-Backed Cryptocurrency Pegged to the Euro

Version 2.2 – April 10th 2025

©Francesco Claudio Mazza

CriptoEuro: Proposal for a Bank-Backed Cryptocurrency Pegged to the Euro

Version 2.2 – April 2025

---

1. Introduction

The growing popularity of cryptocurrencies has highlighted the need for digital solutions that combine the stability of fiat currency with the security and transparency of blockchain technology. CriptoEuro proposes a digital monetary system backed by real bank reserves, built on a decentralized protocol based on Litecoin and the Scrypt algorithm. The system is designed to issue a digital currency backed by actual euros deposited with authorized banking institutions.

This document provides a detailed description of the technical architecture, functionalities, security and governance mechanisms, and operational outlook of the CriptoEuro project. It draws inspiration from the clarity and logical structure of reference whitepapers such as Bitcoin and Litecoin.

---

2. Objectives

The CriptoEuro system aims to achieve the following core objectives:

- **Stability**: To offer a cryptocurrency pegged 1:1 to the euro, backed by real and verifiable bank reserves.

- **Institutional Reliability**: To delegate currency issuance exclusively to authorized banks under mutual oversight.

- **Governance Decentralization**: To introduce a distributed approval mechanism for new banks joining the system.

- **Transparency**: To guarantee full auditability of every issuance, transaction, and redemption through a public blockchain.

- **Interoperability**: To build a system compatible with existing financial infrastructure, enabling integration with current accounts and national payment networks.

---

3. System Architecture

3.1 Banks

Banks are the only entities authorized to issue new CriptoEuro. Each issuance must correspond to an equivalent deposit in euros, held and verifiable. Banks use advanced digital signatures (multi-signature systems) to authorize operations, including the proposal and approval of new banks.

3.2 Wallets

Each wallet is uniquely linked to a current account held at a participating bank. This linkage ensures traceability and user identification, and enables redemption features through the Payout function. Wallets support peer-to-peer transactions, CriptoEuro deposits, and redemption requests.

3.3 Blockchain and Miners

The CriptoEuro network operates on a public and immutable blockchain, validated using the **Proof-of-Work** consensus mechanism based on the **Scrypt** algorithm, similar to Litecoin. Miners are responsible for validating transactions, creating blocks, maintaining network security, and earning transaction fees.

---

4. CriptoEuro Issuance

4.1 Issuance and Usage Flow Simulation

Use Case: Mario wants to purchase digital goods using CriptoEuro

Step 1 – Issuance:

1. Mario deposits €1,000 into his bank account at Bank X.

2. Bank X generates a signed MintRequest, specifying the amount and Mario's wallet.

3. The request is broadcast to the blockchain and validated by miners.

4. 1,000 CriptoEuro are created and credited to Mario's wallet.

Step 2 – User Transaction:

1. Mario wants to pay 100 CriptoEuro to Luca for a service.

2. Mario sends a TransferTx to Luca's wallet.

3. The transaction is signed, propagated, and validated.

4. Luca receives 100 CriptoEuro.

Step 3 – Payout Redemption:

1. Luca submits a PayoutRequest to his bank, Bank Y, for 100 CriptoEuro.

2. Bank Y verifies and signs the request within 24 hours.

3. The 100 CriptoEuro are burned.

4. Bank Y transfers €100 to Luca's account.

4.2 Flow Diagram (Textual Description)

[User] --> [Euro deposit at bank] --> [Bank issues MintRequest]

  --> [Blockchain validation] --> [Wallet receives CriptoEuro]

  --> [P2P Wallet Transaction]

  --> [Payout Request to bank]

  --> [Bank signs] --> [CriptoEuro burned]

  --> [Euro transfer to user]

This flow simulates the full interaction among the banking system, users, and the blockchain. It illustrates the complete lifecycle of a CriptoEuro: from issuance to transaction and back to fiat redemption.

The issuance process follows strict and verifiable steps:

1. **Euro Deposit**: The user deposits euros with a participating bank.

2. **Request Generation**: The bank creates a digitally signed MintRequest transaction that specifies the amount, the destination wallet, and a banking reference.

3. **Blockchain Registration**: The transaction is propagated to the network, validated by miners, and recorded publicly.

4. **Issuance**: CriptoEuro are generated and credited to the user's wallet.

This mechanism ensures that every CriptoEuro in circulation is backed by an equivalent euro deposit, making the entire system transparent and auditable.

5. Wallet-to-Wallet Transactions

Transactions between wallets follow a standardized and secure protocol:

- The sender generates a transaction containing the recipient's address, the amount, and a digital signature.

- The transaction is broadcast to the network nodes.

- Miners validate the transaction and include it in a block.

- The recipient sees the CriptoEuro credited to their wallet.

Each transaction is irreversible, publicly visible, and subject to decentralized consensus.

---

6. Payout Mechanism

The Payout function allows users to redeem CriptoEuro for real euros:

1. The user submits a PayoutRequest to their bank, specifying the amount and bank account details.

2. The bank has a maximum of 24 hours (measured in blocks) to sign the transaction.

3. If the request is signed, the CriptoEuro are **burned**, and the equivalent amount in euros is credited to the user.

4. If the bank does not sign within the time frame, the request is automatically **canceled**, and the funds remain in the wallet.

This system prevents excess CriptoEuro liquidity and provides a secure fiat exit channel.

---

7. Onboarding New Banks

Adding a new bank follows a distributed approval mechanism:

- An active bank creates a NewBankProposal containing the candidate institution's data.

- Other banks can sign asynchronously via BankApprovalSignature transactions.

- Once the required threshold (e.g., absolute majority) is reached, a NewBankActivation is generated.

This process ensures collaborative governance and resilience against centralization.

---

8. Security and Auditability

8.1 Block Structure

Each CriptoEuro block contains:

- BlockHeader: previous block hash, timestamp, nonce, Merkle root

- TxList: list of transactions (TransferTx, MintRequest, PayoutRequest, BankApproval)

- BlockHash: miner's valid signature under PoW (Scrypt)

8.2 Transaction Format (Simplified JSON Example)

```
{

 "type": "TransferTx",

 "from": "wallet_A",

 "to": "wallet_B",

 "amount": 150,

 "signature": "hex_signature",

 "timestamp": 1712740000

}

{

 "type": "MintRequest",

 "bank": "Bank_X",

 "to": "wallet_M",

 "amount": 1000,

 "euro_reference": "DEP20250410",

 "signature": "hex_bank_signature"

}
```

8.3 User Security: Wallet Management

The desktop wallet will function similarly to the official Litecoin wallet, with full control over private keys, recovery seed, and transaction signing.

A lightweight **mobile wallet** will also be developed in Phase 2, similar to **Guarda Wallet** (Android/iOS), offering:

- CriptoEuro sending/receiving

- Biometric device integration

- Simplified linking with bank accounts

Both wallet versions will support local encryption and secure backup features.

8.4 Regulatory Compliance

CriptoEuro is designed to comply with the principles of the **MiCA** regulation and is compatible with **KYC/AML** requirements thanks to wallet linkage with real bank accounts.

It can also integrate with existing infrastructure via **PSD2-compliant banking APIs** and standard open banking protocols.

CriptoEuro adheres to high security standards:

- **Bank-level Multi-Sig**: critical operations require multiple signatures from the issuing bank.

- **Public Blockchain**: all transactions are publicly viewable and traceable in real-time.

- **Decentralized Validation**: no entity can censor or modify data without network consensus.

- **Issuance Control**: every CriptoEuro is tied to a real deposit, independently verifiable by third parties.

---

9. Comparison with Other Stablecoins

Feature	CriptoEuro	EURC (Circle)	EURCV (SG)	EURM (Monei)
Issuer	Multiple banks	Circle	Société Générale	Monei (Spain)
1:1 Euro Backing	Yes	Yes	Yes	Yes
Public Blockchain	Yes	Yes	Limited	Yes
Consensus Mechanism	PoW (Scrypt)	Varies	N/A	Varies
Distributed Governance	Yes	No	No	No

CriptoEuro stands out for its on-chain transparency, multi-institution participation, and distributed bank authorization governance.

---

10. Technical Roadmap

Phase 1 – Architecture and Testnet (Q3–Q4 2025)

- Launch of dedicated PoW Scrypt blockchain

- Implementation of basic transactions (mint, transfer, payout)

- Testnet validation and desktop wallet testing

Phase 2 – Bank Integration (Q1 2026)

- First bank onboarding (pilot institution)

- Linking of bank accounts and seed wallet generation

- Prototype mobile app similar to Guarda Wallet

Phase 3 – Audit & Regulation (Q2 2026)

- Independent code and security audits

- MiCA and anti-money laundering compliance alignment

- Protocols for official banking recognition

Phase 4 – Public Launch (Q3 2026)

- Mainnet deployment

- Official wallet distribution

- Public sector partnerships for institutional use

---

11. Conclusion

CriptoEuro offers a hybrid solution that combines the stability of the banking system with blockchain transparency. Each digital unit is backed by real euros deposited with participating banks, and all operations are public and verifiable.

Thanks to distributed governance, the redemption mechanism, and wallets linked to bank accounts, CriptoEuro provides a robust tool for Europe's digital economy.

Future developments include:

- Support for regulated smart contracts

- Integration with payment and banking systems

- Interfaces for private and institutional users

- Partnerships with public entities for CriptoEuro-based services and subsidies

CriptoEuro is the foundation for a transparent, secure, and euro-pegged digital economy.