Blockchain

Abstract

CRED Standard è una blockchain decentralizzata progettata per essere una riserva di valore digitale accessibile, sicura e sostenibile. Il protocollo si basa su un algoritmo Proof of Work resistente agli ASIC, pensato per funzionare su hardware consumer come CPU e GPU standard, promuovendo una reale equità nella partecipazione al mining. Supporta nodi leggeri su smartphone tramite SPV, favorendo una diffusione capillare e una decentralizzazione globale. Le transazioni sono gratuite per l’utente, grazie a un meccanismo di ricompensa dinamica che incentiva i miner senza costi diretti. La tokenomics è fondata su una scarsità programmata lenta, priva di pre-mine, ICO o distribuzioni privilegiate. Il progetto rifiuta ogni forma di governance centralizzata e promuove un codice open source, immutabile e verificabile da chiunque. In un contesto di crescente sfiducia e centralizzazione, CRED Standard propone un’alternativa semplice, equa e resiliente.

Sommario

[Blockchain 1](#_Toc201011527)

[Abstract 1](#_Toc201011528)

[1. Introduzione 4](#_Toc201011529)

[2. Il problema 5](#_Toc201011530)

[3. Soluzione proposta 6](#_Toc201011531)

[4. Architettura tecnica 7](#_Toc201011532)

[4.1. Meccanismo di consenso: Proof of Work (PoW) anti-ASIC 7](#_Toc201011533)

[4.2. Struttura dei nodi 8](#_Toc201011534)

[4.3. Sicurezza 9](#_Toc201011535)

[4.4. Transazioni 9](#_Toc201011536)

[4.5. Esempio di ciclo di vita di una transazione 9](#_Toc201011537)

[5. Riepilogo tecnico per sviluppatori 11](#_Toc201011538)

[6. Specifiche tecniche del protocollo 12](#_Toc201011539)

[6.1. Struttura del blocco 12](#_Toc201011540)

[6.2. Formato delle transazioni 13](#_Toc201011541)

[6.3. Algoritmo di consenso 13](#_Toc201011542)

[6.4. Crittografia e hash 13](#_Toc201011543)

[6.5. Compatibilità e requisiti minimi 13](#_Toc201011544)

[6.6. Specifiche di protocollo 14](#_Toc201011545)

[7. Tokenomics 14](#_Toc201011546)

[7.1. Emissione 15](#_Toc201011547)

[7.2. Transizione programmata del tempo di blocco 15](#_Toc201011548)

[7.3. Incentivi 15](#_Toc201011549)

[7.4. Sostenibilità 16](#_Toc201011550)

[8. Vantaggi competitivi 16](#_Toc201011551)

[8.1. Decentralizzazione reale 16](#_Toc201011552)

[8.2. Transazioni gratuite 16](#_Toc201011553)

[8.3. Sostenibilità a lungo termine 16](#_Toc201011554)

[8.4. Privacy modulabile 17](#_Toc201011555)

[8.5. Semplicità e trasparenza 17](#_Toc201011556)

[8.6. Incentivi anche per i light node 17](#_Toc201011557)

[9. Roadmap 17](#_Toc201011558)

[10. Team e governance 19](#_Toc201011559)

[10.1. Nessuna governance on-chain o off-chain 19](#_Toc201011560)

[10.2. Anonimato e contributo aperto 19](#_Toc201011561)

[11. Aspetti legali e conformità 19](#_Toc201011562)

[11.1. Nessuna ICO, IEO o vendita pubblica 20](#_Toc201011563)

[11.2. Open source, protocollo neutrale 20](#_Toc201011564)

[11.3. Conformità globale 20](#_Toc201011565)

[11.4. Esclusione di responsabilità 20](#_Toc201011566)

[12. Conclusione 20](#_Toc201011567)

[12.1. Uno sguardo al futuro: Credix 21](#_Toc201011568)

[13. Visione a lungo termine 21](#_Toc201011569)

[14. Contributi e licenza 22](#_Toc201011570)

1. Introduzione

Negli ultimi anni, la crescente adozione delle tecnologie blockchain ha evidenziato non solo le straordinarie potenzialità di questo paradigma decentralizzato, ma anche i limiti strutturali e filosofici di molte implementazioni esistenti. Tra questi, si annoverano problemi di scalabilità, centralizzazione nascosta, costi elevati per le transazioni e una generale difficoltà nel conciliare privacy, trasparenza e semplicità d’uso.

Questo whitepaper presenta una nuova blockchain progettata come riserva di valore digitale resiliente, trasparente e indipendente. L’obiettivo primario è costruire un’infrastruttura decentralizzata accessibile a chiunque, sicura per definizione e sostenibile nel lungo periodo, con particolare attenzione all’equilibrio tra efficienza tecnica, equità di accesso e robustezza crittografica.

Il protocollo è stato ideato per funzionare efficacemente anche su hardware non specializzato, comprese CPU consumer e dispositivi mobili, al fine di massimizzare la decentralizzazione e ridurre le barriere tecniche e finanziarie all’ingresso. La rete adotta un approccio ibrido con full node su PC e light node su smartphone, garantendo interoperabilità e leggerezza.

Al centro della progettazione vi è un meccanismo di consenso Proof of Work (PoW) ottimizzato per resistere agli ASIC, favorendo così un’equa distribuzione della capacità di mining e contrastando fenomeni di centralizzazione. Il sistema è completato da una tokenomics definita da una scarsità programmata lenta, pensata per garantire valore nel tempo senza compromettere l’accessibilità iniziale.

Il nome CRED Standard non è casuale: rappresenta un chiaro richiamo al Gold Standard, il sistema monetario che per oltre un secolo ha ancorato il valore delle valute fiat a una riserva concreta e verificabile.

Allo stesso modo, CRED Standard si propone come nuova base decentralizzata per un valore digitale ancorato alla scarsità programmata, alla trasparenza del codice e alla fiducia distribuita.

“CRED” evoca credibilità, fiducia e credito sociale, mentre “Standard” indica la volontà di offrire una misura stabile, verificabile e condivisa del valore, destinata a durare nel tempo, oltre le logiche speculative.

In un contesto dominato da inflazione, manipolazioni monetarie e sfiducia sistemica, CRED Standard vuole essere ciò che fu l’oro per le economie del passato: una base solida e imparziale su cui costruire libertà economica e cooperazione globale.

1. Il problema

Nonostante l’esistenza di numerose blockchain affermate, il settore continua a soffrire di criticità strutturali che ne limitano l’efficacia come vera alternativa ai sistemi finanziari e informatici centralizzati. Tra i problemi più rilevanti si evidenziano:

* Centralizzazione del mining: l’adozione massiva di ASIC e il predominio di grandi mining pool hanno concentrato il potere computazionale in poche mani, minando la promessa originaria di decentralizzazione.
* Costi di transazione elevati: in molte reti consolidate, il costo per singola transazione è diventato proibitivo, scoraggiando l’uso quotidiano e l’inclusione finanziaria.
* Scarsa accessibilità ai nodi: la crescente complessità e i requisiti hardware elevati dei full node hanno escluso utenti comuni dalla possibilità di partecipare attivamente alla rete.
* Trasparenza in conflitto con la privacy: molte blockchain pubbliche offrono totale trasparenza delle transazioni, ma non prevedono meccanismi nativi per la riservatezza selettiva, rendendo difficile conciliare esigenze legittime di privacy.
* Governance ambigua o opaca: diversi progetti non forniscono meccanismi chiari e democratici per la gestione dell’evoluzione del protocollo, aprendo la strada a decisioni centralizzate o arbitrarie.
* Eccessiva complessità: la proliferazione di feature non essenziali e l’adozione di sistemi tecnicamente sofisticati ma poco comprensibili rendono molte blockchain difficili da analizzare, verificare e utilizzare da parte della comunità.

Questi limiti impediscono a molte blockchain di fungere da strumenti realmente democratici, trasparenti e duraturi nel tempo. Il progetto qui presentato nasce con l’obiettivo di affrontare in modo diretto e sistemico tali criticità.

1. Soluzione proposta

La blockchain proposta rappresenta una risposta concreta e mirata alle principali problematiche che affliggono i sistemi distribuiti esistenti. Essa è stata progettata per essere un’infrastruttura digitale essenziale, solida e durevole, con l’obiettivo dichiarato di diventare una riserva di valore decentralizzata, resistente alla censura e accessibile a livello globale.

I pilastri su cui si fonda il protocollo sono:

1. Decentralizzazione reale

Il sistema è strutturato per essere operabile su hardware consumer, evitando la dipendenza da dispositivi ASIC o configurazioni specialistiche. La rete è composta da:

* Full node: eseguibili su PC desktop e server tradizionali, che mantengono l’intera blockchain e partecipano attivamente al consenso.
* Light node: eseguibili su smartphone e dispositivi leggeri, che verificano solo l’ultima parte della blockchain e si affidano a full node selezionati per la validazione, mantenendo la sicurezza attraverso SPV (Simplified Payment Verification).

1. Consenso PoW anti-ASIC

Il protocollo utilizza un algoritmo di Proof of Work progettato per resistere all’ottimizzazione via ASIC, incentivando così una partecipazione equa da parte di utenti dotati di CPU e GPU standard. Il tempo di blocco è fissato a 2,5 minuti, bilanciando efficienza e sicurezza.

1. Transazioni gratuite con reward dinamico per transazione

Il sistema non impone fee all’utente, ma integra un meccanismo chiamato reward dinamico per transazione:

* Ogni transazione inclusa in un blocco genera un piccolo incentivo aggiuntivo per il miner, calcolato a livello protocollo.
* Questo incentivo proviene direttamente dall’emissione monetaria, non è prelevato dall’utente.
* In caso di congestione, è possibile includere fee opzionali per aumentare la priorità, mantenendo il principio di accessibilità universale.
* Il meccanismo funge anche da protezione contro lo spam, dato che ogni transazione ha un costo computazionale per

1. Scarsità programmata

La tokenomics è strutturata per favorire la rivalutazione nel lungo periodo, con un reward iniziale di 50 unità per blocco, soggetto a halving ogni 500.000 blocchi. Questo modello rallenta la curva di emissione rispetto ad altre criptovalute, incentivando la conservazione e riducendo l’inflazione.

1. Privacy modulabile

Il protocollo integra meccanismi opzionali per la riservatezza selettiva delle transazioni, permettendo agli utenti di scegliere se rendere pubblici o anonimi determinati dettagli, nel rispetto della legalità e della trasparenza controllata.

1. Semplicità e verificabilità

Il codice della blockchain sarà open source, leggibile e documentato, al fine di garantire auditabilità pubblica, ispezione continua da parte della comunità e facilità di adozione per sviluppatori indipendenti.

1. Architettura tecnica

L’architettura della blockchain proposta è concepita per garantire robustezza, scalabilità, accessibilità e sicurezza. Ogni componente è stato progettato con criteri di essenzialità, verificabilità e sostenibilità.

* 1. Meccanismo di consenso: Proof of Work (PoW) anti-ASIC

Il protocollo adotta un algoritmo di Proof of Work appositamente studiato per resistere all’ottimizzazione tramite ASIC, favorendo l’utilizzo di CPU e GPU consumer. L’algoritmo, caratterizzato da un’elevata intensità di memoria e varietà computazionale, rende economicamente svantaggioso lo sviluppo di hardware dedicato, preservando così la distribuzione equa della capacità di mining.

* Tempo medio di blocco: 2,5 minuti
* Algoritmo proposto: [Nome da definire] – derivato o ispirato a RandomX/ProgPoW (personalizzabile)
* Target di difficoltà: regolato dinamicamente ogni N blocchi per mantenere la media temporale
  1. Struttura dei nodi

La rete è composta da due categorie distinte ma interoperabili di nodi:

1. Full Node

* Mantiene l’intera cronologia della blockchain
* Esegue la validazione completa delle transazioni e dei blocchi
* Partecipa attivamente al consenso (mining o validazione passiva)
* Richiede spazio disco e risorse computazionali moderate
* Costituisce il fondamento della sicurezza e dell’integrità della rete

1. Light Node

* Conserva solo le intestazioni degli ultimi 2048 blocchi, per ridurre al minimo l’utilizzo di risorse su dispositivi mobili
* Verifica le transazioni utilizzando SPV (Simplified Payment Verification), tramite prove crittografiche fornite dai full node
* Non partecipa direttamente al consenso, ma consente all’utente di verificare autonomamente la legittimità delle proprie transazioni
* Può interagire con più full node, adottando un modello a quorum per rafforzare la fiducia e mitigare la censura

Nota: anche se i light node non ricevono ricompense dirette dal protocollo di consenso, potranno comunque beneficiare di sistemi di incentivazione esterni, quali:

* ricompense integrate nei wallet mobili
* micropagamenti per funzioni di relay, validazione o supporto alla rete
* airdrop o cashback per utenti attivi

Questi meccanismi, integrabili su livelli superiori (app, servizi di rete, layer 2), hanno lo scopo di:

* promuovere la diffusione capillare dei nodi leggeri,
* incentivare la partecipazione attiva anche da parte di utenti senza competenze tecniche o hardware dedicato, e soprattutto
* massimizzare la decentralizzazione della rete, rendendo la blockchain realmente globale, distribuita e resistente alla censura.
  1. Sicurezza

La sicurezza è garantita da un insieme sinergico di componenti:

* Immutabilità: ogni blocco è legato crittograficamente al precedente tramite hash, garantendo integrità della catena.
* Distribuzione geografica dei nodi: la facilità di esecuzione su hardware generico riduce il rischio di attacchi centralizzati.
* Protezione contro il double-spending: affidata al PoW e alla sincronizzazione dei full node.
* Validazione dei light node: sebbene non conservino la catena completa, possono verificare la legittimità di una transazione in modo autonomo, garantendo fiducia locale.
  1. Transazioni
* Formato essenziale: input, output, timestamp, firma digitale
* Supporto multi-output e multisig
* Transazioni opzionalmente private: mediante tecniche selettive (es. commitment, stealth address, ring signature)
* Priorità automatica: gestita in base al tempo d’ingresso nella mempool e alla presenza eventuale di fee opzionali
* Reward dinamico per transazione: ogni tx include un bonus per il miner, finanziato dall’emissione monetaria
  1. Esempio di ciclo di vita di una transazione

Il seguente esempio descrive passo dopo passo cosa accade quando un utente invia una transazione all’interno della rete CRED Standard.

*1. Creazione della transazione*

L’utente apre il proprio wallet mobile (light node), seleziona il destinatario e l’importo. Il wallet firma digitalmente la transazione e la prepara secondo il formato standard del protocollo.

*2. Trasmissione ai full node*

Il wallet trasmette la transazione a uno o più full node selezionati, attraverso un canale SPV (Simplified Payment Verification). Non tutta la blockchain è scaricata localmente, ma il light node conserva l'intestazione degli ultimi blocchi per validare la coerenza delle risposte.

*3. Verifica e inserimento nella mempool*

Il full node verifica la validità della transazione (firma, disponibilità di fondi, formato, eventuali flag di privacy) e la inserisce nella mempool. Se ci sono fee opzionali, ne tiene conto per la priorità.

*4. Inclusione nel blocco*

Un miner seleziona transazioni dalla mempool per costruire un nuovo blocco, includendo la transazione dell’utente. Al momento del mining, il blocco assegna al miner:

* il reward base (es. 50 CRED);
* un reward dinamico proporzionale al numero di transazioni (senza prelevarlo dall’utente).

*5. Propagazione e conferma*

Il blocco viene propagato nella rete. Una volta che i nodi lo verificano, la transazione è confermata. Il wallet dell’utente mostra lo stato “completato” dopo la prima conferma, e può opzionalmente attendere più conferme per maggiore sicurezza.

*6. Verifica successiva tramite SPV*

Il light node verifica l’effettiva inclusione del blocco attraverso i Merkle proof ricevuti dal full node, assicurandosi che la transazione sia legittima anche senza avere l'intera blockchain in locale.

*7. Stato finale*

Il saldo del destinatario viene aggiornato. Se la transazione era privata (es. con indirizzo stealth o output nascosto), solo mittente e destinatario conoscono i dettagli reali. La rete conserva comunque l'integrità e l’immutabilità del record.

1. Riepilogo tecnico per sviluppatori

Questa sezione fornisce una panoramica sintetica degli aspetti tecnici essenziali per sviluppatori e contributori interessati all’implementazione, all’hosting di nodi o alla verifica del codice sorgente di CRED Standard.

*Algoritmo di consenso:*

Proof of Work basato su Yespower, progettato per resistere all’ottimizzazione ASIC. Memory-hard, CPU-friendly, compatibile con hardware consumer.

*Linguaggio di implementazione:*

Core in C++ (compatibile con derivazioni Bitcoin Core), con interfacce REST e API estendibili. Componenti leggeri (es. light wallet) scritti in JavaScript / TypeScript e supporto per versioni mobili (Android/iOS) via librerie native.

*Distribuzione e client:*

Il codice sarà ospitato su GitHub in un repository open source con licenza MIT. Saranno distribuiti:

* Eseguibili CLI per Linux/Windows/macOS
* Immagini Docker ufficiali per nodo full
* Wallet light per mobile (in fase successiva)

*Requisiti minimi nodo full:*

* CPU dual-core (64-bit)
* 4 GB RAM
* 50 GB spazio su disco
* Connessione stabile con IP pubblico (consigliato)

*Struttura del progetto*

bash

CopiaModifica

/src → codice sorgente core (C++)

/docs → documentazione tecnica

/scripts → tool CLI, build, gestione nodi

/wallet-light → codice JS/TS del light wallet

/api → endpoint REST e documentazione OpenAPI

/docker → file Dockerfile e compose

/test → suite di test unitari e integrazione

Questa struttura sarà accompagnata da una guida README.md, una documentazione tecnica completa (docs/spec.md) e da istruzioni per l’installazione rapida (install.md).

1. Specifiche tecniche del protocollo

Il protocollo CRED Standard è progettato per essere semplice da verificare, solido nella struttura e coerente con i principi di accessibilità e trasparenza. Di seguito si riportano le specifiche tecniche fondamentali.

* 1. Struttura del blocco

Ogni blocco contiene:

* Version: numero della versione del blocco
* Previous Block Hash: hash del blocco precedente (collega la catena)
* Merkle Root: radice dell’albero delle transazioni
* Timestamp: data e ora di creazione del blocco
* Difficulty Target: livello di difficoltà corrente
* Nonce: valore variabile per trovare un hash valido
* ExtraNonce: campo libero usato per segnature opzionali o metadata
* Transactions: lista di tutte le transazioni incluse
  1. Formato delle transazioni

Ogni transazione contiene:

* Input[]: riferimenti a output precedenti (come in Bitcoin)
* Output[]: nuovi destinatari e importi
* Locktime: opzionale, per transazioni temporizzate
* Signature: firma crittografica dell’utente
* Flags opzionali: indicano privacy selettiva (es. indirizzi stealth, ring signature)

Le transazioni possono essere:

* Standard: completamente visibili
* Private selettive: con mascheramento degli importi, indirizzi o struttura
  1. Algoritmo di consenso
* Tipo: Proof of Work (PoW)
* Algoritmo: Yespower (o derivato, selezionabile via parametri di build)
* Difficoltà: aggiustata dinamicamente ogni N blocchi per mantenere media 2,5 minuti
* Resistenza ASIC: alta (algoritmo memory-hard e anti-parallelizzazione)
  1. Crittografia e hash
* Hashing delle transazioni: SHA-256 doppio
* Merkle tree: SHA-256 per le foglie, hash binari ricorsivi
* Indirizzi: generati da chiavi ECDSA (curve secp256k1)
* Stealth addresses (opzionali): con supporto per chiavi one-time e ricezione anonima
  1. Compatibilità e requisiti minimi
* Requisiti full node: CPU consumer dual core, 4GB RAM, 50+ GB disco
* Requisiti light node (SPV): smartphone o browser con storage minimo, senza database completo
* Protocollo di comunicazione: TCP/IP con struttura P2P classica + estensioni SPV

Queste specifiche potranno essere estese e formalizzate ulteriormente nella documentazione tecnica ufficiale e nei file di implementazione open source.

* 1. Specifiche di protocollo

La seguente tabella riassume le principali specifiche tecniche del protocollo CRED Standard, in formato sintetico:

|  |  |
| --- | --- |
| **Componente** | **Specifica** |
| Algoritmo PoW | Yespower (memory-hard, ASIC-resistant, ottimizzato per CPU/GPU consumer) |
| Tempo blocco medio | 2,5 minuti (fino al blocco 2.499.999), poi 5 minuti |
| Difficoltà | Regolazione dinamica ogni N blocchi per stabilizzare il tempo medio |
| Struttura blocco | Header (version, prevHash, merkleRoot, timestamp, difficulty, nonce) + lista transazioni |
| Formato transazione | Input[] – Output[] – Firma digitale – Locktime – Flag privacy opzionali |
| Supporto privacy | Indirizzi stealth, ring signature, commitment selettivi (opzionale) |
| Hashing | SHA-256 doppio (tx, blocchi, Merkle tree) |
| Crittografia | ECDSA – curva secp256k1 per firme e indirizzi |
| Formato indirizzi | crd1... (prefisso custom base32 per identificare CRED Standard) |
| SPV | Supportato tramite intestazioni blocchi + Merkle proof |
| Nodo leggero | Conserva le header degli ultimi 2048 blocchi, verifica con quorum full node |

1. Tokenomics

L’asset nativo della blockchain si chiama CRED. Esso rappresenta l’unità di misura del valore all’interno della rete, utilizzata per le transazioni, il mining e i sistemi di incentivazione.

La tokenomics di CRED è progettata per garantire scarsità programmata, distribuzione equa e sostenibilità a lungo termine, senza ricorrere a pre-mine, vendita privata o assegnazioni privilegiate. Tutti i CRED in circolazione sono creati esclusivamente attraverso il processo di mining, a fronte di reale lavoro computazionale.

* 1. Emissione
* Block reward iniziale: 50 CRED
* Halving: ogni 500.000 blocchi
* Reward minimo garantito: 1 CRED per blocco, attivo a partire dal sesto ciclo di halving (~12 anni)
* Meccanismo di emissione: asintotico; la quantità totale di CRED tende a un limite nel tempo, ma senza un hard cap esplicito
* Distribuzione: il 100% dei CRED viene emesso tramite mining; non sono previsti pre-mine, ICO, fondi riservati o ricompense iniziali
  1. Transizione programmata del tempo di blocco

Per bilanciare adozione iniziale e sostenibilità futura, il protocollo prevede un cambio programmato del tempo medio di blocco:

* Fase iniziale (blocchi 0 – 2.499.999): tempo medio per blocco = 2,5 minuti
* Fase successiva (dal blocco 2.500.000 in poi): tempo medio per blocco = 5 minuti

Questa transizione ha lo scopo di:

* Accelerare l’emissione e incentivare l’attività nei primi anni
* Ridurre gradualmente il ritmo di emissione nel lungo termine
* Migliorare l’efficienza della rete, stabilizzandone il funzionamento
  1. Incentivi
* Miner: ricevono la block reward e un reward dinamico per transazione, proporzionale al numero di transazioni incluse nel blocco, prelevato dalla stessa emissione e non dagli utenti
* Light node: non partecipano alla creazione monetaria, ma possono accedere a sistemi di incentivazione esterni (es. cashback, micropagamenti, premi integrati nei wallet) per favorire la diffusione della rete
  1. Sostenibilità

Il modello è concepito per essere:

* prevedibile: l’emissione è pubblica, codificata e immutabile senza consenso collettivo
* distribuito: chiunque, con hardware consumer, può contribuire al mining e ottenere CRED
* libero da interessi centralizzati: nessuna entità controlla la moneta, né all’origine né nel futuro

1. Vantaggi competitivi

CRED nasce con l’ambizione di essere una riserva di valore decentralizzata, sostenibile e realmente accessibile. Il progetto si distingue nel panorama blockchain per una serie di caratteristiche tecniche e filosofiche che ne rafforzano l’unicità e la solidità.

* 1. Decentralizzazione reale
* Nessun pre-mine, vendita privata o assegnazione privilegiata
* Algoritmo PoW resistente agli ASIC, ottimizzato per CPU e GPU consumer
* Architettura a doppio livello con light node su smartphone per massimizzare la distribuzione globale della rete
  1. Transazioni gratuite
* Nessuna fee obbligatoria: le transazioni sono accessibili a tutti, senza discriminazioni economiche
* Reward dinamico per transazione integrato nel protocollo per incentivare i miner senza gravare sugli utenti
  1. Sostenibilità a lungo termine
* Emissione monetaria asintotica, con reward minimo garantito: il mining è sempre incentivato
* Cambio programmato del tempo di blocco per adattare la rete all’evoluzione del progetto
* Nessun affidamento esclusivo su commissioni di transazione per la sicurezza futura
  1. Privacy modulabile

Gli utenti possono scegliere se rendere pubblici o anonimi alcuni aspetti delle transazioni, nel rispetto della legalità e del controllo individuale dei dati

* 1. Semplicità e trasparenza
* Codice open source, leggibile e documentato, auditabile dalla comunità
* Protocollo snello, pensato per essere compreso e verificato da chiunque, non solo da esperti
  1. Incentivi anche per i light node
* 1mobili o nei layer superiori
* Meccanismo studiato per promuovere una partecipazione diffusa e incentivata, anche senza potere computazionale

Questa combinazione di accessibilità, sostenibilità, trasparenza e inclusività rende CRED una blockchain progettata non solo per durare, ma per prosperare in un ecosistema decentralizzato, equo e globale

1. Roadmap

La roadmap di CRED è costruita per garantire una crescita progressiva, trasparente e verificabile. Ogni fase mira a consolidare la rete, testarne la resilienza e favorire l’adozione senza compromettere i principi di decentralizzazione, sicurezza e sostenibilità.

1. Ricerca e progettazione (completata / in corso)

* Definizione degli obiettivi strategici e delle caratteristiche fondamentali della blockchain
* Stesura del whitepaper e revisione tecnica
* Analisi comparativa con altri protocolli PoW
* Modellazione della tokenomics e dei meccanismi

1. Sviluppo del protocollo base

* Implementazione del core della blockchain: mining, consenso, transazioni, validazione
* Creazione del primo full node di riferimento (CLI + API)
* Supporto per light node e architettura SPV su dispositivi mobili
* Testnet privata per validazione tecnica iniziale

1. Testnet pubblica

* Lancio di una testnet aperta a sviluppatori e early adopter
* Stress test, bug bounty e audit comunitario del codice
* Verifica della difficoltà, sincronizzazione dei nodi e meccanismi di sicurezza
* A/B testing su varianti di reward dinamico e tempo di blocco

1. Lancio della mainnet

* Avvio della blockchain principale (mainnet) con reward iniziale di 50 CRED/blocco
* Nessun pre-mine, tutti i blocchi minati pubblicamente fin dal blocco 0
* Pubblicazione di client ufficiali: full node, light node e wallet mobile
* Monitoraggio continuo e aggiornamenti correttivi in caso di necessità

1. Ecosistema e adozione

* Integrazione con wallet hardware e multi-chain
* Supporto per strumenti di sviluppo (SDK, documentazione API, librerie)
* Incentivi per installazione di light node tramite wallet e campagne partner
* [Opzionale ma strategico] Sviluppo di un wallet ufficiale open source, leggero e mobile, per eseguire light node, gestire CRED e visualizzare i reward
* Coinvolgimento della comunità per sviluppo di interfacce user-friendly
* Supporto architetturale per servizi Layer 2, come micropagamenti, token secondari, reputazione o DEX: non prioritari nella fase iniziale, ma pienamente compatibili con l’evoluzione del protocollo

1. Governance distribuita e adattiva

* Studio e possibile implementazione di un sistema di proposta e voto on-chain
* Meccanismi trasparenti per aggiornamenti futuri, modifiche a parametri critici e utilizzo di fondi comunitari (se introdotti)
* Monitoraggio dell’equilibrio tra decentralizzazione, sicurezza e performance

Questa roadmap è concepita come modulare e adattiva: ogni fase viene avviata solo dopo la piena validazione della precedente. La trasparenza nello sviluppo e nella comunicazione sarà un pilastro costante del progetto.

1. Team e governance

CRED nasce con l’obiettivo di essere una blockchain completamente decentralizzata, neutrale e resistente alla manipolazione. Per questo motivo, il progetto non prevede alcun sistema di governance attiva o centralizzata, né temporanea né permanente.

* 1. Nessuna governance on-chain o off-chain
* Non esistono meccanismi di voto, controllo del protocollo o interventi diretti da parte di sviluppatori, enti o fondatori.
* Il codice sorgente è pubblico, immutabile e soggetto solo al consenso della rete: nessuna modifica può essere applicata senza aggiornamento volontario da parte di tutti i partecipanti.
* Eventuali miglioramenti futuri potranno essere proposti pubblicamente, ma l’adozione avverrà solo tramite aggiornamento spontaneo del software da parte degli utenti (come avviene in Bitcoin).
  1. Anonimato e contributo aperto
* CRED è un progetto senza fondatori identificati: chiunque può contribuire, sviluppare strumenti, proporre miglioramenti o creare derivazioni.
* Il codice sarà ospitato in repository open source, supervisionato dalla comunità senza gerarchie o comitati centrali.

1. Aspetti legali e conformità

CRED è un protocollo decentralizzato e open source, privo di entità giuridica, struttura societaria o controllo centralizzato. Non effettua raccolte fondi, distribuzioni privilegiate o vendita diretta di asset. Di conseguenza, il progetto si colloca fuori dall’ambito delle normative finanziarie tradizionali.

* 1. Nessuna ICO, IEO o vendita pubblica
* CRED non ha mai effettuato, né effettuerà, Initial Coin Offering (ICO), Initial Exchange Offering (IEO) o qualsiasi forma di collocamento iniziale a pagamento.
* Tutti i CRED in circolazione vengono emessi esclusivamente tramite Proof of Work, attraverso un processo equo e accessibile a tutti.
  1. Open source, protocollo neutrale
* Il codice sorgente è disponibile pubblicamente e può essere ispezionato, utilizzato, copiato o modificato secondo i termini della licenza open source scelta (es. MIT, GPL o simile).
* Nessuna parte del protocollo obbliga l’utente a fornire dati personali, né raccoglie informazioni sensibili.
* CRED non fornisce servizi finanziari, né funge da intermediario per alcuna attività regolamentata.
  1. Conformità globale
* Poiché CRED è una rete decentralizzata senza gestione centralizzata, la responsabilità legale di utilizzo ricade interamente sui singoli partecipanti.
* Gli sviluppatori iniziali non hanno alcun controllo sui CRED generati né sulla rete dopo il lancio.
* L’utilizzo di CRED deve avvenire nel rispetto delle leggi locali di ciascun utente.
  1. Esclusione di responsabilità
* CRED non costituisce un prodotto di investimento, né una promessa di rendimento.
* Nessuna garanzia è fornita in merito alla stabilità del valore, alla continuità tecnica o alla futura adozione della rete.

1. Conclusione

CRED è una blockchain progettata per incarnare i principi originari delle reti decentralizzate: equità, accessibilità, sicurezza e indipendenza. In un panorama sempre più dominato da soluzioni complesse, centralizzate o orientate al profitto di pochi, CRED si distingue come strumento essenziale, sobrio e sostenibile, pensato per durare.

La rete è costruita per:

* essere veramente decentralizzata, grazie a un algoritmo PoW accessibile e nodi leggeri operabili anche da smartphone
* offrire transazioni gratuite senza compromettere la sicurezza economica del sistema, grazie al reward dinamico integrato
* garantire una tokenomics stabile e trasparente, senza pre-mine né emissioni privilegiate
* evolvere senza imposizioni, attraverso un protocollo immutabile, pubblico e senza governance centralizzata

CRED non nasce per promettere guadagni facili o rivoluzioni effimere. Nasce per offrire una base solida, verificabile e accessibile a chiunque voglia costruire, scambiare, conservare o semplicemente partecipare a una rete globale libera.

In un’epoca di sfiducia, complessità e manipolazione, CRED propone una via diversa: essenziale, concreta, aperta.

* 1. Uno sguardo al futuro: Credix

CRED Standard nasce come riserva di valore decentralizzata, ma il progetto prevede un’estensione futura: Credix, una moneta derivata ancorata al valore di CRED, pensata per l’uso quotidiano e le microtransazioni.

Credix sarà frazionabile in unità familiari, stabili e spendibili (es. fino ai centesimi), ma sempre coperta da riserva.

Non sarà listata né scambiata liberamente: il suo unico scopo sarà offrire stabilità d’uso senza compromettere la natura scarsa e durevole di CRED.

Questa dualità – CRED come riserva e Credix come strumento di spesa – rappresenta una visione più ampia: creare un’infrastruttura monetaria completa, decentralizzata, trasparente e accessibile a tutti, fondata sul principio del “CRED Standard”.

1. Visione a lungo termine

CRED Standard nasce per rispondere a problemi urgenti legati alla centralizzazione, all’inflazione e alla perdita di fiducia nei sistemi economici tradizionali. Tuttavia, la sua architettura essenziale e scalabile è pensata per durare nel tempo, adattandosi a contesti sociali, tecnologici e normativi in continua evoluzione.

Nel lungo termine, CRED Standard punta a:

* Diventare un riferimento stabile e verificabile per il valore digitale, analogo a ciò che fu l’oro nel sistema monetario tradizionale.
* Supportare un’economia decentralizzata mista, in cui CRED svolge il ruolo di riserva e unità di conto, mentre valute derivate come Credix fungono da strumenti di spesa e scambio quotidiano.
* Favorire l’inclusione globale, consentendo anche a utenti senza competenze tecniche o mezzi economici di partecipare alla rete tramite nodi leggeri e wallet mobili.
* Evolvere senza governance centralizzata, attraverso un codice pubblico, immodificabile senza consenso della rete, e aggiornamenti volontari da parte della comunità.
* Mantenere la coerenza con i principi fondanti: nessun controllo centralizzato, nessuna manipolazione monetaria, nessuna discriminazione economica.

In definitiva, l’obiettivo è quello di fornire una base monetaria condivisa, trasparente e resiliente, in grado di supportare nuove forme di cooperazione economica, di risparmio e di scambio in un mondo sempre più interconnesso ma instabile.

1. Contributi e licenza

Il progetto CRED Standard è sviluppato in modalità open source, senza gerarchie, comitati centrali o controlli proprietari. Chiunque può contribuire al codice, proporre miglioramenti o creare fork del protocollo, nel rispetto delle regole comunitarie.

*Come contribuire*

* Tutto il codice sorgente sarà disponibile pubblicamente su GitHub.
* Saranno fornite istruzioni dettagliate per installare nodi, eseguire test e aprire pull request.
* È incoraggiata la partecipazione volontaria tramite sviluppo, testing, documentazione, traduzione o diffusione.
* Le discussioni tecniche avverranno tramite issue tracker, forum tecnici e (opzionalmente) canali federati come Mastodon o Matrix.

*Licenza*

* Il codice di CRED Standard sarà rilasciato sotto licenza MIT: una delle licenze open source più permissive, compatibile con progetti commerciali e non.
* Gli utenti sono liberi di utilizzare, copiare, modificare, distribuire o forkare il codice, purché venga mantenuta la nota di copyright e la licenza originale.

*Clausole etiche*

Anche se non vincolanti a livello giuridico, si invita chi partecipa al progetto a:

* rispettare il principio di decentralizzazione come valore fondante;
* non utilizzare CRED Standard per attività contrarie alla libertà, alla trasparenza e alla giustizia economica;
* contribuire con spirito collaborativo e senza scopi speculativi a breve termine.