White Paper Istituzionale Annurax Chain e ANRX

Tecnologia governance economia e perimetro legale

Versione 0.10 per revisione legale e audit

31 ottobre 2026

Elemento	Stato dichiarato
Rete	Software e infrastruttura Testnet verificati in ambito controllato; Mainnet non autorizzato
Token	ANRX nativo con supply massima proposta di 1.000.000.000 unità, da creare una sola volta al genesis
Emittente	Struttura proposta: Superlab Technologies El Salvador S.A.S. in associazione e per conto di Superlab Technologies Georgia LLC; da validare legalmente
Documento	Informativo e tecnico; non costituisce offerta, prospetto, promessa di rendimento o autorizzazione al lancio

Questo documento definisce il progetto e le condizioni di avvio. Le sezioni legali descrivono un percorso di conformità e non sostituiscono un parere professionale nelle giurisdizioni di offerta, negoziazione, custodia o prestazione di servizi.

Indice dei contenuti

- 1 Sintesi per il lettore istituzionale
- 2 Stato del progetto e limiti delle evidenze
- 3 Architettura della rete
- 4 ANRX funzioni diritti e limiti
- 5 Supply allocazione e circolazione
- 6 Wallet Master e gestione delle chiavi
- 7 Validatori governance e percorso bancario
- 8 Commissioni e sostenibilità economica
- 9 Sicurezza audit e continuità operativa
- 10 Inquadramento giuridico proposto
- 11 Rischi principali
- 12 Roadmap verso il Mainnet
- 13 Informazioni da congelare prima del genesis
- 14 Riferimenti ufficiali

Registro dello stato delle affermazioni

Categoria	Significato nel documento
Osservato	Risultato supportato da codice, test, release, runtime o documento verificato.
Decisione	Scelta espressa da Count Oceanus, soggetta ai gate legali e tecnici indicati.
Raccomandazione	Soluzione proposta per sicurezza, credibilità istituzionale o sostenibilità.
Da decidere	Dato che non può essere inserito nel genesis o presentato come definitivo prima dell'approvazione.

1 Sintesi per il lettore istituzionale

Annurax Chain è progettata come rete pubblicamente verificabile con validazione istituzionale permissioned. Il modello obiettivo prevede trentuno validatori a peso uguale: trenta banche indipendenti e Superlab. Il consenso richiede almeno ventuno firme su trentuno per finalizzare un blocco. Nessun singolo partecipante può finalizzare o riscrivere il ledger da solo.

ANRX è il token nativo della rete. Serve a pagare il gas, sostenere i servizi di rete e distribuire le commissioni previste dal protocollo. Non è progettato come stablecoin, deposito, moneta elettronica, quota societaria, titolo di debito, quota di fondo o diritto a un rendimento garantito. L'effettiva classificazione giuridica dipende dai diritti, dal marketing, dall'offerta e dalle giurisdizioni coinvolte.

La raccomandazione centrale è separare fin dal genesis gli indirizzi delle riserve, pur derivandoli da una sola frase Master a 24 parole. Questa struttura rende i saldi verificabili nell'Explorer, riduce l'ambiguità contabile e consente a banche e mercato di distinguere la quota personale del fondatore, la tesoreria societaria, la sicurezza, la liquidità e gli incentivi. Non garantisce il prezzo di ANRX, ma rende la gestione più credibile e controllabile.

Il Mainnet con valore reale non deve partire con i trentuno validatori controllati sullo stesso VPS. Una Testnet bancaria può iniziare con undici banche, ma il Mainnet richiede operatori indipendenti, audit esterno concluso, pareri legali, genesis firmato, backup geografico e procedure di emergenza provate.

Conclusioni operative

- Procedere con il wallet BIP39 a 24 parole e derivazione deterministica di indirizzi separati.
- Mantenere le frasi delle banche fuori dai sistemi Superlab: ogni banca genera e custodisce le proprie chiavi e comunica solo dati pubblici e prove di possesso.
- Usare El Salvador come possibile centro di emissione soltanto dopo verifica CNAD e parere sulla struttura tra la società salvadoregna e quella georgiana.
- Trattare MiCA come applicabile quando ANRX viene offerto al pubblico o ammesso alla negoziazione nell'Unione Europea, salvo esenzione o diversa classificazione confermata per iscritto.

2 Stato del progetto e limiti delle evidenze

Area	Stato al 31 ottobre 2026	Limite
Software Chain	Candidato locale e release VPS con 31 processi validatori	Non prova una federazione indipendente
Token Testnet	tANRX senza valore reale usato nei test	Non è ANRX Mainnet
Explorer e portale	Componenti funzionali e verificabili nell'ambiente corrente	La pubblicazione definitiva e la prova da dispositivo restano gate separati
Wallet	Wallet browser ed estensione Testnet; recupero BIP39 a 24 parole implementato in candidato	Non autorizzato per il Master Mainnet prima di audit e cerimonia offline
MFA amministrativa	Supporto TOTP disponibile	Attivazione richiede abbinamento fisico del telefono
Mainnet	Non autorizzato	Mancano operatori indipendenti, audit, pareri, genesis e firma finale

3 Architettura della rete

Annurax Chain utilizza un'architettura applicativa deterministica con consenso BFT. I validatori ordinano e firmano i blocchi; i nodi osservatori, l'Explorer e le API consentono la verifica pubblica senza partecipare al voto. Le chiavi di consenso di un validatore non coincidono con le chiavi che custodiscono ANRX.

Livello	Funzione	Controllo principale
Accesso	Wallet, applicazioni e API	Firma locale, verifica dei dati e protezione dell'utente
Perimetro	RPC, sentry node e protezione del traffico	Rate limit, segmentazione, TLS e difesa DDoS
Consenso	31 validatori a peso uguale	Quorum 21 su 31 e prove di equivocation
Esecuzione	Ledger ANRX, fee, governance e moduli nativi	Regole deterministiche e nessun mint post genesis
Dati	Stato, snapshot, indexer ed Explorer	Replica, hash, backup e restore verificato
Controllo	Metriche, log e incident response	Allarmi, audit trail e responsabilità assegnate

Proprietà e controllo

Superlab conserva proprietà intellettuale, marchio, sviluppo di riferimento e un voto nella federazione. Non può finalizzare un blocco senza quorum, spendere fondi degli utenti, modificare saldi, aggiungere validatori da sola o creare nuovi ANRX dopo il genesis. La credibilità della rete dipende dalla separazione tra proprietà commerciale e controllo del consenso.

4 ANRX funzioni diritti e limiti

- Gas di rete e protezione dallo spam attraverso fee minime e limiti di risorsa.
- Regolamento delle operazioni native e pagamento dei servizi ammessi dal protocollo.
- Distribuzione delle fee ai validatori e ai conti Master e Security secondo regole pubbliche.
- Partecipazione alle funzioni di governance soltanto quando prevista e nei limiti del protocollo.

Diritti che ANRX non attribuisce

Il possesso di ANRX non attribuisce automaticamente proprietà di Superlab, dividendi, interessi, rimborso a valore fisso, tutela dei depositi, diritto a beni di riserva o garanzia di liquidità. Eventuali servizi, vantaggi o diritti aggiuntivi richiedono termini separati e una nuova verifica legale.

Valore e appetibilità

Nessuna struttura tecnica può garantire la crescita del valore di ANRX. Le caratteristiche che possono migliorare la fiducia sono utilità reale, supply verificabile, distribuzione trasparente, liquidità disciplinata, audit pubblico, validatori indipendenti e limiti credibili alla movimentazione delle riserve. Al contrario,

concentrazione opaca, promesse di prezzo e piena trasferibilità immediata di tutte le riserve aumentano il rischio percepito.

5 Supply allocazione e circolazione

La decisione attuale prevede una supply massima di 1.000.000.000 ANRX, creata una sola volta al genesis, con nove decimali e unità base nanrx. Non è previsto mint successivo e le fee non vengono bruciate. La supply totale non coincide con la supply circolante: i token custoditi nelle riserve non diventano circolanti finché non sono trasferiti fuori dai conti controllati.

Allocazione raccomandata da approvare

Indirizzo di destinazione	ANRX	Percentuale	Funzione
Count Oceanus Founder	100.000.000	10%	Quota personale del fondatore, pubblicamente identificata
Superlab Strategic Treasury	200.000.000	20%	Tesoreria strategica dell'emittente e del gruppo
Ecosystem and Adoption	300.000.000	30%	Sviluppo, integrazioni e adozione
Security Reserve	100.000.000	10%	Sicurezza, incidenti e interventi approvati
Liquidity Reserve	100.000.000	10%	Liquidità e market making autorizzato
Validator Incentives	100.000.000	10%	Onboarding e incentivi dei validatori
Contributors and Community	100.000.000	10%	Contributori, comunità e programmi approvati

Raccomandazione: creare tutti gli indirizzi prima del genesis e assegnare direttamente i saldi nel file genesis. Inviare prima tutto all'indirizzo Master e poi redistribuire produrrebbe movimenti iniziali evitabili e renderebbe meno chiaro il controllo economico. Gli indirizzi possono essere derivati dalla stessa frase Master, ma devono apparire separatamente nell'Explorer.

Circolazione iniziale

La raccomandazione è limitare la supply inizialmente circolante a 50.000.000 ANRX, pari al 5% della supply totale. Il saldo può essere composto da 20 milioni per liquidità, 15 milioni per ecosistema, 5 milioni per validatori, 5 milioni per comunità e 5 milioni per operatività. La quantità finale deve derivare dal piano di liquidità e dalle adesioni, non da un obiettivo di prezzo.

Riserve e assenza di lunghi timelock

Count Oceanus ha escluso blocchi temporali rigidi sulle riserve. Senza lock tecnico, ogni riserva è trasferibile da chi controlla la frase Master e la password: il termine riserva descrive quindi una destinazione economica e una policy pubblica, non un vincolo crittografico. Per mantenere credibilità senza ingessare la Chain, si adottano indirizzi separati, limiti operativi configurabili, approvazioni basate sui ruoli, monitoraggio in tempo

reale e pubblicazione trasparente dei trasferimenti materiali. Soglie e procedure potranno essere aggiornate mediante governance documentata, senza imporre un'attesa fissa al movimento dei fondi.

6 Wallet Master e gestione delle chiavi

Il Master wallet usa una frase BIP39 di 24 parole e derivazione BIP32. Una sola frase recupera più sottoconti. Ogni sottoconto ha un indirizzo pubblico e un saldo proprio; non richiede una frase diversa. La derivazione proposta è m/44'/118'/account'/0/index, coerente con lo stack Cosmos. Il coin type 118 deve essere congelato nella specifica prima del Mainnet e non viene presentato come registrazione autonoma Annurax presso SLIP 0044.

Account	Percorso	Uso
0	m/44'/118'/0'/0/0	Master operativo e destinazione del 15% delle fee
1	m/44'/118'/1'/0/0	Count Oceanus Founder
2	m/44'/118'/2'/0/0	Superlab Strategic Treasury
3	m/44'/118'/3'/0/0	Ecosystem and Adoption
4	m/44'/118'/4'/0/0	Security Reserve e 10% delle fee
5	m/44'/118'/5'/0/0	Liquidity Reserve
6	m/44'/118'/6'/0/0	Validator Incentives
7	m/44'/118'/7'/0/0	Contributors and Community

Cerimonia e recupero

1. Generare la frase su un computer offline usando la release firmata e auditata.
2. Trascrivere le stesse 24 parole su due supporti fisici separati e non fotografarle.
3. Eseguire una prova completa di recupero offline e confrontare tutti gli indirizzi pubblici.
4. Salvare sul supporto autorizzato soltanto il wallet cifrato, il manifesto degli indirizzi, gli hash e il verbale.
5. Count Oceanus firma il verbale. Roberto Laurenzi e Paolo Gilli possono attestare data, procedura e hash senza conoscere le 24 parole.

Wallet delle banche

Superlab non deve creare né conoscere le 24 parole di una banca. Il kit nodo deve generare localmente identità e wallet sul sistema della banca o nel suo HSM, mostrare la frase soltanto agli incaricati della banca ed esportare esclusivamente chiave pubblica, node ID, endpoint, indirizzo di payout e firma di una challenge. Un sistema centrale che crea e spedisce seed renderebbe Superlab custode di fatto e indebolirebbe l'indipendenza dei validatori.

7 Validatori governance e percorso bancario

La federazione obiettivo resta composta da trenta banche indipendenti e Superlab. Una no profit, un grande gestore, un'infrastruttura di mercato o una banca centrale potrebbero essere valutati soltanto dopo una modifica formale dei criteri di ammissione. Non devono essere indicati come partecipanti prima di un accordo verificabile.

Fase	Soglia raccomandata	Cosa consente
Pilot iniziale	Almeno 11 banche	Testnet distribuita, prove operative e governance simulata
Testnet istituzionale	31 slot assegnati o in prova	Fault injection, upgrade, recovery e osservabilità pubblica
Mainnet	Operatori indipendenti e nessun controllo comune superiore alla soglia BFT	Avvio con valore reale dopo audit, pareri e genesis firmato
Obiettivo finale	30 banche più Superlab	Federazione conforme al modello dichiarato

Undici banche sono sufficienti per iniziare un pilot, non per giustificare venti validatori Mainnet controllati sullo stesso VPS. Un singolo operatore con undici chiavi può raggiungere la soglia di rischio BFT e con più di dieci nodi può impedire la progressione. Per il Mainnet la distribuzione reale deve precedere il lancio, anche se ciò comporta ritardi.

Soglie di governance proposte

Decisione	Quorum	Attesa
Finalizzazione dei blocchi	21 su 31	Nessuna attesa aggiuntiva
Membership e parametri ordinari	25 su 31	7 giorni
Upgrade binario programmato	25 su 31	14 giorni
Modifiche fondamentali	26 su 31 incluso Superlab	30 giorni
Pausa di emergenza dei gateway	Autorità definita e ratifica 25 su 31	Massimo 72 ore

8 Commissioni e sostenibilità economica

La baseline approvata fissa la commissione minima a 4.500 nanrx per ogni 200.000 unità di gas dichiarate. A un uguale prezzo del token, questo valore nominale è il 10% inferiore alla fee base Solana di 5.000 lamport per una transazione con una firma. La comparazione non garantisce un costo fiat inferiore, perché il prezzo dei token e il carico computazionale possono differire.

La formula minima è max(1, arrotondamento per eccesso del gas dichiarato diviso 200.000) moltiplicato per 4.500 nanrx. Il genesis deve congelare i profili di gas misurati e il prezzo minimo finale. Le operazioni più pesanti possono pagare multipli della fee base secondo una tabella pubblica.

Quota	Destinazione	Regola
75%	Validatori bancari idonei	Distribuzione secondo partecipazione e criteri pubblici
15%	Master Annurax	Sviluppo, coordinamento e operazioni
10%	Security Annurax	Sicurezza e incident response
0%	Burn	Nessun ANRX viene distrutto dalle fee

9 Sicurezza audit e continuità operativa

L'audit deve legarsi a un commit, una configurazione e un pacchetto riproducibile. Una revisione generica del progetto non autorizza il Mainnet. Il fornitore deve ricevere un ambiente isolato, documentazione, codice, test, SBOM, threat model, runbook e risultati precedenti; non deve ricevere le 24 parole Master o chiavi di produzione.

Consegna minima all'auditor

Materiale	Forma di consegna	Contiene segreti
Codice e dipendenze	Repository o archivio firmato con commit, tag, hash e istruzioni di build	No
Pacchetto nodo	Release Linux, container, configurazione di esempio e checksum	No
Architettura e threat model	Diagrammi, trust boundary, consenso, chiavi, upgrade e incidenti	No
Evidenze di test	Report, log selezionati, fault injection, carico, restore e upgrade	No
Ambiente di prova	VPS o laboratorio isolato con credenziali temporanee e logging	Solo credenziali temporanee
Wallet e signing	Test vector, formati cifrati, derivazione HD e transazioni Testnet	Solo seed di test
Questionario e contatti	Responsabili tecnici, finestra di test, regole di disclosure e SLA	No

Indipendenza dell'auditor

Future Italia o un'altra no profit può eseguire una revisione tecnica se dispone di competenze dimostrabili, metodologia, personale identificato, indipendenza dal progetto e responsabilità contrattuale. Se è controllata, finanziata o diretta da soggetti collegati a Superlab, il rapporto va presentato come revisione interna o peer review, non come audit esterno indipendente. Per la credibilità bancaria è preferibile affiancare una società con esperienza pubblica su Layer 1, consenso, crittografia e infrastrutture.

Strategia di audit raccomandata

- Prima fase: CPU ITech o altro revisore infrastrutturale per hardening, deployment, portale, CI, backup e procedure.
- Seconda fase: specialista internazionale Layer 1 e crittografia, ad esempio Trail of Bits, NCC Group o Halborn, selezionato tramite proposta tecnica e conflitti dichiarati.
- Terza fase: retest indipendente sullo stesso commit corretto e pubblicazione di un rapporto con rilievi chiusi, rischi accettati e limiti di perimetro.

10 Inquadramento giuridico proposto

Per classificazione legale si intende stabilire quale insieme di norme si applica ad ANRX e alle attività collegate. Le categorie da escludere o confermare includono crypto asset diverso da stablecoin, utility token, asset referenced token, e money token, strumento finanziario, valore mobiliare, deposito, servizio di pagamento e virtual asset oggetto di servizi VASP. La classificazione dipende dai diritti e dal modo in cui ANRX viene offerto, non dal nome scelto nel white paper.

El Salvador

La Ley de Emisión de Activos Digitales disciplina le offerte pubbliche di asset digitali effettuate nel territorio di El Salvador e regola emittenti, fornitori e altri partecipanti. La CNAD indica che una registrazione pubblica richiede il Documento de Información Relevante, un rapporto di un certificatore registrato e la partecipazione dei soggetti abilitati previsti dal procedimento. Anche un'offerta privata a investitori qualificati segue requisiti e notifica specifici.

La struttura proposta individua Superlab Technologies El Salvador S.A.S. come emittente in associazione e per conto di Superlab Technologies Georgia LLC. Prima di usarla occorre verificare esistenza e poteri societari, mandato o accordo tra le due società, titolarità della proprietà intellettuale, responsabilità verso gli acquirenti, trattamento fiscale, contabilità della supply e percorso CNAD applicabile.

Georgia

La National Bank of Georgia include tra i servizi su virtual asset convertibili lo scambio, il trasferimento, la custodia o amministrazione, la gestione di piattaforme, il lending e l'offerta iniziale o i servizi collegati. Superlab Technologies Georgia LLC deve ottenere un parere scritto su quali attività svolge direttamente e se richiedono registrazione VASP o altra autorizzazione. ANRX non è descritto come stablecoin, ma ogni funzione effettiva deve essere valutata.

Unione Europea e MiCA

Costituire l'emittente in El Salvador non sottrae automaticamente un'offerta rivolta all'Unione Europea al Regolamento MiCA. Per un crypto asset diverso da asset referenced token ed e money token, MiCA può richiedere persona giuridica, white paper, notifica, pubblicazione, comunicazioni corrette e rispetto delle regole per l'ammissione alla negoziazione. Le esenzioni dipendono da condizioni precise e non devono essere usate senza parere legale.

Classificazione tecnica raccomandata

Sulla base delle funzioni oggi descritte, ANRX dovrebbe essere presentato tecnicamente come crypto asset nativo di rete senza peg e senza diritti finanziari garantiti. Questa è una descrizione progettuale, non una conclusione legale. Il parere finale deve analizzare tokenomics, fee ai validatori, governance, marketing, distribuzione iniziale e mercati target.

11 Rischi principali

Rischio	Effetto possibile	Mitigazione richiesta
Concentrazione dei validatori	Censura, arresto o perdita di fiducia	Operatori, provider, gruppi e giurisdizioni indipendenti
Compromissione del Master	Perdita o movimento delle riserve	Cerimonia offline, copie fisiche, file cifrato, limiti e monitoraggio
Bug di consenso o esecuzione	Fork, blocco o stato errato	Audit, fuzzing, test distribuiti, upgrade governato e rollback
Errore legale di classificazione	Sanzioni, stop all'offerta o responsabilità	Pareri scritti per El Salvador, Georgia e mercati target
Liquidità insufficiente	Volatilità e impossibilità di uscita	Piano di liquidità trasparente senza promesse di prezzo
Riserve immediatamente trasferibili	Rischio di overhang e conflitto	Conti pubblici, policy, soglie e preavviso
Wallet utente	Furto da phishing o perdita della frase	PWA verificata, firma locale, educazione, recovery e passkey per servizi web
Dipendenze operative	Outage comune o perdita dati	Backup geografico cifrato e prove di restore

12 Roadmap verso il Mainnet

Fase	Esito necessario
Wallet e portale	BIP39 a 24 parole, PWA installabile, MFA amministrativa attiva e prova completa dal dispositivo di presentazione
Pilot bancario	Almeno 11 banche su Testnet, nodi indipendenti, chiavi locali, metriche e incident exercise
Federazione	Trentuno operatori conformi o configurazione alternativa formalmente approvata e pubblicata
Audit	Codice, consenso, wallet, portale e infrastruttura auditati; rilievi critici e alti chiusi; retest completato
Legale	Emittente, classificazione, white paper, giurisdizioni e condizioni di offerta approvati
Genesis	Indirizzi, supply, allocazioni, fee, governance, timestamp, hash e firme congelati
Cerimonia	Master creato offline, verbale firmato, input pubblici dei validatori verificati
Avvio	Mainnet autorizzato da Count Oceanus dopo tutti i gate, seguito da stabilizzazione e reporting pubblico

13 Informazioni da congelare prima del genesis

- Identità giuridica definitiva dell'emittente e accordo tra Superlab El Salvador e Superlab Georgia.
- Chain ID, timestamp del genesis, versione binaria e hash della release.
- Indirizzi pubblici di tutte le allocazioni e destinazioni delle fee.
- Percentuale personale Founder e allocazione completa approvata.
- Supply circolante iniziale e regole di rilascio delle riserve.
- Profili di gas misurati, minimum gas price definitivo e fee Asset Factory.
- Elenco, chiavi pubbliche, node ID, endpoint e payout dei validatori.
- Quorum, attese di governance, autorità di emergenza e procedura di revoca.
- Rapporto audit, retest, SBOM, threat model e piano incident response.
- Verbale della cerimonia e firme degli operatori sul genesis candidate.

14 Riferimenti ufficiali

- **El Salvador Ley de Emisión de Activos Digitales:** https://www.asamblea.gob.sv/sites/default/files/documents/decretos/0CDA225C-1B6C-4098-AC3A-D608933C643B.pdf
- **CNAD Domande frequenti su emittenti ed emissioni:** https://cnad.gob.sv/es/preguntas-frecuentes/
- **CNAD Marco normativo:** https://cnad.gob.sv/es/portal-de-transparencia/marco-normativo/
- **National Bank of Georgia VASP Supervision:** https://nbg.gov.ge/en/page/virtual-asset-service-providers-vasps
- **Regolamento UE 2023 1114 MiCA:** https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng
- **ESMA MiCA:** https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica
- **CometBFT Documentation:** https://docs.cometbft.com/
- **Cosmos SDK Documentation:** https://docs.cosmos.network/sdk/latest
- **BIP 0039 Mnemonic code:** https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- **BIP 0032 Hierarchical deterministic wallets:** https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki
- **Solana Transaction Fees:** https://solana.com/docs/core/fees
- **NIST SP 800 57 Part 1 Revision 5:** https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final
- **Trail of Bits Blockchain Security:** https://trailofbits.com/services/blockchain/
- **NCC Group Public Blockchain Security Reports:** https://www.nccgroup.com/research/public-report-zcash-zebra-security-assessment/
- **Halborn Blockchain Layer 1 Assessment:** https://www.halborn.com/solutions/blockchain-layer-1-assessment

Approvazioni ancora necessarie

La pubblicazione come white paper di offerta, il lancio Mainnet, la creazione degli ANRX reali e l'ammissione alla negoziazione richiedono approvazioni separate. Fino ad allora il documento descrive il progetto, le decisioni assunte e le raccomandazioni da sottoporre a legali, auditor e partecipanti istituzionali.