

CARGE

L'Infrastructure Blockchain pour Workflows IA-Humains Vérifiables

Conçu pour l'Audit & la Conformité

Technologie Opérationnelle - Phase de Validation Go-to-Market

La solution est développée et fonctionnelle

Statut actuel : TRL 7 (Technology Readiness Level 7)

- **Blockchain Ragchain** : Opérationnelle avec pallets RAG, PKI et CryptoTrail déployés
- **Human Context Protocol (MCP)** : Validé et fonctionnel avec agents IA (Claude, Mistral, Cursor)
- **Interface carge.fr** : En production avec workflows IA-humains actifs
- **Workflows hybrides** : Collaboration IA-humains testée et validée techniquement

Objectif Phase 1 France 2030 : La technologie est développée. L'enjeu est maintenant la validation du go-to-market :

- Identifier des cas d'usage métier prioritaires (finance, santé, industrie)
- Déployer 3 workflows en conditions réelles
- Valider la conformité réglementaire (audit DORA/RGPD/AI Act)
- Mesurer les gains opérationnels et économiques

Aucun développement requis : 100% validation terrain

Vision et Positionnement

Infrastructure blockchain pour processus métier vérifiables

Solution décentralisée pour workflows humains-IA avec preuves cryptographiques. Architecture zero-trust garantissant la conformité réglementaire (RGPD, AI Act, DORA) via horodatage blockchain et chiffrement de bout en bout.

Chiffres Clés

Métrique	Valeur
Vérifiable	100% On-Chain
Standards	W3C Conforme
Stockage	IPFS Décentralisé
Sécurité	\$250M+ stake (Symbiotic)

Contexte et Problématique

Risques réglementaires des processus IA non traçables

Exposition financière croissante :

- RGPD** : amendes jusqu'à 4% du CA mondial (précédents : Amazon 746M€, Google 90M€)
- AI Act (2025)** : sanctions jusqu'à 35M€ ou 7% du CA
- DORA (finance)** : exclusion du marché européen en cas de non-conformité
- NIS2 (cyber)** : pénalités jusqu'à 10M€ ou 2% du CA

Lacunes opérationnelles identifiées :

- Impossibilité de prouver l'identité du décideur (humain ou IA)
- Absence d'horodatage fiable et infalsifiable
- Traçabilité insuffisante des données sources utilisées
- Processus de décision non documentés de manière vérifiable

Constat : Les logs serveur traditionnels sont modifiables par les administrateurs système, sans valeur probante devant les autorités réglementaires (ACPR, CNIL, tribunaux).

Solution Proposée

Architecture tripartite pour workflows vérifiables

Carge transforme les processus métier en pistes d'audit cryptées et vérifiables via trois composants complémentaires :

1. **Ragchain** - Blockchain Substrate avec pallets spécialisés (RAG + PKI + CryptoTrail)
 2. **Human Context Protocol (MCP)** - Interface standardisée pour agents IA
 3. **Interface Web Zero-Trust (carge.fr)** - Application client-side avec chiffrement de bout en bout
-

Fonctionnement Opérationnel

3 Étapes pour des Processus Vérifiables

1. Déployer le Processus

Envoyez vos processus, documents ou contrôles à l'IA

- L'IA analyse vos documents (langage naturel, PDF, tableurs)
- Elle code des workflows structurés on-chain via son MCP local
- Déploiement automatique sur Ragchain (pallets RAG) sous supervision et validation humaine

Composants du workflow (RAG on-chain) :

- **Instruction CID** : Prompt IA (ce qu'il faut faire)
- **Resource CID** : Documents de référence (base de connaissances)
- **Schema CID** : JSON Schema de validation (format attendu)
- **Étapes** : Séquence humain-IA avec points de contrôle

Le RAG est injecté dans le contexte de l'IA via le MCP :

- Le MCP récupère les CIDs depuis Ragchain
- Il charge le contenu depuis IPFS (instruction + resource + schema)

- Ce contexte RAG est injecté à l'agent IA pour qu'il accomplisse correctement sa tâche
- Double fonction : **exécution correcte** (contexte temps réel) + **traçabilité** (preuve on-chain)

Exemple concret - Processus KYC bancaire :

```
Étape 1 : IA collecte documents client (horodaté blockchain)
Étape 2 : IA vérifie conformité ACPR (instruction + resource CID)
Étape 3 : Validation humaine obligatoire si risque > seuil
Étape 4 : Décision finale signée cryptographiquement
→ Preuve immuable consultable par ACPR/CNIL
```

2. Exécuter Ensemble

Humains et IA collaborent sur les workflows - chacun faisant ce qu'il fait de mieux

Orchestration multi-agents :

- **IA** : Analyse, synthèse, recommandations (Claude, Mistral via MCP)
- **Humain** : Validation, décision finale, cas limites
- **Blockchain** : Horodatage cryptographique de chaque étape

Ouvert par conception, mais vous contrôlez qui participe :

- PKI décentralisée (clés publiques on-chain)
- Chiffrement X25519 + ChaCha20-Poly1305
- Signature sr25519 (Substrate)

Chaque action crée une trace d'audit cryptographique immuable :

- Timestamp blockchain (impossible à falsifier)
- Hash du contenu (IPFS CID)
- Identité de l'acteur (humain ou agent IA)
- Workflow step ID

3. Stocker pour Audit

Chaque exécution est archivée sur la blockchain

Transparence totale pour auditeurs et autorités réglementaires :

- Consultation publique ou privée (selon chiffrement)
- Export compatible formats réglementaires
- Vérification indépendante des preuves

Preuve immuable de qui a fait quoi, quand :

Format de preuve standardisé (toutes les preuves précédentes peuvent être reconstituées et vérifiées pour éviter l'altération) :

```
{
  "ragData": {
    "ragHash": "0x5e4985e555c2bef150394a2e037fd7213d2ced20cba6e94a1679fc8aa",
    "stepHash": "0xc84f18e49b2b0b27d8d4d5cb24c8b47c704a77a244a284eef03f86c2",
    "livrable": {
      "work": {
        "title": "KYC Validation Client ABC123",
        "type": "compliance_check",
        "description": "Vérification conformité ACPR - score risque 7/10",
        "creationDate": "2026-03-15",
        "contentHash": "bafkreigdy3gjet32etkcme4kvsvb2ybih36jkc lamrkxyp3hmt"
      },
      "creator": {
        "legalName": "Agent IA Claude 3.5 + Compliance Officer",
        "email": "compliance@bank.example",
        "country": "FR"
      }
    }
  }
}
```

Archivage inaltérable :

- Blockchain : métadonnées + hash
 - IPFS : contenu complet chiffré
 - Durée : permanente (tant que réseau existe)
-

Applications Concrètes

De la finance à la santé, Carge transforme les processus critiques en workflows vérifiables

1. Finance - Conformité DORA

Processus KYC/AML Automatisés avec Validation Humaine

Workflow :

1. Agent IA collecte documents identité (passeport, justificatif domicile)
2. Vérification automatique bases sanctions (OFAC, UE)
3. Scoring risque IA (PEP, pays sensibles)
4. Si score > seuil → validation obligatoire compliance officer
5. Décision finale signée et horodatée blockchain

Bénéfices mesurables :

- Conformité DORA (audit trail complet)
- Réduction 70% temps de traitement
- Preuve inaltérable pour ACPR
- Traçabilité complète des décisions IA vs humain

ROI : 500k€ à 5M€ de pénalités évitées + 40% réduction coûts audit

2. Santé - RGPD Données Sensibles

Workflows Diagnostics IA avec Validation Médicale

Workflow :

1. IA analyse imagerie médicale (scanner, IRM)
2. Recommandation diagnostic + score confiance
3. Validation obligatoire médecin senior
4. Consentement patient horodaté blockchain
5. Archivage sécurisé conforme HDS

Bénéfices mesurables :

- Conformité RGPD (consentement tracé)
- Responsabilité médicale claire (qui a décidé)
- Chiffrement E2E des données santé
- Audit CNIL facilité

Cas d'usage : GHT (Groupement Hospitalier de Territoire) - essais cliniques, diagnostics IA

3. Industrie - Traçabilité Supply Chain

Chaîne d'Approvisionnement Aéronautique Vérifiable

Workflow :

1. IA vérifie conformité pièces (certificats matériaux)
2. Contrôle qualité automatique (IA vision)
3. Validation humaine si non-conformité détectée
4. Signature cryptographique fournisseur
5. Traçabilité blockchain de bout en bout

Bénéfices mesurables :

- ISO 9001 facilité (audit trail automatique)
- Traçabilité composants critiques
- Preuve origine matériaux (sanctions Russie, Chine)
- Réduction fraude supply chain

Cas d'usage : ETI aéronautique - maintenance prédictive, contrôle qualité

4. Contrôle de Gestion - Audit Financier

Audits Financiers avec Transparence Totale

Workflow :

1. IA analyse factures et justificatifs
2. Détection anomalies (montants, doublons)
3. Validation DAF si anomalie
4. Export automatique vers CAC/expert-comptable

5. Enregistrements immuables blockchain

Bénéfices :

- Audit externe facilité (preuves cryptographiques)
 - Détection fraude automatique
 - Conformité fiscale (archivage 10 ans)
 - Réduction coûts audit -40%
-

5. Procédures Administratives - Marchés Publics

Permis et Autorisations Automatisés

Workflow :

1. IA vérifie complétude dossier
2. Contrôle conformité réglementaire
3. Validation service instructeur
4. Horodatage décision blockchain
5. Publication transparente

Bénéfices :

- Transparence marchés publics
 - Anti-corruption (décisions tracées)
 - Délais traitement réduits
 - Contentieux simplifiés (preuves immuables)
-

6. Certification Qualité - ISO/Normes

Audits ISO avec Preuve Cryptographique Vérifiable

Workflow :

1. IA collecte preuves conformité (docs, photos, mesures)
2. Analyse écarts vs référentiel ISO
3. Validation auditeur interne
4. Export direct vers organisme certificateur

5. Certification on-chain

Bénéfices :

- ISO 9001, 27001, 14001 facilités
 - Audit continu (pas seulement annuel)
 - Preuve vérifiable par certificateur
 - Réduction coûts certification -30%
-

Intégration Systèmes Existants

Carge s'intègre parfaitement avec votre infrastructure actuelle

Human Context Protocol (MCP)

Interface standardisée pour agents IA - Injection du contexte RAG

Compatibilité :

- Claude Desktop (Anthropic)
- Mistral AI
- Cursor IDE
- Tout client MCP compatible

Fonctionnement du MCP : Le MCP ne sert pas qu'à la traçabilité, il alimente activement l'IA :

1. **Récupération du RAG :** Le MCP lit les CIDs depuis Ragchain (instruction + resource + schema)
2. **Chargement du contexte :** Il télécharge le contenu depuis IPFS
3. **Injection à l'IA :** Le contexte RAG est fourni à l'agent IA pour qu'il accomplisse sa tâche
4. **Horodatage :** Chaque action est enregistrée on-chain avec preuve cryptographique

Serveur Local d'Interface :

- Le MCP est l'interface entre les agents IA et la blockchain Ragchain + IPFS
- Exécutez un serveur MCP local totalement décentralisé
- Vos systèmes se connectent directement à la chaîne
- Pas d'intermédiaires, pas de serveurs tiers

Architecture :



Avec ou Sans IA

Flexibilité maximale selon vos besoins

Mode IA (Workflows Complexes) :

- Agents IA analysent, recommandent, exécutent
- Validation humaine aux points critiques
- Orchestration multi-étapes
- Accès via une IA disposant du MCP (Claude, Mistral, etc.)

Mode Sans IA (Attestations Simples) :

- Via le site [cargo.fr](https://www.cargo.fr) directement
- OU via votre ERP/SI connecté aux outils du MCP (utilisé comme API)
- Signature cryptographique directe
- Horodatage blockchain sans analyse IA
- Cas d'usage : certification document, validation simple

Vous choisissez : hybride, 100% IA, ou 100% humain selon le processus

Échange de Données Certifiées

Souveraineté totale des données

Chaque échange est crypté et signé cryptographiquement on-chain :

- Chiffrement X25519 ECDH (échange de clés)
- ChaCha20-Poly1305 AEAD (chiffrement authentifié)
- Signature sr25519 (Substrate native)

Vous contrôlez qui accède à vos informations :

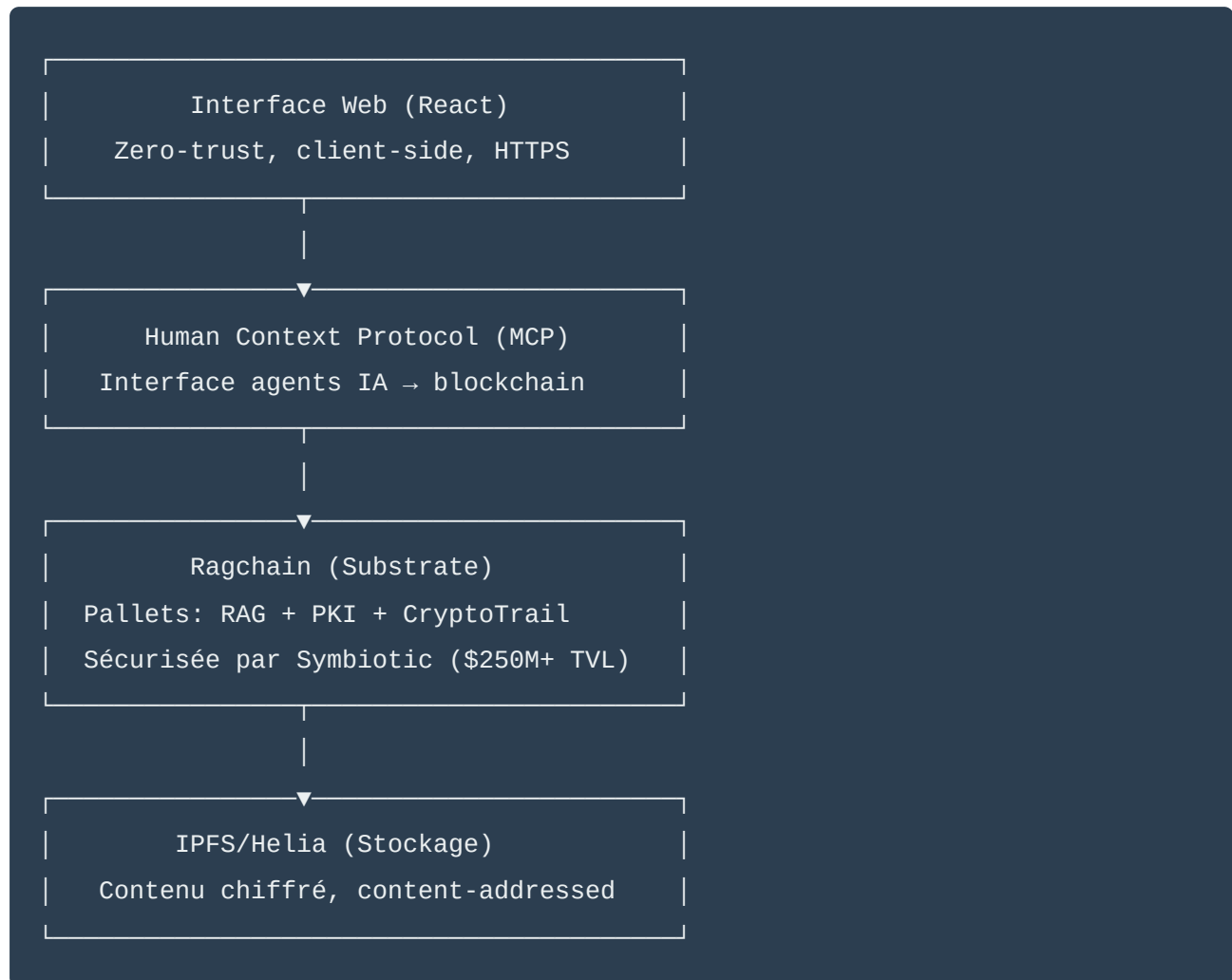
- PKI décentralisée (pas d'autorité centrale)
- Clés publiques affichées on-chain pour transparence
- Partage sélectif par chiffrement avec clé publique destinataire
- Révocation possible via suppression des clés de chiffrement

Intégration ERP/CRM :

- API REST pour systèmes legacy
 - SDK JavaScript/Python (disponible Q2 2026)
 - Webhooks pour notifications temps réel
-

Architecture Technique

Stack 100% Souverain et Open-Source



Composants Clés

1. Ragchain (Tanssi Appchain - Substrate)

- **Pallet RAG** : Registre workflows (instruction + resource + schema CIDs)
- **Pallet PKI** : Gestion clés publiques décentralisée
- **Pallet CryptoTrail** : Preuves cryptographiques horodatées
- **Consensus** : Proof-of-Stake sécurisé par Symbiotic restaking

2. IPFS (Stockage Décentralisé)

- Content-addressed (CID = hash du contenu)
- Chiffrement avant upload (IPFS ne voit que ciphertext)
- Pinning optionnel (Kubo node local ou services w3.storage/Pinata)

3. Cryptographie

- **@noble/curves** : X25519, sr25519 (audit Trail of Bits)
 - **@noble/ciphers** : ChaCha20-Poly1305
 - **BLAKE2b-256** : Hash on-chain
 - **SHA-256** : CID IPFS
-

Sécurité et Conformité

Conçu pour l'Audit & la Conformité Dès la Conception

Modèle de Sécurité

Ce qui EST protégé :

- Immutabilité des données (blockchain)
- Confidentialité (chiffrement E2E)
- Authentification (signatures cryptographiques)
- Horodatage fiable (consensus blockchain)
- Disponibilité (P2P décentralisé)

Responsabilités utilisateur :

- Sécurité du wallet (Polkadot.js extension)
- Gestion des clés de chiffrement
- Sécurité de l'appareil (navigateur)

Infrastructure :

- **Symbiotic Network** : \$250M+ stake (restaking Ethereum)
 - **Pas de Single Point of Failure** (architecture P2P)
 - **Code open-source** (GPL-3.0) : auditabilité publique
-

Conformité Réglementaire

Réglementation	Conformité Charge
RGPD	Privacy by design, chiffrement E2E, droit à l'oubli (suppression clés)
AI Act	Traçabilité IA, transparence décisions, human-in-the-loop
DORA	Audit trail complet, test résilience, gestion incidents
NIS2	Cybersécurité renforcée, reporting incidents, gestion risques
Archivage légal	Immutabilité, horodatage qualifié, durée conservation

Standards respectés :

- W3C Decentralized Identifiers (DID)
- W3C Verifiable Credentials (VC) - roadmap Q3 2026
- ISO 27001 (sécurité information) - certification en cours
- eIDAS (signature électronique qualifiée) - intégration prévue 2027

Traction et Reconnaissance

Pré-sélection Concours Européen EBSI

European Blockchain Services Infrastructure - Commission Européenne

Charge a été **pré-sélectionné** au concours européen de l'EBSI sur les blockchains, validation par la Commission Européenne de la pertinence technique et stratégique du projet pour l'infrastructure blockchain européenne.

EBSI (European Blockchain Services Infrastructure) :

- Initiative de la Commission Européenne
- Réseau blockchain pour services publics européens
- Focus : identité numérique, diplômes vérifiables, registres décentralisés
- Charge reconnu pour son approche workflows vérifiables et conformité réglementaire

Bénéfices Attendus

Réduction des coûts de conformité :

- Automatisation des audits via preuves cryptographiques
- Diminution temps de réponse aux régulateurs (preuves immédiatement disponibles)
- Réduction exposition aux pénalités (RGPD, AI Act, DORA, NIS2)

Efficacité opérationnelle :

- Détection automatique d'anomalies par IA
- Traçabilité complète des décisions humain-IA
- Processus de validation accélérés

Roadmap Produit

Phase 1 : Validation Métier (Déc 2025 - Juin 2026) - En cours

Objectifs :

- Valider 3 workflows production (finance, santé, industrie)
- 300 exécutions réelles avec horodatage blockchain
- 3 clients pilotes (banque, GHT, ETI aéro)
- Conformité DORA/RGPD/AI Act certifiée

Livrables :

- M2 : 3 spécifications workflows + rapport conformité juridique
- M4 : 3 workflows opérationnels + audit blockchain sécurité
- M6 : Rapport validation 300 preuves + analyse ROI

Budget : 120k€ (France 2030 - Phase 1 faisabilité)

Phase 2 : Industrialisation (Juillet 2026 - Déc 2026)

Objectifs :

- Déploiement mainnet Polkadot production

- 10 clients payants (SaaS 30k€/an/client)
- Intégrations ERP (SAP, Odoo, Salesforce)
- ARR : 300k€

Développements :

- SDK Python/TypeScript complets
- Templates workflows pré-configurés (20+ cas d'usage)
- Dashboard analytics avancé
- API REST v2 + webhooks

Financement : 500k€ (levée de fonds Seed/Série A visée) + acquisition 32 ETH pour node Symbiotic (~60k€)

Phase 3 : Scale-up Européen (2027-2028)

Objectifs :

- 50+ clients européens (France, Allemagne, Suisse, Benelux)
- Conformité multi-juridictions (AI Act, GDPR variantes)
- Partenariats Big 4 (Deloitte, EY, PwC, KPMG)
- ARR : 1,5M€+

Développements :

- Intégration eIDAS (signature électronique qualifiée)
- Support multi-chaînes (Ethereum, Avalanche via bridges)
- Marketplace workflows (communauté)
- Certification ISO 27001

Exit : IPO ou acquisition stratégique (target : acteur RegTech/GovTech EU)

Contact & Partenariats

Clients Pilotes Recherchés

Nous recherchons activement des partenaires pour Phase 1 :

Secteur Financier (1 place disponible)

- Banques régionales, assurances, fintechs
- Cas d'usage : KYC/AML, conformité DORA, audit interne

Secteur Santé (1 place disponible)

- GHT, cliniques privées, labos pharmaceutiques
- Cas d'usage : diagnostics IA, essais cliniques, RGPD santé

Industrie (1 place disponible)

- ETI aéronautique, automobile, électronique
- Cas d'usage : supply chain, contrôle qualité, ISO 9001

Avantages clients pilotes :

- Licence gratuite Phase 1 (6 mois)
- Personnalisation workflow à vos besoins
- Support dédié
- Visibilité (cas d'usage référence)

Conditions :

- 10+ utilisateurs pour tests réels
- Accès système pour intégration API
- Feedback régulier
- Participation rapport final Phase 1

Équipe & Partenaires

Porteur de Projet :

- **Jean-François Meneust** - Founder & Lead Developer
 - Ancien Commissaire des Armées (officier en droit, finance et logistique)
 - Reconversion développeur blockchain et MCP pour IA
 - Spécialisation : Tanssi/Polkadot ecosystem, cryptographie (X25519 + ChaCha20)

Reconnaissance :

- **Pré-sélection concours européen EBSI** (European Blockchain Services Infrastructure)

- Validation Commission Européenne de la pertinence technique du projet

Partenaires Techniques :

- **Parity Technologies** (Berlin) - Support Substrate parachain
 - **Symbiotic Network** - Restaking infrastructure (\$250M+ TVL)
 - **Protocol Labs** - IPFS/Helia integration
-

Informations Légales

CARGE

- SIREN : 939981247
- Forme juridique : Auto-entrepreneur (Micro-entreprise)
- Siège social : 14 rue de la mutualité, 49300 Cholet, France
- Effectif : 1 ETP (fondateur)
- CA 2024 : 0€ (pré-revenue)

Licence :

- Code : GPL-3.0 (open-source)
- Documentation : CC BY-SA 4.0

Contact :

- Email : jf.meneust@gmail.com
 - Site web : <https://carge.fr>
 - GitHub : <https://github.com/polykrate/carge>
 - Twitter/X : @carge_crypto
 - LinkedIn : carge-fr
-

Ressources

Documentation & Démonos

Démono Live :

- Interface Web : carge.fr/workflows

- Vérificateur de preuves : charge.fr/verify

Documentation Technique :

- README : github.com/polykrate/charge
- Architecture : github.com/polykrate/charge/blob/master/README.md
- Human Context Protocol : github.com/polykrate/human-context-protocol (*unreleased*)

Démo Vidéo :

- Concours Startup CMA CMG :
<https://www.loom.com/share/55b5d225b5d94096bafc8bfd85ede809?sid=440c6ba7-50d1-4a8a-b283-80077097cbd2>

Pourquoi Choisir Charge ?

L'Alternative Européenne aux Solutions US

Critère	Solutions US (AWS, Azure)	Charge (EU)
Souveraineté	Cloud Act (accès US gov)	Stack 100% européen
Vendor Lock-in	Propriétaire	Open-source (GPL-3.0)
Conformité	Clauses contractuelles	Privacy by design
Audit Trail	Logs modifiables	Blockchain immutable
Coût Scaling	Exponentiel	Logarithmique (P2P)
Transparence	Boîte noire	Code open-source

Charge est la seule solution blockchain européenne dédiée aux workflows IA-humains vérifiables.