ITS-MINE — PRONODEALGO.XYZ

Timestamp Service + Vault

Blockchain-anchored proof of existence & quantum-safe encrypted storage

Preuve d'existence blockchain & stockage chiffre quantum-safe

Algorand • Falcon-1024 • AES-256-GCM • x402 • HKDF-SHA256

English	*Francais en italique orange*

Privacy First	Pay-per-use	~3 seconds	Quantum-safe	100% On-chain
Confidentialite totale	*Paiement a l'usage*	*~3 secondes*	*Resisant quantique*	*100% On-chain*

01 — WHAT IS ITS-MINE?

01 — QU'EST-CE QU'ITS-MINE ?

Two services, one platform

Its-Mine combines two complementary services built on the Algorand blockchain. The **Timestamp Service** creates an immutable cryptographic proof that a document existed at a specific point in time — at 0.05 USDC per timestamp. The **Vault** goes further: it stores your files encrypted directly on-chain, retrievable only by you, with quantum-safe cryptography.
Live: **pronodealgo.xyz/its-mine/** (Testnet) • **pronodealgo.xyz/its-mine-mainnet/** (Mainnet)

Deux services, une plateforme

*Its-Mine combine deux services complementaires construits sur la blockchain Algorand. Le **Timestamp Service** cree une preuve cryptographique immuable qu'un document existait a un instant precis — a 0,05 USDC par horodatage. Le **Vault** va plus loin : il stocke vos fichiers chiffres directement on-chain, recuperables uniquement par vous, avec une cryptographie post-quantique.*
*En ligne : **pronodealgo.xyz/its-mine/** (Testnet) • **pronodealgo.xyz/its-mine-mainnet/** (Mainnet)*

The problem solved

Proving that a document existed **before** a given date — without a notary, without any centralized authority, at a fraction of traditional costs. And storing sensitive documents so that **no server, no hacker, no future quantum computer** can ever access them.

- Musician whose work is plagiarized months after creation
- Developer whose algorithm is patented by a competitor
- Journalist whose sources are disputed in court
- AI agent whose generated reports require verifiable audit trails

- Any sensitive document that must remain confidential forever

Le probleme resolu

*Prouver qu'un document existait **avant** une date precise — sans notaire, sans organisme centralise, a une fraction des couts traditionnels. Et stocker des documents sensibles de sorte qu'**aucun serveur, aucun pirate, aucun futur ordinateur quantique** ne puisse jamais y acceder.*

- *Musicien dont l'oeuvre est copiee des mois apres sa creation*
- *Developpeur dont l'algorithme est brevete par un concurrent*
- *Journaliste dont les sources sont contestees devant un tribunal*
- *Agent IA dont les rapports doivent etre audites de facon verifiable*
- *Tout document sensible devant rester confidentiel pour toujours*

02 — TIMESTAMP SERVICE

02 — SERVICE D'HORODATAGE

How it works

The user connects their Algorand wallet (Pera, Defly, Lute, Kibisis), selects any file, and the SHA-256 hash is computed **locally in the browser** — the file never leaves the device. A 0.05 USDC payment is made via the x402 protocol, the hash is anchored on Algorand in ~3 seconds, and a **downloadable PDF certificate** is generated.

Comment ca fonctionne

*L'utilisateur connecte son wallet Algorand, selectionne un fichier, et le hash SHA-256 est calcule **localement dans le navigateur** — le fichier ne quitte jamais l'appareil. Un paiement de 0,05 USDC est effectue via le protocole x402, le hash est ancre sur Algorand en ~3 secondes, et un **certificat PDF telechargeable** est genere.*

Comparison with existing solutions / Comparaison avec les solutions existantes

Method / Methode	Cost / Cout	Time / Delai	Trust / Fiabilite
Notary / Notaire	$200-500	1-2 weeks / semaines	★★★★★
INPI / USPTO	$50-200	2-4 weeks / semaines	★★★★
Self-email / Email a soi	Free / Gratuit	Instant	★
OpenTimestamps (Bitcoin)	Free / Gratuit	1h+	★★★
Its-Mine Timestamp	**$0.05**	**~3 seconds / secondes**	★★★★★

SHA-256 properties / Proprietes du SHA-256

Property / Propriete	English	Francais
Unique	Different files = different hashes	Fichiers differents = hash differents
Deterministic / Deterministe	Same file always = same hash	Meme fichier = toujours meme hash
Irreversible	Cannot reconstruct file from hash	Impossible de retrouver le fichier
Sensitive / Sensible	1 byte different = totally different hash	1 octet different = hash totalement different

03 — VAULT — ENCRYPTED ON-CHAIN STORAGE

03 — VAULT — STOCKAGE CHIFFRE ON-CHAIN

The concept: storage without a storage server

The Vault stores your files encrypted **directly in Algorand transaction notes** — no IPFS, no AWS, no S3. The file is split into 620-byte chunks, each encrypted with a unique AES-256-GCM key. Only the owner's Falcon-1024 wallet can reconstitute and decrypt the file. Maximum file size: **1 MB**.

Le concept : stockage sans serveur de stockage

*Le Vault stocke vos fichiers chiffres **directement dans les notes de transactions Algorand** — sans IPFS, sans AWS, sans S3. Le fichier est decouped en chunks de 620 octets, chacun chiffre avec une cle AES-256-GCM unique. Seul le wallet Falcon-1024 du proprietaire peut reconstituer et dechiffrer le fichier. Taille maximum : **1 Mo**.*

File types supported (up to 1 MB)

The 1 MB limit covers the vast majority of professional and legal documents:

- PDF contracts, legal documents, patents (50-800 KB) ■
- Word documents, scripts, source code (10-300 KB) ■
- Compressed images, logos, illustrations (100-800 KB) ■
- Music scores, certificates, diplomas (100-500 KB) ■
- HD photos, MP3 audio, videos ■ (too large)

Types de fichiers supportes (jusqu'a 1 Mo)

La limite de 1 Mo couvre la grande majorite des documents professionnels et juridiques :

- *Contrats PDF, documents juridiques, brevets (50-800 Ko) ■*
- *Documents Word, scripts, code source (10-300 Ko) ■*
- *Images compressees, logos, illustrations (100-800 Ko) ■*
- *Partitions, certificats, diplomes (100-500 Ko) ■*
- *Photos HD, audio MP3, videos ■ (trop volumineux)*

04 — CRYPTOGRAPHIC ARCHITECTURE (VAULT-V2)

04 — ARCHITECTURE CRYPTOGRAPHIQUE (VAULT-V2)

Two independent factors

The vault-v2 encryption scheme uses **two completely independent secrets**. Breaking Falcon alone is not enough — the wallet password is also required. And breaking the password alone is not enough — the Falcon secret key is also required.

Deux facteurs independants

*Le schema de chiffrement vault-v2 utilise **deux secrets completement independants**. Casser Falcon seul ne suffit pas — le mot de passe wallet est aussi requis. Et trouver le mot de passe seul ne suffit pas — la cle secrete Falcon est aussi requise.*

Cryptographic formula per chunk / Formule cryptographique par chunk

```
ikm = secretKey_Falcon (2305B) || fileKeyMaterial (32B)
fileKeyMaterial = PBKDF2-SHA256(password, walletSalt||'-file-key', 100k iter)
chunkKey_i = HKDF-SHA256(ikm, salt=chunkSalt_i, info='its-mine-vault-v2-{hash}-{i}')
encChunk_i = AES-256-GCM(chunkKey_i, chunkIv_i, plainChunk_i)
```

Security layers / Couches de securite

Attack / Attaque	Result / Resultat
Break AES-256-GCM / Casser AES-256-GCM	■ Mathematically impossible / Mathematiquement impossible
Break Falcon-1024 (quantum) / Casser Falcon-1024	■ Post-quantum safe / Resistant post-quantique
Find the password / Trouver le mot de passe	■ 600k PBKDF2 iterations — brute-force impractical
Two identical chunks / 2 chunks identiques	■ Unique random salt per chunk / Sel aleatoire unique
Steal encrypted chunks / Voler les chunks	■ Useless without both secrets / Inutile sans les 2 secrets

Quantum resistance

Falcon-1024 is a post-quantum signature algorithm selected by NIST, based on lattice cryptography — mathematically unsolvable even by a quantum computer. AES-256-GCM and SHA-256 are also quantum-resistant. The entire vault-v2 stack is **quantum-safe end-to-end**.

Resistance quantique

*Falcon-1024 est un algorithme de signature post-quantique selectionne par le NIST, base sur la cryptographie sur reseaux euclidiens — mathematiquement insoluble meme par un ordinateur quantique. AES-256-GCM et SHA-256 sont egalement resistants au quantique. Toute la stack vault-v2 est **quantum-safe de bout en bout**.*

05 — TECHNICAL STACK

05 — STACK TECHNIQUE

Component / Composant	Technology	Role / Role
Frontend (users / utilisateurs)	Vite + use-wallet	Local hash + wallet + x402 payment
Frontend (AI agents / agents IA)	@x402-avm/fetch	Automated x402 payment flow
Backend	Node.js + Express	REST API + x402 middleware

Payment protocol / Protocole paiement	x402 + @x402-avm/express	Pay-per-use USDC — no account
Blockchain	Algorand (Testnet + Mainnet)	Immutable anchoring / Ancrage immuable
Vault encryption / Chiffrement Vault	@noble/post-quantum/falcon.js	Falcon-1024 — pure JS, zero WASM
Key derivation / Derivation cle	SubtleCrypto HKDF + PBKDF2	2-factor — quantum-safe
Chunk encryption / Chiffrement chunks	AES-256-GCM (SubtleCrypto)	Unique key per chunk / Cle unique par chunk
PDF certificate / Certificat PDF	Python + ReportLab	TX ID + QR Code
Verification	Public free API / API publique	GET /verify/:hash — no auth
Database / Base de donnees	SQLite	TX IDs + timestamps + hashes
AI discovery / Decouverte IA	llms.txt	Emerging LLM standard

Why Algorand / Pourquoi Algorand

Property / Propriete	Algorand	Bitcoin	Ethereum
Finality / Finalite	~3 seconds	60 minutes	15 minutes
TX cost / Cout TX	~$0.0002	~$1-50	~$1-20
Note field / Champ note	1024 bytes	80 bytes	Limited
Quantum-safe / Post-quantique	Falcon ready ■	■	■
Immutability / Immuabilite	■ Guaranteed	■	■

06 — PRICING & BUSINESS MODEL

06 — TARIFICATION & MODELE ECONOMIQUE

Timestamp pricing / Tarification Timestamp

Item / Element	Value / Valeur	Detail
Sale price / Prix de vente	$0.05 USDC	Per timestamp / Par horodatage
Blockchain fee / Frais blockchain	$0.00015	Algorand fee (~0.001 ALGO)
Hosting / Hebergement	$0.002	VPS share per request / Part VPS
PDF generation / Generation PDF	$0.001	Certificate / Certificat
Total cost / Cout total	~$0.003	Per timestamp / Par horodatage
Net margin / Marge nette	**~94%**	**~$0.047 USDC pure profit / profit pur**

Vault dynamic pricing formula / Formule de tarification dynamique du Vault

```
N_tx = ceil(size_bytes / 620) + 1
algo_cost = N_tx x 0.001 (in ALGO)
price_usdc = max(tier_floor, round_up(algo_cost x ALGO_price x 2.2 + 0.10, 0.05))
```

Vault pricing tiers / Paliers de tarification Vault

Tier	Max size / Taille max	Floor / Plancher USDC	Example at $0.32 ALGO
XS	50 KB	$0.15	$0.15
S	200 KB	$0.25	$0.25
M	500 KB	$0.45	$0.45
L	1 MB	$0.70	$0.70

Revenue projections / Projections de revenus

Based on 100 timestamps/agent/day and Vault uploads at average $0.45 USDC.

Base sur 100 horodatages/agent/jour et uploads Vault a 0,45 USDC en moyenne.

Scenario	AI Agents / Agents IA	Timestamps/day	Vault uploads/day	Revenue/day / Revenu/jour
Start / Demarrage	10	100	5	~$52
Growth / Croissance	50	100	20	~$259
Scale / Echelle	100	100	50	~$523

07 — VAULT — UPLOAD & RECOVERY FLOW

07 — VAULT — FLUX UPLOAD & RECUPERATION

Upload flow (5 steps)

1. User imports their Falcon wallet JSON + password — key never leaves the browser. 2. File is selected locally — hash computed, price fetched dynamically. 3. File is encrypted chunk-by-chunk (AES-256-GCM, unique key per chunk). 4. Single x402 USDC payment — server posts all chunks as Algorand transactions in groups of 16. 5. User receives the INDEX TX ID — their permanent recovery key.

Flux d'upload (5 etapes)

1. L'utilisateur importe son JSON wallet Falcon + mot de passe — la cle ne quitte jamais le navigateur. 2. Le fichier est selectionne localement — hash calcule, prix recupere dynamiquement. 3. Le fichier est chiffre chunk par chunk (AES-256-GCM, cle unique par chunk). 4. Paiement x402 USDC unique — le serveur poste tous les chunks en transactions Algorand par groupes de 16. 5. L'utilisateur recoit le TX ID INDEX — sa cle de recuperation permanente.

Recovery flow (anytime, any device)

1. Import Falcon wallet JSON + enter password → re-derive fileKeyMaterial. 2. Enter INDEX TX ID (or scan by fingerprint). 3. App fetches INDEX + all CHUNK transactions from Algorand Indexer. 4. Chunks sorted, decrypted one by one, merged into original file. 5. File name decrypted → automatic download. **Standalone recovery also available** (vault-recovery.html) — no server required, direct Indexer queries.

Flux de recuperation (n'importe quand, n'importe quel appareil)

1. Importer le JSON wallet Falcon + entrer le mot de passe → re-deriver fileKeyMaterial. 2. Saisir le TX ID INDEX (ou scanner par fingerprint). 3. L'app recupere l'INDEX + tous les chunks depuis l'Indexer Algorand. 4. Chunks tries, dechiffres un par un, fusionnes en fichier original. 5. Nom de fichier dechiffre → telechargement automatique. ***Recuperation standalone disponible*** *(vault-recovery.html) — aucun serveur requis, requetes Indexer directes.*

08 — FALCON-1024 WALLET

08 — WALLET FALCON-1024

A separate wallet for encryption

Current Algorand wallets (Pera, Defly, Daffi) do not support Falcon. The Vault therefore uses a **dedicated Falcon-1024 keypair**, generated entirely in the browser via @noble/post-quantum — pure JavaScript, zero WebAssembly dependency. The private key is encrypted with AES-256-GCM + PBKDF2 and stored in localStorage. Export as JSON is mandatory for multi-device access.

Un wallet distinct pour le chiffrement

Les wallets Algorand actuels (Pera, Defly, Daffi) ne supportent pas Falcon. Le Vault utilise donc une ***keypair Falcon-1024 dediee****, generee entierement dans le navigateur via @noble/post-quantum — JavaScript pur, zero dependance WebAssembly. La cle privee est chiffree AES-256-GCM + PBKDF2 et stockee dans le localStorage. L'export JSON est obligatoire pour un acces multi-appareils.*

Wallet architecture / Architecture du wallet

Wallet	Role	Managed by / Gere par
Algorand (Pera/Defly)	Pay USDC via x402 / Payer USDC	User / Utilisateur (classic wallet)

Falcon-1024	Encrypt / decrypt files / Chiffrer / dechiffrer	App — 100% in-browser / dans le navigateur

Critical warning / Avertissement critique : If you lose your Falcon key, your vaulted files are permanently unrecoverable — even by us. This is not a bug — it is the service promise.
Si vous perdez votre cle Falcon, vos fichiers vaultes sont irrecuperables pour toujours — meme par nous. Ce n'est pas un bug — c'est la promesse du service.

09 — TARGET CLIENTS

09 — CLIENTS CIBLES

■ Creators & Freelancers
Createurs & Independants

Timestamp photos, designs, code, music before any dispute.
Horodatez photos, designs, code, musique avant tout litige.

■ Timestamp

■ Autonomous AI Agents
Agents IA Autonomes

Auto-timestamp every generated report via x402 — no account, no human.
Horodatage automatique de chaque rapport via x402 — sans compte, sans humain.

■ Timestamp

■ Journalists & Media
Journalistes & Medias

Proof of prior existence for confidential sources and documents.
Preuve d'anteriorite sur sources confidentielles et documents sensibles.

■ Timestamp + Vault

■■ Law Firms
Cabinets Juridiques

Evidence timestamping in legal proceedings — tamper-proof.
Horodatage de preuves dans procedures legales — inalterable.

■ Timestamp + Vault

■ Music & Film Producers
Producteurs Musique & Cinema

Quantum-safe vault storage of masters, scripts, contracts.
Stockage quantum-safe de masters, scripts, contrats dans le Vault.

■ Vault

■ Startups & Inventors
Startups & Inventeurs

Pre-patent proof of concept — 1000x cheaper than USPTO.
Preuve de concept avant brevet — 1000x moins cher que l'INPI.

■ Timestamp

10 — X402 PROTOCOL

10 — PROTOCOLE X402

Native internet payments — no account, no KYC

x402 is an open standard built around HTTP status code 402 (Payment Required). Any HTTP server can accept cryptographic payments without accounts, without KYC, without subscriptions. The wallet signs a transaction, the payment header is attached to the request — the server verifies and responds. **One API call = one payment = one result.**

Paiements natifs sur Internet — sans compte, sans KYC

x402 est un standard ouvert base sur le code HTTP 402 (Payment Required). N'importe quel serveur HTTP peut accepter des paiements cryptographiques sans compte, sans KYC, sans abonnement. Le wallet signe une transaction, le header de paiement est joint a la requete — le serveur verifie et repond. ***Un appel API = un paiement = un resultat.***

Traditional / Traditionnel	With x402 / Avec x402
Mandatory account / Compte obligatoire	No account required / Aucun compte requis ■
KYC required / KYC requis	Instant access / Acces instantane ■

Subscription / Abonnement	Pure pay-per-use ■
Complex OAuth middleware	Native HTTP 402 + 1 header ■

11 — IMPORTANT NOTES

11 — NOTES IMPORTANTES

Current status — Testnet (Beta)

The Vault is currently in beta on Algorand Testnet. Access is restricted to authorized addresses (VAULT_ALLOWED list). Mainnet deployment planned after full validation. The Timestamp Service is live on Mainnet.

Statut actuel — Testnet (Beta)

Le Vault est actuellement en beta sur Algorand Testnet. L'acces est restreint aux adresses autorisees (liste VAULT_ALLOWED). Deploiement Mainnet prevu apres validation complete. Le Timestamp Service est actif sur Mainnet.

Live URLs / URLs en production

Environment / Environnement	URL	Status
Testnet (Timestamp + Vault beta)	pronodealgo.xyz/its-mine/	Live ■
Mainnet (Timestamp)	pronodealgo.xyz/its-mine-mainnet/	Live ■
Public verification API	/its-mine/api/verify/:hash	Free / Gratuit ■
Standalone vault recovery	/its-mine/vault-recovery.html	No server required

Legal value of timestamps

A blockchain timestamp provides **technical proof of prior existence**. It may serve as supporting evidence in legal proceedings, but is not equivalent to a notarial act. Users are solely responsible for verifying legal admissibility in their jurisdiction.

Valeur juridique des horodatages

*Un horodatage blockchain fournit une **preuve technique d'anteriorite d'existence**. Il peut servir de preuve dans des procedures juridiques, mais n'est pas equivalent a un acte notarial. Les utilisateurs sont seuls responsables de verifier la validite juridique dans leur juridiction.*

This document is a general-purpose product overview. No sensitive information, private keys or server configuration data is included. | Ce document est un apercu produit general. Aucune information sensible, cle privee ou donnee de configuration serveur n'est incluse.

April 2026 — PronodeAlgo — pronodealgo.xyz