TECHNICAL PAPER · VERSION 1.0 · NOVEMBRE 2026

# ACTUARUS

*Le séquestre programmable : échanger un bien de valeur entre inconnus, sans que personne ne détienne les fonds*

> *« La blockchain n'a d'intérêt que si elle résout un problème concret. »*
> ACTUARUS

**Etan Fouquet** · Développement commercial et distribution
**Arthur Veneau** · Responsable technique
**Wilfrid Dubreuil** · Core developer

SOMMAIRE

Résumé
1 · Prologue : 2008
2 · Le pari de la confiance
3 · Ce que les solutions actuelles ne résolvent pas
4 · Genèse : une grange, trois amis
5 · Des contrats programmables
6 · Le principe ACTUARUS
7 · Architecture technique
8 · Le traitement des litiges
9 · Sécurité
10 · Modèle économique
11 · Cadre juridique
12 · Feuille de route
13 · Conclusion
Références

## RÉSUMÉ

Acheter un bien de valeur à un inconnu reste un pari. L'acheteur qui paie d'avance risque de ne rien recevoir ; le vendeur qui livre d'abord risque de ne jamais être payé. Les solutions existantes — séquestre bancaire ou notarial, crédit documentaire, plateformes de paiement sécurisé — réduisent ce risque au prix de délais de plusieurs jours, de coûts élevés, et en confiant les fonds à un intermédiaire.

ACTUARUS propose un **séquestre on-chain non-custodial**. Les fonds de l'acheteur sont bloqués dans un smart contract public sur la blockchain Solana, et ne peuvent en sortir que par l'accord de deux des trois signataires de la transaction : l'acheteur, le vendeur et l'arbitre. ACTUARUS orchestre le contrat, la preuve et l'horodatage, sans jamais entrer en possession des fonds ni pouvoir les déplacer seule. Le règlement s'effectue en quelques minutes, en stablecoins agréés, et chaque étape laisse une trace vérifiable par tous.

Ce document raconte d'où vient ACTUARUS, explique le problème qu'elle résout, et décrit son fonctionnement technique tel qu'il est inscrit dans le code public du programme.

### Ce que ce document n'est pas

Ce technical paper n'est ni une offre au public de crypto-actifs, ni une sollicitation d'investissement. ACTUARUS n'émet aucun jeton et ne promet aucun rendement.

CHAPITRE 1

## PROLOGUE : 2008

*Une preuve à la place de la confiance*

Le 31 octobre 2008, en pleine crise financière, un auteur signant Satoshi Nakamoto publie un texte de neuf pages : *Bitcoin: A Peer-to-Peer Electronic Cash System* [1]. Le constat est simple : le commerce en ligne repose presque entièrement sur des institutions financières qui servent de tiers de confiance. Ces intermédiaires arbitrent les litiges, ce qui rend les paiements réversibles, coûteux, et oblige chaque commerçant à se méfier de ses clients.

> *« Ce qu'il faut, c'est un système de paiement électronique fondé sur la preuve cryptographique plutôt que sur la confiance, permettant à deux parties consentantes de transiger directement l'une avec l'autre, sans avoir besoin d'un tiers de confiance. »*
>
> Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008 [1]

Bitcoin a résolu le premier problème : envoyer de la valeur à un inconnu, sans banque, sans possibilité de double dépense. Mais dès son introduction, Nakamoto pointait une limite. Un paiement irréversible protège le vendeur ; il laisse l'acheteur sans recours. Sa réponse tient en une phrase : des mécanismes de séquestre courants pourraient être facilement mis en place pour protéger les acheteurs.

Dix-huit ans plus tard, ce séquestre « courant » n'est toujours pas entré dans les usages. Échanger un bien réel — un véhicule, une machine, un actif numérique — contre un paiement, entre deux personnes qui ne se connaissent pas, reste aussi risqué qu'avant. C'est ce chaînon manquant qu'ACTUARUS veut construire.

CHAPITRE 2

## LE PARI DE LA CONFIANCE

*Pourquoi un échange entre inconnus échoue*

En 1970, l'économiste George Akerlof décrit le « marché des citrons » [2]. Sur le marché de l'occasion, le vendeur connaît l'état réel du bien ; l'acheteur, non. Faute de pouvoir distinguer un bon véhicule d'un mauvais, l'acheteur se méfie de tous, propose un prix moyen, et les bons vendeurs finissent par quitter le marché. L'asymétrie d'information ne fait pas seulement des victimes : elle détruit des échanges qui auraient profité aux deux parties.

Une transaction directe concentre deux risques, symétriques et impossibles à éliminer par la seule bonne foi :

- **Le risque de l'acheteur** : payer un bien qui n'existe pas, n'arrive jamais, ou ne correspond pas à ce qui était promis.
- **Le risque du vendeur** : livrer un bien et ne jamais être payé, ou subir l'annulation d'un paiement après la livraison.

L'ampleur du problème est mesurable. Pour la seule année 2024, le centre de signalement de la cybercriminalité du FBI a enregistré **49 572 plaintes** pour non-paiement ou non-livraison, pour **plus de 785 millions de dollars** de pertes déclarées aux États-Unis [3]. Ces chiffres ne comptent que les victimes qui ont porté plainte, et ne mesurent pas les transactions qui n'ont jamais eu lieu, faute de confiance.

À ces deux risques s'ajoute l'opacité de l'actif lui-même : son historique, ses propriétaires successifs, son état réel au moment de chaque vente restent invérifiables.

CHAPITRE 3

## CE QUE LES SOLUTIONS ACTUELLES NE RÉSOLVENT PAS

*Sécuriser a toujours voulu dire confier*

Des outils existent pour sécuriser un échange. Tous reposent sur le même principe : confier temporairement les fonds à un tiers. Ce principe a un prix.

| Solution | Fonctionnement | Limites |
|---|---|---|
| **Séquestre bancaire ou notarial** | Un établissement ou un officier public conserve les fonds jusqu'à la réalisation des conditions. | Plusieurs jours de délai, frais significatifs, horaires ouvrés, réservé aux montants élevés. |
| **Crédit documentaire** | La banque de l'acheteur s'engage à payer le vendeur sur présentation de documents conformes, selon les règles RUU 600 de la Chambre de commerce internationale [4]. | Procédure lourde, coûts bancaires, plusieurs semaines ; la banque vérifie des documents, pas le bien. |
| **Plateformes de paiement sécurisé** | Un intermédiaire encaisse le paiement et le reverse au vendeur après confirmation. | Les fonds sont détenus par la plateforme : l'utilisateur dépend de sa solvabilité et de ses décisions. |
| **Paiement direct** | Virement ou espèces, sans intermédiaire. | Aucune protection : l'une des deux parties prend tout le risque. |

Aucune de ces solutions n'offre à la fois la rapidité, un coût prévisible, une preuve vérifiable par tous, et l'assurance que personne ne peut disposer seul des fonds. C'est ce quadruple objectif qui a guidé la conception d'ACTUARUS.

CHAPITRE 4

## GENÈSE : UNE GRANGE, TROIS AMIS

*Comment ACTUARUS est née*

Tout commence par une amitié d'enfance. Etan et Arthur ont grandi ensemble, puis la vie les a éloignés. Des années plus tard, le hasard les remet face à face. Chacun a suivi sa route, et leurs compétences n'ont plus rien en commun.

Etan, lui, fait du commerce. Il achète et revend, le plus souvent de particulier à particulier, et il connaît intimement le problème que décrit Akerlof : aucune de ses transactions n'est réellement sécurisée, et il arrive que les produits livrés ne soient pas à la hauteur de ce qui avait été promis. Chaque achat est un pari.

Arthur, de son côté, évolue dans la blockchain depuis 2021. Il sait ce qu'un smart contract peut garantir là où la confiance fait défaut. Ensemble, ils décident de chercher une solution. Mais le constat est vite fait : Arthur maîtrise la blockchain sans avoir l'expérience du code nécessaire à un tel projet, et Etan n'a ni l'une ni l'autre.

C'est Etan qui connaît la pièce manquante : Wilfrid, un vétéran de l'informatique. Des années passées au service de grandes entreprises françaises, notamment dans l'assurance, et une participation à la création de la carte Vitale. Le genre de profil qui sait ce que veut dire construire un système auquel des millions de personnes doivent pouvoir se fier.

Les deux amis vont le trouver, leur idée en tête. Un jour, tous les trois se retrouvent dans une grange, à la campagne. Ils discutent, confrontent ce qu'ils savent, cherchent à comprendre ce que chacun voit du problème. Au fil des échanges, l'idée prend forme : un séquestre où le code remplace le tiers de confiance, et où personne ne peut disposer seul de l'argent des autres.

ACTUARUS est née là : d'une amitié retrouvée devenue un trio, d'un problème vécu, et d'une grange.

CHAPITRE 5

## DES CONTRATS PROGRAMMABLES

*De la machine à café au smart contract*

En 1997, l'informaticien et juriste Nick Szabo formalise la notion de *smart contract* [5] : un protocole qui exécute lui-même les clauses d'un contrat, de sorte qu'aucune partie ne puisse s'y soustraire. Son exemple fondateur est le distributeur automatique : la machine ne rend le produit qu'une fois la pièce reçue, sans qu'il soit besoin de faire confiance au commerçant.

Il faut attendre 2014 et le livre blanc d'Ethereum, rédigé par Vitalik Buterin [6], pour que ces contrats deviennent programmables sur une blockchain publique. Puis, en 2017, Anatoly Yakovenko présente Solana [7], une architecture conçue pour traiter un très grand nombre de transactions à très faible coût.

### Pourquoi Solana

- **Le coût** : les frais de réseau sur Solana représentent une fraction de centime par opération, ce qui permet à ACTUARUS de les prendre entièrement à sa charge. Sur Ethereum, ces frais auraient pesé directement sur le prix payé par les utilisateurs.
- **La vitesse** : une transaction est confirmée en quelques secondes, ce qui rend le verrouillage et la libération des fonds quasi instantanés.
- **L'écosystème** : l'EURC et l'USDC, les stablecoins de Circle, et le multisig Squads, qui sécurise les comptes d'ACTUARUS, sont disponibles nativement sur Solana.

CHAPITRE 6

## LE PRINCIPE ACTUARUS

*Le code tient les fonds, ACTUARUS orchestre la preuve*

Une transaction ACTUARUS suit quatre étapes. Les règles sont fixées avant le dépôt et ne peuvent plus être modifiées unilatéralement une fois les fonds bloqués.

**1** **Accord**
Les parties fixent le prix, l'état du bien, les conditions de réception et les critères de conformité. Ces termes forment un contrat électronique signé par les deux parties, via Firma, avec double authentification par e-mail.

**2** **Verrouillage**
L'acheteur dépose les fonds dans le smart contract, en EURC, en USDC ou en SOL. Ils sont bloqués par le code, dans un coffre propre à la transaction.

**3** **Vérification**
Le vendeur livre et dépose ses justificatifs ; l'acheteur inspecte le bien et confirme sa conformité. Une période de garantie s'ouvre, pendant laquelle l'acheteur peut contester.

**4** **Libération**
Le smart contract verse les fonds au vendeur. La transaction est close, horodatée, et inscrite dans l'historique infalsifiable du bien.

| Acteur | Son rôle | Ce qu'il ne peut pas faire |
|---|---|---|
| **Acheteur** | Dépose les fonds, confirme la conformité, peut ouvrir un litige. | Récupérer les fonds sans l'accord du vendeur ou de l'arbitre. |
| **Vendeur** | Livre le bien, dépose les justificatifs, reçoit le paiement. | Encaisser sans l'accord de l'acheteur, de l'arbitre, ou sans l'échéance de la garantie. |
| **Smart contract** | Conserve les fonds et exécute l'issue décidée. | Exécuter autre chose que ce que les parties ont signé. |
| **ACTUARUS** | Rédige le contrat, horodate, paie les frais de réseau, arbitre les litiges. | Déplacer les fonds seule, ou imposer un partage. |

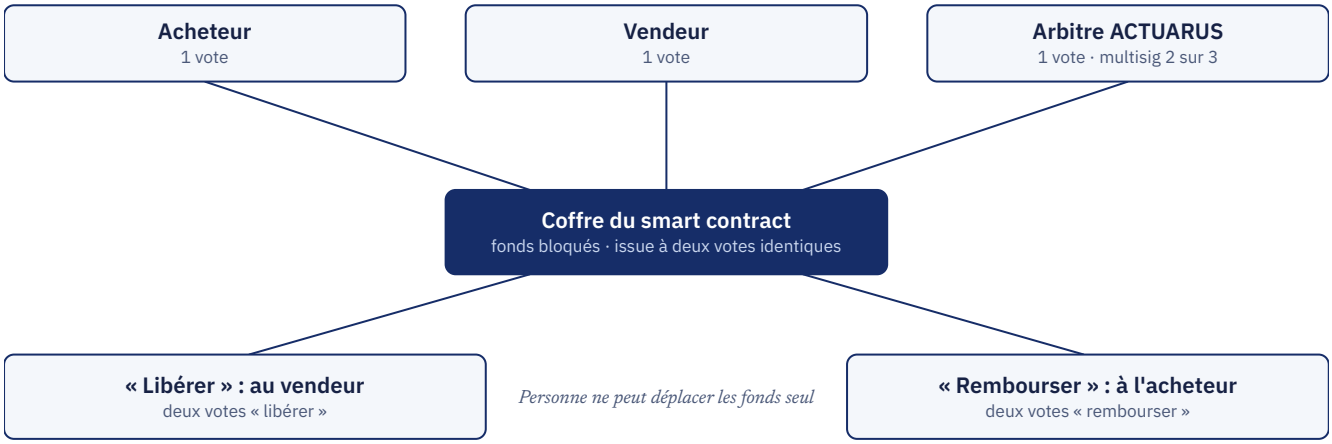
CHAPITRE 7

# ARCHITECTURE TECHNIQUE

*Ce que le code garantit*

Le programme de séquestre ACTUARUS est déployé sur Solana à l'adresse **DNwHyasEkHQYfswjPAxvnudCgN1gdZuHA2y2TSp8GVXE**. Il est développé avec le framework Anchor et son code source est publié sous licence Apache 2.0 [8].

**Un séquestre en multisignature deux sur trois.** Chaque dépôt réunit trois signataires distincts : l'acheteur, le vendeur et l'arbitre. Chacun vote une seule fois, « libérer » ou « rembourser », et son vote est définitif. Au deuxième vote identique, les fonds partent : au vendeur pour « libérer », à l'acheteur pour « rembourser ». Le programme vérifie que les trois comptes sont différents, afin qu'aucun signataire ne dispose de deux voix.




**Une période de garantie.** Une fois les justificatifs du vendeur déposés, une période de garantie s'ouvre, d'au moins 24 heures et d'au plus un an. À son terme, si aucun vote « rembourser » n'a été émis et qu'aucun litige ne l'a suspendue, n'importe qui peut déclencher le versement au vendeur. Les fonds ne restent donc jamais bloqués faute d'un second vote, et l'acheteur dispose toujours d'une journée entière au moins pour contester.

**Le remboursement partiel.** Le vendeur peut proposer de rendre une partie du montant ; si l'acheteur accepte ce montant exact, la part proposée lui revient et le reste va au vendeur, dans la même transaction. L'arbitre ne peut pas imposer de partage.

**Les frais réseau pris en charge.** Un compte de la plateforme, distinct de l'arbitre, paie les frais de réseau et la réserve de stockage de chaque compte. Les parties reçoivent exactement les montants prévus au dépôt. Ce compte n'est ni arbitre, ni destinataire des commissions.

| Élément | Détail |
|---|---|
| **Actifs acceptés** | SOL, USDC et EURC — pour les jetons, uniquement les émissions officielles de Circle, vérifiées par le programme. |
| **Commission** | Fixée et prélevée au moment du dépôt ; elle ne peut pas être modifiée en cours de transaction. |
| **Arbitre** | Coffre multisig Squads : chacun de ses votes exige l'approbation de deux signataires sur trois. |
| **Clôture** | Une fois le dépôt soldé, les comptes de la transaction sont fermés ; l'historique reste inscrit sur la blockchain. |

| Élément | Détail |
|---|---|
| **Preuve** | Contrat signé via Firma, empreinte et horodatage de chaque étape, consultables dans l'historique du bien. |

CHAPITRE 8

## LE TRAITEMENT DES LITIGES

*Une décision humaine, éclairée par un jury d'IA*

Un séquestre ne vaut que par la façon dont il traite les désaccords. Lorsqu'un litige est ouvert, la période de garantie est suspendue et les fonds restent bloqués.

**1 Ouverture**
L'une des parties ouvre le litige. Chacune transmet ses preuves : photos, échanges, documents.

**2 Jury**
Cinq agents d'intelligence artificielle sont tirés au sort parmi cent, selon la nature de la transaction. Aucune partie ne choisit ses jurés.

**3 Analyse**
Chaque agent examine le contrat signé, les preuves et les sources juridiques, puis rend un avis motivé.

**4 Décision**
Un membre de l'équipe ACTUARUS vérifie le dossier et les avis du jury, et décide sous cinq jours du remboursement de l'acheteur ou du paiement du vendeur.

La décision se traduit sur la blockchain par le vote de l'arbitre. Ce vote ne suffit jamais à lui seul : il doit rejoindre celui de l'une des deux parties pour atteindre la majorité de deux voix. Aucun fonds n'est remboursé ou libéré par une intelligence artificielle seule, et aucun ne peut l'être par ACTUARUS seule.

D'autres projets ont exploré l'arbitrage entièrement décentralisé, en confiant la décision à des jurés anonymes rémunérés en jetons [9]. ACTUARUS a fait un autre choix : celui d'une décision humaine identifiable et responsable, appuyée par l'analyse systématique d'un jury d'IA.

CHAPITRE 9

## SÉCURITÉ

*Vérifiable par tous, pas seulement par nous*

| Garantie | Mise en œuvre |
|---|---|
| **Audit** | Smart contract audité par AMJI-CONCEPT ; version 1.3.0, audit du 6 novembre 2026. Les corrections issues de l'audit sont référencées dans le code. |
| **Code public** | Source publiée sur GitHub (Actuarus/escrow-program), sous licence Apache 2.0. |
| **Build vérifiable** | Le programme se recompile de façon reproductible : chacun peut vérifier que le code publié est bien celui qui est déployé sur Solana. |
| **Mises à jour encadrées** | L'autorité de mise à jour est un multisig Squads deux sur trois, assorti d'un délai de 48 heures avant toute modification. |
| **Immuabilité** | Le contrat devient immuable à l'issue d'une période de maintenance corrective de trois mois suivant son lancement. |
| **Séparation des clés** | Le compte qui paie les frais, l'arbitre et l'autorité de mise à jour sont trois comptes distincts. La clé de test ne peut pas être compilée pour le réseau principal. |
| **Signalement** | Contact sécurité publié : contact@actuarus.com. |

CHAPITRE 10

## MODÈLE ÉCONOMIQUE

*Un tarif connu avant de s'engager*

ACTUARUS se rémunère par une commission dégressive, calculée par tranches : chaque taux ne s'applique qu'à la part du prix comprise dans sa tranche. Les frais de réseau, le contrat électronique, la preuve on-chain et le traitement des litiges sont inclus. Il n'y a ni frais d'inscription, ni abonnement, et les parties choisissent qui règle la commission.

| Tranche du prix | Taux sur la tranche |
|---|---|
| **Jusqu'à 10 000 €** | 5,5 % |
| **De 10 000 à 50 000 €** | 5 % |
| **De 50 000 à 100 000 €** | 3,8 % |
| **De 100 000 à 500 000 €** | 2,5 % |
| **De 500 000 à 1 000 000 €** | 2 % |
| **Au-delà de 1 000 000 €** | 1 % |

À titre d'exemple, une transaction de 15 000 € coûte 800 €, soit 5,33 % ; une transaction de 100 000 € coûte 4 450 €, soit 4,45 %. Le montant minimal est de 5 € par transaction. Un devis personnalisé est proposé aux gros volumes et aux places de marché.

**Le parrainage.** Tout utilisateur peut recommander ACTUARUS. Lorsque le vendeur a été parrainé, le parrain reçoit 20 % de la commission d'ACTUARUS sur chacune de ses ventes, sans plafond. Le parrainage ne modifie pas le prix payé par les parties.

CHAPITRE 11

## CADRE JURIDIQUE

*Une architecture conçue pour le droit européen*

La solution ACTUARUS se situe **hors du champ du règlement européen MiCA** [10]. ACTUARUS n'est ni établissement de paiement, ni dépositaire : elle ne conserve, n'échange ni ne transfère de crypto-actifs pour le compte de ses utilisateurs, et ne peut déplacer seule aucun fonds séquestré. La conversion entre euros et stablecoins s'effectue auprès de prestataires agréés, choisis par les utilisateurs.

**Le règlement en stablecoins agréés.** L'EURC et l'USDC sont des jetons de monnaie électronique émis par un établissement agréé dans l'Union européenne, adossés un pour un et remboursables à leur valeur nominale.

**La signature électronique.** Les contrats sont signés via Firma, sous la forme d'une signature électronique au sens du règlement eIDAS [11], renforcée par une double authentification. Le contrat signé, son horodatage et la trace on-chain constituent ensemble la preuve de la transaction.

**Les données personnelles.** Aucune donnée d'identité n'est inscrite en clair sur la blockchain. Les obligations propres aux utilisateurs sont détaillées dans les notes de conformité publiées par ACTUARUS.

CHAPITRE 12

## FEUILLE DE ROUTE

*Ce qui est fait, ce qui vient*

| Étape | Statut |
|---|---|
| **Programme de séquestre déployé sur Solana, code source publié** | Réalisé |
| **Audit du smart contract par AMJI-CONCEPT, version 1.3.0** | Réalisé · novembre 2026 |
| **Contrat électronique Firma, jury d'IA et décision humaine** | Réalisé |
| **Programme de parrainage** | Réalisé |
| **Fin de la maintenance corrective : contrat définitivement immuable** | Trois mois après le lancement |
| **Offre dédiée aux places de marché, intégrée à leur parcours** | À venir |
| **Ouverture à d'autres réseaux, dont Ethereum, lorsque les coûts le permettront** | Horizon |

CHAPITRE 13

# CONCLUSION

*Le contrat, et rien que le contrat*

En 2008, Nakamoto imaginait un séquestre « courant » pour protéger les acheteurs. ACTUARUS en propose une réalisation concrète : un contrat signé par deux parties libres, exécuté par un code que chacun peut lire, et dont aucune partie — pas même ACTUARUS — ne peut détourner les fonds seule.

Cette idée est plus ancienne que la blockchain. Au XIXe siècle déjà, le juriste américain Lysander Spooner défendait que l'autorité d'un engagement ne tient qu'au consentement de ceux qui s'y lient [12] :

> *« La Constitution n'a aucune autorité ou obligation qui lui soit propre. Elle n'a d'autorité ou d'obligation que comme contrat entre les hommes. »*
>
> Lysander Spooner (1808-1887), *No Treason*, n° VI, 1870 [12]

ACTUARUS applique ce principe à l'échange : la seule règle qui compte est celle que les parties ont signée. Et parce que la blockchain n'a d'intérêt que si elle résout un problème concret, nous avons choisi d'en résoudre un, que chacun a déjà rencontré : faire confiance à un inconnu.

# RÉFÉRENCES

[1] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. bitcoin.org/bitcoin.pdf

[2] Akerlof, G. A. (1970). The Market for “Lemons”: Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, 84(3), 488-500.

[3] Federal Bureau of Investigation (2025). *Internet Crime Report 2024*. Internet Crime Complaint Center (IC3).

[4] Chambre de commerce internationale (2007). *Règles et usances uniformes relatives aux crédits documentaires*, publication n° 600 (RUU 600).

[5] Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, 2(9).

[6] Buterin, V. (2014). *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*.

[7] Yakovenko, A. (2017). *Solana: A new architecture for a high performance blockchain*.

[8] ACTUARUS (2026). Programme de séquestre, version 1.3.0. github.com/Actuarus/escrow-program

[9] Lesaege, C., Ast, F. et George, W. (2019). *Kleros*, short paper.

[10] Règlement (UE) 2023/1114 du 31 mai 2023 sur les marchés de crypto-actifs (MiCA).

[11] Règlement (UE) n° 910/2014 du 23 juillet 2014 (eIDAS), modifié par le règlement (UE) 2024/1183.

[12] Spooner, L. (1870). *No Treason, No. VI: The Constitution of No Authority*. Boston.

Ce technical paper décrit le fonctionnement d'ACTUARUS à la date de sa publication. Il ne constitue ni une offre au public de crypto-actifs, ni un conseil en investissement, ni une consultation juridique ou fiscale. ACTUARUS n'émet aucun jeton. Contact : contact@actuarus.com