

**Sauge (\$SAL)** /'salviam/

*Nom* (du latin salvus, signifiant sûr, sécurisé, salut) Un protocole privé de première couche avec génération de rendement, jalonnement et concentration sur la conformité réglementaire.

---

## Introduction

Salvium est une blockchain privée de preuve de travail de pointe qui combine de manière transparente les capacités de jalonnement, de confidentialité et de DeFi tout en naviguant dans les réglementations cryptographiques. Construit sur un fork de Monero, il conserve les fonctionnalités avancées de confidentialité de Monero telles que les adresses furtives et les signatures en anneau. Cependant, Salvium introduit des innovations révolutionnaires qui modifient considérablement les mécanismes de transaction, créant ainsi une solution unique dans l'espace DeFi.

## Innovation

Salvium a commencé comme un projet de recherche visant à explorer le potentiel de CryptoNote pour la DeFi privée. L'équipe a revisité et prototypé les travaux des chercheurs de Monero, en se concentrant sur l'évolutivité, l'extensibilité et l'interopérabilité multi-chaînes. Cette recherche a également pris en compte les changements réglementaires mondiaux, notamment dans le cadre de MiCA, positionnant Salvium comme une évolution essentielle de CryptoNote et Monero.

Salvium adopte une approche « axée sur la confidentialité d'abord » et s'efforce de se conformer pleinement à la réglementation des marchés de crypto-actifs (MiCA). Les premières phases incluent des fonctionnalités telles que les paiements remboursables et les modes d'échange pour assurer la conformité. Au cours de la dernière année, nous avons réalisé des progrès en matière de paiements conditionnels (CP), de paiements remboursables, de rendement natif et de jalonnement. Certaines de ces fonctionnalités sont prêtes à être lancées, tandis que d'autres seront incluses dans les futures mises à jour.

Salvium introduit des avancées technologiques uniques, telles que les déséquilibres transactionnels (TI) et les transactions asynchrones (AT), formant le premier système natif CryptoNote système de jalonnement et de rendement, qui stimule le développement futur et constitue le fondement de l'écosystème.

## DeFi privé

S'appuyant sur ces avancées technologiques, Salvium est sur le point de fournir des fonctionnalités robustes de finance décentralisée (DeFi) axées sur une confidentialité conforme et programmable.

**Confidentialité programmable:** La couche de base Salvium a hérité des niveaux d'intimité exceptionnels de Monero. Dans les cas où ce niveau de confidentialité n'est pas possible, comme

dans le cas d'interactions CEX et d'applications DeFi conformes, Salvium permettra aux développeurs de DApp de créer des DApp avec différentes couches de confidentialité, qui permettront à leurs utilisateurs de sélectionner le type de données qu'ils partagent. Il en résulte une confidentialité contrôlable ou programmable, sans les limitations typiques des pièces de confidentialité traditionnelles.

## L'avenir de la DeFi

Salvium inclut déjà des fonctionnalités qui permettent mathématiquement de créer des applications DeFi sur la couche 1. Celles-ci seront développées davantage dans la phase 3, où une solution de couche 2 pourra être incorporée, avec des avantages inhérents en termes de performances et d'évolutivité. Dans les deux cas, ces innovations fondamentales contribueront à rendre DeFi plus privée.

**Paiements conditionnels** : CP permet aux transactions d'être exécutées conditionnellement en fonction de critères prédéfinis. Cela permettra Les Smart Contracts, qui débloquent un torrent d'applications potentielles.

**Intergiciel**: Salvium proposera un middleware pour une intégration transparente avec d'autres plateformes de cryptographie. Cela permettra aux développeurs d'adapter facilement des applications écrites dans des langages comme Solidity (le principal langage DApp d'Ethereum) pour une utilisation sur Salvium. En conséquence, les DApp existantes peuvent être lancées rapidement et efficacement sur le réseau Salvium.

## Applications DeFi potentielles

Une fois que ces fonctionnalités seront disponibles sur Salvium, les tiers créeront rapidement des DAAP, positionnant Salvium comme une alternative à Ethereum axée sur la confidentialité.

Cela inclut les échanges décentralisés (DEX), les protocoles de prêt et d'emprunt, l'agriculture de rendement, les Stablecoins, les NFT, les Memecoins et les jeux de hasard.

## Pourquoi Crypto a-t-il besoin de Salvium ?

P.La rivalité est un droit humain fondamental, mais cela ne signifie pas qu'elle doit être utilisée à des fins néfastes. Salut s'efforce de créer une plate-forme décentralisée qui défend une utilisation éthique, en protégeant la confidentialité des utilisateurs tout en restant conforme aux lois et réglementations applicables.

Le de nouvelles réglementations affectant les crypto-monnaies privées existantes créent un besoin pressant d'une nouvelle pièce de confidentialité garantissant la confidentialité et la conformité. La plupart Les jetons DeFi fonctionnent sur des blockchains publiques, exposant les données sensibles des utilisateurs. Salut résoudra ce problème en permettant aux utilisateurs d'équilibrer la confidentialité et la conformité réglementaire.

## Réalisation confidentialité conforme

La réglementation MiCA de l'UE exige que les jetons de confidentialité s'adaptent, ce qui est au cœur du projet Salvium. Dans un premier temps, la réglementation obligera les échanges centralisés à démasquer les transactions impliquant des pièces de confidentialité comme Monero et ZCash. P.les pièces de monnaie de rivalité qui ne respectent pas ces réglementations risquent épicerie finechose.

Le règlement 2023/1114 du Parlement européen stipule :

*" Les règles de fonctionnement de la plateforme de négociation de crypto-actifs empêchent l'admission à la négociation de crypto-actifs dotés d'une fonction d'anonymisation intégrée, à moins que les détenteurs de ces crypto-actifs et leur historique de transactions puissent être identifiés par les prestataires de services sur crypto-actifs opérant une plateforme de trading de crypto-actifs. »*

Source: <https://eur-lex.europa.eu/eli/reg/2023/1114/oj> Article 76, paragraphe (3)

## Principales fonctionnalités pour Cconformité

Pour respecter cette réglementation particulière, le protocole exigera :

1. **Capacité à rejeter et retour transactions:** Un protocole conforme doit permettre aux bourses de rejeter les transactions non autorisées provenant de portefeuilles non autorisés. Cette fonctionnalité n'est généralement pas possible avec les pièces de confidentialité traditionnelles.
2. **Visibilité des wallets autorisés :** Les bourses nécessitent la capacité de surveiller les transactions dans les portefeuilles autorisés utilisés pour déposer des fonds sur leur plateforme.

Salvium répondra à cette exigence par:-

1. Anonymement rtransactions remboursables : une fonctionnalité rare dans les autres pièces de confidentialité.
2. Un portefeuille visible (ou sous-adresse) histoire. Les utilisateurs peuvent fournir une clé d'affichage complète qui donnera des échanges un « mécanisme de visualisation du portefeuille », non seulement la vue limitée actuellement fournie, mais aussi l'historique complet comme l'exigent les régulateurs.

L'approche de Salvium permet une transparence sélective permettant aux utilisateurs de contrôler leur vie privée. Par exemple, les utilisateurs peuvent garder leurs transactions privées mais partager une « clé d'affichage » avec les bourses pour vérifier l'historique de leurs transactions lorsque cela est nécessaire pour des raisons de conformité. Cela équilibre les besoins en matière de confidentialité et de réglementation, comme les relevés bancaires révélateurs à des fins fiscales.

L'objectif est de maintenir une position de leader en matière de respect de la vie privée alors que la communauté surveille et analyse de manière proactive les évolutions réglementaires dans diverses juridictions du monde, en mettant particulièrement l'accent sur la réglementation des États-Unis et de l'UE sur les marchés d'actifs cryptographiques (MiCA).

## Projet Phases

### Phase 1 : Lancer le sauvetage

Jalonnement et rendement Génération:

Pour démontrer les capacités améliorées fournies par la confidentialité évoluée de Salvium et l'un des fondements du concept Salvium, depuis le lancementLes utilisateurs peuvent miser leurs jetons SAL pour gagner des récompenses, favorisant ainsi un réseau sécurisé et engagé.

La première étape vers une conformité totale est également fournie au lancement ; transactions remboursables, qui permettent le retour de transactions non autorisées ou incorrectes. Les transactions remboursables permettent au destinataire de toute transaction de renvoyer cette entrée précise (moins les frais de transaction standard) à l'expéditeur d'origine sans avoir besoin de demander une adresse. Cette fonctionnalité est triviale sur les blockchains publiques, mais elle constitue une étape majeure vers la conformité pour une chaîne basée sur Monero.

## Phase 2 : fonctionnalités de conformité supplémentaires

### Blockchain privée avec fonctionnalités de conformité :

Salvium se développera continuellement pour répondre aux exigences réglementaires strictes, en particulier les réglementations MiCA de l'UE. La phase 2 permettra aux utilisateurs de garder leurs transactions privées tout en fournissant aux entités autorisées, comme les bourses, une clé de vue pour vérifier l'historique de leurs transactions. Cette approche garantit la confidentialité des utilisateurs tout en restant conforme aux exigences réglementaires.

L'équipe de développement de Salvium se consacre à l'avancement des technologies fondamentales de Monero et CryptoNote. Nous nous engageons à contribuer et à soutenir les initiatives de conformité, notamment les preuves d'adhésion à la chaîne complète, SERAPHIS et JAMTIS, à mesure que les opportunités se présentent. Cet engagement reflète nos efforts continus pour améliorer la confidentialité, la sécurité et la compatibilité réglementaire au sein de l'écosystème Salvium.

## Phase 3 : prise en charge DeFi

### Fonctionnalité de contrat intelligent et émission de jetons privés:

En tirant parti de l'innovation `protocol_tx`, Salvium permettra des fonctionnalités de contrat intelligent, permettant aux applications DeFi complexes de fonctionner de manière sécurisée et privée sur son réseau.

### Middleware pour la solidité :

Pour rationaliser l'adoption et le développement, Salvium proposera un middleware qui permettra aux DApps développés dans Solidity, le langage de programmation incontournable pour les DApps Ethereum, d'être rapidement ajustés et déployés sur son réseau. Cette décision vise à simplifier la transition des projets Ethereum existants vers Salvium, réduisant ainsi la barrière à l'entrée pour les développeurs.

## Frais et incitations

### Récompenses de mise

Détenteurs de Salvium (SAL) qui mettent en jeu leurs jetons volonté gagner un récompense de mise. Pour participer, les utilisateurs doivent verrouiller leur SAL pour un prédéterminé période (21 600 blocs - environ 30 jours). Les récompenses de mise sont distribuées à l'expiration de la période de verrouillage. Les récompenses proviennent de l'une des deux sources selon la phase du projet.

### Bloquer le partage de récompenses

Les grévistes bénéficiera d'une part de 20 % des récompenses de bloc pendant la phase initiale du projet. Ces récompenses seront distribuées proportionnellement parmi tous les acteurs actifs, incitatif les utilisateurs à participer au réseau et justificatif sa sécurité.

## Long terme - Frais DeFi

À l'avenir, les récompenses de mise passeront d'une part de la récompense globale à un modèle de distribution de frais basé sur l'utilisation. Les jalonneurs et les mineurs recevront des frais système, similaires aux frais de gaz sur d'autres réseaux blockchain.

## Technologie

Salvium prolonge la CryptoNote protocole avec plusieurs innovations clés, notamment des adresses de remboursement, des transactions asynchrones et des clés d'affichage affichant l'intégralité des soldes du portefeuille. Ces améliorations garantissent un anonymat de haut niveau tout en permettant des règles complexes et des tokenomics pour la génération de rendement et la fourniture de fonctionnalités defi.

En tirant parti de technologies avancées de confidentialité telles que les signatures en anneau, les adresses furtives et les preuves sans connaissance, Salvium préserve la confidentialité tout en permettant une transparence sélective à des fins de conformité. Ces fonctionnalités répondent collectivement aux demandes de fonctionnalité DeFi, de confidentialité des transactions, de décentralisation et de réglementation responsable, faisant de Salvium une solution pionnière en matière de finance numérique.

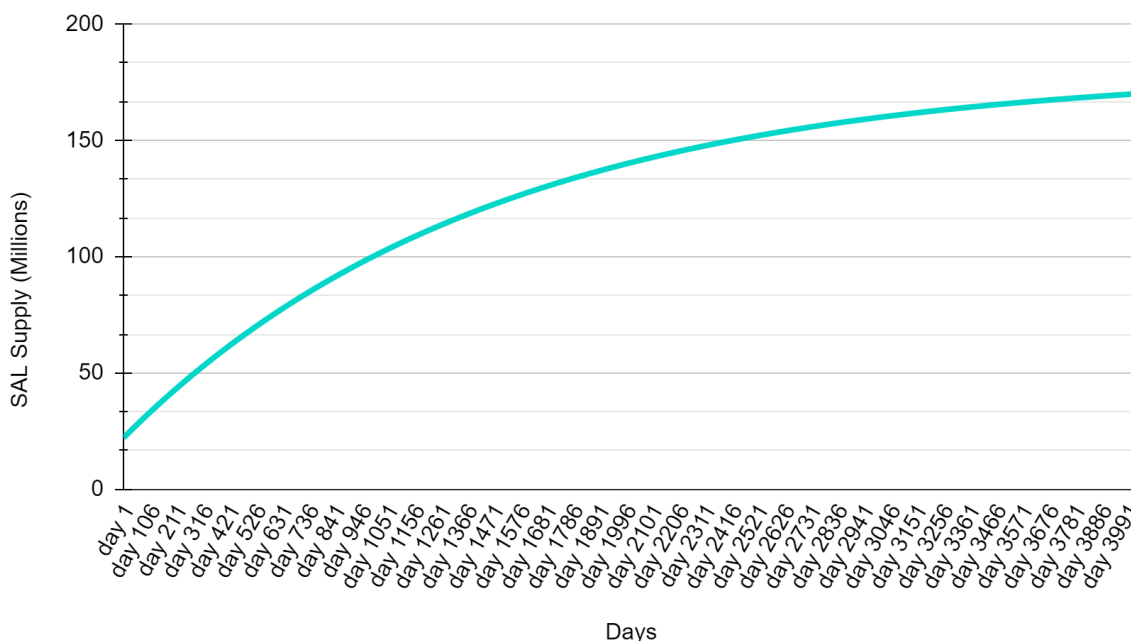
## Exploitation minière

Salvium est une pièce de preuve de travail qui utilise l'algorithme de minage RandomX. Une fois les fonctionnalités DeFi opérationnelles, les mineurs recevront également une part des frais système.

## Calendrier d'émission

Le calendrier d'émission est basé sur une version modifiée de Monero, pour promouvoir une plus grande liquidité et une adoption grâce à une distribution plus large. Alors que le temps de blocage reste à 120 secondes, l'émission par bloc a été multipliée par cinq et la durée d'approvisionnement initiale a été doublée. Cela se traduit par une offre initiale de 184,4 millions de pièces, présentant une courbe d'émission plus plate et plus large que celle de Monero.

Salvium Emissions Curve



## Émissions de queue

Comme Monero, Salvium intègre une émission résiduaire pour garantir des incitations minières à long terme et la sécurité du réseau. Une fois l'offre maximale atteinte, le protocole émettra 3 SAL par bloc.

## Frais de transaction

Les frais de transaction Savlium, tout comme ceux de Monero, sont dynamiques et dépendent de plusieurs facteurs. Le calcul peut être simplifié comme suit :

Frais = Frais de base × Taille de la transaction (Ko)

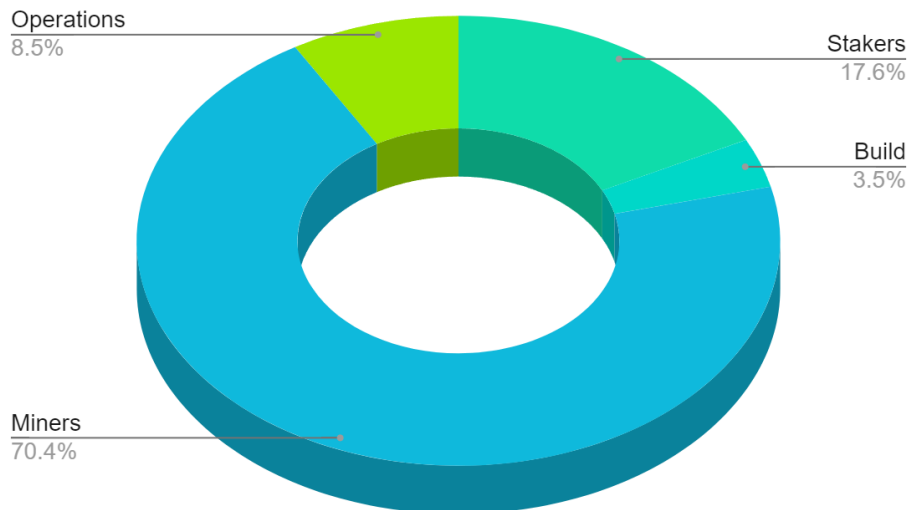
Les coûts de transaction typiques seront très faibles.

**Structure de récompense de bloc :** Chaque bloc extrait sur le réseau Savlium comprend toutes les transactions soumises depuis le dernier bloc. Le mineur qui réussit à extraire un bloc recevra tous les frais des transactions incluses dans ce bloc, ainsi que toutes les pièces Savlium nouvellement émises.

## Salut Allocation de jetons

Le projet est financé par une pré-mine de 12,01%, partiellement verrouillée. Ces fonds seront alloués à la construction et aux opérations. Les mineurs et les jalonneurs gagneront 88 % de l'offre totale,

plus les émissions résiduelles.



*Remarque : les pourcentages indiqués correspondent à la proportion des pièces de 184 millions de Salvium, à l'exclusion des émissions finales.*

### 1. Construire - 3,5%

Salvium est devenu une réalité début 2023 grâce à la vision et au dévouement de ses premiers développeurs et contributeurs. 3,53 % de la pré-mine sera allouée pour inciter ces membres actifs de l'équipe et ces fournisseurs à soutenir le lancement du projet.

### 2. Opérations - 8.48% (verrouillé)

Le succès et la durabilité à long terme du protocole Salvium reposent sur un développement et une innovation continus. Pour soutenir cela, 8,48 % de l'offre initiale est réservée aux améliorations continues, à l'intégration de contrats intelligents et à la mise en œuvre de nouvelles fonctionnalités via des programmes de primes et de subventions.

Ces jetons sont verrouillés dans le temps dans un portefeuille de gouvernance et libérés en 24 versements mensuels égaux. À la fin de cette période, le projet vise à être autonome, financé par les redevances système (taxes sur le gaz) générées au sein de l'écosystème.

### 3. Bloc Récompenses - 87,99%

La récompense de bloc est initialement répartie entre les jalonnes (20 %) et les mineurs (80 %). Une fois les fonctionnalités DeFi opérationnelles, les mineurs recevront 100 % de la récompense de bloc, tandis que les intervenants recevront une part des frais du système.

# Vérifications indépendantes

Salvium sera soumis à des audits de sécurité indépendants avant les mises à niveau majeures. Les rapports d'audit seront rendus publics, démontrant notre engagement en faveur de la transparence et de la sécurité. Les commentaires de la communauté et les résultats des audits guideront les améliorations continues du protocole.

## Audit préalable au lancement par Cypher Stack

L'audit préalable au lancement de Salvium se concentre sur l'examen de la validité mathématique et de la sécurité des technologies clés uniques à Salvium, à savoir :

1. Le mécanisme du « déséquilibre transactionnel ». Ceci a été conçu par l'équipe et utilisé pour implémenter la technologie « protocol\_tx », et
2. Le « Return Address Scheme », initialement proposé par knacc, incluant les adaptations pour prendre en charge les transactions asynchrones mises en œuvre par la technologie « protocol\_tx » contenue dans Salvium

L'audit pré-lancement de Salvium a été réalisé par Cypher Stack, spécialiste de la sécurité Monero. L'expertise de Cypher Stack en matière de recherche, de développement et de consultation cryptographique garantit que notre plateforme repose sur une base solide de sécurité et d'innovation.

## Équipe

L'équipe est composée d'une large communauté et de développeurs. Tous les passionnés de cryptomonnaies sont engagés et incités à agir dans le meilleur intérêt du projet. Ils apportent chacun une richesse d'expérience et un historique de réussite avéré dans la finance décentralisée et la crypto-monnaie privée.

## Coordonnées

Site

web: [salvium.io](https://salvium.io)

Discorde

: [discord.gg/YJmdGcdtDt](https://discord.gg/YJmdGcdtDt)

X : [x.com/salvium\\_io](https://x.com/salvium_io)

GitHub : [github.com/somerandomcryptoguy/salvium](https://github.com/somerandomcryptoguy/salvium)

Faire un

don: <https://salvium.io/donate/>



# Annexe 1

## Distribution de jetons et position réglementaire

Suite au Dans le cadre de la réglementation de l'Union européenne sur les crypto-actifs, notamment l'exigence d'un « livre blanc sur les crypto-actifs », nous présentons les informations suivantes :

1. Informations sur l'émetteur : Salvium est développé par une équipe décentralisée de passionnés de cryptographie et de développeurs déterminés à faire progresser la technologie blockchain axée sur la confidentialité.
2. Aperçu du projet : Salvium vise à créer une blockchain centrée sur la confidentialité qui combine les avantages des fonctionnalités de confidentialité de Monero avec la conformité réglementaire et les capacités DeFi.
3. Distribution et statut réglementaire :
  - Salvium (SAL) ne procède pas à une offre publique. La distribution initiale des jetons SAL se fait uniquement via le minage.
  - Une petite partie de l'offre totale a été pré-exploitée pour soutenir le développement et les opérations.
  - Comme Salvium ne fait pas d'offre au public (ICO), il n'entre pas actuellement dans le champ d'application de la réglementation européenne sur les crypto-actifs qui exige un livre blanc sur les crypto-actifs pour les offres publiques.
  - Bien que nous ne soyons pas actuellement soumis à ces réglementations spécifiques, nous nous engageons à maintenir la transparence et à adhérer aux meilleures pratiques dans le domaine des cryptomonnaies.
4. Droits, obligations et vote : a) Droits :
  - Les mineurs de SAL participent au consensus du réseau via l'exploitation minière, les détenteurs peuvent s'engager dans des mises pour obtenir des récompenses et utiliser le jeton pour des transactions au sein de l'écosystème Salvium.
5. Obligations :
  - Les détenteurs de jetons sont tenus de se conformer aux lois et réglementations applicables dans leurs juridictions.
6. Droit de vote:
  - La détention de jetons SAL ne confère aucun droit de vote ni contrôle de gouvernance sur le projet Salvium.
  - Les processus de développement et de prise de décision du projet sont ouverts et collaboratifs, avec des contributions bienvenues de l'ensemble de la communauté Salvium. Même si un groupe central de développeurs peut guider certains aspects du projet, nous nous efforçons de décentraliser à la fois notre technologie et notre gouvernance.
7. Technologie sous-jacente : Salvium est construit sur un fork de la base de code Monero, utilisant le protocole CryptoNote avec des innovations supplémentaires telles que les déséquilibres transactionnels (TI) et les transactions asynchrones (AT).
8. Risques associés :
  - Risque réglementaire : le paysage réglementaire des cryptomonnaies évolue rapidement. Bien que Salvium s'engage à respecter la réglementation, rien ne garantit que nous serons en mesure de répondre à toutes les exigences réglementaires futures. Les changements de réglementation pourraient potentiellement avoir un impact sur les opérations de Salvium, l'utilisation des jetons SAL ou leur valeur. Les utilisateurs doivent être conscients que : a) De nouvelles réglementations peuvent être introduites et susceptibles d'affecter le statut juridique ou le modèle opérationnel de Salvium. b) Notre interprétation des réglementations

existantes peut différer de celle des autorités de régulation. c) Malgré tous nos efforts, nous ne serons peut-être pas en mesure de nous adapter rapidement à tous les changements réglementaires. d) Les offres futures de Salvium peuvent être soumises à des exigences réglementaires différentes.

- Risque technologique : comme pour tous les projets blockchain, il existe un risque de vulnérabilités non découvertes dans le code ou dans les principes cryptographiques sous-jacents.
- Risque de marché : la valeur des jetons SAL peut être volatile et soumise aux conditions du marché.
- Risque d'adoption : Le succès de Salvium dépend de l'adoption et du développement de la communauté.

Ces informations sont fournies de bonne foi et représentent notre compréhension et nos projets actuels. Cela ne doit pas être considéré comme un conseil financier. Nous encourageons tous les participants potentiels à mener leurs propres recherches et à demander conseil à un professionnel si nécessaire.