

ZKP - zkPass

zkPass est un protocole d'oracle décentralisé qui révolutionne la manière dont les données privées d'Internet sont vérifiées sur la blockchain. Sa technologie clé, zkTLS, est une fusion de 3P-TLS (Three-Party Transport Layer Security) et de cryptographie Hybrid-ZK (Zero-Knowledge). Cette combinaison permet aux utilisateurs de prouver l'authenticité de leurs informations provenant de n'importe quel site web HTTPS sans jamais révéler les données brutes elles-mêmes. Cela est rendu possible grâce à la génération locale de preuves cryptographiques, garantissant ainsi la confidentialité et la sécurité des utilisateurs.

L'utilité principale de zkPass réside dans sa capacité à créer un pont entre les données Web2 et les applications Web3 de manière sécurisée et privée. Les cas d'usage potentiels sont vastes et incluent, sans s'y limiter, la vérification d'identité pour la conformité (KYC, AML), la preuve d'historique financier ou d'éducation, l'accès à des services ou des airdrops conditionnels, et la participation à la gouvernance décentralisée. Le protocole élimine le besoin de partage de documents, de clés API ou d'intermédiaires centralisés, offrant ainsi une solution plus fiable et respectueuse de la vie privée.

Le token ZKP est le cœur économique de l'écosystème zkPass. Il s'agit d'un token utilitaire et de gouvernance, basé sur la norme ERC-20, avec une offre totale fixe d'un milliard de tokens. Les fonctions du token ZKP sont multiples :

- **Règlement des preuves** : ZKP est utilisé comme moyen de paiement pour la génération et la vérification des preuves cryptographiques au sein du réseau.
- **Garantie pour les validateurs** : Les validateurs doivent mettre en jeu des tokens ZKP comme garantie opérationnelle pour assurer l'intégrité, la disponibilité et la fiabilité du réseau.
- **Crédits réseau** : ZKP sert de crédits sur la chaîne pour enregistrer et comptabiliser les contributions au réseau, y compris le calcul vérifiable et les intégrations.
- **Accès aux services** : Les entreprises et les développeurs utilisent ZKP pour accéder aux APIs de vérification natives à ZK et à l'infrastructure de données préservant la vie privée.
- **Gouvernance** : Le token ZKP permet aux détenteurs de participer aux décisions de

gouvernance via la DAO (Organisation Autonome Décentralisée) de zkPass, influençant ainsi l'évolution du protocole.

La tokenomique de ZKP prévoit une allocation de 48,5% à la communauté, comprenant des airdrops vérifiables, des incitations au réseau et des ventes communautaires. Les investisseurs initiaux reçoivent 22,5%, les contributeurs principaux 14%, la trésorerie de la DAO 10%, et 5% sont dédiés à la liquidité. Des mécanismes déflationnistes, tels que la combustion d'une partie des frais de règlement et des rachats périodiques menés par la DAO, sont prévus pour maintenir la rareté du token.

zkPass a levé des fonds significatifs auprès d'investisseurs de premier plan, renforçant sa position dans le secteur de l'identité décentralisée et de la confidentialité. Le projet a développé des partenariats stratégiques, notamment avec des plateformes comme Binance et Coinbase, qui témoignent de la reconnaissance croissante de sa technologie. Malgré ses avantages en matière de confidentialité et de sécurité, le projet fait face à des défis réglementaires potentiels, notamment concernant les 'privacy coins'. Néanmoins, avec son approche innovante et ses applications concrètes, zkPass et son token ZKP sont positionnés pour jouer un rôle important dans l'évolution de l'infrastructure de données décentralisée.