

Lancement d'une application de messagerie privée sur xx network, le réseau décentralisé à résistance quantique

La première application de messagerie à résistance quantique au monde, [xx messenger](#), est lancée aujourd'hui sur le xx network. xx messenger permet aux utilisateurs de communiquer en temps réel via des centaines de nœuds décentralisés déployés à l'échelle mondiale. L'application est téléchargeable sur IOS et Android, est dotée d'une messagerie de groupe ainsi que d'un partage de photo et d'audio, et conçue pour une facilité d'utilisation et une transition depuis les applications de messagerie existantes.

Ce communiqué de presse contient des éléments multimédias. Voir le communiqué complet ici : <https://www.businesswire.com/news/home/20220125005777/fr/>

David Chaum (Photo: Business Wire)



À la différence des applications de messagerie existantes, xx messenger utilise une cryptographie à résistance quantique pour protéger le contenu des messages contre le décodage et le logiciel cMix afin d'obscurcir et parceller les informations de métadonnées à propos de qui envoie, de l'heure d'envoi, du lieu d'envoi, et de qui reçoit. Des groupes de nœuds xx sélectionnés aléatoirement encryptent des ensembles anonymes de 1 000 messages, qui sont ensuite mélangés plusieurs fois et encryptés à l'aide d'une cryptographie à résistance quantique. Les informations qui relient les envoyeurs aux destinataires sont détruites, empêchant les tiers de tracer les détails personnels à propos de nos habitudes et de la structure de nos vies.

Les fournisseurs de services centralisés suivent et profilent la majorité des utilisateurs numériques. Nos informations personnelles ont été commercialisées, mises aux enchères et monétisées d'une manière de plus en plus abusive pour des groupes d'annonceurs et de politiques, qui les utilisent pour microcibler et manipuler les consommateurs ou les électeurs. Les

plateformes décentralisées offrent une opportunité unique de déployer les principes de confidentialité des débuts d'internet dans la structure de l'écosystème web3 émergent. xx messenger est dédié à la protection et au renforcement des droits inaliénables de confidentialité à l'aube du web3.

- L'encodage actuel des messages ne dispose pas de résistance quantique: il est communément admis que, dans des délais réalistes, les ordinateurs quantiques seront en mesure de décoder les communications encodées par une cryptographie conventionnelle. Les messages envoyés sur toutes les autres messageries existantes, mêmes celles dotées d'un « solide encodage de bout en bout », seront aisément décodés rétroactivement et analysés par l'intelligence artificielle. Seules les communications réalisées à l'aide de xx messenger resteront privées.
- xx est le seul à offrir le parcellement des métadonnées: toutes les messageries généralistes actuelles peuvent saisir et potentiellement exploiter les métadonnées. Le parcellement des métadonnées consiste en l'envoi de messages via des nœuds xx network choisis aléatoirement à l'échelle mondiale. Chaque nœud change l'ordre et l'encodage avant le transfert puis efface tout enregistrement des opérations réalisées. Chaque partie des métadonnées relative à qui parle à qui est donc détruite avant qu'aucune des différentes parties ne puisse être assemblée pour un traçage.
- Décentralisation xx exhaustive: chaque message envoyé sur xx messenger passe par cinq nœuds choisis aléatoirement parmi des centaines de nœuds xx dans le monde. Il n'existe aucune entité centralisée susceptible d'être contrainte par des gouvernements, aucune entreprise pour insérer un logiciel espion ou dévoiler des données de sa base de données. Le xx network soutenant le xx messenger est une blockchain distribuée et décentralisée, dorénavant sur un mainnet, et fonctionne sur un logiciel transparent exécuté par plus de 350 nœuds indépendants répartis dans plus de 80 pays. L'application xx est une application véritablement décentralisée (dApp), ce qui signifie qu'elle opère de manière autonome sur une blockchain décentralisée via des contrats intelligents.

L'équipe pionnière derrière la création du xx messenger a développé très tôt des systèmes cryptographiques pratiques, anonymes et vérifiables, et est dirigée par un cryptographe de renom, David Chaum, qui propose et déploie des devises numériques, des réseaux de mélange, des solutions cryptographiques sans permission, et des systèmes de vote vérifiables depuis les années 1980.

« Les récentes préoccupations en matière de confidentialité ont sensibilisé le public aux problèmes liés au contrôle d'informations personnelles par des entités centralisées comme Facebook. En prenant conscience que leurs informations sont détournées par des entités commerciales, les personnes essaient désormais de comprendre comment utiliser la cryptographie et les smartphones pour se protéger et changer la société de façon positive; xx messenger sécurise la décentralisation des communications privées tout comme le Bitcoin a décentralisé la finance. Il faut agir: prenons le contrôle de nos informations, et de notre destin. » déclare David Chaum, inventeur de la monnaie électronique et fondateur de xx network.

Le xx messenger est téléchargeable sur les app stores [Android](#) et [Apple](#). Suivez-nous sur [Twitter](#) et rejoignez notre [Telegram](#) et [Discord](#).

À propos de xx network

xx network est un nouveau type de plateforme, offrant une sphère numérique protégée via laquelle ses utilisateurs partagent des idées et échangent des valeurs dans un environnement sécurisé et privé. La blockchain xx network s'appuie sur un algorithme de consensus à sécurisation quantique innovant qui atteint efficacement une complexité d'authentificateur linéaire et une finalité à bloc unique, garantissant ainsi des opérations basées sur un consensus évolutif. Le réseau a été construit par des équipes dirigées par David Chaum, le Parrain de la cryptomonnaie.

Pour de plus amples renseignements, veuillez visiter <https://xx.network/>.

Le texte du communiqué issu d'une traduction ne doit d'aucune manière être considéré comme officiel. La seule version du communiqué qui fasse foi est celle du communiqué dans sa langue d'origine. La traduction devra toujours être confrontée au texte source, qui fera jurisprudence.



Consultez la version source sur [businesswire.com](https://www.businesswire.com) : <https://www.businesswire.com/news/home/20220125005777/fr/>