Blockchain & Identité numérique

Implémentation, protocoles, avantages et défis.

Par: Pascal Ngu Cho, BA-GIS/Consultant Blockchain senior.

Contexte

À l'ère des services web, le défi auquel nous faisons face est celui de **l'identification**. Comment savoir que c'est la bonne personne quand j'offre des produits/services en ligne? Dans le monde physique, nous utilisons des pièces d'identités pour prouver notre identité: réservation d'hôtel, soin médicaux, location de livre etc. Pourquoi n'avons nous pas l'équivalent numérique d'un passeport, d'un permis de conduire ou d'une pièce permettant de se connecter en ligne?

Vulnérabilité

La forme d'authentification la plus utilisée aujourd'hui pour se connecter sur les réseaux sociaux ou sur les sites de commerce électronique est l'utilisation d'un nom d'utilisateur et d'un mot de passe. Avec la perte massive des données personnelles qu'on a connue au cours des dernières années[1], de plus en plus d'organismes réglementaires mettent en place des normes pour protéger les utilisateurs. L'exemple est la norme européenne GDPR qui définie la manière dont les entreprises collectent, gèrent et sécurisent les données des utilisateurs. Sans standards technologiques, il est difficile aux entreprises et organismes de répondre aux exigences réglementaires. La faiblesse des solutions centralisées utilisées aujourd'hui résident dans le fait qu'elles représentent plus souvent un point d'accès unique, ce qui les rend vulnérables aux attaques. Les mots de passe restent encore la principale méthode de protection des comptes.

Blockchain & identité numérique

L'avènement des technologies de la chaîne des blocs [blockchain] rendent l'utilisation des mots de passe obsolètes. Par leurs conceptions, elles fournissent un environnement de protection inhérent. Les bases de données distribuées sont plus sures car elles stockent les

[1] https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

informations dans plusieurs endroits. Dans l'environnement blockchain, il n'y a pas de mots de passe à voler.

On distingue principalement 2 types d'implémentation blockchain de système d'identité numérique: **L'identité souveraine et l'identité d'entreprise**.

L'identité souveraine (SSI)

Les systèmes d'identité souveraine (SSI) sont conçus pour fonctionner sur une blockchain publique (ouvert à tous et sans permission). Dans ces systèmes, l'identité numérique de chaque personne est décentralisée, détenue et contrôlée par la personne. L'identité souveraine place la personne au centre de sa vie numérique et lui offre des outils qui permettent de préserver la confidentialité et d'interagir en toute sécurité. Les protocoles tels que **Sovrin**, **Remme** ou **Identity** proposent des écosystèmes pour leurs développements.

L'identité d'entreprise(s)

Les systèmes d'identité d'entreprise(s) sont conçus pour fonctionner sur une blockchain privée au sein d'une entreprise ou d'un ensemble d'entreprises et organisation (consortium). L'entreprise ou le consortium joue le rôle d'émetteur de certificats, de vérificateur et de contrôle d'identité. Dans le cas d'un consortium, ce sont les membres qui jouent le rôle d'émetteurs et de vérificateurs. Les membres sont préalable validés pour faire partie de la blockchain. Ils servent alors d'autorités de certification et peuvent partager les informations d'identification vérifiées telles que le KYC. L'identité est aussi transférable entre les membres.

Protocoles d'identités numériques

Le marché des protocoles et solutions d'identité numérique est en plein développement. De grands acteurs comme **Microsoft** ou **IBM** proposent des solutions. En 2019, Microsoft dévoilait **ION** (Identity Overlay Network), un protocole d'identité décentralisée fonctionnant sur la blockchain Bitcoin.

Avec la blockchain, les utilisateurs contrôlent leurs identités car les clés privées d'accès restent sur leurs appareils. **REMME** propose par exemple l'utilisation d'une infrastructure de clés publiques distribué (dPKI) pour résoudre les problèmes de gestion des accès. Au lieu d'utiliser les mots de passe pour se connecter à leurs applications préférées, les utilisateurs génèrent des certificats SSL/TLS spécifiques à leurs appareils et les données de certifications sont gérées à travers la blockchain. Pas besoin de centraliser la gestion des certifications car la blockchain agit comme autorité de certification. En plus des certificats SSL/TLS, il est aussi possible d'y ajouter des éléments

de protection contre la réutilisation et la violation des mots de passe, l'enregistrement des clés, le phishing et attaques de type "force brute".

Un autre exemple concerne le protocole d'identification **Paymail**, un protocole libre et ouvert d'envoi/réception de valeur sur la blockchain **BitcoinSV**. L'extensibilité du protocole lui permet d'être utilisé pour les signatures numériques, l'encryptage, les portefeuilles dépositaires et non-dépositaires. Il est compatible avec les services d'identifications de messagerie comme Google SSO. MoneyButton et Handcash ont adopté Paymail.

Toujours sur BitcoinSV, le protocole **BAP** (Bitcoin Attestation Protocol) offre la possibilité d'implémenter un système d'identification qui permet à l'utilisateur de créer et de gérer plusieurs identités sans compromettre sa vie privée.

De son côté **Sovrin** avec un réseau de plus de 40 partenaires a mis en place un nouveau standard ouvert d'identité numérique souveraine conçu pour assurer confiance, contrôle et facilité d'utilisation des différentes identifiants de l'utilisateur en ligne.

Avantages d'une identité numérique décentralisée:

Les avantages d'une identité numérique décentralisée sont nombreux, tant pour l'utilisateur que pour l'entreprise:

- **Convivialité**: Les systèmes d'identifications décentralisés sont plus simples pour les utilisateurs car elles éliminent le besoin d'avoir des multiples mots de passe. La gestion des comptes est aussi plus simplifiée.
- **Efficience**: L'identité numérique décentralisée augmente l'efficience des processus: sécurité des données, acquisition de clients, distribution etc.
- **Confidentialité**: Par leur conception, ils sont plus privés car ils donnent le contrôle total à l'utilisateur sur la gestion de son identité.
- **Réduction des fraudes et sécurité**: La réduction des mots de passe réduit de façon considérablement les possibilités de fraude. Les entreprises sont plus en sécurité car elles ne contrôlent plus les mots de passe susceptibles d'être des cibles d'attaques.
- **Nouvelles opportunités**: L'identité numérique décentralisée ouvre la porte à de nouvelles opportunités, de nouveaux modèles d'affaires pas encore explorés pour les entreprises et pour les utilisateurs.

Cas d'utilisation de l'identité numérique

- **Utilisateur**: Créer un compte ou se connecter sans mot de passe sur un site web ou une application.
- **Entreprise**: Intégrer l'authentification sans mot de passe sur mon site ou mon application.

Les premiers cas d'utilisation de l'identité numérique concernent l'authentification sans mot de passe. Pour une meilleure adoption de l'identité numérique souveraine, les solutions devront pouvoir offrir non seulement l'authentification sans mot de passe, mais aussi l'authentification à deux facteurs (2-FA) et des méthodes de récupération de comptes.

Dans le cas par exemple d'une application blockchain d'envoi d'argent ou de paiement, l'utilisateur devrait pouvoir effectuer certaines opérations sans compromettre son identité, ni la sécurité de ses clés:

- **Vérification**: Prouver son identité sans compromettre sa vie privée
- **Sauvegarde**: Permettre de garder ses jetons numériques
- **Paiement**: Envoyer facilement de l'argent à la famille et aux amies
- **Protection**: Offrir la protection contre le vol de ses jetons numériques.

Défis de l'identité numérique décentralisée

Les utilisateurs et entreprises ne tireront profits de ces avantages que si l'écosystème en place réponds aux nombreux défis en place:

- **Manque de standards**: L'absence de standard rend la mise en place des fonctions d'interopérabilité et de portabilité des données difficiles. La fondation pour l'identité décentralisée (DIF) et la fondation Sovrin avec chacune plus de 30 membres travaillent au développement des standards d'identité numérique.

- **Éducation et formation**: Si les utilisateurs deviennent gardien de leur identité numérique, ils doivent être éduqués et formés sur leurs avantages, sur la gestion de leur identité et sur l'utilisation des outils disponibles.

- **Développement des infrastructures**: chaîne de blocs, portefeuille, garde de valeur, outils de développement (API)

- **Gestion des clés**: L'identité dépend de l'encryption et de la sauvegarde des clés privées. La chaîne de bloc ne stockant que les clés publiques, les utilisateurs ou les entreprises deviennent alors responsables des clés privées. Il y a donc un défi à sécuriser et à gérer à grande échelle les clés.

Conclusion:

Sans standards technologiques, il est difficile aux entreprises et organismes de répondre aux exigences réglementaires en matières de protection et sécurité des données. La faiblesse des solutions d'identification en ligne résident dans la centralisation de données.

Avec l'avènement des technologies blockchain, il devient possible d'offrir des solutions d'identité numérique qui répondent aux exigences de l'ère numérique. Tant pour les utilisateurs que pour les entreprises et organismes, les avantages d'une identité numérique décentralisée sont nombreux, malgré les défis de l'heure.