À propos du protocole KILT

Chaque mois, nous lisons des informations sur les scandales de données. Les grandes plateformes sont attaquées par des pirates informatiques qui volent des millions de mots de passe, causant ainsi des dommages importants. Parfois, ce sont les plateformes elles-mêmes qui vendent ces données et sont responsables des conséquences.

En guise de solution, il est toujours recommandé aux utilisateurs d'employer une multitude de mots de passe différents et aussi complexes que possible. Mais cela ne change rien au fait que les mots de passe sont collectés dans des silos centraux de plateformes Internet principalement américaines. **En raison de leur taille, ces silos constituent une incitation énorme pour les pirates informatiques et, en même temps, conduisent à des structures monopolistiques sur l'Internet:** une fois qu'une plateforme Internet compte des millions d'utilisateurs, la concurrence est à peine possible. Les bonnes idées ne sont pas financées, les investisseurs craignant le pouvoir de marché du monopoliste; l'innovation est ainsi empêchée.

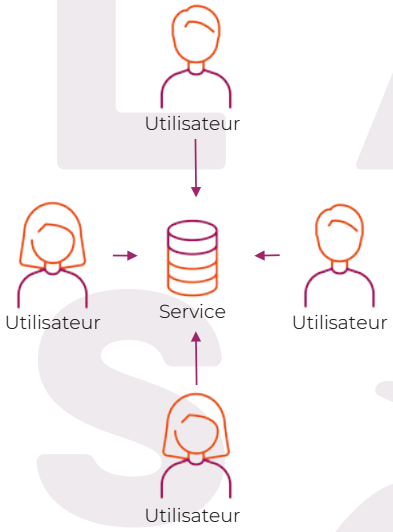

Illustration 1: Beaucoup d'utilisateurs enregistrent leurs noms d'utilisateur et mots de passe dans un service central.

L'entreprise berlinoise BOTLabs s'attaque à ce problème en fournissant des mécanismes à l'Internet qui rendent inutiles les noms d'utilisateurs et les mots de passe et rendent ainsi leur stockage obsolète. L'idée de base est aussi simple que captivante: dans le monde analogique, nous n'avons pas de noms d'utilisateur et de mots de passe, mais des documents avec lesquels nous nous identifions. **Le protocole KILT développé par BOTLabs permet désormais d'émettre et de présenter des documents sur l'Internet.**

Le procédé fonctionne comme suit: un émetteur (en anglais: « Attester ») délivre sur demande un document aux utilisateurs (« Claimer ») concernant une propriété particulière, signé de façon électronique par cet émetteur. **Le document n'est pas stocké de manière centralisée chez l'émetteur, mais directement chez l'utilisateur**, comme si l'on

avait mis sa carte d'identité dans son portefeuille.

Le protocole KILT stocke une somme de contrôle du document signé sur la blockchain KILT. La technologie blockchain permet à l'utilisateur de prouver l'authenticité de son document à tout moment, tout en garantissant que **les informations personnelles ne sont jamais rendues publiques.**

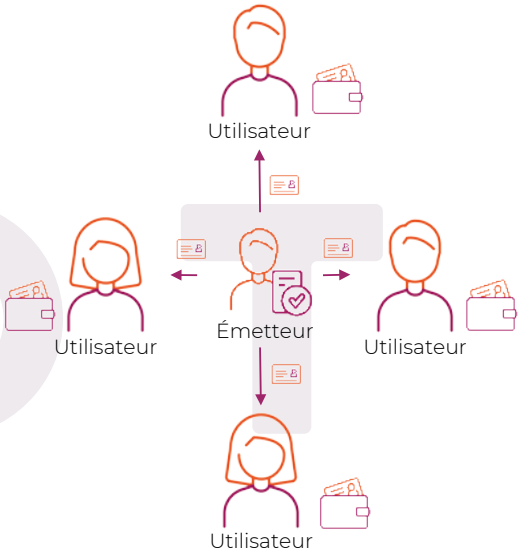

Illustration 2: Chaque utilisateur reçoit un document individuel, signé de façon électronique, et le place dans son portefeuille digital.

Si l'utilisateur souhaite maintenant s'identifier à une propriété spécifique, il envoie son document signé au lieu d'un identifiant ou d'un mot de passe. Si le destinataire (« Verifier ») est également l'émetteur du document, il peut vérifier sa propre signature et laisser l'utilisateur entrer. Si le destinataire est un autre service, mais il fait confiance à l'émetteur, il peut vérifier la validité du document sur la blockchain.

Comme pour les documents du monde analogique, l'utilisateur peut rassembler différents documents dans son portefeuille numérique et les utiliser au besoin. Par exemple, plusieurs services différents pourraient accepter un do-

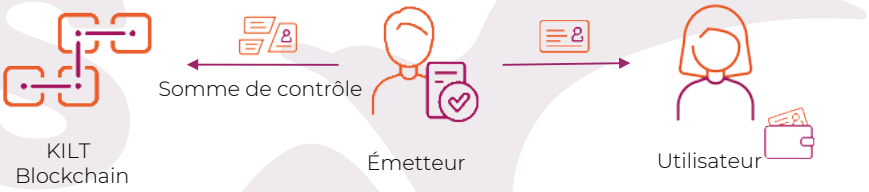

Illustration 3: Une empreinte numérique du document signé est stockée sur la blockchain KILT.

cument émanant d'une institution particulièrement fiable, comme c'est le cas dans le monde analogique des cartes d'identité. L'utilisateur conserve toujours un contrôle total sur ses données: il décide à qui il rend quel document accessible et même quelle partie de l'information doit être visible sur le document. Il a la souveraineté complète sur ses données.

Le protocole KILT dissocie le processus de vérification du document de l'émetteur: la personne à qui le document est présenté décide seulement à l'aide de la blockchain si elle accepte le document. L'émetteur n'est plus impliqué. Cela correspond au processus dans le monde analogique, dans lequel, par exemple, l'émetteur d'une carte d'identité ne reçoit aucune information indiquant que l'uti-

Illustration 4: L'utilisateur s'identifie avec son document à un service.

lisateur a présenté l'identification à une banque. Ce découplage, caractéristique importante du protocole KILT, **protège la vie privée des utilisateurs** tout en créant **une énorme scalabilité du système**, puisqu'un nombre arbitraire de contrôles simultanés peuvent avoir lieu sans que l'émetteur soit obligé d'être actif à chaque fois.

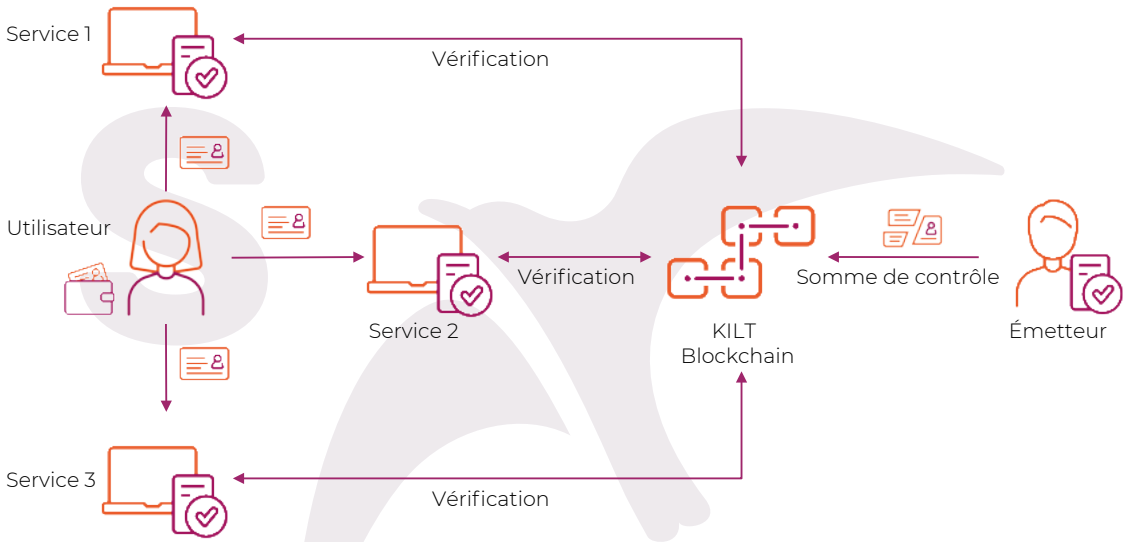

Illustration 5: Un utilisateur emploie son document à différents services. Ceux-ci vérifient la validité du document sur la blockchain.

À propos de BOTLabs

La BOTLabs GmbH a été fondée en janvier 2018 par Ingo Rübe, informaticien et ancien directeur technique de la maison d'édition Burda, en collaboration avec Hubert Burda Media. En octobre 2018, la maison d'édition Ringier a également participé à BOTLabs.

L'objectif de BOTLabs est de rendre la technologie de blockchain accessible et utilisable pour le grand public. BOTLabs développe des technologies de base pouvant être utilisées par les entreprises et les administrations publiques pour développer de nouveaux modèles économiques et améliorer les processus existants.

Le 14 mai 2019 à Berlin, BOTLabs va présenter le protocole KILT, qui permet de résoudre l'un des problèmes les plus importants et les plus urgents de l'Internet d'aujourd'hui: la perte de confiance.

À propos de Ingo Rübe

Ingo Rübe est le fondateur et gérant de BOTLabs GmbH.

De 2012 à 2017, Rübe a été le directeur technique de la maison d'édition Hubert Burda Media. Il y a initié et a été responsable du système de gestion de contenu open source « Thunder ». L'informaticien berlinois avait auparavant travaillé pendant six ans en tant que directeur de projet chez Axel Springer SE.

Déjà en 1995 il avait fondé avec « Network Department » sa première entreprise dans le domaine de l'informatique médicale qui, en 2000, a fusionné avec le département informatique de Fresenius AG pour former l'actuelle Fresenius Netcare GmbH.

Ingo Rübe est membre fondateur de l'organisation internationale de blockchain INATBA (www.inatba.org) ainsi que membre du conseil d'administration de l'association Drupal (www.drupal.org).