ID-Blockchain

Kévin Atighehchi, Loubna Ghammam, et Morgan Barbier
Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France

Résumé

Le projet ID-Blockchain [1] a pour objectif de tirer profit des possibilités offertes par les technologies blockchain dans le cadre de la gestion de l'identité numérique, avec une attention particulière sur la protection des données personnelles. Le service proposé vise à rendre possible l'inscription d'un utilisateur auprès d'un fournisseur de services sans la présence en ligne du fournisseur d'identité. L'utilisateur peut obtenir plusieurs identités et les gère de façon autonome. Lors d'une authentification auprès du fournisseur de service, ce dernier peut ne dévoiler qu'une partie de ses attributs. Le projet met également en avant des notions de e-réputation et d'authentification forte à deux facteurs.

1 Introduction

ID-Blockchain est un projet impliquant les partenaires ATOS Worldline, Ledger, Paymium, le GREYC et le LIRIS. Il fournit un service fiable et décentralisé pour améliorer la gestion par les fournisseurs d'identité et par les fournisseurs de services des données collectées auprès des utilisateurs. Le service proposé se veut respectueux du règlement général sur la protection des données (GDPR – mai 2018). Le service ID-Blockchain fait intervenir plusieurs entités :

- L'utilisateur aura une extension d'un wallet Bitcoin, un wallet ID-Blockchain. Ce dernier lui permet d'interagir avec des fournisseurs d'identités, des fournisseurs de services et la Blockchain Bitcoin.
- Le fournisseur d'identité (IDP), tel qu'une banque ou une université, qui s'appuie sur un composant logiciel du service ID-Blockchain afin de certifier les données déclarées par l'utilisateur.
- Une blockchain publique (ex. la Blockchain Bitcoin ou Ethereum), ou tout autre technologie de registre distribué.
- Le fournisseur de services (SP), qui s'appuie sur un composant logiciel du service ID-Blockchain pour inscrire un utilisateur avec des attributs déclarés valides par le service, et assurer son authentification forte avec le standard FIDO U2F.

Le service s'appuie sur le modèle de l'identité auto-souveraine où l'utilisateur conserve et protège ses données identitaires, comme il le ferait dans son quotidien non numérique. L'utilisateur devient son propre fournisseur d'identité en contrôlant son identité sans dépendre d'une seule autorité. Le service proposé donne le pouvoir aux utilisateurs afin qu'ils puissent collectivement jouer le rôle d'un IDP. En 2016, Allen [1] a énoncé dix principes qui pourraient caractériser une identité auto-souveraine : l'existence, le contrôle, l'accès, la transparence, la persistence, l'intéropérabilité, le consentement, la minimalisation et la protection. Le projet prévoit également une utilisation de tokens physiques pour le stockage sécurisé et l'utilisation de données critiques d'un utilisateur : la clé privée de son wallet ID-Blockchain, ses données identitaires et ses réputations.

2 Scénario d'utilisation

L'utilisateur commence par s'enregistrer sur une application compatible avec ID-Blockchain, alors une association avec un token sécurisé est faite. L'utilisateur enregistre son identité numérique et interagit avec un IDP pour lier sa nouvelle identité à des déclarations d'identité, qui sont validées par l'IDP et mises dans la blockchain. L'utilisateur légitime peut ainsi contacter le SP grâce à une authentification forte en lui fournissant une déclaration d'identité que l'utilisateur souhaite utiliser. Le SP peut vérifier et valider les éléments de preuve de cette déclaration, qui sont disponibles

1. Ce projet a été en partie financé par l'état français grâce au Projet d'Ivestissement d'Avenir lancé en 2016.

publiquement sur la blockchain. Pour une solution détaillée d'un protocole semblable, se réferer à [2].

3 Exigences de privacy

Brandão *et al.* ont identifié dans [3] les principaux problèmes du système d'identité à grande échelle basé sur le hub et ils ont proposé des solutions afin d'assurer la confidentialité d'un système d'identité Blockchain. Sans rentrer dans les détails, le protocole qu'on utilise doit résister face aux attaques par collusion malveillante d'acteurs (SPs ou IDPs) et aussi face aux acteurs honnêtes mais curieux. Pour le deuxième cas, ces acteurs agissent honnêtement lors des transactions mais ils dérivent des informations des communications observées. Pour résister à ces attaques, il faut par exemple éviter de stocker en public les informations personnelles, aussi divuguler de manière sélective les données en ne donnant que le minimum nécessaire.

4 Divulgation sélective d'attributs vérifiables

On s'intéresse ici à la création et à l'utlisation d'une preuve pour l'ensemble des attributs d'un utilisateur. Cette preuve, qui est ancrée sur la blockchain via le champ OP_RETURN d'une transaction, doit permettre à un utilisateur de dériver des preuves pour certains de ses attributs. À partir d'une seule attestation d'un IDP, un utilisateur peut ne transmettre que les données utiles lors d'une inscription à un SP, répondant ainsi au principe de minimisation des données. Supposons, en guise d'exemple, qu'un utilisateur possède une attestation concernant un ensemble de quatre attributs : nom, prénom, date de naissance et lieu de naissance. Lorsqu'il s'inscrit sur un site, il a la possibilité d'en dériver une preuve cryptographique concernant ses trois premiers attributs, sans dévoiler le quatrième. Mieux encore, au lieu de fournir le troisième attribut avec exactitude, il peut fournir une preuve d'intervalle de sa valeur numérique. Les outils cryptographiques permettant de concrétiser ce type de mécanisme sont les signatures expurgeables/rectifiables [4, 5], les preuves d'appartenance à un ensemble [6, 7, 8] souvent basés sur des accumulateurs à sens unique [7, 8] ou des arbres de Merkle [9], et enfin les preuves d'intervalle [6].

À terme, un service adoptant le modèle de l'identité auto-souveraine doit permettre à un utilisateur de se composer une identité vérifiable à partir de plusieurs attestations.

Références

[1] C. Allen. The Path to Self-Sovereign Identity, April 2016.

[2] D. Augot, H. Chabanne, T. Chenevier, W. Georges, and L. Lambert. A User-Centric System for Verified Identities on the Bitcoin Blockchain. In *ESORICS, DPM and CBT*, pages 390–407, 2017.

[3] L. Brandão, N. Christin, and G. Danezis. Toward Mending Two Nation-Scale Brokered Identification Systems. *PoPETs*, pages 135–155, 2015.

[4] R. Johnson, D. Molnar, D. Song, and D. Wagner. Homomorphic signature schemes. In *Topics in Cryptology — CT-RSA 2002*, pages 244–262, 2002.

[5] K. Samelin, H. Pöhls, A. Bilzhause, J. Posegga, and H. de Meer. Redactable signatures for independent removal of structure and content. In *Information Security Practice and Experience*, pages 17–33, 2012.

[6] J. Camenisch, R. Chaabouni, and A. Shelat. Efficient protocols for set membership and range proofs. In Josef Pieprzyk, editor, *Advances in Cryptology - ASIACRYPT 2008*, pages 234–252, 2008.

[7] J. Benaloh and M. De Mare. One-Way Accumulators : A Decentralized Alternative to Digital Sinatures. In *Advances in Cryptology - EUROCRYPT*, pages 274–285, 1993.

[8] C. Papamanthou, R. Tamassia, and N. Triandopoulos. Authenticated hash tables. In *ACM Conference on Computer and Communications Security*, pages 437–448, 2008.

[9] R. Merkle. A Digital Signature Based on a Conventional Encryption Function. In *Advances in Cryptology - CRYPTO 93*, pages 369–378, 1987.