Technologie des registres distribués

Cybersécurité: Défis pour la Suisse politique

Etat des lieux

La blockchain est une forme spéciale de technologie des registres distribués TRD. La TRD peut être considérée comme une base de données (registre) distribuée, tenue et mise à jour indépendamment par chaque nœud participant à un réseau. Aucune autorité centrale ne gère la base de données et ne transmet les enregistrements aux nœuds. Au lieu de cela, les enregistrements sont créés indépendamment et conservés par chaque nœud. Chaque nœud traite donc chaque transaction et arrive à sa propre conclusion. Un protocole de consensus garantit que chaque nœud conserve une copie identique de la base de données.

Il existe plusieurs façons d'implémenter la TRD, la plus connue étant la blockchain. La blockchain est très fréquemment associée à des cryptomonnaies comme le Bitcoin. Il convient de noter que les termes ne doivent pas être utilisés de manière interchangeable. La blockchain est la technologie sur laquelle sont basées la plupart des cryptomonnaies.

La Suisse compte un nombre particulièrement élevé de start-up actives dans la blockchain. Un rapport récemment publié recense plus de 800 entreprises composées de plus de 4000 spécialistes travaillant dans le domaine de la technologie blockchain et de la cryptologie monétaire, et qui sont principalement situées dans la «Crypto Valley» suisse à Zoug.

Défis

Avec la blockchain, il n'est plus nécessaire de faire confiance à une autorité centrale telle que les banques, les compagnies d'assurance ou les notaires. Au niveau sécuritaire, l'absence d'une autorité centrale présente des avantages et des inconvénients. Il n'y a pas de point de défaillance unique, mais il n'y a pas non plus de point de contrôle capable de détecter et de réagir à des problèmes imprévus. Au lieu de cela, il faut se fier à la technologie blockchain elle-même et à la tolérance aux erreurs intégrée.

Les problèmes de sécurité liés à la blockchain et signalés jusqu'à présent ne se rapportent généralement pas à la plate-forme blockchain elle-même, mais aux applications qui y sont actives. En ce sens, les applications blockchain ne sont pas différentes des applications traditionnelles; ces deux catégories sont confrontées à des problèmes de sécurité similaires.

Du point de vue de l'utilisateur final, les mauvaises pratiques de gestion de clés sont une préoccupation majeure. La perte ou le vol de clés est un problème largement répandu et les répercussions financières sont immédiates dans le cas des cryptomonnaies.

Recommandations

De manière générale, la blockchain et la TRD ouvrent de nouvelles perspectives pour un large éventail d'applications commerciales. Les solutions basées sur la blockchain actuellement en cours de développement et promues par des start-up continueront à évoluer. Il est recommandé aux organisations qui prévoient de déployer des solutions basées sur la blockchain de procéder à une évaluation des risques appropriée, en se concentrant sur l'application fonctionnant sur la plate-forme sous-jacente de la chaîne de blocs.

Nécessité d'agir

La technologie blockchain et ses applications continueront à évoluer. Une amélioration des performances permettant d'augmenter la vitesse de traitement des transactions et de nouvelles caractéristiques de sécurité et de confidentialité sont notamment attendues.

Sur le plan juridique, l'utilisation de la blockchain dans le secteur financier a soulevé plusieurs questions. C'est pourquoi le Conseil fédéral a adopté en novembre 2019 le message relatif à la poursuite de l'amélioration du cadre légal régissant la blockchain et la TRD. Des amendements à neuf lois fédérales sont proposés, qui touchent à la fois le droit civil et le droit des marchés financiers. Ils visent à accroître la sécurité juridique, à supprimer les obstacles aux applications de la TRD et à réduire le risque d'abus.

Références

- VC: The Crypto Valley's Top 50 H1 2019, July 2019. https://cvvc.com/application/files/2115/6453/7847/CVVC-Top50-H1-2019.pdf
- Swiss Federal Council: Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register, Nov. 2019. https://www.newsd.admin.ch/newsd/message/attachments/59301.pdf

Contact

Nicole Wettstein
Responsable du programme prioritaire Cybersécurité
+41 44 226 50 13

https://www.satw.ch/cybersecurity-defis

Impressum
Académie suisse des sciences techniques SATW
Contributions d'experts
Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Verwaltungsrat und Berater | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab
Rédaction et graphisme
Beatrice Huber; Claude Naville, Adrian Sulzer, Nicole Wettstein

www.satw.ch
Septembre 2020