Un regard technique sur la blockchain Libra

L'objectif de cette étude est de dresser une analyse technique synthétique de la technologie sous-jacente à la cryptomonnaie LIBRA et plus précisément de lister les principaux risques relatifs au choix d'architecture et des technologies adoptées par le projet.

L'analyse des risques ci-dessous est conduit suivant les principaux critères d'évaluation d'une technologie Blockchain à savoir :

- **La gouvernance** : modalité de gestion des conditions d'accès, d'utilisation et d'évolution du LIBRA par ses utilisateurs et membres
- **La performance** : capacité en nombre de transaction par seconde
- **La confidentialité** : capacité à garantir la confidentialité des données des transactions à caractère personnel ou sensible
- **La gestion de l'identité** : gestion de l'anonymat des utilisateurs
- **La sécurité** : mécanismes de protection contre les attaques informatiques
- **La maturité** : stabilité et fiabilité du système au cours du temps. Retour d'expérience sur les technologies employés.

Critère	Risque	Explications techniques	Probabilité	Sévérité	Synthèse
Gouvernance	Prise de contrôle par un groupement d'intérêts économique.	Une coalition de nœuds regroupant plus de 33% des droits de vote peut prendre le contrôle du système.	Très faible	Importante	Scénario peu probable compte tenu des conséquences dramatiques sur l'image du Libra.
Performance	Limitations en termes de transactions par secondes (environ 1000tx/s).	Un protocole de paiements hors blockchain de type Lightning comme utilisé sur Bitcoin sera proposé dans le futur afin de lever cette limitation.	Moyenne	Moyenne	Pas de réelles limitations en termes de performances.
Confidentialité	Exploitation libre des données transactionnelles.	Le ledger contenant l'historique complet des transactions (date, origine, destination, montant) est accessible aux membres.	Très haute	Moyenne	Aucun mécanisme permettant de limiter la confidentialité des données vis-à-vis des membres de l'association n'est disponible à ce jour.
Identité	Contrôle de l'identité par l'association Libra.	Le mode de gestion de l'identité n'est pas suffisamment documenté à ce jour.	Moyenne	Importante	En l'état des connaissances sur les mécanismes et acteurs de gestion et contrôle de l'identité, il est difficile d'estimer le respect des règles d'anti-blanchiment d'argent.
Sécurité	Attaque externe de type DDoS, 51% ou vol de clefs privées etc.	Réseau fermé, accès filtrés, base de données sécurisée pour la gestion des clefs.	Faible	Importante	Faible risque identifié compte tenu du caractère permissionné de la blockchain et du savoir faire des membres de l'association Libra (spécialistes du paiement en ligne, experts en, sécurité etc.).
Maturité	Dysfonctionnement et maintien en conditions opérationnelles.	Libra propose ses propres choix technologiques tels que : le langage de programmation Move, le LibraBFT etc.	Haute	Importante	Le développement de Libra ne pourra se faire sans rencontrer d'obstacles techniques tant certaines solutions annoncées semblent complexes et innovantes (ex : gestion décentralisée de l'identité)

Les résultats de l'étude

D'un point du vue technique, le projet Libra concentre les choix d'architecture les plus pertinent lui permettant de répondre aux principaux enjeux d'une cryptomonnaie d'un point de vue de la

performance et de sécurité associé à des mécanismes de gouvernance solides favorisant une large adoption par l'ensemble des utilisateurs.

On peut cependant relever une conception qui à ce jour ne permet pas de garantir la confidentialité des transactions manipulants des données à caractère personnel ou sensible.

Enfin, la relative maturité de certaines technologies adoptée a de fort risques d'induire son lot de défaillances techniques aux conséquences plus ou moins graves lors de sa phase de déploiement.

En conclusion

L'objectif était de donner un point de vue technologique sur les aspects clés du projet, tels que la gestion et la confidentialité des données, et la gouvernance. Ce faisant, cela nous permettra d'avoir un premier aperçu de la solution blockchain du Libra, qui, à son tour, peut nous éclairer sur les questions actuellement mises en avant par les régulateurs.

Pour ce qui est de la résistance réglementaire, elle s'est avérée impressionnante et efficace. Mais rien de tout cela ne signifie que des stablecoins ou des projets similaires ne pourront jamais décoller. Tout porte à croire que les gouvernements devront les adopter – ou leur faire concurrence. La semaine dernière, Rob Kaplan, président de la Banque fédérale de réserve de Dallas, a déclaré que tôt ou tard, « quelqu'un va trouver comment faire fonctionner tout ça ».

Les choses restent chaotiques pour la première phase du Libra, mais il est indéniable qu'il a été un moteur, stimulant le débat international sur le sujet et suscitant l'intérêt des entreprises pour la monnaie numérique.

Retrouvez l'ensemble de l'étude ici