« Smart contract » : une sécurité des développements à revoir ?

La sécurité serait le point faible de développeurs à l'origine des lignes de code de contrats intelligents (ou « smart contracts ») de la blockchain, la chaîne de blocs, technologie décentralisée de gestion des transactions.

C'est ce qui ressort d'un document publié par des chercheurs en sciences et technologies de l'information de l'université de l'Illinois (UIUC), document dont The Register s'est fait l'écho.

Selon les universitaires, 680 millions de dollars contrôlés par des contrats intelligents auraient été détournés ou volés en raison de vulnérabilités de sécurité en 2021. Comment, dans ce contexte, des développeurs de contrats intelligents abordent l'enjeu de sécurité ?

Une étude qualitative exploratoire a été menée.

Revue de code source

Les répondants ont été interrogés sur leurs priorités à propos du développement de contrats intelligents. La sécurité n'est pas la priorité pour 83% d'entre eux.

Les attentes concernant la rapidité des déploiements applicatifs l'emportent. Par ailleurs, les projets peuvent être une émanation (« fork ») d'un projet déjà validé par la communauté (par exemple Uniswap, protocole d'échange décentralisé orienté finance).

De surcroît, un audit de sécurité interne ou externe peut avoir été mené. Après tout, un programmeur n'est pas responsable de la sécurité des systèmes d'information.

Chacun(e) son métier ?

Une poignée de développeurs de contrats intelligents ont été appelés à identifier des vulnérabilités dans le code de « smart contracts« .

Sans grande surprise, les développeurs qui débutent dans ce domaine ont obtenu un taux de réussite bien plus faible (15%) que celui des plus expérimentés (55%) concernant l'identification des vulnérabilités de sécurité lors de la révision de code initiale.

Les documents techniques et les logiciels dédiés ne suffisent pas à faire du DevSecOps (développement applicatif, sécurité et opérations combinés) une réalité, semble-t-il.

(crédit photo © Shutterstock)