Dans quelle mesure la sécurité et la régulation des blockchains peuvent-elles générer des coûts financiers ?

VICTOR WARHEM,
Économiste
chez BSI Economics

Depuis quelques années, avec l'explosion du secteur des cryptoactifs, les blockchains se sont imposées comme des solutions populaires pour échanger et stocker des données en ligne. Les blockchains se développent de plus en plus dans le domaine de la finance, mais également dans bien d'autres, comme celui des chaines d'approvisionnement, des services notariaux, de la comptabilité, etc. Le secteur de la blockchain pourrait représenter à ce titre plus de 1 000 milliards USD d'ici 2030, contre moins de 20 aujourd'hui.

Néanmoins, même si elles présentent par nature un degré de sécurité cryptographique élevé, elles peuvent être sujettes à des cyberattaques, engendrant ainsi des coûts de cybersécurité supplémentaires et incitant les régulateurs à définir un cadre réglementaire stricte. Qu'en est-il plus précisément dans leur secteur « historique », le secteur financier ?

Des blockchains publiques bien plus perméables aux cyberattaques que les blockchains privées

La blockchain est un registre numérique distribué et décentralisé auquel il est possible d'accéder selon certaines modalités, qu'il est possible d'utiliser pour émettre ou stocker des informations, des actifs numériques, pour valider des transactions, et qui fonctionne grâce à des protocoles algorithmiques déterminant comment une transaction est validée – ce qu'on appelle communément le mécanisme de consensus.

Il convient de distinguer trois types de blockchains : de manière schématique, les blockchains publiques présentent les registres les plus distribués et décentralisés en matière d'émission, d'accès, d'utilisation, et de participation au mécanisme de consensus, tandis que les blockchains privées se caractérisent par un contrôle d'une autorité ad-hoc des acteurs pouvant émettre les actifs, accéder aux registres, utiliser la blockchain, et/ou participer à la validation des transactions. Enfin les blockchains hybrides, où l'autorité ad-hoc donne accès à tout le monde tout en gardant la main sur le mécanisme de consensus, constitue une catégorie à part tout en présentant des caractéristiques pour la plupart comparables aux blockchains privées.

Les blockchains privées – dont les plus grandes sont produites par Hyperledger Fabric, Quorum ou R3-Corda – sont utilisées pour tout type d'application blockchain, y compris dans le domaine financier. Peu d'informations publiques relatives à leurs coûts de cybersécurité ou de régulation sont disponibles – probablement, justement, en raison

de leur caractère privé. Elles peuvent néanmoins en théorie faire face à des attaques de déni de service, ou à des attaques « des 51 % » - où les pirates prennent le contrôle de plus de 50 % des nœuds utilisés pour la validation des transactions et corrompent le mécanisme de consensus pour extraire des fonds de la blockchain. Néanmoins, les organisations à l'origine des grandes blockchains privées (Linux Foundation pour Hyperledger Fabric, ou JP Morgan puis ConsenSys pour Quorum) sont réputées présenter des niveaux de cybersécurité adéquats tout en étant conformes aux régulations si elles existent. Leurs blockchains sont d'ailleurs généralement sollicitées pour améliorer le niveau de cybersécurité des organisations qui y souscrivent. Les montants qui ont été volés ou perdus sur ces blockchains ont ainsi très nettement inférieures à ceux qui l'ont été sur les blockchains publiques.

En effet, la question de la cybersécurité se pose bien davantage pour les blockchains publiques. Si elles portent en elles une promesse de sécurité – en réalité plutôt de résilience – et de transparence, elles connaissent de nombreux types de défaillance depuis leurs débuts. Tout d'abord, les plus petites, malgré leur décentralisation, peuvent au même titre que les blockchains privées être corrompues par une attaque « des 51 % » (comme l'a subi le Ronin Network en mars 2022 avec une perte de 624 millions USD). Au-delà des attaques touchant au mécanisme de consensus, elles sont surtout vulnérables dans leur « périphérie », à commencer par les « contrats intelligents » – algorithmes de service financier impliquant des cryptoactifs – dont le code n'a pas été suffisamment testé et présentent des failles comme dans le cas du piratage de la blockchain Poly Network en 2021 ayant conduit à une perte de 611 millions USD. Les portefeuilles de dépôts des fonds présentent aussi souvent des failles de sécurité et l'hameçonnage est monnaie courante pour s'emparer des identifiants des portefeuilles d'utilisateur. Par ailleurs, d'autres types de cyberattaques sont possibles : malwares, ransomware, exploitation des « ponts » entre blockchains, etc. Il a ainsi été démontré que, parmi les projets sur blockchains publiques présentant un montant total sous gestion supérieur à 10 millions €, 6,2 % avaient été piratés ces dernières années, selon KPGM. En 2022, les montants volés ou perdus excédaient ainsi les 3 milliards USD, bien que ces vols et pertes aient dans certains cas été le travail de créateurs de blockchain malveillants, et pas de failles de cybersécurité.

Les fournisseurs de service financier : au cœur des enjeux de cybersécurité

Sur qui reposent les coûts de cybersécurité « possibles » dans l'univers des blockchains publiques ? Sur plusieurs types d'acteurs : les fournisseurs de service financier (FSF[1]), les émetteurs de cryptoactifs s'il y en a, les utilisateurs qui stockent leurs fonds, et enfin les « validateurs » (*miners* en anglais) des mécanismes de consensus qui permettent à la blockchain de fonctionner et qui participent aussi généralement à sa gouvernance. Hormis les FSF, ces acteurs sont souvent difficilement identifiables et leurs coûts de cybersécurité sont mal connus.

Les FSF représentent au contraire des acteurs financiers plus « classiques ». Leurs coûts de cybersécurité se concentrent potentiellement sur la sécurisation de leur interface sur Internet, des liquidités dont ils disposent et des services qu'ils vendent. Le mécanisme de consensus des plus grandes blockchains publiques de l'écosystème ne leur sont pas accessibles, mais les plus utilisées, Bitcoin et Ethereum, n'ont jamais été piratées grâce à leur niveau très élevé de décentralisation. Compte tenu des liquidités importantes qu'on y trouve, les fournisseurs les plus susceptibles de connaitre des cyberattaques sont les *exchanges*, plateformes d'échange de cryptoactifs, qu'elles soient centralisées (comme Binance) ou décentralisées. Par exemple, l'*exchange* Coincheck a subi un vol d'environ 500 millions USD de liquidités en 2018.

Comment les fournisseurs de services peuvent-ils concrètement améliorer leur cybersécurité ? En auditant régulièrement par le biais de cabinets externes leurs différents services et/ou en engageant un responsable ou une équipe en charge

1/ Ces fournisseurs n'incluent pas les protocoles – notamment ceux de la finance décentralisée – non gérés par une entité unique. Pour ces contrats intelligents de la finance décentralisée, il est très difficile d'améliorer la cybersécurité même si nombre d'entre eux présentent des failles exploitables. Si une faille est découverte, il faut compter sur un développeur spécialisé pour créer une nouvelle version depuis le protocole de base.

de la cybersécurité. Pour l'heure, il manque cruellement de ressources humaines dans ce domaine, avec un nombre d'expert en cybersécurité de contrats intelligents compris entre 1 000 à 1 500 à l'échelle mondiale, selon KPMG.

Renforcement de la cybersécurité, cap sur 2025 avec la réglementation MiCA

Le règlement MiCA, dont le vote a été repoussé au Parlement européen en avril 2023, et dont l'application est attendue à horizon 2024-2025, devrait néanmoins constituer une manière efficace de stimuler ce secteur en obligeant les FSF utilisant les blockchains publiques dans l'Union européenne (UE) à élever leur niveau de cybersécurité. En France, ils sont une soixantaine disposant d'un enregistrement PSAN – pour Prestataire de Services sur Actifs Numériques –, qui les oblige déjà à mettre en place un dispositif de lutte contre le blanchiment et de financement du terrorisme et donc à identifier les utilisateurs.

En effet, les Fournisseurs de Service de Cryptoactifs (Crypto-Asset Service Providers, CASP) – statut qui va remplacer tous les autres pour les fournisseurs de services dans l'Union – seront bientôt tenus à des exigences en matière de gestion des risques et de sécurisation des fonds, notamment en souscrivant à une assurance, ce qui semble pour l'heure difficile à obtenir dans ce secteur et pourrait finalement s'avérer très coûteux. Ils n'auront par ailleurs d'autres choix que d'allouer des ressources pour sécuriser portefeuilles, interfaces, contrats intelligents, et éventuellement mécanismes de consensus de validation si possible. S'agissant des autres coûts réglementaires des CASP, ils seront liés notamment aux obligations de respecter les exigences prudentielles en matière de fonds propres (allant de 50 000 à 150 000 euros minimum en fonction du type de structure), de réserves (au moins 25 % de leurs frais généraux de l'année précédente), et de liquidité (déterminées dans les textes à venir de l'Autorité européenne des Marchés Financiers).

Les coûts liés à la mise en place du règlement européen MiCA ont été estimés par l'étude d'impact du règlement. Ainsi pour ce qui est des fournisseurs de services devant se mettre au diapason de la régulation européenne d'ici 2024-2025, il faut compter entre 35 000 et 75 000 euros pour la confection obligatoire du « livre blanc » définissant le projet – si cela n'est pas déjà fait. À cela s'ajoute entre 2,8 et 16,5 millions € pour la mise au niveau réglementaire, qu'il s'agisse de la mise au niveau en termes de cybersécurité ou en termes de gouvernance, etc. Il faudrait compter en plus de ces coûts uniques des coûts annuels compris entre 2,2 et 24 millions € pour satisfaire les exigences réglementaires européennes. Pour ce qui est du cas spécifique des *stablecoins*, les exigences réglementaires sont encore plus drastiques compte tenu d'une part de l'interdiction de toucher des intérêts pour les utilisateurs des *stablecoins* mais aussi de l'obligation de maintenir un niveau de réserve prudentiel extrêmement élevé pour pouvoir endurer de grandes fluctuations dans le niveau de la demande.

Coûts de cybersécurité en Europe : forte hausse mais effets incertains

Ainsi, les coûts obligatoires de cybersécurité et de régulation pour les FSF sur blockchain publique vont drastiquement s'élever ces prochaines années dans l'Union européenne. Le pari est fait que cette mise au pas réglementaire pourrait aider les acteurs des blockchains publiques à minimiser les vols et pertes liés à leurs services, générant ainsi une confiance et une demande accrue en Europe.

Néanmoins, puisque ces utilisateurs auront toujours accès aux services fournis par des acteurs extra-européens via Internet – à leurs risques et périls –, le règlement européen pourrait au contraire entraver le développement du secteur en Europe. Les prochains mois seront décisifs pour mieux comprendre la tendance qui l'emportera. Un premier test sera la mise en place d'ici l'automne 2023 d'un enregistrement PSAN renforcé en France.

À long-terme, la menace des ordinateurs quantiques et l'arrivée du règlement « MiCA 2 », destiné en théorie à réguler les autres acteurs des blockchains publiques, devraient constituer une nouvelle source de coûts pour le secteur, qui aura peut-être d'ici là connu un essor suffisant pour que « le jeu en vaille la chandelle ». ■

Article rédigé en janvier 2023