Blockchain and cyber security

Rapport thématique préparé par le European Union Blockchain Observatory & Forum

Catégorie de tensions	Extraits du rapport		Tension identifiée	Analyse contextuelle	Note d'interprétation				
	Extraits	*Page et paragraphe*			*Lien avec la ventriloquie*	*Lien avec l'imaginaire sociotechnique*	*Acteurs impliqués*	*Recommandations*	*Comparaison internationale*
Tension sur les vulnérabilités des contrats intelligents	Smart contracts can make blockchains very powerful, but they also open a Pandora's box of security vulnerabilities – the more sophisticated a smart contract programming language is, the more possibilities there are for bugs. At our Cyber Security workshop a smart contract auditor reported that, of the 22 contracts he had audited in the previous year, none was error free, an indication of how difficult it is to get smart contract code right the first time. These errors can have serious consequences. Famous incidents involving smart contracts include The DAO hack, in which USD 70 million was stolen, and the Parity Multisig bug which resulted in USD 300 million being lost forever.	Page 11, paragraphe 6	Les contrats intelligents développés par les blockchains permettent des contrats uniques dans leur exécution, néanmoins plus le contrat est sophistiqué ou complexe celui-ci peut présenter plus de failles de sécurité.	Les erreurs dans le code des contrats intelligents, comme les bugs de re-entrance, peuvent entraîner des pertes massives. Ces vulnérabilités sont exacerbées par un manque de standards et de pratiques établies pour le développement sécurisé des contrats intelligents, rendant la technologie risquée pour les utilisateurs et les investisseurs.	Les développeurs invoquent l'importance de la flexibilité des contrats intelligents mais souvent au détriment de la sécurité. Les utilisateurs invoquent les contrats intelligents comme étant une preuve de sécurité en ne connaissant pas les failles de sécurité existantes.	L'imaginaire d'une automatisation transparente et fiable, via les contrats intelligents, est compromis par des erreurs humaines et des failles dans la conception technique.	Développeurs blockchain, régulateurs	Imposer des audits obligatoires pour les contrats intelligents, développer des outils automatisés pour détecter les vulnérabilités, et établir des standards internationaux de sécurité pour les contrats intelligents.	La Suisse propose des régulations spécifiques pour les contrats intelligents dans les secteurs financiers, ce qui pourrait servir de modèle pour d'autres régions.
Tension sur la vulnérabilité et la confidentialité des données sur les blockchains	If quantum computing becomes powerful enough, this process could be sped up dramatically with regards to current cryptography, exposing existing blockchain ledgers. Therefore there are some risks involved, although these are not imminent and are not related solely to blockchain. Despite these risks, users today can be highly confident that data on a blockchain is secure, that blockchain ledgers are indeed append-only (information can only be added, not removed), and that they are for all intents and purposes immutable. We would, however, note that just because a blockchain ledger is immutable does not mean that the data it contains is correct or private.	Page 8, paragraphe 2	Les données sur les blockchains publiques sont exposées à des danger de sécurité constant. Les écosystèmes blockchains paraissent sécurisés mais face à l'arrivée d'ordinateurs quantiques une faille de sécurité est possible. Il est également important de comprendre le trilemme qui est posé lors de la création d'une blockchain; celle-ci doit choisir dans quelle branche elle veut être la plus performante.	Bien que les blockchains publiques garantissent la transparence, elles permettent également de tracer des transactions jusqu'aux individus en combinant des analyses approfondies et des informations externes (Ip, matériel informatique, etc). Cela crée un paradoxe entre la transparence souhaitée et la protection des données personnelles, notamment dans un cadre réglementaire comme le RGPD.	Les utilisateurs des blockchains invoquent la sécurité de ces systèmes en comparaison avec ceux existant mais en omettant que la sécurité des blockchains ne reste pas inviolable. Les blockchains invoquent la sécurité totale du système en omettant le trilemme de base des blockchains, si celle-ci est hyper sécurisée en contrepartie elle sera plus lente dans l'encodage de block.	L'imaginaire d'une blockchain respectant la vie privée tout en étant transparente est difficile à réaliser, nécessitant des compromis technologiques et éthiques.	Régulateurs, entreprises technologiques, développeurs	Promouvoir des techniques de confidentialité comme les preuves à divulgation nulle ainsi que des blockchains hybrides combinant transparence et confidentialité.	Monero et Zcash utilisent des protocoles avancés de confidentialité, mais ces solutions restent peu intégrées dans les environnements régulés.
	Blockchain trilemma : The blockchain trilemma posits that blockchains are restricted to two of the following three properties: scalability (performance in terms of speed and volume), decentralisation and or security. If a blockchain is to be highly decentralised and highly secure, itwill come at the cost of scalability. If it is highly performant and highly decentralised, it will not be secure. Similarly, if one is willing to accept a degree of centralisation, it is possible to build highly secure and performant blockchains.	Page 9, paragraphe 6							
	Another misconception is that data on a blockchain is encrypted. This is not necessarily the case. Cryptocurrencies use cryptography to function, but the transactions in Bitcoin, for example, are not encrypted. It is possible to inspect the transaction amounts and public keys of all entries in the ledger. Indeed, thatis the point. Furthermore, as we pointed out in our GDPR paper, even if data is encrypted, no encryption is 100% foolproof. History has shown that most cryptographic functions are eventually cracked. Many people also worry that as quantum computing becomes a reality, all existing cryptography will immediately be vulnerable, and that the transaction history of every transaction on every blockchain up to that point will be exposed for all to see.	Page 16, paragraphe 5							
Tension sur le manque de connaissance des utilisateurs de blockchain	One issue facing blockchain is the fact that not enough people understand cryptography and how to use it properly. There are incidents of blockchain projects not using it properly or developing their own cryptography, which does not necessarily work as intended. We recommend efforts to increase education, expertise and dissemination of best practice in this area. The same can be said of smart contract technology. It is equally important that people understand how big the consequences can be of errors in immutable contracts and with blockchain protocols.	Page 21, paragraphe 5	La tension repose sur le déficit de connaissances et de compétences des utilisateurs en matière de cryptographie et de smart contracts, ce qui expose les utilisateurs à des risques élevés d'erreurs et de mauvaises implémentations.	Bien que la blockchain soit souvent perçue comme une technologie sécurisée, son utilisation correcte repose sur une bonne compréhension des concepts cryptographiques et des smart contracts. Le manque de connaissances dans ces domaines entraîne des incidents et des vulnérabilités pouvant compromettre la fiabilité des projets blockchain. Cette situation souligne l'importance d'investir dans la formation et la sensibilisation des utilisateurs et développeurs.	Les experts en sécurité mobilisent un discours sur la formation pour réclamer davantage d'efforts en matière d'éducation de la part des gouvernements. Les investisseurs utilisent le discours de la surréglementation des gouvernements face à une technologie en plein essor.	L'imaginaire sociotechnique d'une blockchain fiable et sans risque entre en tension avec la réalité d'une adoption parfois mal maîtrisée par des utilisateurs insuffisamment formés, ce qui montre la nécessité d'un renforcement des compétences et de la sensibilisation.	Développeurs, gouvernements, utilisateurs de blockchain, institutions académiques	Le développement de programmes de formation et de certification sur les technologies blockchains et cryptographiques, encourager la diffusion des bonnes pratiques au sein des communautés blockchain. Néanmoins un effort d'éducation du grand public est important, celui-ci ne doit pas être réservé qu'à ceux qui s'intéressent à la blockchain.	Des initiatives comme celles du MIT et de l'Université de Zurich offrent déjà des formations spécialisées sur les technologies blockchains et cryptographiques permettant de réduire les risques liés aux erreurs d'implémentation.
Tension sur la sécurité des actifs numériques	While blockchains are generally secure, digital assets held on blockchains unfortunately are often not. This is a major problem as many blockchain platforms are designed to handle transactions and store value, making them a prefered target of cyber criminals. It can also make errors extremely costly in the literal sense: a lost private key can mean an irrecoverable loss of funds. According to one report, some USD 1.7 billion were lost or stolen on blockchains in 2018.	Page 11, paragraphe 3	La tension repose sur le fait que, bien que les blockchains soient sécurisées, les actifs numériques qui y sont stockés restent vulnérables aux cyberattaques et aux erreurs humaines.	Les blockchains offrent une architecture sécurisée grâce la décentralisation et la cryptographie. Cependant, les actifs numériques (cryptomonnaies, NFT, etc.) détenus sur ces plateformes sont des cibles privilégiées pour les cybercriminels. De plus, les erreurs telles que la perte de clés privées peuvent entraîner des pertes irrécupérables de fonds. Cette problématique freine l'adoption massive de la blockchain par le grand public et les institutions.	Les blockchains utilisent le discours de la responsabilité individuelle pour justifier l'importance de la gestion des clés privées. A l'inverse, les systèmes financiers classiques basés sur la sécurité de récupération utilisent le discours de la responsabilité individuelle comme dangereux à l'exploitation de la blockchain.	L'imaginaire sociotechnique d'une économie numérique sécurisée, décentralisée et accessible entre en tension avec la réalité des risques élevés liés à la sécurité des actifs numériques soulignant la nécessité d'améliorations dans la gestion des clés et les protocoles de sécurité.	Développeurs de protocoles blockchain, fournisseurs de portefeuilles numériques, régulateurs, utilisateurs, système financier	Encourager le développement de solutions de récupération de clés privées, renforcer la sécurité des portefeuilles numériques et promouvoir l'éducation des utilisateurs sur les bonnes pratiques de gestion des actifs numériques.	Des initiatives comme celle de la plateforme Coinbase qui propose des services de récupération de clés et de gestion sécurisée des actifs numériques visent à améliorer la sécurité et à réduire les pertes d'actifs numériques. Coinbase se positionne comme un intermédiaire de confiance.