Smart Contracts

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 entre l'immutabilité des smart contracts et la nécessité de flexibilité juridique	Second, a blockchain-based smart contract is "written in stone", i.e., cannot be altered. The blockchain is decentralized, and usually that is a good thing. But it also means that no central authority or referee will be able to step in, in case one party feels wronged or even defrauded.	Page 29, paragraphe 10	La tension réside dans l'opposition entre l'immutabilité des smart contracts, qui garantit leur sécurité, et la nécessité de flexibilité des contrats juridiques pour s'adapter aux circonstances imprévues.	L'immutabilité des smart contracts est essentielle pour leur sécurité et leur intégrité, elle pose un problème lorsqu'une erreur doit être corrigée ou lorsqu'une modification devient nécessaire pour s'adapter à de nouvelles conditions. Ce manque de flexibilité juridique peut freiner l'adoption des smart contracts, en particulier pour les entreprises ou utilisateurs.	Les régulateurs et les juristes mobilisent la voie de la flexibilité juridique pour réclamer des mécanismes permettant d'amender ou de révoquer les smart contracts en cas de litige ou d'erreur.	L'imaginaire sociotechnique des smart contracts repose sur une exécution automatique, immuable et fiable. Cependant, cet imaginaire est remis en question par la réalité des besoins juridiques qui nécessitent des mécanismes de flexibilité.	Régulateurs, juristes, développeurs de blockchains, entreprises	Promouvoir des outils permettant aux parties contractantes de gérer les imprévus en toute sécurité et d'éduquer les personnes sur les mécanismes et les codes informatiques qui régissent les smarts contracts.	Le Royaume-Uni adopte une approche plus flexible pour les smart contracts avec des cadres juridiques explorant des options de modification et d'interprétation pour répondre aux imprévus.
	It is likely that the EU will rely on harmonised requirements and standards to facilitate the use of smart contracts if the current smart contract provisions are approved in more or less their current form. The EC is taking a different stance than the UK in terms of the need to legislate for enabling the effective adoption of smart contracts. UK appears to be on the more flexible and adoptive side, but still, it seems that businesses entering into smart contracts with EU counterparties, will want to align with Article 30 Data Act requirements, even if the contracts are governed by English law.	Page 30, paragraphe 2							
Tension entre la transparence des smart contracts et la confidentialité des données	Privacy and multi-party computation are matters that must be addressed in the execution of smart contracts. For this reason, tools like Raziel (Sánchez) implement a variety of methods to ensure their private, correct, and verifiable execution. The aforementioned tool uses Zero-Knowledge Proofs to confirm validity prior to the execution of the smart contract to any third party and keep the information private. Related work is from accountable algorithms (Kroll) where a commit and prove scheme is implemented for zk-SNARKs.	Page 13, paragraphe 1	Cette tension repose sur le conflit entre la transparence nécessaire pour assurer la vérifiabilité et la traçabilité des smart contracts et la confidentialité indispensable pour protéger les données sensibles des différentes parties, particulièrement dans des secteurs tels que la finance ou la santé.	La transparence des smart contracts garantit la traçabilité et réduit le risque de manipulation mais elle entre en conflit avec la nécessité de protéger les données sensibles.	Les régulateurs utilisent un discours sur la vie privée pour mobiliser la voie de la protection des données afin de réclamer des solutions garantissant la confidentialité.	L'imaginaire d'une transparence totale et sécurisé des transactions grâce aux smart contracts se heurte à la réalité des exigences en matière de protection des données personnelles et de confidentialité. Cette tension souligne la nécessité de développer des technologies permettant de concilier transparence et confidentialité.	Développeurs, régulateurs, entreprises, citoyens	Développer et promouvoir des solutions techniques comme les preuves à divulgation nulle de connaissance (ZKP) et des oracles de confidentialité indépendants.	La Suisse a adopté un cadre réglementaire encourageant l'utilisation de solutions blockchains basé sur des systèmes hybrides. La solution serait d'avoir un oracle publique qui valide les données intégrées à la blockchain.
Tension entre la sécurité des smart contracts et les risques de vulnérabilité	Decentralised finance (DeFi) is a highly volatile market where millions of people become victims of large-scale privacy breaches and theft. If we look at the number, we find that within the first three months of 2022 USD 682 million was lost due to hacks and crypto fund owners and businesses lost USD 3.3+ billion as a result of hacker attacks and security breaches. Deliberate hacks that exploit blockchain-type technologies can include 'rug-pulls', 'flashloan attacks', and a combination of these attacks with traditional types of irregular behaviour. Opportunistic attacks on smart-contracts can also exploit vulnerabilities, bugs and errors in the contract code.	Page 9, paragraphe 6	La tension réside dans le fait que bien que les smart contracts offrent une automatisation fiable, leur sécurité repose sur la qualité du code. Ceci expose les utilisateurs de la technologie à des risques importants en cas de bugs ou d'attaques.	Les smart contracts automatisent les transactions sans intermédiaire, mais les vulnérabilités dans leur code peuvent être exploitées, entraînant des pertes financières et une perte de confiance des utilisateurs dans cette nouvelles technologies.	Les dévloppeurs utilisent le discours de l'innovation pour justifier les bugs ou les possibilités d'arnaque, cette voie se retourne contre eux en étant mobilisée par les régulateurs qui mettent en avant les failles des smarts contracts.	L'imaginaire d'un écosystème automatisé et sécurisé, où les smart contracts fonctionnent sans intermédiaire humain, se heurte à la réalité des vulnérabilités techniques et des bugs, montrant que des audits de code sont importants pour garantir la confiance dans ces nouvelles technologies.	Développeurs, plateformes décentralisées, régulateurs, utilisateurs	Proposer des audits de sécurité systématiques pour les smart contracts.	Singapour a adopté des cadres réglementaires exigeant des audits de sécurité pour les smart contracts financiers.