

Taxonomie des vulnérabilités liées aux incitations dans les blockchains

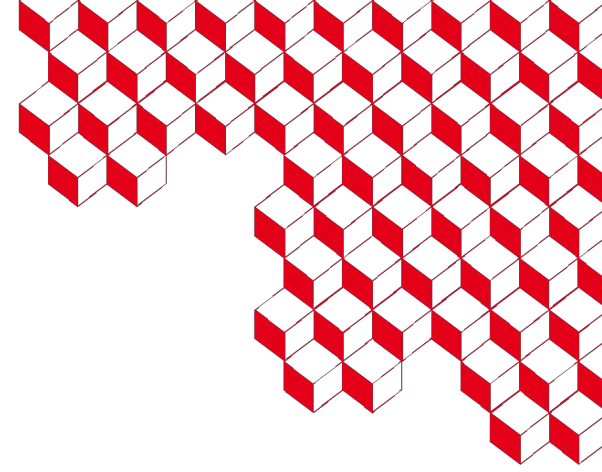
JFSMA 2023

Hector Roussille : Université Paris Saclay CEA LIST / Université de Montpellier LIRMM

Önder Gürçan : Université Paris Saclay CEA LIST

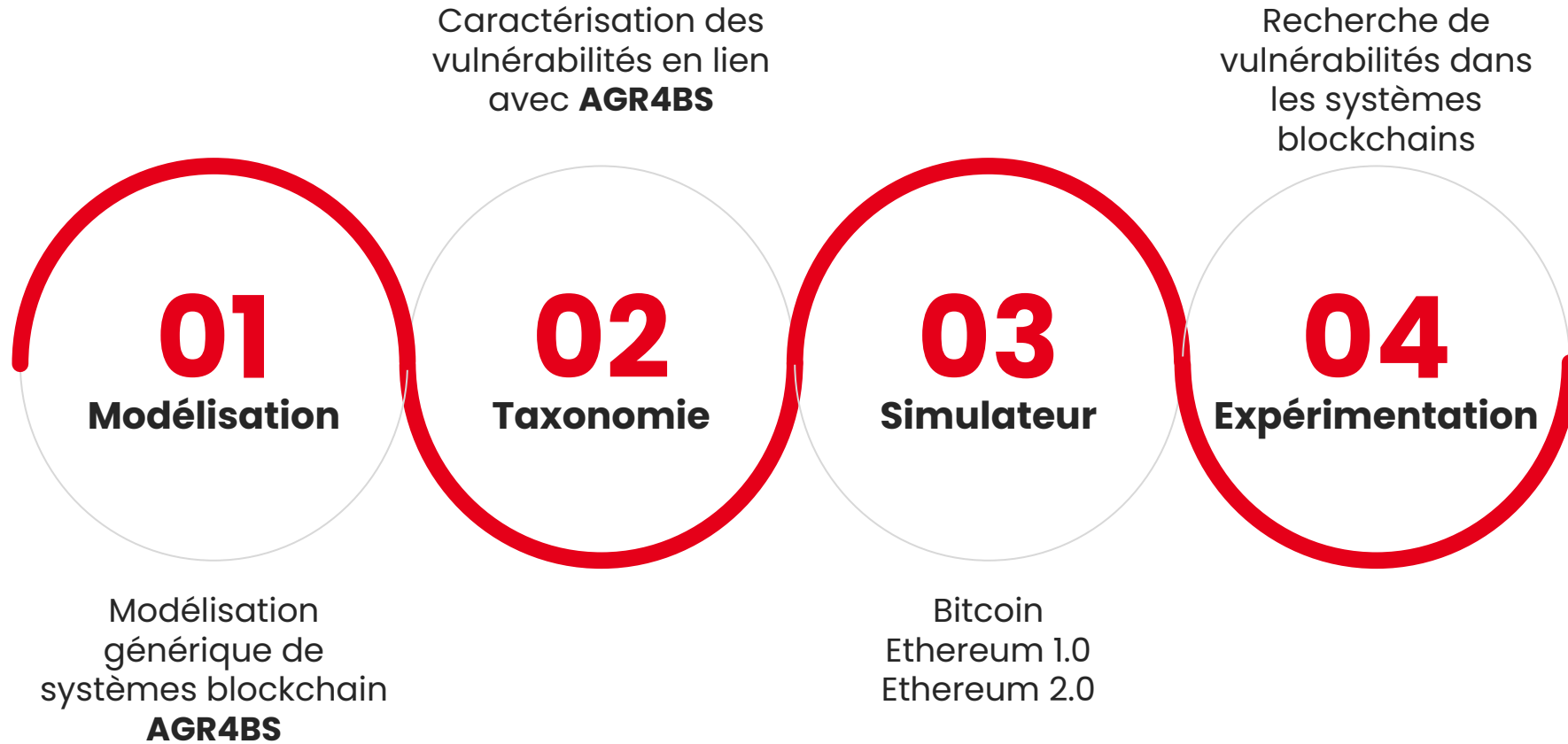
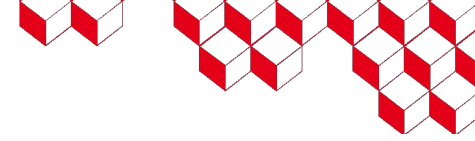
Fabien Michel : Université de Montpellier LIRMM






**Comment utiliser l'apprentissage
par renforcement pour sécuriser
les systèmes blockchain ?**

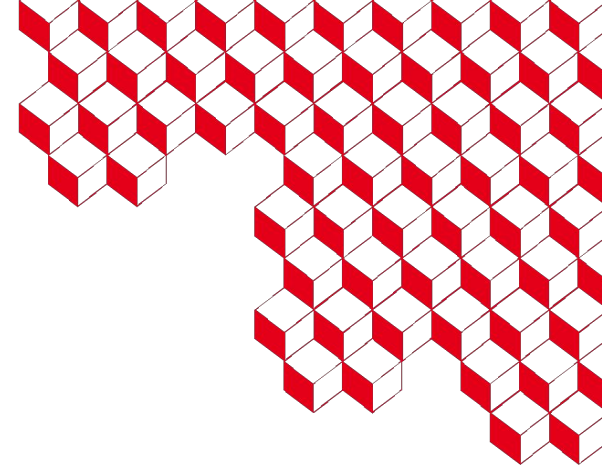
Contexte



28/10/2022

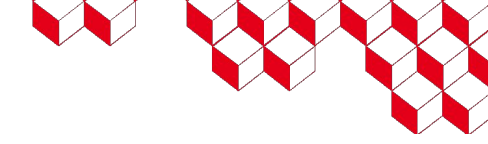


1. Blockchain

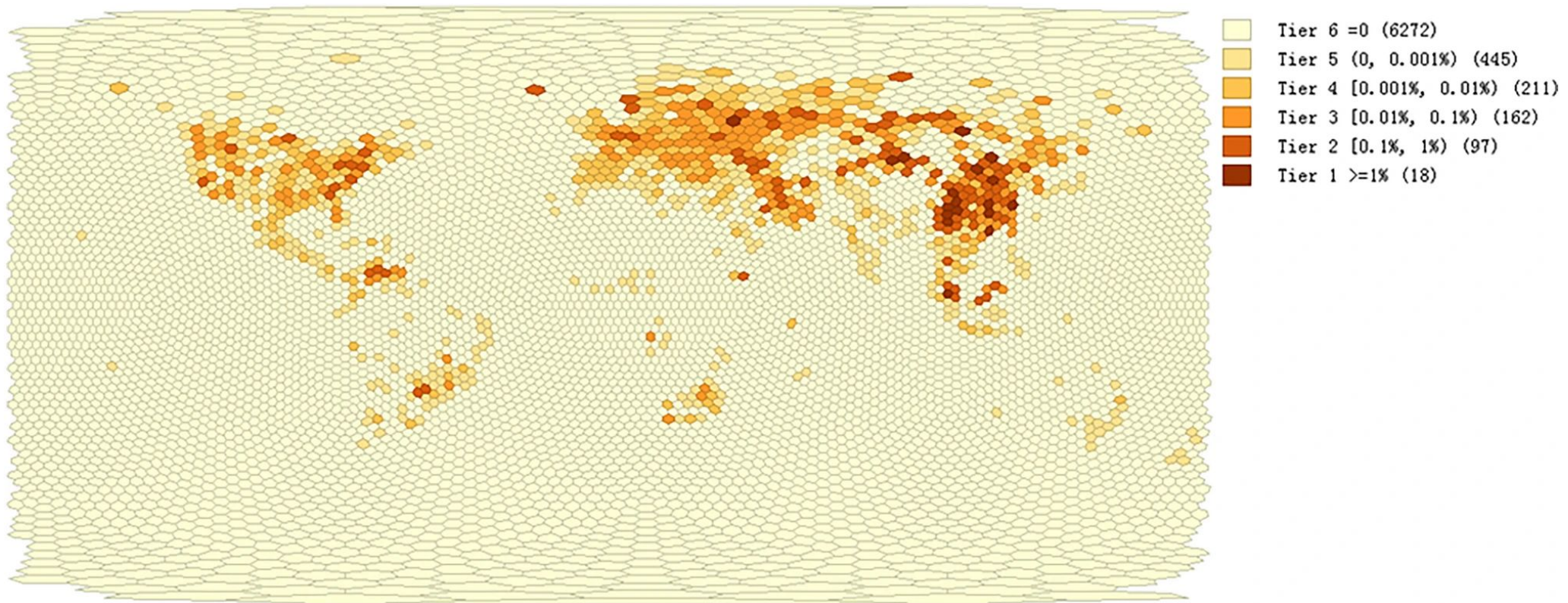


Les systèmes blockchain sont des registres distribués, décentralisés et inviolables.

Des systèmes distribués



Sun, W., Jin, H., Jin, F. *et al.* Spatial analysis of global Bitcoin mining. *Sci Rep* 12, 10694 (2022). <https://doi.org/10.1038/s41598-022-14987-0>



Sun, W., Jin, H., Jin, F. *et al.* Spatial analysis of global Bitcoin mining. *Sci Rep* 12, 10694 (2022). <https://doi.org/10.1038/s41598-022-14987-0>

Blocs, Transactions et Transition

Un système blockchain est composé de :

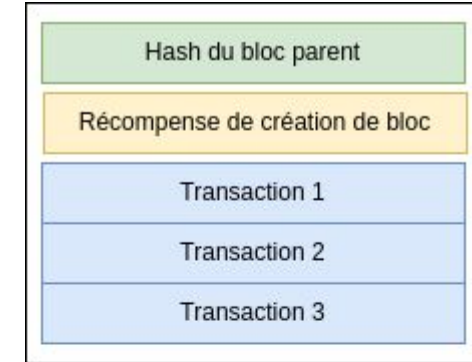
- Participants contributeurs (Mineurs, Validateurs, etc.)
- Participants utilisateurs
- (Contrats Intelligents)

Tous les participants peuvent envoyer des transactions.

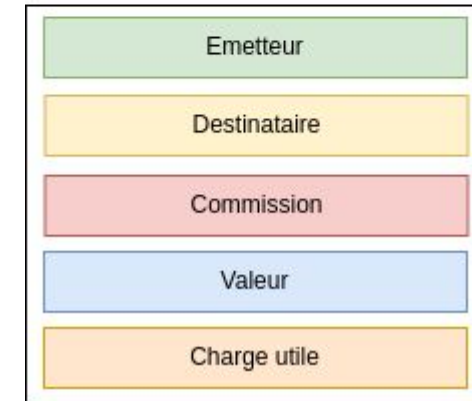
Seuls les contributeurs peuvent créer des blocs

- ex : Mineurs Bitcoin ou Validateurs Ethereum 2.0

Exemple de bloc :



Exemple de transaction :



Des systèmes décentralisés

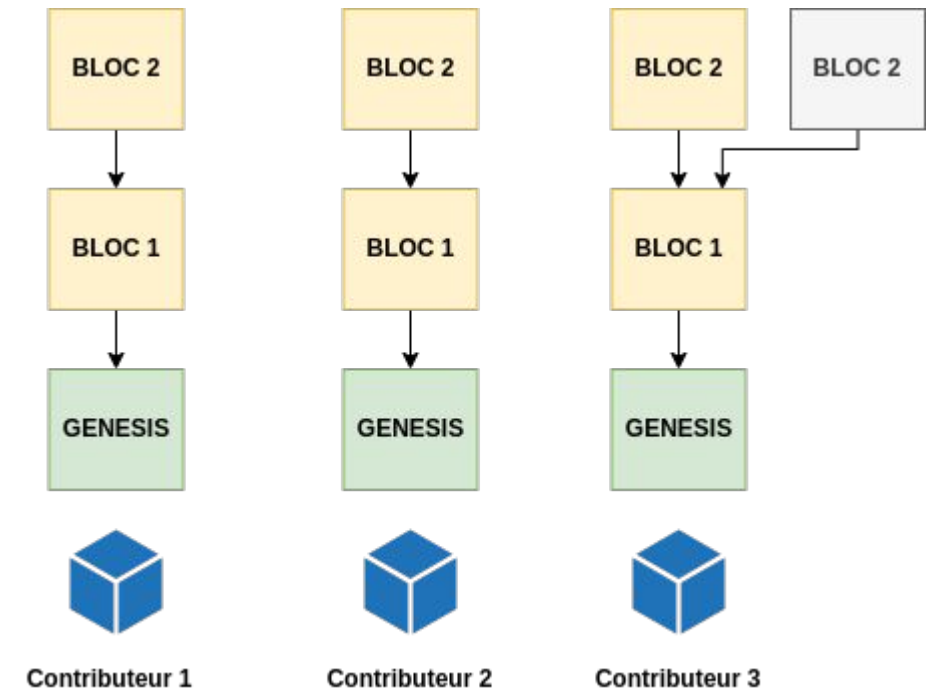
Chaque contributeur


- Dépense ou verrouille des ressources pour contribuer
- maintient une copie locale de la blockchain
- Infère un état en fonction de sa vue du système
- est récompensé pour son travail : *incitations*

Les vues peuvent diverger au cours d'un *fork*

Le mécanisme de consensus donne aux agents les règles pour définir la chaîne canonique.

- comment / quand créer un bloc valide
- comment résoudre un fork





2 ■ Modélisation

Agent Group Roles for Blockchain Systems : AGR4BS^[1]

[1] Roussille, H.; Gürçan, Ö.; Michel, F. AGR4BS: A Generic Multi-Agent Organizational Model for Blockchain Systems. Big Data Cogn. Comput. 2022, 6, 1. <https://doi.org/10.3390/bdcc6010001>

AGR4BS : Un outil de modélisation blockchain

Une modélisation organisationnelle inspirée du modèle AGR^[2]



[2] Ferber, Jacques et al. "From Agents to Organizations: An Organizational View of Multi-agent Systems." *International Workshop on Agent-Oriented Software Engineering* (2003).

Les rôles de haut niveau dans AGR4BS



1

Blockchain Maintainer

- Gestion blockchain
- Validation des blocs
- Validation des txs
- Transition d'état

2

Block Proposer

- Création de blocs
- Inclusion des txs

3

Transaction Proposer

- Création de txs

4

Transaction Endorser

- vote pour des txs

5

Block Endorser

- Vote pour des blocs

6

Investor

- Investis des ressources

7

Investee

- Reçois des investissements

8

Contractor

- Contrat Intelligent sur la blockchain

9

Group Manager

- Autorise l'entrée / sortie dans un groupe

10

Oracle

- Injecte des données dans le système blockchain

3

Taxonomie

- Caractérisation des vulnérabilités d'incitations^{[3][4]}

[3] H. Roussille, O. Gurcan and F. Michel, "A Taxonomy of Blockchain Incentive Vulnerabilities for Networked Intelligent Systems," in IEEE Communications Magazine, doi: 10.1109/MCOM.005.2200904.

[4] H. Roussille, O. Gurcan and F. Michel, "Taxonomie des vulnérabilités liées aux incitations dans les blockchains" in JFSMA 2023.

Incitations



Les contributeurs sont récompensés pour leur travail :

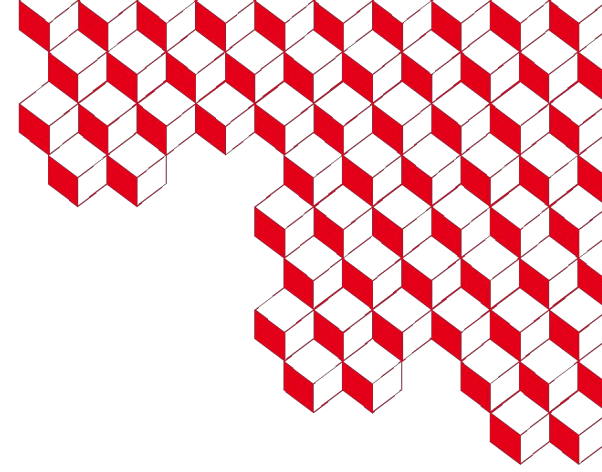
- Récompense de création de bloc
- Frais de transactions
- (Attestations)

Ces récompenses guident vers le comportement désiré.

Et, dans certains systèmes, punis en cas de mauvais comportement :

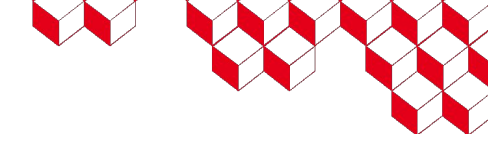
- Pénalités
- Slashing

Ces pénalités punissent un comportement qui ne correspond pas au comportement attendu.



Que se passe-t-il si la rationalité impose un comportement différent du comportement désiré ?

Vulnérabilités d'incitations



Une vulnérabilité d'incitation est un problème de non-alignement entre le comportement rationnel et le comportement désiré.

Plusieurs exemples :

- Double dépense^[5]
- Selfish Block Creation^[6]
- Nothing at Stake^[7]

[5] U. W. Chohan, "The Double Spending Problem and Cryptocurrencies," SSRN Electronic Journal, 2018.

[6] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in International Conference on Financial Cryptography and Data Security. Springer, 2014

[7] W. Li, S. Andreina, J.-M. Bohli, and G. Karame. "Securing proof-of-stake blockchain protocols". In J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, and J. Herrera-Joancomartí, editors, Data Privacy Management, Cryptocurrencies and Blockchain Technology, pages 297–315, Cham, 2017. Springer International Publishing

Pourquoi une autre taxonomie ?

Il existe différentes taxonomies dans la littérature^{[8] [9] [10] [11] [12]}

Mais elles :

- Ne se concentrent pas uniquement sur les vulnérabilités d'incitations
- S'intéressent peu aux causes des déviations (*i.e.*, incitations)
- Utilisent généralement un découpage en couches technologiques

[8] Muhammad Saad et al, Exploring the Attack Surface of Blockchain : A Comprehensive Survey. IEEE Communications Surveys and Tutorials, 22(3) :1977–2008, 2020.

[9] Khizar Hameed, et al, A taxonomy study on securing blockchain-based industrial applications : An overview, application perspectives, requirements, attacks, countermeasures, and open issues. J Ind Inf Integr, 26 :100312, 2022

[10] arwar Sayeed, Hector Marco-Gisbert, and Tom Caira. Smart Contract : Attacks and Protections. IEEE Access, 8 :24416– 24427, 2020.

[11] Ayman Alkhalifah et al.. A Taxonomy of Blockchain Threats and Vulnerabilities, pages 3–25. CRC Press, United States, 1 edition, August 2020.

[12] iaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. A survey on the security of blockchain systems. Future Generation Computer Systems, 107 :841–853, 2020

Catégorisation des types d'impact



Nous distinguons 3 grandes catégories d'impact :

Équité

- censure
- gains disproportionnés

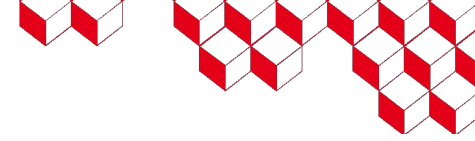
Sécurité

- Impact de finalité
- Données invalides

Économie

- manipulation du prix
- augmentation artificielle des frais

Sévérité, Risque et Échelle



La **sévérité** dénote la gravité d'une attaque réussie en termes d'impact sur :

- les participants ciblés
- les groupes ciblés
- le système

Le **risque** exprime la faisabilité / probabilité de réussir une attaque.

Ces caractéristiques varient en fonction de l'**échelle** de l'attaque définie selon la quantité de ressources requises :

- puissance de calcul
- stakes
- connexion réseau
- Identités blockchain

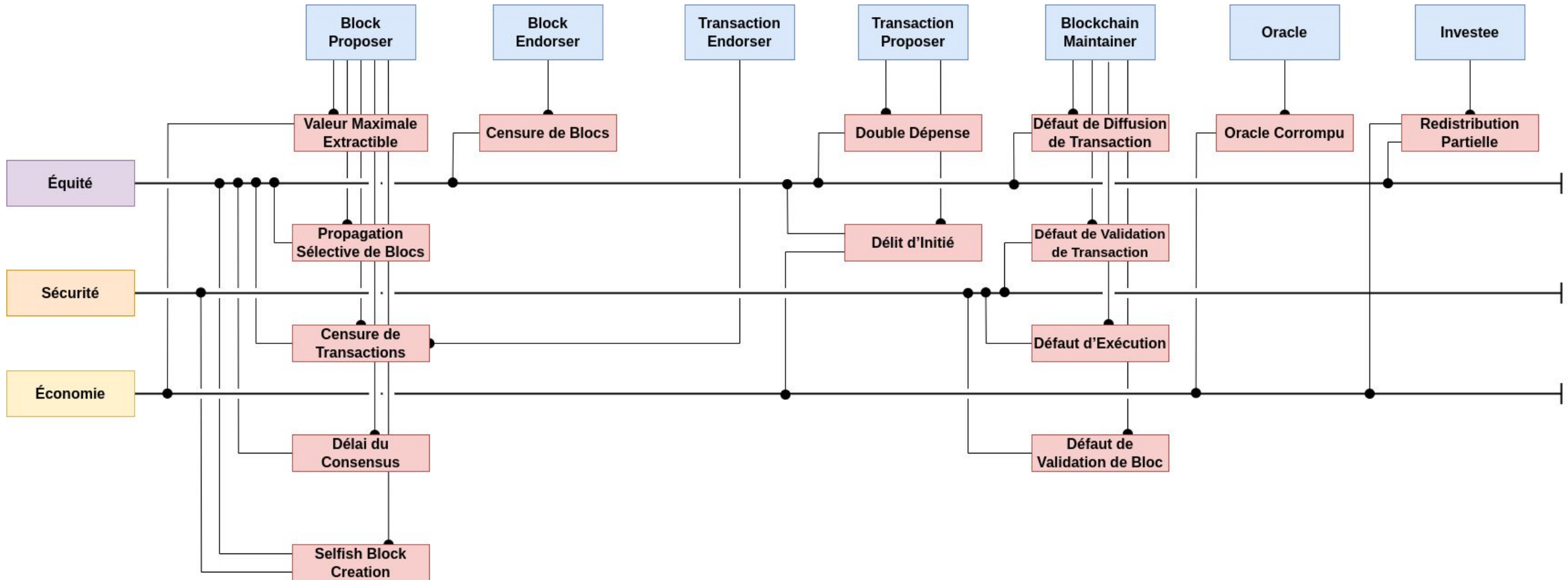
Vue d'ensemble de la taxonomie

Rôle	Déviations Exploitant une vulnérabilité d'incitation				Métriques						
	Déviation	Comportements Déviés	Rôles Impactés	Références	Impact	Petite Échelle		Grande Échelle		Priorité	Système
						Sévérité	Risque	Sévérité	Risque		
Block Proposer	Censure de Transactions	selectTransactions	Transaction Proposer	[9]	Équité	●○○○○	●●●○○	●●●○○	●●●○○	0.16	Tous
	Propagation Sélective de Blocs	proposeBlock	Blockchain Maintenir Block Proposer	N/A		●○○○○	●○○○○	●●●○○	●●○○○	0.24	Tous
	Délai du Consensus	createBlock proposeBlock	Tous	N/A		●○○○○	●○○○○	●●●●●	●○○○○	0.80	PBFT
	Selfish / Stubborn Block Creation	createBlock proposeBlock	Blockchain Maintenir Block Proposer	[7]	Équité Sécurité	●●○○○	●●○○○	●●●●●	●○○○○	0.25	PoW
	Valeur Maximale Extractible	selectTransaction createBlock	Transaction Proposer	[4]	Équité Économie	●●○○○	●●●●○	●○○○○	●●●●○	0.32	Tous
Block Endorser	Censure de Blocs	endorseBlock	Block Proposer Transaction Proposer	N/A	Équité	●○○○○	●●●●○	●●●●○	●○○○○	0.16	Approbation Explicite
Transaction Endorser	Censure de Transactions	endorseTransaction	Transaction Proposer	[13]		●○○○○	●●●●○	●●●●○	●○○○○	0.16	Approbation Explicite
Transaction Proposer	Double Dépense	createTransaction	All	[3]	Équité	●○○○○	●○○○○	●●●●○	●○○○○	0.25	Tous
	Délit d'Initié	createTransaction	Transaction Proposer	[6]	Économie	●●○○○	●●●●○	●●●○○	●●●●○	0.60	Tous
Blockchain Maintenir	Défaut de Validation de Transaction	validateTransaction	None	[12]	Sécurité	●○○○○	●●●●○	●●●●○	●●○○○	0.40	Tous
	Défaut de Validation de Bloc	validateBlock	None			●○○○○	●●●●○	●●●●○	●●○○○	0.40	Tous
	Défaut d'Exécution	validateTransaction executeTransaction	None			●○○○○	●●●●○	●●●●○	●●○○○	0.40	Tous
	Défaut de Diffusion	diffuseTransaction	Blockchain Maintenir	[5]	Équité	●○○○○	●●●●○	●●●○○	●●●●○	0.64	Tous
Oracle	Oracle Corrompu	oracleBehavior	Contractor Investor Investee	[2]	Économie	●●○○○	●●●●○	●●●●○	●●○○○	0.40	Tous
Investee	Redistribution Partielle	redistribute	Investor	N/A	Équité Économie	●●○○○	●●●●○	●●●○○	●●○○○	0.32	Tous

TABLE 1 – Taxonomie des vulnérabilités d'incitation basée rôles.

Très Bas : ●○○○○ , Bas : ●●○○○ , Moyen : ●●●○○ , Haut : ●●●●○ , Très Haut : ●●●●●

Vue d'ensemble de la taxonomie



Perspectives



Les vulnérabilités les plus critiques ont un impact sur la **Sécurité** et s'attaquent au **consensus**.

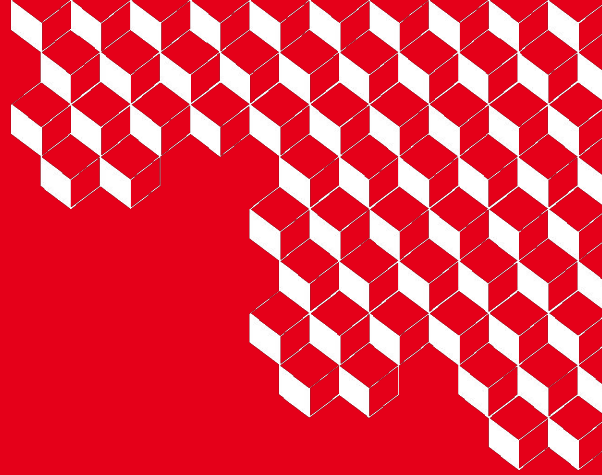
Le rôle central du consensus implique que tous les participants sont impactés s'il venait à être perturbé.

Nous étudions actuellement la **Bouncing Attack**^[13] sur Ethereum 2.0 dans notre simulateur.

[13] Caspar Schwarz-Schilling et al. Three Attacks on Proof-of-Stake Ethereum, Arxiv eprint 2110.10086, 2021



list



MERCI