Université de Strasbourg

Étude de la probabilité de fork dans les blockchains

Thomas Lelièvre
28 août 2024


In Memoriam
to Kabosu (2005-2024)
A good doge!

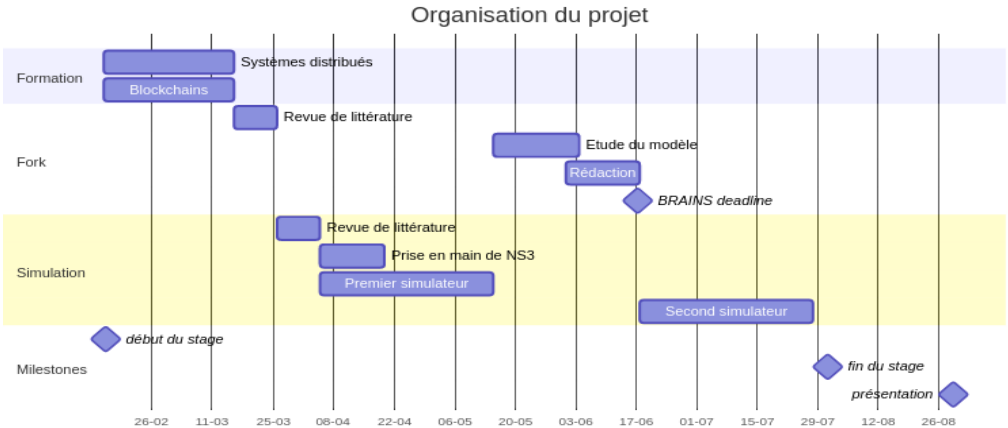
Présentation du stage
Objectifs

Objectif général : étude de la probabilité de fork dans les blockchains utilisant la Preuve d'intéraction (PoI).

En particulier :

- Établir un modèle théorique
- Simuler le comportement la blockchain

Présentation du stage
Déroulement



Anatomie d’un DLT

Blockchains

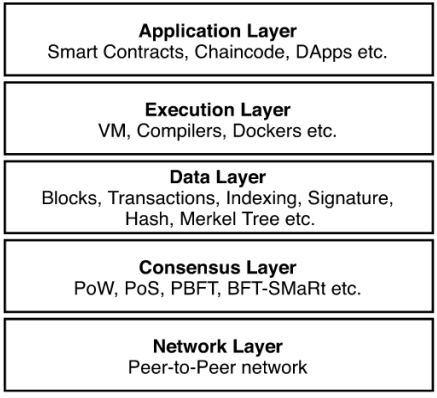


FIGURE 3. **Abstraction layer model for DLT.**

Applications

- Crypto-monnaie
- DAO (Decentralized Autonomous Organization)
- NFT (Non-Fungible Token)

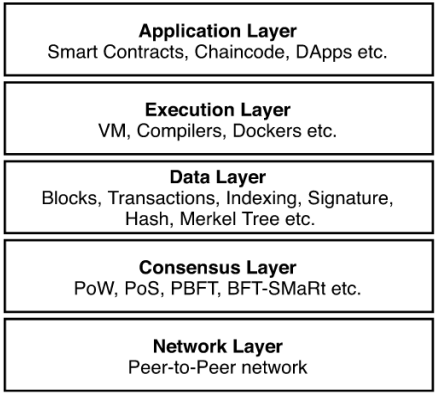


FIGURE 3. **Abstraction layer model for DLT.**

Applications

```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.8.2 <0.9.0;

/**
 * @title Storage
 * @dev Store & retrieve value in a variable
 */
contract Storage {

    uint256 number;

    function store(uint256 num) public {
        number = num;
    }

    function retrieve() public view returns (uint256){
        return number;
    }
}
```

Listing 1 – Exemple de Smart Contract écrit en Solidity

Blockchains

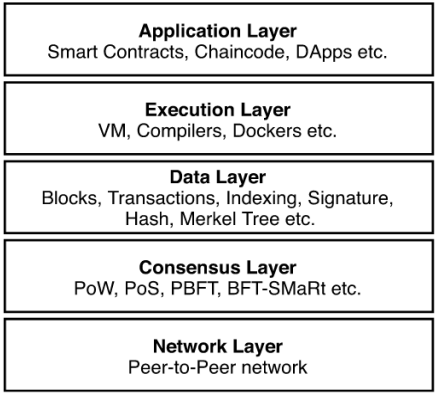


FIGURE 3. **Abstraction layer model for DLT.**

Exécution

```
{
  "functionDebugData": {},
  "generatedSources": [],
  "linkReferences": {},
  "object": "6080604052348015600e575f80fd5b50 ...",
  "opcodes": "PUSH1 0x80 PUSH1 0x40 MSTORE CALLVALUE DUP1 ISZERO ...",
  "sourceMap": "199:356:0:-:0;;;;;;;;;;;;;;;;;;;"
}
```

Listing 2 – Bytecode EVM (Ethereum Virtual Machine)

Blockchains

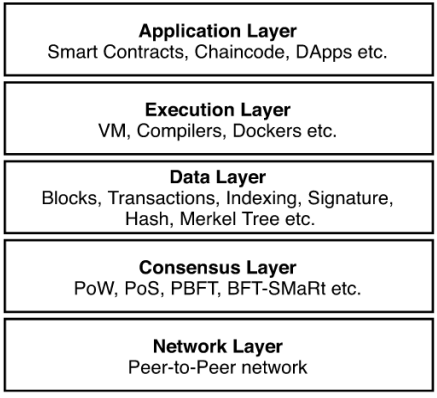


FIGURE 3. **Abstraction layer model for DLT.**

Données

- Blockchain

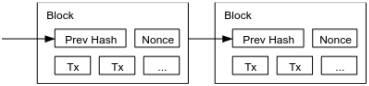


Figure –

- DLT DAG (Directed Acyclic Graph)

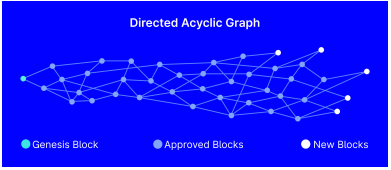


Figure – The Tangle. Source : [Pop18]

Blockchains

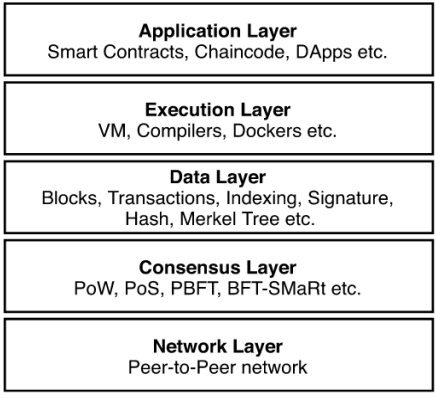


FIGURE 3. **Abstraction layer model for DLT.**

Consensus

Un algorithme de consensus tend à résoudre le problème du consensus [KS11] :

- **Accord (Agreement)** : Tous les processus non-défaillant doivent s'accorder sur une même valeurs.
- **Validité (Validity)** : Toute valeur renvoyer doit avoir été proposée par un des processus.
- **Finalisation (Termination)** : Tous les processus non-défaillant doivent renvoyer une valeurs en un temps fini.

Mais le consensus ne peut pas être résolut dans le cas général [FLP85].

Blockchains

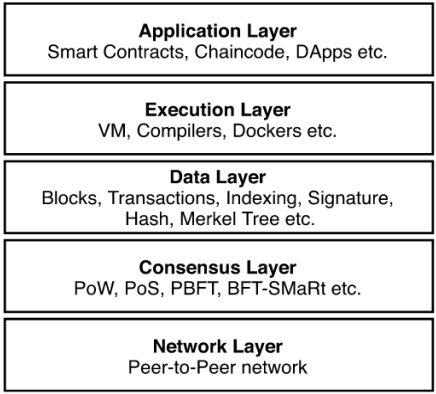


FIGURE 3. Abstraction layer model for DLT.

Consensus

La couche consensus garentira plutôt les propriété suivantes :

1. Accord
2. Sureté (safety) : deux blocs ne peuvent pas entrer en conflit (double dépense, ...)
3. Résistance aux attaques Sybil : il est improbable (ou très coûteux) qu'un attaquant puisse créer une chaine plus grande que la chaine légitime ($\sim$ validité)
4. Liveness : La chaine doit pouvoir continuer de grandir ($\sim$ finalisation)

Blockchains

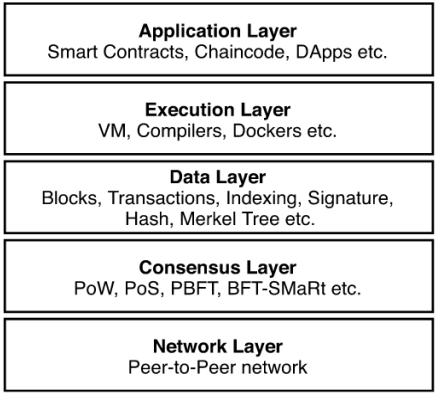


FIGURE 3. **Abstraction layer model for DLT.**

Consensus

Les plus algorithmes les plus connus sont :

- Preuve de travail (PoW)
- Preuve d'enjeux (PoS)
- Raft, PBFT-Like

Blockchains

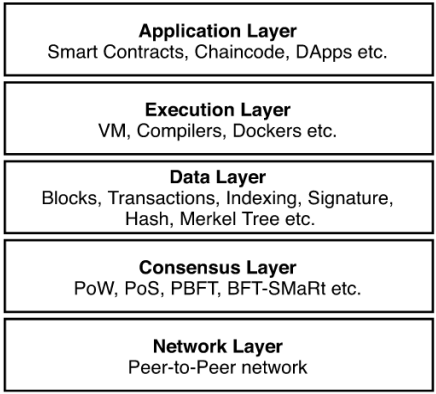


FIGURE 3. **Abstraction layer model for DLT.**

Réseau

Les noeuds de la blockchain sont connecter sur un réseau de pair à pair (Peer-to-Peer). Les conditions d'accès à ce réseau permettent de distinguer deux types de blockchains.

- Permissioned : Les noeuds sont connus et l'ajout de nouveaux noeuds est contrôlé par une autorité
- Permissionless : Les noeuds peuvent rejoindre le réseau librement les noeuds sont trouvé par des mécanisme de découvertes (gossip)

Analyse d’un algorithme de consensus :

La Preuve d’Interaction

Proof of Interation
Dépasser la preuve de travail

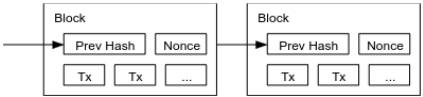


Figure – Preuve de Travail. Source : [Nak07]

Principe :

- Le consensus est resolu en élisant un leader qui gagne le droit de créer un bloc.
- Le leader est le premier participant à trouver un nonce tel que le hash du bloc soit inférieur à une certaine valeur.

Proof of Interation
Principe

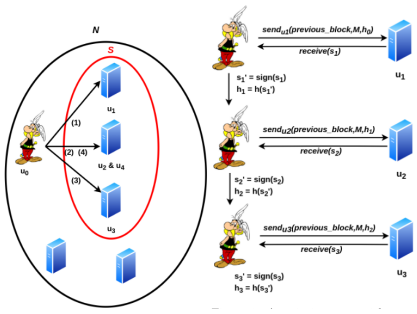


Figure – Preuve d'intéraction. Source : [ABN21]

Hypothèses :

- Le nombre de noeuds est fixe.
- Les noeuds sont connectés en un graphe complet.

Déroulement d'un tour :

1. Selection d'un sous-groupe de noeuds

Proof of Interation
Principe

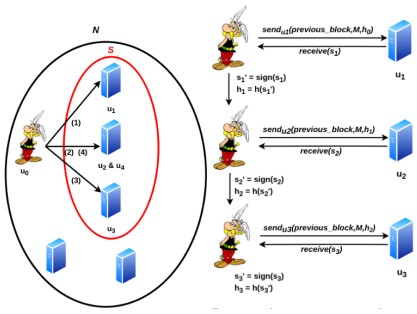


Figure – Preuve d'intéraction. Source : [ABN21]

Hypothèses :

- Le nombre de noeuds est fixe.
- Les noeuds sont connectés en un graphe complet.

Déroulement d'un tour :

1. Selection d'un sous-groupe de noeuds
2. Choix de la longueur du tour

Proof of Interation
Principe

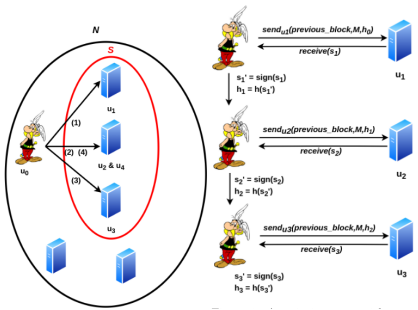


Figure – Preuve d'intéraction. Source : [ABN21]

Hypothèses :

- Le nombre de noeuds est fixe.
- Les noeuds sont connectés en un graphe complet.

Déroulement d'un tour :

1. Selection d'un sous-groupe de noeuds
2. Choix de la longueur du tour
3. Réalisation du tour

Proof of Interation
Principe

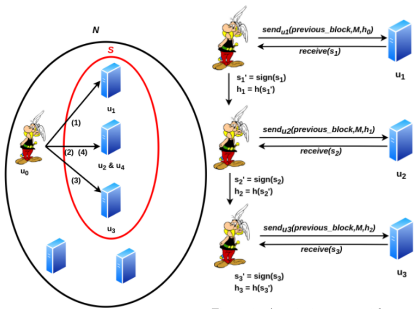


Figure – Preuve d'intéraction. Source : [ABN21]

Hypothèses :

- Le nombre de noeuds est fixe.
- Les noeuds sont connectés en un graphe complet.

Déroulement d'un tour :

1. Selection d'un sous-groupe de noeuds
2. Choix de la longueur du tour
3. Réalisation du tour

L'avantage de ce système est que le coût de l'élection est faible. De plus, il possède plusieurs paramètres qui permettent de régler la distribution des blocs.

Étude des Forks

Fork
Définition

Un **fork** est une divergence dans la blockchain en deux branches temporairement ou définitivement imcompatible.

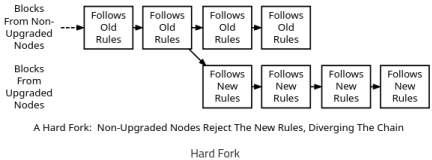


Figure – Hard Fork. Source : bitcoin.org

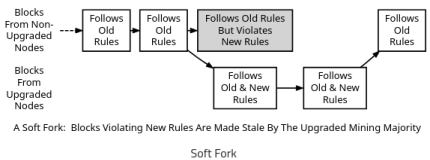


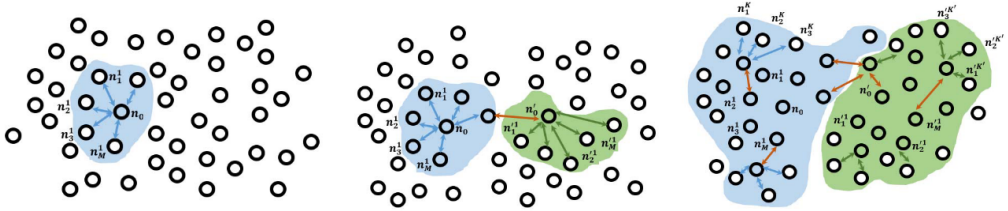
Figure – Soft Fork. Source : bitcoin.org

Fork
Causes

	Process-based $(A = B = S)$	**Protocol-based** $(A \neq B)$
Unintentional	Probabilistic Block Race	Client Incompatibility • Soft Fork • Hard Fork • Forced Fork
Deliberate	Block Withholding & Forced Block Race	Rule Change • Soft Fork • Hard Fork • Forced Fork

Figure – Quatre types de fork. Source : [Sch20]

Fork
Fork de processus involontaire



(a) Wave W_1 (b) Wave W_1' (c) Waves W_K and W_k'

Figure – Fork de processus créé par la propagation de deux blocs différents. Source : [DW13]

Fork
Travaux existants

L'étude de la probabilité de fork a été abordé sous différents angles :

- caractéristiques du réseau [Cro+16]
- vitesse de propagation des blocs [DW13]
- présence de pool de minage [ES13]

Fork
Travaux existants

L'étude de la probabilité de fork a été abordé sous différents angles :

- caractéristiques du réseau [Cro+16]
- vitesse de propagation des blocs [DW13]
- présence de pool de minage [ES13]

Notre contribution dans [LB24] :

- Impact de la distribution des temps de minage sur la probabilité de fork.
- Distribution optimale des temps de minage.

Fork
Modèle

Hypothèses :

- Les temps du minage sont discrets et bornés ($X(\Omega) = \{0, \ldots, T\}$)
- Les temps de minage sont indépendants et identiquement distribués.

Fork
Modèle

Hypothèses :

- Les temps du minage sont discrets et bornés ($X(\Omega) = \{0, \ldots, T\}$)
- Les temps de minage sont indépendants et identiquement distribués.

Un fork est possible si l'écart entre les temps de minage est inférieur au temps de transmission d'un bloc.

L'écart moyen entre le premier et le deuxième noeuds est donnée par :

$$E(X_{(2)}) - E(X_{(1)})$$

où $X_{(1)}$ et $X_{(2)}$ sont les temps de minage des deux premiers blocs.

Fork
Problème d'optimisation

$$\text{argmax}_{p \in [0,1]^{T+1}} E(X_{(2)}) - E(X_{(1)})$$

tel que

$$\sum_{i=0}^{T} p_i = 1$$

$$E(X_{(1)}) = m \in]0, T[$$

Proposition :

L'unique solution de ce problème est la loi de probabilité définit par

$$\mathbb{P}(X = 0) = 1 - \left(\frac{m}{T}\right)^{1/n}$$

$$\mathbb{P}(X = T) = \left(\frac{m}{T}\right)^{1/n}$$

Fork
Conclusion et limitations

Dans la PoI, la distribution des temps de minage est plus facilement adaptable. Et pourrait être ajusté pour minimiser les forks.

Limitations :

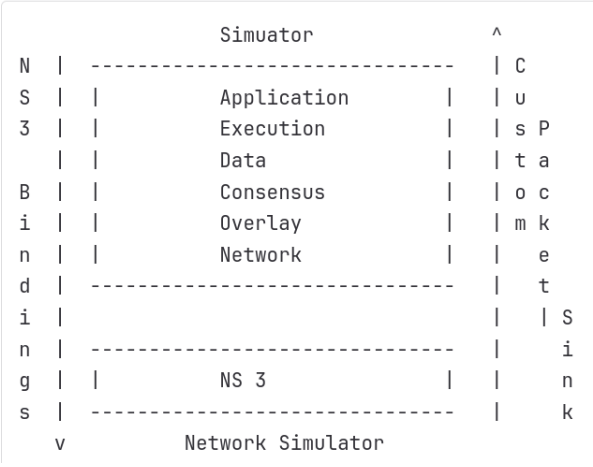
1. Ce résultat théorique ne s'intéresse qu'à l'écart entre le premier et le deuxième mineurs à trouver un bloc. La probabilité de fork dépend en plus du réseau.

$$\mathbb{P}(\text{fork}) = \mathbb{P}\Big(\bigcup_{1 \leq i < j \leq N} [|X_i - X_j| < t_{i,j}]\Big)$$

2. Il faut encore réaliser des simulations pour vérifier la pertinence de ce modèle d'ignorer le réseau (cas de blockchain permissioned).

Simuler le fonctionnement d’une blockchain

Simulator
Architecture



Conclusion

Conclusion
Tenue des objectifs

- **Modèle théorique** : Rédaction de [LB24]
- **Simulateur** : Première simulations pas encore au niveau de l'état de l'art
- **Amélioration de la PoI** : Pas encore réaliser

Conclusion
Travaux futurs

- PoI : rapprocher le protocole d'une distribution optimale
- Simulateur
  - Améliorer la colecte des données dans les noeuds
  - Inclure NS3

Bibliographie I

[ABN21] Jean-Philippe Abegg, Quentin Bramas et Thomas Noël. “Blockchain Using Proof-of-Interaction”. In : Networked Systems. Sous la dir. de Karima Echihabi et Roland Meyer. T. 12754. Springer International Publishing, 2021, p. 129-143. isbn : 978-3-030-91013-6 978-3-030-91014-3. doi : 10.1007/978-3-030-91014-3_9. url : https://link.springer.com/10.1007/978-3-030-91014-3_9 (visité le 20/03/2024).

[Cro+16] Kyle Croman et al. “On Scaling Decentralized Blockchains : (A Position Paper)”. en. In : Financial Cryptography and Data Security. Sous la dir. de Jeremy Clark et al. T. 9604. Series Title : Lecture Notes in Computer Science. Berlin, Heidelberg : Springer Berlin Heidelberg, 2016, p. 106-125. isbn : 978-3-662-53356-7 978-3-662-53357-4. doi : 10.1007/978-3-662-53357-4_8. url : http://link.springer.com/10.1007/978-3-662-53357-4_8 (visité le 19/08/2024).

Bibliographie II

[DW13] Christian Decker et Roger Wattenhofer. “Information propagation in the Bitcoin network”. In : IEEE P2P 2013 Proceedings. Trento, Italy : IEEE, sept. 2013, p. 1-10. isbn : 978-1-4799-0515-7. doi : 10.1109/P2P.2013.6688704. url : http://ieeexplore.ieee.org/document/6688704/ (visité le 19/08/2024).

[ES13] Ittay Eyal et Emin Gun Sirer. Majority is not Enough : Bitcoin Mining is Vulnerable. arXiv :1311.0243 [cs]. Nov. 2013. url : http://arxiv.org/abs/1311.0243 (visité le 19/08/2024).

[FLP85] Michael J. Fischer, Nancy A. Lynch et Michael S. Paterson. “Impossibility of distributed consensus with one faulty process”. In : Journal of the ACM 32.2 (avr. 1985), p. 374-382. issn : 0004-5411, 1557-735X. doi : 10.1145/3149.214121. url : https://dl.acm.org/doi/10.1145/3149.214121 (visité le 18/04/2024).

[KS11] Ajay D. Kshemkalyani et Mukesh Singhal. Distributed computing : principles, algorithms, and systems. 1. paperback edition(with corrections). Cambridge University Press, 2011. 736 p. isbn : 978-0-521-18984-2.

Bibliographie III

[LB24] Thomas Lelièvre et Quentin Bramas. “The impact of block mining time distribution on the probability of forks”. In : BRAINS ; 5th Conference on Blockchain Research & Applications for Innovative Networks and Services. Berlin, Germany, oct. 2024. url : https://hal.science/hal-04675227.

[Nak07] Satoshi Nakamoto. “Bitcoin : A Peer-to-Peer Electronic Cash System”. In : (2007). url : https://bitcoin.org/bitcoin.pdf (visité le 08/08/2024).

[Pop18] Sergei Popov. “The Tangle”. In : (2018). url : https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf.

[Sch20] Fabian Schär. “BLOCKCHAIN FORKS : A FORMAL CLASSIFICATION FRAMEWORK AND PERSISTENCY ANALYSIS”. In : The Singapore Economic Review (2020), p. 1-11. url : https://api.semanticscholar.org/CorpusID:225355815.

Université de Strasbourg

Merci de votre attention. Questions ?