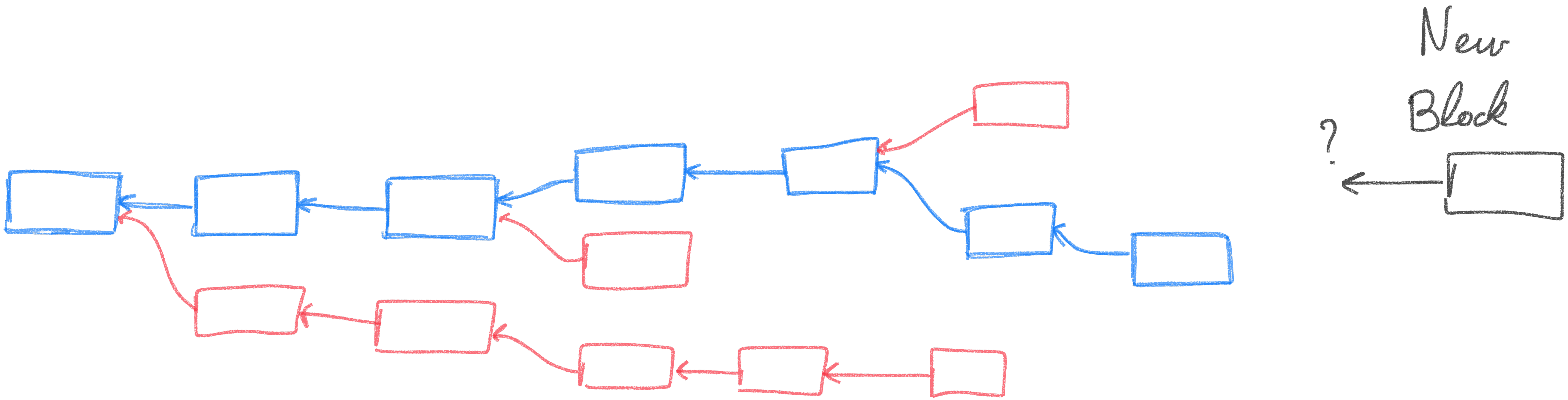
Maximiser un sous-DAG sans conflit

Quentin Bramas
ICUBE, University of Strasbourg

ANR-22-CE25-0012

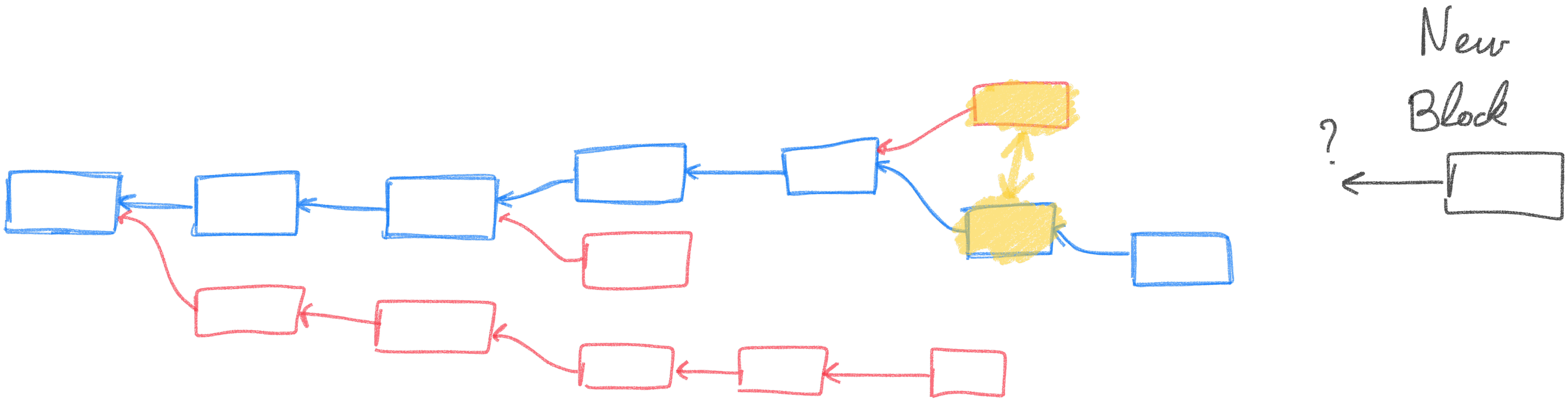
Contexte

État Courant = le parent choisi pour un nouveau block

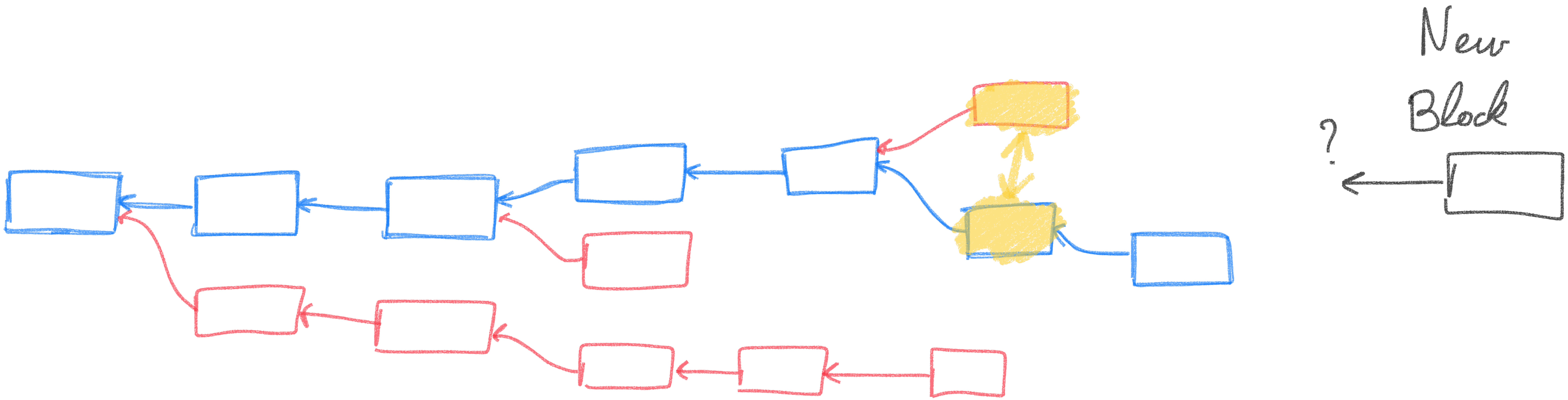


= branche la plus lourde

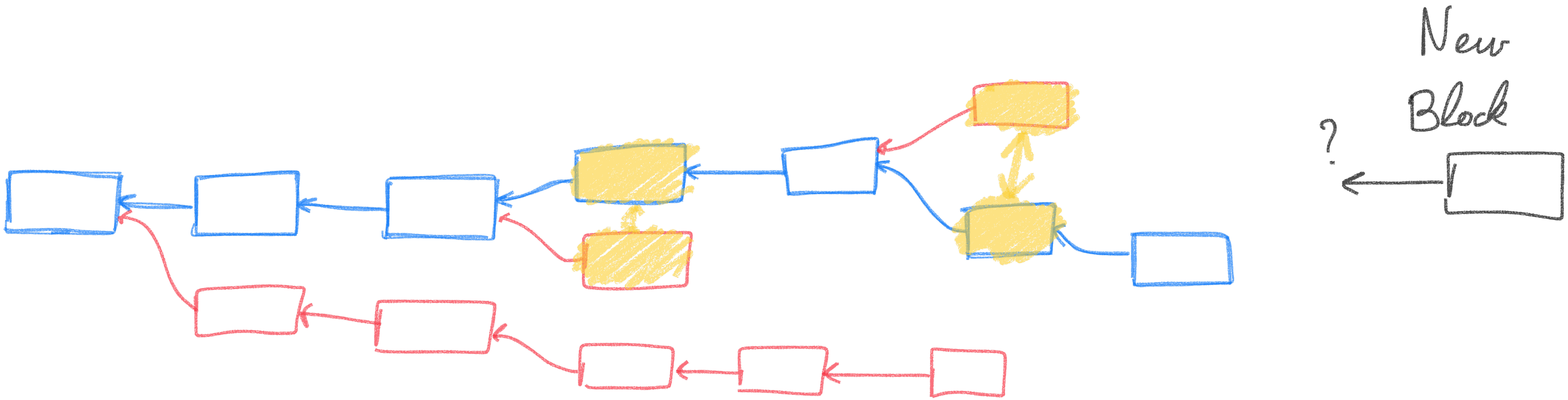
Résoudre les Conflits dans une Blockchains



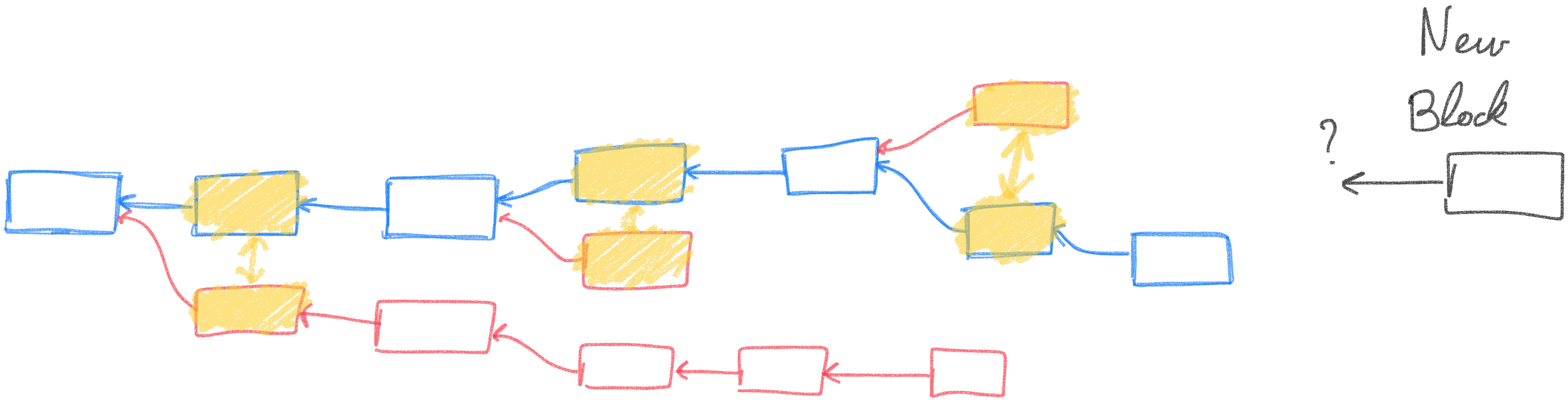
Résoudre les Conflits dans une Blockchains



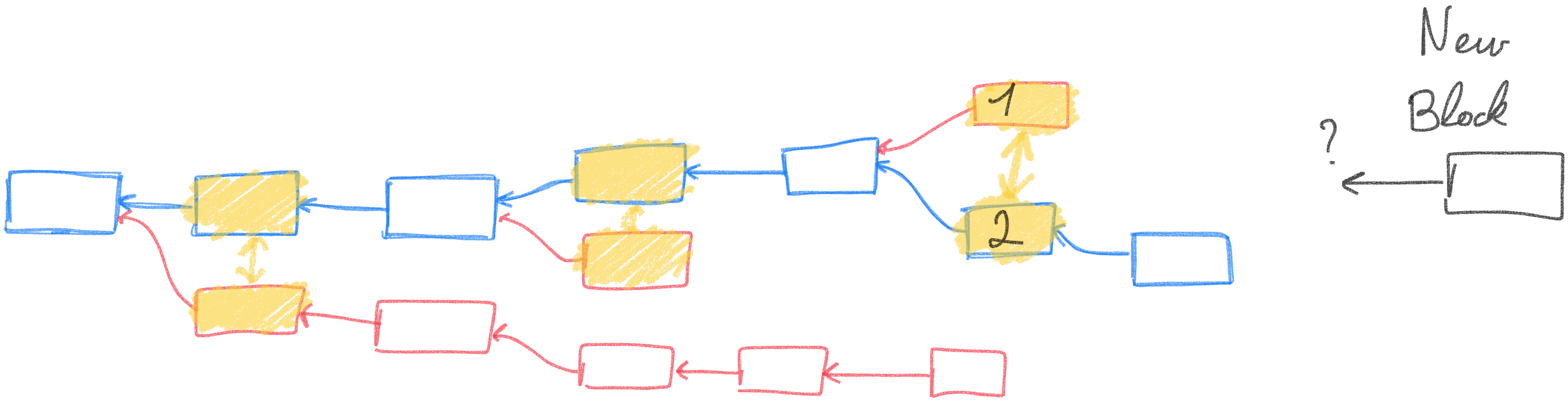
Résoudre les Conflits dans une Blockchains



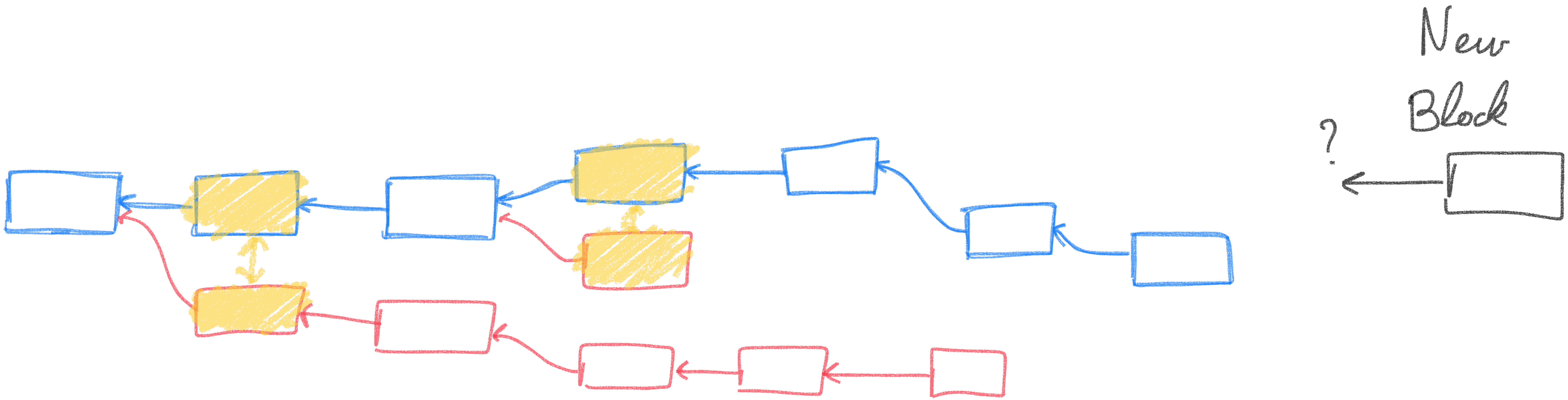
Résoudre les Conflits dans une Blockchains



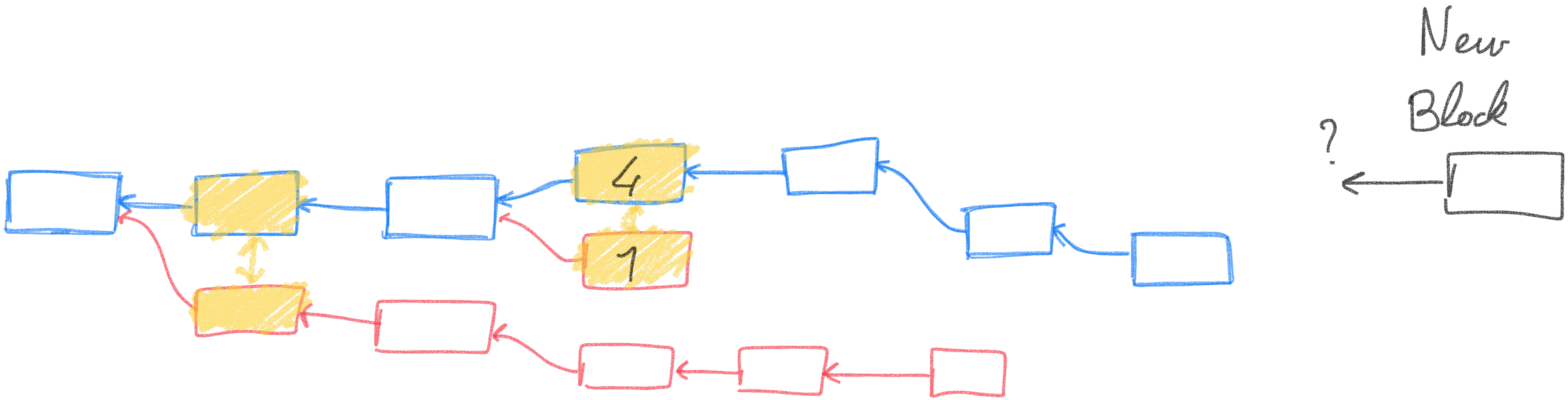
Résoudre les Conflits dans une Blockchains



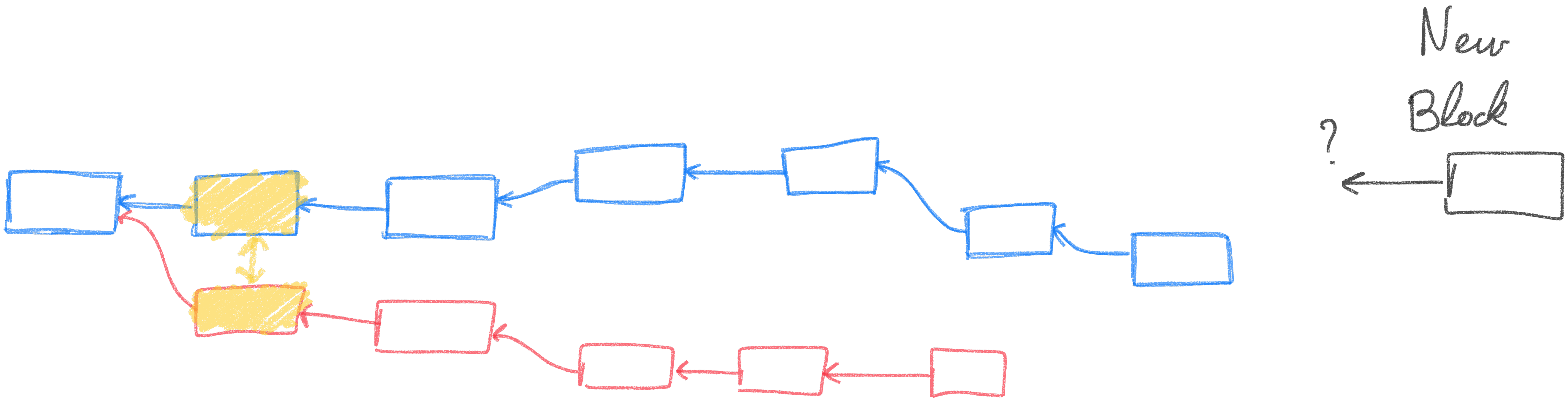
Résoudre les Conflits dans une Blockchains



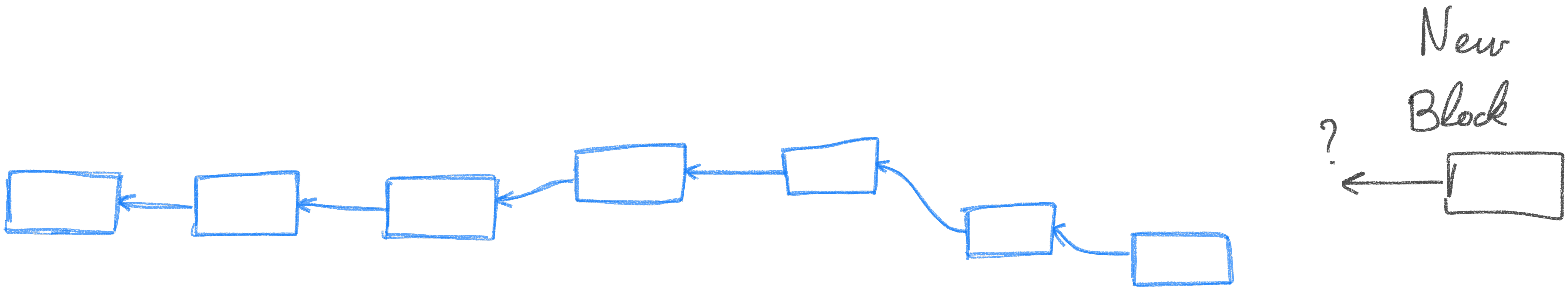
Résoudre les Conflits dans une Blockchains



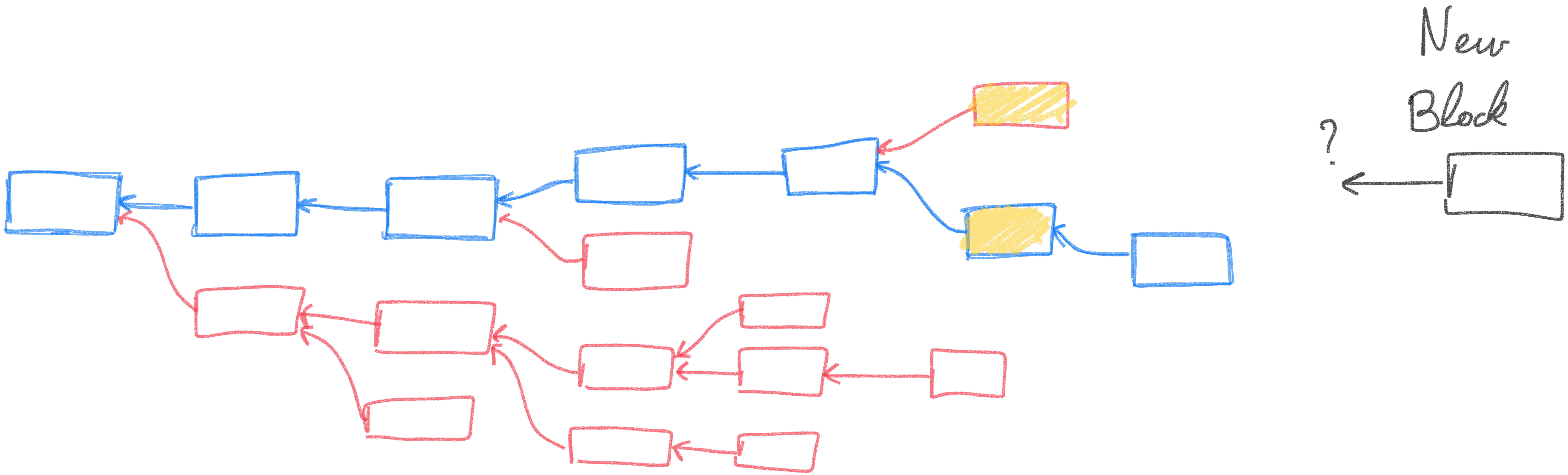
Résoudre les Conflits dans une Blockchains



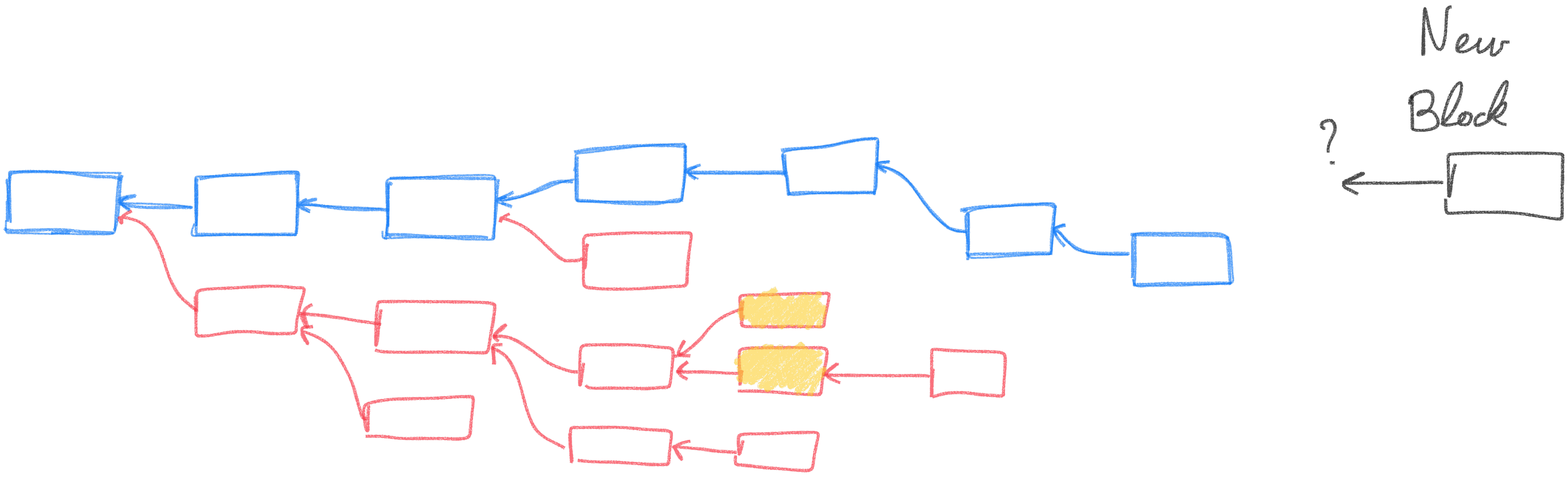
Résoudre les Conflits dans une Blockchains



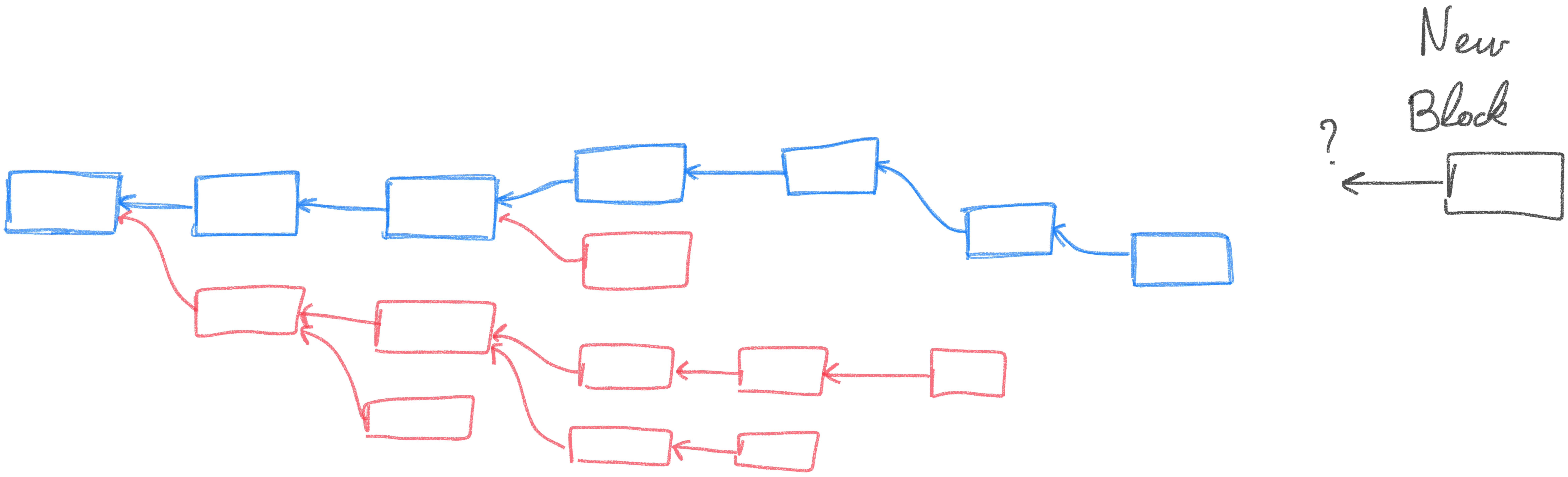
Résoudre les Conflits dans une Blockchains



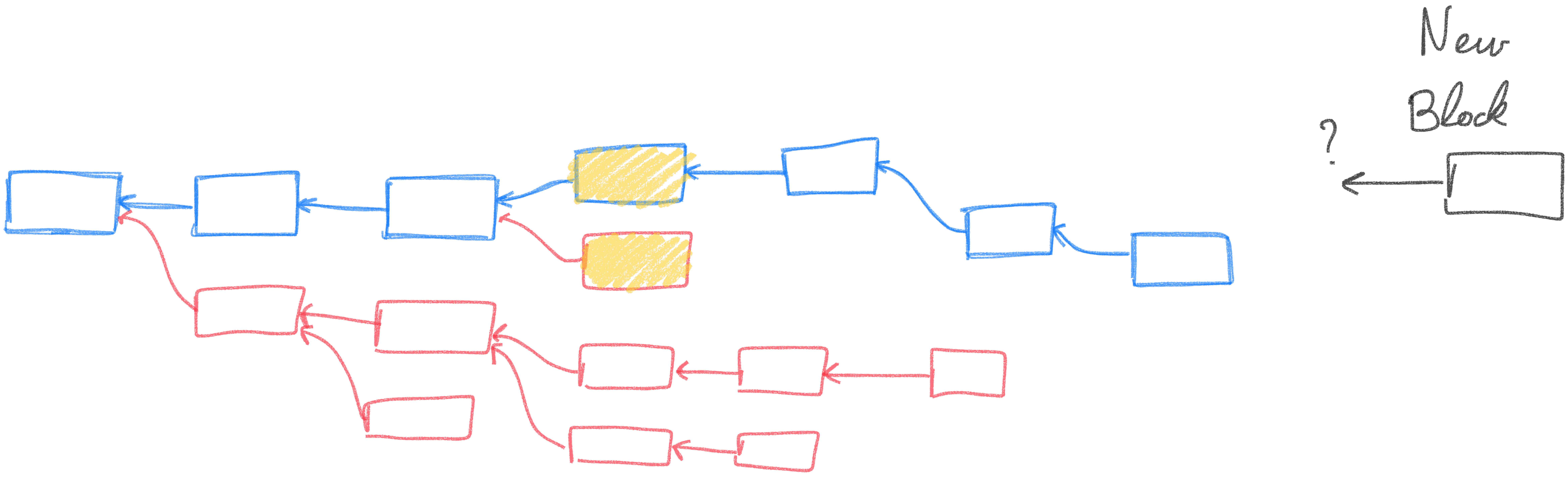
Résoudre les Conflits dans une Blockchains



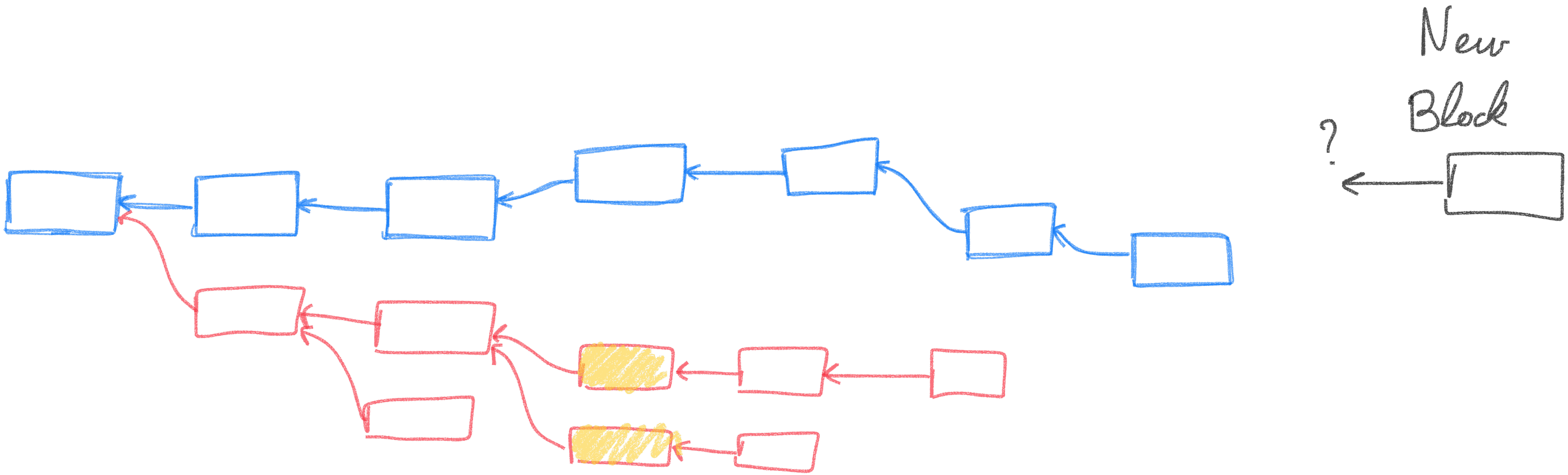
Résoudre les Conflits dans une Blockchains



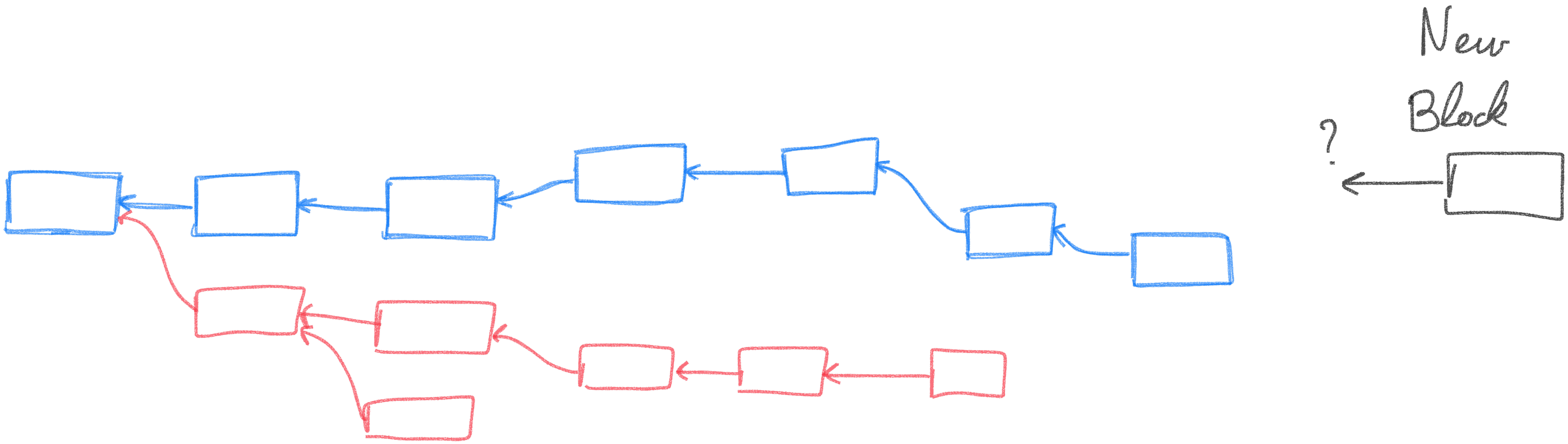
Résoudre les Conflits dans une Blockchains



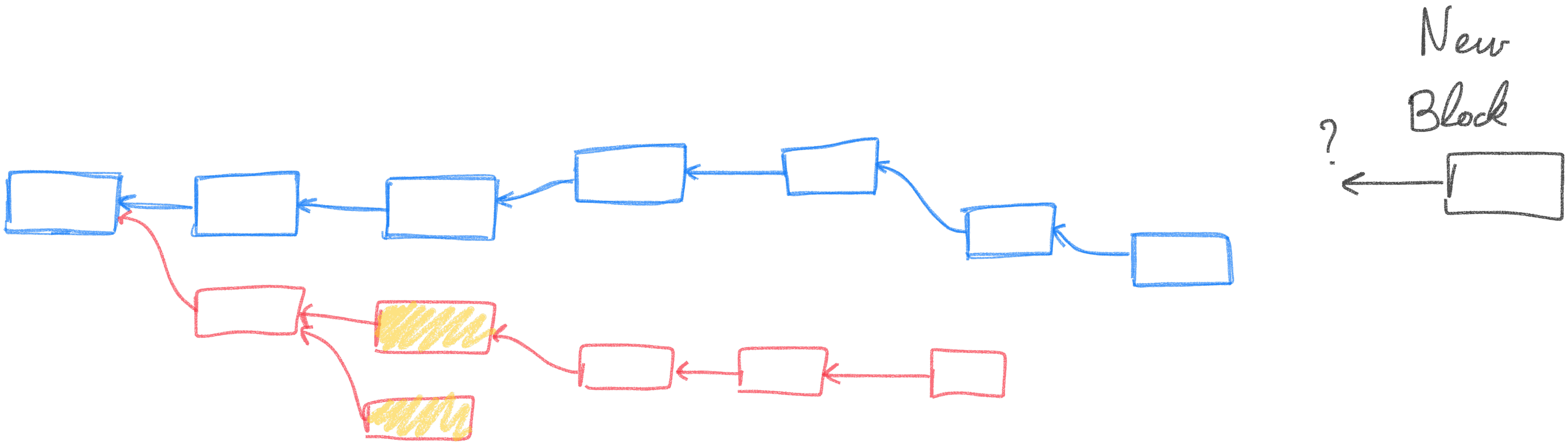
Résoudre les Conflits dans une Blockchains



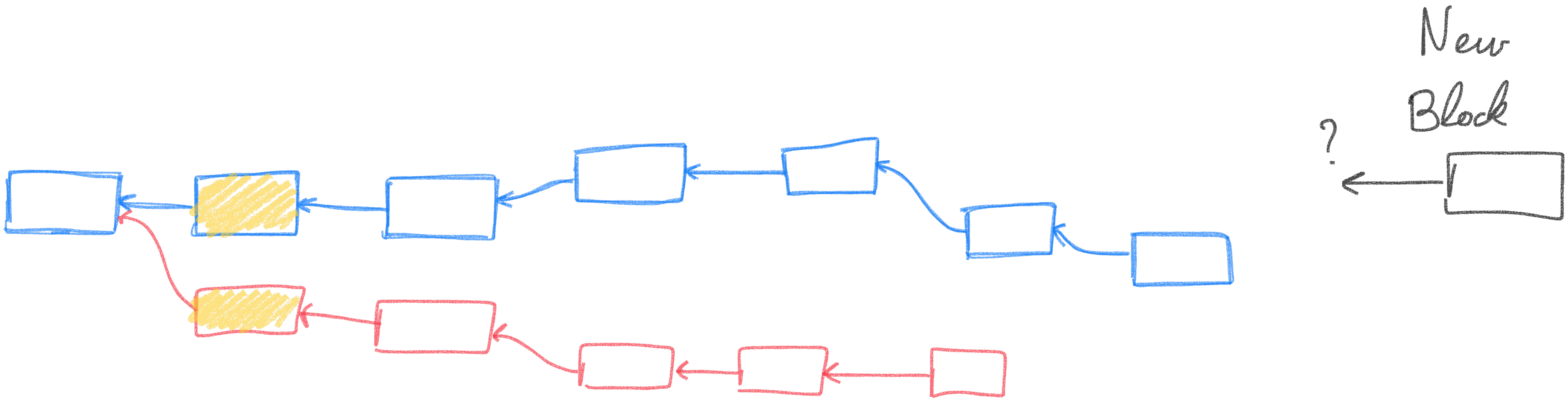
Résoudre les Conflits dans une Blockchains



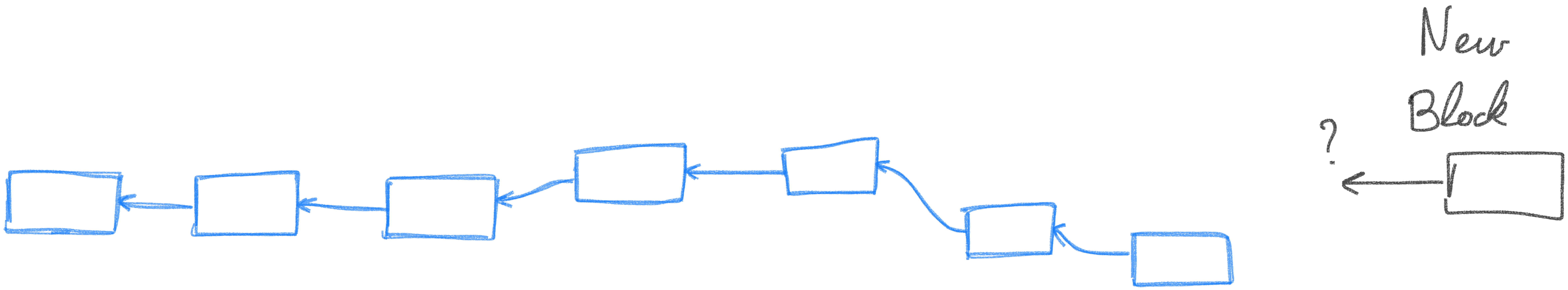
Résoudre les Conflits dans une Blockchains



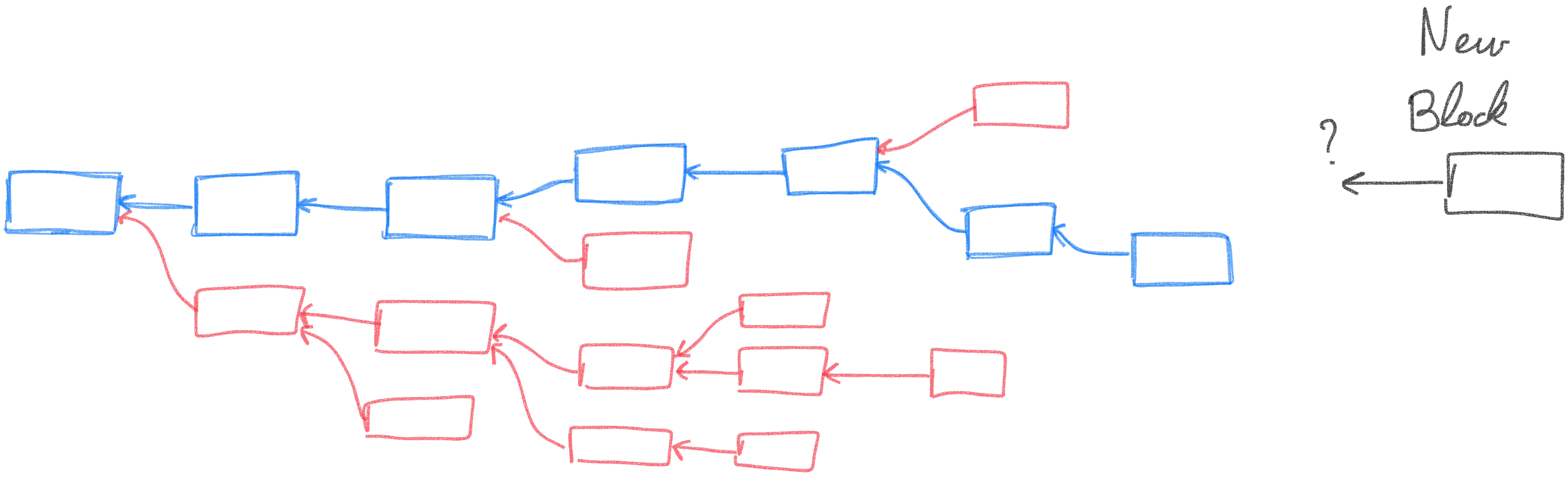
Résoudre les Conflits dans une Blockchains



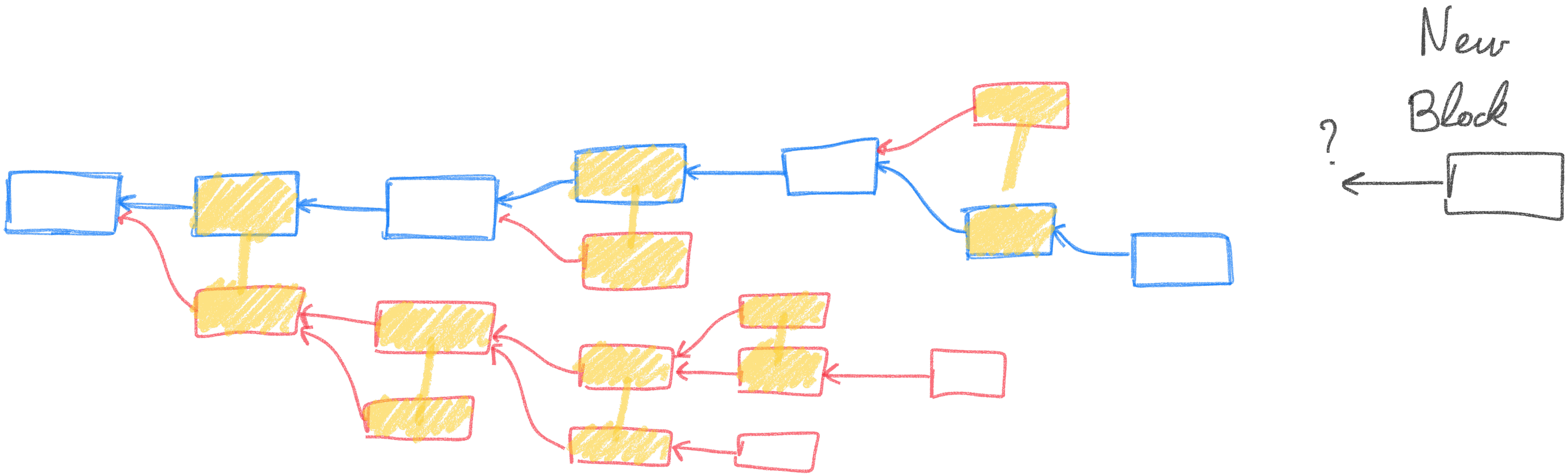
Résoudre les Conflits dans une Blockchains



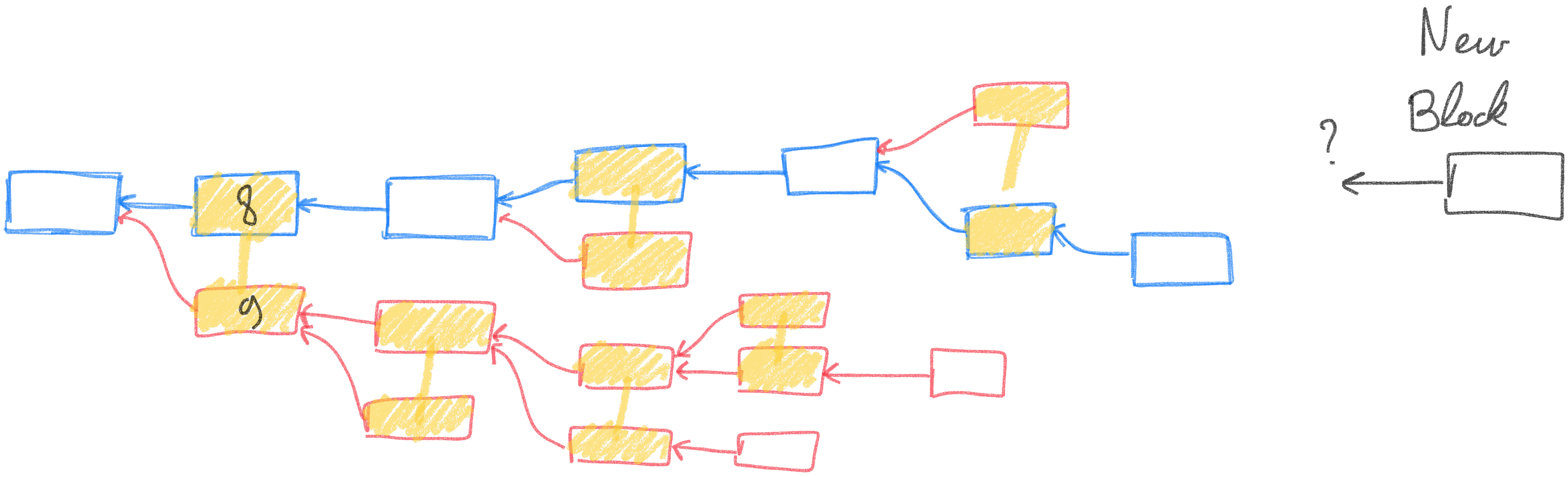
Résoudre les Conflits dans une Blockchains



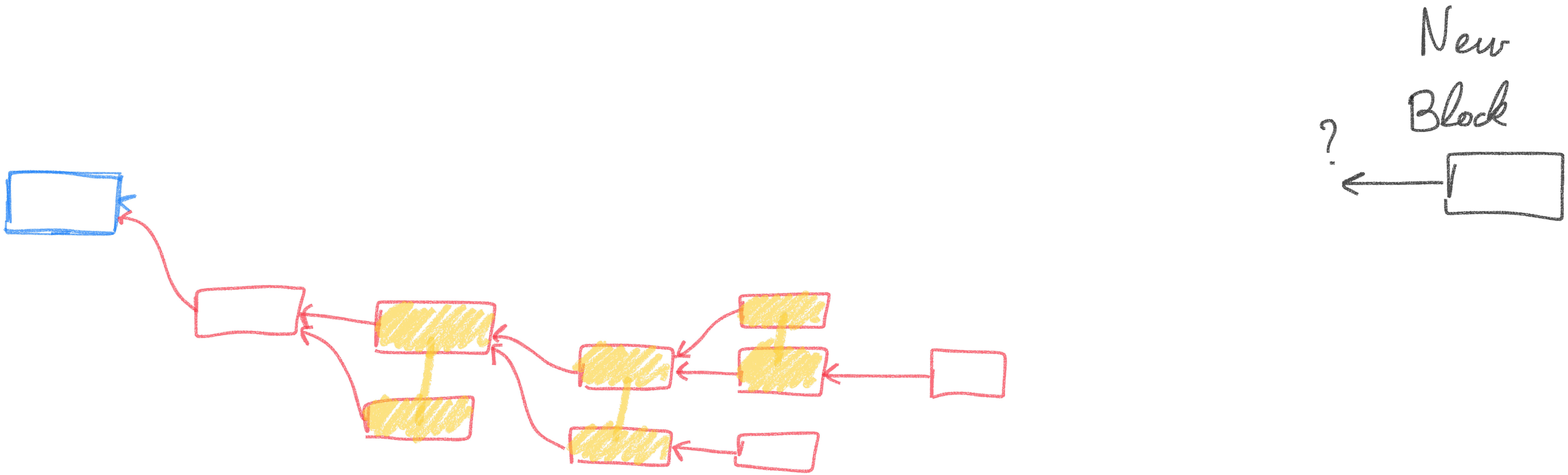
Résoudre les Conflits dans une Blockchains



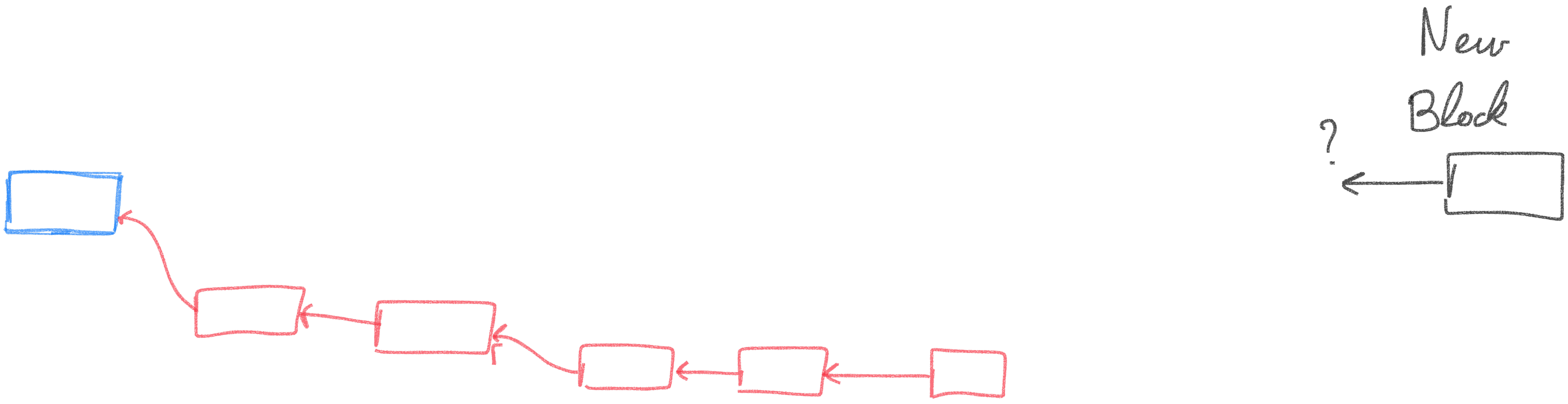
Résoudre les Conflits dans une Blockchains



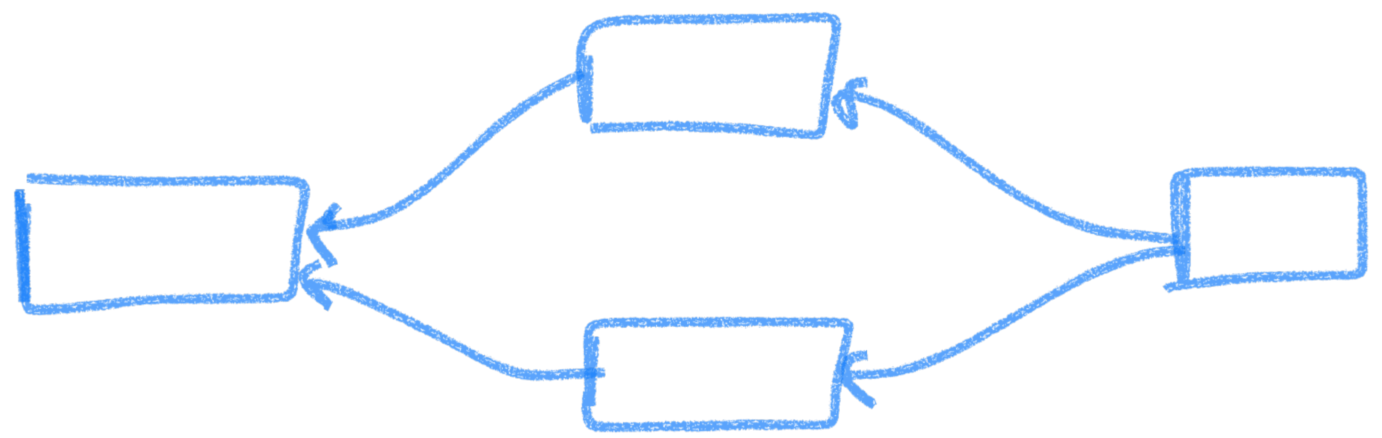
Résoudre les Conflits dans une Blockchains



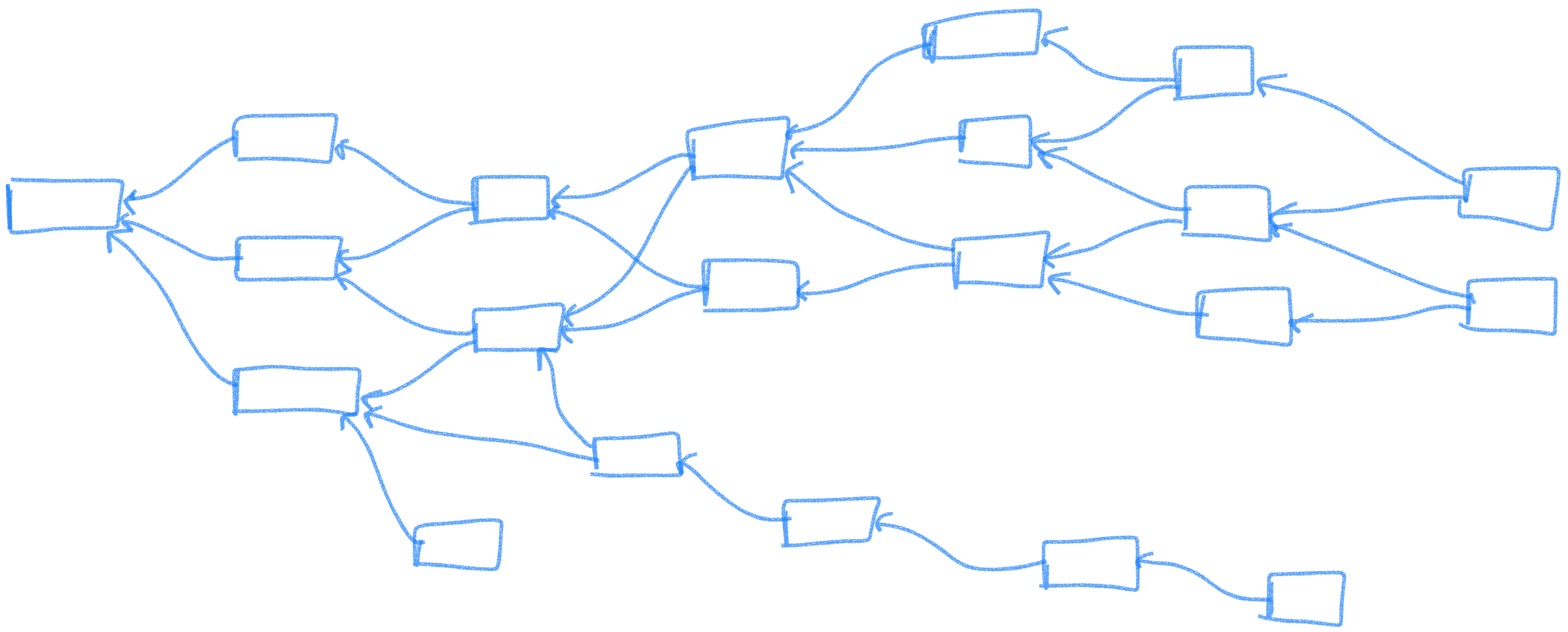
Résoudre les Conflits dans une Blockchains



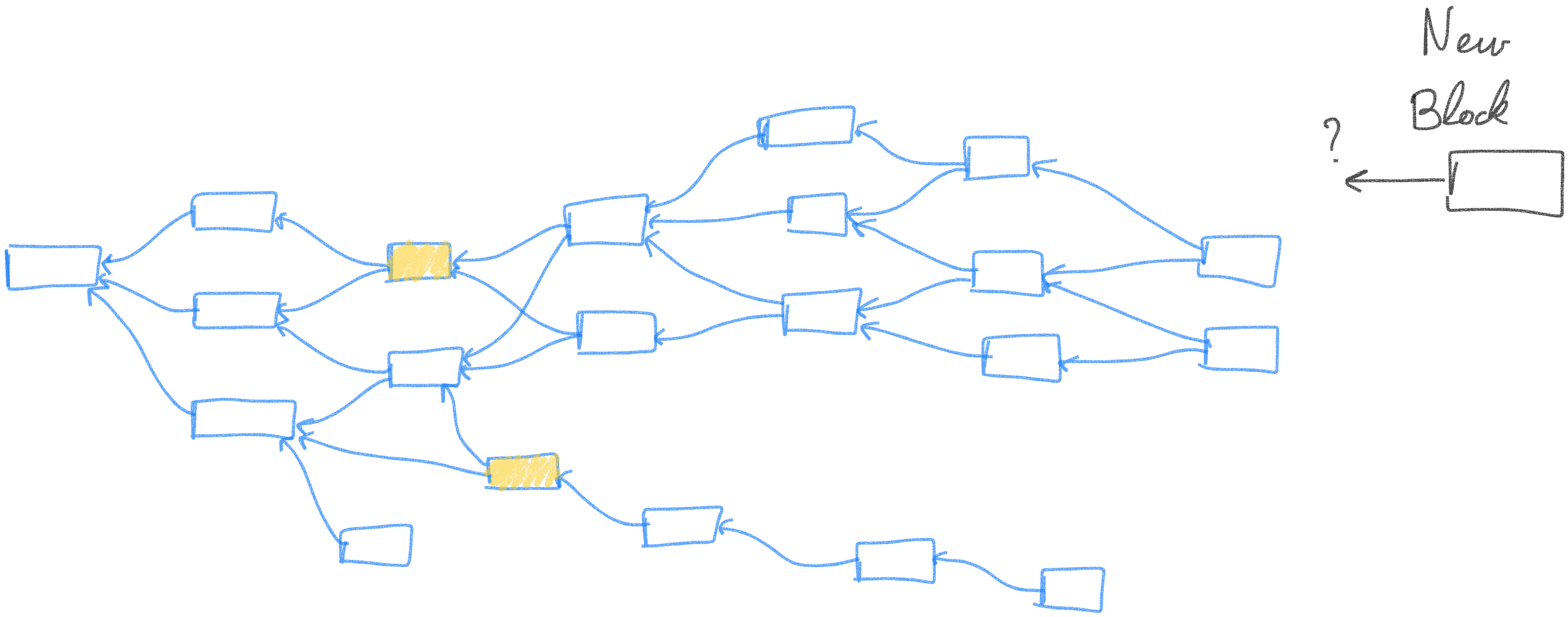
Résoudre les conflits dans un BlockDAG



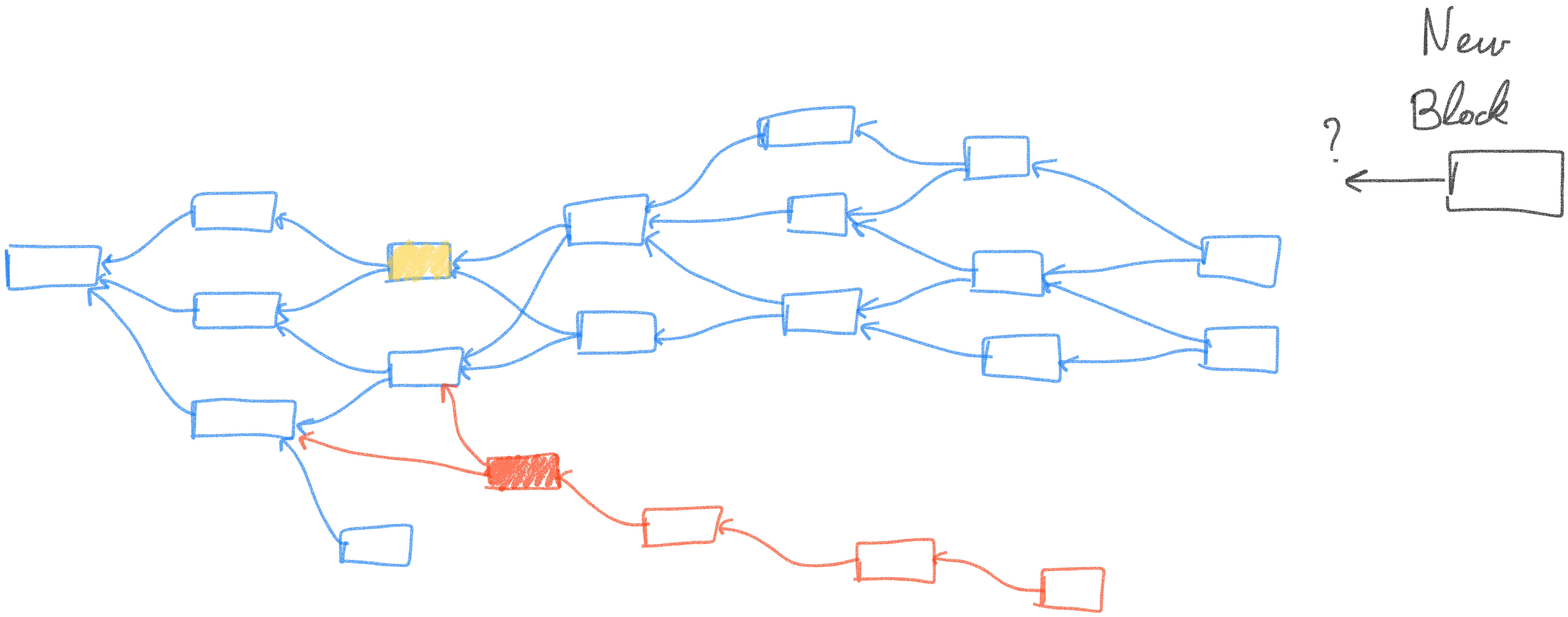
Résoudre les conflits dans un BlockDAG



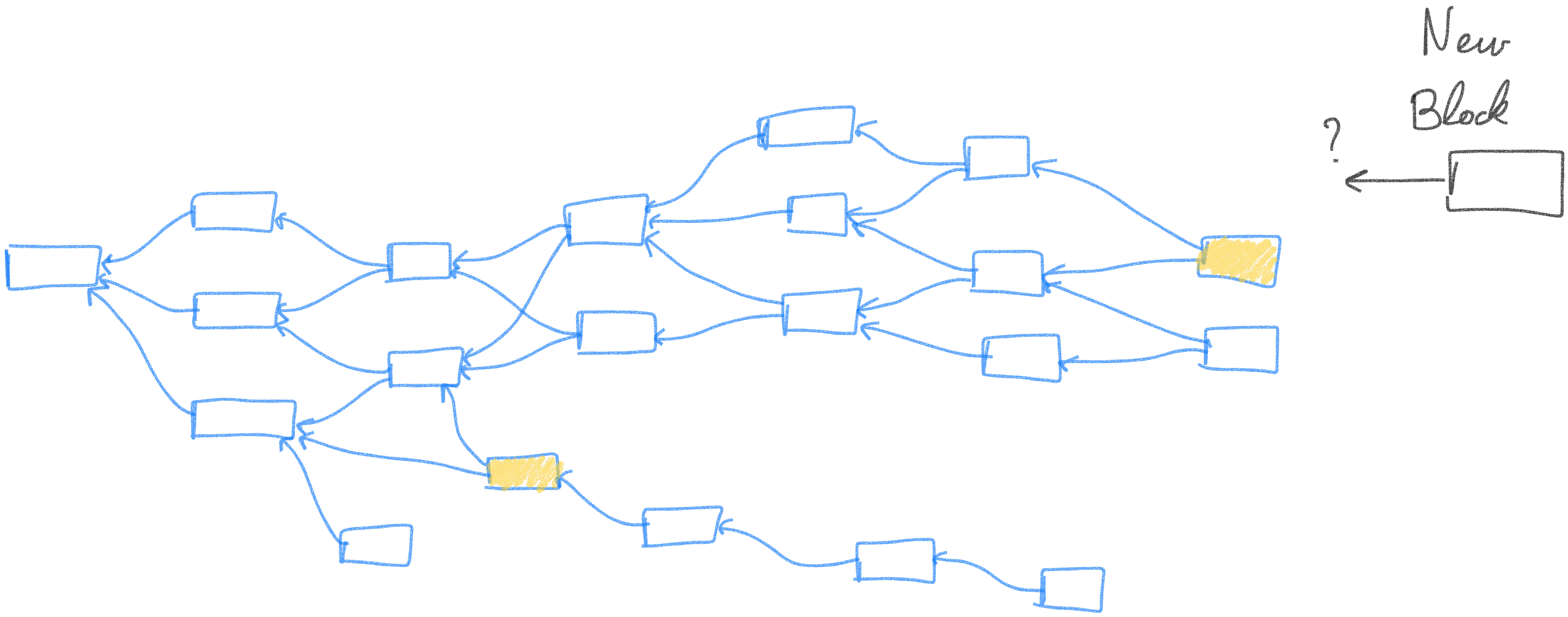
Résoudre les conflits dans un BlockDAG



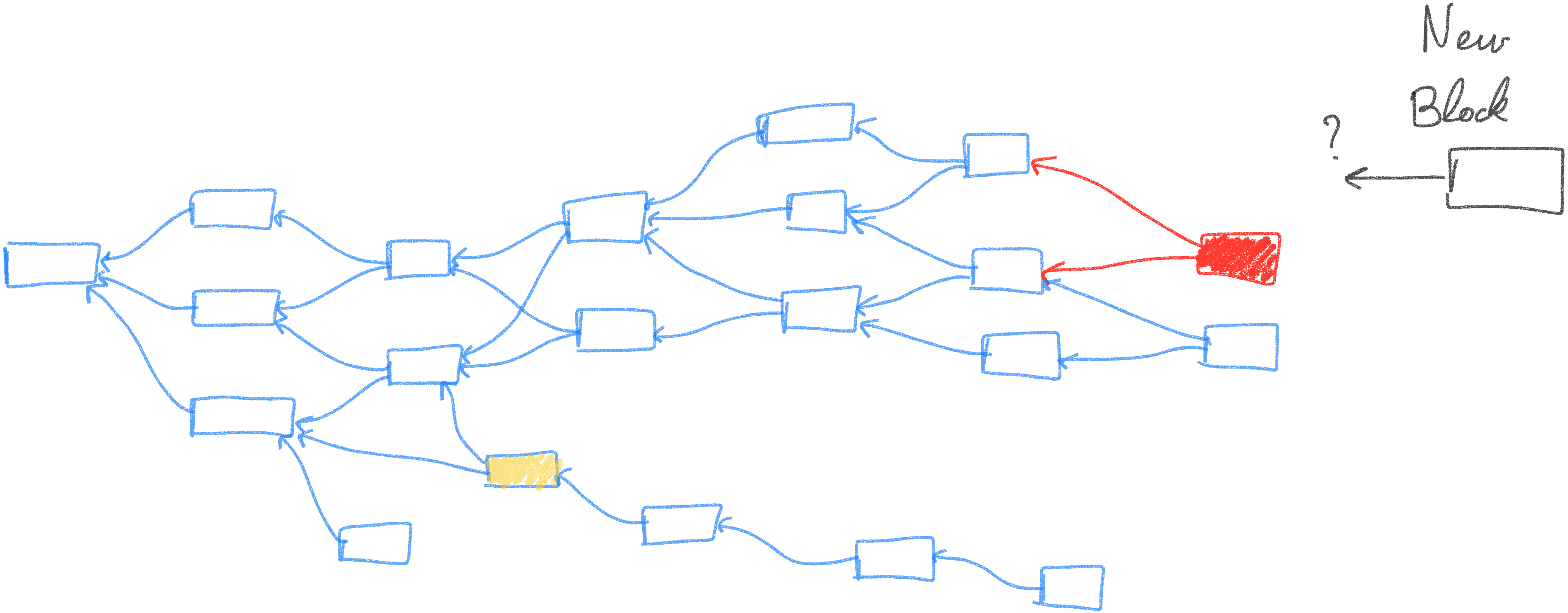
Résoudre les conflits dans un BlockDAG



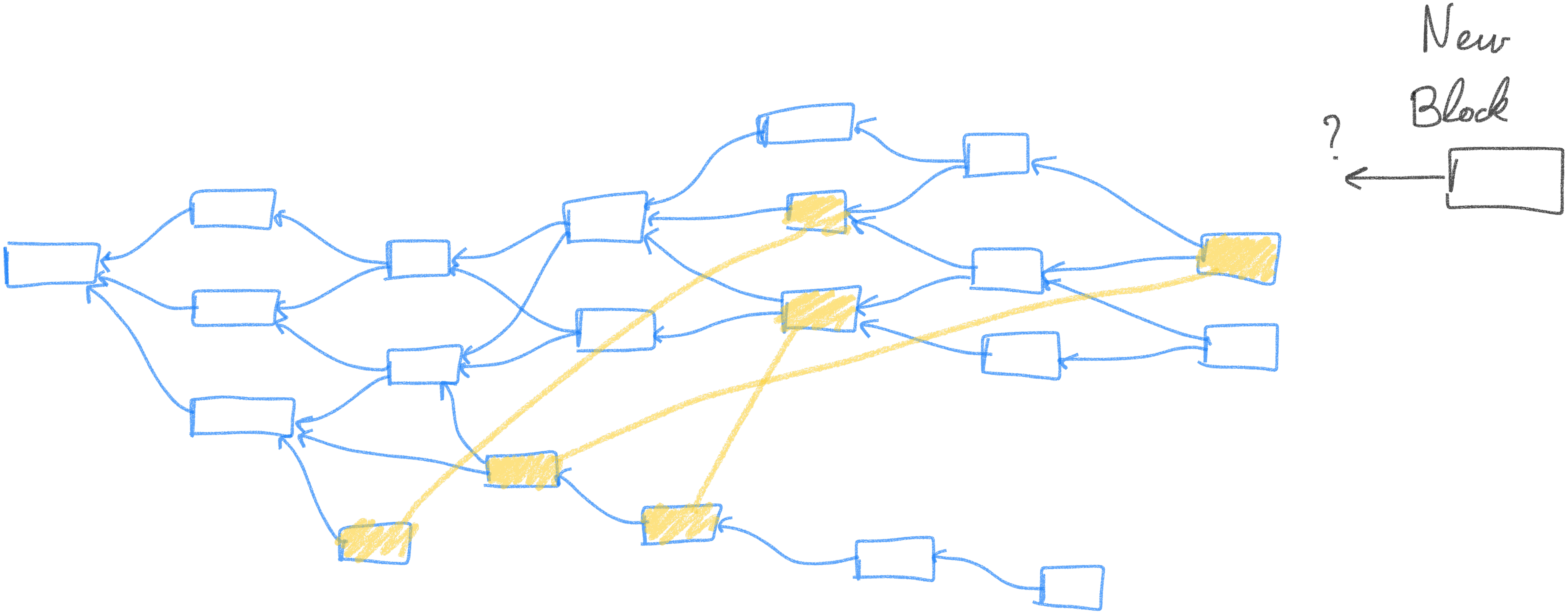
Résoudre les conflits dans un BlockDAG



Résoudre les conflits dans un BlockDAG



Problème: résoudre les conflits?



État de l'art

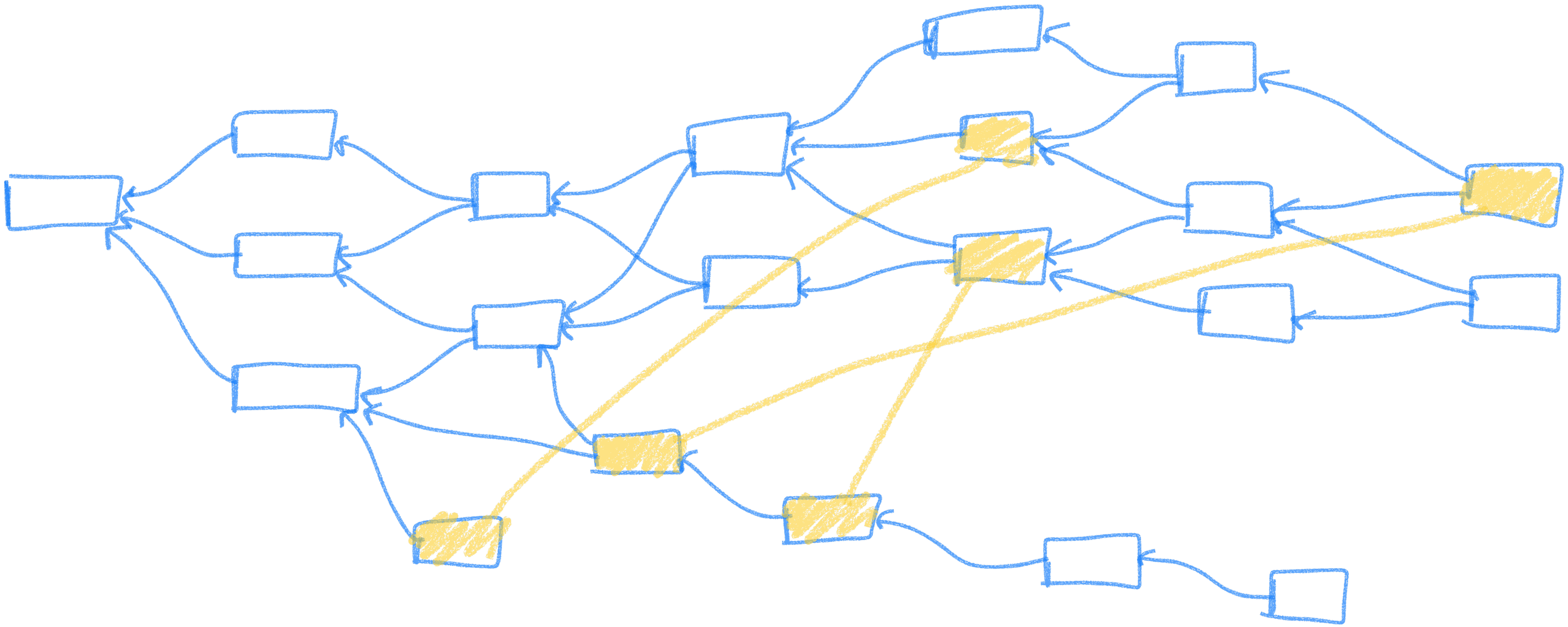
IOTA Tangle (v1) : randomisé, utilisant le poids des noeuds

GHOSTDAG : choisit un sous-DAG avec une « petite » largeur (k-cluster)

Autres protocoles utilisant PoS ou mécanismes de vote

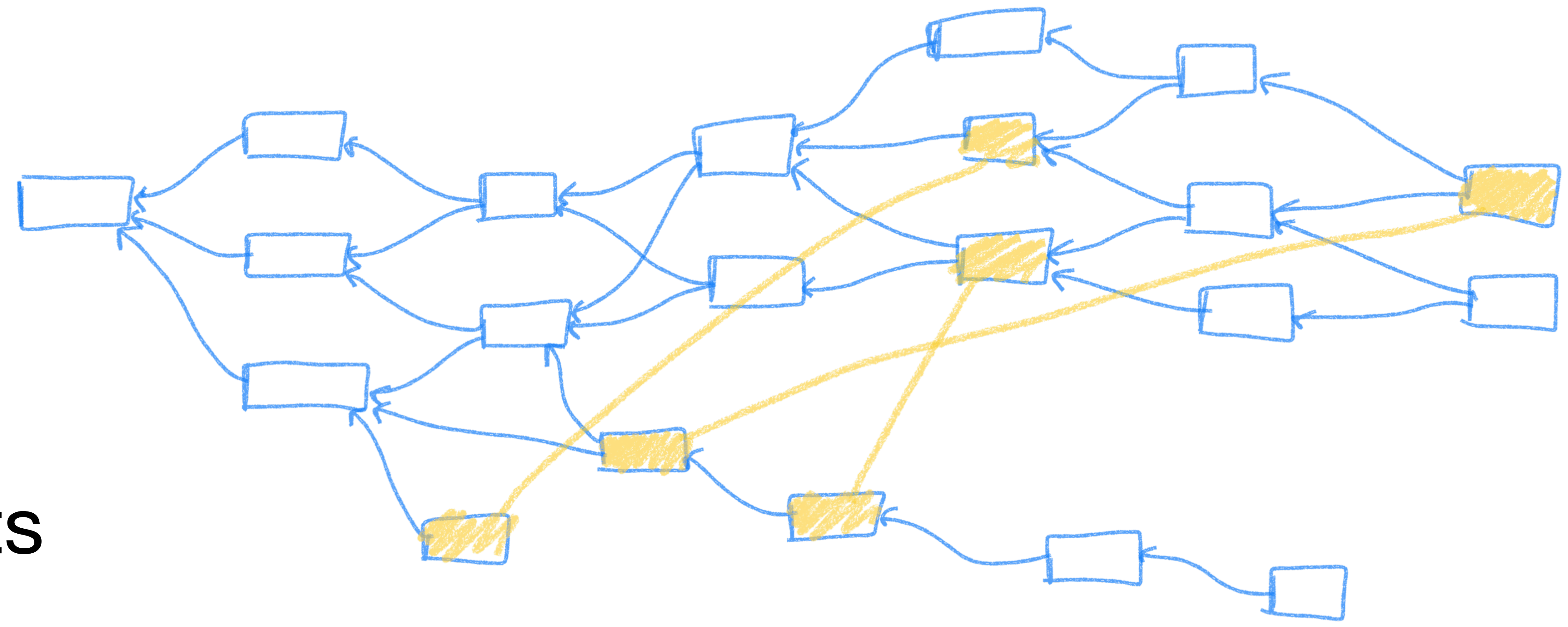
Sompolinsky, Yonatan, Shai Wyborski, and Aviv Zohar. "PHANTOM GHOSTDAG: a scalable generalization of Nakamoto consensus: September 2, 2021." Proceedings of the 3rd ACM Conference on Advances in Financial Technologies. 2021.

sous-DAG le plus lourd



sous-DAG le plus lourd

Étant donnés :



- Un BlockDAG G
- Un ensemble $Conflicts$ de conflits

On veut :

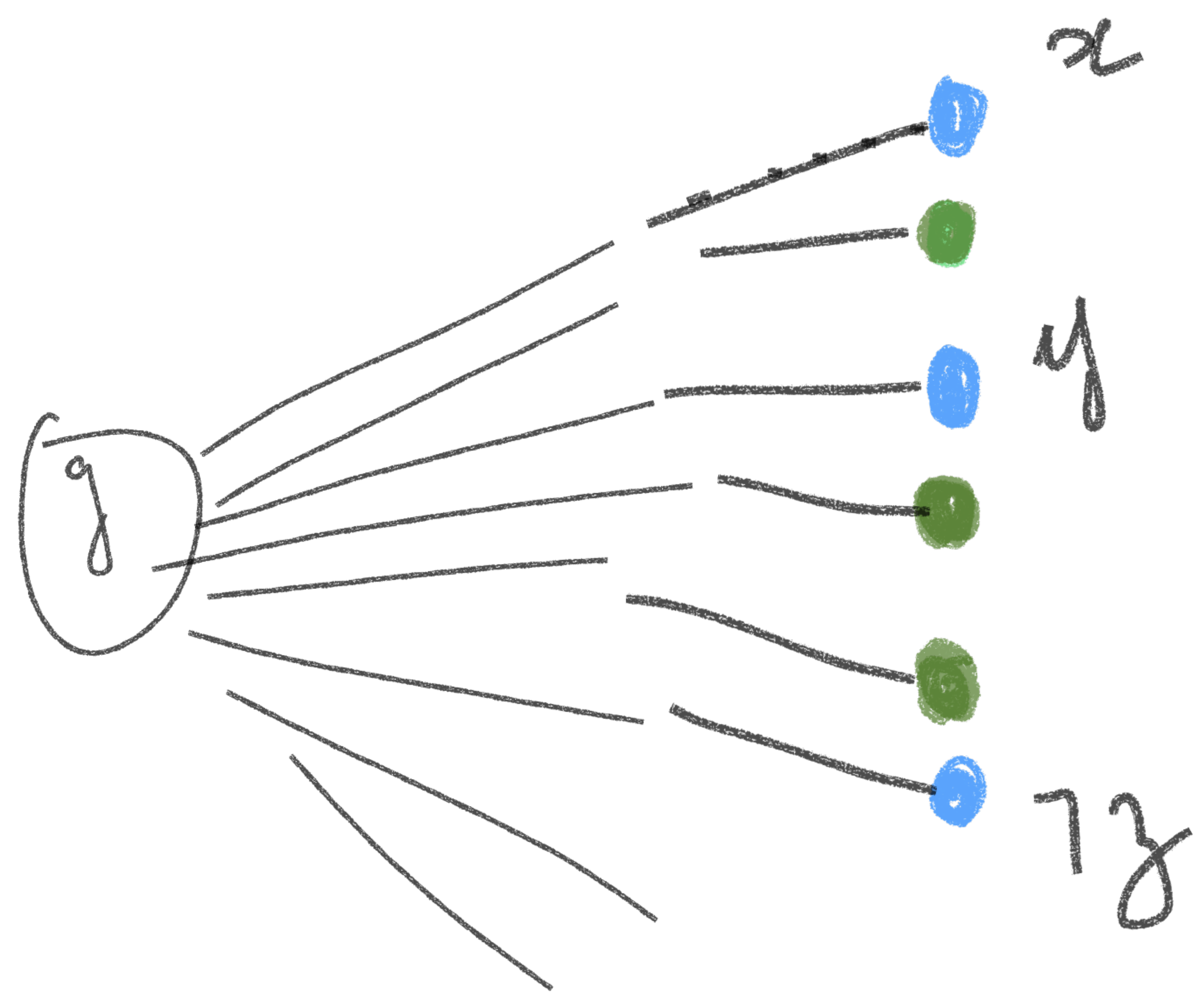
- Le sous-DAG S le plus lourd sans conflit

sous-DAG le plus lourd

Théorème : NP-complet

Preuve : depuis 3-SAT

Clause $C : x \vee y \vee \neg z$

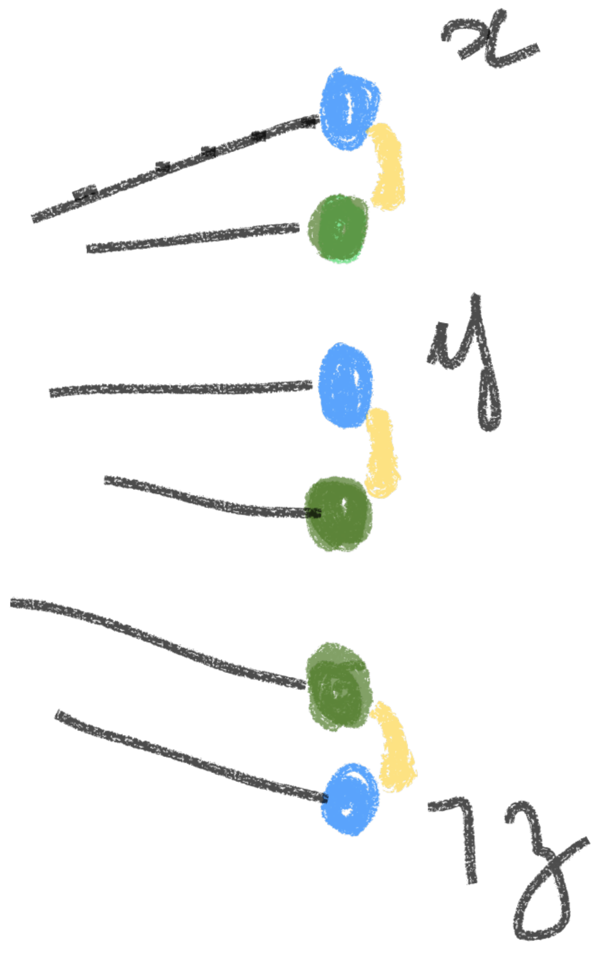


sous-DAG le plus lourd

Théorème : NP-complet

Preuve : depuis 3-SAT

Clause $C : x \vee y \vee \neg z$

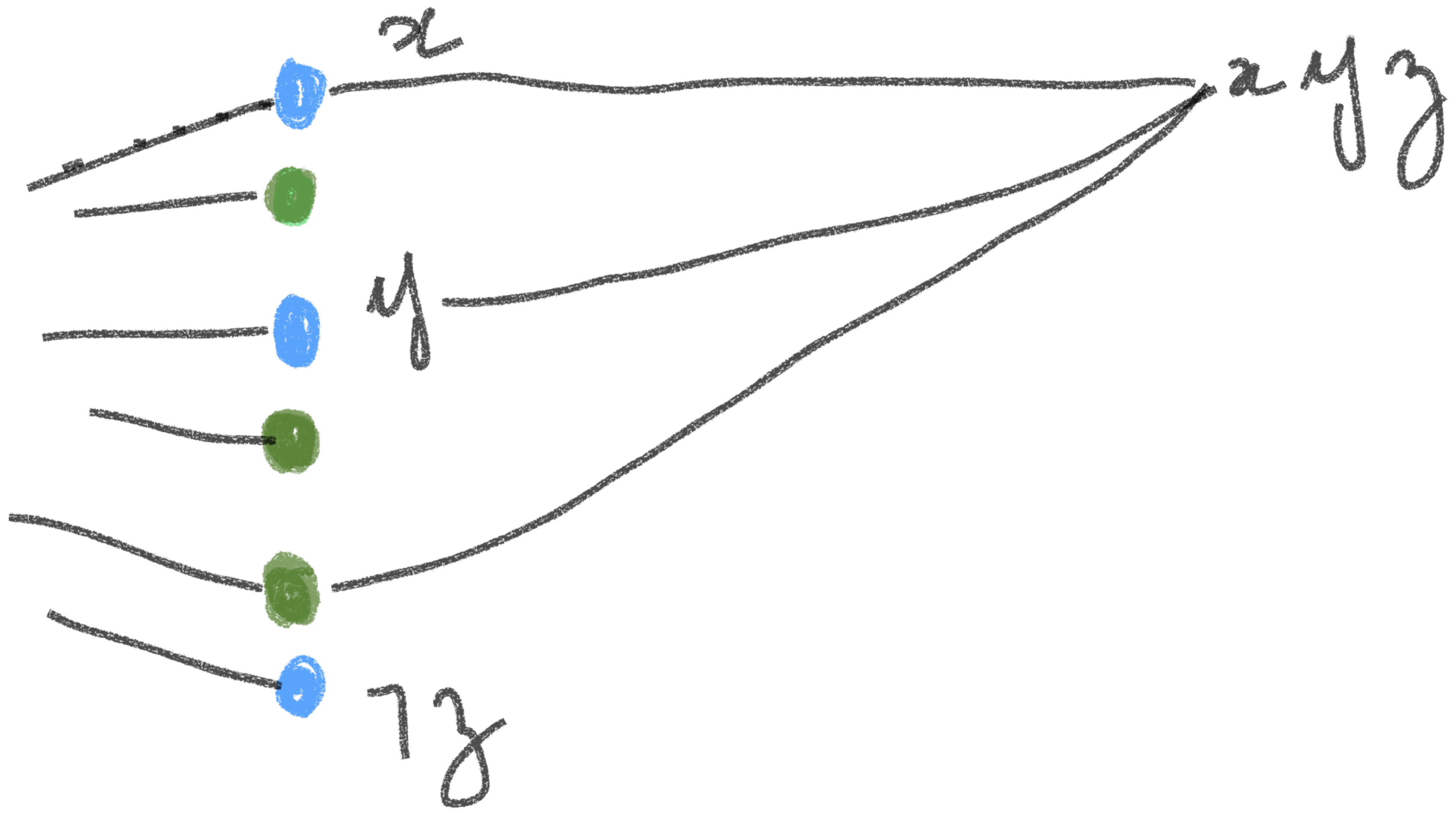


sous-DAG le plus lourd

Théorème : NP-complet

Preuve : depuis 3-SAT

Clause $C : x \vee y \vee \neg z$

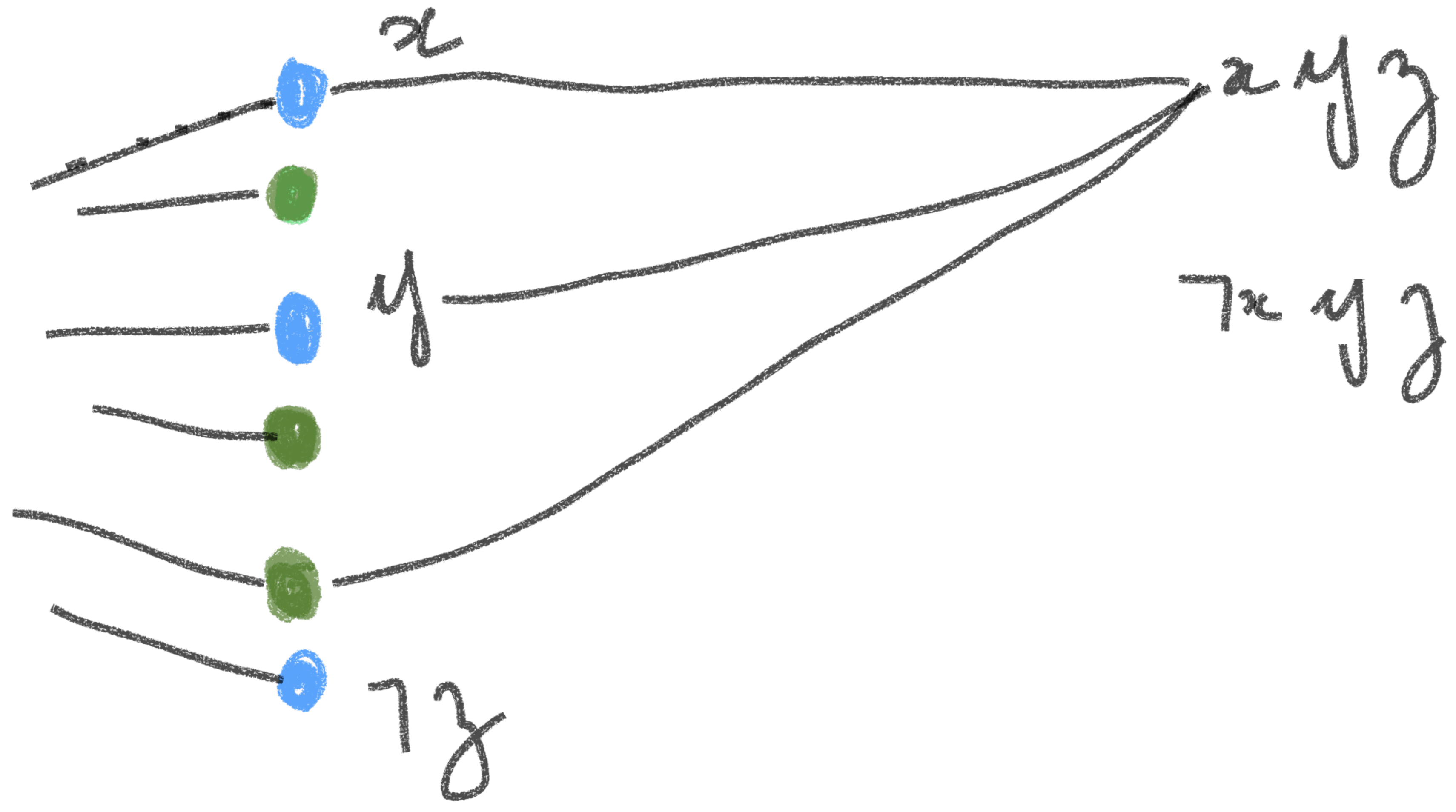


sous-DAG le plus lourd

Théorème : NP-complet

Preuve : depuis 3-SAT

Clause $C : x \vee y \vee \neg z$

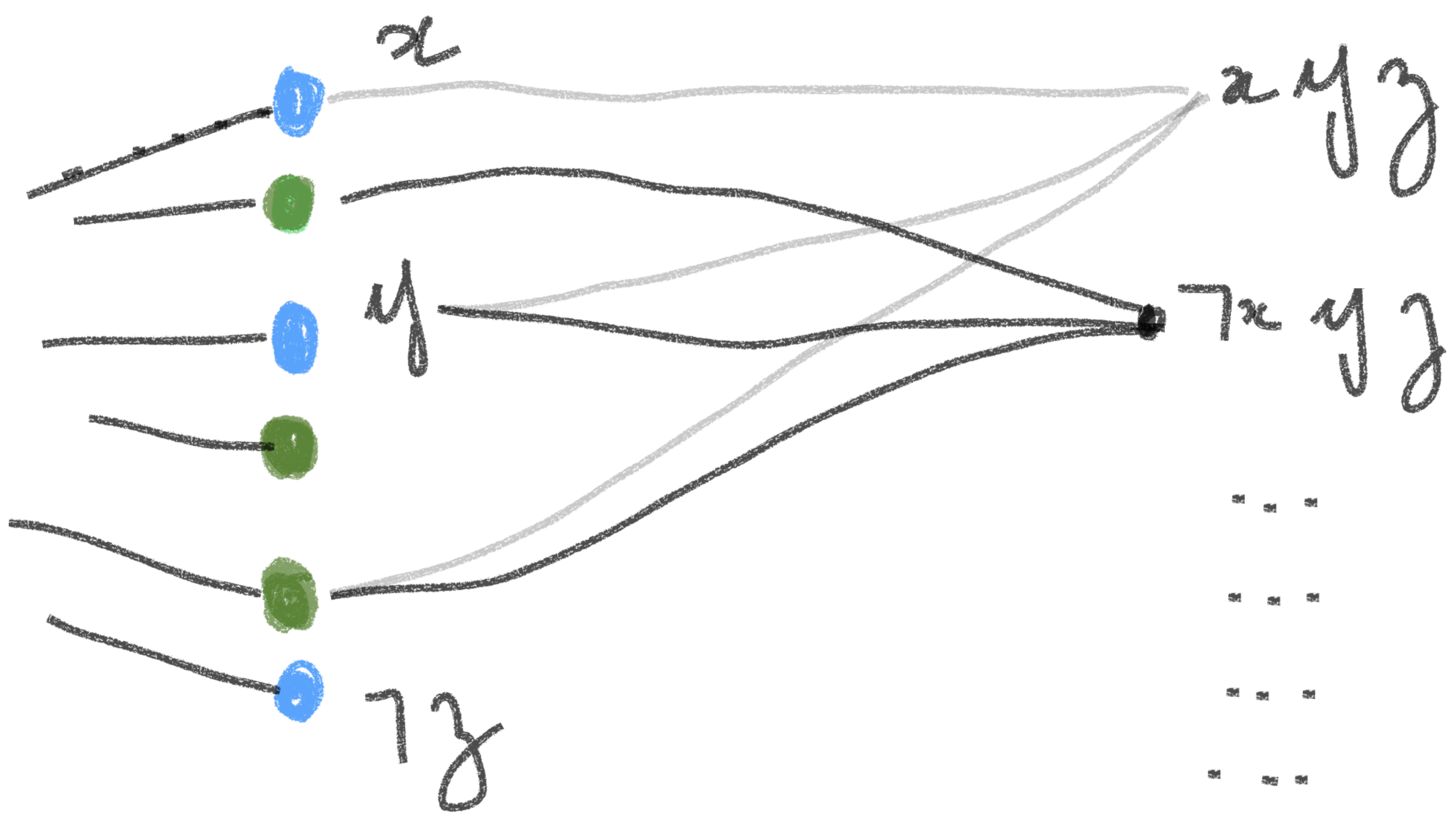


sous-DAG le plus lourd

Théorème : NP-complet

Preuve : depuis 3-SAT

Clause $C : x \vee y \vee \neg z$

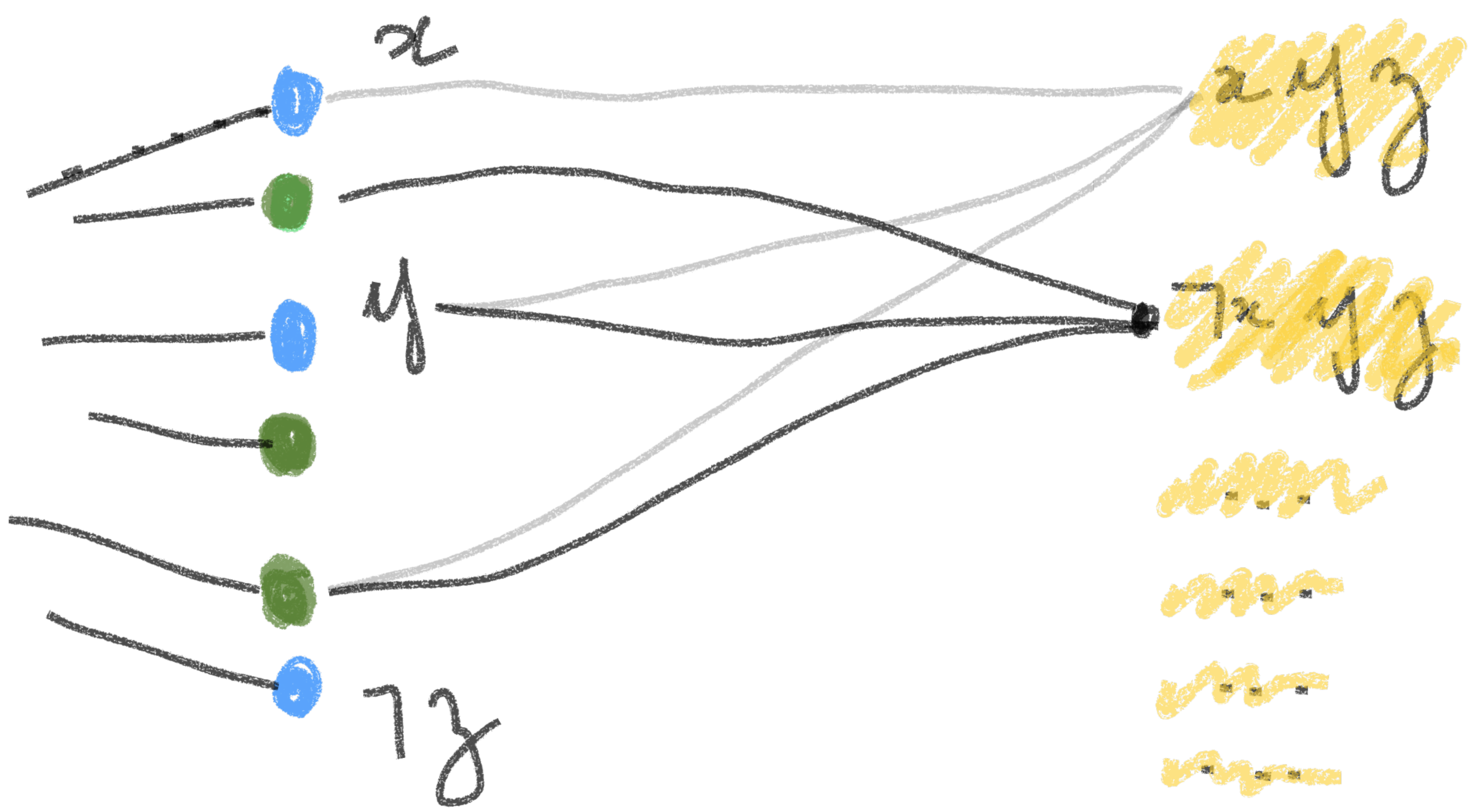


sous-DAG le plus lourd

Théorème : NP-complet

Preuve : depuis 3-SAT

Clause $C : x \vee y \vee \neg z$

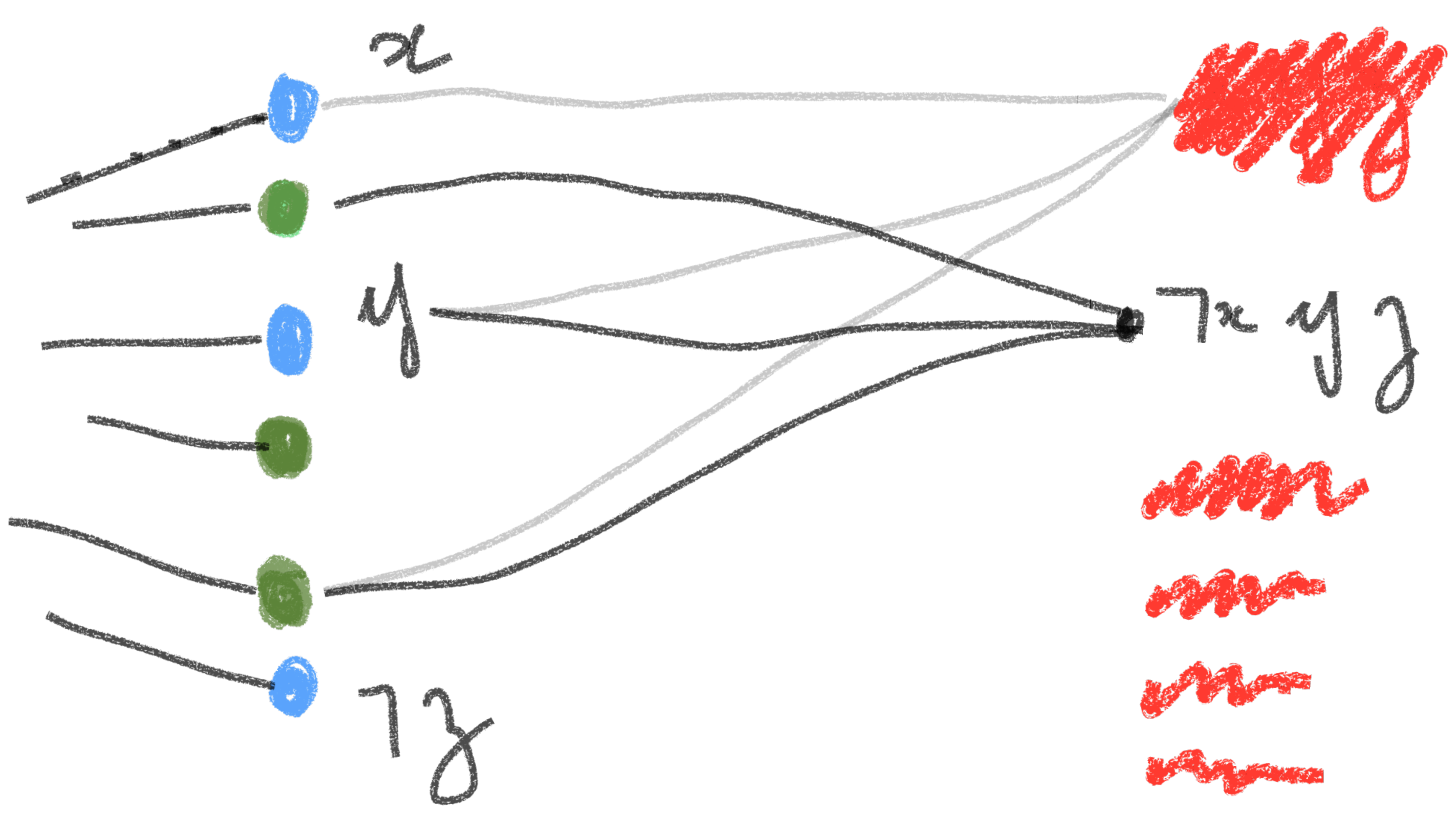


sous-DAG le plus lourd

Théorème : NP-complet

Preuve : depuis 3-SAT

Clause C : $x \vee y \vee \neg z$

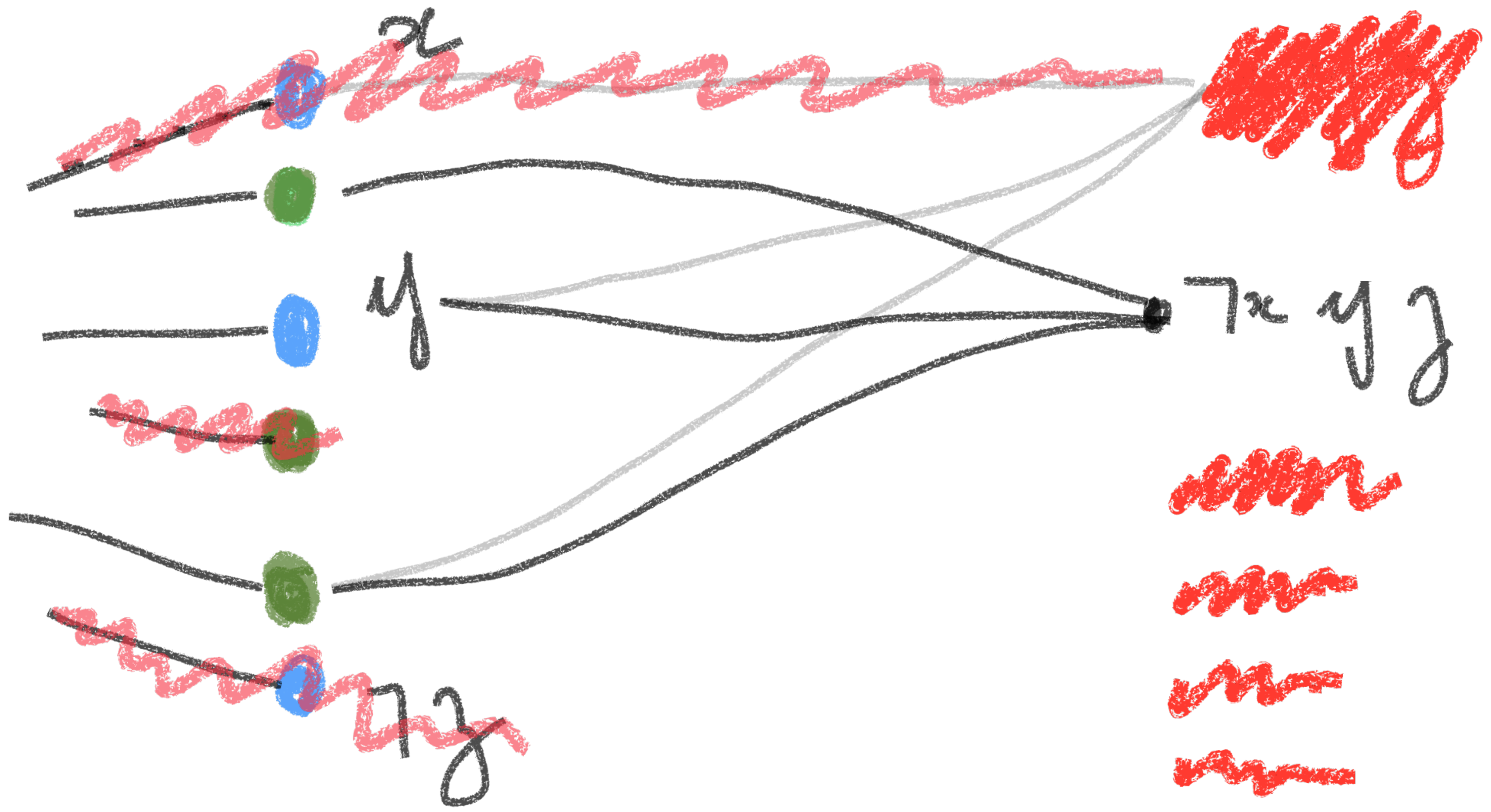


sous-DAG le plus lourd

Théorème : NP-complet

Preuve : depuis 3-SAT

Clause $C : x \vee y \vee \neg z$

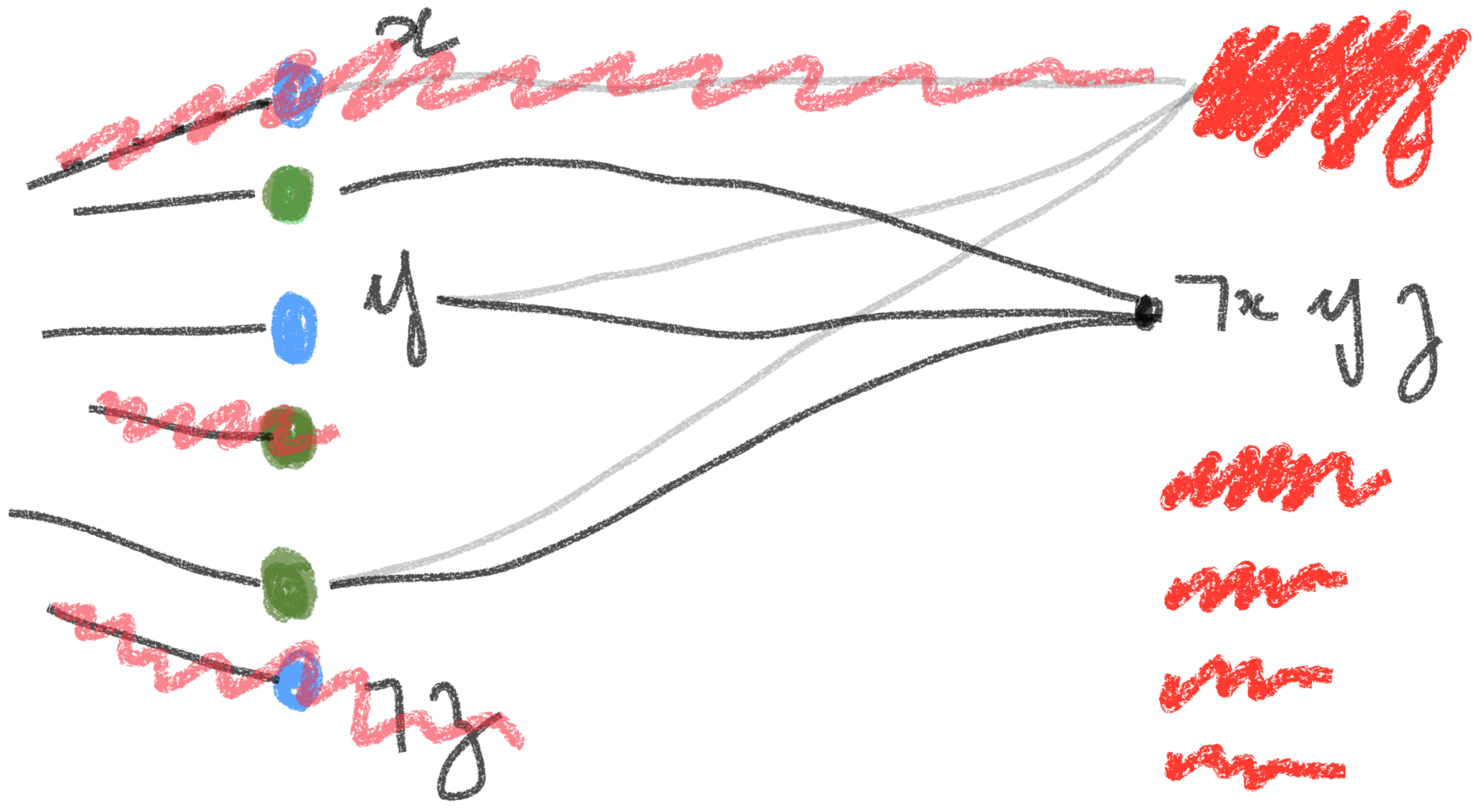


sous-DAG le plus lourd

Théorème : NP-complet

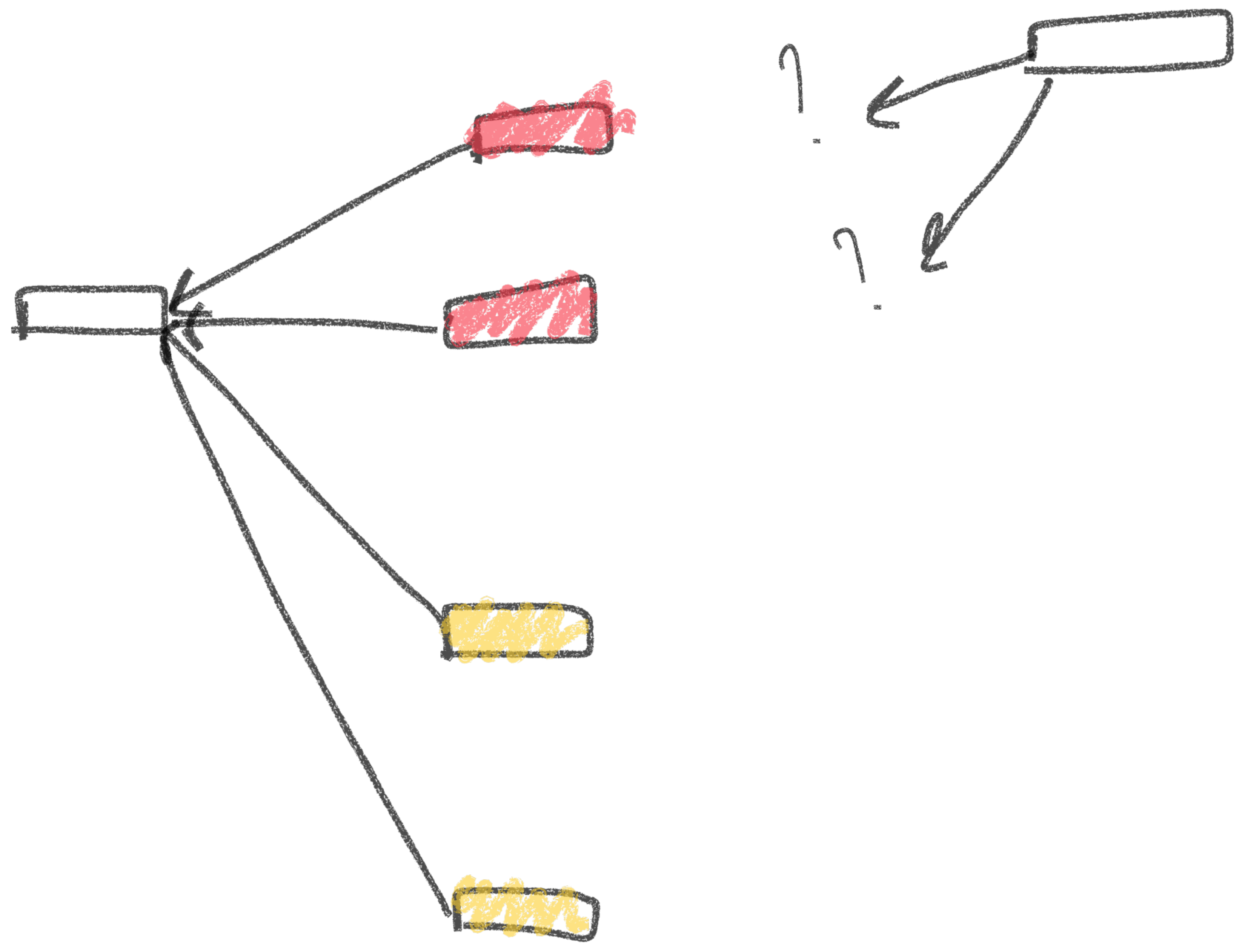
Preuve : depuis 3-SAT

Clause $C : x \vee y \vee \neg z$

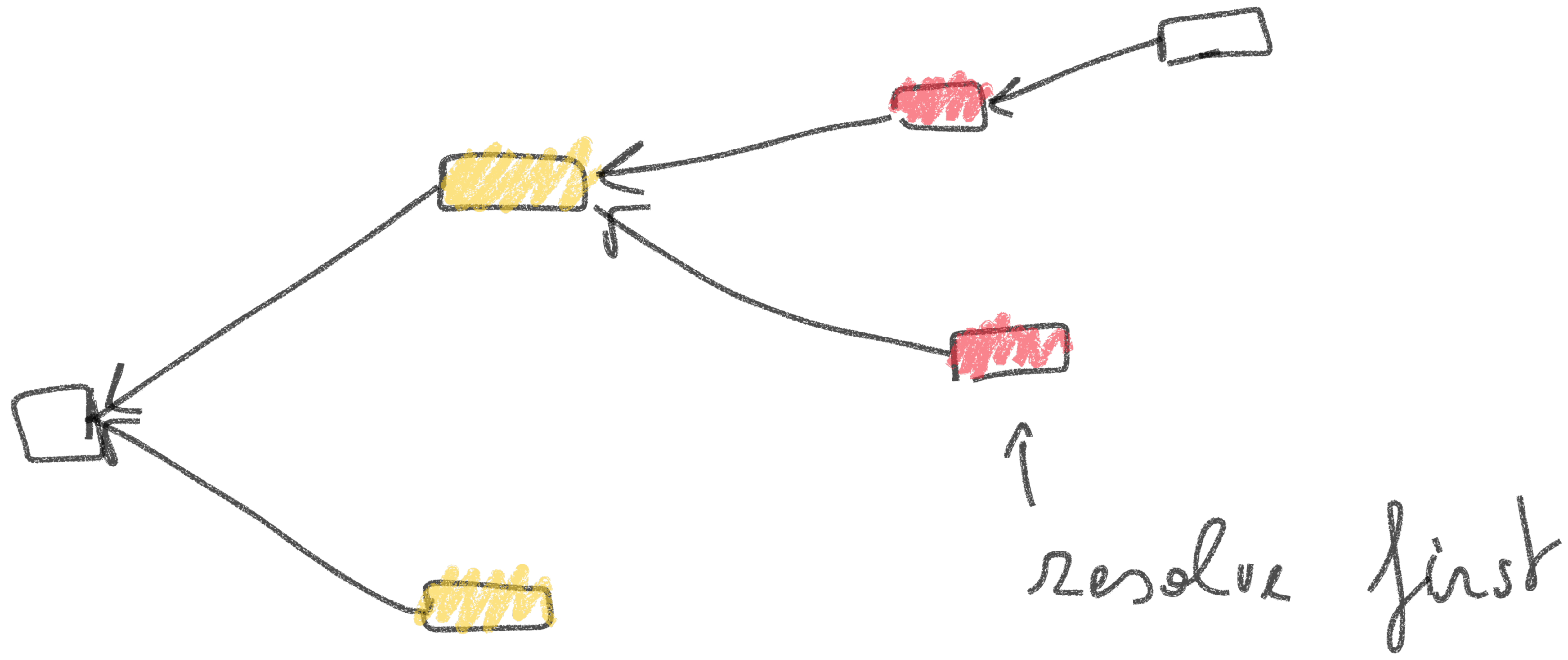


Boolean affectation satisfying all clauses $\Longleftrightarrow$ total weight $\geq m + n + 1$

Conflits concurrents



Conflits concurrents



SeHes Algorithme

"Sequential" Heaviest SubDAG

- find a "small" set of conflicts C (not concurrent with the other conflicts)
- Resolve C (exponential in $|C|$)
- if conflicts remain, goto step 1

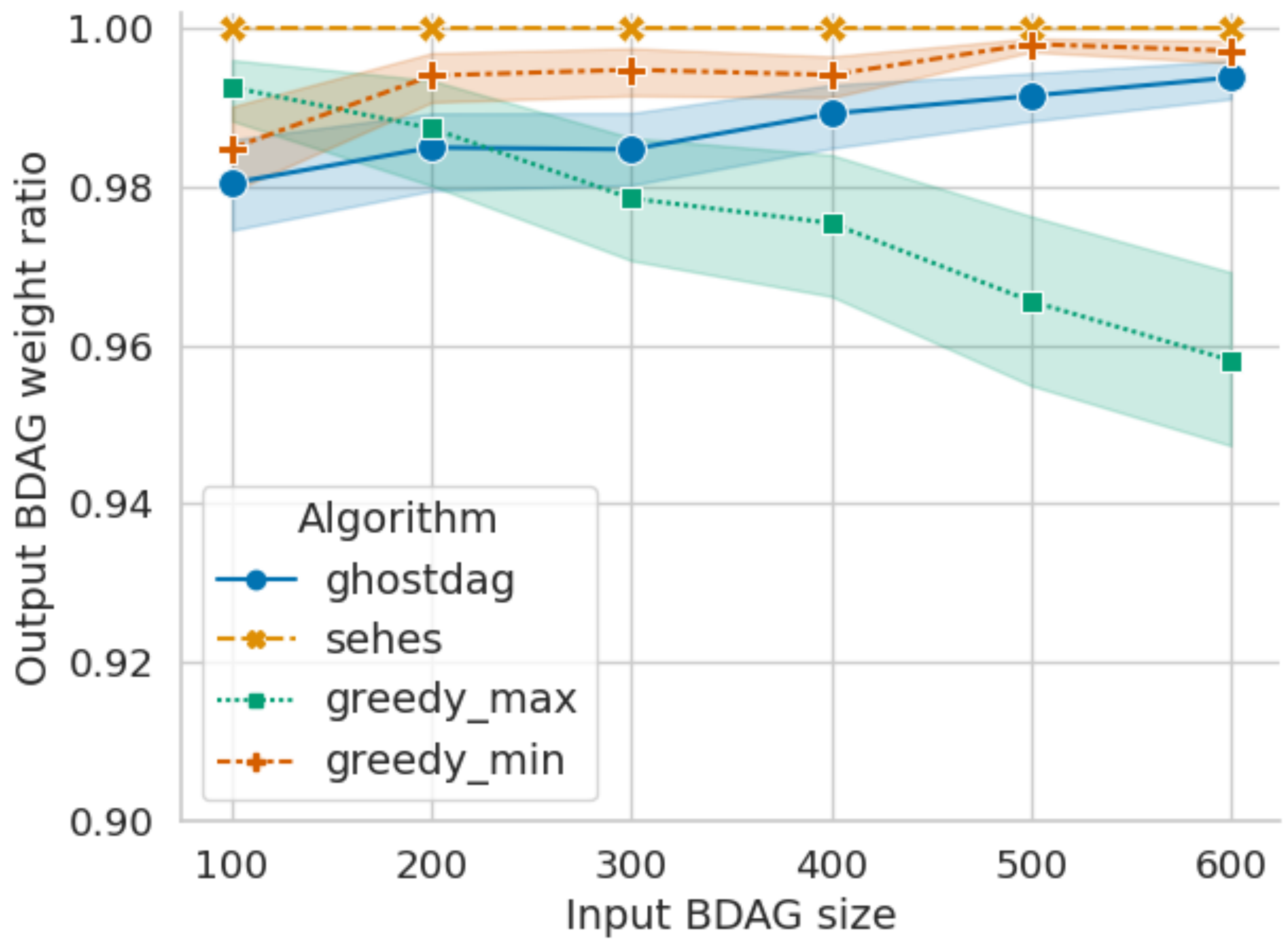
Évaluation

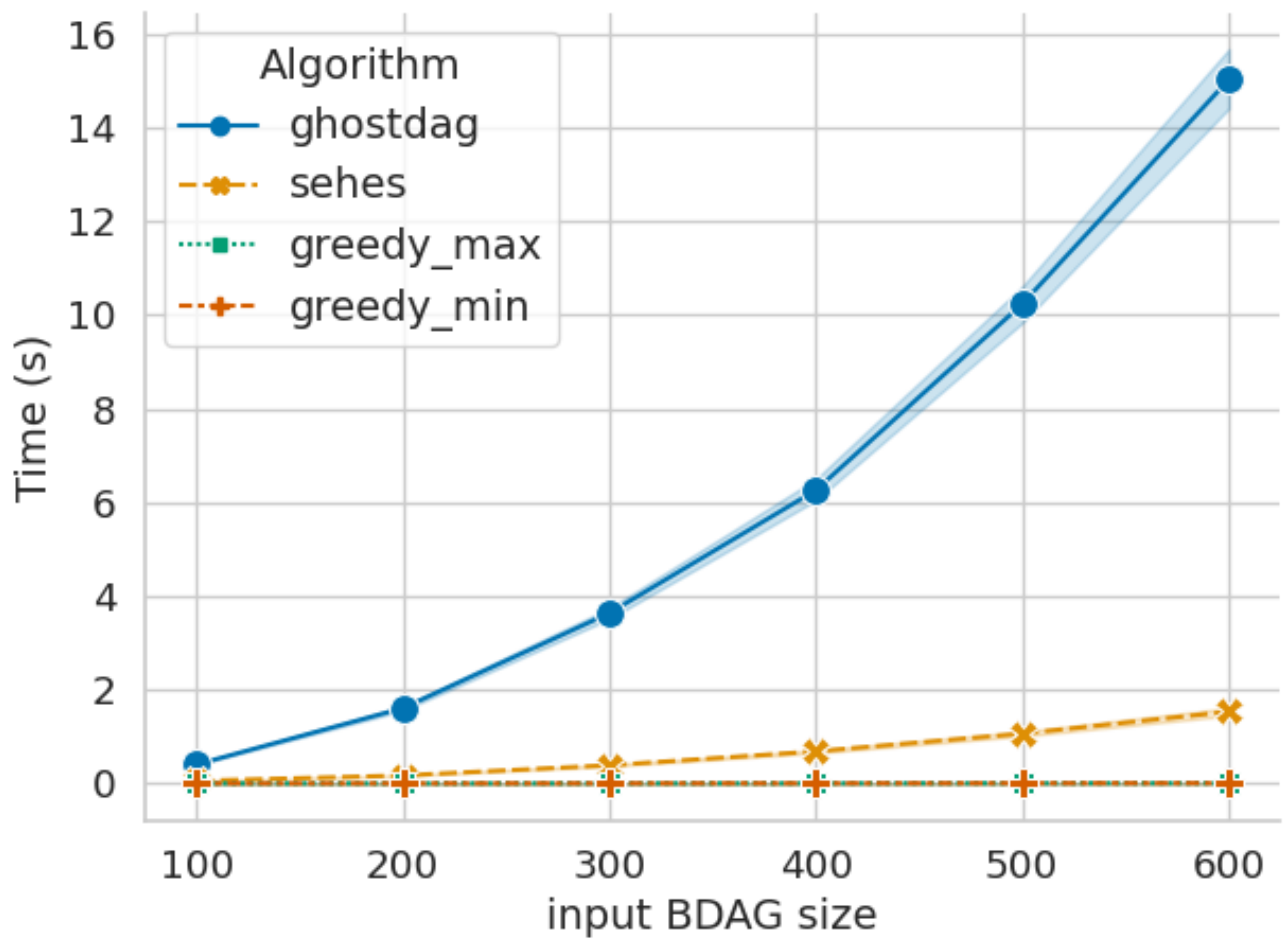
Simulation :

- SeHeS algorithme ;
- GHOSTDAG (avec $k = \infty$) ;
- Deux approches gloutonnes (min et max)

DAG générés aléatoirement en ajoutant des blocs 10 par 10 avec uneven probabilité constante de créer des conflits ou d'être ignoré.

Évaluation





Run on MACbook pro 2,6 GHz Intel Core i7 6-core. 200 random BlockDAGs per size

Code available online: https://doi.org/10.5281/zenodo.8052827

Conclusion

Algorithme efficace pour trouver le sous-DAG🗡️ le plus lourd

Algorithme incr🧀 efficace

Perspectives

Évaluer les performances sur plus de topologies

Conclusion

Algorithme efficace pour trouver le sous-DAG🗡️ le plus lourd
Algorithme incr🧀 efficace

Perspectives

Évaluer les performances sur plus de topologies

https://brains.dnac.org
Deadline 15 juin

Conclusion

Algorithme efficace pour trouver le sous-DAG🗡️ le plus lourd

Algorithme incr🧀 efficace

Perspectives

Évaluer les performances sur plus de topologies

https://brains.dnac.org

Deadline 15 juin

Défense d'HDR

Le 23 juin à 14h

Visible en visio : le lien sera affiché sur https://bramas.fr

Conclusion

Algorithme efficace pour trouver le sous-DAG🗡️ le plus lourd

Algorithme incr🧀 efficace

Perspectives

Évaluer les performances sur plus de topologies

https://brains.dnac.org
Deadline 15 juin

Défense d’HDR

Le 23 juin à 14h

Visible en visio : le lien sera affiché sur https://bramas.fr

Merci !