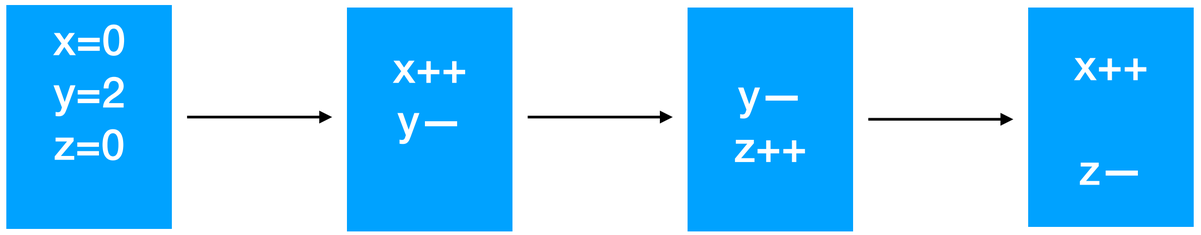
Un aperçu des blockchains

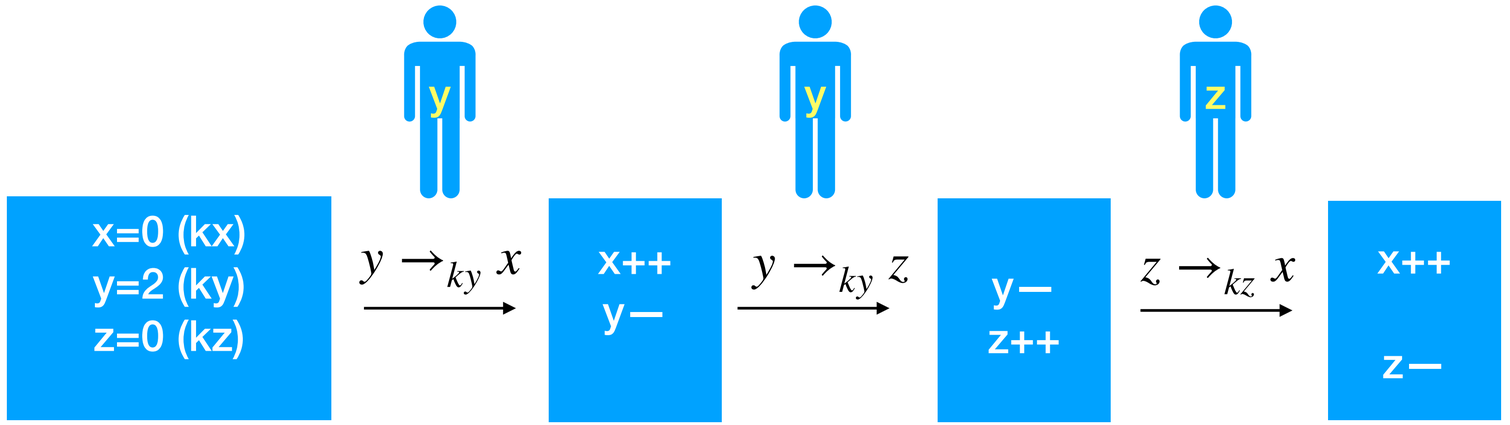
Execution décentralisée de programmes open-source

Jean Krivine - CNRS, IRIF, Univ. Paris Cité

Un carnet de comptes public

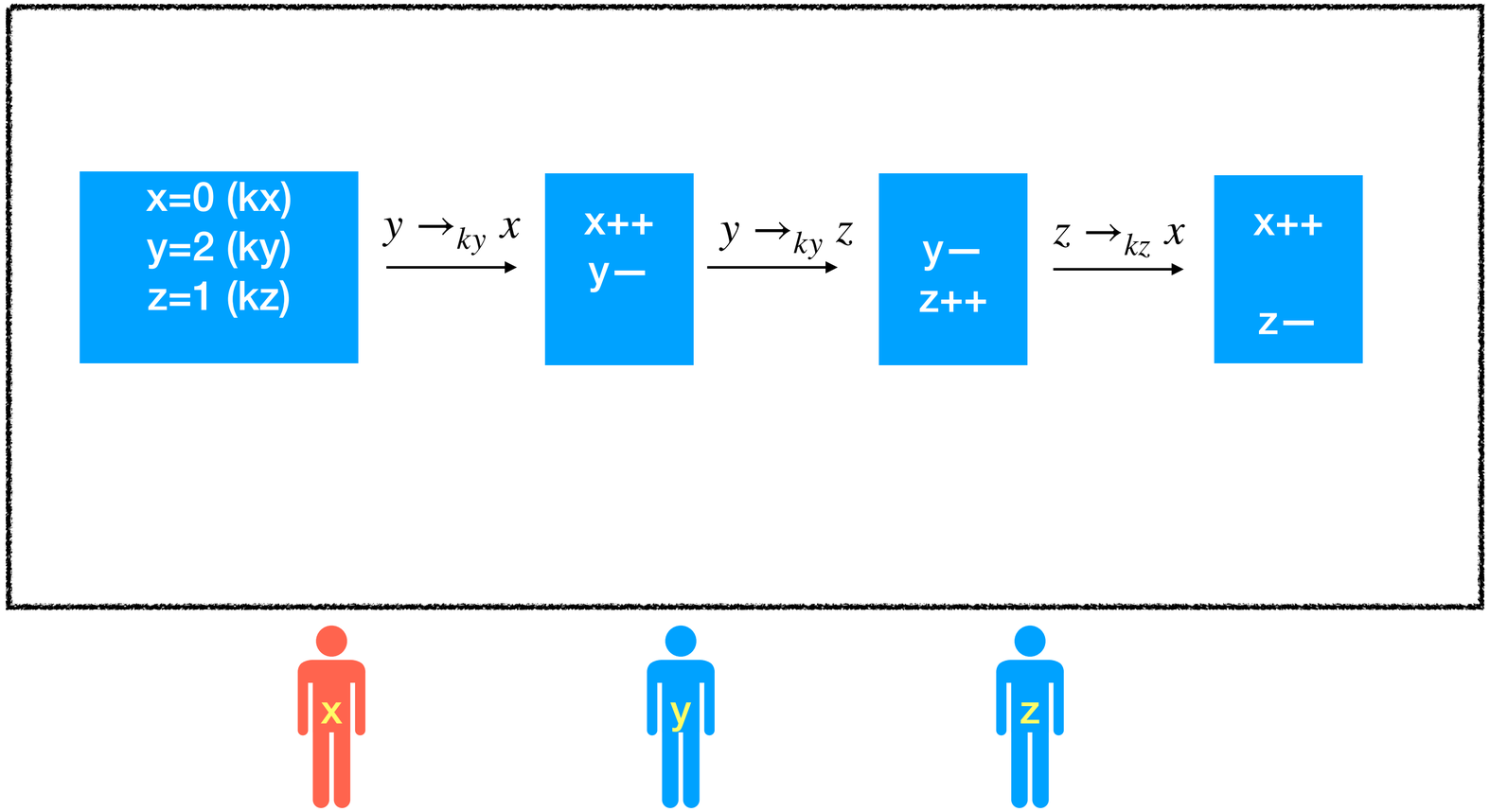


Chaine de “diffs”



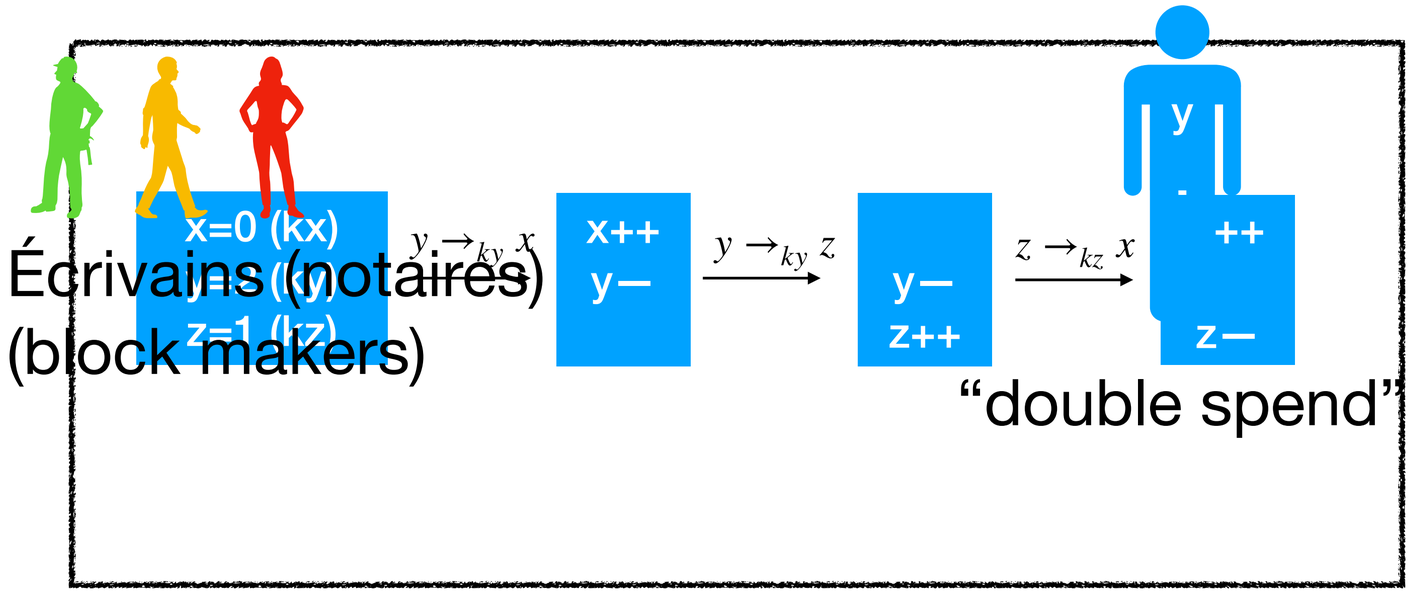
Gestion des comptes sécurisé: clef <—> adresses

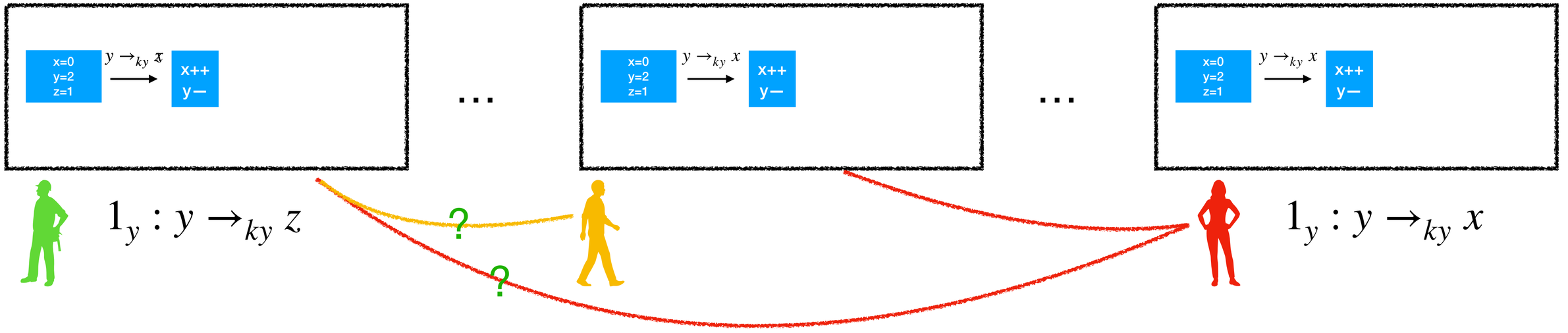
Le problème de la censure



Le serveur rejète en secret certaines transactions…

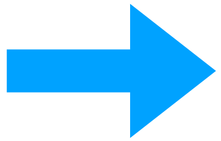
Décentralisation



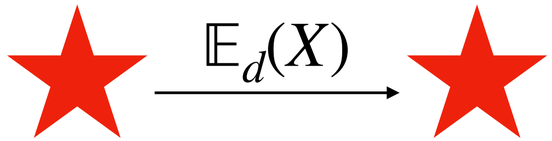


Travail simple ou consensus simple?

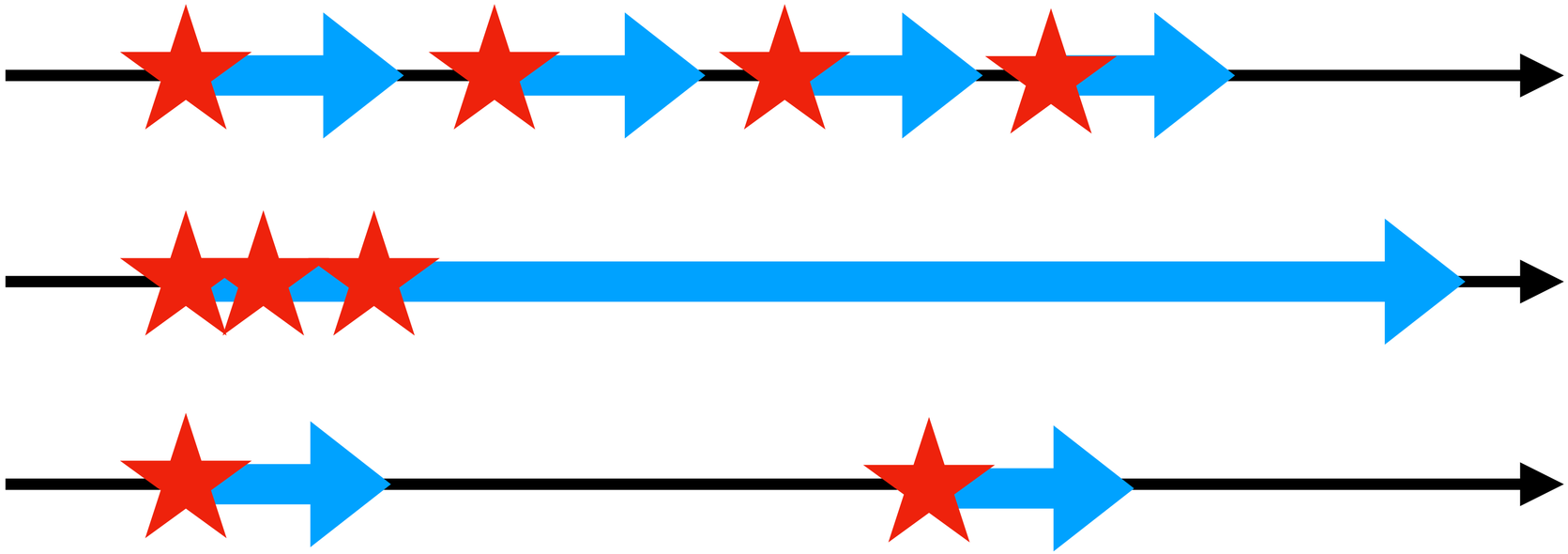
Proposition d'un nouveau bloc



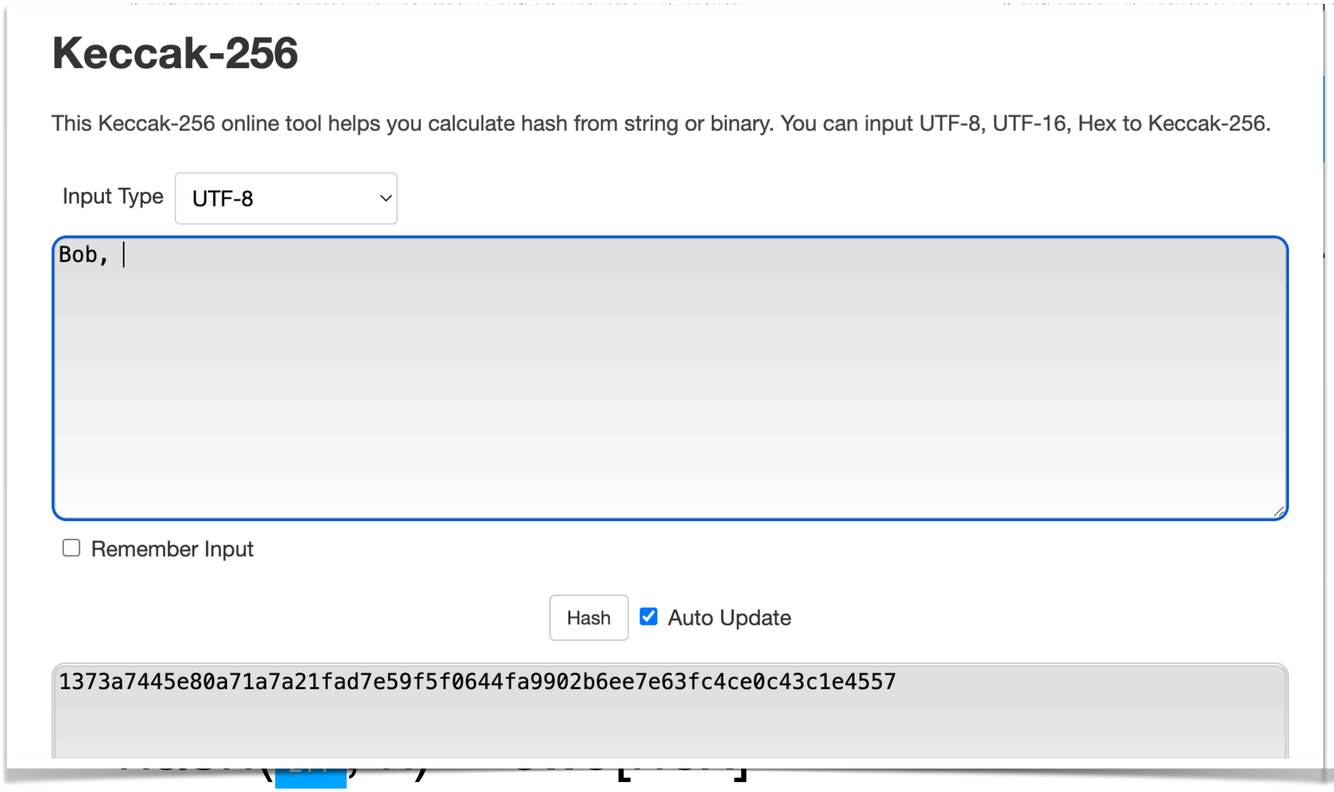
Temps pour atteindre le consensus

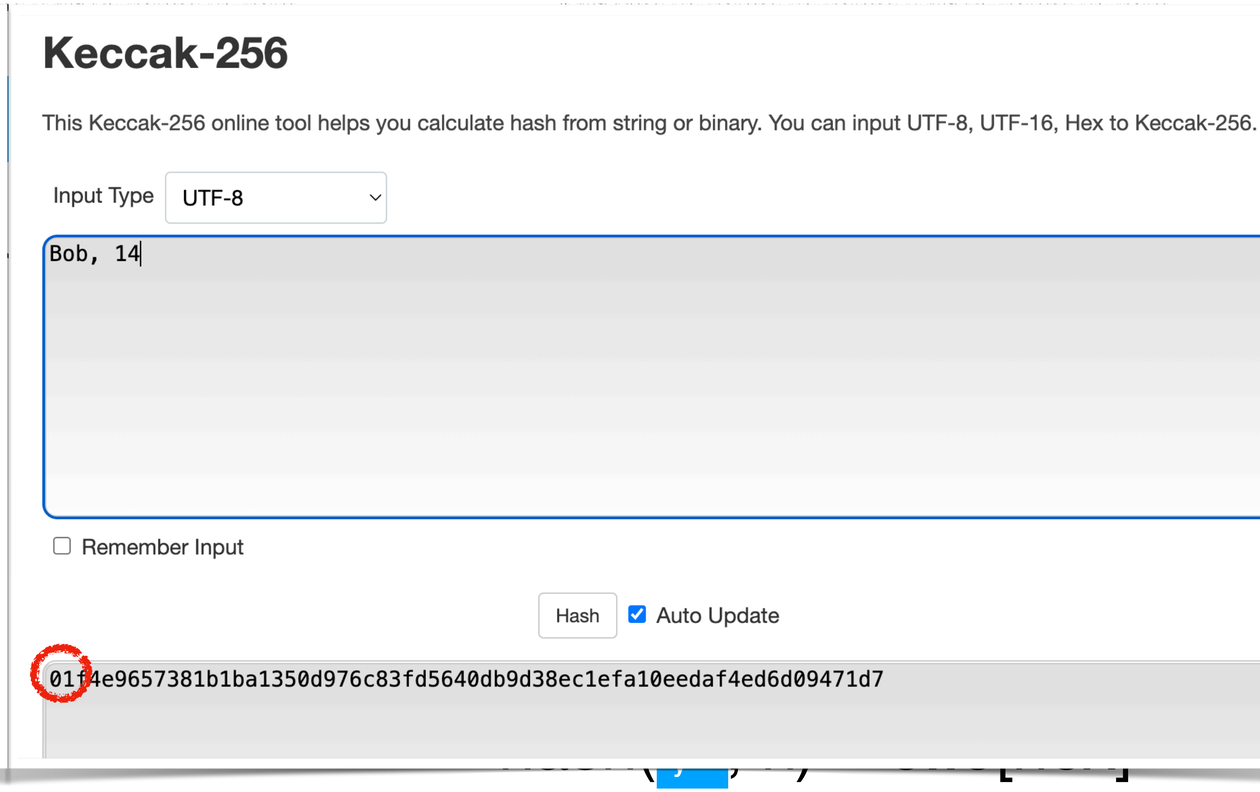


Nakamoto 2008



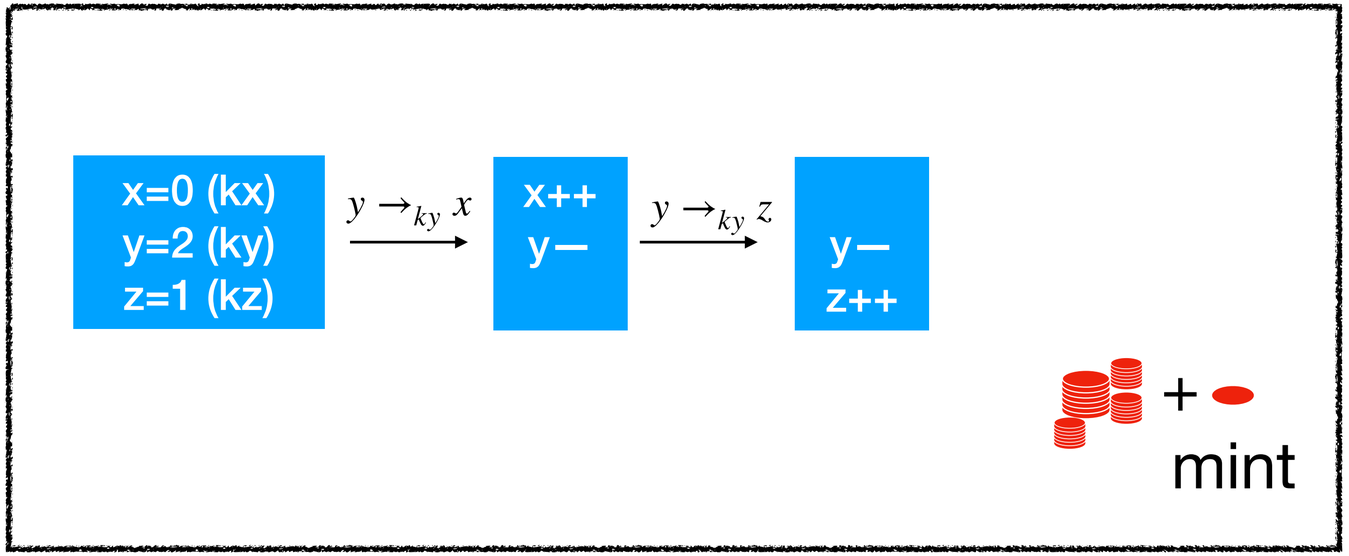
“Proof of work” (bitcoin)

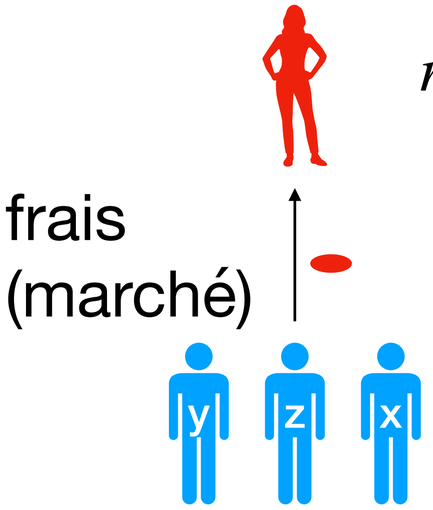




Le nombre de 0 en préfixe est la difficulté du problème…

Incitations économiques



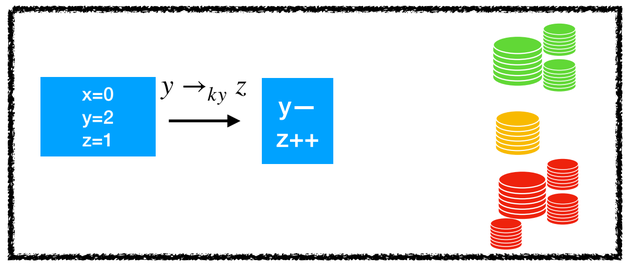


$n_z : z \rightarrow_{kz} x$

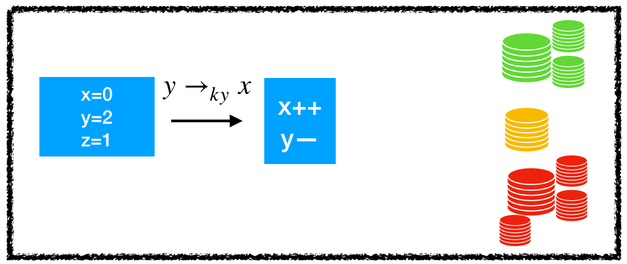
L'écrivain à des coûts (CPU) **opérationnels**:

- trouver le hash (miner)
- maintenir un serveur
- verifier la validité de la transaction
- construire le bloc et le proposer

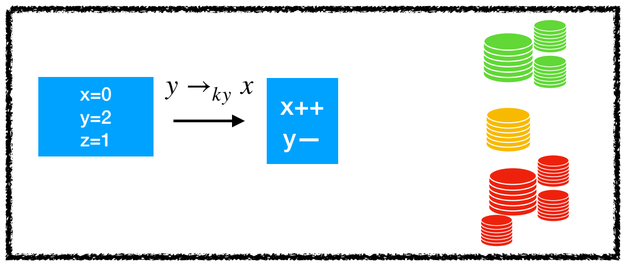
Minimiser les désaccords:
“Proof of stake” (modern blockchains)



…



…



$1_y : y \to_{ky} z$

$1_y : y \to_{ky} x$

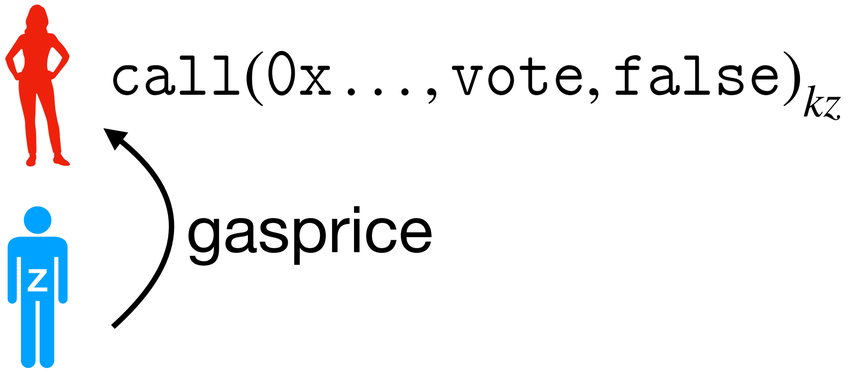
Proba que rouge soit le prochain écrivain:

La mise d’un “block maker” est amputée si le block maker rate son tour (griefing)

La mise d’un “block maker” est “brûlée” si le block maker tente des “double spend”

Blockchain programmables

```
Contract VoteAMainLevee {

  enum Choice {
    NotVoted,
    Yes,
    No
  }

  hasVoted public mapping(address => Choice);

  function vote(bool vote_yes) public {
    require(hasVoted[msg.sender] == NotVoted, “Cannot vote twice”);
    hasVoted[msg.sender] = vote_yes ? Yes : No;
  }
}
```



Le mineur a des coûts opérationnels:

- ~~trouver le hash (miner)~~

- maintenir un serveur

gas!

- verifier la validité de la transaction

- construire le block et le proposer

Interprète (VM)

$$\frac{\neg\mathsf{OutOfGas}(\varepsilon, \delta_{\mathsf{mr}}, 0) \quad \mathtt{B}'' = \begin{cases} \mathtt{B}'; \mathtt{B} & \text{if } \mu(x_{\mathbb{B}}) \\ \mathtt{B} & \text{else} \end{cases}}{\varepsilon : (\mathtt{if}(x_{\mathbb{B}}, \mathtt{B}'); \mathtt{B}, \vec{\varrho}, \mu, \mathbf{S}) \cdot \mathbf{E} \to \varepsilon\{\gamma = \varepsilon.\gamma + \delta_{\mathsf{mr}}\} : (\mathtt{B}'', \vec{\varrho}, \mu, \mathbf{S}) \cdot \mathbf{E}}\ \mathtt{if}$$

Les écrivains sur blockchain programmables sont équipés d'un interprète (une machine virtuelle) qui exécute les transaction et évalue le nombre d'unité de gas nécessaire.

Lorsque l'interprète est bien écrit, le nombre d'unité de gas calculé reflète le coût CPU de l'exécution!

“Crypto-monnaies”

Crypto-monnaies

Native

Monnaie “émise” par le protocole à chaque événement d’écriture. Sa valeur marchande dépend de la demande en écriture sur la chaîne et soumise à intense spéculation.
(ex. bitcoin (Bitcoin bc), ether (Ethereum bc), sol (Solana bc) etc.)

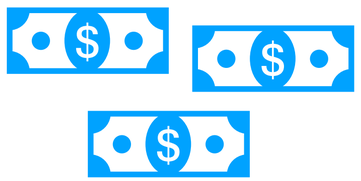
ERC-20

Contrat sur chaîne de gestion de “conservation de biens” (sur ou hors chaîne)

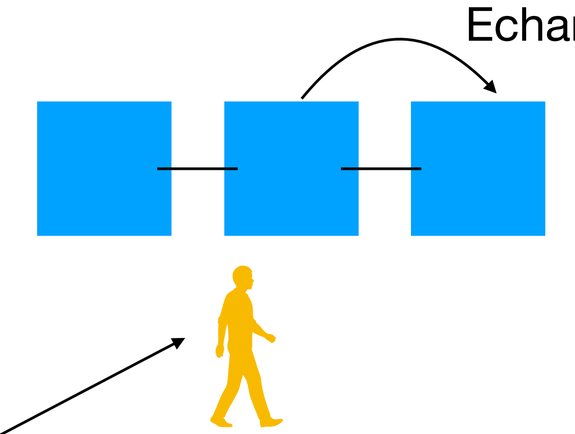
```
balanceOf(address) returns (uint)

transfer(address to, uint amount)

mint(address to, uint amount) onlyAdmin
```

“Stable” coins:
collatéral hors chaîne (tiers de confiance)

Bank



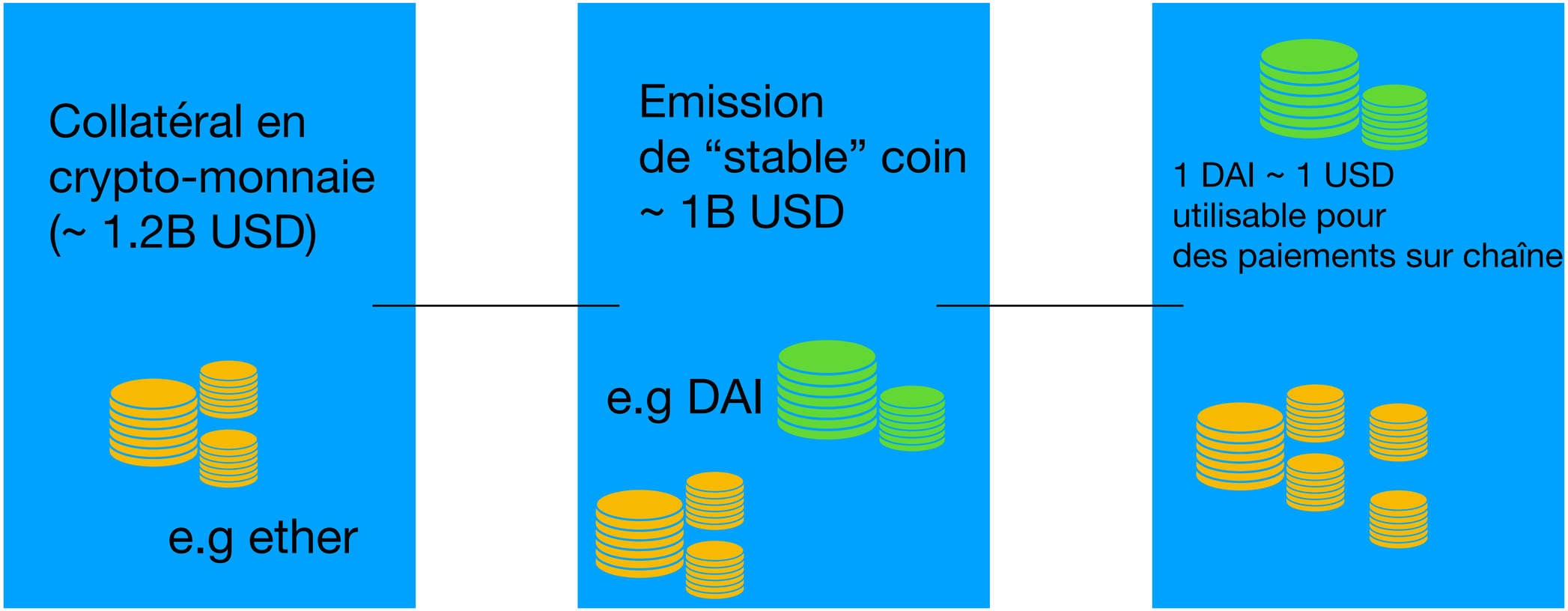
Collatéral (e.g 1B USD)
(investi et/ou en dépot)



$\texttt{USDC} = \texttt{new ERC20}(\{\texttt{decimals} : 8, \texttt{admin} : \texttt{k}_{\texttt{bnk}}\})$

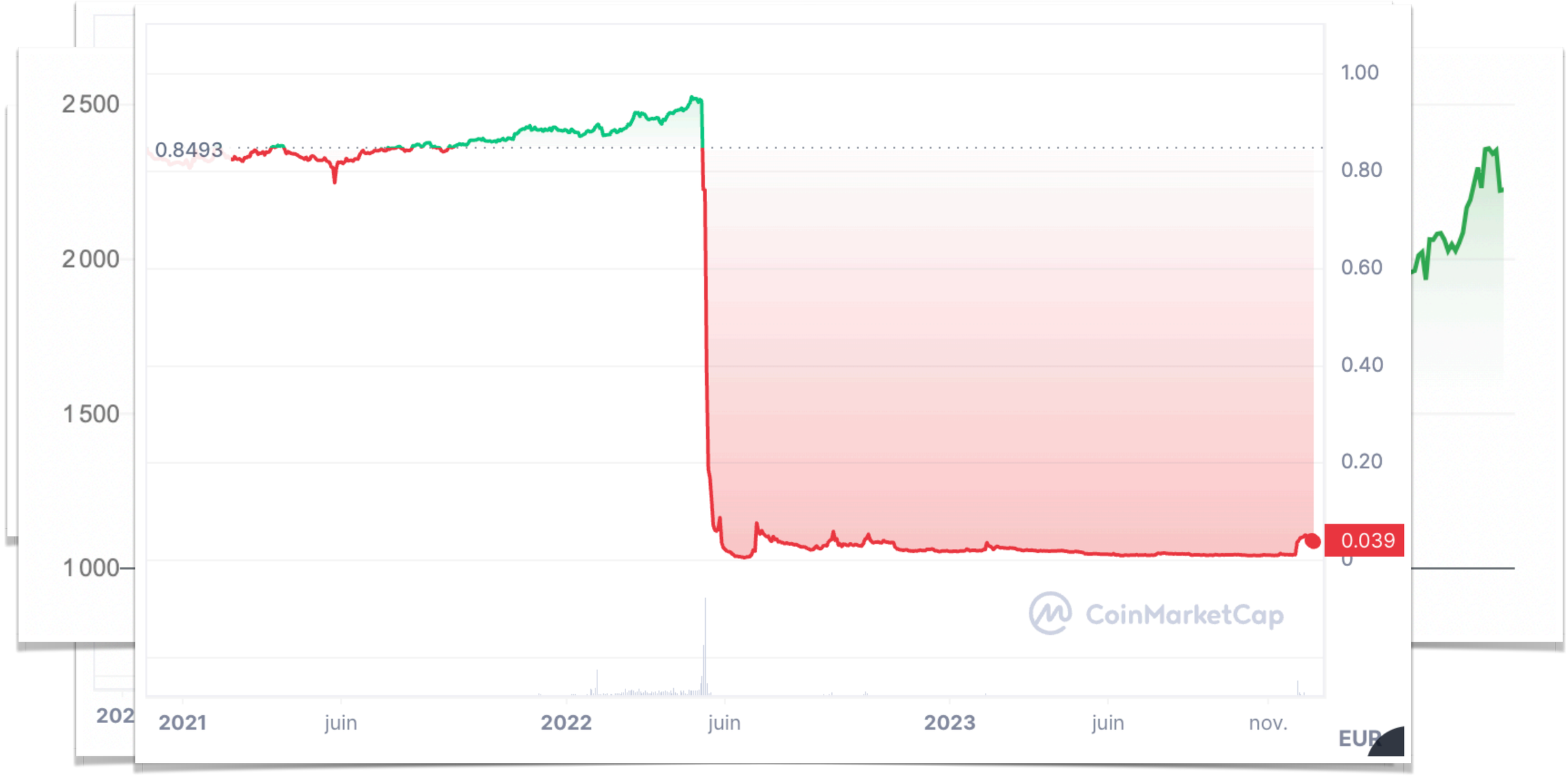
$\texttt{USDC.mint}(10^8 * 10^9)$

“Stable” coins: collatéral sur chaîne



Si le prix (de marché) du collatéral approche de 1B USD, le protocole requiert un ajout de collatéral ou procède a des **liquidations** (rachat de DAI contre du collatéral)

Volatilité


2 500
2 000
1 500
1 000
0.8493
1.00
0.80
0.60
0.40
0.20
0.039
0
CoinMarketCap
2021
juin
2022
juin
2023
juin
nov.
EUR

Parts de protocoles

- Certains protocoles sur chaînes prélèvent des frais à leurs utilisateurs.
- Les frais accumulés peuvent être utilisés pour financer des amélioration du protocole.
- Ces jetons permettent aussi souvent de voter sur des paramètres de “gouvernance” de ces projets (le pendant blockchain d’actions d’entreprises).
- La gestion de ces jetons peut-être confiée à un contrat ERC20 et parfois librement échangeables (et donc soumis à un marché hautement spéculatif et peu régulé).