Duniter

Une blockchain atypique

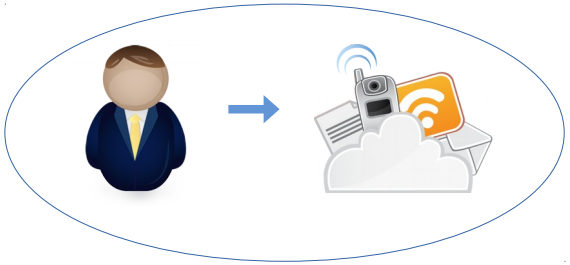
Vincent Texier

Monnaie Libre

- **Duniter gère une Monnaie Libre**
- **Une Monnaie Libre est créé par les humains**
- **Utilisateurs uniques**
- **Humain → Identité numérique**

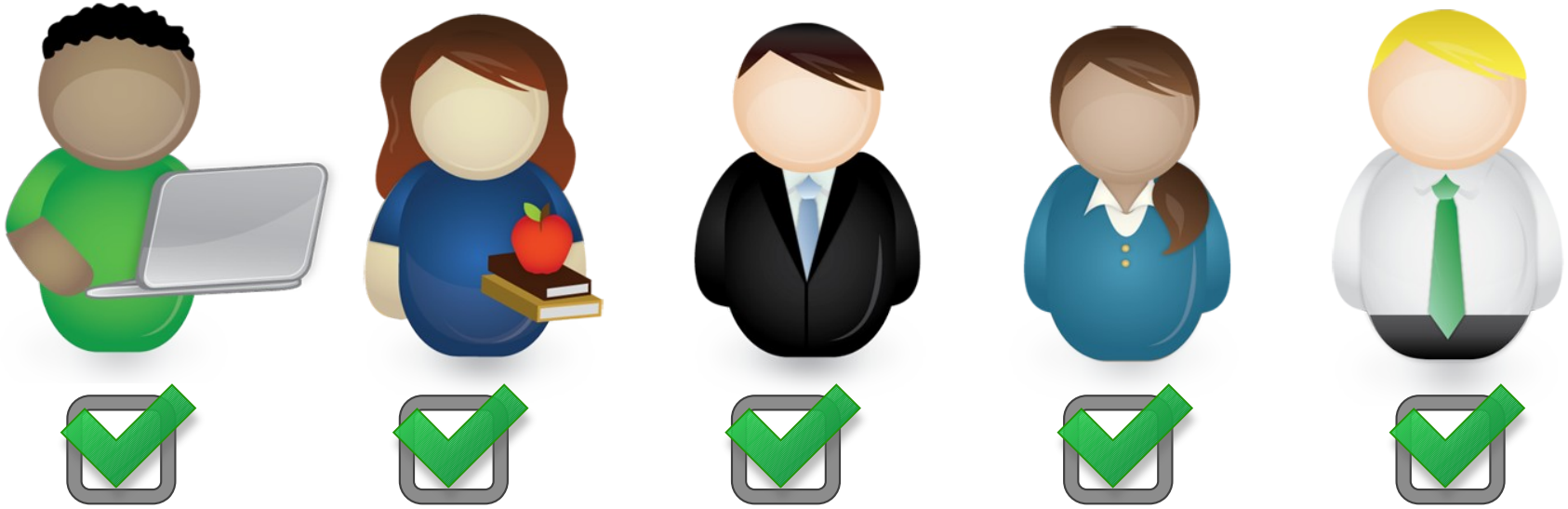
Toile de confiance

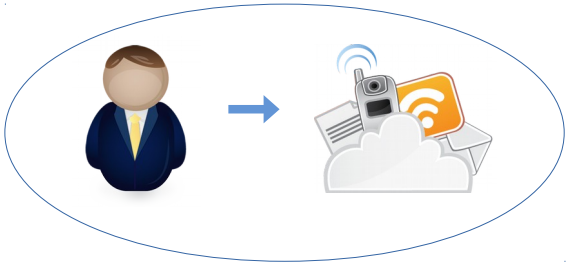
- **Duniter utilise une Toile de Confiance**
- **Inspirée de la communauté PGP**



Toile de confiance

- **Duniter utilise une Toile de Confiance**
- **Inspirée de la communauté PGP**





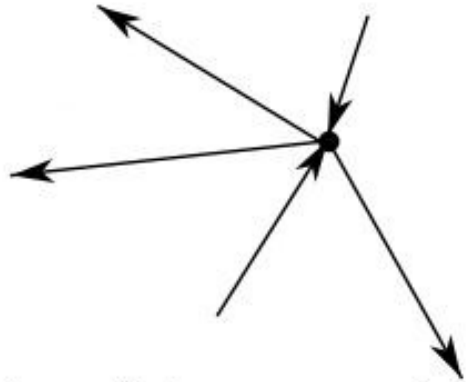
Toile de confiance

- Acte d'adhésion impliquant les membres pour plus de vigilance.
- Rendre la fraude difficile, donc marginale.
- Éviter les attaques Sybilles.
- Ralentir la croissance des régions Sybilles pour pouvoir réagir.

Toile de confiance

1. Règle de distance et membres référents

- ***Un membre A est référent si et seulement si ses deux demi-degrés sont supérieurs ou égaux à CEIl(N^(1/stepMax)) où N est le nombre total de membres et stepMax (5) la distance max.***



degré du sommet : 5
demi-degré extérieur : 3
demi-degré intérieur : 2

Exemple :

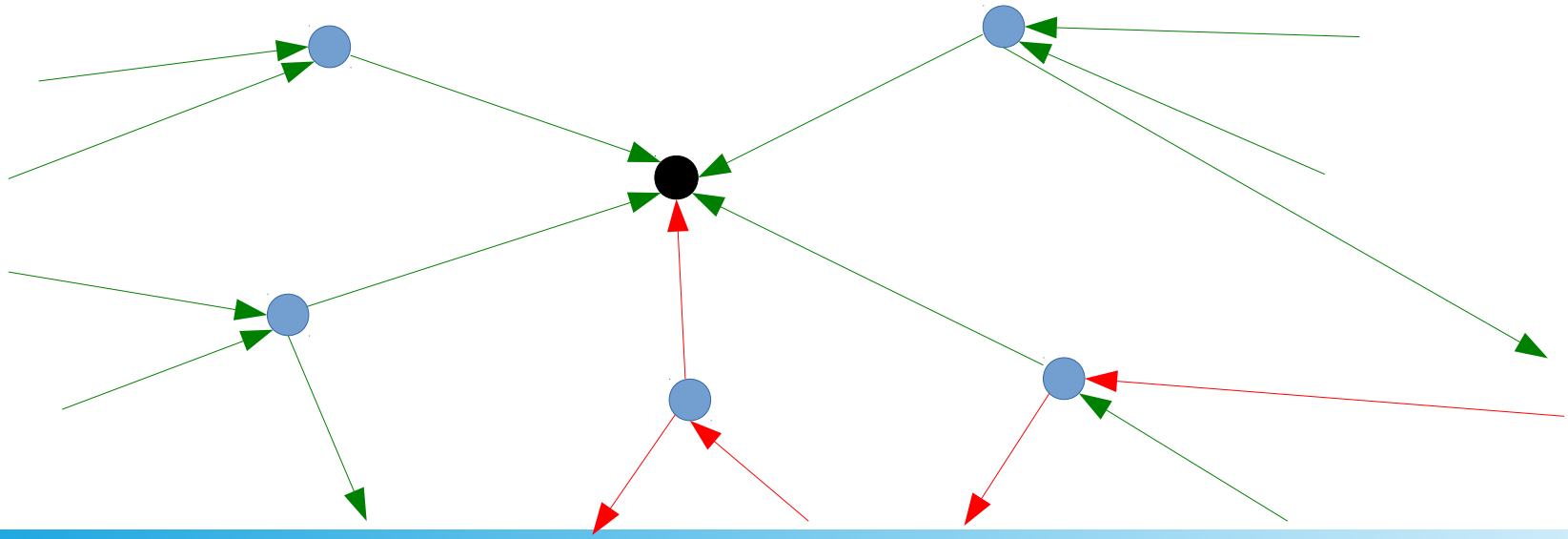
3000^(1/5) = 5
6000^(1/5) = 6

Certifications reçues et données

Toile de confiance

1. Règle de distance et membres référents

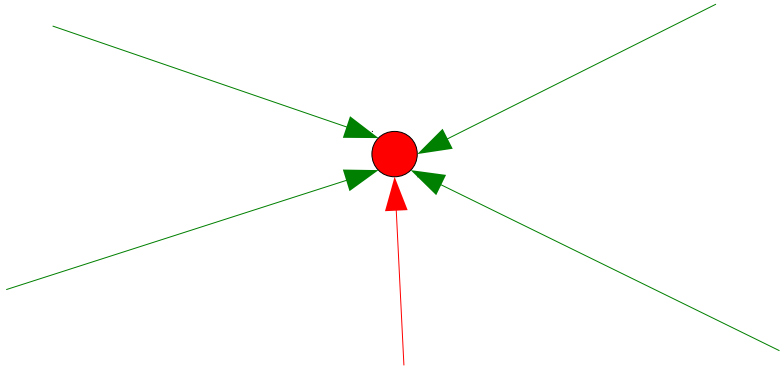
Un membre A respecte la règle de distance si et seulement si pour plus de xPercent (80%) des membres référents R il existe un chemin de R vers A d'une longueur inférieure ou égale à stepMax (5).



Toile de confiance

2. Règle du nombre minimal de certifications reçus

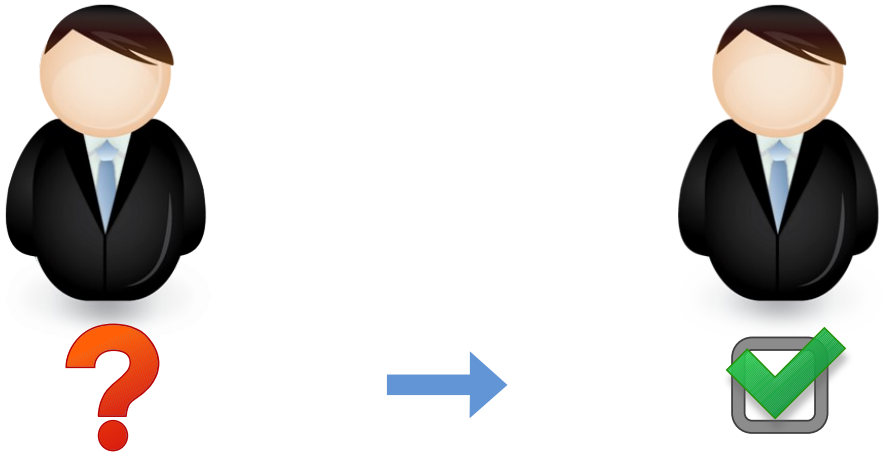
A chaque bloc, si une identité n'a pas sigQty (5) certifications valides, elle perd son statut de membre.



Toile de confiance

3. Règle de renouvellement de l'adhésion

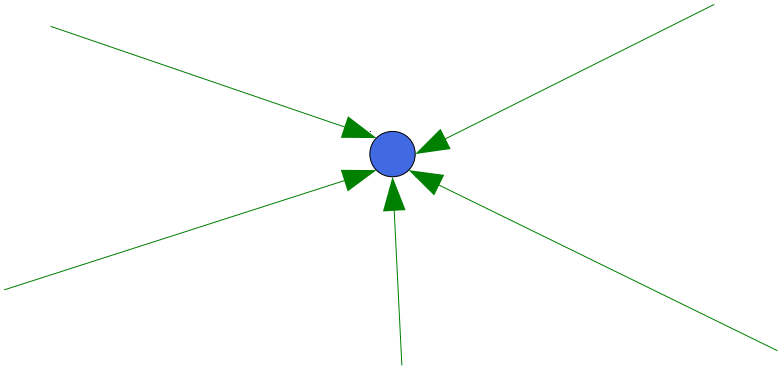
L'adhésion n'est pas éternelle et a une durée de ***msValidity*** *(1 an). On peut faire une demande de renouvellement après* ***msPeriod*** *(2 mois) de la précédente. La demande reste en attente pendant* ***msWindow*** *(2 mois).*

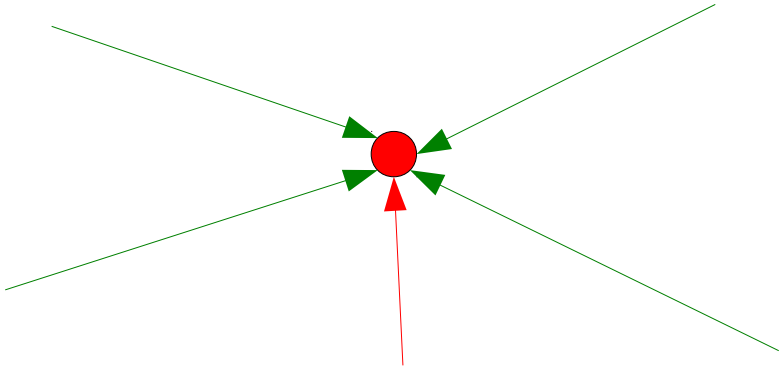


Toile de confiance

4. Règle d'expiration des certifications

Toute certification inscrite en blockchain expire sigValidity secondes (2 ans) après son émission.

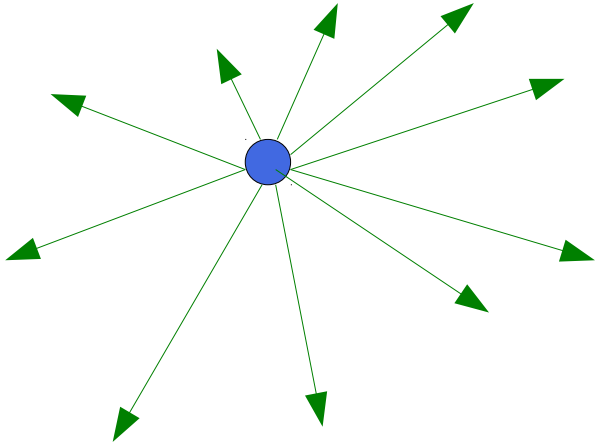




Toile de confiance

5. Règle du stock limité de certifications actives

À tout bloc et pour tout membre, l'ensemble des certifications actives émises par ce membre doit être inférieur ou égal à sigStock (100).



Toile de confiance

6. Règle de l'intervalle d'écriture entre deux certifications

Lorsqu'une certification émise par un membre A est écrite en blockchain, aucune autre certification émise par A ne pourra être écrite en blockchain avant sigPeriod secondes (5 jours).

Toile de confiance

7. Règle de la fenêtre d'écriture d'une certification

Lorsqu'une certification est émise par un membre A, elle restera stockée en attente pour au plus sigWindow secondes (2 mois).

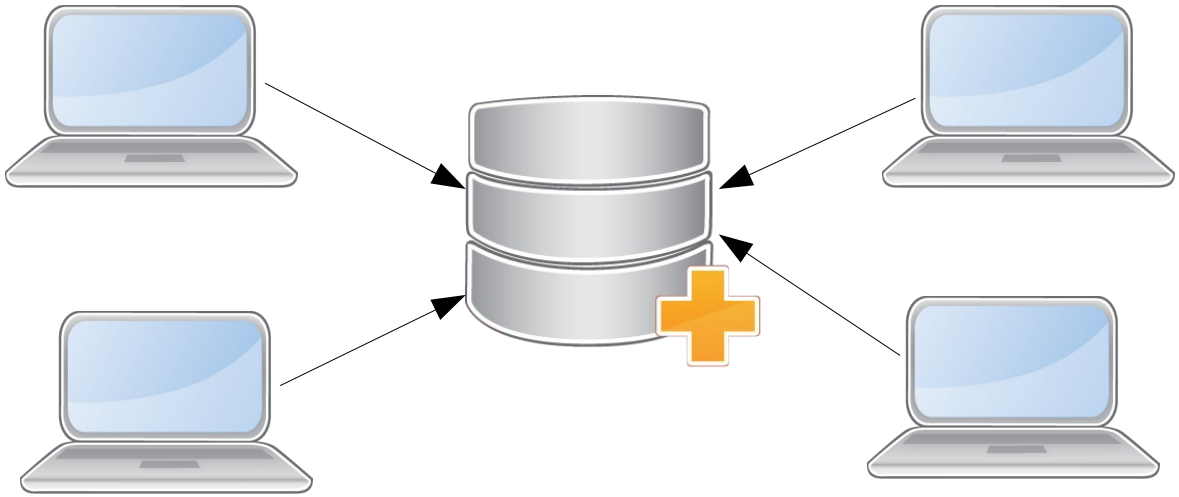
Toile de confiance

8. Règle de la fenêtre d'écriture d'une identité

Lorsqu'une identité est émise, elle restera stockée en attente pour au plus idtyWindow secondes (2 mois).

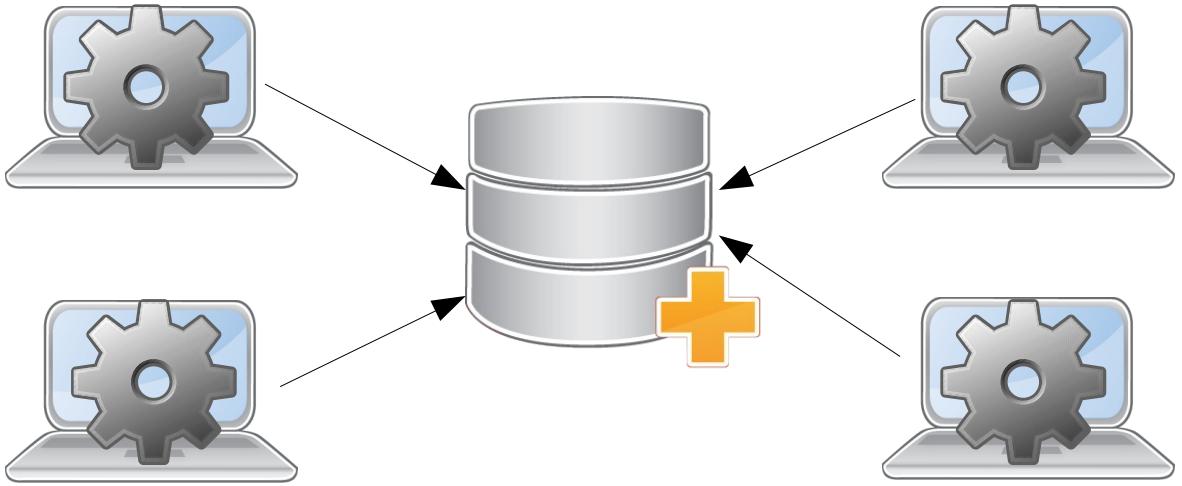
Preuve de travail

Comment fait-on lorsque plusieurs machines souhaitent ajouter en même temps une nouvelle donnée ?



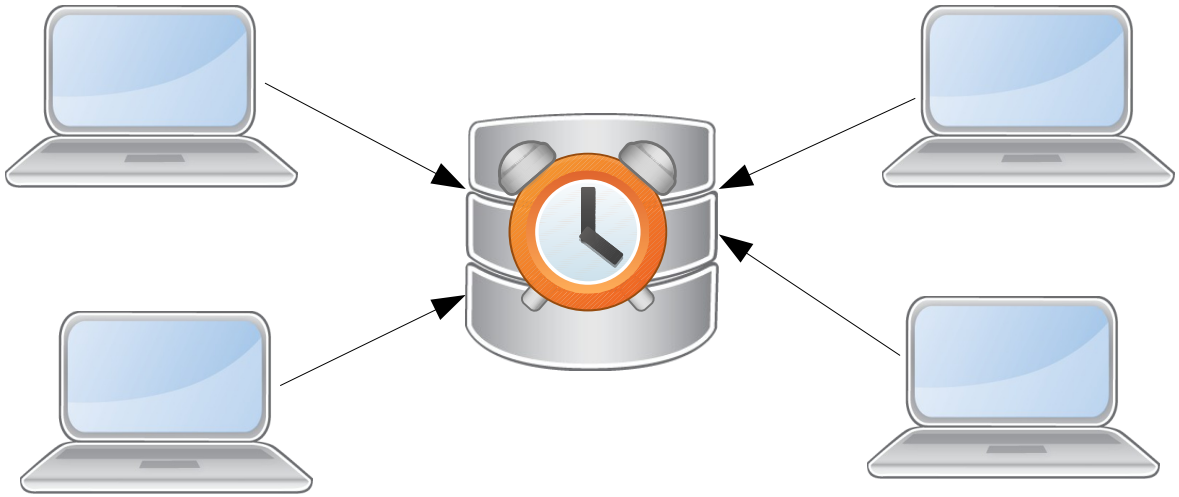
Preuve de travail

Pour avoir le droit d'écrire un nouveau bloc, il faut résoudre un défi qui demande du travail à la machine, ce défi doit être difficile pour qu'il n'y ait pas deux machines qui le résolvent en même temps.



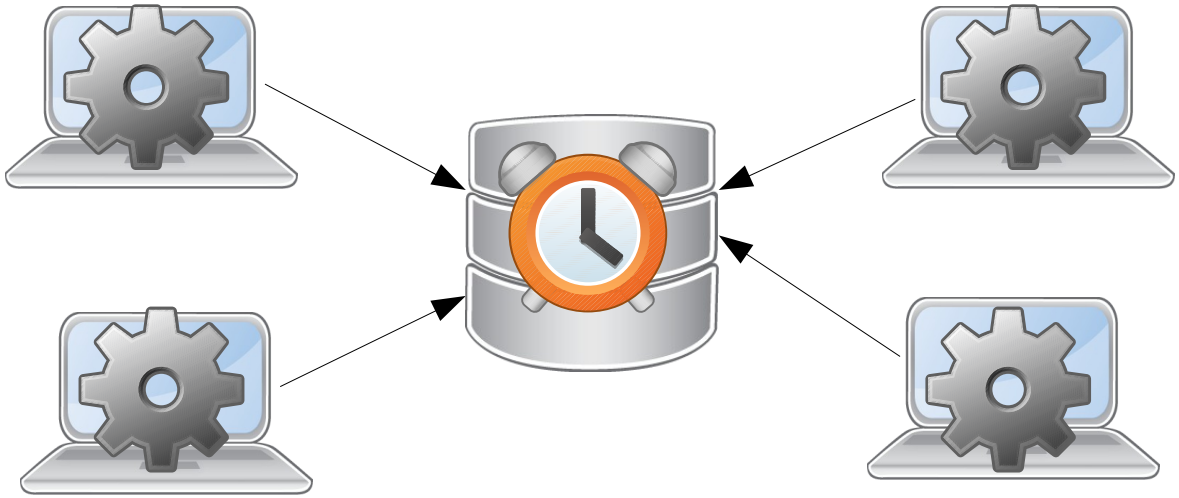
Preuve de travail

Comment fait-on pour nous mettre d'accord sur le temps qui s'est écoulé ?



Preuve de travail

Il suffit de choisir une durée entre chaque nouveau bloc, (ex : 5 min) puis d'adapter la difficulté du défi pour que le réseau trouve bien en moyenne un bloc toutes les 5 min.



Preuve de travail

L'empreinte (le hash)

- 0000[0-9,A-F]XXXXXXXXXXX

00009276902793AA44601A9D43099E7B6
3DBF9EBB55BCCFD6AE20C729B54C653

044601A9D43099…
B55BCCFD6AE20C…
00AA44601A9D43…
01A9D43099E460…
00009B54C653…

Preuve de travail

La difficulté commune

0000[0-9,A-F]XXXXXXXXXXX

powMin // 16 = X reste Y

70 // 16 = 4 reste 6

4 Zéros + Valeur 6 en partant de F (9)

HASH : 00009...

Preuve de travail

Le Nonce

XYY00000000000

X correspond au numéro de pair si plusieurs serveurs utilisent la même clef.

Y correspond au nombre de cœurs du processeur.

Nonce	Hash
10400000000001	044601A9D43099…
10400000000002	B55BCCFD6AE20C…
10400000000003	00AA44601A9D43…
10400000000004	01A9D43099E460…
10400000000005	00009B54C653…

Preuve de travail

La difficulté personnalisée

Soient powMin la difficulté commune, exFact le facteur d'exclusion d'un membre et handicap son handicap. La difficulté personnalisée diff de ce membre est :

$$diff = powMin * exFact + handicap$$

Preuve de travail

Le facteur d'exclusion

Soient **nbPreviousIssuers** *la valeur du champ* **issuersCount** *du dernier bloc trouvé par le membre et* **nbBlocksSince** *le nombre de blocs trouvés par le reste du réseau depuis que le membre considéré a trouvé son dernier bloc.*

exFact = MAX [1 ; FLOOR (0.67 * nbPreviousIssuers / (1 + nbBlocksSince))]

Preuve de travail

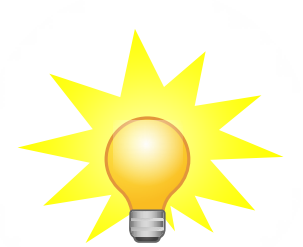
Le handicap

Soient **nbPersonalBlocksInFrame** *le nombre de blocs écrits par le membre considéré dans la fenêtre courante et* **medianOfBlocksInFrame** *le nombre médian de blocs écrits par les membres au sein de la fenêtre courante.*

handicap = FLOOR(LN(MAX(1; (nbPersonalBlocksInFrame + 1) / medianOfBlocksInFrame)) / LN(1.189))

Consommation énergétique

- ***Seuls les membres de la monnaie peuvent calculer des blocs.***
- ***Exclut en permanence 1/3 du réseau de calculateurs.***
- ***Pas de rémunération.***



Consommation énergétique

Centrale nucléaire : 7,5 TWh par an

Duniter++ 0,000048 TWh par an*

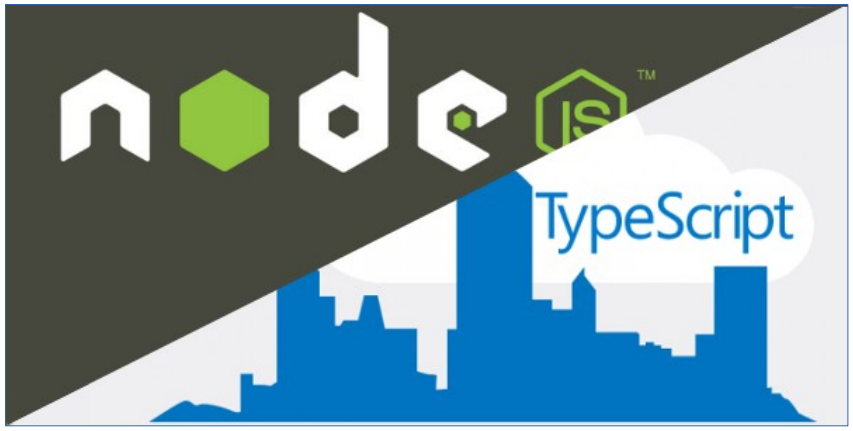
Bitcoin 38,7 TWh par an**

* Janvier 2020, 100 serveurs à 55 W

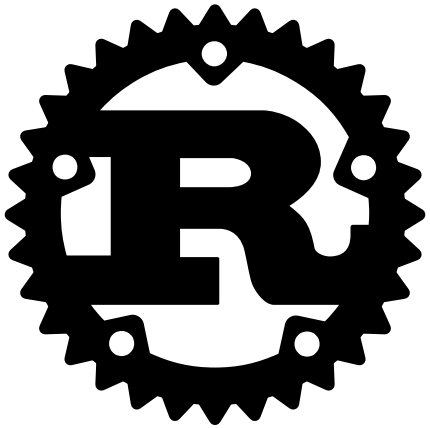
** Mars 2019, https://bitcoin.fr/quelle-est-la-consommation-electrique-du-reseau-bitcoin/

Recherche Contributeurs

- **Développement de modules**
- **Correction de bogues**
- **Amélioration des tests**



NodeJS/TypeScript



Rust

Duniter
Une blockchain atypique

- https://duniter.org
- https://forum.duniter.org
-
- https://monnaie-libre.fr
- https://forum.monnaie-libre.fr

Vincent Texier