Enjeux de la blockchain pour les collectivités

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

Enjeux de la blockchain pour les collectivités

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

afnic

La chaîne de blocs, solution à tout

[Amendement au récent projet de loi sur les soi-disant *fake news*]

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 9, insérer l'article suivant:

Le Gouvernement remet au Parlement, dans les six mois suivant la promulgation de la présente loi, un rapport sur la possibilité d'utiliser la technologie des chaînes de blocs pour assurer la certification des informations, photographies, illustrations diverses dans tous les supports diffusant des informations : réseaux sociaux, internet, plateformes. Ce rapport précise les conditions indispensables de mise en place, dans le respect de la préservation de la liberté d'expression de cette chaîne de blocs de certification.

Petit rappel sur la chaîne de blocs

Petit rappel sur la chaîne de blocs

- Inventée pour Bitcoin en 2008,

Petit rappel sur la chaîne de blocs

- Inventée pour Bitcoin en 2008,
- mais utilisable en dehors du Bitcoin,

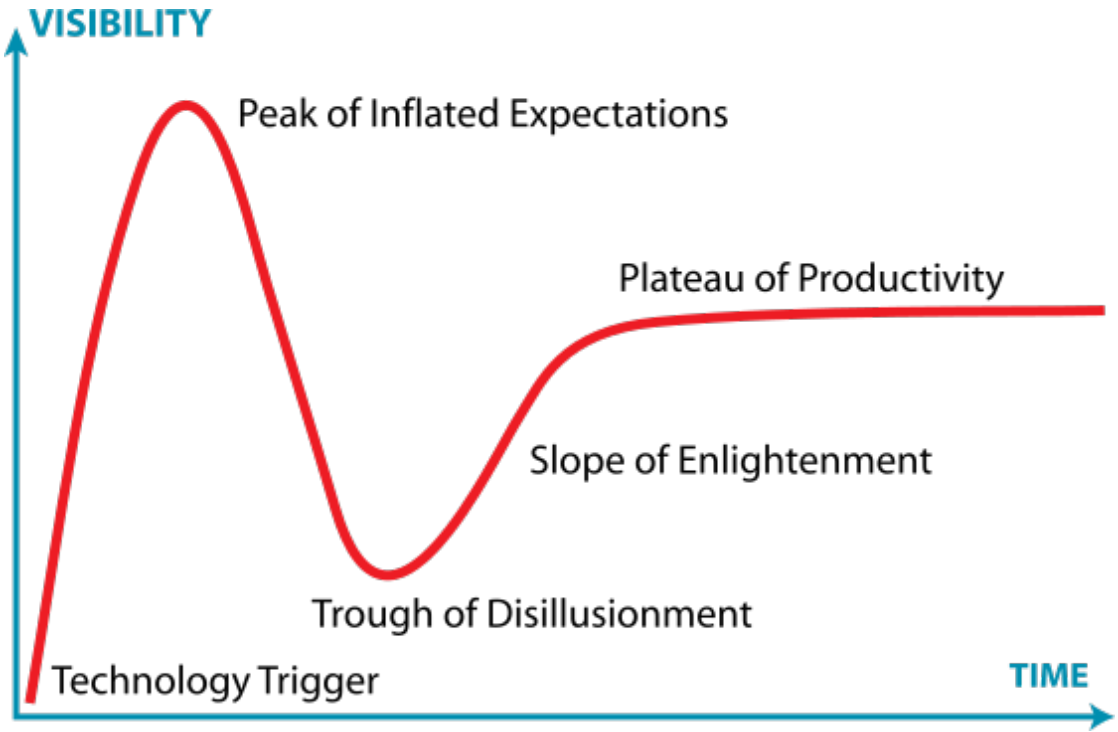
Petit rappel sur la chaîne de blocs

- Inventée pour Bitcoin en 2008,
- mais utilisable en dehors du Bitcoin,
- Une très importante percée scientifique,

afnic

Petit rappel sur la chaîne de blocs

- Inventée pour Bitcoin en 2008,
- mais utilisable en dehors du Bitcoin,
- Une très importante percée scientifique,
- Actuellement haut placée dans le *hype cycle*.



Mais ça sert à quoi

Mais ça sert à quoi

- À obtenir un **consensus** entre les membres,

Mais ça sert à quoi

- À obtenir un **consensus** entre les membres,
- qui ne se font pas **confiance** entre eux,

Mais ça sert à quoi

- À obtenir un **consensus** entre les membres,
- qui ne se font pas **confiance** entre eux,
- un consensus sur un **état** du système.

afnic

Mais ça sert à quoi

- À obtenir un **consensus** entre les membres,
- qui ne se font pas **confiance** entre eux,
- un consensus sur un **état** du système.
- Exemple Bitcoin : l'état est la liste des comptes avec leur montant (ou, ce qui revient au même, la liste des transactions qui a mené à cet état).

afnic

Oui, mais c'est quoi

Oui, mais c'est quoi

- Une chaîne de transactions : transaction 1 « Alice donne 1 bitcoin à Bob », transaction 2 « Bob donne un demi-bitcoin à Charlie » (l'ordre est crucial),

afnic

Oui, mais c'est quoi

- Une chaîne de transactions : transaction 1 « Alice donne 1 bitcoin à Bob », transaction 2 « Bob donne un demi-bitcoin à Charlie »,
- En pratique, les transactions sont regroupées en blocs, d'où le nom de chaînes de blocs ; du fait du chaînage vers le bloc précédent, la chaîne est techniquement immuable,

Oui, mais c'est quoi

- Une chaîne de transactions : transaction 1 « Alice donne 1 bitcoin à Bob », transaction 2 « Bob donne un demi-bitcoin à Charlie »,
- En pratique, les transactions sont regroupées en blocs, d'où le nom de chaînes de blocs,
- Les transactions sont signées, il y a de la cryptographie, on est sûrs que la transaction 1 a été signée avec la clé d'Alice,

afnic

Oui, mais c'est quoi

- Une chaîne de transactions : transaction 1 « Alice donne 1 bitcoin à Bob », transaction 2 « Bob donne un demi-bitcoin à Charlie »,
- En pratique, les transactions sont regroupées en blocs, d'où le nom de chaînes de blocs,
- Les transactions sont signées, il y a de la cryptographie,
- La chaîne est gérée en **pair-à-pair**, tout le monde peut regarder, chaque pair peut ajouter des blocs. Autrement, ce n'est qu'une vulgaire base de données.

afnic

Attention

- Danger pipeautage !

Attention

- Danger pipeautage !
- Toute liste chaînée n'est pas une *blockchain*,

afnic

Attention

- Danger pipeautage !
- Toute liste chaînée n'est pas une *blockchain*,
- Toute base de données accessible publiquement n'est pas une *blockchain*,

afnic

Attention

- Danger pipeautage !
- Toute liste chaînée n'est pas une *blockchain*,
- Toute base de données accessible publiquement n'est pas une *blockchain*,
- Toute base de données « ajout seulement » n'est pas une *blockchain*. (Pensez aux journaux comme ceux de *Certificate Transparency*.)

afnic

Exemple de fausse chaîne de blocs

Rapport du PNUD (Nations Unies) à propos des projets de cadastre en Inde

Exemple de fausse chaîne de blocs

Rapport du PNUD (Nations Unies) à propos des projets de cadastre en Inde

- « un représentant entrera alors l'acte de vente dans le système, alimenté par la technologie blockchain. [...] La beauté de ce système est que les citoyens engagés dans l'achat et la vente de propriétés n'auront pas besoin d'un compte blockchain [...] La technologie fonctionne simplement en arrière-plan. »

Exemple de fausse chaîne de blocs

Rapport du PNUD (Nations Unies) à propos des projets de cadastre en Inde

- « un représentant entrera alors l'acte de vente dans le système, alimenté par la technologie blockchain. [...] La beauté de ce système est que les citoyens engagés dans l'achat et la vente de propriétés n'auront pas besoin d'un compte blockchain [...] La technologie fonctionne simplement en arrière-plan. »
- À quoi sert la chaîne alors ? C'est une bête base de données, même pas accessible publiquement !

Contrats automatiques

Contrats automatiques

- Les transactions sont l'exécution d'un programme,

Contrats automatiques

- Les transactions sont l'exécution d'un programme,
- Chaque pair exécute le même programme, tout le monde est d'accord sur l'état,

afnic

Contrats automatiques

- Les transactions sont l'exécution d'un programme,
- Chaque pair exécute le même programme, tout le monde est d'accord sur l'état,
- Des possibilités illimitées, du moment qu'on sait programmer,

afnic

Contrats automatiques

- Les transactions sont l'exécution d'un programme,
- Chaque pair exécute le même programme, tout le monde est d'accord sur l'état,
- Des possibilités illimitées, du moment qu'on sait programmer,
- Le programme (« contrat ») fait loi,

afnic

Contrats automatiques

- Les transactions sont l'exécution d'un programme,
- Chaque pair exécute le même programme, tout le monde est d'accord sur l'état,
- Des possibilités illimitées, du moment qu'on sait programmer,
- Le programme (« contrat ») fait loi,
- Exemple : la chaîne de blocs Ethereum.

afnic

Les oracles

Les oracles

- La chaîne de blocs marche très bien quand on gère des ressources entièrement numériques (exemple : les cryptomonnaies, comme Bitcoin, ou les noms, comme Namecoin),

Les oracles

- La chaîne de blocs marche très bien quand on gère des ressources entièrement numériques,
- Mais si on veut un lien avec le monde physique, on ne peut plus le faire en pair à pair,

Les oracles

- La chaîne de blocs marche très bien quand on gère des ressources entièrement numériques,
- Mais si on veut un lien avec le monde physique, on ne peut plus le faire en pair à pair,
- Exemple : un contrat de pari / assurance sur la météo, où il faut qu'un organisme de confiance dise le temps qu'il a fait,

afnic

Les oracles

- La chaîne de blocs marche très bien quand on gère des ressources entièrement numériques,
- Mais si on veut un lien avec le monde physique, on ne peut plus le faire en pair à pair,
- Exemple : un contrat de pari / assurance sur la météo,
- Un acteur privilégié, l'**oracle**, doit pouvoir écrire dans la chaîne, et tout le monde lui faire confiance. On n'est plus en pair-à-pair.

afnic

Chaînes privées ?

- Chaîne où tout le monde ne peut pas écrire (et où parfois tout le monde ne peut pas lire),

Chaînes privées ?

- Chaîne où tout le monde ne peut pas écrire (et où parfois tout le monde ne peut pas lire),
- Un thème très *hype* (surtout chez les startupeurs disruptifs),

Chaînes privées ?

- Chaîne où tout le monde ne peut pas écrire (et où parfois tout le monde ne peut pas lire),
- Un thème très *hype*,
- À quoi sert une chaîne de blocs dans ce cas ? N'importe quelle base de données ferait mieux.

Chaînes privées ?

- Chaîne où tout le monde ne peut pas écrire (et où parfois tout le monde ne peut pas lire),
- Un thème très *hype*,
- À quoi sert une chaîne de blocs dans ce cas ? N'importe quelle base de données ferait mieux.
- À la rigueur, une chaîne en lecture seule pour le public peut avoir un sens (elle reste vérifiable par tous).

afnic

Chaînes privées ?

- Chaîne où tout le monde ne peut pas écrire (et où parfois tout le monde ne peut pas lire),
- Un thème très *hype*,
- À quoi sert une chaîne de blocs dans ce cas ? N'importe quelle base de données ferait mieux.
- À la rigueur, une chaîne en lecture seule pour le public peut avoir un sens.
- À la rigueur, une chaîne « semi-privée » (pas accessible au public mais pas non plus un seul acteur) peut avoir un sens.

afnic

Enjeux et risques

Enjeux et risques

- Qui dit cryptographie dit clé secrète :

Enjeux et risques

- Qui dit cryptographie dit clé secrète :
  - Ne pas la perdre,

Enjeux et risques

- Qui dit cryptographie dit clé secrète :
  - Ne pas la perdre,
  - Faire en sorte qu'elle ne soit pas copiée.

Enjeux et risques

- Qui dit cryptographie dit clé secrète :
  - Ne pas la perdre,
  - Faire en sorte qu'elle ne soit pas copiée.
- Les bogues dans la chaîne (quel recours si je perds 100 cryptobrouzoufs suite à une bogue ?),

Enjeux et risques

- Qui dit cryptographie dit clé secrète :
  - Ne pas la perdre,
  - Faire en sorte qu'elle ne soit pas copiée.
- Les bogues dans la chaîne,
- Les bogues dans les contrats automatiques (plusieurs cas célèbres comme The_DAO).

afnic

Enjeux et risques

- Qui dit cryptographie dit clé secrète :
  - Ne pas la perdre,
  - Faire en sorte qu'elle ne soit pas copiée.
- Les bogues dans la chaîne,
- Les bogues dans les contrats automatiques.
- La question du **recours** est cruciale.

afnic

Applications possibles de la chaîne de blocs

Applications possibles de la chaîne de blocs

- La monnaie, bien sûr (le grand succès des chaînes de blocs),

Applications possibles de la chaîne de blocs

- La monnaie, bien sûr,
- Les preuves d'antériorité (on met un condensat cryptographique signé d'un document dans la chaîne),

Applications possibles de la chaîne de blocs

- La monnaie, bien sûr,
- Les preuves d'antériorité,
- La gestion de noms (identités, noms de domaine), les enregistrer, les utiliser,

afnic

Applications possibles de la chaîne de blocs

- La monnaie, bien sûr,
- Les preuves d'antériorité,
- La gestion de noms, les enregistrer, les utiliser,
- La vente d'électricité auto-produite ? (Attention, il faudra un oracle.)

afnic

Spécifiques aux collectivités locales

la gazette.fr

NUMÉRIQUE

Expérimentation de la blockchain dans les collectivités : quelles possibilités ?

Publié le 31/10/2017 • Par Gabriel Zignani • dans : France

Déjà expérimentée par certaines administrations centrales, la blockchain devrait prochainement l'être dans les collectivités territoriales. Une table ronde a été organisée le 26 octobre dernier pour débattre des possibilités les plus intéressantes.

SUR LE MÊME SUJET

Pourquoi les collectivités
de la digitalisation du dro

Les effets de la blockchai
services juridiques des co

Spécifiques aux collectivités locales

- Les paiements : les collectivités locales peuvent-elles payer en bitcoins ?

Spécifiques aux collectivités locales

- Les paiements : les collectivités locales peuvent-elles payer en bitcoins ?
- Le vote : tout dépend de s'il doit être secret ou pas. . .

Spécifiques aux collectivités locales

- Les paiements : les collectivités locales peuvent-elles payer en bitcoins ?
- Le vote : tout dépend de s'il doit être secret ou pas. . .
- Le cadastre : plus besoin de notaires ?

afnic

Le vote

[Communiqué de presse d'Orange]

24.01.18

L'un des symboles de la démocratie, c'est l'acte de voter. Mais le taux d'abstention peut, parfois, s'avérer très élevé. Face à cet enjeu, Le Vote, un service de la Civic Tech créé par Orange, apporte une solution intéressante. Elle se compose d'un site web pour les élus et d'une application mobile pour les citoyens. Fondée sur la technologie blockchain, cette innovation est déjà utilisée par un certain nombre de municipalités. A découvrir...

Le vote

- Technique possible : chacun vote en signant une transaction, inscrites dans la chaîne, elles sont vérifiables,

Le vote

- Technique possible : chacun vote en signant une transaction, inscrites dans la chaîne, elles sont vérifiables,
- Si le vote n'a pas besoin d'être secret, c'est parfait (à part la difficulté de prouver la sécurité du système),

Le vote

- Technique possible : chacun vote en signant une transaction, inscrites dans la chaîne, elles sont vérifiables,
- Si le vote n'a pas besoin d'être secret, c'est parfait,
- Si le vote doit être secret, il n'y a pas de solution (c'est l'escroquerie du vote électronique).

Le cadastre

- Un cadastre est un registre, et la chaîne de blocs est bien adaptée à la tenue de registres,

Le cadastre

- Un cadastre est un registre,
- Technique possible : les achats et ventes de terrain se font via un contrat automatique,

Le cadastre

- Un cadastre est un registre,
- Technique possible : les achats et ventes de terrain se font via un contrat automatique,
- Le cadastre dans la chaîne serait ainsi toujours à jour et vérifiable,

Le cadastre

- Un cadastre est un registre,
- Technique possible : les achats et ventes de terrain se font via un contrat automatique,
- Le cadastre dans la chaîne serait ainsi toujours à jour et vérifiable,
- Des politiques comme la préemption peuvent être ajoutées au contrat,

Le cadastre

- Un cadastre est un registre,
- Technique possible : les achats et ventes de terrain se font via un contrat automatique,
- Le cadastre dans la chaîne serait ainsi toujours à jour et vérifiable,
- Des politiques comme la préemption peuvent être ajoutées au contrat,
- Il faut un cadastre fiable au début : ce n'est pas une solution pour les pays sans cadastre (projet fréquemment mis en avant par certains médias, tantôt au Ghana, tantôt au Honduras),

afnic

Le cadastre

- Un cadastre est un registre,
- Technique possible : les achats et ventes de terrain se font via un contrat automatique,
- Le cadastre dans la chaîne serait ainsi toujours à jour et vérifiable,
- Des politiques comme la préemption peuvent être ajoutées au contrat,
- Il faut un cadastre fiable au début : ce n'est pas une solution pour les pays sans cadastre,
- Excellente solution pour dynamiser un projet *open data* : racontez que c'est une *blockchain*.

afnic

Initialisation du cadastre

Record Land Data

Use this form to record land data that you own

*Required

What is your first name? *

Your answer

What is your last name? *

Your answer

What type of land is this? *

- ○ Residential
- ○ Business
- ○ Public
- ○ Government
- ○ Other:

GPS Latitude Coordinate *

Your answer

GPS Longitude Coordinate *

Conclusion

Pour en savoir plus : le dossier thématique de l'AFNIC
`http://urlz.fr/7dLu`

Conclusion

Pour en savoir plus : le dossier thématique de l'AFNIC
`http://urlz.fr/7dLu`

- La chaîne de blocs, c'est bien. Vraiment.

afnic

Conclusion

Pour en savoir plus : le dossier thématique de l'AFNIC
`http://urlz.fr/7dLu`

- La chaîne de blocs, c'est bien. Vraiment.
- Cela permet des vraies nouveautés, par exemple dans le domaine financier.

afnic

Conclusion

Pour en savoir plus : le dossier thématique de l'AFNIC
`http://urlz.fr/7dLu`

- La chaîne de blocs, c'est bien. Vraiment.
- Cela permet des vraies nouveautés, par exemple dans le domaine financier.
- Mais ce n'est pas une solution à tout.

afnic

Conclusion

Pour en savoir plus : le dossier thématique de l'AFNIC
`http://urlz.fr/7dLu`

- La chaîne de blocs, c'est bien. Vraiment.
- Cela permet des vraies nouveautés, par exemple dans le domaine financier.
- Mais ce n'est pas une solution à tout.
- Et cela ne résoud pas les problèmes politiques. (Ne faisons pas de solutionnisme.)

afnic

Merci !

www.afnic.fr
contact@afnic.fr