DE LA RECHERCHE À L'INDUSTRIE

cea

Blockchain : quelles réalités au-delà du phénomène du bitcoin ?

Contact réalisation SBEM : CEA/DRT/VALO/SBEM

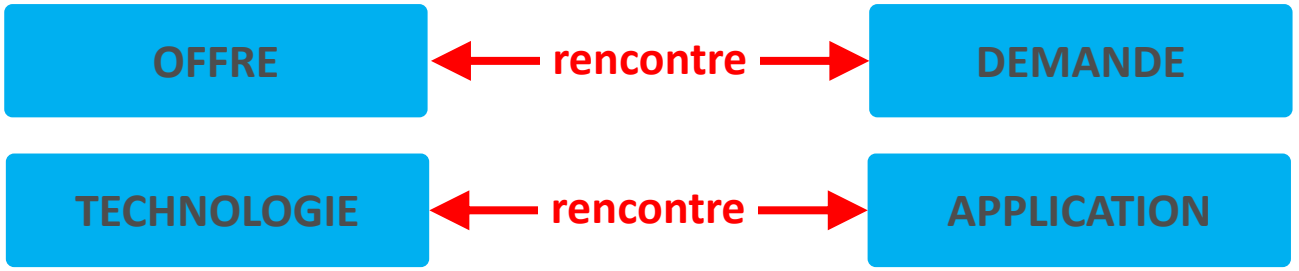
Eric Bévillard | T. +33 (0)4 38 78 23 66 | eric.bevillard@cea.fr

Sébastien Guinard | T. +33 (0)4 38 78 65 13 | sebastien.guinard@cea.fr

Drtq/DValo/SBEM-FO26a – 30/04/2015 - Document lié aux indicateurs qualité DRT/VALO/SBEM - toute nouvelle édition annule et remplace l'édition précédente.

www.cea.fr

Les études de marché faites au CEA en 1 coup d'œil



Y a-t-il des technologies en cours de développement au CEA qui puissent répondre à une demande - TECHNO PUSH ?

Quelles sont les technologies à développer au CEA pour répondre à une demande - MARKET PULL ?

Application aux blockchains
« Phénomène 2016/2017 »

NOTRE POINT DE VUE & NOS LIMITES

- Nous ne sommes pas des experts des blockchains mais nous sommes plongés dans cet univers depuis 9 mois et avons échangé avec une trentaine d'acteurs du domaine.
- Aujourd'hui, nous vous présentons une partie de nos analyses : qu'elles soient un solide point de départ pour mener vos propres réflexions !

9 mois de veille

30 entretiens avec des experts

Quelques réunions

Partage de quelques analyses
=
Votre point de départ

Qu'est ce qu'une blockchain ?

Pourquoi est-ce révolutionnaire ?

Au-delà du buzz, où en est-on aujourd'hui
et où en sera-t-on, peut-être, dans 10 ans ?

Quels sont les sujets de recherche potentiels associés ?

Vos questions et nos tentatives de réponses

UNE BLOCKCHAIN PERMET A DES ACTEURS D'ÉCHANGER ET D'ARCHIVER DES INFORMATIONS SANS INTERVENTION D'UN TIERS DE CONFIANCE PRÉDÉSIGNÉ

Une blockchain s'appuie sur un protocole d'échange…

« Etant donné au moins 2 acteurs, A et B, si A veut échanger avec B de l'information dans un format numérique, alors cet échange et son archivage se feront selon les modalités suivantes… »

… fonctionnant avec une double assise technologique

- Technologies de cryptographie
- Technologies des réseaux informatiques distribués

➢ **A un maillon de la chaine, est associé un bloc contenant N fois : « qui est l'émetteur / qui est le récepteur / quelle est l'information échangée »**

Bloc schématique

Emetteur	*Récepteur*	*Echange*
N° 1	N° 5 432	Bla bla bla
N° 765	N° 23	Tchache
…	…	…

Ce cas constitue un exemple simplifié de fonctionnement d'une blockchain ; d'autres modes de fonctionnement existent...

➢ **Seul le gagnant d'un jeu mathématique est autorisé à accrocher un nouveau maillon à la chaine existante ; en plus de cette autorisation il va gagner une récompense (token).**

1 énigme mathématique
(fonction de hachage cryptographique)

1 seul gagnant : le plus rapide
tous les acteurs de la blockchain participent

2 lots

- **Un honneur : le droit d'accrocher le dernier maillon**
- **Une valeur : le token, qui l'incite à participer au jeu**

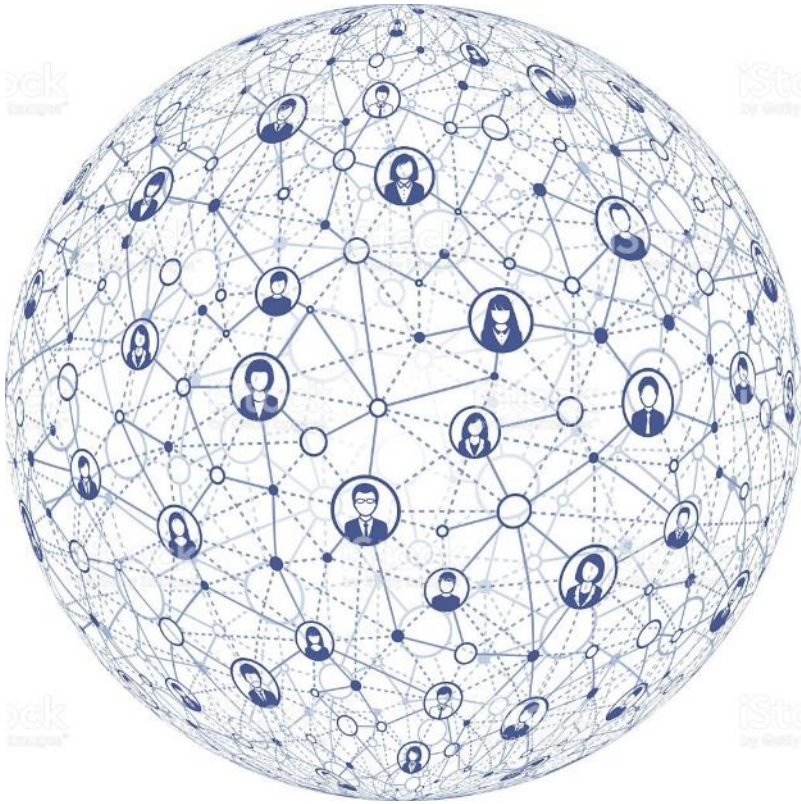
Ce cas constitue un exemple simplifié de fonctionnement d'une blockchain.

- **A chaque fois qu'un nouveau maillon a été accroché, de nombreuses copies de la chaine « allongée » sont faites et distribuées sur le réseau informatique des acteurs de la blockchain**

Si 1 maillon en plus :

Alors plein de copies

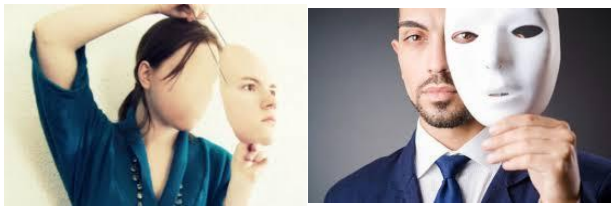
sont distribuées sur le réseau



Ce cas constitue un exemple simplifié de fonctionnement d'une blockchain.

➢ **La sécurité induite par la blockchain est alors extrêmement forte !**

La cryptographie garantit l'identité de l'émetteur et du récepteur



Chaque participant au jeu peut gagner : personne n'est en position centrale d'abus de pouvoir

Le jeu mathématique est conçu pour rendre très difficile le changement de l'un des maillon sans qu'il ne casse toute la chaîne

Changer un maillon dans la chaîne implique de changer également toutes les copies pour ne pas se faire repérer

« encore et encore »

Ce cas constitue un exemple simplifié de fonctionnement d'une blockchain.

➢ **Il convient de parler « des » blockchains » car il en existe de très nombreuses déclinaisons ; chaque blockchain est unique et voit son mode de fonctionnement décrit dans un protocole qui lui est propre**

Piochez dans toutes les options suivantes pour créer une blockchain unique !

Les acteurs afférents à la blockchain sont-ils connus à l'avance ?

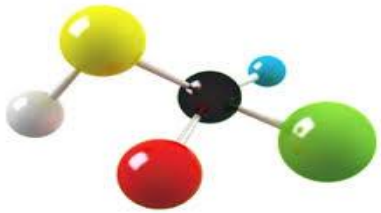
La blockchain permet-elle l'exécution automatique d'actions prédéfinies ?

Y a-t-il échange de valeur par le biais d'une cryptomonnaie ?

…

Technologies de cryptographie
- *Option 1*
- *Option 2*
- *Option 3…*

Technologies des réseaux informatiques distribués
- *Option 1*
- *Option 2*
- *Option 3…*



*Capture d'écran d'une partie du protocole de la blockchain du bitcoin**

*. https://fr.wikipedia.org/wiki/Bitcoin

Qu'est ce qu'une blockchain ?

Pourquoi est-ce révolutionnaire ?

Au-delà du buzz, où en est-on aujourd'hui
et où en sera-t-on dans 10 ans ?

Quels sont les sujets de recherche potentiels associés ?

Vos questions et nos tentatives de réponses

TOUT EN UN !

(la spécificité tient au cumul des avantages)

Offre une vision partagée d'un historique d'échanges d'information

+

Offre un historique infalsifiable

+

Ne fait pas intervenir de tiers de confiance préalablement désigné

+

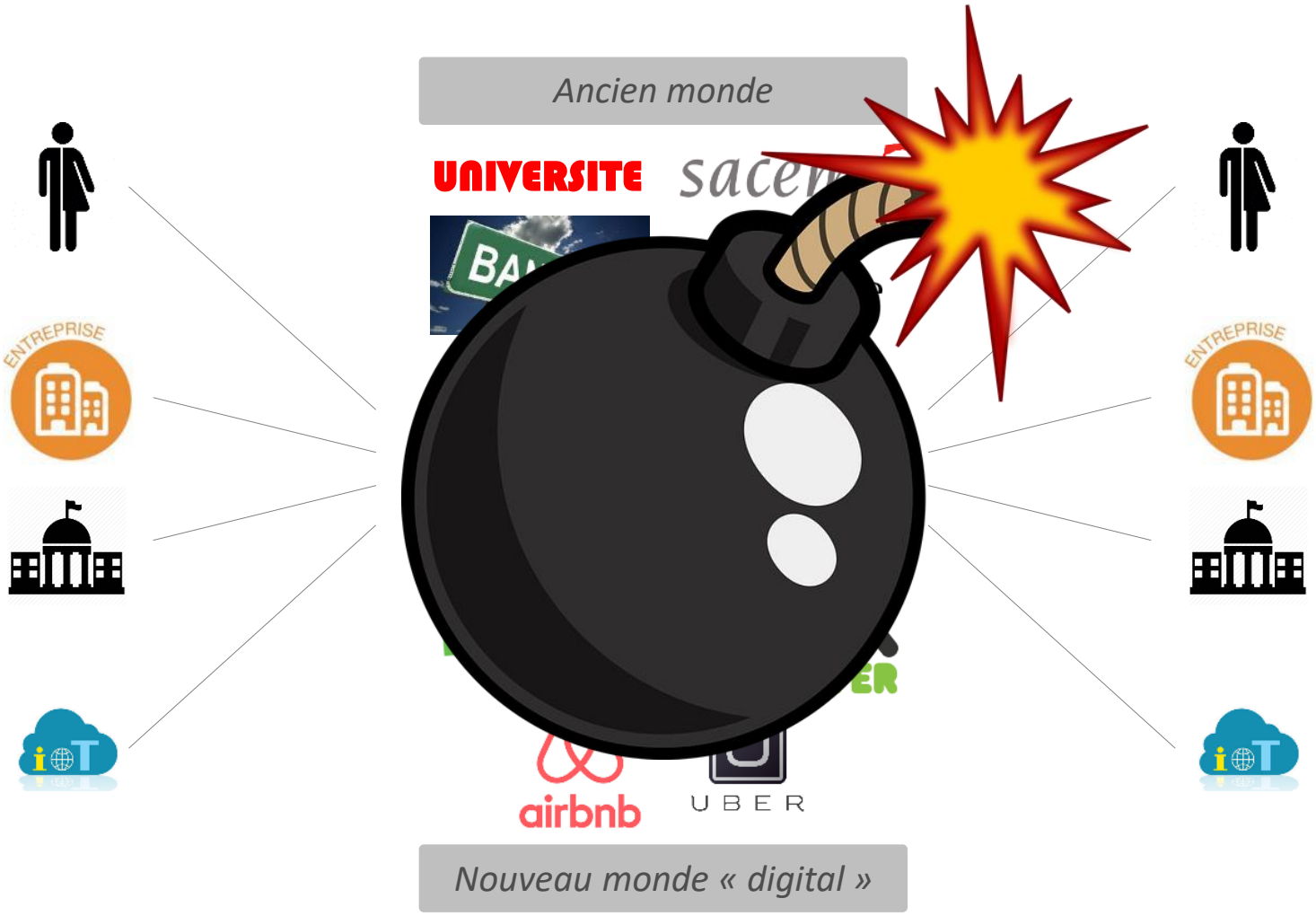
Abaisse les coûts liés à l'archivage et à l'échange d'information

+

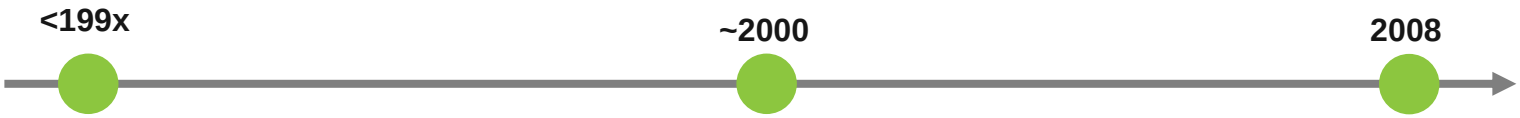
Permet l'exécution automatique de contrats

LÀ AU BON MOMENT

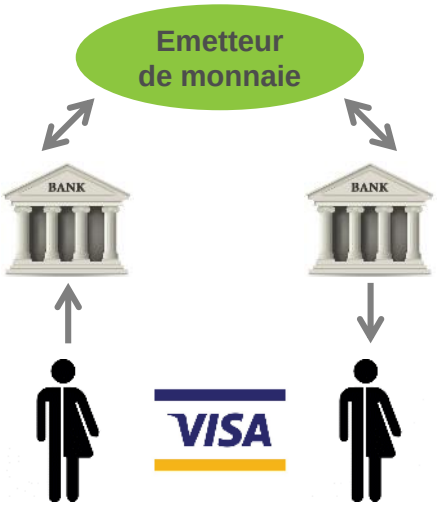
- **En cas d'utilisation généralisée des blockchains, les tiers de confiance qui sont systématiquement associés à tous les échanges d'information pourraient tout simplement disparaitre**



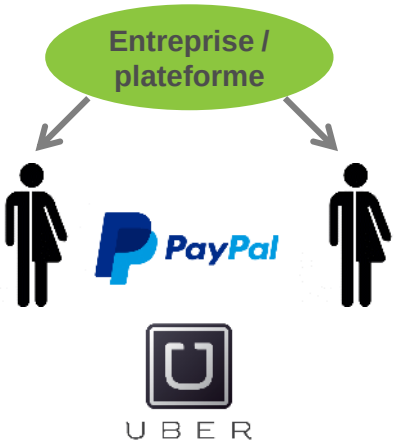
Schématisation des différents modèles d'échanges et d'archivage d'information



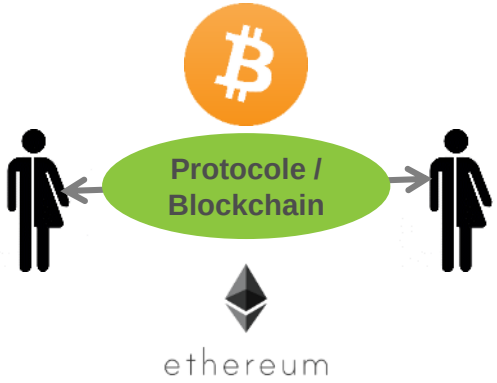
Modèle ADMINISTRATIF
1/3 de confiance
= ETAT



Modèle INTERNET
1/3 de confiance
= ENTREPRISE



Modèle BLOCKCHAIN
1/3 de confiance
= PROTOCOLE ET COMMUNAUTE



Qu'est ce qu'une blockchain ?

Pourquoi est-ce révolutionnaire ?

Au-delà du buzz, où en est-on aujourd'hui et où en sera-t-on dans 10 ans ?

Quels sont les sujets de recherche potentiels associés ?

Vos questions et nos tentatives de réponses

2016-2018

UNE EUPHORIE SUR LA BLOCKCHAIN

NOMBRE DE CRYPTOMONNAIES

1 en 2009, 28 en 2014, 1 384 au 7 janvier 2018

NOMBRE D'ICO *(Initial Coin Offering)*

50 pour tout l'année 2016, plus de 50 par mois en ce début 2018

FONDS LEVÉS VIA LES ICO

100 M$ en 2016 / 3 Mds$ en 9 mois en 2017

2016-2018

➢ **Pourtant, force est de constater que l'on est très loin d'un déploiement à grande échelle des blockchains**

La percée réelle des blockchains perçue au travers de nos entretiens

2017 EST L'ANNÉE OÙ LES ENTREPRISES EXPÉRIMENTENT
(preuve de concept : POC)

LA COMPRÉHENSION SUR LES BLOCKCHAINS EST FAIBLE

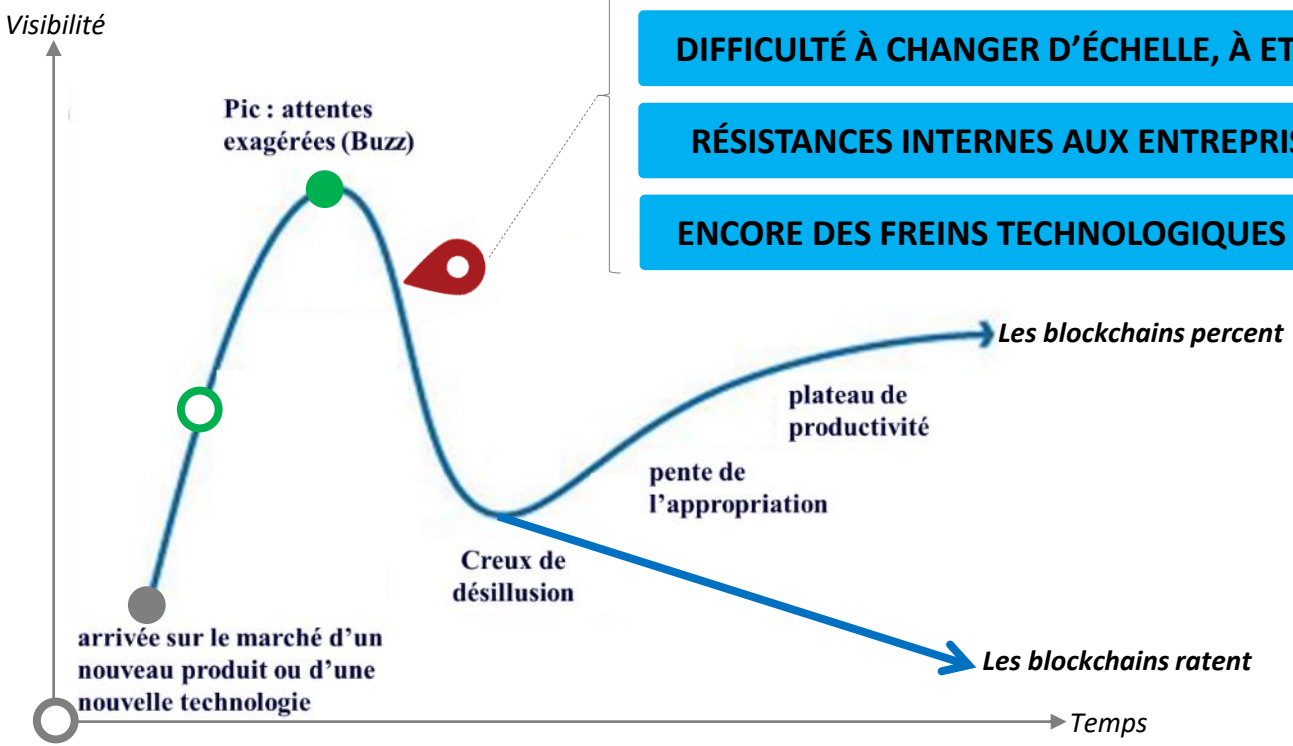
LES ÉQUIPES SONT SOUVENT TRÈS PETITES

IBM

« En décembre 2016, parmi quelque 300 expérimentations lancées sur Hyperledger, une seule était entrée en phase d'industrialisation »

2016-2018

Les blockchains sur la courbe de Gartner



DÉCEPTION = ESPÉRANCE / RÉALITÉ

- **PAS LA MEILLEURE SOLUTION POUR CERTAINES POC**
- **DIFFICULTÉ À CHANGER D'ÉCHELLE, À ETRE DÉPLOYÉE**
- **RÉSISTANCES INTERNES AUX ENTREPRISES : SI & RH**
- **ENCORE DES FREINS TECHNOLOGIQUES IMPORTANTS**

< 2008
Dév. Techno. PtoP & crypto

2008
Publication du Protocole Bitcoin

~ 2015
1ers intérêts industriels les banques ; Ethereum

2017
Multiples POC et marques d'intérêt

Dans 5, plutôt 10 ans?

LES BLOCKCHAINS SERONT D'ABORD UTILISÉES POUR AMÉLIORER DES PROCESSUS

UTILISATION DE BLOCKCHAINS PRIVÉES…

… POUR ACCOMPAGNER LA DIGITALISATION DE PROCESSUS…

… D'ABORD SUR DES PETITS PROCESSUS POUR MAITRISER LA TECHNOLOGIE ET SON DÉPLOIEMENT

Dans 5, plutôt 10 ans?

	FINANCE	ASSURANCE	LOGISTIQUE
applications	▪ Le know your customer ▪ Le swap de taux d'intérêt ▪ Le trade finance ▪ La gestion de titre (obligation…) ▪ Le plus utopique: payement	▪ Automatisation par contrats intelligents ▪ Détection de fraude plus facile ▪ Augmentation de l'efficacité des prix ▪ Réduction des coûts administratifs	▪ Traçage des flux et des acteurs associés ▪ Améliorer la confiance en rendant infalsifiable le flux des marchandises ▪ Automatisation par contrats intelligents *(des pièces s'achèteraient toutes seules)*
	DIGITALISATION DU BACK-OFFICE	**MICRO-ASSURANCE ENFIN POSSIBLE** **Gestion du contrat qui passe de 1,5/4€ à 0,4€**	**AMÉLIORATION DE L'EFFICACITÉ OPERATIONNELLE**
Économie annuelle	**80 à 110 Mds$**	**5 à 10 Mds$**	**> 100 Mds$**

Dans 10 ans ?

RUPTURE MAJEURE ?

LES BLOCKCHAINS PORTENT EN ELLES LES GERMES D'UN MONDE RADIALEMENT DIFFÉRENT

CTO d'une banque centrale

« Au début elle sera utilisée pour améliorer des processus, et je pense qu'à terme de nouveaux acteurs vont totalement transformer le monde bancaire grâce à cette technologie »

IoT & blockchains

QUESTION : PEUT-ON ENVISAGER L'AVÈNEMENT DE L'IOT SANS :

- **CONFIANCE**
- **GESTION DE L'IDENTITÉ**
- **RESPECT DE LA VIE PRIVÉE ET DE LA CONFIDENTIALITÉ DES DONNÉES**
- **PORTEFEUILLE AUX OBJETS…**

Portefeuille

Smart contract

Authentification / Archivage

LES BLOCKCHAINS : DES SOLUTIONS ?

Energie & blockchains

QUESTION : PEUT-ON ENVISAGER L'ÉNERGIE DE DEMAIN SANS :

- **CONFIANCE**
- **UNE GESTION DE CONTRATS COMPÉTITIVE**
- **TENUE DES REGISTRES DE CERTIFICATS D'AUTHENTICITÉ POUR L'ÉLECTRICITÉ VERTE OU D'ATTESTATIONS DE QUOTAS DE CO2**
- **UNE GESTION DE COMMUNAUTÉ AUTO-SUFFISANTE**
- **PEER TO PEER TRADING**

Ma Facture énergétique dans le futur

J'ACHETE

- **De l'énergie à EDF : 128 €**
- **De l'énergie certifiée verte à une association : 35 greencoins**

JE VENDS

- **De l'énergie solaire à un voisin : 12 solarcoins**
- **Le surplus d'énergie de ma voiture à ma commune : 5 batteriecoins**

LES BLOCKCHAINS : DES SOLUTIONS ?

Qu'est ce qu'une blockchain ?

Pourquoi est-ce révolutionnaire ?

Au-delà du buzz, où en est-on aujourd'hui
et où en sera-t-on dans 10 ans ?

Quels sont les sujets de recherche potentiels associés ?

Vos questions et nos tentatives de réponses

IL Y A ENCORE BEAUCOUP À FAIRE SUR LES BLOCKCHAINS

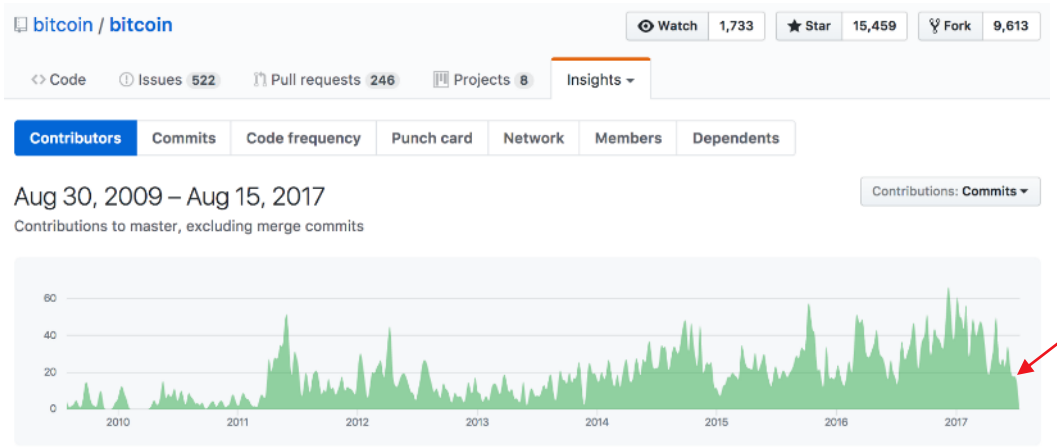
Peu d'experts ou d'équipes comprennent en détail leur fonctionnement
CRYPTO. + RÉSEAU + APPLI. + ÉCO. + JURIDIQUE…

Cette communauté est diluée sur les nombreuses blockchains crées

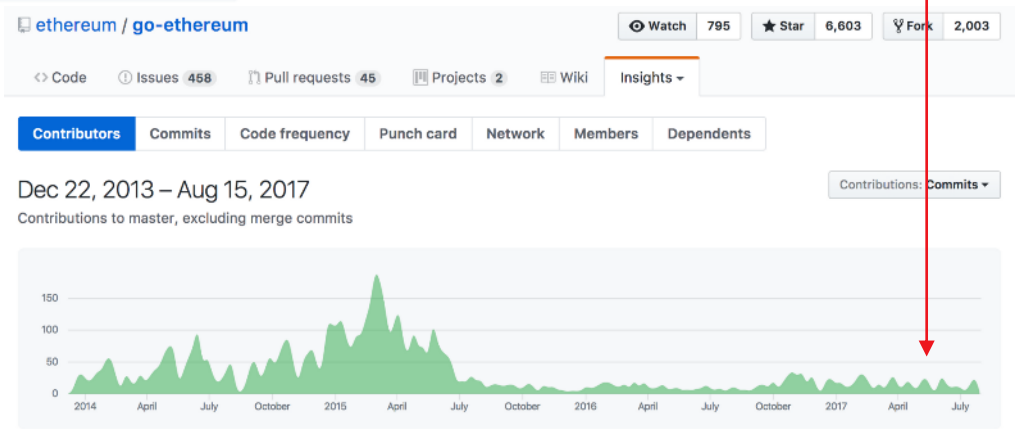
La plus mature, celle du bitcoin, « ne serait qu'à TRL 5 ou 6 »

**. C'est le niveau TRL attribué par les scientifiques interrogés lors de l'étude. L'idée est là, même si on peut noter que cette évaluation est partiellement erronée vis-à-vis de la définition exacte du niveau car le bitcoin n'est mis en œuvre ni dans un laboratoire, ni dans un environnement simulé*
(« TRL 6 : Démonstration du modèle système / sous-système ou du prototype dans un environnement significatif. Le modèle ou le système prototype représentatif (bien au-delà de l'artefact testé en TRL 5) est testé dans un environnement significatif. Il représente une avancée majeure dans la maturité démontrée d'une technologie. Les exemples incluent le test d'un prototype dans un laboratoire "haute fidélité" ou dans un environnement opérationnel simulé ».)

La communauté travaillant réellement sur les protocoles des blockchains se compte presque sur les doigts d'une main !



Moins de 20 contributeurs !



https://medium.com/@FEhrsam/funding-the-evolution-of-blockchains-87d160988481

QUELQUES LIMITES DE LA BLOCKCHAIN DU BITCOIN

parmi d'autres !

Le temps de validation d'un bloc est de 10 minutes et une transaction est considérée comme validée si elle est enfouie sous 6 blocs, soit 1h00.
Sacré temps de passage en caisse !

Des tiers de confiance réapparaissent de facto

- **6 sociétés chinoises remportent le jeu 3 fois sur 4**
- **1 société chinoise leur fournit l'essentiel du matériel informatique**

En 2014 déjà, la consommation du réseau du bitcoin était probablement de l'ordre de grandeur de la consommation électrique d'un pays comme l'Irlande, soit environ 3 GW !

Karl J. O'Dwyer et David Malone, Bitcoin Mining and its Energy Footprint, 2014 ; attention toutes les estimations de consommation sont fragiles !
Blockchain.info ; https://blockchain.info/fr/pools
IEEE Spectrum ; https://spectrum.ieee.org/computing/networks/why-the-biggest-bitcoin-mines-are-in-china

ANALYSER LES BLOCKCHAINS EN TANT QUE « SYSTÈME »

- *Comment décrire les blokchains avec un même référentiel ?*
- *Comment les comparer les unes aux autres ?*
- *Quels sont les avantages des technologies retenues et du protocole associé ? en regard, quelles en sont les limites ?...*

DÉTECTER AUTOMATIQUEMENT DES FAILLES DANS LES PROTOCOLES ET LES SMART CONTRATS

« CODE IS LAW »
(Lessig ; 2000)

DÉVELOPPER DES COMPOSANTS SPÉCIALISÉS SUR LE MINAGE

- *Les composants utilisés pour gagner le jeu mathématique sont de plus en plus puissants et optimisés : CPU, GPU, FPGA, ASIC…*
- *Aujourd'hui, Bitmain a développé l'ASIC le plus performant et équipe les plus grosses fermes de minage. Quels seront les leaders demain ?*

**. Mineur : désigne un participant au jeu mathématique ; engage parfois des moyens informatiques conséquents afin de maximiser leur chance de gagner*