



Bitcoin: It's Alive!

Un organisme vivant ?



Sosthène



www.sosthene.net



contact@sosthene.net



[@Sosthene__](https://twitter.com/Sosthene__)



[@Sosthene@bitcoinhackers.org](https://masto.host/@Sosthene@bitcoinhackers.org)

23AA B267 CA6A B731 DCD1 4254 014A 7F46 6A0E EE28

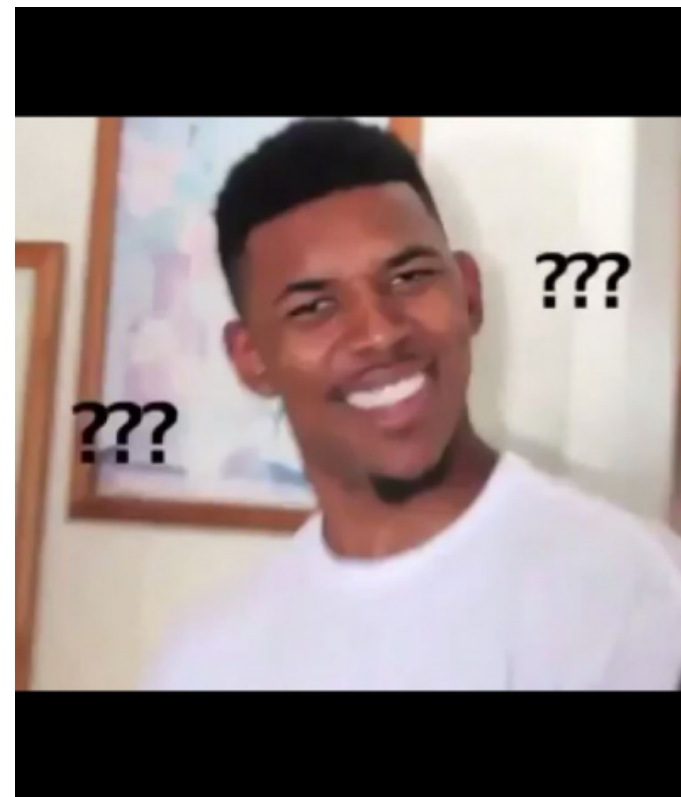
MON IDÉE DE LA LIBERTÉ. — La valeur d'une chose réside parfois non dans ce qu'on gagne en l'obtenant, mais dans ce qu'on paye pour l'acquérir, — dans ce qu'elle coûte.

Nietzsche

Qu'est-ce que Bitcoin ?

Qu'est-ce que Bitcoin ?

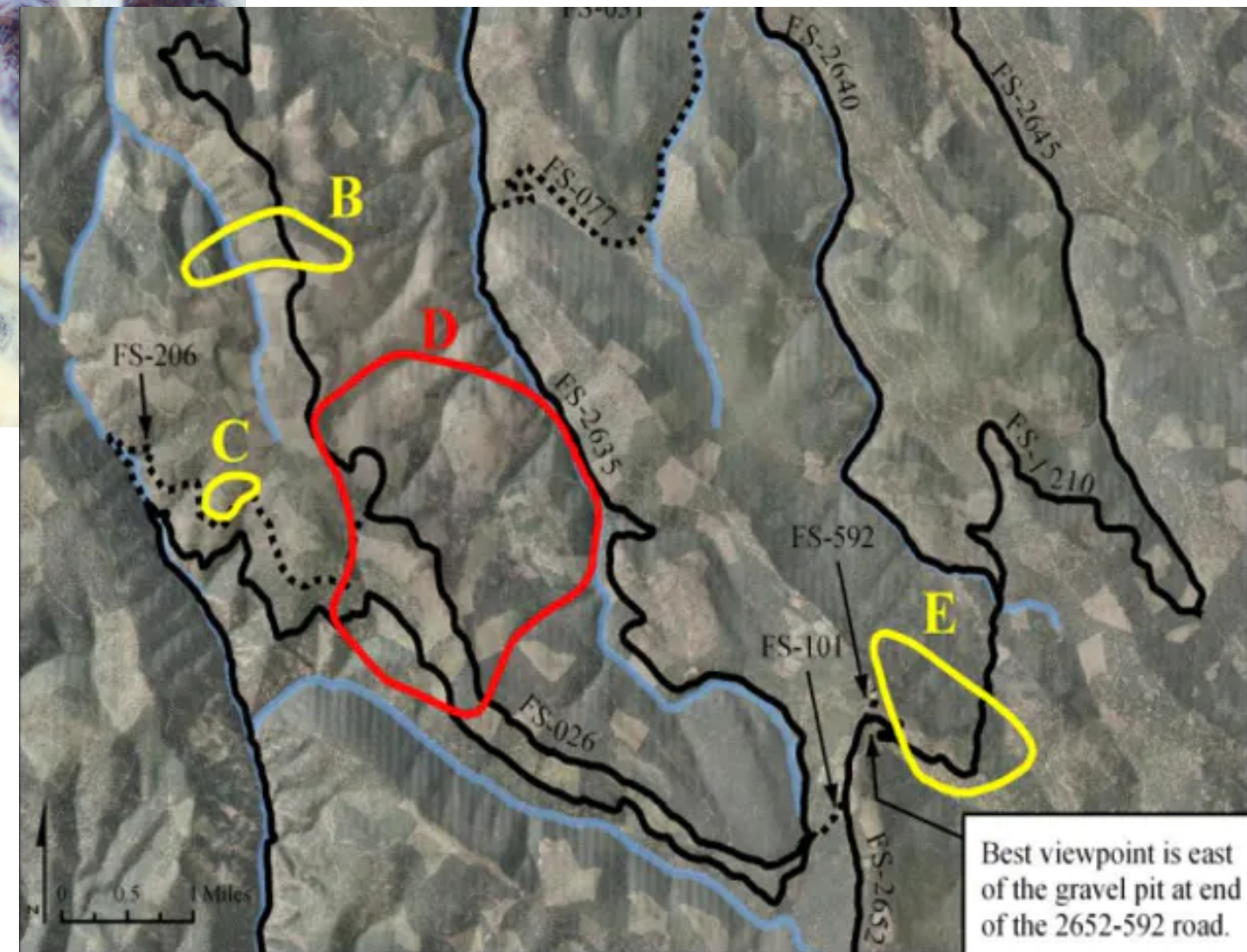
- La blockchain ?
- Une monnaie ?
- De l'or numérique ?
- Du code ?
- Une idée ?
- ...un champignon ?



Pourquoi un champignon ?

...ou plutôt un *fungus*. Les fungi appartiennent à un règne à part (ce ne sont pas des végétaux), et présentent des caractéristiques qu'on attribue souvent à Bitcoin :

- Décentralisation : un réseau souterrain, le *mycelium*, sans SPOF
- Échange permanent avec son environnement : les fungi sont en symbiose avec certains êtres vivants et en concurrence avec d'autres pour les ressources disponibles.
- Anti-fragilité : les fungi sont capables de transformer chimiquement les ressources dont ils disposent et de s'adapter à leur environnement. Ils ont ainsi survécu aux 5 dernières grandes extinctions.



Croissance par cycles

L'activité d'un fungus est la plupart du temps souterraine et invisible, et les seules manifestations visibles à la surface sont les éruptions soudaines des champignons qui jouent le rôle d'organes reproducteurs.

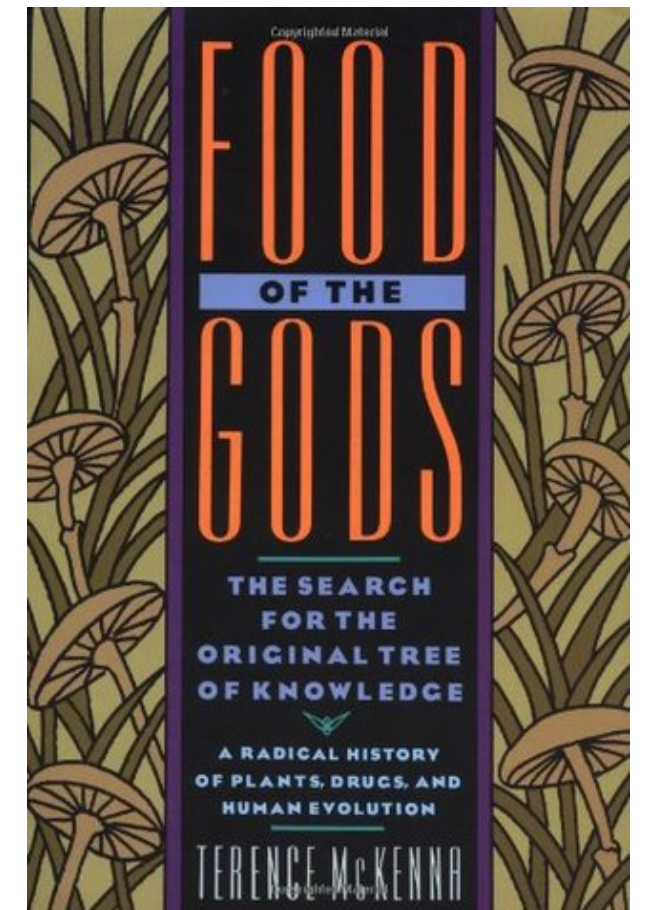
De la même façon l'activité de Bitcoin est très nettement distincte entre la surface (le prix et son explosion spectaculaire et soudaine) et toute l'activité de développement et de réflexion qui est plus importante mais cachée.



Les champignons sont nos amis

Nous avons aujourd'hui un certain nombre de preuves que les champignons faisaient partie de l'alimentation de nos ancêtres paléolithiques, ou peut-être même encore plus tôt !

Il existe en effet une théorie dite du "singe défoncé" (*Stoned Ape*), selon laquelle nous descendrions de primates ayant consommés des psylocibes hallucinogènes qui leur auraient conféré (à faible dose) un avantage évolutif.



Une symbiose entre l'humain et la technologie

L'analogie avec le fungus attire notre attention sur un point très important, Bitcoin se distingue des autres technologies en étant dans une relation d'influence réciproque avec ses utilisateurs :

- Bitcoin lui-même est défini et redéfini en permanence par le code que choisissent d'exécuter les utilisateurs
- et il exerce en retour une influence très importante sur les plus zélés d'entre-eux (modification des comportements économiques), mais aussi sur d'autres humains exposés moins directement (avez-vous remarqué ? On dit "Monnaie fiat" dans les média mainstream désormais)

Pourquoi Bitcoin ?

Société de coercion vs société libre

Les progrès technologiques et l'apathie politique réduisent rapidement la possibilité pour les individus de ne pas être identifiés (et donc contrôlé) en permanence dans toutes leurs actions :

- Reconnaissance faciale d'abord dans les aéroports, bientôt dans tous les endroits publics
- Enregistrement de données biométriques sur l'ensemble des populations
- Omniprésence du système bancaire, guerre contre le cash
- En ligne : transformation d'internet en "intranets" contrôlés au mieux par une poignée d'entreprises, au pire par un état totalitaire

La monnaie fiat, catalyseur du totalitarisme

Les conséquences économiques (inflation) de la monnaie fiat sont largement discutées, mais elle a aussi des impacts politiques majeurs.

En permettant aux États d'emprunter sans aucune limite, le système monétaire actuel leur a permis de prendre un poids économique et social de plus en plus important.

L'un des points communs des différents totalitarismes est une monnaie totalement soumise aux caprices du politique.

Aujourd'hui, une guerre généralisée contre le cash est en train de se mettre en place de l'Europe à la Chine.

Bitcoin, instrument de la crypto anarchie

*Crypto anarchy is the cyberspatial realization of **anarcho-capitalism**, transcending national boundaries and freeing individuals to **consensually** make the economic arrangement they wish to make.*

Tim May

Les valeurs de la crypto anarchie

- Les individus ont tous des droits fondamentaux (liberté, propriété etc) qui doivent être inconditionnellement respectés (pas de "raison d'État")
- L'appartenance à une communauté ou à une organisation politique doit être librement consentie par chaque individu
- La confidentialité et l'anonymat font partie des droits fondamentaux de chaque individu ("J'ai le choix de révéler ou non aux personnes de mon choix les informations me concernant")

Les armes de la crypto anarchie

- La cryptographie, et en particulier la cryptographie asymétrique
- Technique purement défensive :
 - anonymat
 - non attribution
 - identité
- Adaptation aux enjeux de l'essor d'une société de l'information à la fin du XXe siècle
- Pour permettre une défense efficace, il faut disposer au minimum d'un outil de communication, d'un outil d'identification et d'un outil monétaire

*Security and **cryptology** provide the ontological support for [the] cyberspatial worlds, for enduring structures that permit "**colonization**" of these spaces and structures.*

Tim May

Les objectifs de la crypto anarchie

- Supprimer autant que possible tout échange (information, marchandises, valeur...) exercé sous la contrainte. Tout échange doit être volontaire et consenti par les deux parties
- Neutraliser la force de coercition des États en s'attaquant à leur capacité à observer les actions des individus plus qu'à celle de contraindre physiquement les individus
- Créer les conditions pour l'émergence de communautés physiques ou virtuelles sur le fondement du volontariat et de la liberté

Une utopie ?

- En-dehors de ses quelques principes, la crypto anarchie n'implique pas d'opinions sur la plupart des sujets. Il ne s'agit pas de créer une société "parfaite".
- Au contraire, on favorise l'émergence d'une grande variété d'organisations régies par des règles et des valeurs différentes, et donc plus adaptables et anti-fragiles
- Ce n'est pas un absolu ! La crypto anarchie est un processus, elle peut être (et est déjà) partiellement, ou pas partout, coexister avec les États-Nations...

Bitcoin est vivant, parce que c'est "nous"

- Opinion impopulaire : Bitcoin est aujourd'hui plus proche de l'échec que de la réussite.
- La décentralisation dans Bitcoin signifie que chaque utilisateur est responsable de l'intégrité et de la survie du système. Bitcoin est anti-fragile, mais pour le tuer il suffit d'une mauvaise décision adoptée par tous les utilisateurs, par ignorance ou tromperie
- Un principe directeur : Bitcoin est un outil de souveraineté et d'autonomie, tout ce qui les renforce pour chacun va dans la bonne direction, toute décision qui restreint cette caractéristique est néfaste et doit être rejetée

Sources

- La série *Bitcoin is a Decentralized Organism (Mycelium)* de Brandon Quittem
- Le podcast *What is crypto anarchy?* de Frank Braun et Smuggler
- *True Nyms and Crypto Anarchy* de Tim May

Questions ?