**E = M x C\*\*N ;** **N→∞**

**Réflexion sur l’Indestructibilité de Bitcoin**

[Jean-Marie Choffray](https://www.amazon.com/kindle-dbs/entity/author/B00DNUGN64?_encoding=UTF8&node=283155&offset=0&pageSize=12&searchAlias=stripbooks&sort=author-sidecar-rank&page=1&langFilter=default#formatSelectorHeader)\*

Liège, le 10 avril 2024.

Dans cette courte note, j’expose pourquoi **Bitcoin** pourrait être indestructible, même si son évolution technique et sa diffusion opérationnelle connaîtront sans doute de nombreux et brutaux soubresauts – bonds et reculs aléatoires. Soit **M**, la *Masse* de sa capitalisation boursière – de l’ordre de $1,4 x 10\*\*12 aujourd’hui ; **C**, La *Croissance* des transactions transcrites – de l’ordre de 500 x 10\*\*3 transactions par jour ; et **N**, le *Nombre* de blocs – de l’ordre de 840 x 10\*\*3, chacun comportant en moyenne 3 x 10\*\*3 transactions. L’*énergie économique* **E** produite par le réseau **Bitcoin** peut être exprimée sous la forme : E = M x C\*\*N, N→∞. Dans la mesure ou le nombre de blocs (~ transactions) ne peut décroître du fait de l’irréversibilité du mécanisme de *Proof of Work*, cette *énergie économique* est potentiellement infinie ; la chaîne originelle (*base layer*) devenant une chaîne de chaînes (*successive layers*)… *ad infinitum*.

\* Professeur Ordinaire Honoraire d’Informatique Décisionnelle à l’Université de Liège.

PhD-77, Management Science, Massachusetts Institute of Technology.

*« Aucune force sur terre, à l’exception d’un manque*

*de volonté, ne peut arrêter Bitcoin ! »*

**E = M x C\*\*N ; N→∞**

**Réflexion sur l’Indestructibilité de Bitcoin**

Soit :

* **M**, la *Masse* correspondant à la capitalisation boursière de Bitcoin – de l’ordre de $1,4 x 10\*\*12 aujourd’hui,
* **C**, la *Croissance* des transactions transcrites – de l’ordre de 500 x 10\*\*3 par jour,
* **N**, le *Nombre* de blocs – de l’ordre de 840 x 10\*\*3, chacun comportant en moyenne 3 x 10\*\*3 transactions.
* E, l’*énergie économique* produite par le réseau **Bitcoin**.

La *Force* F de développement économique du réseau Bitcoin peut être exprimée par la relation suivante :

[1] F = M x C,

Et, l’*énergie économique* du système global devient (hors éventuel recours à l’endettement) :

[2] E = M x C\*\*N ; avec N→∞.

Dans la mesure où le nombre de blocs (comportant chacun ~ 3 x 10\*\*3 transactions) ne peut décroître du fait de l’irréversibilité du mécanisme de *Proof of Work*, l’*énergie économique* produite par Bitcoin est potentiellement infinie. La chaîne originelle (*base layer*) devient une chaîne de chaînes (*successive layers*)… *ad infinitum*. [Lightning](https://lightning.network/) et [Fedimint](https://fedimint.org/) constituent de bons exemples de chaînes secondaires. Quant à [Bitkey](https://bitkey.world/en-US), c’est véritablement l’équivalent conceptuel, dans l’écosystème Bitcoin, du premier [iPhone d’Apple](https://www.apple.com/newsroom/2007/01/09Apple-Reinvents-the-Phone-with-iPhone/). En théorie, seuls les utilisateurs de la chaîne initiale (*base layer*) pourraient être à l’origine de sa destruction, de sa « dématérialisation », en renonçant inconditionnellement aux *préceptes* (~ l’ADN de Bitcoin) encodés dans son *logiciel originel* (cf. [Satoshi Nakamoto](https://bitcoin.org/bitcoin.pdf)).

Accessoirement, cette dernière expression [2] constitue une « généralisation » de la célèbre formule d’Albert Einstein, dans le contexte d’une *dimensionalité* croissante, conséquence d’une réaction en chaînes hiérarchisées… *ad infinitum*.