



HAL
open science

Bitcoin : une monnaie dématérialisée

Pascal Lafourcade, Jean-Guillaume Dumas

► **To cite this version:**

Pascal Lafourcade, Jean-Guillaume Dumas. Bitcoin : une monnaie dématérialisée. Les Big Data à découvert, CNRS Editions, 2017. hal-02291296

HAL Id: hal-02291296

<https://hal.science/hal-02291296v1>

Submitted on 18 Sep 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

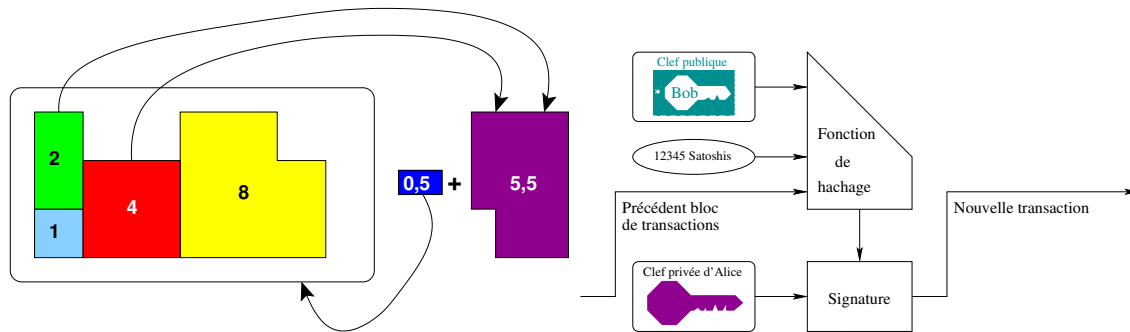


FIGURE 1 – Fonctionnement d’une transaction en Bitcoins, à gauche un portefeuille, à droite une partie de la chaîne.

3 Anonymat

Le modèle bancaire traditionnel garantit un certain degré d’anonymat en limitant l’accès aux informations de transactions aux seules parties intervenant dans la transaction et à leurs banques respectives. Au contraire, le modèle Bitcoin révèle publiquement toutes les transactions passées. Toutefois, une forme différente d’anonymat est préservée puisque l’identité des possesseurs des clefs publiques n’est pas nécessaire, seule une preuve de possession de la clef privée associée (la signature électronique de la transaction) est demandée. Le monde entier peut voir qu’un montant est transféré d’une clef publique à une autre, mais sans lien avec des personnes physiques ou morales. Cela ressemble au niveau d’information révélé par les bourses, quand les dates et tailles d’échanges individuels sont rendues publiques (le carnet d’ordres), mais sans révéler quelles étaient les parties impliquées.

Toutefois, pour Bitcoin, toutes les transactions d’une clef donnée sont liées, donc au moment où une personne entre ou sort du système Bitcoin (par exemple par un échange avec une autre monnaie) l’anonymat doit être levé, au moins auprès de l’organisme d’échange, et l’ensemble des transactions associées à cette clef peut alors être tracé.

4 Bitcoin un système monétaire

Le minage décentralisé, dans lequel n’importe quel agent économique peut créer un Bitcoin, et la circulation décentralisée du Bitcoin sur Internet, dans laquelle aucun acteur ne prélève de commission, a l’apparence du libéralisme économique. En réalité, le danger est que la décroissance des rendements implique que les fermes de minage doivent se concentrer afin de rester rentables. À partir du moment où quelques entités privées détiennent une majorité du marché de la certification des transactions en Bitcoin, elles détiennent en pratique la capacité d’émission monétaire et l’aspect distribué est perdu.

Références

[DLR15] Jean-Guillaume Dumas, Pascal Lafourcade, and Patrick Redon. *Architectures PKI et communications sécurisées*. Dunod, 2015.