

Comprendre Bitcoin

Rapport de projet INFRES357

Pierre Galland, Benoît de Laitre

18 avril 2015

Table des matières

1	Briques de base	2
1.1	Chiffrement asymétrique	2
1.2	Signature	2
1.3	Hachage	2
2	Un paiement Bitcoin	2
3	Diffuser les paiements	2
4	Empêcher le double-spend	2
5	Le minage	2

1 Briques de base

Le protocole de Bitcoin utilise plusieurs briques de bases de la cryptographie : le chiffrement asymétrique, la signature et le hachage. C'est d'ailleurs là que réside l'intérêt de ce protocole, c'est un assemblage astucieux de briques qui existent depuis de nombreuses années et qui sont très bien connues, pourtant cet assemblage crée une technologie totalement nouvelle.

1.1 Chiffrement asymétrique

Le principe du chiffrement asymétrique est que les clefs vont par paire, une clef publique et une clef privé (K_{Pub}, K_{Pri}). Il est possible de chiffrer un message avec la clef privé et alors le message chiffré ne pourra être déchiffré qu'avec la clef publique correspondante. De même on peut chiffrer un message avec la clef publique et alors il ne pourra être déchiffré qu'avec la clef privé correspondante. Considérons l'exemple classique de Bob et Alice, ils possèdent chacun une paire clef publique/clef privée. La paire de clefs de Bob est (K_{Pub}^B, K_{Pri}^B) et celle d'Alice est (K_{Pub}^A, K_{Pri}^A) .

Si Bob veut envoyer un message *mess* à Alice qu'elle seule pourra lire, alors il chiffre son message avec la clef publique d'Alice, et il obtient le message chiffré **mess** :

$$chiffrer(mess, K_{Pub}^A) \rightarrow *mess*$$

Il envoie alors ce message **mess** à Alice, qui quand elle le reçoit le déchiffre avec sa clef privée K_{Pri}^A :

$$dechiffrer(*mess*, K_{Pri}^A) \rightarrow mess$$

Si Alice essayait de déchiffrer le message **mess** avec une autre clef que sa clef privée K_{Pri}^A alors cela ne marcherait pas, elle obtiendrait n'importe quoi (une suite de symbole qui n'a rien à voir avec le message *mess*). Donc comme on considère qu'Alice est la seule à connaître sa clef privée, elle est la seule à pouvoir déchiffrer le message.

$$dechiffrer(*mess*, K_{Pri}^{autre}) \rightarrow n'importe\ quoi$$

1.2 Signature

1.3 Hachage

2 Un paiement Bitcoin

3 Diffuser les paiements

4 Empêcher le double-spend

5 Le minage