Comprendre Bitcoin
Rapport de projet INFRES357

Pierre Galland, Benoît de Laitre

18 avril 2015

Table des matières

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

1.2 Signature

1.3 Hachage