Notes on Cryptocurrency

August 13, 2019

Contents

1 Cryptography and Cryptocurrencies

Definition 1.1. A hash function is an efficiently computable map with domain String and codomain String_N.

Definition 1.2. A hash function H is said to be *cryptographically secure* if it has the following properties:

- It is infeasible to find $x, y \in \mathsf{String}$ such that $x \neq y$ and $H(x) = H(y)$.
- If r is chosen from a probability distribution that has *high min-entropy*, then given $H(r\|x)$, it is infeasible to find x.
- (Optional)