crypto-currency

cryptographic hash function: 密码学中的 hash 函数

性质:

①collision resistance: 哈希碰撞.

$x \neq y$, $H(x) = H(y)$, 则 collision resistance.

但是, 无好办法人为制造 collision resistance.

用途: 对 message 作 digest

$H(m)$ is the digest of m.

一旦有人更改 m, 则 $H(m)$ 不可能不变.

no hash function can be proved collision resistance in the mathmetics.

②给出 x, 可推 $H(x)$, 但不能由 $H(x)$ 推 x.

hiding

digital commitment = collision resistance + hiding

digital equivalent of a sealed envelope

$H(x \| nonce)$ → 保证输入维度 big enough.

③puzzle friendly: 哈希值的计算不可预测

want a hash value:

$H(x) = 0000\cdots xxx$, 求 x (block head.)

手动可: 找一个 nonce, 与区块组合考虑.

使 $H(\text{block header} + \text{nonce})$ in target space

puzzle friendly

bitcoin 的 hash function: SHA-256

签名:

·1. 以钱币系统中的账户管理

创立公一私钥对即可.

[public key, private key]

this opinion comes from asymmetric encryption algorithm

加密用公钥,解密用私钥

A want to send a message to B, then:

A should use the public key of B to process the message, and B use the private key of himself to explain the message

·2. 签名

A给B 10 bitcoin.

sign 用A的PVK, others 用A的PVK来 validify.