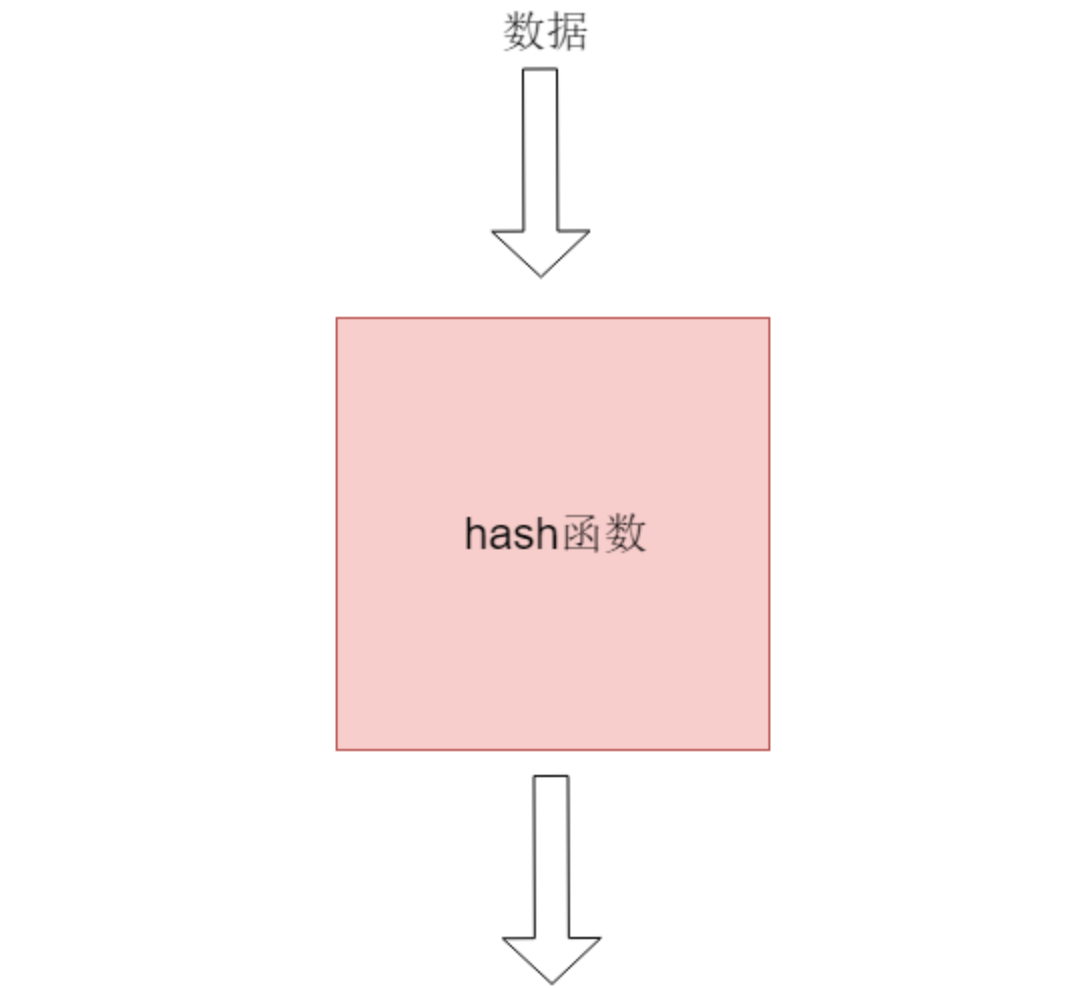
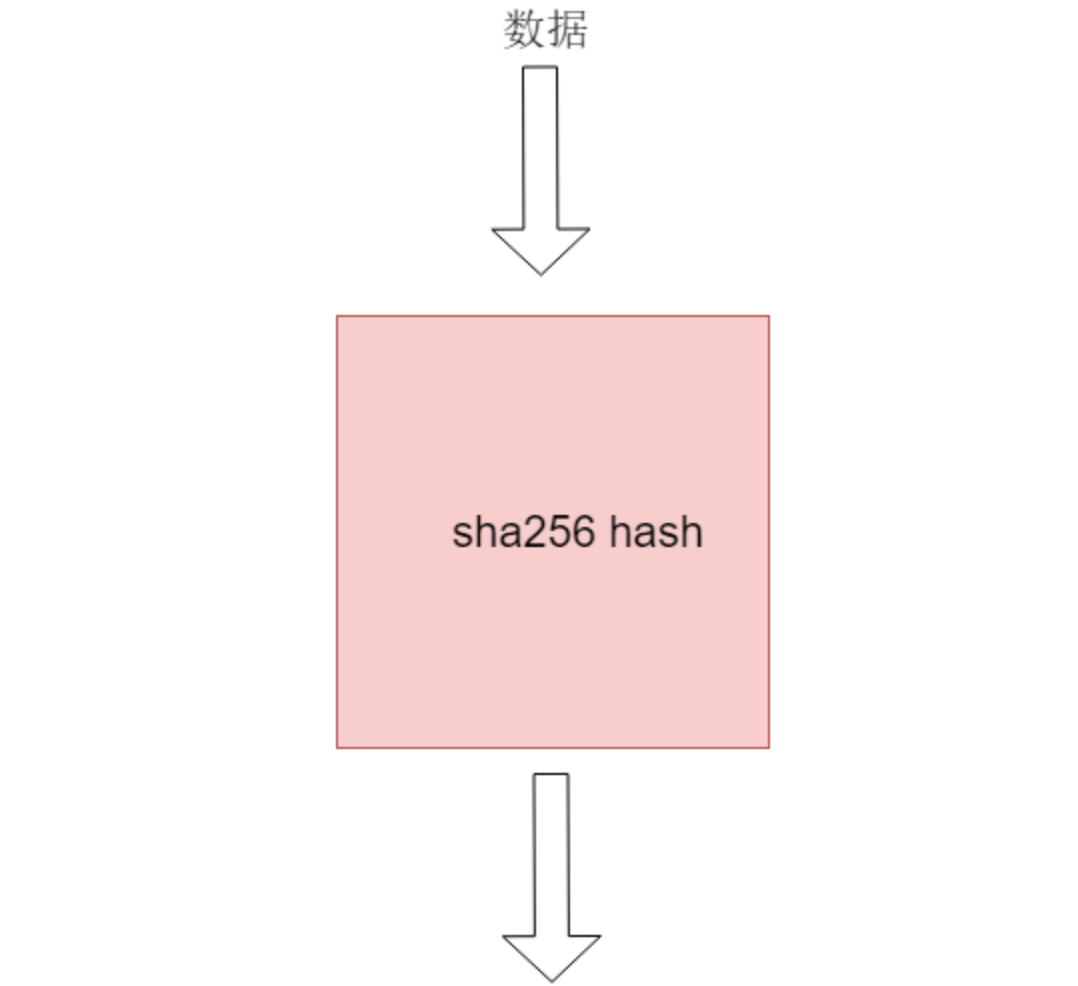
Hash算法的安全性


数据
hash函数
一串固定长度的特征码
906b400bf50f7a08b1be4e6ad6f64d62f850165fa2ab4f8907a8ac0ebf54cbd5



一串固定长度的特征码 64位16进制 256位二进制
906b400bf50f7a08b1be4e6ad6f64d62f850165fa2ab4f8907a8ac0ebf54cbd5

sha256

1001000001101011 0100000000001011
1111010100001111 0111101000001000
1011000110111110 0100111001101010
1101011011110110 0100110101100010
1111100001010000 0001011001011111
1010001010101011 0100111110001001
0000011110101000 1010110000001110
1011111101010100 1100101111010101

可能性

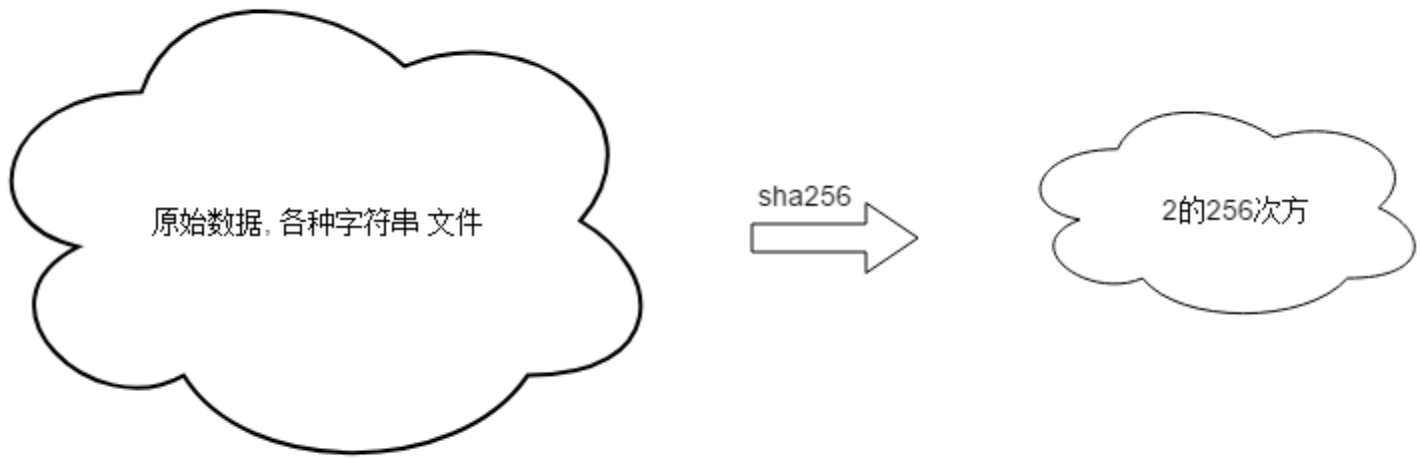
- 2的256次方
- 1.157920892373162e+77

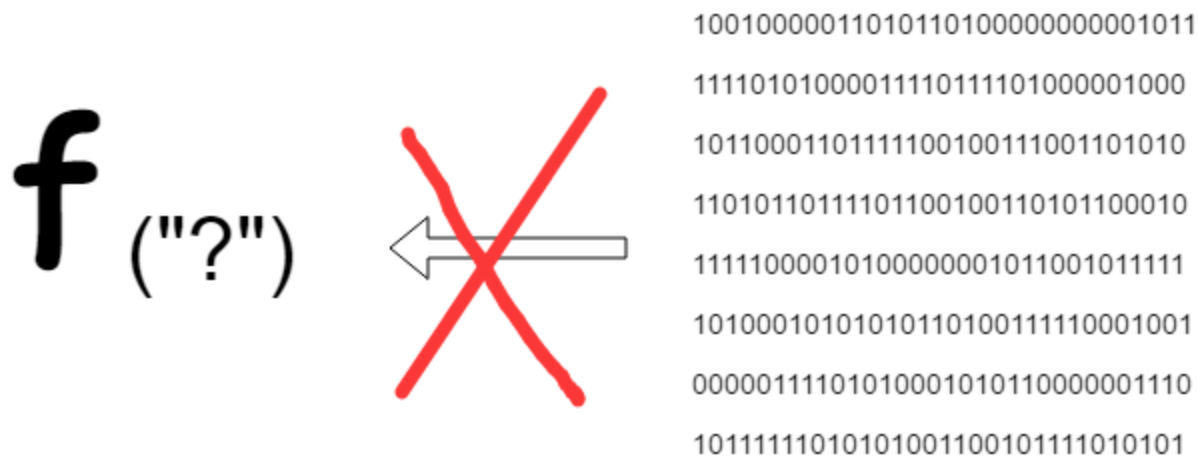
多大

- 比宇宙中原子的数量还多

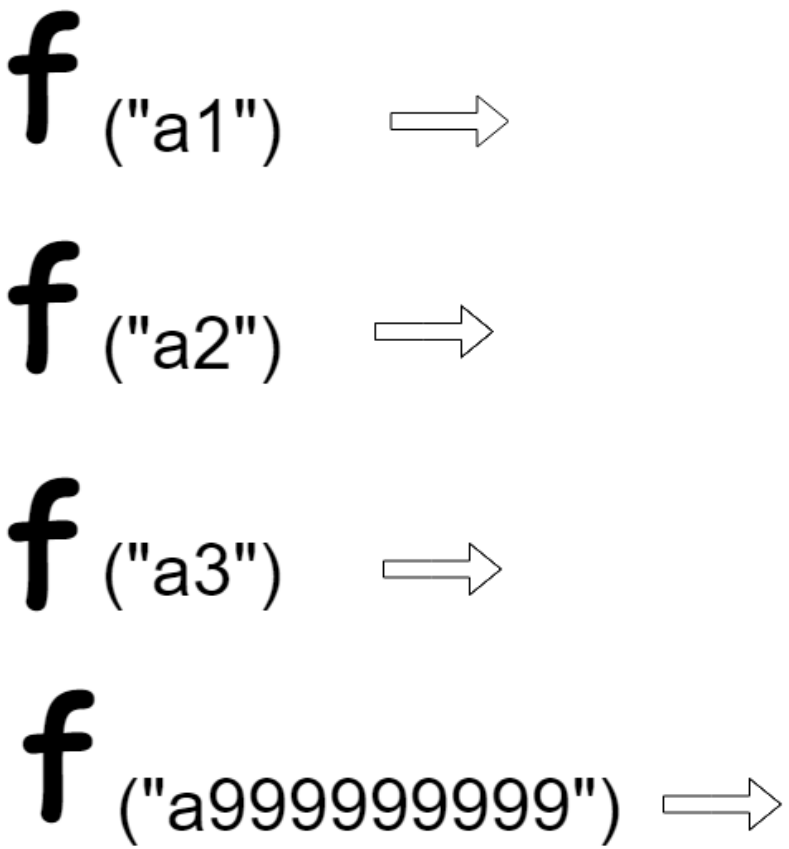
Hash碰撞

- 1.157920892373162e+77
- 世界上的所有信息, 文本,数据.组合可能是无穷的


原始数据, 各种字符串 文件
sha256
2的256次方


f ("?")
10010000011010110100000000001011
11110101000011110111101000001000
10110001101111100100111001101010
11010110111101100100110101100010
11111000010100000001011001011111
10100010101010110100111110001001
00000111101010001010110000001110
10111111010101001100101111010101

暴力穷举



100100000110101101000000000001011 2的32次方

11110101000011110111101000001000 2的32次方

10110001101111100100111001101010 2的32次方

11010110111101100100110101100010 2的32次方

11111000010100000001011001011111 2的32次方

10100010101010110100111110001001 2的32次方

00000111101010001010110000001110 2的32次方

10111111010101001100101111010101 2的32次方

$$\mathbf{2}^{32} = 4294967296$$

2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32}

4G hash/s

2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32}

4G hash/s

aliyun Hs/s

2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32}

4G hash/s

aliyun Hs/s

ipv4 Hs/s

2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32}


4G hash/s


aliyun Hs/s


ipv4 Hs/s


galaxy Hs/s

2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32} 2^{32}


4G hash/s

aliyun Hs/s


ipv4 Hs/s


galaxy Hs/s


universe Hs/s

比特币全网基本信息 (自动刷新:33秒)							
货币名称	比特币/Bitcoin/BTC	预计全网算力	25,574 PH/s	已开采BTC	16,990,175	未开采BTC	4,009,825
总市值	$153,686,326,980	Block总数	519,214	24h开采	132 块 1,650 BTC	平均1h开采	5.5 块 69 BTC
当前难度	3,839,316,899,029	预计下次难度	4,075,440,755,325 (+6.2%)	难度调整	913 块以后	预计需时	6天18小时

钱包的创建

- 无需网络
- 无需服务商
- 甚至可以无需电脑(算盘)