

1.需要对ring signature , zk-snark进行比较 , ring signature decoy的数量在多少的时候更消耗时间空间 , zk-snark在使用上占用多少空间 , 计算时间相比哪个更快

For the ring signature, I modified code from github t-bast/ring-signatures. I used time and runtime go libraries to measure.

Below is the result of time and memory of signing and verifying a message by different numbers of ring decoys (I simplified with ring size). I think the computation time increases almost linearly with ring size, but the space/memory does not increase linearly.

Ring Size	Signing Time (milliseconds)	Signing Memory (KB)	Verifying Time (milliseconds)	Verifying Memory (KB)
5	31.4	1860	34.3	1538
10	64.6	858	65.6	3845
20	127.5	1886	129.9	3034
50	324.3	3446	327.5	1291
100	645.8	1451	649	1254
500	3243	2586	3252.4	2674

For zk-snark, I complied it, but somehow didn't get it work on my mac. I read that its computation is more expensive than that of ring signature.

2、将bitcoin , ethereum , monero , zcash , EOS 的交易、相关交易属性、块大小以及填入多少交易写在report

I searched online tracker & explorers for these coins, and my data was mainly obtained around 9/26 3pm Beijing time. Height and difficulty was from most recent block that I saw.

transactions in the block and block size was from the range of most recent blocks that I saw.

	Height	Difficulty	# Transactions	Block size
bitcoin	543123	7,152,633,351,906.41	90 - 2000	30 KB - 1MB
ethereum	6401451	3,227,200,368,667,784	30 - 200	24 KB - 33 KB
monero	1669621	74121030741	3 - 20	30 KB - 260 KB
zcash	400404	35,894,148	3 - 10	2 KB - 70 KB

EOS	18403929		4 - 15	0.08 KB - 1.5KB
-----	----------	--	--------	-----------------