1.Q1

Ring signature 比zk-SNARK 更轻量级，更快。

环签名被破解的难度，依赖于decoy（引诱人）数量的大小，decoy越多，破解难度越高，当然消耗的时间和空间也越多。单一门罗币币环签名中参与者数量的最高记录是4500名。
而zk-starks不依赖于公钥密码术，其安全性唯一的加密假设是哈希函数（如SHA2），是不可预测的。
zk-snark**需要28分钟和18.9 GB的通信**（主要是由于可靠的设置计算和证明密钥大小），而Zcash最新的树苗升级，将采用zk-starks技术，会将计算时间减少到几分之一秒，通信复杂度减少到1.2 MB。

2. Q2

Bitcoin：https://www.blockchain.com/explorer
1）交易：是指比特币转送被广播到比特币网络，并被记录到区块中的一个过程。
具体包括如下步骤：用户在钱包，创建交易， 钱包广播交易。在内存池，交易等待被确认。 矿工将交易写入他的下一个区块。
2）交易属性：
可以作为现实世界的点对点电子现金系统，使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的金融机构。
3）块大小： 1M。
4）一个区块填入的交易数量：从 225B~几十K。而旷工是以时间来打包区块的，并不是非要等1M装满了才工作。在十分钟内只有1笔交易，时间到了也会打包；十分钟有很多笔交易，也只会挑手续费高的理论上4400笔交易，剩下的在Mempool里等着。平均2500左右。

ETH：
https://etherscan.io/
1）交易：指用户填入目标地址及交易金额，以及需要的gas和gas limit，然后用账户私钥进行签名，提交交易到缓冲池中，通知EVM执行，广播交易给其它节点。
2）交易属性：为了避免网络堵塞，加入了Gas，让交易者为交易执行的每一条

指令付费。

3）块大小：目前 28688 Bytes

4）一个区块填入的交易数量：100~200

Menero

https://moneroblocks.info/

1）交易：Menero用户可以像比特币一样交易，但是它通过使用**使用环签名、混淆地址、环机密技术实现了交易的匿名性。**

2）交易属性：

自适应区块大小限制:门罗币从一开始就设置了自适应的区块大小，这意味着，它可以自动的根据交易量的多少来计算需要多大的区块。因此门罗币从设计上不存在需要通过硬分叉和共识来提高区块大小的问题。

隐匿性：门罗币除了能隐藏货币发送者/接受者的交易地址、交易金额外，同时还将隐藏参与交易双方的IP地址。

3）块大小：94~201302 bytes

4）一个区块填入的交易数量：0~18

Zcash

https://bitinfocharts.com/zh/zcash/

1）交易：Zcash用户可以像比特币一样公布交易、金额、交易双方信息等。也可以选择公布某证据，证明某私密交易遵守Zcash网络规则， 同时隐去交易双方及交易金额。Zcash交易被称为护盾交易（shielded transactions）。

2）交易属性：使用零知识证明zk-SNARK。

3）块大小：13.671 KBytes

4）一个区块填入的交易数量：8.3 平均每小时（过去24小时）

EOS

1）交易：指用户填入目标账户及交易金额，然后用账户私钥进行签名，提交交易到缓冲池中，广播交易给超级节点记账。

2）交易属性：使用账户。无手续费。

3）块大小：1M，dynamic，块生产者可以扩展

4）一个区块填入的交易数量：1~11