Homework9

Read the following materials about Monero & ZCash. Note that Monero & ZCash contain many cryptographic and theory details which you may find hard to understand. You should focus on the high-level ideas of these systems and what these systems are capable of. Of course, you are welcome to dive into these crypto details if you can.

1. ByteCoin White paper (Monero is a fork of Bytecoin and uses the same technique): https://whitepaperdatabase.com/bytecoin-bcn-whitepaper/
2. zkSNARK in a nut-shell: https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/
3. More zkSNARK articles (Optional): https://medium.com/@VitalikButerin/quadratic-arithmetic-programs-from-zero-to-hero-f6d558cea649 https://medium.com/@VitalikButerin/zk-snarks-under-the-hood-b33151a013f6 https://medium.com/@VitalikButerin/exploring-elliptic-curve-pairings-c73c1864e627
4. ZCash white paper (Optional): http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

Then answer the following questions.

1. In Section 4.3 of the ByteCoin whitepaper, it mentions the linkable payment problem. Suppose if all users follow the practice of always creating new address when receiving payment and never reuse address. Would this problem go away?

2. According to Section 4.4 of the ByteCoin whitepaper, how does the ring signature algorithm prevent an adversary from tracing transactions?

3. Monero chooses a ring size of five. Do you think this size is large enough (Open question)?

4. Many people believe that zkSNARK/ZCash provides a much stronger privacy guarantee than Monero? Why? Explain a case where Monero can be traced by ZCash cannot.

5. Now a significant amount of transactions in ZCash is transparent transactions. That means that although ZCash is marketed for its strong privacy, the privacy functionality of ZCash is rarely used. Why (Hint: look numbers in Section 7 in ZCash white paper)?