NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Tutorial

Bitcoin Constructions

CE/CZ4153

Blockchain Technology

Question 1

Ref : Week 2 Lectures

Suppose you have broken the 2nd preimage resistance property of a Hash Function.

What else can you break in effect?

- Preimage Resistance of the Hash Function
- Collision Resistance of the Hash Function
- Neither Preimage Resistance nor Collision Resistance
- Both Preimage Resistance and Collision Resistance

Question 2

Ref : Week 2 Lectures

In case of a cryptographic hash function H mapping arbitrary sized input {0,1}* to a fixed side output {0,1}^n, finding two different inputs x != y such that the hash values H(x) = H(y) are the same is

- Impossible
- Possible

Question 3

Ref : Week 2 Lectures

Can you commit to a single bit data using the Hash Function commitment mentioned in the lecture?

What happens if someone just memorizes the commitment for the cases : data = 0 and data = 1?

Question 4

Ref : Week 2 Lectures

Suppose a digital asset is transmitted to a person, without revealing the personal identity of recipient.

Can the recipient prove the ownership of the digital asset without revealing their personal identity?

Justify your answer, briefly.

Question 5

Ref : Week 2 Lectures

Given a specific piece of Data, can you prove that it "exists" in the Hash Chain discussed in the lecture?

What is the computational complexity for the proof?

Question 6

Ref : Week 2 Lectures

Given a piece of Data, what is the computational complexity to prove that it is

- a member of an *n*-leaf-nodes Merkle Tree?
- not a member of an *n*-leaf-nodes Merkle Tree?

Question 7

Ref : Week 2 Lectures

Suppose at a certain point of time in a blockchain, you have *n* blocks in the hash-chain, and you want to insert *m* transactions as a part of the next block.

What will be the total computational complexity (number of hash pointer computations) to append a new block with all these *m* transactions?