CS4501 PS2

Ziqi Liu (zl3kh)

October 9, 2015

1

Because if he plays against the rule, the whole system of Bitcoin will collapse. Once the infrastructure collapse, the power and the wealth he gains within this system would become useless and worth nothing. Thus, he's more willing to play by the rules and secretly gains himself wealth depends on the system.

2

It says, if we want to achieve a scenario that it's highly unlikely the attack catch up with the honest miner for 340 blocks(P ¡ 0.001), the possibility that the attack finds the next block needs to be 0.45 (the attacker needs to control 45% of total hashing power);

3

P ¡ 0.05 && P 0.01

q = 0.200000, z = 5

q = 0.300000, z = 10

q = 0.350000, z = 20

q = 0.350000, z = 25

q = 0.400000, z = 40

4

a

When you retrieve data[i], you can only identify its data integrity with your signature, but you cannot verify whether this data is actually the data your stored on ith position.

b

We can be sure about this item is written by us, but cannot be sure its position is correct.
Same as above mentioned, the signature only provides the authentication that this data is uploaded by you, because only you have your private key of signature.But you cannot verify whether it is the correct data at the corresponding position.
Also, if the data storage provider is evil, he may break our private key since we have so many signature items uploaded.(In case the signing schema is not a good hash function)

5

a.

Write:
We need to download all the storage data, concatenate all of them. And hash them. Store the hash locally
In case we don't have large local storage space, we probably need to upload the part of the concatenation.
Verify: Download all the records, concatenate them, and compare the result with the local hash value.

b.

Space cost: sum of all record's size // impossible to do this locally Time Cost: O(n) :
Download n items(O(n)), concatenate them (O(1)), hash them (O(1)).

6

a.

Write:

Suppose we want to write data data[k]. We need to get the Merkle tree nodes of its siblings, another subtree root, and the root of the tree. And then write this put hash of data[k] into this Merkle tree, which updates the subtree it stays and the root of Merkle tree.

Verify:

Suppose we download data[k], and calculate the hash of data[k] We need to get the Merkle tree nodes of its siblings, another subtree root, hash them to according to Merkle tree strucutre, and compare the result with the Merkle tree root (stored locally).

b.

We need to do log(n) hashes for Merkle tree.

7

a.

Each block takes 10 minutes, and we have 0.15 of the hashing power. It means we need 67 minutes to mine a block. Since there are

$$24 * 60 = 1440$$

minutes per day. Thus. we can find

$$1440/67 = 21.5$$

blocks per day.

b.

The number expected is

$$t * \frac{\alpha}{10}$$

8

Assume we still have about 10 minutes per block the block rate: it would probably have:

$$\frac{10/\alpha}{L}$$

9

Assume we still have about 10 minutes per block the block rate: it would probably have:

$$10/\alpha + \frac{10/(1-\alpha)}{L}$$

10

B

I want to ask what's the typical method they use to trace down from a bitcoin address to a physical criminal site. (From online information to physical person)

My guess is they have some off-line methods, i.e. checking the IP, or trigger some bitcion transactions to continuously gather enough information.