Homework 13: Bitcoin Reading

Introduction to Big Data Systems course

Due: January 1, 2023 23:59 China time. Late submission results in lower (or even no) scores.

For questions or concerns, contact TA (Huanqi Cao, Mingzhe Zhang) by WeChat. Or send an email to caohq18@mails.tsinghua.edu.cn or zmz21@mails.tsinghua.edu.cn if you could not use WeChat.

Overview

Read the bitcoin paper (https://bitcoin.org/bitcoin.pdf) and answer the following questions.

Submit a PDF report to Tsinghua web learning, or by email if you can't access web learning.

Q1

Please briefly summarize how the bitcoin system avoids double spending? (Multiple choices)

- **A.** Sign the transactions with payer's private key and payee's public key
- **B.** Sign the transactions with payer's public key and payee's private key
- **C.** Use a trusted central authority which oversees all transactions
- **D.** Broadcast transactions to all participants

Q2

As there will be network partition problems, a bitcoin node may fail to receive a block. When and how it becomes aware of it and how it could get the missing block?

Q3

When generating the block ID, we know that it is generated by applying hash function to transactions, last block ID and guess (in the paper it is called Nonce). In the lecture, we also discussed that the transactions of the hash is generated hierarchically with a Merkel tree. Why this is necessary in bitcoin hash generation?