Exam Protocol - Blockchain Technologies - SoSe 2021

Exam Type: Oral Exam

Examiner: Prof. Dr. Florian Tschorsch

Semester: Sommersemester 2021

1. **State replication**
   - Why do you do it?
   - How is it done?
     - Master and Slave and 2PL
       - What are the failure tolerances of those algorithms, i.e. how good are they?
2. Paxos
   - Explain the idea. Why do we do it? Give a rough outline
   - Then he showed me a picture of the general algorithm and asked some specific questions on it
     - What is sequence number for?
     - Aren't sequence numbers the same as locking in 2PL?
     - Why do we do the first phase? Isn't the accept phase sufficient?
3. Quorum systems
   - Give formal definition (Answer: Intersection between two sets is not empty)
   - Then he gave me a list of sets and I should decide whether that is a quorum
4. **Bitcoin Scalability**
   - How do you calculate transaction rate?
   - How could you change the individual parts to improve on that?
   - What are the disadvantages of that?
     - Answer: Larger blocks ⇒ longer propagation in network ⇒ more forks ⇒ waste of computational power ⇒ easier attack
     - Faster block generation ⇒ more forks ⇒ same
5. GHOST
   - How does it work? I gave brief description and then he drew something and I should decide which chain GHOST would choose.
   - How does it help against an attacker?
   - What does it do in the case of selfish mining? (Answer: The same, it protects against that)
   - Problems with it?
6. Private Channel networks
   - How does it improve transaction rate?
   - How does it work? What is needed for it?

- Spillman channel:
    - How exactly does the input (initialization) transaction look like?
        - I.e. what is input, output, who signs it, is it normal script sig or something else.
    - Why is it a unidirectional channel?
    - What are problems of that?

7. **Consensus**
    - 3 Requirements of it
    - Types of node failures (fail stop, fail recover, byzantine)
    - n >= ..f
        - Why do we do it that way?
        - What bounds did we find? (I.e. name the formulas)
            - Different for synchronous and asynchronous networks, whether we assume byzantine or something else
    - Nakamoto consensus bound
        - What is it? (Answer: n>=2f+1)
        - What do n and f represent here?
            - Answer: Mining power, not peers!