Technische Universität Berlin
WS 2019/2020

Software Architecture for Blockchain Applications

Practice Exam

(1) Time allowed: ≤ 45 minutes (typically: 30-35 min)

(2) Reading time: 5 minutes

(3) Total points: 17

(4) Total number of questions: 6

(5) Answer all questions

(6) Questions are not of equal value

(7) No examination materials or auxiliary means permitted

(8) Make sure to write clearly and properly, as answers that cannot be read do not count

Print your student number and name in the top right-hand corner of this page.

All answers must be written in black or blue ink. Except where they are expressly required, pencils may be used only for drawing, sketching or graphical work. Do not use an ink eradicator, TippEx, or similar.

Each question has a different number of points allocated. The total number of points for each question is indicated.

For Q1-Q3, circle the MOST appropriate answer. Select only one answer.

Question 1.   (1 Point)

Referring to the definitions, which of the following statements is correct?
   A. In a Distributed Ledger, transactions can be deleted or updated at any point in time
   B. A Blockchain is a type of distributed ledger
   C. A block in a blockchain always contains the hash of the following block
   D. Smart contracts are a convenient way to update all account balances in a blockchain
   E. Smart contracts can be changed flexibly when the business requirements change (hence 'smart')

Question 2.   (1 Point)

Which of the following statements is correct?
   A. Scripts in Bitcoin and Smart Contracts in Ethereum are basically the same
   B. In Bitcoin, there are two distinct types of transactions: 'normal' ones, and transactions with Scripts attached
   C. Given all blocks strictly after the genesis block, it is possible to compute the entire state of any blockchain
   D. Bitcoin produces blocks less frequently than Ethereum, but a Bitcoin block can hold more transactions than an Ethereum block
   E. On Ethereum, the sender of a transaction specifies how much gas the transaction will use, and therefore how much gas they will pay as fee

Question 3.   (1 Point)

Increasing the block size will NOT cause
   A. Slower replication
   B. Lower throughput
   C. Potential more empty blocks
   D. Potential DoS (Denial-of-Service)
   E. Any of the above

For Q4, write down the MOST appropriate word(s) that could fill in Blank A, Blank B, Blank C, and Blank D.

Question 4.   (2 Points Total)

Immutability of a blockchain using Proof-of-work Nakamoto consensus is of a (a)_____ nature. There is always a chance that the most recent few blocks are replaced by a competing (b)_____. The transactions that were tentatively included before "discarded" go back to the (c)_____and may be added into a later block. From the application perspective, one security strategy is to (d)_____ _____, which is known as X-confirmation.

For Q5-Q6, write the answer in ink. Try to be neat in your hand writing.

Question 5.   (4 Points Total)

Draw and explain how transactions in Bitcoin are connected, and explain what UTXO is.

_____

_____

_____

_____

_____

Question 6. (8 Points Total)

Imagine that a consortium of Universities is considering to implement a blockchain-based system to share information about their students, to let students more easily take modules from any University in the consortium, or transfer module results between those Universities. The blockchain-based system will integrate with existing conventional University student management systems.

a) Discuss whether and why public blockchain or private blockchain could suitable (or not) for this system. For each one (public and private), discuss at least two aspects: performance, and privacy.

(4 Points)

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

b) Consider the information elements of student names, and student results for a subject. If a public blockchain is used, discuss which of these elements should be on-chain and which should be off-chain, and why. **(2 Points)**

_____

_____

_____

_____

_____

c) If a public blockchain is used, a registry of relationships between equivalent courses could be maintained on-chain or off-chain. Describe two cost factors that should be considered when making this design decision. **(2 Points)**

_____

_____

_____

_____

_____

END OF EXAM PAPER