Software Architecture for Blockchain Applications: Practice Exam Discussion

Technische Universität Berlin

Prof. Dr. Ingo Weber | Chair for Software and Business Engineering
ingo.weber@tu-berlin.de | Twitter: @ingomweber

Question 1

- 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

Technische Universität Berlin

- 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

- 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

Note:

- All answers given in the following are **sample answers**.
- They are **NOT** the only correct answers.
- Points can also be obtained with other terms, argumentation, etc. as long as your arguments are sound and in line with content of the course.
- Sample answers are brief; shorter than your answers should typically be

Question 4

- 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.
  A. probabilistic
  B. fork / chain fork/ transaction history
  C. transaction pool
  D. wait for X confirmation blocks

Question 5

- Draw and explain how transactions in Bitcoin are connected, and explain what UTXO is.
  - See Lecture 3: Bitcoin, slides 18 and 19

Question 6

Technische Universität Berlin

- 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.

- Blockchain is by default not strong on privacy, due to (wide) replication
  - Personal data should not go on public blockchain; private blockchain may not be confidential enough
  - Visibility of data needs to be restricted (e.g., pseudonymous IDs, hashes, etc), but then data still needs to be interpretable by the universities
- Performance:
  - throughput (for writes) is typically limited, but can very well be enough for the actual load – even in public setting
  - Read performance will be high in either case
  - (consider performance of off-chain systems)

Question 6

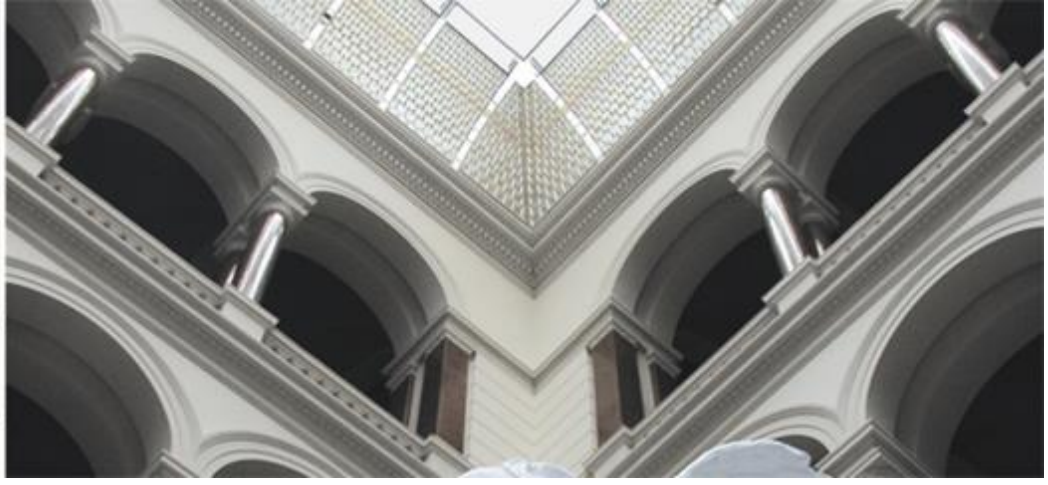
b) Consider the information elements of student names, and student results for a subject. If a public blockchain is used, discuss which of these elements should be on-chain and which should be off-chain, and why.

- Student names: Names are personal data, so private → keep off-chain. Mention options to deal with linking to ID
- Student results for a subject: could be on-chain, but identifiable association to a student should be off-chain (personal data)

Question 6

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.

- If relationship changes frequently, will increase total number of transactions, which will increase operational cost if on-chain
- If on-chain data about relationships is large, will increase cost of storage on-chain
- For off-chain storage: how to organize an acceptable solution? Registry running at one university might not be fair (cost) and gives them a privileged role (may be acceptable to others, or not)
- (other arguments can be valid, too)



Thank you for your attention!

Software Architecture for Blockchain Applications: Practice Exam Discussion

Technische Universität Berlin

Course email: saba@sbe.tu-berlin.de

Prof. Dr. Ingo Weber | Chair for Software and Business Engineering
ingo.weber@tu-berlin.de | Twitter: @ingomweber