# Modul Distributed Systems Advanced & Blockchain (DSA) Prüfung

## Nachname: _____ Vorname: _____
## HSR PID:_____

| Nr. | Aufgabe | Max. Punkte | Erreichte Punkte |
|---|---|---|---|
| 1 | Blockchain Basics | 15 | |
| 2 | Distributed Systems | 22 | |
| 3 | UTXO | 15 | |
| 4 | Praktische Aufgaben | 26 | |
| 5 | Blockchains | 12 | |
| | | **Total 90** | |

Hinweise allgemein:

- Zeit: 120 min.
- Zuerst diese Hinweise, dann die Prüfungsteile ganz durchlesen.
- Diese Prüfung ist **"Closed Book".**
- Taschenrechner ist nicht erlaubt.
- Sonst sind keine Hilfsmittel zugelassen; auch kein Handy oder Smart Watch.
- Alle Antworten und Lösungen in diese Aufgabenblätter schreiben.
- Keinen Bleistift und keine rote Farbe verwenden.
- Die Antworten und Lösungen müssen nachvollziehbar sein. Bitte alles in leserlicher Schrift!
- Keine Fragen während der Prüfung. Bei Unklarheiten sind sinnvolle Annahmen zu treffen und diese klar zu dokumentieren.
- Die Bewertungspunkte der Aufgaben können nach der Korrektur noch etwas variieren.

Hinweise zum Prüfungsbeginn:

- Versehen Sie das Titelblatt beider Teile mit Ihrem Namen.
- HSR-Badge sichtbar auf den Tisch legen.
- Allfällig bereitliegende Prüfung nicht umdrehen oder umblättern, bis die Aufsichtsperson explizit das OK dazu gegeben hat.

Hinweise zur Prüfungsabgabe:

- Kontrollieren Sie nochmals, ob die Prüfung mit Ihrem Namen versehen ist. Geben Sie alle Blätter – auch von nicht gelösten Aufgaben – geordnet und geheftet ab.
- Nach Prüfungsende: Drehen Sie Ihre Prüfung um und warten Sie, bis die Prüfung eingesammelt wird. Bleiben Sie dann sitzen bis die/eine Aufsichtsperson die Prüfungen gezählt hat und ein Zeichen zum Verlassen des Raums gegeben hat.

## Aufgabe 1: Blockchain Basics (15 Punkte)

a) (5P) Kreuzen Sie Zutreffendes an.

Bitte beachten Sie, dass keine Punkte für ein falsch gesetztes Kreuz abgezogen werden.

| | Statement | True | False |
|---|---|---|---|
| 1 | Ringsignaturen in Monero dienen der Anonymisierung. | | |
| 2 | Transaktionsdaten in einer Blockchain (wie z.B. Bitcoin) müssen verschlüsselt werden, sonst kann jeder die Transaktionen mitlesen. | | |
| 3 | Jedes Problem lässt sich mit Blockchains lösen. | | |
| 4 | Krypto-Mining kann nur von professionellen Firmen betrieben werden. | | |
| 5 | Die Kostenfaktoren bei Krypto-Mining sind Anschaffungs- und Stromkosten. | | |

b) (4P) Wieso fallen in der Regel Transaktionsgebühren für Transaktionen in einer Blockchain an?

d) (6P) Was passiert bei einer 51% Attacke? Erklären Sie das Problem mit einem Käufer und Verkäufer, der Waren mit einer Kryptowährung kauft.

## Aufgabe 2: Distributed Systems (22 Punkte)

a) (5P) Kreuzen Sie Zutreffendes an.

Bitte beachten Sie, dass keine Punkte für ein falsch gesetztes Kreuz abgezogen werden.

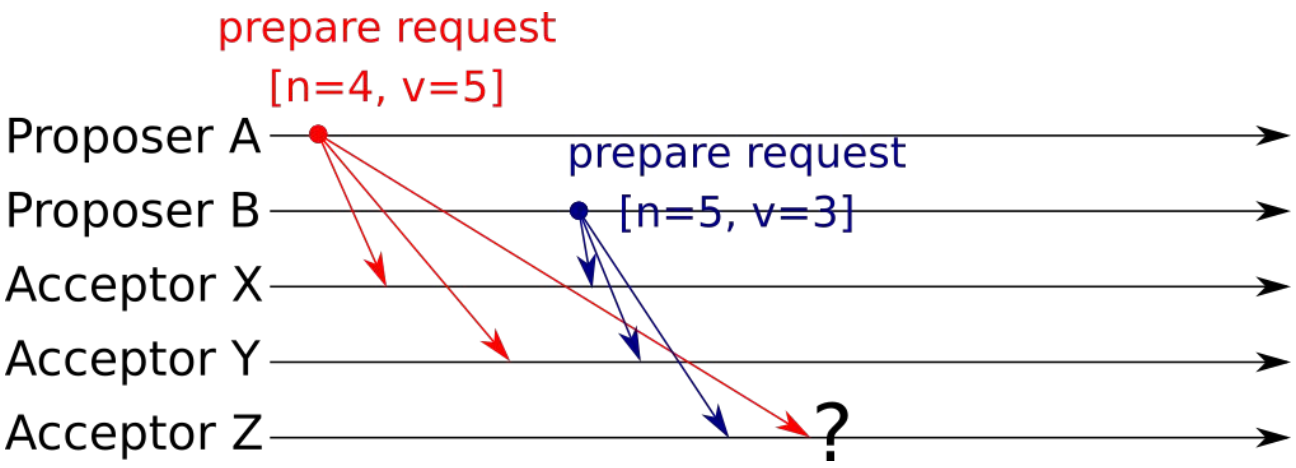
| | Statement | True | False |
|---|---|---|---|
| 1 | In verteilten Systemen gibt es eine globale Zeit, welche überall gleich ist. | | |
| 2 | Verteilte Systeme sind immer einfacher zu bauen als zentrale, da diese skalieren. | | |
| 3 | Paxos ist eine Gruppe von Protokollen mit dem Ziel, einen Konsensus in einem Netzwerk von unzuverlässigen Entitäten zu erzielen. | | |
| 4 | Raft ist ebenfalls ein Konsensus Algorithmus und kann als Alternative zu Paxos verwendet werden. | | |
| 5 | In verteilten Systemen kann man davon ausgehen, dass nichts schief gehen kann. | | |

b) (2P) Was ist der Unterschied zwischen direkter Replikation und indirekter Replikation

c) (2P) Wozu wird eine Bootstrap Peer/Node verwendet?

d) (4P) Was für Probleme sehen sie, wenn sie eine DHT in ihrer Applikation implementieren und es auf einem mobilen Gerät laufen lassen?

e) (3P) In der folgenden Grafik schicken beide A und B einen “prepare request”. Was macht Acceptor Z zum Zeitpunkt, welcher mit “?” markiert ist? Schickt er [n=4, v=5], [n=5,v=3], [n=4, v=3] oder gar nichts?




Lösung:

f) (3P) Warum ist in Raft der Heartbeat für die Leader Election wichtig?

g) (3P) Wofür steht beim CAP Theorem von Brewer, das C, A, und P. Erklären sie die Begriffe mit maximal je einem Satz.

C:

A:

P:

## Aufgabe 3: UTXO (15 Punkte)

Die folgende Tabelle zeigt Transaktionen in einem Block. Der Input einer Transaktion (TX) ist ein Pointer zu einer vorherigen Transaktion mit einem Index (z.B. der erste index wird mit id:0 bezeichnet) zum Output. Es fallen keine Mininggebühren an. (Hinweis: es müssen nicht alle Inputs und Outputs verwendet werden).

| TX | Input | Output | Betrag (Coins) |
|---|---|---|---|
| 4 | 1, id:0 / 1, id:1 | G, H | 1, 1 |
| 5 | 2, id:0 | I | 2 |
| 6 | 3, id:0 | J, E | 3, 1 |
| 7 | 4, id:1 | K, P | 4, 9 |
| 8 | Coinbase | F | 5 |

a) (4P) Alice besitzt die Schlüssel zu den folgenden Adressen F und H. Bob besitzt den Schlüssel zur Adresse M. Erstellen Sie eine Transaktion in welcher Alice 6 Coins an Bob schickt.

| TX | Input | Output | Betrag (Coins) |
|---|---|---|---|
| 9 | | | |

b) (4P) Transaktion 9 ist bestätigt. Bob besitzt den Schlüssel zur Adresse P. Konsolidieren sie Bobs UTXOs zum Output X (zu dem Bob ebenfalls den Schlüssel besitzt):

| TX | Input | Output | Betrag (Coins) |
|---|---|---|---|
| 10 | | | |

c) (4P) Transaktion 11 ist bestätigt und Charlie besitzt den Schlüssel zur Adresse N. Erstellen Sie eine Transaktion in der Bob 1 Coin an Charlie schickt:

| TX | Input | Output | Betrag (Coins) |
|---|---|---|---|
| 11 | | | |

d) (3P) Um was für eine Wallet könnte es sich handeln, wenn eine Transaktion in einer UTXO Blockchain mehr als 3 Outputs hat?

## Aufgabe 4: Praktische Aufgaben (26 Punkte)

Sie entwickeln eine verteilte Chat Applikation mit Anbindung an eine Blockchain. Um den Seed möglichst einfach dem Benutzer zugänglich zu machen speichern Sie den Seed mit einer vordefinierten List von Wörtern ab. Die 4-bit Liste besteht aus den folgenden Wörtern:

| | | | |
|---|---|---|---|
| 0 Apple | 1 Kiwi | 2 Mango | 3 Banana |
| 4 Cherry | 5 Peach | 6 Melon | 7 Lime |
| 8 Grape | 9 Pear | 10 Pineapple | 11 Avocado |
| 12 Coconut | 13 Blueberry | 14 Orange | 15 Pear |

a) (2P) Welche Wörter soll der Benutzer aufschreiben, wenn der Seed 0x1a09 ist?

b) (2P) Um sicher zu gehen, dass alle Zahlen stimmen, wird eine Checksum hinzugefügt. Die Checksum addiert alle 4-bit Zahlen mit einem einfachen Overflow (Modulo 16). Der Overflow dient dazu, dass die Checksum nie grösser als 15 wird. Welches Wort wird als Checksumme verwendet?

c) (4P) In Ihrer dezentralen Chat Applikation speichern Sie die Identitäten in einem Bloomfilter ab, welche den User kontaktieren dürfen. Was sind die Vor- und Nachteile dieses Ansatzes?

d) (2P) Sie entwerfen ihre Chat Applikation so, dass jeder getippte Buchstaben übertragen wird. Was für ein bereits existierendes und standardisiertes Layer 4 Protokoll wählen Sie, um eine möglichst kleine Latenz zu haben, aber dennoch sicher zu sein?

e) (3P) Ihr Vorschlag für ein eigenes 0-RTT Protokoll wurde vom Management abgelehnt, und nun sollen Sie stattdessen TCP mit TLS verwenden. Die Anwender ihrer Applikation haben im Schnitt eine RTT von 200ms. Wie lange geht es mit TCP+TLS, bis Sie die ersten Applikationsdaten schicken können?

f) (4P) Sie verwenden für Ihre Applikation eine DHT. In einer DHT kann man entweder direkt oder indirekt replizieren. Welchen Replikationsmechanismus wählen Sie für den Online/Offline Status Ihrer Chat Applikation und warum?

g) (9P) Für Ihre Applikation haben Sie die Wahl zwischen NEO, Ethereum oder IOTA. Welche werden Sie in Ihrer Applikation verwenden? Nennen Sie je 3 Eigenschaften pro Blockchain.

## Aufgabe 5: Blockchains (12 Punkte)

Dieser Smart Contract hält in der Variable ***balances*** fest, welche Adresse wie viele Tokens hat. Die Funktion ***dividend()*** zahlt jeder Adresse einen Token aus.

```
pragma solidity ^0.4.25;

contract Exam {
    address private owner;
    mapping (address => uint256) private balances;
    address[] private balances_keys;

    constructor() {
        owner = msg.sender;
    }

    function dividend() public {
        require(owner == msg.sender);
        for(uint256 i=0;i<balances_keys.length;i++) {
            balances[balances_keys[i]] = balances[balances_keys[i]] + 1;
        }
    }
}
```

a) (4P) Was ist das Problem in der Funktion ***dividend()***

b) (4P) Bei einem ICO, welcher einen ERC-20 Token heraus gibt, könnte der Token direkt nach der Überweisung von Ethers an einem Smart Contract erstellt werden. Was ist der Nachteil für den Benutzer/Investor wenn man einen Token direkt erstellt?

c) (4P) Sie entwickeln eine eigene Blockchain mit PoW. Sie wissen, dass ein Miner 1.067 H/s leisten kann. Sie möchten, dass ein Miner in einer Minute alle Varianten mit der Nonce durchrechnen kann. Wie viele Bits muss die Nonce haben? (Hinweis: die Anzahl Bits ist ganzzahlig)