Verteilte Systeme VO

Hallo und willkommen, bei diesem Versuch einige Altprüfungen gemeinsam auszuarbeiten 🙂

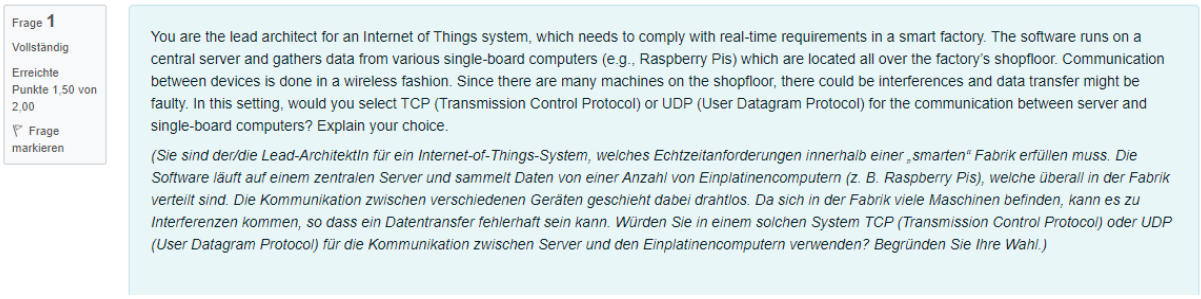
Feel free to:

- Comment answers to questions if you think there is a mistake.
- Add new questions from VOWI and add your answers. Please always add the name from VOWI as headline to provide a clear structure.

Vorsicht: Die Lösungen sind großteils keine offiziellen Lösungen sondern nur meine Idee, wie man die jeweiligen Beispiele lösen könnte. Manches davon ist sicherlich fehlerhaft. Solltest du einen Fehler finden, bitte kommentieren!

Pruefung_2021-02-19

https://vowi.fsinf.at/images/4/4b/TU_Wien-Verteilte_Systeme_VO_%28Dustdar%29_-_Pruefung_2021-02-19.zip


Frage 1

Vollständig

Erreichte Punkte 1,50 von 2,00

Frage markieren

You are the lead architect for an Internet of Things system, which needs to comply with real-time requirements in a smart factory. The software runs on a central server and gathers data from various single-board computers (e.g., Raspberry Pis) which are located all over the factory's shopfloor. Communication between devices is done in a wireless fashion. Since there are many machines on the shopfloor, there could be interferences and data transfer might be faulty. In this setting, would you select TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) for the communication between server and single-board computers? Explain your choice.

(Sie sind der/die Lead-ArchitektIn für ein Internet-of-Things-System, welches Echtzeitanforderungen innerhalb einer „smarten" Fabrik erfüllen muss. Die Software läuft auf einem zentralen Server und sammelt Daten von einer Anzahl von Einplatinencomputern (z. B. Raspberry Pis), welche überall in der Fabrik verteilt sind. Die Kommunikation zwischen verschiedenen Geräten geschieht dabei drahtlos. Da sich in der Fabrik viele Maschinen befinden, kann es zu Interferenzen kommen, so dass ein Datentransfer fehlerhaft sein kann. Würden Sie in einem solchen System TCP (Transmission Control Protocol) oder UDP (User Datagram Protocol) für die Kommunikation zwischen Server und den Einplatinencomputern verwenden? Begründen Sie Ihre Wahl.)

TCP, wenn es sich um Daten handelt, die übertragen werden müssen und für Funktionieren der Fabrik wichtig sind. UDP bei Daten, die zu einem späteren Zeitpunkt keinen Sinn mehr machen z.B. Thermometer

Frage 2

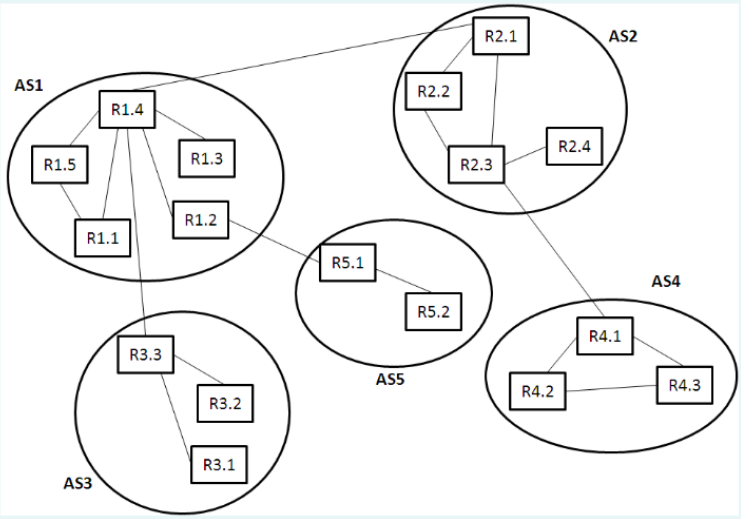
Vollständig

Erreichte Punkte 1,00 von 1,00

Frage markieren

Consider the following topology of Internet Autonomous Systems (ASs), where each circle corresponds to an AS. Each AS is composed of a number of interconnected routers (boxes), and ASs interconnect with each other.

(Betrachten Sie die folgende Topologie von Internet Autonomen Systemen (Internet Autonomous Systems - ASs), wobei jeder Kreis einem AS entspricht. Jedes AS besteht aus mehreren miteinander verbundenen Routern (Boxen), und ASs sind miteinander verbunden.)



You have to select **where to place two replica servers.** Each replica server should be **placed at a router location**. Execute an appropriate algorithm for replica server placement that uses the above topology as input, in order to **provide a placement of the two servers.** That is, decide at which router each server should be installed (e.g., "Server 1 at Router Rx.y, Server 2 at Router Rm.n"), explaining how you reached your decision step by step.

(Sie müssen auswählen, wo **zwei Replikatserver platziert werden sollen**. Jeder Replikatserver sollte an einem **Router-Standort platziert werden**. Führen Sie einen geeigneten Algorithmus für die Platzierung von Replikatservern aus, der die obige Topologie als Eingabe verwendet, um eine Platzierung der beiden Server bereitzustellen. Entscheiden Sie also, auf welchem Router jeder Server installiert werden soll (z. B. "Server 1 auf Router Rx.y, Server 2 auf Router Rm.n"), und erläutern Sie Schritt für Schritt, wie Sie zu Ihrer Entscheidung gelangt sind.)

Mittels Greedy Algorithmus aus der VO: finde größtes AS und platziere Server bei Router mit den meisten connections.
Gewählt werden daher die Router **R1.4** und **R2.3**
(*Consistency and Replication part II*, Seite 20 ff.)

Frage 3

Vollständig

Erreichte Punkte 1,00 von 1,00

Frage markieren

Imagine a distributed storage system with 1,000,000 users which stores some billions of objects. Each user has access rights (read, update) on up to five objects. Which approach (**Access Control List** or **Capabilities**) would you select to implement the **Access Control Matrix** and why? Explain in maximum two sentences.

(Stellen Sie sich ein verteiltes Speichersystem mit 1.000.000 Benutzern vor, in dem Milliarden von Objekten gespeichert sind. Jeder Benutzer hat Zugriffsrechte (Lesen, Aktualisieren) auf bis zu fünf Objekte. Welchen Ansatz (**Zugriffssteuerungsliste** oder **Rechte** (Capabilities)) würden Sie wählen, um die **Zugriffssteuerungsmatrix** zu implementieren, und warum? Erklären Sie dies in maximal zwei Sätzen.)

Rechte ist im gegeben Szenario der bessere Ansatz, da er (Speicher-)effizienter ist. In diesem Fall benötigen wir eine Liste pro Nutzer, mit Zugriffssteurungsliste würden wir Milliarden von Listen benötigen.
(*Security*, Seite 60 ff.)

Frage 4

Vollständig

Erreichte Punkte 2,00 von 2,00

Frage markieren

Consider a distributed shared file system where the shared data store is replicated across local machines. Each user operates on a local copy of the file system located in her/his local machine. The file system middleware takes care of file consistency and replication. A user can open a file only if it is not in use (locked) by another user. If the file is in use, the user receives the message "File is in use. Please try again later." If the machine of a user crashes while the user is updating the file (holds the lock), other users keep receiving the same message when they try to open the file, until the lock is automatically released after a timeout of 15 minutes. Which forms of transparency are violated in this system and why?

(Stellen Sie sich ein verteiltes gemeinsam genutztes Dateisystem vor, in dem der gemeinsam genutzte Datenspeicher auf lokalen Computern repliziert wird. Jeder Benutzer bearbeitet eine lokale Kopie des Dateisystems auf seinem lokalen Computer. Die Dateisystem-Middleware sorgt für Dateikonsistenz und Replikation. Ein Benutzer kann eine Datei nur öffnen, wenn sie nicht von einem anderen Benutzer verwendet wird, also gesperrt wurde. Wenn die Datei verwendet wird, erhält der Benutzer die Meldung "Datei wird verwendet. Bitte versuchen Sie es später erneut." Wenn der Computer eines Benutzers abstürzt, während der Benutzer die Datei aktualisiert (die Sperre besteht), erhalten andere Benutzer beim Versuch, die Datei zu öffnen, dieselbe Meldung, bis die Sperre nach einer Zeitüberschreitung (Time-Out) von 15 Minuten automatisch aufgehoben wird. Welche Formen der Transparenz werden in diesem System verletzt und warum?)

Concurrency transparency, da nicht gleichzeitig auf eine Datei zugegriffen werden kann. Möglicherweise auch failure transparency, da auf einer Datei nicht gearbeitet werden kann, wenn diese noch von einem anderen abgestürzten Computer blockiert wird.

Frage 5

Vollständig

Erreichte Punkte 1,00 von 1,00

Frage markieren

Provide one advantage of Edge Computing compared to Cloud Computing.

(Nennen Sie einen Vorteil von Edge Computing im Vergleich zu Cloud Computing.)

Edge Computing ist besser als Cloud Computing, wenn es um Prozesse geht, die sehr anfällig für Latenz sind. Das heißt, Edge Computing hat einen Vorteil gegenüber des Cloud Computings hinsichtlich der schnellen Datenverarbeitung.

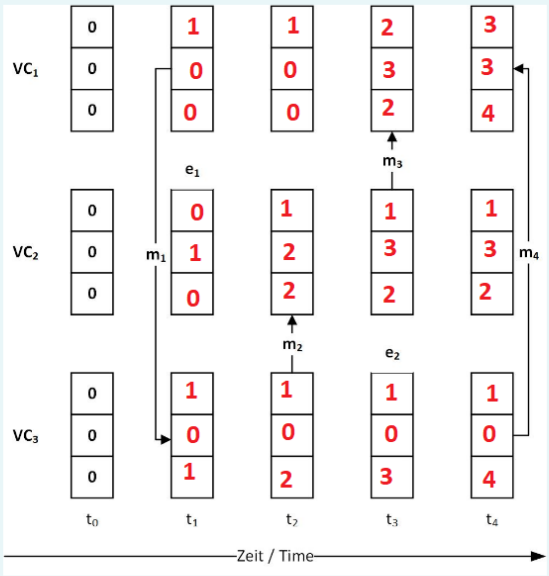
Beurteilte Lösung bereits in Screenshot vorhanden

Frage 6

Teilweise richtig

Erreichte Punkte 1,00 von 2,00

Frage markieren



Three processes p_1, p_2 and p_3 use vector clocks VC_1, VC_2 and VC_3, respectively. In the figure above, you see the initial state of the vector clocks as well as some events e_x and messages m_y. Fill in the missing values of the vector clocks for each time step $t_{1..4}$ in the format (X,Y,Z), e.g., (0,0,1). This is important, your answer is not graded correctly if you use a different format. If the vector value is not defined yet, use "0" to indicate this. In your answers, do not use blanks, but provide the brackets.

Hints: To simplify the figure, the vector clocks are shown in parallel for the three processes. Fill in all empty boxes, even if there is no change for a particular process. Events only apply to one process and are applied instantly to the according vector clock. Messages are delivered instantly (which is of course not possible in reality).

(Drei Prozesse p_1, p_2 und p_3 verwenden jeweils eine Vektoruhr VC_1, VC_2 bzw. VC_3. In der Abbildung sehen Sie den initialen Status der Vektoruhren sowie Ereignisse e_x und Nachrichten m_y. Tragen Sie die fehlenden Werte der Vektoruhren für die einzelnen Zeitpunkte $t_{1..4}$ ein. Nutzen Sie das Format (X,Y,Z), z. B. (0,0,1). Dies ist wichtig, weil Ihre Antworten nicht korrekt bewertet werden, falls Sie ein anderes Format nutzen. Falls ein Vektorwert bisher nicht definiert wurde, nutzen Sie "0", um dies anzugeben. Verwenden Sie in Ihren Antworten keine Leerzeichen, aber geben Sie die Klammern an.

Hinweise: Um die Grafik einfacher zu gestalten, werden die Vektoruhren für die drei Prozesse parallel dargestellt. Füllen Sie alle leeren Felder ein, auch wenn es keine Änderung für einen bestimmten Prozess gibt. Ereignisse wirken sich nur auf einen Prozess aus und werden sofort auf die Vektoruhr angewendet. Nachrichten werden sofort ausgeliefert (was natürlich in der Realität nicht der Fall ist.))

Lösung bereits in rot in den Screenshot eingefügt (meine Lösung, nicht die beurteilte!)

Frage 7

Vollständig

Erreichte Punkte 1,00 von 1,00

Frage markieren

Entities A and B wish to establish a secret key using the Diffie-Hellman protocol. The public information that A selects as the configuration of the system is **n = 19** (modulo) and **g = 5** (base). What is the secret key that will be derived if A and B pick values **a = 3** and **b = 2**, respectively, as their private information?

*(Die Entitäten A und B möchten einen geheimen Schlüssel unter Verwendung des Diffie-Hellman-Protokolls einrichten. Die öffentliche Information, die A als Konfiguration des Systems auswählt, ist **n = 19** (Modulo) und **g = 5** (Basis). Was ist der geheime Schlüssel, der abgeleitet wird, wenn A und B die Werte **a = 3** bzw. **b = 2** als private Informationen auswählen?)*

Der geheime Schlüssel ist g^(ab) mod n also konkret 5^(3*2) mod 19 und ergibt 7.

Beurteilte Lösung bereits in Screenshot vorhanden

Frage 8

Vollständig

Erreichte Punkte 1,00 von 1,00

Frage markieren

In a distributed system with **N = 10** replica servers, each replicated file is updated once per day, while it is read once per minute. Read and write operations are executed using a quorum-based consistency protocol. Propose appropriate values for the **read and write quorums** and justify your answer using maximum 2 sentences.

*(In einem verteilten System mit **N = 10** Replikatservern wird jede replizierte Datei einmal pro Tag aktualisiert, während sie einmal pro Minute gelesen wird. Lese- und Schreibvorgänge werden unter Verwendung eines Quorum-basierten Konsistenzprotokolls ausgeführt. Schlagen Sie geeignete Werte für die Lese- und Schreibquoren vor und begründen Sie Ihre Antwort in maximal zwei Sätzen.)*

Das System muss auf Lese-Operationen optimiert werden, weshalb für das **Lese-Quorum der Wert 1** und für das **Schreib-Quorum der Wert 10** vorgeschlagen wird (ROWA - Read one, write all).
(*Consistency and Replication part I*, Seite 46 ff.)

Frage 9

Vollständig

Erreichte Punkte 0,00 von 2,00

Frage markieren

We use Paxos in order to find consensus in a distributed system made up from five acceptors and one proposer – these are the only nodes in our system, but they may not be online at the same time, since the system is faulty.

Each acceptor has stored information about the last message ID it promised, and an accepted value (note: "---" means that no value has been accepted for this ID):

- Acceptor 1: ID 5, Value "---"
- Acceptor 2: ID 5, Value "---"
- Acceptor 3: ID 4, Value "No"
- Acceptor 4: ID 4, Value "No"
- Acceptor 5: ID 4, Value "No"

Is this an acceptable state in a valid Paxos run, i.e., can this state be reached if Paxos has run correctly? If this is not a valid state, explain the reason for it. If it is a valid state, explain why the acceptors can store two different IDs.

(Wir nutzen Paxos, um Konsensus in einem verteilten System zu erreichen, welches aus fünf Akzeptoren und einem Vorschlagenden besteht – dies sind die einzigen Knoten in unserem System, aber sie müssen nicht zwangsläufig zum gleichen Zeitpunkt online sein, da das System fehlerhaft ist.

Jeder Akzeptor hat Informationen über die letzte „versprochene" (engl. „promise") Nachrichten-ID sowie den momentan akzeptierten Wert gespeichert (Hinweis: „---" bedeutet, dass kein Wert für diese ID akzeptiert wurde):

- Akzeptor 1: ID 5, Wert "---"
- Akzeptor 2: ID 5, Wert "---"
- Akzeptor 3: ID 4, Wert "Nein"
- Akzeptor 4: ID 4, Wert "Nein"
- Akzeptor 5: ID 4, Wert "Nein"

Ist dies ein zulässiger Zustand in einem validen Paxos-Durchlauf? Kann dieser Zustand also erreicht werden, wenn Paxos korrekt ausgeführt wurde? Falls es sich um keinen validen Zustand handelt, geben Sie den Grund hierfür an. Falls es sich um einen validen Zustand handelt, erklären Sie, warum die Akzeptoren zwei verschiedene IDs gespeichert haben.)

Zulässiger Zustand, der folgendermaßen erreicht werden kann:

1. Akzeptoren 1 und 2 sind offline
2. Proposer sendet PREPARE 4
3. Akzeptoren 3, 4 und 5 senden PROMISE 4
4. Proposer sendet ACCEPT-REQUEST 4 'Nein'
5. Akzeptoren 3, 4 und 5 senden ACCEPT 4 'Nein'
6. Akzeptoren 3, 4 und 5 gehen offline
7. Akzeptoren 1 und 2 kommen online
8. Proposer sendet PREPARE 5
9. Akzeptoren 1 und 2 senden PROMISE 5

(*Fault Tolerance*, Seite 22 ff.)

Frage 10
Vollständig
Erreichte Punkte 0,50 von 1,00
Frage markieren

Consider the following Read/Write events.

- Does this system provide sequential consistency? Why/Why not?
- Does this system provide causal consistency? Why/Why not?

(Betrachten Sie die folgenden R/W-Ereignisse.

- *Bietet dieses System sequentielle Konsistenz? Warum/Warum nicht?*
- *Bietet dieses System kausale Konsistenz? Warum/Warum nicht?)*

P1:	W(x)2			W(x)1		
P2:		R(x)2	W(x)0		R(x)0	R(x)1
P3:				R(x)2	R(x)1	R(x)0

Nicht sequentiell konsistent, da P2 und P3 1 und 0 in unterschiedlicher Reihenfolge wahrnehmen
Kausal konsistent, da P2 und P3 sowohl 2 vor 0 als auch 2 vor 1 wahrnehmen
(*Consistency and Replication part I*, Seite 14 ff.)

Frage 11
Vollständig
Erreichte Punkte 1,00 von 1,00
Frage markieren

Consider a distributed storage which is storing data items of a few bytes each, and where clients are connected over the same 1 Gbps local area network. The data items are transparently replicated at each client's local store. Clients are performing reads and updates on their local replicas. Each data item is modified once per hour on average and is read on average once per second. **Which of the following strategies would you select to propagate the updates to the replicas and why?**

- Invalidation
- Data transfer
- Active replication

Provide your answer in maximum 2 sentences.

(Stellen Sie sich einen verteilten Speicher vor, in dem Datenelemente mit jeweils wenigen Bytes gespeichert werden und in dem Clients über dasselbe lokale 1-Gbit / s-Netzwerk verbunden sind. Die Datenelemente werden im lokalen Speicher jedes Clients transparent repliziert. Clients führen Lesevorgänge und Aktualisierungen für ihre lokalen Replikate durch. Jedes Datenelement wird durchschnittlich einmal pro Stunde geändert und durchschnittlich einmal pro Sekunde gelesen. ***Welche der folgenden Strategien würden Sie auswählen, um die Aktualisierungen an die Replikate weiterzugeben, und warum?***

- *Invalidierung*
- *Datentransfer*
- *Aktive Replikation*

Geben Sie Ihre Antwort in maximal zwei Sätzen.)

Datentransfer, da die read-to-write ratio hoch ist und die Datenelemente sehr klein sind, weswegen die verbrauchte Bandbreite gering ist.
(*Consistency and Replication part II*, S. 49 ff.)

Frage 12
Vollständig
Erreichte Punkte 1,00 von 1,00
Frage markieren

For each of the following two examples, name the Cloud Computing service model that characterizes it.

1. A Cloud provider offers a runtime environment to developers to deploy Java Web applications.
2. A client is leasing a virtual machine with 4 virtual CPUs and 8 GB RAM from a Cloud provider for 1 day.

(Nennen Sie für jedes der beiden folgenden Beispiele das entsprechende Cloud-Computing-Dienstmodell.

1. *Ein Cloud-Anbieter bietet Entwicklern eine Laufzeitumgebung zum Bereitstellen von Java-Webanwendungen.*
2. *Ein Client leased eine virtuelle Maschine mit 4 virtuellen CPUs und 8 GB RAM für einen Tag von einem Cloud-Anbieter.)*

1. PaaS - Cloud Platform as a Service
2. IaaS - Cloud Infrastrukture as a Service

(*Processes and Communications I*, S. 18 ff.)

Frage 13
Vollständig
Erreichte Punkte 2,00 von 2,00
Frage markieren

You have to implement a Web browser. Explain why you would design the software as either a singlethreaded process, a multithreaded process, or a multiprocess program.

(Sie haben die Aufgabe, einen Webbrowser zu entwickeln. Erklären Sie, warum Sie die Software als Single-Thread-Prozess, als Multi-Thread-Prozess, oder als Multi-Prozess-Programm designen würden?)

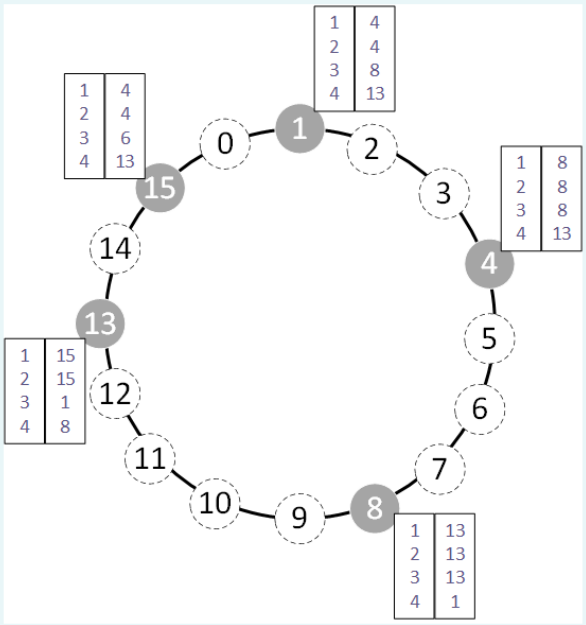
Multi-Thread-Programm: mehrere parallele Threads um z.B. an ein HTML-Dokument angehängte Multimedia-Daten gleichzeitig herunterladen zu können. Mit einem Single-Thread-Programm wäre das nicht möglich, da HTTP(S)-Requests blockierend sind.
Ein Multi Thread Programm ist in diesem Fall außerdem einem Multi-Prozess-Programm vorzuziehen, da Threads deutlich geringere Contexit-Switching Cost haben
(*Processes and Communications I*, S. 9 ff.)

Frage **14**

Richtig

Erreichte Punkte 2,00 von 2,00

Frage markieren



In the figure, you can see a simplified Chord system with a 4-bit identifier space. Grey circles denote nodes, while black/dotted circles denote other entities. For the nodes, finger tables are given. One of these finger tables is wrong, i.e., all four values given are wrong. Identify which finger table is wrong (by naming the ID of the linked node) and also provide the correct finger table entries in the boxes below.

(In der Abbildung sehen Sie ein vereinfachtes Chord-System mit 4-bit Identifikatoren. Graue Kreise kennzeichnen Knoten, schwarze/gestrichelte Kreise kennzeichnen andere Entitäten. Für die Knoten sind die sogenannten „Finger Tables" angegeben. Eine dieser „Finger Tables" ist falsch, d. h. alle vier Werte sind falsch. Identifizieren Sie, welches „Finger Table" falsch ist, indem Sie die ID des zugehörigen Knotens bestimmen und geben Sie zudem die korrekten IDs in die leeren Boxen ein.)

Finger Table von15 ist falsch. Die korrekten IDs lauten:

1. 1
2. 1
3. 4
4. 8

(*Naming*, S. 16)

Pruefung_2021-04-21

https://vowi.fsinf.at/wiki/TU_Wien:Verteilte_Systeme_VO_(Dustdar)/Pruefung_2021-04-21

Frage 1:

You have to conceptualize and implement a new backend system for the Austrian public health sector, i.e., a server-based software which is able to store all patient data and allows doctors and pharmacists to access patient-related data. Explain why you would design the server as either an iterative or a concurrent server. Assume that the software is not running on a single host, but rather in a server cluster, able to serve all incoming requests.

(Sie sollen ein neues Backend-System für das österreichische Gesundheitswesen konzipieren, d. h. eine serverbasierte Software, welche die gesamten Patientendaten speichert und es ÄrztInnen und ApothekerInnen erlaubt, auf diese Patientendaten zuzugreifen. Erklären Sie, warum Sie den Server als iterativen oder nebenläufigen ("concurrent") Server designen würden. Gehen Sie davon aus, dass Ihre Software nicht auf einem einzelnen Host läuft, sondern in einem Server-Cluster, welches alle Anfragen bearbeiten kann.)

Design als concurrent Server, da dieser mehrere Anfragen gleichzeitig bearbeiten kann und nicht blockiert. Nutzt die gegebene Ressourcen effizienter als der iterative Server.

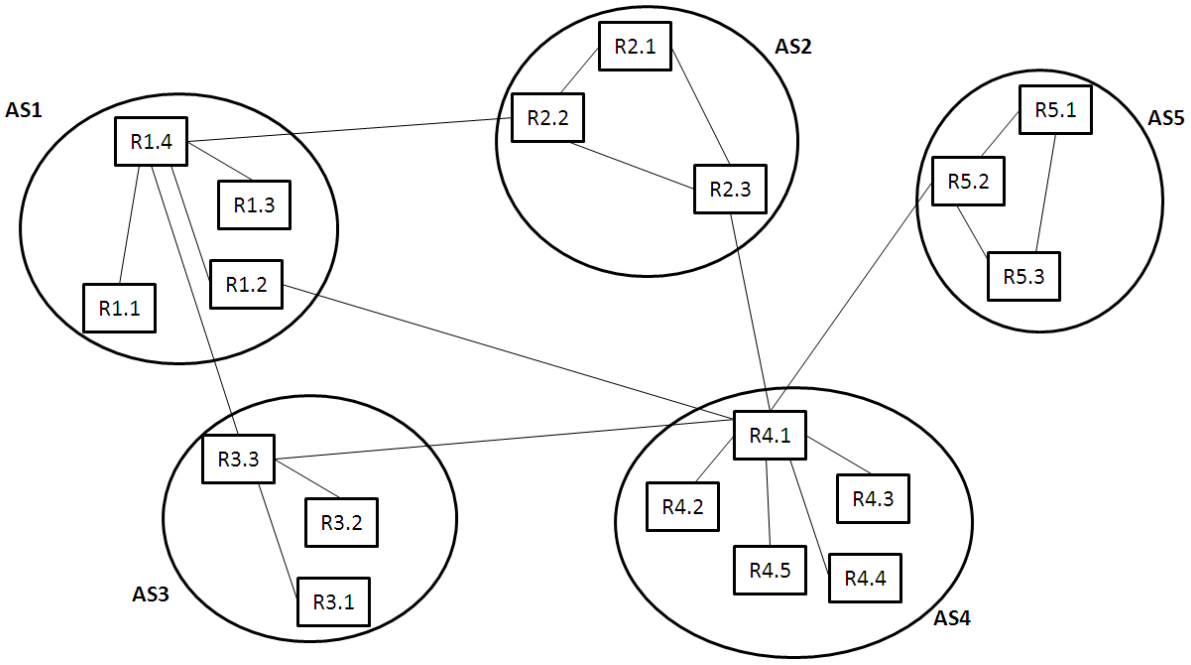
Frage 2:

Consider the following topology of Internet Autonomous Systems (ASs), where each circle corresponds to an AS. Each AS is composed of a number of interconnected routers (boxes), and ASs interconnect with each other.

(Betrachten Sie die folgende Topologie von Internet Autonomen Systemen (Internet Autonomous Systems - ASs), wobei jeder Kreis einem AS entspricht. Jedes AS besteht aus mehreren miteinander verbundenen Routern (Boxen), und ASs sind miteinander verbunden.)

You have to select where to place two replica servers. Each replica server should be placed at a router location. Execute an appropriate algorithm for replica server placement that uses the above topology as input, in order to provide a placement of the two servers. That is, decide at which router each server should be installed (e.g., “Server 1 at Router Rx.y, Server 2 at Router Rm.n”), explaining how you reached your decision step by step.

(Sie müssen auswählen, wo zwei Replikatserver platziert werden sollen. Jeder Replikatserver sollte an einem Router-Standort platziert werden. Führen Sie einen geeigneten Algorithmus für die Platzierung von Replikatservern aus, der die obige Topologie als Eingabe verwendet, um eine Platzierung der beiden Server bereitzustellen. Entscheiden Sie also, auf welchem Router jeder Server installiert werden soll (z. B. "Server 1 auf Router Rx.y, Server 2 auf Router Rm.n"), und erläutern Sie Schritt für Schritt, wie Sie zu Ihrer Entscheidung gelangt sind.)



Mittels Greedy Algorithmus aus der VO: finde größtes AS und platziere Server bei Router mit den meisten connections. Fahre fort mit zweitgrößtem AS…
Gewählt werden daher die Router **R4.1** und und **R1.4** (in dieser Reihenfolge)
(*Consistency and Replication part II*, Seite 20 ff.)

Frage 3:

Despite the fact that the Domain Name System (DNS) has been originally deployed in the 1980s, when the number of objects in the Internet was way smaller than today, DNS still works very well. One reason for this is that DNS scales very well. Please explain how DNS achieves scalability.

(Obwohl das Domain Name System (DNS) bereits in den 1980er-Jahren entwickelt wurde, als die Anzahl an Objekten im Internet sehr viel kleiner war als heute, funktioniert DNS immer noch sehr gut. Ein Grund hierfür ist, dass DNS sehr gut skaliert. Erklären Sie, wie DNS Skalierbarkeit umsetzt.)

DNS ist hierarchisch organisiert. Jede Domain wird hierarchisch aufgelöst: zuerst die TLD (Global Layer), anschließend der Administration Layer und abschließend der Managerial Layer.
Die Informationen auf Ebene des Global Layers ändern sich sehr selten und können daher gut repliziert und gecached werden, was zu einer guten Skalierbarkeit führt.
(*Naming*, S. 20 ff.)

Frage 4:

Consider the following public-key cryptosystem: (Betrachten Sie das folgende Kryptosystem mit öffentlichen Schlüsseln:)

```
   Each user's key information includes a key pair (K+, K-) and a value n, where K+ is the public key, K- is the private key, and n is a modulus used in the encryption and decryption
operations of these specific keys, as shown below. The modulus n and key K+ are public information. K- is kept secret by the user.
   (Die Schlüsselinformationen jedes Benutzers umfassen ein Schlüsselpaar (K+, K-) und einen Wert n, wobei K+ der öffentliche Schlüssel, K- der private Schlüssel und n ein Modulus
(Teilungsrest) ist, der bei den Verschlüsselungs- und Entschlüsselungsoperationen dieser spezifischen Schlüssel verwendet wird, wie nachfolgend dargestellt. Der Modulus n und der
Schlüssel K+ sind öffentliche Informationen. K- wird vom Benutzer geheim gehalten.)
```

```
   The following function is used for encryption and decryption: E(K, m, n) = mK mod n, where K is the key, m the message, and n the modulus corresponding to the specific key. When this
function is used for encryption, K is the encryption key, m is the plaintext message, and the output of the function is the ciphertext (encrypted message). When it is used for
decryption, K is the decryption key, m is the ciphertext, and the output is the original plaintext message.
   (Die folgende Funktion wird zum Ver- und Entschlüsseln verwendet: E(K, m, n) = mK mod n, wobei K der Schlüssel, m die Nachricht und n der dem spezifischen Schlüssel entsprechende
Modulus ist. Wenn diese Funktion zur Verschlüsselung verwendet wird, ist K der Verschlüsselungsschlüssel, m die Klartextnachricht und die Ausgabe der Funktion ist der Chiffretext
(verschlüsselte Nachricht). Wenn die Funktion zur Entschlüsselung verwendet wird, ist K der Entschlüsselungsschlüssel, m der Chiffretext und die Ausgabe die ursprüngliche
Klartextnachricht.)
```

```
   To produce message digests, the following hash function is used: H(m) = m mod 5, where m is the message whose hash value we want to compute, and the output is the message digest.
   (Um Nachrichtenübersichten zu erzeugen, wird die folgende Hash-Funktion verwendet: H (m) = m mod 5, wobei m die Nachricht ist, deren Hashwert wir berechnen möchten, und die Ausgabe
die Nachrichtenübersicht ist.)
```

User A wishes to send a message to user B using this cryptosystem. This plaintext message is the integer m = 8. The two users have the following keys:

(Benutzer A möchte mit diesem Kryptosystem eine Nachricht an Benutzer B senden. Diese Klartextnachricht ist die Ganzzahl m = 8. Die beiden Benutzer haben die folgenden Schlüssel:)

```
   User A: K+A = 7 (public key / öffentlicher Schlüssel), K-A = 3 (private key / privater Schlüssel), nA = 33 (modulus / Modulus),
   User B: K+B = 3 (public key / öffentlicher Schlüssel), K-B = 11 (private key / privater Schlüssel), nB = 15 (modulus / Modulus).
```

Answer the following questions filling in the correct integer values: (Beantworten Sie die folgenden Fragen und geben Sie die richtigen Ganzzahlwerte ein:)

```
   If A wishes to send the message encrypted in order to ensure confidentiality, what is the ciphertext value that B will receive?
   (Wenn A die Nachricht verschlüsselt senden möchte, um Vertraulichkeit zu gewährleisten, welchen Chiffretext erhält dann B?)
   Antwort
```

```
   If A wishes to assure B of the authenticity and integrity of the message, but not its confidentiality, what is the value of the message signature that B will receive?
   (Wenn A B die Authentizität und Integrität der Nachricht, aber nicht deren Vertraulichkeit versichern möchte, welchen Wert hat die Nachrichtensignatur, die B erhält?)
```

(Darstellungs-)Fehler in der Angabe: Die Verschlüsselungsfunktion E muss so aussehen:

E(K,m,n) = m^K mod n

- Verschlüsselte Nachricht: E(K,m,n) = E(3,8,15) = 8^3 mod 15 = 2
- Signatur: H(m) = H(8) = 8 mod 5 = 3, E(K,m,n) = E(3,3,33) = 3^3 mod 33 = 27

Frage 5:

Consider a social network where data are replicated across a number of distributed servers. Each user accesses the social network via the closest replica server.

Then, consider the following sequence of events:

```
   User A accesses the social network via replica server L1 and adds a "like" to B's profile picture.
   B accesses her profile via replica server L1 and sees the "like" from A.
   User C accesses the social network via replica server L1 and adds a "like" to B's profile picture.
   B accesses her account from a different location served by replica server L2, and sees the "like" from A but not the one from C.
```

Does this system provide monotonic read consistency and why?

(Stellen Sie sich ein soziales Netzwerk vor, in dem Daten auf mehreren verteilten Servern repliziert werden. Jeder Benutzer greift über den nächstgelegenen Replikatserver auf das soziale Netzwerk zu.

Betrachten Sie dann die folgende Abfolge von Ereignissen:

```
   Benutzer A greift über den Replikatserver L1 auf das soziale Netzwerk zu und fügt dem Profilbild von B ein "like" hinzu.
   B greift über den Replikatserver L1 auf ihr Profil zu und sieht das "like" von A.
   Benutzer C greift über den Replikatserver L1 auf das soziale Netzwerk zu und fügt dem Profilbild von B ein "like" hinzu.
   B greift von einem anderen Ort, der vom Replikatserver L2 bedient wird, auf ihr Konto zu und sieht das "like" von A, aber nicht das von C.
```

Bietet dieses System eine monotone Lesekonsistenz und warum?)

Ja, das System bietet monotonic read consistency. Per Definition muss jeder Lesezugriff das gleiche oder ein neueres Resultat liefern als vorherige Lesezugriffe. In diesem Fall wird das gleiche Resultat zurückgeliefert, wodurch die Definition erfüllt ist.
(*Consistency and Replication part I*, S. 28)

Frage 6:

You are the provider of a fitness tracking application which runs on a smartphone. The application collects useful data (e.g., user GPS coordinates, environment temperature, user velocity, heartbeat, and other health-related information) from the smartphone itself and from a wearable device (e.g., a smart watch), and sends them to a data analysis component for storage and processing. This component performs big data analytics to extract per user and aggregate fitness-related information, and provides an API to third parties to access anonymized user data for a fee. As the application provider, you have the option of running the data analysis component (i) directly on the user's smartphone, (ii) on another edge computing device of the user, or (iii) in the cloud. Which option would you select and why?

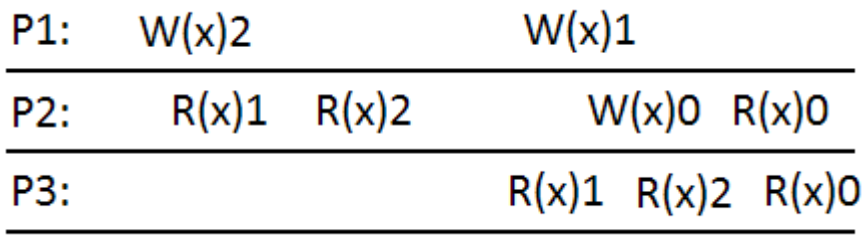
(Sie sind der Anbieter einer Fitness-Tracking-Anwendung, die auf einem Smartphone ausgeführt wird. Die Anwendung sammelt nützliche Daten (z. B. GPS-Koordinaten des Benutzers, Umgebungstemperatur, Benutzergeschwindigkeit, Herzschlag und andere gesundheitsbezogene Informationen) vom Smartphone selbst und von einem tragbaren Gerät (z. B. einer Smartwatch) und sendet sie an eine Datenanalysekomponente zur Verarbeitung und Speicherung. Diese Komponente führt Big-Data-Analysen durch, um Informationen pro Benutzer zu extrahieren und Fitnessinformationen zu aggregieren, und stellt Dritten eine API zur Verfügung, mit der sie gegen eine Gebühr auf anonymisierte Benutzerdaten zugreifen können. Als Anwendungsanbieter haben Sie die Möglichkeit, die Datenanalysekomponente (i) direkt auf dem Smartphone des Benutzers, (ii) auf einem anderen Edge-Computing-Gerät des Benutzers oder (iii) in der Cloud auszuführen. Welche Option würden Sie wählen und warum?)

Analyse in der Cloud, da hier eine deutlich bessere Scalability gegeben ist als am Smartphone bzw. einem anderen Edge-Computing-Gerät des Benutzers. Beispielsweise könnte der Nutzer über ein sehr altes Smartphone verfügen, dass für die Big-Data-Analysen zu lange braucht - in der (automatisch skalierbaren) Cloud gibt es dieses Problem nicht.

Frage 7:

Consider the following Read/Write events. Does this system provide sequential consistency? If yes, why? If not, explain why and propose an ordering that offers sequential consistency.

(Betrachten Sie die folgenden R/W-Ereignisse. Bietet dieses System sequentielle Konsistenz? Wenn ja, warum? Wenn nicht, erklären Sie warum und schlagen Sie eine Reihenfolge vor, die sequentielle Konsistenz bietet.)



Nicht sequentiell Konsistent, da 2 vor 1 geschrieben aber 1 vor 2 gelesen wird.
Würde P1 erst 1 und dann 2 schreiben, wäre das System sequentiell konsistent.
(*Consistency and Replication part I*, Seite 14 ff.)

Frage 8:

You are the lead architect for an Internet of Things system, which needs to comply with real-time requirements in a smart factory. The software runs on a central server and gathers data from various single-board computers (e.g., Raspberry Pis) which are located all over the factory's shopfloor. Communication between devices is done in a wireless fashion. Since there are many machines on the shopfloor, there could be interferences and data transfer might be faulty. In this setting, would you select TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) for the communication between server and single-board computers? Explain your choice.

(Sie sind der/die Lead-ArchitektIn für ein Internet-of-Things-System, welches Echtzeitanforderungen innerhalb einer „smarten" Fabrik erfüllen muss. Die Software läuft auf einem zentralen Server und sammelt Daten von einer Anzahl von Einplatinencomputern (z. B. Raspberry Pis), welche überall in der Fabrik verteilt sind. Die Kommunikation zwischen verschiedenen Geräten geschieht dabei drahtlos. Da sich in der Fabrik viele Maschinen befinden, kann es zu Interferenzen kommen, so dass ein Datentransfer fehlerhaft sein kann. Würden Sie in einem solchen System TCP (Transmission Control Protocol) oder UDP (User Datagram Protocol) für die Kommunikation zwischen Server und den Einplatinencomputern verwenden? Begründen Sie Ihre Wahl.)

TCP, wenn es sich um Daten handelt, die übertragen werden müssen und für Funktionieren der Fabrik wichtig sind. UDP bei Daten, die zu einem späteren Zeitpunkt keinen Sinn mehr machen z.B. Thermometer
(vergleiche 2021-02-19, Frage 1)

Frage 9:

In Paxos, the proposer needs a majority of PROMISE messages from the acceptors in order to proceed after a PREPARE message. What would happen if the proposer does not wait for such a majority of PROMISE messages? Would it still be possible to finish a Paxos run successfully? What would be the risk if doing so? Please explain your answer.

(In Paxos benötigt der Vorschlagende eine Mehrheit von PROMISE-Nachrichten von den Akzeptoren, um nach einer PREPARE-Nachricht fortfahren zu können. Was würde passieren, wenn der Vorschlagende nicht auf eine solche Mehrheit von PROMISE-Nachrichten wartet? Wäre es immer noch möglich, eine Paxos-Runde erfolgreich abzuschließen? Was wäre das Risiko dabei? Bitte erklären Sie Ihre Antwort.)

Würde nicht auf eine Mehrheit gewartet werden, könnte ein Proposer mit einem Accept-Request fortfahren, obwohl bereits ein Request mit einer höheren ID von einer Mehrheit der Akzeptoren akzeptiert wurde. Diese würden den Request zwar ignorieren, jene Akzeptoren, die den vorherigen Request aber u.U. nicht mitbekommen haben, würden den neuen Request akzeptieren. Dadurch könnte es passieren, dass verschiedene Akzeptoren verschiedene Werte akzeptieren und es somit keine einheitliche Entscheidung gibt.
(*Fault Tolerance*, Seite 22 ff.)

Frage 10:

A small company is developing a mobile application. In order to host the application's back end, which includes user authentication, authorization, and data storage functionality, the company has the option of using either an Infrastructure-as-a-Service (IaaS) or a Platform-as-a-Service (PaaS) solution. For each of the two potential cloud solutions, provide one advantage and one disadvantage.

(Ein kleines Unternehmen entwickelt eine mobile Anwendung. Um das Back-End der Anwendung zu hosten, das Benutzerauthentifizierung, Autorisierung und Datenspeicherungsfunktionen umfasst, kann das Unternehmen entweder eine Infrastructure-as-a-Service- (IaaS) oder eine Platform-as-a-Service-Lösung (PaaS) verwenden. Geben Sie für jede der beiden möglichen Cloud-Lösungen einen Vorteil und einen Nachteil an.)

IaaS:

- Vorteil: Unabhängiger von Konkretem Anbieter. Wenn dieser das Angebot einstellt, kann die VM leicht zu einem anderen Anbieter migriert werden.
- Nachteil: Viele Funktionen müssen selbst entwickelt werden, Instandhaltung der Virtuellen Maschine

Paas:

- Vorteil: Möglicherweise fertige Funktionen, die ohne viel Aufwand verwendet werden können
- Nachteil: Größere Abhängigkeit von Anbieter, wenn spezifische Lösungen verwendet werden (Migration zu anderem Anbieter schwer bis unmöglich)

Frage 11:

In the lecture, we have discussed the “election by bullying” algorithm. In this algorithm, a process sends an ELECTION message to all processes with a higher ID. Why is this necessary? If a process knows that it does not have the highest ID, why does it have to send ELECTION messages – would the algorithm not also work without these messages?

Also, would it not be an alternative to send exactly one ELECTION message only to the process with the highest ID, instead of all processes with a higher ID?

(In der Vorlesung wurde der „Bully-Algorithmus“ diskutiert. Dieser Algorithmus sorgt dafür, dass ein Prozess eine WAHL-Nachricht (ELECTION) an alle Prozesse mit einer höheren ID sendet. Warum ist dies notwendig? Wenn einem Prozess bekannt ist, dass er selbst nicht der Prozess mit der höchsten ID ist, warum sollten dann von diesem Prozess überhaupt WAHL-Nachrichten gesendet werden – würde der Algorithmus nicht auch ohne diese Nachrichten funktionieren?

Weiterhin stellt sich die Frage, ob es nicht ausreichen würde, wenn ein Prozess nur eine WAHL-Nachricht an den Prozess mit der höchsten ID senden würde, statt Nachrichten an alle Prozesse mit einer höheren ID zu senden?)

Der Prozess weiß nicht, ob die anderen Prozesse mit höherer ID online sind. Würde die Wahl-Nachricht nur vom Prozess mit der höchsten ID ausgeschickt werden, würde nie eine Wahl-Nachricht ausgeeschickt werden, da diese ja nur sinnvoll ist, wenn der Prozess mit der höchsten ID nicht online ist.
Ebenso gilt dass das System nicht mehr funktioniert, wenn nur an den Prozess mit der höchsten ID eine Wahl-Nachricht geschickt wird. Denn genau dieser Prozess mit der höchsten ID ist ja offline, wenn ein neuer Koordinator gewählt werden muss. Ist er mittlerweile wieder online, kann die Wahl ohnehin entfallen.
(*Synchronization and Coordination*, S. 30 f)

Frage 12:

A website is replicated across a large number of servers. The domain name of the website is resolved to the IP address of an HTTP load balancer. The load balancer receives a client request and dispatches it to one of the available servers in a random manner. Explain how this setup helps to provide failure transparency, and argue whether it provides replication transparency or not.

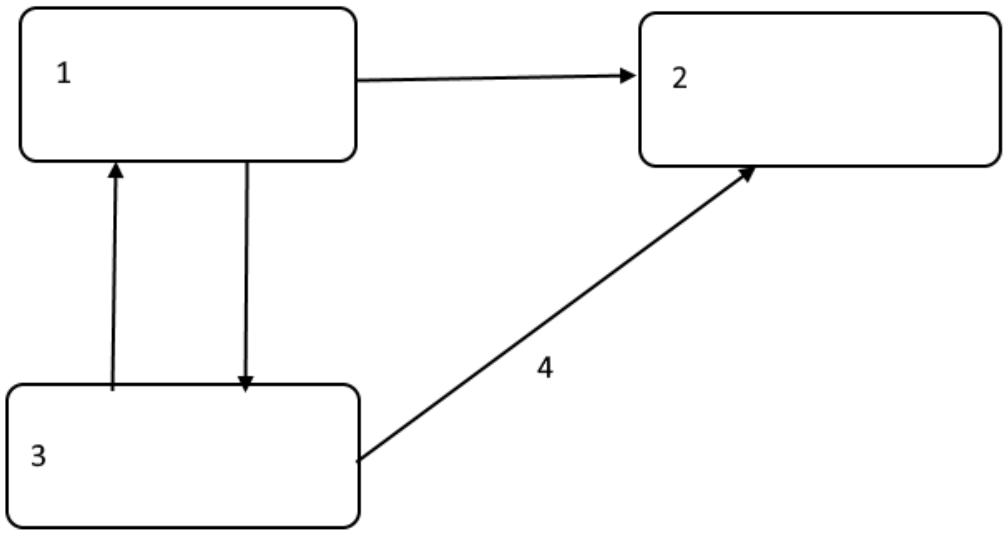
(Eine Website wird auf einer großen Anzahl von Servern repliziert. Der Domainname der Website wird in die IP-Adresse eines HTTP-Load-Balancers aufgelöst. Der Load Balancer empfängt eine Client-Anfrage und sendet sie nach einem Zufallsprinzip an einen der verfügbaren Server. Erläutern Sie, wie dieses Setup zur Bereitstellung von Fehlertransparenz beiträgt, und diskutieren Sie, ob es Replikationstransparenz bietet oder nicht.)

Fehlertransparanz: Wenn einer der Replikatsserver ausfällt, bekommt das ein Besucher der Website nicht mit.
Das System bietet auch Replikationstransparanz, da Clients einen Single Point of Entry haben und nicht merken, dass die Website Repliziert wurde.
(Consistency and Replication part II, S 35 ff.)

Pruefung 2020-08-12

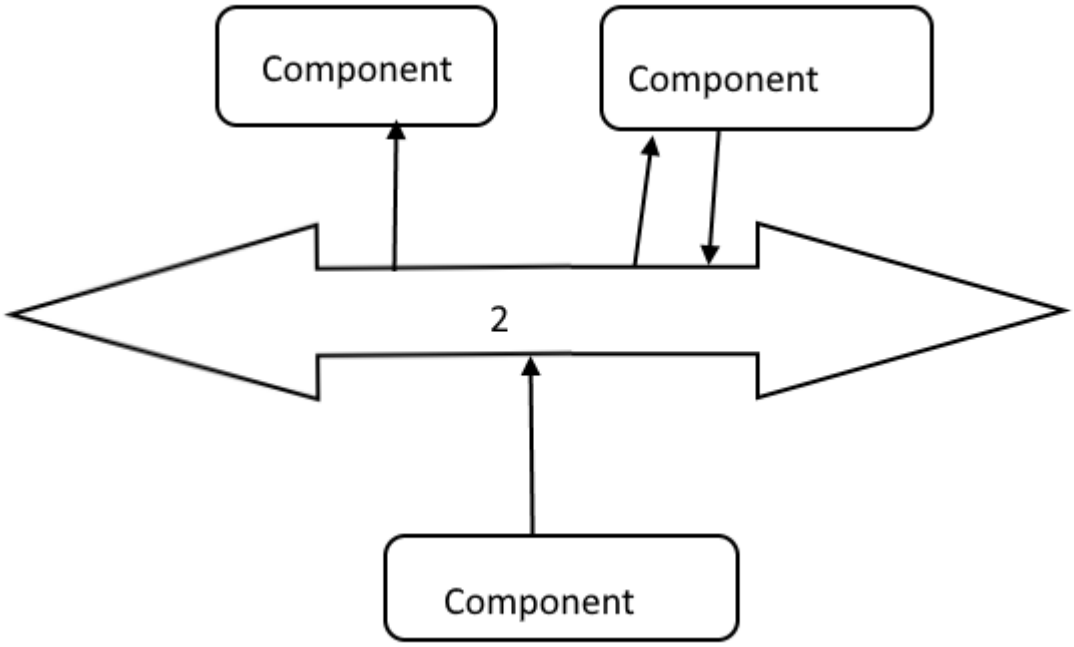
```
Die folgenden Abbildung zeigt den objektbasierten Architekturs
til. Füllen Sie die nummerierten Felder aus.
```

Aufgabe 1.1



1. Object
2. Object
3. Object
4. Method Call

```
Die folgende Abbildung zeigt den ereignisbasierten Architektur
stil. Füllen Sie die nummerierten Felder aus.
```



2. Event Bus

```
Sie haben die Aufgabe, einen Client zu eintwickeln, welcher Do
kumente von verschiedenen Servern herunterlädt. Lange Wartezei
ten sollten dabei vermieden werden. Wenn sich der Client bei e
inem Server anmeldet, erhält er zunächst eine Liste zu den Dok
umenten. Mithilfe dieser Links kann der Client diese Dokumente
von verschiedenen Servern herunterladen.
2.1: Würden Sie den Client als Single-Thread-Prozess, als Mult
i-Thread Prozess oder als Multi Prozess-Programm designen? Erk
lären Sie Ihre Wahl in max. drei Sätzen.
2.2: Ihre Client-Software verwendet Sockets für die Interaktio
n mit den Serverne. Skizzieren Sie die grundlegenden Schritte
(Kommunikationsmuster) zwischen dem Client und einem Server wä
hrend des Herunterladens einer Datei.
```

2.1: Multi Threaded Prozess. Client kann erst die Liste herunterladen und anschließend jedes Dokument mit einem eigenen Thread herunterladen

2.2:

1. Server stellt Socket zur Verfügung (bind → listen →accept)
2. Client verbindet sich (connect)
3. Client sendet, Server empfängt, verarbeitet und sendet zurück, Client empfängt

4. Wiederhole 3. so oft wie nötig
5. Close sockets

```
Beschreiben Sie in max. 3 Sätzen die grundlegende Idee von zus
tandsbehafteten (stateful) Servern und nennen Sie ein praktisc
hes Beispiel, in dem die Verwendung von zustandsbehafteten Ser
vern zu bevorzugen ist.
```

Server behält Information über Clients und kann diese bei Anfragen berücksichtigen. Kann die Performance verbessern, erhöht aber auch die Gefahr von Inkonsistenzen.
z.B. ein Server, der weiß, welche Dateien ein Client bereits zu welchem Zeitpunkt heruntergeladen hat. Wenn sich der Client erneut zur Synchronisation verbindet müssen nur die veränderten Dateien erneut heruntergeladen werden, was die Performance verbessert.
z.B.2 Content Distribution mit Push Based Protokollen. Server weiß, welche Informationen ein Client benötigt und sendet push-updates nur an diese Server

```
Sie haben die Aufgabe, in einem Peer-to-Peer-Netzwerk Informat
ionen von verschiedenen Peers abzufragen. Das Netzwerk ändert
sich stetig, was dazu führt, dass laufend Peers dem Netzwerk b
eitreten oder es verlassen. Erklären Sie in max. drei Sätzen,
ob Sie synchrone oder asynchrone Kommunikation zwischen den Pe
ers verwenden würden.
```

Asynchrone Kommunikation. Bei Synchroner Kommunikation blockiert ein Client, bis er eine Antwort des Servers erhalten hat. Da laufend Peers das Netzwerk verlassen, würde es daher oft dazu kommen, dass ein angefragter Peer nicht online ist und unnötig lange gewartet wird. Bei asynchroner Kommunikation wird nur auf den Accept-Request gewartet, nicht auf das Ergebnis der Remote Procedure, weshalb Timeouts deutlich geringer gewählt werden können.

```
Erläutern Sie in max. drei Sätzen, was ein Namensraum und eine
Namensdomäne ist. Wie ist die Beziehung zwischen diesen beiden
Konzepten?
```

Namensraum: Raum aller möglichen validen Namen, die von einem Service verwaltet werden
Namensdomäne: Namensraum, der von einer einzelnen Administrativen Autorität verwaltet wird

```
In der folgenden Tabelle finden Sie drei Beispiele für Namensinformationen. Sind diese entweder Beispiele für flache Benennung, strukturierte Benennung oder Attribut-basierte Bennenung?
Examples:
        1) uid=schahram.dustar, ou=People, dc=example, dc=at
        2) 84-99-96-45-44-55
        3) www.tuwien.ac.at
```

1. Attribut-basierte Benennung
2. Flat Naming
3. Strukturierte Benennung

```
Erklären Sie in max. drei Sätzen Fehlschläge (Failures), Störungen (Errors) oder Mängel (Faults) und wie diese drei Bedrohungen für Zuverlässigkeit zueinander in Beziehung stehen.
```

- Ein Mangel/Fault (z.B. ein Bug in einer Funktion) führt potentiell zu einer
- Störung/Error (z.B. weil ein Wert eines Funktionsaufrufs aufgrund des Bugs falsch berechnet wird - Bug wird aktiv), was wiederrum zu einem
- Fehlschlag/Failure führen kann (z.B. falscher Rückgabewert verhindert Login mit korrekten Nutzerdaten)

```
Erklären Sie in jeweils einem Satz, wie groß eine k-Fehler-tolerante Gruppe sein muss, um entweder (i) zeitliche Mängel oder (ii) Byzantinische Mängel zu tolerieren. Brgründen Sie die Gruppengrüßen.
```

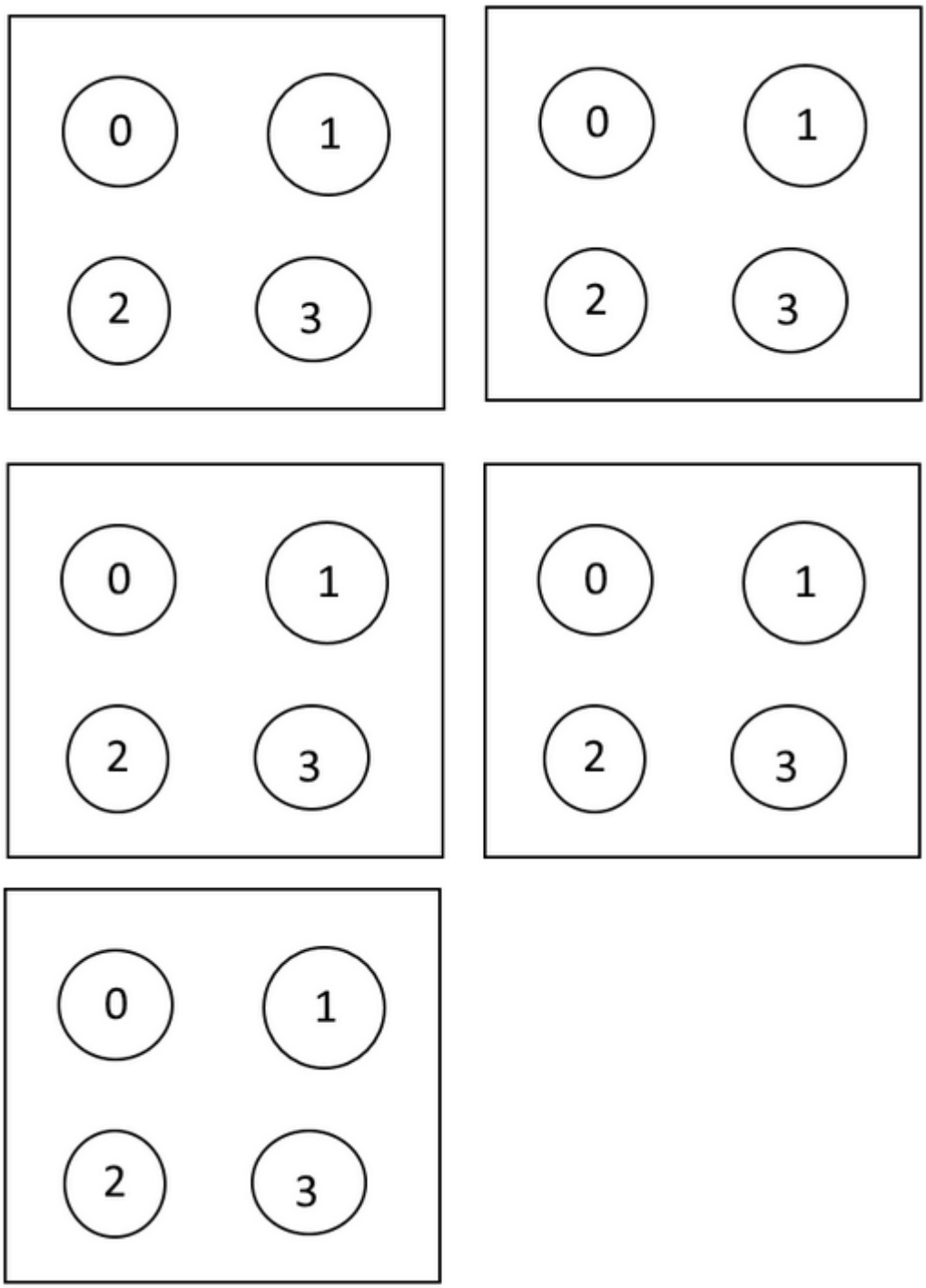
Gruppe kann die Fehlerhaftigkeit von bis k Mitgliedern tolerieren

- Zeitliche Mängel: Gruppe muss Größe k+1 haben, da es reicht, wenn ein Resultat zeitgerecht einlangt
- Byzantinische Fehler: Gruppe muss Größe 2k+1 haben, da die Korrektheit eines Ergebnisses per Mehrheitsentscheidung bestimmt wird

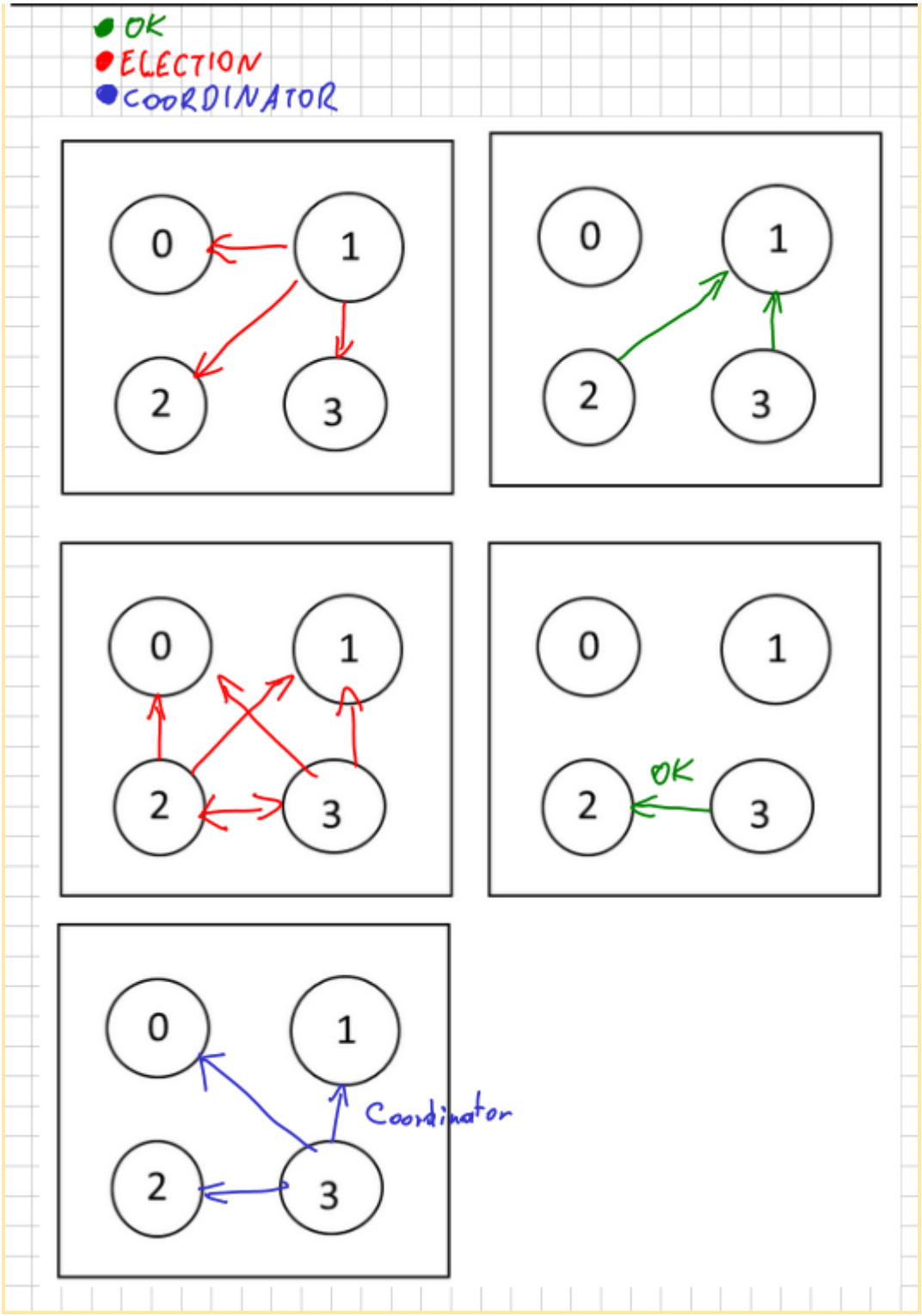
```
Im Bereich der physikalischen Uhren unterscheiden wir zwischen Präzision (precision) und Genauigkeit (accuracy). Definieren Sie diese beiden Konzepte in jeweils einem Satz.
```

Präzission: Halte Abweichungen zwischen einzelnen Prozessen in einem DS innerhalb eines Limits (interne Synchronisation)
Genauigkeit: Halte Abweichung zu Referenzwert innerhalb eines Limits (externe Synchronisation)

Vier Prozesse 0-3 nutzen den Bully-Algorithmus, um einen neuen Koordinator auszuwählen. In der Abbildung finden Sie fünf Rund en, die benötigt werden, um einen neuen Koordinator zu identif izieren. Nehmen Sie dabei an, dass Prozess 1 die Wahl anstößt. Tragen Sie für jede Runde die Nachrichten ein, welche von den Prozessen gesendet werden, d.h. WAHL-, KOORDINATOR- und OK-Nac hrichten. Hinweis: Verwenden Sie pro Runde nur einen Nachricht entypen. Antworten auf Nachrichten werden in der nachfolgenden Runde gesendet.

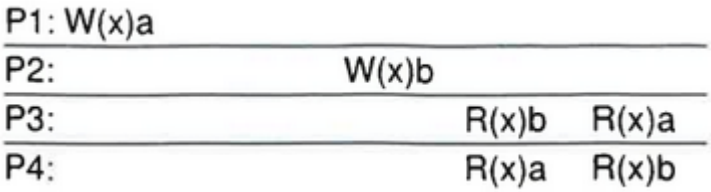


1. 1 an 2 und 3 ELECTION
2. 2 und 3 an 1 OK
3. 2 an 3 ELECTION
4. 3 an 2 OK
5. 3 an alle COORDINATOR



7.1a: Betrachten Sie die R/W-Ereignisse. Ist diese Sequenz in einem System zulässig, das kausale Konsistenz bietet? Wenn ja, warum? Wenn nicht, schlagen Sie eine kausal-konsistente-Ereignisreihenfolge vor.

```
7.1b: Geben Sie in max. 2 Sätzen ein Anwendungsbeispiel an, bei dem monotone Lesekonsistenz nützlich ist.
```



7.1a: Ja. W(x)a und W(x)b sind nicht causally related sondern concurrent, ihre Lesereihenfolge ist daher egal
7.1b: Ein online-Kalender, der auf mehreren Servern verteilt liegt (z.B. Google Kalender). Neu eingetragene (und gleich danach gelesene) Termine können nicht “verschwinden”, wenn ich den Kalender zu einem späteren Zeitpunkt über einen anderen Server erneut abrufe.

```
7.2a: Definieren Sie letztendlicher Konsistenz (eventual consistency) in einem Satz.
7.2b: Erklären Sie in maximal zwei Sätzen, warum das Domain Name System (DNS) mit letztendlicher Konsistenz gut funtioniert.
```

7.2a: Nach einem Update werden alle Replikas im Lauf einer bestimmten Zeit ebenfalls erneuert; ist nur möglich wenn es keine gleichzeitigen Schreib-Zugriffe gibt
7.2b: Jede Domain wird von einer zentralen Autorität verwaltet, weswegen es keine gleichzeitigen Änderungen geben kann.

```
Nennen Sie einen Vorteil und einen Nachteil von Push-basierten Protokollen zur Verteilung von Inhalten.
```

Vorteil: Consistency wird schneller erreicht, da Clients nicht nach updates fragen müssen
Nachteil: Schlechte Saklierbarkeit, wenn alle Clients auf einmal upgedated werden sollen

```
Nennen Sie einen Vorteil von nicht-blockierenden Primär-Backup-Konsistenzprotokollen.
```

Da nicht auf Antwort aller Prozesse gewartet werden muss, sind nicht-blockierende Primär-Backup-Konsistenzprotokolle resilient gegenüber dem Ausfall einzelner Prozesse.

```
Geben Sie in max. zwei Sätzen eine Definition von starker Kollisionsresistenz.
```

Es ist nicht möglich, zwei unterschiedliche Eingaben zu finden, die die gleiche Ausgabe eine kryptographischen Funktion erzeugen.

```
Nennen Sie einen Grund, warum wir typischerweise eine Nachtrichten-Kurzfassung digital signieren, der einer von einer Hash-Funktion erstellt wird, anstelle der Nachricht selbst.
```

Um Signaturwerte kurz zu halten?
Do not mix authentication and secrecy

```
Während der Errichtung eines sicheren Kanals zwischen zwei Parteien verwenden die kommunizierenden Parteien nach Abschluss der Authentifizierungsphase im Allgemeinen einen eindeutigen gemeinsamen Sitzungsschlüssel für die Vertraulichkeit, der verworfen wird, wenn der sichere Kanal nicht mehr verwendet wird. Nennen Sie zwei Vorteile dieses Ansatzes.
```

- Keys können leichter geknackt werden, je öfter sie verwendet werden
- Wird für jede Session der gleiche Key verwendet, können alte Nachrichten in eine neue Session eingefügt werden, da die Verschlüsselung gleich geblieben ist

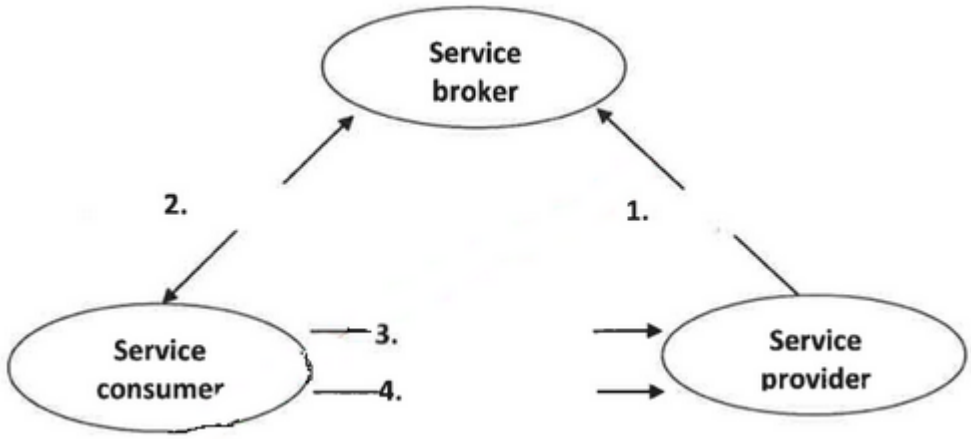
```
Erläutern Sie das Konzept der Ressourcenüberversorgung anhand einer Abbildung.
```

Kapazität einer Ressource ist höher, als der tatsächliche Bedarf

```
Nennen Sie ein Problem, mit dem ein Dienstanbieter möglicherweise konfrontiert ist, wenn Ressourcen nicht ausreichend bereitgestellt werden.
```

Nicht alle Clients können bedient werden, was zu verlorenen Umsätzen und Kunden führen kann

```
Serviceorientierte Architekturen umfassen drei maßgebliche Rollen, wie in der folgenden Abbildung dargestellt wird. Die nummerierten Pfeile geben die Abfolge der Vorgänge an, die zum Aufrufen eines Service ausgeführt werden müssen. Beschriften Sie die Pfeile.
```



1. Veröffentliche Service
2. Finde Service
3. Bind Service
4. Führe Service aus

Bsp mit korrekten benoteten Lösungen

Frage 1
Vollständig
Erreichte Punkte 1,00 von 1,00
Frage markieren

Consider a social network where data are replicated across a number of distributed servers. Each user accesses the social network via the closest replica server.

Then, consider the following sequence of events:

1. User A accesses the social network via replica server L1 and adds a "like" to B's profile picture.
2. B accesses his profile via replica server L1 and sees the "like" from A.
3. User C accesses the social network via replica server L1 and adds a "like" to B's profile picture.
4. B accesses her account from a different location served by replica server L2, and sees the "like" from A but not the one from C.

Does this system provide monotonic read consistency and why?

(Stellen Sie sich ein soziales Netzwerk vor, in dem Daten auf mehreren verteilten Servern repliziert werden. Jeder Benutzer greift über den nächstgelegenen Replikatserver auf das soziale Netzwerk zu.

Betrachten Sie dann die folgende Abfolge von Ereignissen:

1. *Benutzer A greift über den Replikatserver L1 auf das soziale Netzwerk zu und fügt dem Profilbild von B ein "like" hinzu.*
2. *B greift über den Replikatserver L1 auf sein Profil zu und sieht das "like" von A.*
3. *Benutzer C greift über den Replikatserver L1 auf das soziale Netzwerk zu und fügt dem Profilbild von B ein "like" hinzu.*
4. *B greift von einem anderen Ort, der vom Replikatserver L2 bedient wird, auf ihr Konto zu und sieht das "like" von A, aber nicht das von C.*

Bietet dieses System eine monotone Lesekonsistenz und warum?)

It does, because even though the newest value is not accessed in L2, B can see the amount of likes they had read before, so the previously read value is still accessed.

Frage 5
Vollständig
Erreichte Punkte 1,00 von 1,00
Frage markieren

Consider the following Read/Write events. Does this system provide sequential consistency? If yes, why? If not, explain why and propose an ordering that offers sequential consistency.

(Betrachten Sie die folgenden R/W-Ereignisse. Bietet dieses System sequentielle Konsistenz? Wenn ja, warum? Wenn nicht, erklären Sie warum und schlagen Sie eine Reihenfolge vor, die sequentielle Konsistenz bietet.)

P1:	W(y)0		W(y)2		
P2:		W(y)1			
P3:			R(y)1	R(y)2	R(y)0
P4:		R(y)1		R(y)2	R(y)0

No, it does not. In P1 there are two writing operations which happen one after the other, first y gets assigned the value 0, and then the value 2. However, in P3 and P4 where y is read, its value changes from 2 to 0, implying that the writing operations happened the other way around, and so changing the specified order. If in P3 and P4 the values of y read 0, 2 and 1 or 0, 1 and 2, the system would provide sequential consistency.

Frage 10
Vollständig
Erreichte Punkte 2,00 von 2,00
Frage markieren

Consider the following example of a distributed system: A user wishes to access a web resource, which is replicated at different server locations managed by a content delivery network (CDN). To access the resource, the user places a URL of the form http://www.example.com.cdn-x.com/resource.html in the browser's address bar. The resource content will eventually be delivered over the closest CDN server location. Explain if location and replication transparency are provided or not.

(Betrachten Sie das folgende Beispiel eines verteilten Systems: Ein Benutzer möchte auf eine Webressource zugreifen, die an verschiedenen Serverstandorten repliziert wird, welche von einem Content-Delivery-Netzwerk (CDN) verwaltet werden. Um auf die Ressource zuzugreifen, fügt der Benutzer eine URL der Form http://www.example.com.cdn-x.com/resource.html in die Adressleiste des Browsers ein. Der Ressourceninhalt wird schlussendlich über den nächstgelegenen CDN-Serverstandort bereitgestellt. Erläutern Sie, ob Standort- und Replikationstransparenz gewährleistet sind oder nicht.)

Both are provided, because the user can only connect through the URL, which does not give any information as to where the server is located and the replication of the server is also in no way shown to the user.

Frage **7**

Vollständig

Erreichte Punkte 1,00 von 1,00

Frage markieren

An online game for mobile devices involves rendering in real time complex game scenes. This requires a lot of processing and has stringent latency requirements so that a smooth user experience is provided to the player. The application developers have created the game software in such a way that rendering can be offloaded to a remote service component, which sends back game scenes to the mobile device. This involves streaming of real-time high-definition video to the device. Would you run this rendering service at an edge computing server or in the Cloud and why?

(Bei einem Online-Spiel für mobile Geräte werden komplexe Spielszenen in Echtzeit gerendert. Dies erfordert viel Rechenaufwand und stellt strenge Latenzanforderungen, sodass dem Spieler eine reibungslose Benutzererfahrung geboten werden kann. Die Anwendungsentwickler haben die Spielesoftware so erstellt, dass das Rendern auf eine Remote-Service-Komponente verlagert werden kann, die Spielszenen an das mobile Gerät zurücksendet. Dies beinhaltet das Streaming von hochauflösendem Echtzeitvideo auf das Gerät. Würden Sie diesen Rendering-Service auf einem Edge-Computing-Server oder in der Cloud ausführen und warum?)

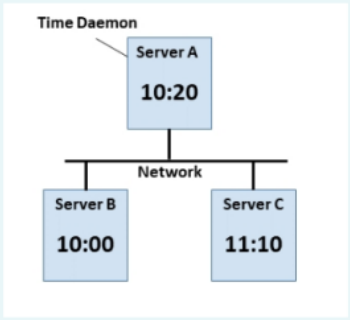
To increase performance and so that the game runs faster, I would run the rendering servie at an edge computing service, however if the high definition video were to be the client's priority I would run it in the Cloud, since it has more capacity to render the video.

Weitere Bsp

Explain why HTTP-based communication is usually transient and synchronous. What are the benefits of this communication approach?

(Erklären Sie, warum HTTP-basierte Kommunikation üblicherweise transient (flüchtig) und synchron ist. Was sind die Vorteile eines solchen Kommunikationsansatzes?)

Da transient, müssen keine Nachrichten gespeichert werden. Der Vorteil ist außerdem, dass die Implementation von transienten und synchronen System einfach geht im Vergleich zu asynchroner/persistener Kommunikation (z.B. keine aufwendigen Speicherungsabläufe um Nachrichten zu speichern). Da synchron ist das aber auch nicht notwendig, da Clients warten, bis ihre Anfrage behandelt wurde.



Three servers use the Berkeley Algorithm in order to adjust their clocks. In the figure, you will find these three servers as well as their according clocks, with Server A being the time daemon. To adjust the clocks using the Berkeley Algorithm, three rounds of message passing between the servers are performed.

Below, fill in the messages which are sent in these three rounds. It is already indicated which server sends a message to which other server, but you have to fill in the numbers.

(Drei Server nutzen den Berkeley-Algorithmus zum Uhrenabgleich. In der Grafik sehen Sie diese drei Server sowie deren Uhren; Server A dient als Zeitdämon. Um die Uhrzeiten anzupassen, werden beim Berkeley-Algorithmus Nachrichten in drei Runden ausgetauscht.

Füllen Sie die Nachrichten, welche in diesen drei Runden gesendet werden, bitte in die entsprechenden Felder ein. Es ist bereits angegeben, welcher Server eine Nachricht an welchen anderen Server sendet, aber Sie müssen noch die entsprechenden Werte eintragen.)

Round 1:

- *Server A to Server A:* 10:20 ✔
- *Server A to Server B:* 10:20 ✔
- *Server A to Server C:* 10:20 ✔

Round 2:

- *Server A to Server A:* 0 ✔
- *Server B to Server A:* -20 ✔
- *Server C to Server A:* +50 ✔

Round 3:

- *Server A to Server A:* +15 ✘
- *Server A to Server B:* +35 ✘
- *Server A to Server C:* -35 ✘

Round 3:

- A to A: +10
- A to B: +30
- A to C: -40

You are connected to the Internet via a public Wi-Fi hotspot, which only allows traffic on TCP port 80 (HTTP), TCP port 443 (HTTPS) and UDP port 53 (unencrypted DNS). All other traffic is filtered. The Wi-Fi hotspot inspects unencrypted DNS queries and blocks them if they request to resolve forbidden domain names. How can you bypass this filtering and access forbidden websites when you only know their domain name (i.e., you do not know their IP addresses to access them directly)?

(Sie sind über einen öffentlichen Wi-Fi-Hotspot mit dem Internet verbunden, der nur Datenverkehr über TCP-Port 80 (HTTP), TCP-Port 443 (HTTPS) und UDP-Port 53 (unverschlüsseltes DNS) zulässt. Der gesamte andere Datenverkehr wird gefiltert. Der Wi-Fi-Hotspot überprüft unverschlüsselte DNS-Abfragen und blockiert sie, wenn sie die Auflösung verbotener Domainnamen anfordern. Wie können Sie diese Filterung umgehen und auf verbotene Websites zugreifen, wenn Sie nur deren Domainnamen kennen (d. h. die IP-Adressen nicht kennen, um direkt darauf zuzugreifen)?)

Mittels DNS over HTTPS (DoH). Ich leite meine DNS-Requests um (verwende dabei nicht den klassischen Stub Resolver meines Computers) und schicke sie über Port 443 mittels HTTPS direkt an einen Recursive Resolver. Dieser schickt mir anschließend über HTTPS die Auflösung meines Requests zurück.

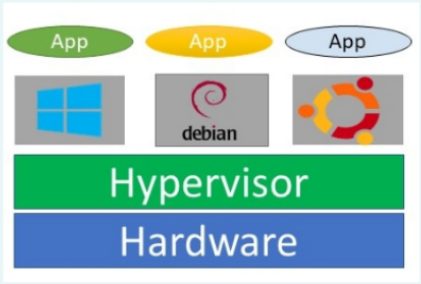
For each of the following two examples, name the Cloud Computing service model that characterizes it.

1. A client uses a Cloud-based system to store arbitrary data objects.
2. A Cloud provider makes available a video conferencing service.

(Nennen Sie für jedes der beiden folgenden Beispiele das entsprechende Cloud-Computing-Dienstmodell.

1. *Ein Client verwendet ein Cloud-basiertes System, um beliebige Datenobjekte zu speichern.*
2. *Ein Cloud-Anbieter stellt einen Videokonferenzdienst zur Verfügung.)*

1. IaaS - Cloud Infrastructure as a Service (in diesem Fall Speicher-Infrastruktur wie z.B. Amazon S3)
2. SaaS - Cloud Software as a Service



In the figure, you see a so-called hypervisor, which provides the means to virtualize a system. Out of the three different types of virtual machines we have discussed in the lecture, which one is equivalent to this type of hypervisor? In addition, name the benefits of this approach, compared to the other two types of virtual machines.

(In der Abbildung ist ein sogenannter Hypervisor abgebildet, welcher die Funktionalitäten zur Virtualisierung eines Systems zur Verfügung stellt. Welcher der drei Typen von virtuellen Maschinen, die wir in der Vorlesung kennengelernt haben, ist äquivalent zu diesem Hypervisor-Typen? Bitte nennen Sie zusätzlich die Vorteile dieses Ansatzes, verglichen mit den beiden anderen Typen von virtuellen Maschinen.)

Native VM Monitor

- Performance-Vorteile gegenüber Hosted VM Monitor, da der Hypervisor direkt auf der Hardware läuft und kein darunterliegendes Betriebssystem benötigt.
- Im Gegensatz zu einer Process VM können jedoch komplett voneinander unabhängige VMs gehostet werden (z.B. shutdown der Windows-VM beeinträchtigt die Debian-VM und darauf ausgeführte App nicht).

We use Paxos in order to find consensus in a distributed system made up from five acceptors and one proposer – these are the only nodes in our system, but they may not be online at the same time, since the system is faulty.

Each acceptor has stored information about the last message ID it promised, and an accepted value (note: "---" means that no value has been accepted for this ID):

- Acceptor 1: ID 5, Value "---"
- Acceptor 2: ID 5, Value "---"
- Acceptor 3: ID 4, Value "Green"
- Acceptor 4: ID 4, Value "Green"
- Acceptor 5: ID 4, Value "Green"

Is this an acceptable state in a valid Paxos run, i.e., can this state be reached if Paxos has run correctly? If this is not a valid state, explain the reason for it. If it is a valid state, explain why the acceptors can store two different IDs.

(Wir nutzen Paxos, um Konsensus in einem verteilten System zu erreichen, welches aus fünf Akzeptoren und einem Vorschlagenden besteht – dies sind die einzigen Knoten in unserem System, aber sie müssen nicht zwangsläufig zum gleichen Zeitpunkt online sein, da das System fehlerhaft ist.

Jeder Akzeptor hat Informationen über die letzte „versprochene" (engl. „promise") Nachrichten-ID sowie den momentan akzeptierten Wert gespeichert (Hinweis: „---" bedeutet, dass kein Wert für diese ID akzeptiert wurde):

- Akzeptor 1: ID 5, Wert "---"
- Akzeptor 2: ID 5, Wert "---"
- Akzeptor 3: ID 4, Wert "Grün"
- Akzeptor 4: ID 4, Wert "Grün"
- Akzeptor 5: ID 4, Wert "Grün"

Ist dies ein zulässiger Zustand in einem validen Paxos-Durchlauf? Kann dieser Zustand also erreicht werden, wenn Paxos korrekt ausgeführt wurde? Falls es sich um keinen validen Zustand handelt, geben Sie den Grund hierfür an. Falls es sich um einen validen Zustand handelt, erklären Sie, warum die Akzeptoren zwei verschiedene IDs gespeichert haben.)

Zulässiger Zustand, der folgendermaßen erreicht werden kann:

1. Akzeptoren 1 und 2 sind offline
2. Proposer sendet PREPARE 4
3. Akzeptoren 3, 4 und 5 senden PROMISE 4
4. Proposer hat eine Mehrheit erhalten und sendet ACCEPT-REQUEST 4 ‘Grün’
5. Akzeptoren 3, 4 und 5 senden ACCEPT 4 ‘Grün’
6. Akzeptoren 1 und 2 kommen online
7. Akzeptoren 3, 4 und 5 gehen offline
8. Proposer sendet PREPARE 5
9. Akzeptoren 1 und 2 senden PROMISE 5
10. Proposer hat keine Mehrheit erhalten und hört deswegen auf

(*Fault Tolerance*, Seite 22 ff.)

The university has installed surveillance cameras at the entrances of all its buildings, which capture and transmit high-definition video. The video is received by a service that executes a face recognition application, and stores the video and the results of the processing. These data include personally identifiable information, such as faces of students, their identities and other personal data. You have the option to host this service either at the University's on-premise servers or in the Cloud. Which option would you select and why?

(Die Universität hat an den Eingängen aller Gebäude Überwachungskameras installiert, die hochauflösende Videos aufnehmen und übertragen. Das Video wird von einem Dienst empfangen, der eine Gesichtserkennungsanwendung ausführt und das Video und die Ergebnisse der Verarbeitung speichert. Diese Daten umfassen personenbezogene Daten wie Gesichter von Studierenden, deren Identität und andere personenbezogene Daten. Sie haben die Möglichkeit, diesen Dienst entweder auf den lokalen Servern der Universität oder in der Cloud zu hosten. Welche Option würden Sie wählen und warum?)

Ich würde das System deaktivieren, da es nicht DSGVO-konform ist.
Wenn mir das egal ist, würde ich den Dienst auf den lokalen Servern der Uni hosten und dieses verteilte System nicht mit dem Internet verbinden, um maximale Sicherheit der personenbezogenen Daten zu garantieren (wenn jemand über das Internet mein System hacken würde, würde ja auffliegen, dass ich illegale Überwachung betreibe - das gilt es zu verhindern!).
Bei Nutzung einer Cloud-Lösung gibt es außerdem die Gefahr, dass der Anbieter eine Sicherheitslücke offen gelassen - auf einem eigenen Server kann man selbst sicherstellen, dass das nicht der Fall ist.

Two replica servers need to be placed, and there are three candidate locations (L1, L2, L3). The replica servers will serve three clients and, for each client, its distance in terms of latency to any of the locations L1, L2, and L3 is known and is given in the table below (each cell of the table shows the latency for the respective client to reach a location):

(Es müssen zwei Replikatserver platziert werden, und es gibt drei Kandidatenstandorte (L1, L2, L3). Die Replikatserver bedienen drei Clients, und für jeden Client ist die Entfernung in Bezug auf die Latenz zu einem der Standorte L1, L2 und L3 bekannt und in der folgenden Tabelle angegeben (jede Zelle der Tabelle zeigt die Latenz für den jeweiligen Client um einen Ort zu erreichen):)

Latency for a user to reach a location *(Latenz für einen Client einen Ort erreichen)*	**L1**	**L2**	**L3**
Client 1	10	150	20
Client 2	200	20	250
Client 3	100	10	30

Execute a **greedy server placement algorithm** that aims to **minimize the total latency** experienced by the clients and provide the derived placement below:

*(Führen Sie einen **gierigen (engl. "greedy") Server-Platzierungsalgorithmus** aus, der darauf abzielt, die **Gesamtlatenz der Clients zu minimieren** und die folgende abgeleitete Platzierung bereitzustellen:)*

- Location of Server 1, selected at step 1 of the algorithm *(Speicherort von Server 1, ausgewählt in Schritt 1 des Algorithmus)*: L2 ✔
- Location of Server 2, selected at step 2 of the algorithm *(Speicherort von Server 2, ausgewählt in Schritt 2 des Algorithmus)*: L1 ✔
- Total latency of the solution (**sum** of the latencies of all clients in the given solution) *(Gesamtlatenz der Lösung (**Summe** der Latenzen aller Clients in der angegebenen Lösung))*: ✖

Die Latenz ergibt sich wie folgt:

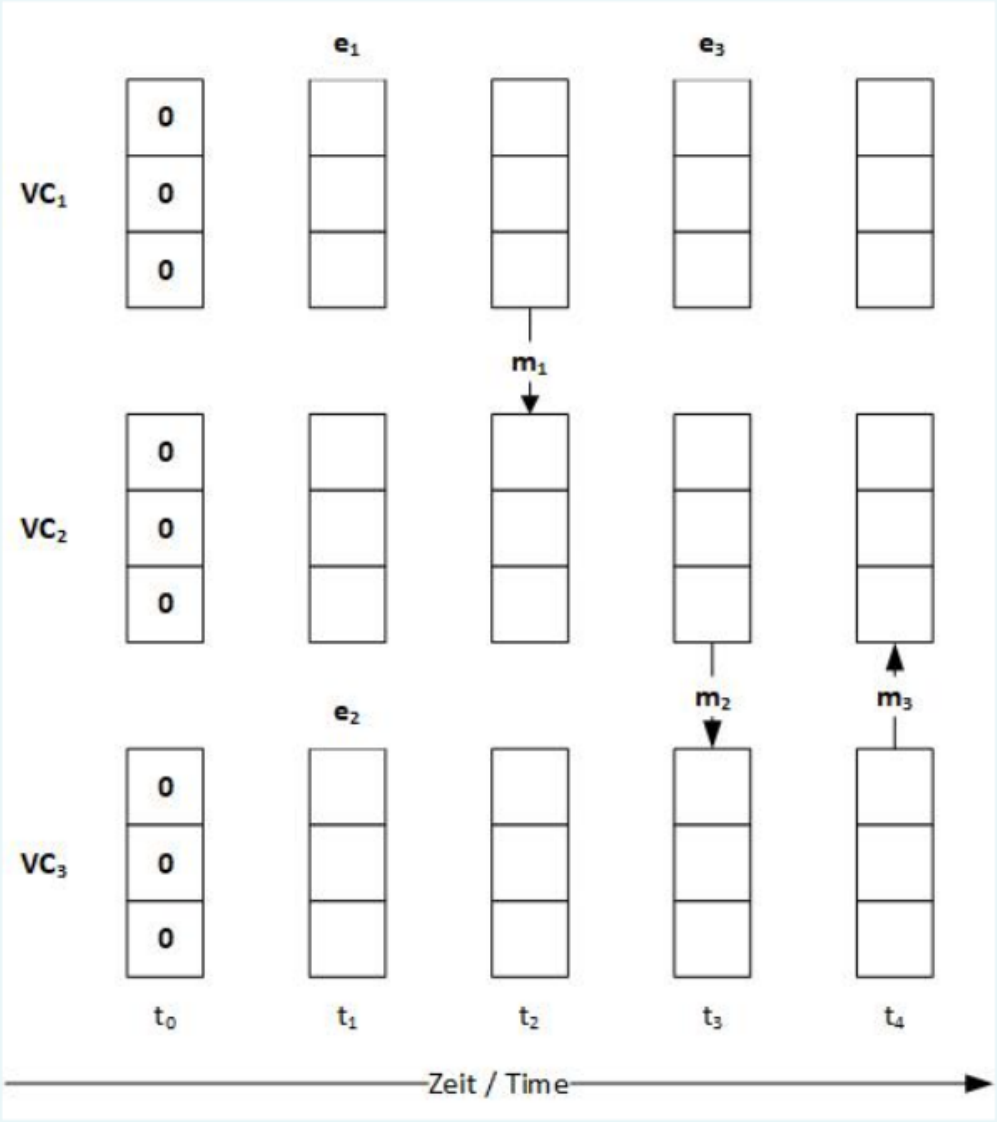
- Client 1 verbindet sich mit L1: 10
- Client 2 verbindet sich mit L2: 20
- Client 3 verbindet sich mit L2: 10

Gesamte Latenz daher 40

Entities A and B wish to establish a secret key using the Diffie-Hellman protocol. The public information that A selects as the configuration of the system is **n = 19** (modulo) and **g = 3** (base). What is the secret key that will be derived if A and B pick values **a = 3** and **b = 2**, respectively, as their private information, and how is this key derived?

*(Die Entitäten A und B möchten einen geheimen Schlüssel unter Verwendung des Diffie-Hellman-Protokolls einrichten. Die öffentliche Information, die A als Konfiguration des Systems auswählt, ist **n = 19** (Modulo) und **g = 3** (Basis). Was ist der geheime Schlüssel, der abgeleitet wird, wenn A und B die Werte **a = 3** bzw. **b = 2** als private Informationen auswählen, und wie wird dieser Schlüssel abgeleitet?)*

- A berechnet g^a mod n = 3^3 mod 19 = 8 und schickt n, g und den berechneten Wert 8 an b
- B berechnet 8^b mod n = 8^2 mod 19 = 7. 7 Ist der geheime Key
- B sendet g^b mod n = 3^2 mod 19 = 9 an A
- A berechnet 9^a mod n = 9^3 mod 19 = 7. Jetzt kennt auch A den geheimen Key


e1
e3
VC1
0
0
0
m1
VC2
0
0
0
m2
m3
e2
VC3
0
0
0
t0
t1
t2
t3
t4
Zeit / Time

Three processes p_1, p_2 and p_3 use vector clocks VC_1, VC_2 and VC_3, respectively. In the figure above, you see the initial state of the vector clocks as well as some events e_x and messages m_y. Fill in the missing values of the vector clocks for each time step t_{1-4} in the format (X,Y,Z), e.g., (0,0,1). This is important, your answer is not graded correctly if you use a different format. If the vector value is not defined yet, use "0" to indicate this. In your answers, do not use blanks, but provide the brackets.

Hints: To simplify the figure, the vector clocks are shown in parallel for the three processes. Fill in all empty boxes, even if there is no change for a particular process. Events only apply to one process and are applied instantly to the according vector clock. Messages are delivered instantly (which is of course not possible in reality).

(Drei Prozesse p_1, p_2 und p_3 verwenden jeweils eine Vektoruhr VC_1, VC_2 bzw. VC_3. In der Abbildung sehen Sie den initialen Status der Vektoruhren sowie Ereignisse e_x und Nachrichten m_y. Tragen Sie die fehlenden Werte der Vektoruhren für die einzelnen Zeitpunkte t_{1-4} ein. Nutzen Sie das Format (X,Y,Z), z. B. (0,0,1). Dies ist wichtig, weil Ihre Antworten nicht korrekt ausgewertet werden, falls Sie ein anderes Format nutzen. Falls ein Vektorwert bisher nicht definiert wurde, nutzen Sie "0", um dies anzugeben. Verwenden Sie in Ihren Antworten keine Leerzeichen, aber geben Sie die Klammern an.

Hinweise: Um die Grafik einfacher zu gestalten, werden die Vektoruhren für die drei Prozesse parallel dargestellt. Füllen Sie alle leeren Felder ein, auch wenn es keine Änderung für einen bestimmten Prozess gibt. Ereignisse wirken sich nur auf einen Prozess aus und werden sofort auf die Vektoruhr angewendet. Nachrichten werden sofort ausgeliefert (was natürlich in der Realität nicht der Fall ist.))

VC_1:

- t_1: (1,0,0)
- t_2: (2,0,0)
- t_3: (3,0,0)
- t_4: (3,0,0)

VC_2:

- t_1: (0,0,0)
- t_2: (2,1,0)
- t_3: (2,2,0)
- t_4: (2,2,2)

VC_3:

- t_1: (0,0,1)
- t_2: (0,0,1)
- t_3: (2,2,1)
- t_4: (2,2,2)

Kommentar:
You unfortunately did not increase the receiving vector clocks for m2 and m3, while you did this for m1. The other mistakes are subsequent mistakes, so I increased the automatic grading from

VC1: (1,0,0) - (2,0,0) - (3,0,0) - (3,0,0)
VC2: (0,0,0) - (2,1,0) - (2,2,0) - (2,3,3)
VC3: (0,0,1) - (0,0,1) - (2,2,2) - (2,2,3)

Let's assume that we are making use of flat naming in a distributed system. The network is very stable, i.e., nodes/entities are very seldomly changing their locations and the number of nodes/entities also does not change a lot. Would you rather use Hierarchical Location Services or Forward Pointers for such a distributed system? Motivate your answer.

(Nehmen wir einmal an, dass wir flache/unstrukturierte Benennung in einem verteilten System verwenden. Das Netzwerk ist sehr stabil, d. h. Knoten/Entitäten wechseln nur sehr selten Ihren Standort und die Menge an Knoten/Entitäten ändert sich auch kaum. Würden Sie eher Hierarchical Location Services (Hierarchische Lokalisierungs-Dienste) oder Vorwärtszeiger (Forward Pointers) für solch ein verteiltes System verwenden? Motivieren Sie Ihre Antwort.)

HLS ist in diesem Fall besser geeignet, da man bei seltenen Umstrukturierungen viele Informationen cachen kann. Dadurch kann die Performance verbessert werden.

In a Peer-to-Peer network, you need to request information from different peers. Since the network is ever-changing, peers are leaving and entering the network constantly. Briefly explain (in max. three sentences) why you would use Multicasting or Remote-Procedure Calls (RPC) to request the information.

(Sie haben die Aufgabe, in einem Peer-to-Peer-Netzwerk Information von verschiedenen Peers abzufragen. Das Netzwerk ändert sich stetig, was dazu führt, dass laufend Peers dem Netzwerk beitreten oder es verlassen. Erklären Sie in max. drei Sätzen, warum Sie Multicasting oder Fernprozeduraufrufe (engl. Remote Procedure Calls - RPC) für Ihre Abfragen verwenden würden.)

Multicasting ist in diesem Fall besser geeignet. RPC kann sehr ineffizient werden, wenn viele der angefragten Peers nicht mehr verfügbar sind. Über Flooding oder Gossip-based-multicasting können Peers in einem sich stetig ändernden Netzwerk besser erreicht werden.

Two replica servers need to be placed, and there are three candidate locations (L1, L2, L3). The replica servers will serve three clients and, for each client, its distance in terms of latency to any of the locations L1, L2, and L3 is known and is given in the table below (each cell of the table shows the latency for the respective client to reach a location):

(Es müssen zwei Replikatserver platziert werden, und es gibt drei Kandidatenstandorte (L1, L2, L3). Die Replikatserver bedienen drei Clients, und für jeden Client ist die Entfernung im Hinblick auf die Latenz zu einem der Standorte L1, L2 und L3 bekannt und in der folgenden Tabelle angegeben (jede Zelle der Tabelle zeigt die Latenz für den jeweiligen Client, um einen Ort zu erreichen):

Latency for a client to reach a location *(Latenz für einen Client um einen Ort erreichen)*	**L1**	**L2**	**L3**
Client 1	100	100	100
Client 2	40	50	60
Client 3	100	15	15

Execute a **greedy server placement algorithm** that aims to **minimize the total latency** experienced by the clients and provide the derived placement below:

*(Führen Sie einen **gierigen (engl. "greedy") Server-Platzierungsalgorithmus** aus, der darauf abzielt, die **Gesamtlatenz der Clients zu minimieren** und die folgende abgeleitete Platzierung bereitzustellen:)*

- Server 1 auf **L2** (hat geringste Gesamtlatenz zu allen Clients)
- Server 2 auf **L1** (Latenz zu Client 1 und Client 3 ist nicht mehr zu verbessern, deshalb kann bei der Auswahl von Server 2 alleine die Latenz von Client 2 beachtet werden)
- Gesamtlatenz: 100 (C1 zu L1 bzw. L2) + 40 (C2 zu L1) + 15 (C3 zu L2) = **155**

(Stellen Sie sich ein soziales Netzwerk vor, in dem Daten auf mehreren verteilten Servern repliziert werden. Jeder Benutzer greift über den nächstgelegenen Replikatserver auf das soziale Netzwerk zu. Wir gehen von folgenden Annahmen aus:

- *Es gibt 3 Benutzer in diesem sozialen Netzwerk, A, B und C.*
- *Es gibt zwei Replikatserver, L1 und L2.*
- *Zu Beginn sind die Lese- und Schreibsätze jedes Benutzers leer.*

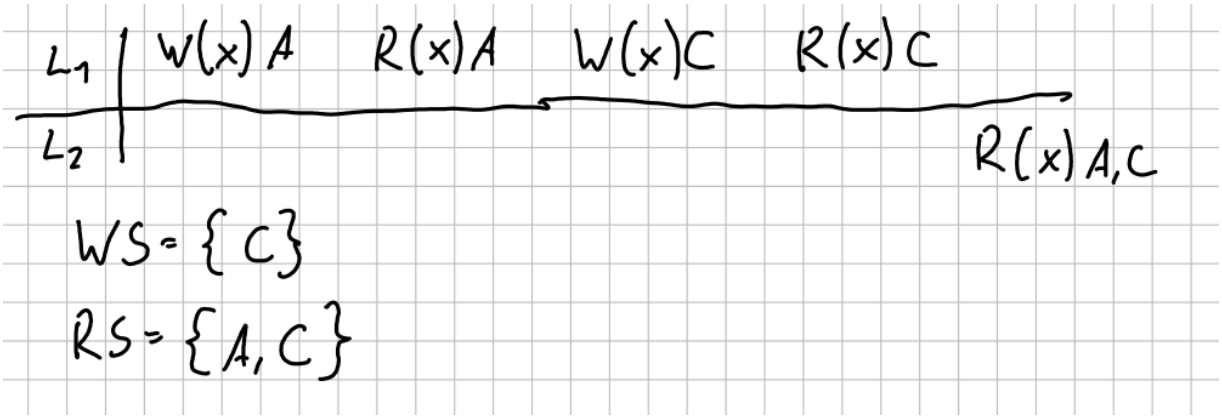
Betrachten Sie dann die folgende Abfolge von Ereignissen:

1. *Benutzer A greift über L1 auf das soziale Netzwerk zu und fügt dem Profilbild von B ein "like" hinzu.*
2. *B greift über L1 auf sein Profil zu und sieht das "like" von A.*
3. *Benutzer C greift über L1 auf das Profilbild von B zu und fügt ihm ein "like" hinzu. Nehmen Sie an, dass C direkt nach dem Hinzufügen des "like" das Profilbild von B erneut liest.*
4. *Am nächsten Tag sieht B das Profilbild von einem anderen Ort aus, der vom Server L2 bedient wird, und sieht die "likes" von A und C.*

*Unter der Annahme einer naiven Implementierung eines clientzentrierten Konsistenzprotokolls für **monotone Lesekonsistenz**, was sind die Inhalte der **Lese-** und **Schreibsätze** (read and write sets) von C am Ende der obigen Abfolge von Ereignissen?)*

- Read Set: (LikePP A-B, LikePP C-B)
- Write Set: (LikePP C-B)

Wobei LikePP X-Y bedeutet dass User X das Profilbild von User Y geliked hat



Consider the following **public-key cryptosystem**:
*(Betrachten Sie das folgende **Kryptosystem mit öffentlichen Schlüsseln**:)*

- Each user's key information includes a key pair **(K^+, K^-)** and a value **n**, where **K^+** is the **public key**, **K^-** is the **private key,** and **n** is a **modulus** used in the encryption and decryption operations of these specific keys, as shown below. The modulus n and key K^+ are public information. K^- is kept secret by the user.
  *(Die Schlüsselinformationen jedes Benutzers umfassen ein Schlüsselpaar **(K^+, K^-)** und einen Wert **n**, wobei **K^+** der **öffentliche Schlüssel**, **K^-** der **private Schlüssel** und **n** ein **Modulus (Teilungsrest)** ist, der bei den Verschlüsselungs- und Entschlüsselungsoperationen dieser spezifischen Schlüssel verwendet wird, wie nachfolgend dargestellt. Der Modulus n und der Schlüssel K^+ sind öffentliche Informationen. **K^-** wird vom Benutzer geheim gehalten.)*

- The following function is used for encryption and decryption: **$E(K, m, n) = m^K \bmod n$**, where K is the key, m the message, and n the modulus corresponding to the specific key. When this function is used for **encryption**, K is the encryption key, m is the **plaintext** message, and the output of the function is the **ciphertext** (encrypted message). When it is used for **decryption**, K is the decryption key, m is the **ciphertext,** and the output is the original **plaintext** message.
  *(Die folgende Funktion wird zum Ver- und Entschlüsseln verwendet: **$E(K, m, n) = m^K \bmod n$**, wobei K der Schlüssel, m die Nachricht und n der dem spezifischen Schlüssel entsprechende Modulus ist. Wenn diese Funktion zur **Verschlüsselung** verwendet wird, ist K der Verschlüsselungsschlüssel, m die **Klartextnachricht** und die Ausgabe der Funktion ist der **Chiffretext** (verschlüsselte Nachricht). Wenn die Funktion zur **Entschlüsselung** verwendet wird, ist K der Entschlüsselungsschlüssel, m der **Chiffretext** und die Ausgabe die ursprüngliche **Klartextnachricht**.)*

- To produce the **hash** of a message, the following function is used: **$H(m) = m \bmod 5$**, where m is the message whose hash value we want to compute, and the output is the hash of the message.
  *(Um den **Hash** einer Nachricht zu erzeugen, wird die folgende Funktion verwendet: **$H(m) = m \bmod 5$,** wobei m die Nachricht ist, deren Hashwert wir berechnen möchten, und die Ausgabe der Hash der Nachricht ist.)*

User A wishes to send a message to user B using this cryptosystem. This plaintext message is the integer **m = 3**. The two users have the following keys:

*(Benutzer A möchte mit diesem Kryptosystem eine Nachricht an Benutzer B senden. Diese Klartextnachricht ist die Ganzzahl **m = 3**. Die beiden Benutzer haben die folgenden Schlüssel:)*

- User A: $\mathbf{K^+_A = 7}$ (public key / *öffentlicher Schlüssel*), $\mathbf{K^-_A = 3}$ (private key / *privater Schlüssel*), $\mathbf{n_A = 33}$ (modulus / *Modulus*),
- User B: $\mathbf{K^+_B = 3}$ (public key / *öffentlicher Schlüssel*), $\mathbf{K^-_B = 11}$ (private key / *privater Schlüssel*), $\mathbf{n_B = 15}$ (modulus / *Modulus*).

Answer the following questions filling in the correct integer values:
(Beantworten Sie die folgenden Fragen und geben Sie die richtigen Ganzzahlwerte ein:)

- If A wishes to send the message encrypted in order to ensure **confidentiality**, what is the **ciphertext** that B will receive?
  *(Wenn A die Nachricht verschlüsselt senden möchte, um **Vertraulichkeit** zu gewährleisten, welchen Chiffretext erhält dann B?)*

- If A wishes to assure B of the **authenticity** and **integrity** of the message, but not its confidentiality, what is the value of the message **signature** that B will receive?
  *(Wenn A B die **Authentizität** und **Integrität** der Nachricht, aber nicht deren Vertraulichkeit versichern möchte, welchen Wert hat die Nachrichtensignatur, die B erhält?)*

1. Verschlüsselte Nachricht von A an B: *E(K,m,n) = m^K mod n = 3^3 mod 15 = 12*
   Verwendet Public Key von B und Modulus von B
2. Signatur der Nachricht von A an B:
   a. *H(m) = m mod 5 = 3 mod 5 = 3*
   b. *E(K,m,n) = m^K mod n = H(m)^K mod n = 3^3 mod 33 = 27*
   Verwendet Private Key von A und Modulus von A

We use Paxos in order to find consensus in a distributed system made up from five acceptors and one proposer – these are the only nodes in our system, but they may not be online at the same time, since the system is faulty.

Each acceptor has stored information about the last message ID it promised, and an accepted value (note: "---" means that no value has been accepted for this ID):

- Acceptor 1: ID 5, Value "---"
- Acceptor 2: ID 4, Value "Blue"
- Acceptor 3: ID 4, Value "Blue"
- Acceptor 4: ID 3, Value "Green"
- Acceptor 5: ID 4, Value "Blue"

Which value can the proposer actually propose in this situation through an "ACCEPT-REQUEST" message? Explain your choice.

(Wir nutzen Paxos, um Konsensus in einem verteilten System zu erreichen, welches aus fünf Akzeptoren und einem Vorschlagenden besteht – dies sind die einzigen Knoten in unserem System, aber sie müssen nicht zwangsläufig zum gleichen Zeitpunkt online sein, da das System fehlerhaft ist.

Jeder Akzeptor hat Informationen über die letzte „versprochene" (engl. „promise") Nachrichten-ID sowie den momentan akzeptierten Wert gespeichert (Hinweis: „---" bedeutet, dass kein Wert für diese ID akzeptiert wurde):

- Akzeptor 1: ID 5, Wert "---"
- Akzeptor 2: ID 4, Wert "Blau"
- Akzeptor 3: ID 4, Wert "Blau"
- Akzeptor 4: ID 3, Wert "Grün"
- Akzeptor 5: ID 4, Wert "Blau"

Welchen Wert kann der Vorschlagende hier mittels einer „ACCEPT-REQUEST"-Nachricht vorschlagen? Erläutern Sie Ihre Wahl.)

~~The proposer checks if already accepted values have been received. In this case this could be "Green" or "Blue". If at least one of the Acceptors 2,3 or 5 is online the Proposer will choose the value "Blue" since the Proposer always uses the value with the highest ID. If None of these Acceptors are online, the Proposer will choose Acceptor 4, i.e. "Green". If Acceptor 4 is also not online and only Acceptor 1 is online then the Proposer will suggest its own value.~~

The Proposer can only suggest the value "Blue" because "Blue" is the only value that has a majority in the system. If none of the "Blue" nodes are online the Proposer will not continue at all because it needs a majority of "PROMISE" messages to continue.

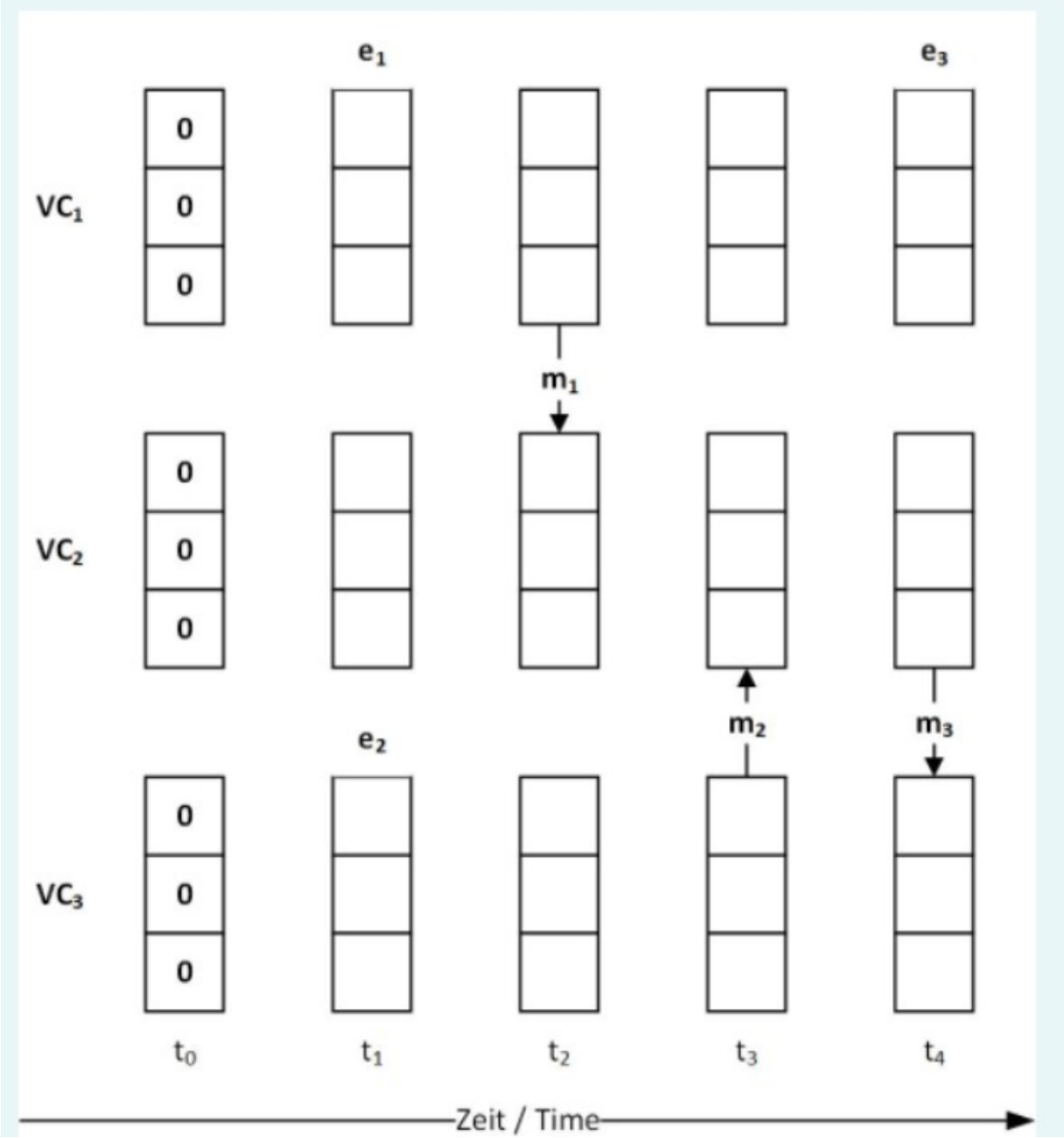
The Domain Name System (DNS) is best-known for resolving the names of hosts, i.e., finding the IP address for a domain name.

Let's assume that our host changes its location frequently, with communication always done through changing Wi-Fi connections, i.e., the network connection is changed frequently. To resolve the name of our host, would you rather recommend iterative or recursive name resolution? Motivate your choice.

(Das Domain-Name-System (DNS) ist vor allem als Mechanismus für das Auflösen von Hostnamen bekannt, d. h. die IP zu einem Domainnamen zu finden.

Nehmen wir an, dass unser Host sehr häufig den Ort wechselt, wobei die Kommunikation stets über wechselnde WLAN-Verbindungen geschieht, d. h. die Netzwerkverbindung wechselt häufig. Würden Sie rekursive oder iterative Namensauflösung empfehlen, um den Namen unseres Hosts aufzulösen? Motivieren Sie Ihre Wahl.)

In diesem Fall ist iterative Namensauflösung besser geeignet, da ein Zugriffspunkt-Wechsel während der Auflösung hier ein geringeres Problem darstellt. Die einzelnen Bestandteile der Domain können problemlos nacheinander über verschiedene Verbindungen aufgelöst werden.



Three processes p_1, p_2 and p_3 use vector clocks VC_1, VC_2 and VC_3, respectively. In the figure above, you see the initial state of the vector clocks as well as some events e_x and messages m_y. Fill in the missing values of the vector clocks for each time step t_{1-4} in the format (X,Y,Z), e.g., (0,0,1). This is important, your answer is not graded correctly if you use a different format. If the vector value is not defined yet, use "0" to indicate this. In your answers, do not use blanks, but provide the brackets.

Hints: To simplify the figure, the vector clocks are shown in parallel for the three processes. Fill in all empty boxes, even if there is no change for a particular process. Events only apply to one process and are applied instantly to the according vector clock. Messages are delivered instantly (which is of course not possible in reality).

(Drei Prozesse p_1, p_2 und p_3 verwenden jeweils eine Vektoruhr VC_1, VC_2 bzw. VC_3. In der Abbildung sehen Sie den initialen Status der Vektoruhren sowie Ereignisse e_x und Nachrichten m_y. Tragen Sie die fehlenden Werte der Vektoruhren für die einzelnen Zeitpunkte t_{1-4} ein. Nutzen Sie das Format (X,Y,Z), z. B. (0,0,1). Dies ist wichtig, weil Ihre Antworten nicht korrekt bewertet werden, falls Sie ein anderes Format nutzen. Falls ein Vektorwert bisher nicht definiert wurde, nutzen Sie "0", um dies anzugeben. Verwenden Sie in Ihren Antworten keine Leerzeichen, aber geben Sie die Klammern an.

Hinweise: Um die Grafik einfacher zu gestalten, werden die Vektoruhren für die drei Prozesse parallel dargestellt. Füllen Sie alle leeren Felder ein, auch wenn es keine Änderung für einen bestimmten Prozess gibt. Ereignisse wirken sich nur auf einen Prozess aus und werden sofort auf die jeweilige Vektoruhr angewendet. Nachrichten werden sofort ausgeliefert (was natürlich in der Realität nicht der Fall ist.))

- VC1: (1,0,0) - (2,0,0) - (2,0,0) - (3,0,0)
- VC2: (0,0,0) - (2,1,0) - (2,2,2) - (2,3,2)
- VC3: (0,0,1) - (0,0,1) - (0,0,2) - (2,3,3)

The university wishes to provide a platform where lecturers will be streaming their lectures live to students. For this purpose, it has the option of either (i) using an Infrastructure-as-a-Service solution to host an open-source video conferencing platform, or (ii) using a Software-as-a-Service solution. For each option, provide one advantage and one disadvantage.

(Die Universität möchte eine Plattform bieten, auf der Dozenten ihre Vorlesungen live an Studierende übertragen können. Zu diesem Zweck besteht die Möglichkeit, entweder (i) eine Infrastructure-as-a-Service-Lösung zum Hosten einer Open-Source-Videokonferenzplattform zu verwenden oder (ii) eine Software-as-a-Service-Lösung zu verwenden. Geben Sie für jede Option einen Vorteil und einen Nachteil an.)

IaaS:

- Vorteil: Universität hat volle Kontrolle darüber, was für ein System eingesetzt und wie dieses Konfiguriert wird
- Nachteil: Größerer Wartungs- und i.A. Installationsaufwand

SaaS:

- Vorteil: Geringer Wartungs- und Installationsaufwand, kann u.U. auch von einem technisch nicht sehr versierten Nutzer eingerichtet werden
- Nachteil: Geringere Flexibilität bei der Einrichtung des Systems und u.U. starke Bindung an einem speziellen Anbieter (Migration zu anderem Anbieter kann schwer bis gar nicht möglich sein)

Consider a social network where data are replicated across a number of distributed servers. Each user accesses the social network via the closest replica server. We make the following assumptions:

- There are 3 users in this social network, A, B, and C.
- There are two replica servers, L1 and L2.
- Initially, the read and write sets of each user are empty.

Then, consider the following sequence of events:

1. User A accesses the social network via L1 and adds a "like" to B's profile picture.
2. B accesses his profile via L1 and sees the "like" from A.
3. User C accesses the social network via L1 and adds a "like" to B's profile picture.
4. The next day, B views the profile picture from a different location served by server L2, and sees the "like" from A but not the one from C.

Assuming a naive implementation of a client-centric consistency protocol for **monotonic read** consistency, what are the contents of B's **read** and **write sets** at the end of the above sequence of events?

(Stellen Sie sich ein soziales Netzwerk vor, in dem Daten auf mehreren verteilten Servern repliziert werden. Jeder Benutzer greift über den nächstgelegenen Replikatserver auf das soziale Netzwerk zu. Wir gehen von folgenden Annahmen aus:

- *Es gibt 3 Benutzer in diesem sozialen Netzwerk, A, B und C.*
- *Es gibt zwei Replikatserver, L1 und L2.*
- *Zu Beginn sind die Lese- und Schreibsätze jedes Benutzers leer.*

Betrachten Sie dann die folgende Abfolge von Ereignissen:

1. *Benutzer A greift über L1 auf das soziale Netzwerk zu und fügt dem Profilbild von B ein "like" hinzu.*
2. *B greift über L1 auf sein Profil zu und sieht das "like" von A.*
3. *Benutzer C greift über L1 auf das soziale Netzwerk zu und fügt dem Profilbild von B ein "like" hinzu.*
4. *Am nächsten Tag sieht B das Profilbild von einem anderen Ort aus, der vom Server L2 bedient wird, und sieht das "like" von A, aber nicht das von C.*

*Unter der Annahme einer naiven Implementierung eines clientzentrierten Konsistenzprotokolls für **monotone Lesekonsistenz**, was sind die Inhalte der **Lese-** und **Schreibsätze** (read and write sets) von B am Ende der obigen Abfolge von Ereignissen?)*

- Read Set: (LikePP A-B)
- Write Set: ()

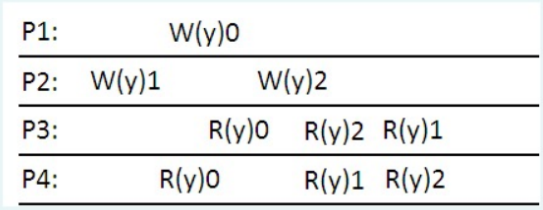
Wobei LikePP X-Y bedeutet dass User X das Profilbild von User Y geliked hat

Consider the following Read/Write events.

- Does this system provide causal consistency? Why/Why not?
- Does this system provide sequential consistency? If yes, why? If not, explain why and propose an ordering that offers sequential consistency.

(Betrachten Sie die folgenden R/W-Ereignisse.

- *Bietet dieses System kausale Konsistenz? Warum/Warum nicht?*
- *Bietet dieses System sequentielle Konsistenz? Wenn ja, warum? Wenn nicht, erklären Sie warum und schlagen Sie eine Reihenfolge vor, die sequentielle Konsistenz bietet.)*



- Nicht kausal konsistent, da die Schreiboperationen von P2 möglicherweise kausal zusammenhängen, aber von P3 und P4 in unterschiedlicher Reihenfolge gelesen werden
- Nicht sequentiell Konsistent, da P3 und P4 unterschiedliche Reihenfolgen der Schreiboperationen von P2 beobachten.
  Würden sowohl P4 als auch P3 die Reihenfolge R(y)0 → R(y)1 → R(y)2 beobachten, würde sequentielle Konsistenz gelten

In a Peer-to-Peer network, you need to request information from different peers. The network is stable, i.e., peers are not leaving or entering the system. Would you use Flooding-based Multicasting or Gossip-based Data Dissemination in order to request the information? Your goal is to query as many peers as possible. Explain your choice in max. three sentences.

(Sie haben die Aufgabe, in einem Peer-to-Peer-Netzwerk Informationen von verschiedenen Peers abzufragen. Das Netzwerk ist stabil, d. h. Peers verlassen oder betreten das Netzwerk nicht. Erklären Sie in max. drei Sätzen, ob Sie „Flooding-based Multicasting" (dt. „Flut-basiertes Multicast") oder „Gossip-basierte Datendissemination" nutzen würden, um die Informationen abzufragen. Ihr Ziel soll es dabei sein, möglichst viele Peers abzufragen.)

Flooding-based Multicasting, da damit maximal viele Peers erreicht werden können. Gossip-based Data Dissemination garantiert nicht, dass jeder Peer erreicht wird.

You have to develop a weather app, running on a smartphone. The app does not only provide the smartphone user with weather forecasts, but is also gathering data from the smartphone sensors. This is done in order to be able to do "participatory sensing", i.e., users contribute by providing data from their smartphone sensors like temperature, humidity, noise levels, etc. over time to a server. Based on this input, the server then generates individualized maps showing the noise level, current humidity, etc. for a paticular timespan, e.g., a week. Should the server be rather stateful or stateless? Explain your choice.

(Sie sollen eine Wetter-App für Smartphones entwickeln. Die App bietet dem Smartphone-Nutzer nicht nur einen Wetterbericht an, sondern sammelt auch Daten von den Smartphone-Sensoren. Dies wird gemacht, um „participatory sensing" (dt. „partizipatorische Erfassung") durchzuführen, d. h. Nutzer liefern über einen bestimmten Zeitraum Daten von den Smartphone-Sensoren, z. B. Temperatur, Luftfeuchtigkeit, Geräuschlevel etc. an einen Server. Der Server generiert basierend auf diesen Daten dann individualisierte Karten, welche die Geräuschbelastung, aktuelle Luftfeuchtigkeit etc. in einem Zeitraum (z. B. einer Woche) anzeigen. Würden Sie den Server eher zustandslos (engl. „stateless") oder zustandsbehaftet (engl. „stateful") designen? Erklären Sie Ihre Antwort.)

In diesem Fall ist ein zustands-behafteter Server die bessere Wahl, da der Server individualisierte Karten erstellen soll. Dafür müssen Daten der Clients gespeichert werden.

Let's assume we've got a Paxos run with eight acceptors and two proposers. Because of network issues, we end up with two partitions of nodes, each containing four acceptors and one proposer. The two partitions (more precisely: the nodes in each partition) agree on two different values in the Paxos run. Would this work? If not, explain why this will not happen.

(Wir haben einen Paxos-Durchlauf mit acht Akzeptoren und zwei Vorschlagenden. Aufgrund von Netzwerkproblemen erhalten wir aber zwei Partitionen, mit jeweils vier Akzeptoren und einem Vorschlagenden. Die beiden Partitionen (oder genauer: die Knoten in jeder Partition) einigen sich auf zwei unterschiedliche Werte in diesem Paxos-Durchlauf. Würde dies funktionieren? Falls nicht, erklären Sie, warum dies nicht geschieht.)

Dies würde nicht funktionieren, da ein Proposer eine Mehrheit der Akzeptoren hinter sich haben muss, um einen Accept-Request senden zu können. Diese Mehrheit kann im gegebenen Beispiel keiner der beiden Proposer vorweisen.

An autonomous vehicle is equipped with a navigation system that works as follows: Every second, it receives the vehicle's coordinates from a GPS hardware module and transmits them over a 4G mobile network connection to a navigation server in an HTTP request. The navigation server is hosted in the Cloud and the navigation system in the vehicle knows the server's domain name (e.g., navigation.server.org). The navigation server then executes an algorithm and provides in its HTTP response instructions to the vehicle, considering the destination of the vehicle and knowledge about the current traffic conditions. Explain if: (i) this system provides migration transparency; (ii) this system provides location transparency from the perspective of the vehicle.

(Ein autonomes Fahrzeug ist mit einem Navigationssystem ausgestattet, das wie folgt funktioniert: Jede Sekunde empfängt es die Fahrzeugkoordinaten von einem GPS-Hardwaremodul und überträgt sie in einer HTTP-Anfrage über eine 4G-Mobilfunknetzverbindung an einen Navigationsserver. Der Navigationsserver wird in der Cloud gehostet und das Navigationssystem im Fahrzeug kennt den Domänennamen des Servers (z. B. navigation.server.org). Der Navigationsserver führt dann einen Algorithmus aus und liefert in seiner HTTP-Antwort Anweisungen an das Fahrzeug unter Berücksichtigung des Ziels des Fahrzeugs und des Wissens über die aktuellen Verkehrsbedingungen. Erklären Sie, ob: (i) dieses System Migrationstransparenz bietet; (ii) dieses System aus Sicht des Fahrzeugs Standorttransparenz bietet.)

Migration Transparency: Ist gegeben, da der Server umgezogen werden kann. Solange der Domänenname anschließend auf den neuen Standort verweist, bekommt das Auto nicht aktiv mit, dass ein Umzug stattgefunden hat.

Location Transparency: Ist gegeben, da das Auto nur den Domänenname des Servers kennt und nicht weiß, wo dieser Server tatsächlich steht.

Frage **1**

Vollständig

Erreichte Punkte 0,00 von 1,00

Frage markieren

Imagine a distributed storage which stores 100 objects and has 100 users. A single user is the administrator, who has read-write access to all files, while all other users have read-write access to a single file each, and no rights on other files. You have the option to select either a **matrix** or a **list** (Access Control List) as the data structure to implement the **Access Control Matrix**. Which data structure would you select and why? Explain in maximum two sentences.

*(Stellen Sie sich einen verteilten Speicher vor, in dem 100 Objekte gespeichert sind und der 100 Benutzer hat. Ein einzelner Benutzer ist der Administrator, der Lese- / Schreibzugriff auf alle Dateien hat, während alle anderen Benutzer Lese- / Schreibzugriff auf jeweils eine einzelne Datei haben und keine Rechte an anderen Dateien haben. Sie haben die Möglichkeit, entweder eine **Matrix** oder eine **Liste** (Zugriffssteuerungsliste) als Datenstruktur für die Implementierung der **Zugriffssteuerungsmatrix** auszuwählen. Welche Datenstruktur würden Sie auswählen und warum? Erklären Sie dies in maximal zwei Sätzen.)*

Eine Liste, da diese im gegebenen Fall deutlich platzsparender ist. Die Matrix hätte 10.000 Datenfelder, von denen 9801 Felder leer wären. Legt man für jedes Dokument eine Liste an, kann man all diese leeren Felder und damit Speicherplatz einsparen.

Frage **2**

Vollständig

Erreichte Punkte 1,00 von 1,00

Frage markieren

Entities A and B wish to establish a secret key using the Diffie-Hellman protocol. The public information that A selects as the configuration of the system is **n = 17** (modulo) and **g = 3** (base). What is the secret key that will be derived if A and B pick values **a = 3** and **b = 2**, respectively, as their private information, and how is this key derived?

*(Die Entitäten A und B möchten einen geheimen Schlüssel unter Verwendung des Diffie-Hellman-Protokolls einrichten. Die öffentliche Information, die A als Konfiguration des Systems auswählt, ist **n = 17** (Modulo) und **g = 3** (Basis). Was ist der geheime Schlüssel, der abgeleitet wird, wenn A und B die Werte **a = 3** bzw. **b = 2** als private Informationen auswählen, und wie wird dieser Schlüssel abgeleitet?)*

- A an B: n, g und g^a mod n = 10
- B berechnet geheimen Schlüssel mittels 10^b mod n = **15**
- B an A: g^b mod n = 9
- A berechnet geheimen Schlüssel mittels 9^a mod n = **15**

We use Paxos in order to find consensus in a distributed system made up from five acceptors and one proposer – these are the only nodes in our system, but they may not be online at the same time, since the system is faulty.

Each acceptor has stored information about the last message ID it promised, and an accepted value (note: "---" means that no value has been accepted for this ID):

- Acceptor 1: ID 5, Value "---"
- Acceptor 2: ID 5, Value "---"
- Acceptor 3: ID 4, Value "Green"
- Acceptor 4: ID 4, Value "Green"
- Acceptor 5: ID 4, Value "Green"

Is this an acceptable state in a valid Paxos run, i.e., can this state be reached if Paxos has run correctly? If this is not a valid state, explain the reason for it. If it is a valid state, explain why the acceptors can store two different IDs.

(Wir nutzen Paxos, um Konsensus in einem verteilten System zu erreichen, welches aus fünf Akzeptoren und einem Vorschlagenden besteht – dies sind die einzigen Knoten in unserem System, aber sie müssen nicht zwangsläufig zum gleichen Zeitpunkt online sein, da das System fehlerhaft ist.

Jeder Akzeptor hat Informationen über die letzte „versprochene" (engl. „promise") Nachrichten-ID sowie den momentan akzeptierten Wert gespeichert (Hinweis: „---" bedeutet, dass kein Wert für diese ID akzeptiert wurde):

- Akzeptor 1: ID 5, Wert "---"
- Akzeptor 2: ID 5, Wert "---"
- Akzeptor 3: ID 4, Wert "Grün"
- Akzeptor 4: ID 4, Wert "Grün"
- Akzeptor 5: ID 4, Wert "Grün"

Ist dies ein zulässiger Zustand in einem validen Paxos-Durchlauf? Kann dieser Zustand also erreicht werden, wenn Paxos korrekt ausgeführt wurde? Falls es sich um keinen validen Zustand handelt, geben Sie den Grund hierfür an. Falls es sich um einen validen Zustand handelt, erklären Sie, warum die Akzeptoren zwei verschiedene IDs gespeichert haben.)

Zulässiger Zustand, der folgendermaßen erreicht werden kann:

1. Akzeptoren 1 und 2 sind offline
2. Proposer sendet PREPARE 4
3. Akzeptoren 3, 4 und 5 senden PROMISE 4
4. Proposer sendet ACCEPT-REQUEST 4 'Grün'
5. Akzeptoren 3, 4 und 5 senden ACCEPT 4 'Grün'
6. Akzeptoren 3, 4 und 5 gehen offline
7. Akzeptoren 1 und 2 kommen online
8. Proposer sendet PREPARE 5
9. Akzeptoren 1 und 2 senden PROMISE 5
10. Proposer hat keine Mehrheit erhalten und fährt deswegen nicht weiter fort

(*Fault Tolerance*, Seite 22 ff.)

A start-up developing a mobile application needs to decide where to host the application's back-end service. Which of the following cloud deployment models is more suitable for that and why?

- Private cloud.
- Public cloud.

(Ein Start-up, das eine mobile Applikation entwickelt, muss entscheiden, wo der Backend-Service der Anwendung gehostet werden soll. Welches der folgenden Cloud-Bereitstellungsmodelle ist dafür besser geeignet und warum?

- *Private Cloud.*
- *Öffentliche Cloud.)*

Eine Öffentliche Cloud ist für das Start-up besser geeignet. Die wichtigsten Vorteile sind:

- Kosteneinsparungen
- Geringerer Wartungsaufwand
- Geringerer Aufwand bei der Einrichtung von Sicherheitsmaßnahmen

Einen guten Vergleich zwischen private und public Cloud gibt es hier: https://www.cloudflare.com/learning/cloud/what-is-a-public-cloud/

Despite the fact that the Domain Name System (DNS) has been originally deployed in the 1980s, when the number of objects in the Internet was way smaller than today, DNS still works very well. One reason for this is that DNS scales very well. Please explain how DNS achieves scalability.

(Obwohl das Domain Name System (DNS) bereits in den 1980er-Jahren entwickelt wurde, als die Anzahl an Objekten im Internet sehr viel kleiner war als heute, funktioniert DNS immer noch sehr gut. Ein Grund hierfür ist, dass DNS sehr gut skaliert. Erklären Sie, wie DNS Skalierbarkeit umsetzt.)

Für die gute Skalierbarkeit des DNS gibt es zwei Gründe:

- Hierarchische Struktur: Es können jederzeit neue Server auf den unteren Ebenen hinzugefügt werden um dem Netzwerk neue Knoten hinzuzufügen, z.B. wenn eine neue Firma ihre neue Website veröffentlichen will
- Die obersten Ebenen (Top Level Domains) ändern sich nur sehr selten, weswegen diese oft repliziert werden kann (viele über die ganze Welt verteilte Replikatsserver)

Explain why HTTP-based communication is usually transient and synchronous. What are the benefits of this communication approach?

(Erklären Sie, warum HTTP-basierte Kommunikation üblicherweise transient (flüchtig) und synchron ist. Was sind die Vorteile eines solchen Kommunikationsansatzes?)

Für den Aufruf einer Webseite müssen sowohl Client als auch Server online sein (Flüchtigkeit) und der Client blockiert, bis er eine Antwort vom Server erhält (Synchronität). Vorteil ist, dass flüchtige Server deutlich unkomplizierter sind als zustands-behaftete Server.

Consider a social network where data are replicated across two servers, L1 and L2. Each user accesses the social network via her/his closest replica server. User A updates her/his profile picture when operating on replica server L1. Then, the user moves to a new location, served by replica server L2, and updates the profile picture again. Describe the operations of the underlying client-centric consistency protocol when the user updates the profile picture at L2, so that the system provides **monotonic write consistency**. If for an operation of the protocol the user's write set is involved, also show the contents of the write set.

Make the following assumptions:

- There are only 2 replica servers (L1 and L2) in the system.
- The user's write set is initially empty.

*(Stellen Sie sich ein soziales Netzwerk vor, in dem Daten auf zwei Servern, L1 und L2, repliziert werden. Jede Benutzerin greift über ihren nächstgelegenen Replikatserver auf das soziale Netzwerk zu. Benutzerin A aktualisiert ihr Profilbild, wenn sie auf dem Replikatserver L1 arbeitet. Anschließend wechselt die Benutzerin an einen neuen Speicherort, der vom Replikatserver L2 bereitgestellt wird, und aktualisiert das Profilbild erneut. Beschreiben Sie die Operationen des zugrundeliegenden Client-zentrierten Konsistenzprotokolls, wenn die Benutzerin das Profilbild bei L2 aktualisiert, damit das System eine **monotone Schreibkonsistenz** bietet. Wenn für eine Operation des Protokolls der Schreibsatz ("write set") der Benutzerin betroffen ist, zeigen Sie auch den Inhalt des Schreibsatzes an.*

Machen Sie folgende Annahmen:

- *Es gibt nur 2 Replikatserver (L1 und L2) im System.*
- *Der Schreibsatz der Benutzerin ist anfangs leer.)*

- Profilbild auf L1 aktualisieren: *RS(write1), WS(write1)*
- Nutzerin will Profilbild auf L2 lesen:
  - L2 schaut im Read Set RS nach, welche Writes für den Read notwendig sind.
  - Falls write1 noch nicht auf L2 stattgefunden hat, holt sich L2 die notwendige Info von L1
  - Lese-Operation kann ausgeführt werden
- Nutzerin will Profilbild auf L2 schreiben:
  - L2 schaut im Write Set WR nach, welche Writes vorher stattgefunden haben
  - In diesem fall ist das nur write1, welches bereits lokal vorhanden ist
  - Schreib-Operation kann ausgeführt werden: *RS(write1, write2), WS(write1, write2)*

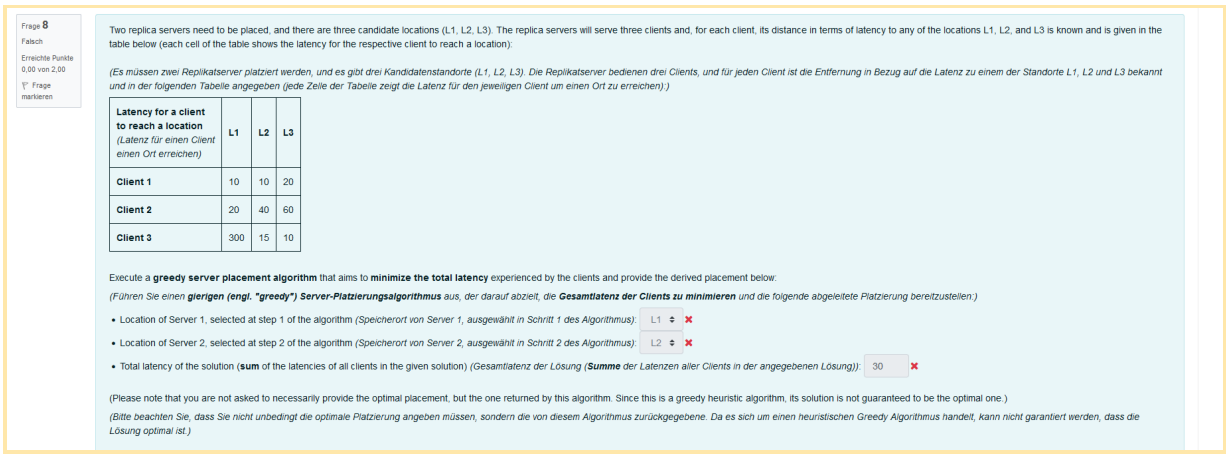
Dabei wird angenommen, dass das Aktualisieren des Profilbilds folgende Schritte beinhaltet:

- Altes Profilbild sehen
- Neues Profilbild schreiben
- Neues Profilbild sehen

You have to develop a weather app, running on a smartphone. The app does not only provide the smartphone user with weather forecasts, but is also gathering data from the smartphone sensors. This is done in order to be able to do “participatory sensing”, i.e., users contribute by providing data from their smartphone sensors like temperature, humidity, noise levels, etc. to a server. Based on this input, the server then generates individualized maps showing the noise level, current humidity, etc. Should the server be rather stateful or stateless? Explain your choice.

(Sie sollen eine Wetter-App für Smartphones entwickeln. Die App bietet dem Smartphone-Nutzer nicht nur einen Wetterbericht an, sondern sammelt auch Daten von den Smartphone-Sensoren. Dies wird gemacht, um „participatory sensing“ (dt. „partizipatorische Erfassung“) durchzuführen, d. h. Nutzer liefern Daten von den Smartphone-Sensoren, z. B. Temperatur, Luftfeuchtigkeit, Geräuschlevel etc. an einen Server. Der Server generiert basierend auf diesen Daten dann individualisierte Karten, welche die Geräuschbelastung, aktuelle Luftfeuchtigkeit etc. anzeigen. Würden Sie den Server eher zustandslos (engl. „stateless“) oder zustandsbehaftet (engl. „stateful“) designen? Erklären Sie Ihre Antwort.)

Zustands-behafteter Server, da dieser individualisierte Karten erstellen soll, wofür er Nutzer-Informationen benötigt.



Frage 8
Falsch
Erreichte Punkte 0,00 von 2,00
Frage markieren

Two replica servers need to be placed, and there are three candidate locations (L1, L2, L3). The replica servers will serve three clients and, for each client, its distance in terms of latency to any of the locations L1, L2, and L3 is known and is given in the table below (each cell of the table shows the latency for the respective client to reach a location):

(Es müssen zwei Replikatserver platziert werden, und es gibt drei Kandidatenstandorte (L1, L2, L3). Die Replikatserver bedienen drei Clients, und für jeden Client ist die Entfernung in Bezug auf die Latenz zu einem der Standorte L1, L2 und L3 bekannt und in der folgenden Tabelle angegeben (jede Zelle der Tabelle zeigt die Latenz für den jeweiligen Client um einen Ort zu erreichen):)

Latency for a client to reach a location *(Latenz für einen Client einen Ort erreichen)*	**L1**	**L2**	**L3**
Client 1	10	10	20
Client 2	20	40	60
Client 3	300	15	10

Execute a **greedy server placement algorithm** that aims to **minimize the total latency** experienced by the clients and provide the derived placement below:

*(Führen Sie einen **gierigen (engl. "greedy") Server-Platzierungsalgorithmus** aus, der darauf abzielt, die **Gesamtlatenz der Clients zu minimieren** und die folgende abgeleitete Platzierung bereitzustellen:)*

- Location of Server 1, selected at step 1 of the algorithm *(Speicherort von Server 1, ausgewählt in Schritt 1 des Algorithmus)*: L1
- Location of Server 2, selected at step 2 of the algorithm *(Speicherort von Server 2, ausgewählt in Schritt 2 des Algorithmus)*: L2
- Total latency of the solution (**sum** of the latencies of all clients in the given solution) *(Gesamtlatenz der Lösung (**Summe** der Latenzen aller Clients in der angegebenen Lösung))*: 30

(Please note that you are not asked to necessarily provide the optimal placement, but the one returned by this algorithm. Since this is a greedy heuristic algorithm, its solution is not guaranteed to be the optimal one.)

(Bitte beachten Sie, dass Sie nicht unbedingt die optimale Platzierung angeben müssen, sondern die von diesem Algorithmus zurückgegebene. Da es sich um einen heuristischen Greedy Algorithmus handelt, kann nicht garantiert werden, dass die Lösung optimal ist.)

- Server 1 auf L2
- Server 2 auf L1
- Gesamtlatenz: 45

In the lecture, we have discussed an algorithm for election in a ring. In this algorithm, the process with the highest priority/ID becomes the new leader. Why is this approach chosen? Isn't it also possible that a process declares itself the new leader and forwards this information along the ring to all other process? Or if we follow the algorithm presented, wouldn't it be possible to choose the first or last process in the list which is forwarded and augmented by the processes in the ring?

(In der Vorlesung wurde ein Algorithmus zur Wahl in einem Ring vorgestellt. Dieser Algorithmus wählt den Prozess mit der höchsten ID/Priorität zum neuen Anführer. Warum wird dieser Ansatz verfolgt? Wäre es nicht auch möglich, dass sich ein Prozess selbst zum neuen Anführer ernennt und diese Information über den Ring an alle anderen Prozesse verteilt? Oder – wenn wir dem ursprünglichen Algorithmus folgen – wäre es nicht auch möglich, dass der in der Liste (welche von den Prozessen im Ring weitergeleitet und erweitert wird) erst- oder letztgenannte Prozess gewählt wird?)

A network file system allows performing read and write operations on remote file objects. The operating system provides system calls such as read() and write() to applications, and a middleware takes care of detecting if these refer to local or to remote objects. In the first case, the middleware executes a local read or write operation and returns the result to the calling application. In the second case, it passes the operation on to a special client, which in turn invokes a remote procedure call on the file server, and returns the result of the operation to the middleware. Finally, the middleware returns the result of the read or write system call to the calling application. Explain if this system guarantees **performance transparency** or not.

*(Ein Netzwerkdateisystem ermöglicht das Ausführen von Lese- und Schreibvorgängen für entfernte Dateiobjekte. Das Betriebssystem stellt Systemaufrufe wie read() und write() für Applikationen bereit, und eine Middleware erkennt, ob sich diese auf lokale oder entfernte Objekte beziehen. Im ersten Fall führt die Middleware eine lokale Lese- oder Schreiboperation aus und gibt das Ergebnis an die aufrufende Applikation zurück. Im zweiten Fall wird die Operation an einen speziellen Client weitergeleitet, der wiederum einen Fernprozeduraufruf (engl. Remote Procedure Call - RPC) auf dem Dateiserver ausführt und das Ergebnis der Operation an die Middleware zurückgibt. Schließlich gibt die Middleware das Ergebnis des Lese- oder Schreibaufrufs an die aufrufende Applikation zurück. Erklären Sie, ob dieses System **Leistungstransparenz** garantiert.)*

System bietet i.A. keine Leistungstransparanze, da die Lese- und Schreibzugriffe auf entfernte Objekte deutlich länger dauern können als jene auf lokal vorhandene Objekte. Nutzer:innen können daher mitbekommen, ob das konkrete Objekt lokal oder remote vorhanden ist.

Der Ansatz aus der VO ist deshalb sinnvoll, weil es nur einen Prozess mit höchster ID gibt - die Wahl ist daher immer eindeutig, egal welcher Prozess die Wahl auslöst.
Wenn sich ein Prozess selbst zum Anführer ernennen könnte, könnten das mehrere Prozesse zeitgleich tun und es gäbe kein eindeutiges Ergebnis. Ebenso wenn der erst- oder letztgenannte Prozess gewinnt, könnten mehrere parallel laufende Abstimmungen zu unterschiedlichen Ergebnissen führen.
Beim ursprünglichen Algorithmus ist es kein Problem, wenn mehrere Abstimmungen gleichzeitig laufen, da alle immer das gleiche Ergebnis liefern (außer zwischenzeitlich fällt ein Server aus - aber dann wäre sowieso eine neue Abstimmung notwendig).