Distributed Systems & Blockchain (DS1) Prüfung

Nachname: _____ Vorname: _____ HSR PID:_____

Nr.	Aufgabe	Max. Punkte	Erreichte Punkte
0	Challenge Task	15	
1	Distributed Systems Basics	15	
2	Distributed Systems Security and Protocols	15	
3	Virtualization and Authentication	9	
4	Praktische Aufgaben	8	
5	Bitcoin / Ethereum	14	

Total 75

Hinweise allgemein:

- Zeit: 60 min.
- Zuerst diese Hinweise, dann die Prüfungsteile ganz durchlesen.
- Diese Prüfung ist **"Closed Book".**
- Taschenrechner ist nicht erlaubt.
- Sonst sind keine Hilfsmittel zugelassen; auch kein Handy oder Smart Watch.
- Alle Antworten und Lösungen in diese Aufgabenblätter schreiben.
- Keinen Bleistift und keine rote Farbe verwenden.
- Die Antworten und Lösungen müssen nachvollziehbar sein. Bitte alles in leserlicher Schrift!
- Keine Fragen während der Prüfung. Bei Unklarheiten sind sinnvolle Annahmen zu treffen und diese klar zu dokumentieren.
- Die Bewertungspunkte der Aufgaben können nach der Korrektur noch etwas variieren.

Hinweise zum Prüfungsbeginn:

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

Hinweise zur Prüfungsabgabe:

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

Aufgabe 1: Distributed Systems Basics (14 Punkte)

a) (6P) Kreuzen Sie Zutreffendes an.

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

	Statement	True	False
1	Bitflips können auch bei DNS Anfragen auftreten, und aus *amazon.com* kann *aeazon.com* werden (m: 0b01101101, e: 0b01100101)		
2	Im Weltraum treten Bitflips häufiger auf als hier auf der Erde.		
3	Die beste Klassifikation für verteilte Systeme basiert auf dem CAP-Theorem.		
4	Jede Applikation lässt sich ohne Modifikationen horizontal skalieren.		
5	Eine Reduktion der Latenz kann durch CDNs erreicht werden.		
6	Bei Server RAM kann man nicht überprüfen ob Bitflips stattgefunden haben.		

b) (2P) Nennen Sie je eine unterschiedliche Eigenschaft von *“Controlled” Distributed Systems* und *“Fully” Decentralized Systems*.

1 Eigenschaft eines “Controlled” Distributed Systems:

1 Eigenschaft eines “Fully” Decentralized Systems (nicht das Gegenteil der ersten Antwort):

c) (6P) Nennen Sie 4 Transparenzprinzipien in verteilten Systemen, und beschreiben Sie in einem Satz was es ist.

Transparenzprinzip 1:

Transparenzprinzip 2:

Transparenzprinzip 3:

Transparenzprinzip 4:

Aufgabe 2: Distributed Systems Security and Protocols (15 Punkte)

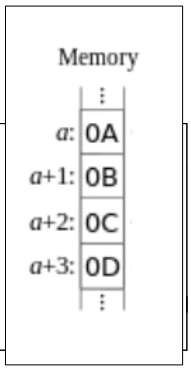
a) (4P) Kreuzen Sie Zutreffendes an.

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

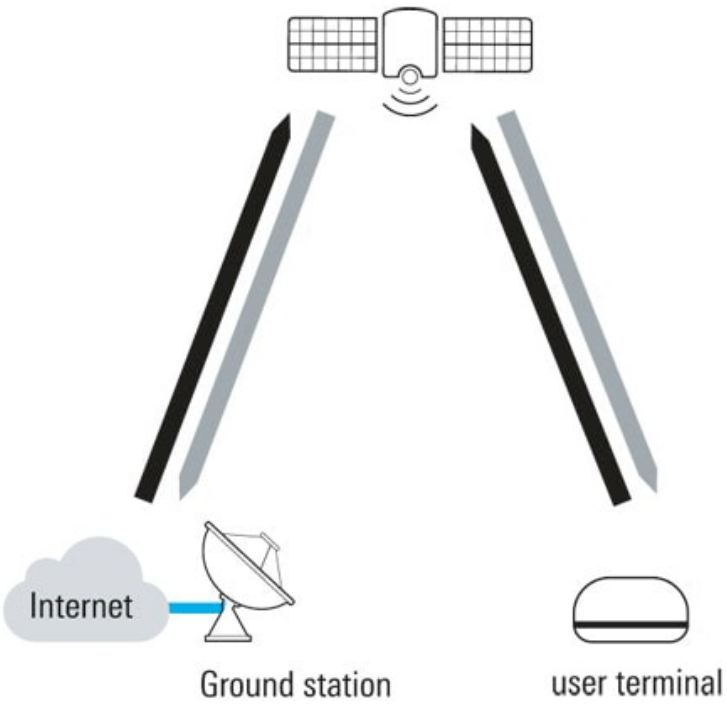
	Statement	True	False
1	HTTP/2 verwendet TCP, während HTTP/3 auf SCTP aufbaut.		
2	Ein L4 Load Balancer kann HTTP/3 Traffic auf Paketbasis mit Round-robin auf verschiedene Nodes aufteilen, da HTTP/3 auf UDP basiert.		
3	Ein Protokoll mit JSON ist optimiert um möglichst wenig Daten zu übertragen.		
4	Ein DDoS Amplification Angriff ist mit TCP nicht möglich.		

b) (2P) Aus einem Speicher (Abbildung rechts) wird ein 32-bit Integer mit Big-endian gelesen. Der ausgelesene 32-bit Integer hat den Wert: `0x0a0b0c0d`. Was wäre der Wert des Integers, wenn es mit Little-endian gelesen wird?

32-bit Integer in Little-endian:



c) (4P) Ein Satellitennetzwerk (z.B. Starlink von SpaceX) hat eine RTT von 30ms vom Endbenutzer (User Terminal) bis zur Bodenstation (Ground Station) (siehe Abbildung unten). Identifizieren Sie je einen Use-cases wo diese zusätzliche RTT akzeptabel ist, und einen Use-case wo diese zusätzliche RTT inakzeptabel ist. Begründen sie jeweils in einem Satz warum diese Use-cases akzeptabel/inakzeptabel sind.



Akzeptabler Use-case mit zusätzlicher RTT von 30ms: Begründung: Inakzeptabler Use-case mit zusätzlicher RTT von 30ms: Begründung:

d) (2P) Ein Endbenutzer in Europa mit Starlink greift auf eine Webseite in den USA zu. Nehmen Sie an, die RTT von Europa (Bodenstation) in die USA ist 100ms. Berechnen Sie das «time to first byte» für diese Webseite. Nehmen Sie an, dass sie HTTP/2 mit TLS1.2 mit 3 RTTs verwenden.

Time to first byte HTTP/2 mit Starlink:

e) (1P) Bei welchen Webseiten hat diese Art von Verbindung über ein Satellitennetzwerk relativ den grössten Einfluss bezüglich RTT. Antworten Sie in max. 1 Satz.

Grösster Einfluss:

f) (2P) Inwieweit profitiert diese Art von Verbindung über ein Satellitennetzwerk von HTTP/3. Antworten Sie in max. 1 Satz.

Vorteil HTTP/3:

Aufgabe 3: Virtualization and Authentication (9 Punkte)

a) (5P) Kreuzen Sie Zutreffendes an.

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

	Statement	True	False
1	Containers und VMs können nicht gleichzeitige betrieben werden.		
2	In einer VM wird in der Regel noch ein Betriebssystem installiert.		
3	Eine Applikation kann mit einem Unikernel ohne ein gängiges Betriebssystem in der VM laufen.		
4	VMs bieten eine bessere Isolation als Container		
5	Jedes Betriebssystem verfügt über die exakt gleichen Isolationsmechanismen, sodass *docker* problemlos auf andere Betriebssysteme portiert werden kann.		

b) (4p) In verteilten Systemen verwendet man in der Regel ein kurzlebiges Access Token und ein langlebiges Refresh Token. Beschreiben Sie je einen Nachteil wenn man nur ein langlebiges Access Token verwendet und einen Nachteil wenn man nur ein Refresh Token verwendet (max. 1 Satz pro Nachteil).

Nachteil langlebiges Access Token:

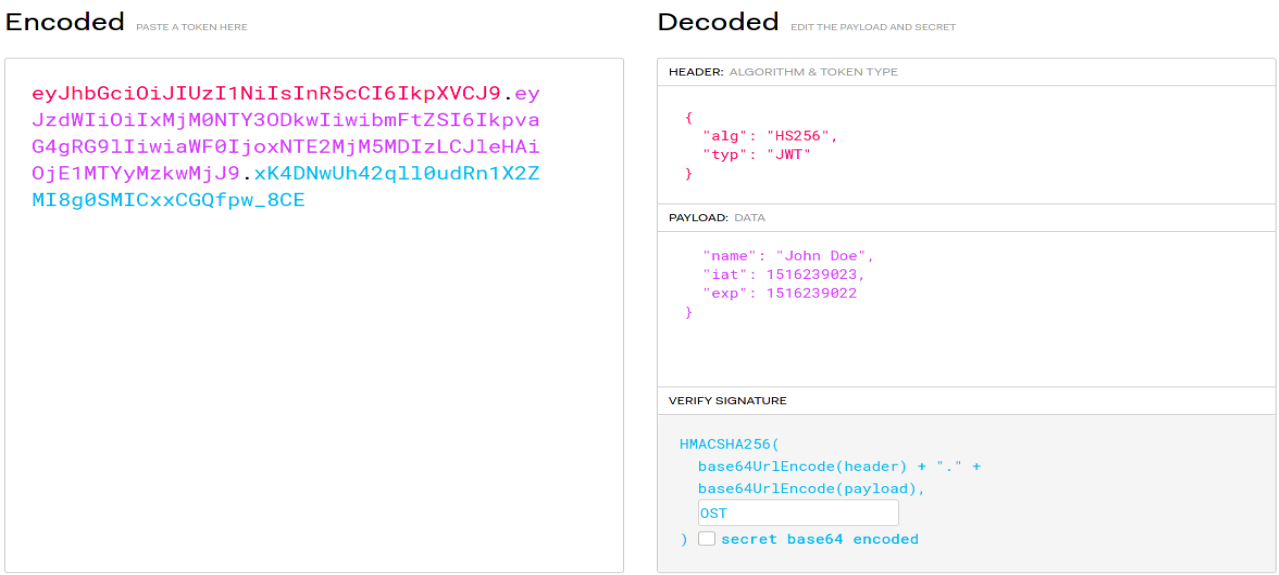
Nachteil Refresh Token (ohne Access Token):

Aufgabe 4: Praktische Aufgaben (8 Punkte)

Sie entwickeln eine verteilte Applikation mit einem Application Server, einer Datenbank, und einem Frontend, welche als separate Dienste laufen.

a) (3P) Unter welchen Voraussetzungen brauchen Sie im HTTP Header eine CORS (Cross-Origin Resource Sharing) Anweisungen? Beantworten Sie die Frage in max. 2 Sätzen.

b) (2P) Sie verwenden für ihr verteiltes System ein JWT Token (wie im Beispiel unten), um auf die Dienste des Application Servers zuzugreifen.



Als Payload geben Sie den Namen (name), das Issue Datum (iat) und das Expiry Datum (exp) mit. Können Sie in max. 1 Satz erklären warum in ihrem System dieses Token ungültig ist?

c) (3P) Für Ihre verteilte Applikation mit den entsprechenden Diensten haben Sie die Wahl zwischen einer VM und einem klassischen Server (Bare Metal). Nennen Sie je 2 Eigenschaften pro VM und klassischem Server. Was werden Sie für Ihre Applikation verwenden (VM oder klassischer Server) und warum?

Eigenschaft VM 1:

Eigenschaft VM 2:

Eigenschaft klassischer Server 1:

Eigenschaft klassischer Server 2:

Ihre Wahl (Begründung in max. 2 Sätzen):

Aufgabe 5: Bitcoin / Ethereum (14 Punkte)

a) (10P) Kreuzen Sie Zutreffendes an.

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

	Statement	True	False
1	Je mehr Miner Blöcke in Ethereum minen, desto höher wird die Belohnung wenn ein Block erfolgreich erstellt wurde.		
2	Wenn die Transaktionsanzahl steigt, braucht es auch mehr mehr Miner, die Blöcke minen.		
3	Jeder kann in einer Bitcoin Transaktion die Beträge nachvollziehen, die in unspent Outputs referenziert werden.		
4	Die Transaktionsgebühren in Bitcoin sind abhängig von der Länge der Transaktion.		
5	Ein Bitcoin Full Node kennt alle Transaktionen (seitdem der erste Bitcoin gemined wurde).		
6	Mit einer 51% Attacke können Transaktionen ausgeschlossen werden.		
7	Proof-of-stake braucht insgesamt weniger Strom als Proof-of-work.		
8	Mit Proof-of-stake können keine 51% Attacken gemacht werden.		
9	Beim Account-basierten Modell muss nicht jedes mal der ganze Betrag ausgegeben werden wie beim UTXO Modell.		
10	Ethereum unterstützt im Gegensatz zu Bitcoin Smart Contracts, welche auch Schleifen (Loops) beinhalten können.		

a) (4P) Im Moment kostet eine Ethereum Transaktion, welche 21000 Gas braucht und 20 Gwei pro Gas kostet, ca. 1.50 CHF. Nennen Sie zwei Gründe warum man länger warten muss, bis eine Transaktion im Block aufgenommen wird, wenn man weniger als 1.50 CHF bezahlt? Antworten Sie pro Grund in max. 2 Sätzen.

Grund 1:

Grund 2: