

Distributed Systems (Dsy) Prüfung

Nachname: _____ **Vorname:** _____

Nr.	Aufgabe	Max. Punkte	Erreichte Punkte
1	Distributed Systems Basics	12	
2	Tor, Protocols	12	
3	Virtualization und WebSockets	10	
4	Consensus, CRDTs, und CORS	12	
5	Bitcoin / Ethereum	14	

Total 60

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 (12 Punkte)

a) (6P) Kreuzen Sie Zutreffendes an.

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

	Statement	True	False
1	Bei TCP Netzwerktraffic führen Bitflips dazu, dass die Daten idealerweise nochmals übertragen werden.		
2	In Consumer-Hardware werden keine Error-correcting RAM Module verwendet, da keine Bitflips auftreten.		
3	Durch horizontales skalieren reduziert man die Komplexität.		
4	Applikationen lassen sich ohne Architektur-Modifikationen vertikal skalieren.		
5	Alle verteilten Systeme können eindeutig in AP oder CP beim CAP Theorem klassifiziert werden.		
6	Blockchains können ein Beispiel von vollständig verteilten Systemen sein.		

b) (3P) Nennen Sie drei Denkfehler (Fallacies) von verteilten Systemen, und beschreiben Sie in einem Satz was es ist.

Denkfehler 1:

Denkfehler 2:

Denkfehler 3:

c) (3P) Nennen Sie 3 Transparenzprinzipien in verteilten Systemen, und beschreiben Sie in einem Satz was es ist.

Transparenzprinzip 1:

Transparenzprinzip 2:

Transparenzprinzip 3:

Aufgabe 2: Tor, Protocols (12 Punkte)

a) (5P) Kreuzen Sie Zutreffendes an.

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

	Statement	True	False
1	Da Tor den Traffic bereits verschlüsselt sollte man SSL/TLS nicht verwenden wenn man auf eine Webseite ausserhalb von Tor zugreifen möchte.		
2	Tor sendet den Traffic über 3 Relays wenn man auf eine Webseite ausserhalb von Tor zugreifen möchte.		
3	Mit Onion (Hidden) Services lassen sich anonym Dienste oder Webseite betreiben.		
4	Es ist schwierig für einen Dienst ausserhalb von Tor herauszufinden ob Traffic von einem Tor Netzwerk kommt.		
5	Da Tor die round trip time (RTT) erhöht, werden Bridges verwendet um die Performance zu erhöhen.		

b) (2P) Was ist der Nachteil bei einem 3-way Handshake bei TCP gegenüber z.B. UDP?

Nachteil:

c) (3P) Sie entwickeln ein eigenes Protokoll, welches auf UDP basiert. Das Request / Reply Protokoll ist Text-basiert, und bei folgendem Request: «now» wird das Datum (z.B. «12. Juli 2022, 18:27:23») zurückgegeben. Für welchen Angriff kann dieses Protokoll missbraucht werden? Beschreiben Sie den Ablauf dieses Angriffs.

Angriff:

d) (2P) Warum hat dieser Angriff im nächsten Monat einen grössere Auswirkung?

Begründung:

Aufgabe 3: Virtualization und WebSockets (10 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 gleichzeitig betrieben werden.		
2	In einem Container braucht es ein vollständiges Betriebssystem.		
3	Jedes Betriebssystem hat unterschiedliche Isolationsmechanismen, sodass z.B. <i>docker</i> nicht problemlos auf andere Betriebssysteme portiert werden kann.		
4	VMs müssen in der Regel gewartet (Sicherheitsupdates) werden.		
5	Containers bieten eine bessere Isolation als VMs.		

b) (3P) Was ist der Unterschied zwischen REST/JSON und WebSockets?

Unterschied:

c) (2P) Für welchen Use-case eignen sich WebSockets?

Use-case:

Aufgabe 4: Consensus, CRDTs, und CORS (12 Punkte)

a) (5P) Kreuzen Sie Zutreffendes an.

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

	Statement	True	False
1	Mit Conflict-free Replicated Data Types (CRDT) können replizierte Daten ohne Konflikte zusammengeführt (merged) werden.		
2	Einfache Algorithmen wie z.B. ein ständig wachsender Zähler lassen sich mit CRDTs realisieren.		
3	CRDT-basierte Algorithmen können bei einem verteilten Versionskontrollsystem wie z.B. <i>git</i> eingesetzt werden um alle Merge Konflikte zu verhindern.		
4	Raft ist ebenfalls ein Konsensus Algorithmus und kann als Alternative zu Paxos verwendet werden.		
5	Der Heartbeat bei Raft ist wichtig, um feststellen zu können, ob alle Follower noch existieren.		

b) (3P) Sie entwickeln eine Finanzapplikation, welche Daten verteilt abspeichert. Sie müssen sich entscheiden ob Sie für die Datenspeicherung eine Distributed Hashtable (DHT) verwenden wollen oder nicht. Begründen Sie ihren Entscheid für oder gegen eine DHT in max. 3 Sätzen.

c) (4P) Bei ihrer verteilten Finanzapplikation stossen Sie auf das folgende Problem. Mit welcher Architekturänderung können Sie dieses Problem lösen und warum?

```
✖ Access to XMLHttpRequest at 'http://localhost:5000/global config' step1:1
  from origin 'http://localhost:8080' has been blocked by CORS policy:
  Response to preflight request doesn't pass access control check: No 'Access-
  Control-Allow-Origin' header is present on the requested resource.
```

Lösung:

Begründung:

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	Der Erfinder von Bitcoin ist Satoshi Nakamoto, welcher regelmässig auf Konferenzen auftritt.		
2	Mit der Bitcoin Scripting Language lassen sich Smart Contracts entwickeln welche auch Schleifen beinhalten können.		
3	Beim Account-basierten Modell muss auch jedes mal der ganze Betrag ausgegeben werden wie beim UTXO Modell.		
4	Bei Bitcoin sind die Transaktionsgebühren für alle Transaktionen gleich hoch.		
5	Proof-of-stake braucht insgesamt weniger Strom als Proof-of-work.		
6	Die «Ice age» bei Ethereum dient dazu um nach einem Protokollupgrade mittels Hardfork das alte Protokoll read-only zu machen.		
7	Durch den Ethereum Preissturz können die GPU Preise sinken, da sich das Minen mit GPUs weniger lohnt.		
8	Bei Bitcoin werden exakt alle 10 Minuten, bei Ethereum alle 14 Sekunden Blöcke erstellt.		
9	Ein Stablecoin ist eine Kryptowährung, welche an eine Fiatwährung wie z.B. Euro oder den US-Dollar gebunden sind.		
10	Da alle Nodes in Bitcoin und Ethereum deterministisch die Smart Contracts respektive die Scripting Language ausführen, sind Zufallszahlen schwierig zu bestimmen.		

b) (4P) Ein Onlineshop für Kleider akzeptiert Zahlungen in Bitcoins. Beschreiben Sie wie ein 51% Angriff in 4 Schritten ablaufen könnte.

51% Angriff, 1 Schritt:

51% Angriff, 2 Schritt:

51% Angriff, 3 Schritt:

51% Angriff, 4 Schritt: