Semesterprüfung FS24
Studienstandort Rapperswil / St.Gallen

NAME: _____ **VORNAME:**_____

MATRIKEL-Nr.: _____

STUDIENGANG: _____

Modulcode:	**M_DSY**
Modulbezeichnung:	**DISTRIBUTED SYSTEMS**
Modulowner:	**INFORMATIK**
Modulverantwortung:	Thomas Bocek
Prüfungsverantwortliche/r:	Thomas Bocek
Datum/Zeit:	**Donnerstag, 11.07.2024,** 13:50 – 14:50 Uhr

erreichte / max. Punktzahl: _____/50 **Prüfungsnote:** _____

Korrektur: Thomas Bocek / _____ ___
(Name/Unterschrift)

Distributed Systems (DSy) Prüfung

Nr.	Aufgabe	Max. Punkte	Erreichte Punkte
1	Distributed Systems Basics	11	
2	Email / Authentication	10	
3	Protocols	5	
4	Containers and VMs	5	
5	Load Balancing	12	
6	Bitcoin / Ethereum	7	

Total 50

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.
- Die Antworten können auf Deutsch oder Englisch sein.
- 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 – 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 (11 Punkte)

a) (5P) Kreuzen Sie Zutreffendes an.

Bitte beachten Sie, dass pro Teilaufgabe 1-5 die Fragen (a-d) richtig beantwortet werden müssen. Ist eine Antwort bei (a-d) falsch, gibt es für die jeweilige Teilaufgabe 0 Punkte.

		Frage	True	False
1		Was besagt Moore's Law (Moores Gesetz)?		
	a	Die Anzahl der Transistoren auf einem Mikrochip verdoppelt sich alle 18 Jahre.		
	b	Die Anzahl der Transistoren auf einem Mikrochip verdoppelt sich etwa alle zwei Jahre.		
	c	Die Kosten für die Herstellung von Transistoren verdoppeln sich alle 24 Monate.		
	d	Die Leistung von Computerprozessoren verdoppelt sich alle 18 Monate.		
2		Welche der folgenden Aussagen beschreiben korrekt das vertikale und horizontale Skalieren?		
	a	Vertikales Skalieren bedeutet, die Kapazität eines bestehenden Servers durch Hinzufügen von Ressourcen wie CPU, RAM oder Speicher zu erhöhen.		
	b	Horizontales Skalieren bedeutet, zusätzliche Server oder Maschinen hinzuzufügen, um die Last zu verteilen.		
	c	Ein Wechsel vom vertikalen Skalieren zum horizontalen Skalieren erfordert häufig Änderungen in der Anwendungsarchitektur.		
	d	Vertikales Skalieren ist immer kostengünstiger und effizienter als horizontales Skalieren.		
3		Warum gilt das Gesetz von Kryder, das besagt, dass sich die Datendichte auf Festplatten etwa alle 13 Monate verdoppelt, heute nicht mehr?		
	a	Die Entwicklung von SSDs (Solid State Drives) hat das Wachstum der Datendichte auf traditionellen Festplatten überflüssig gemacht.		
	b	SSDs bieten schnelleren Datenzugriff und sind für Endkunden oft wichtiger als eine höhere Speicherkapazität, was den Fokus von der Erhöhung der Datendichte auf Festplatten weg verlagert hat.		
	c	Das Nutzerverhalten hat sich geändert, sodass die meisten Daten jetzt in der Cloud statt auf physischen Festplatten gespeichert werden.		
	d	Die physikalischen Grenzen der Festplattentechnologie wurden durch neue magnetische Speichertechnologien überwunden.		
4		Warum sind verteilte Systeme wichtig, insbesondere in Bezug auf Latenz?		
	a	Verteilte Systeme sind wichtig, weil die physikalischen Grenzen der Datenübertragung die Latenz auf demselben Kommunikationsweg nicht weiter verringern lassen.		
	b	Verteilte Systeme sind wichtig, weil sie die Latenz durch kürzere Kommunikationswege verringern können.		
	c	Verteilte Systeme sind wichtig, weil sie die Latenz durch die gleichzeitige Nutzung von mehreren Netzwerken eliminieren.		
	d	Verteilte Systeme sind wichtig, weil die Latenz bei zentralisierten Systemen aufgrund der zunehmenden Netzwerksicherheit steigt.		
5		Was ist das Hauptziel einer fehlerkorrigierenden Codierung, wie z.B. Hamming-Codes?		
	a	Das Hauptziel ist es, die Datenübertragungsgeschwindigkeit zu erhöhen.		
	b	Das Hauptziel ist es, Fehler bei der Datenübertragung zu erkennen und zu korrigieren.		
	c	Das Hauptziel ist es, die Datenkompression zu maximieren.		
	d	Das Hauptziel ist es, die Datensicherheit durch Verschlüsselung zu gewährleisten.		

b) (2P) Das Transparenzprinzip «Security Transparency» in Kontext der verteilten Systeme, hat sowohl Vor- als auch Nachteile. Nennen Sie einen Vorteil und einen Nachteil dieses Prinzips.

Vorteil:

Nachteil:

c) (4P) Im Kontext verteilter Systeme sind Datenreplikas wichtig. Nennen Sie je 2 Vorteile und 2 Nachteile, welche sich durch die Nutzung von Replikas ergeben.

Vorteil 1:

Vorteil 2:

Nachteil 1:

Nachteil 2:

Aufgabe 2: Email / Authentication (10 Punkte)

a) (5P) Kreuzen Sie Zutreffendes an.

Bitte beachten Sie, dass pro Teilaufgabe 1-5 die Fragen (a-d) richtig beantwortet werden müssen. Ist eine Antwort bei (a-d) falsch, gibt es für die jeweilige Teilaufgabe 0 Punkte.

		Frage	True	False
1		Welche der folgenden Aussagen zu DKIM sind richtig oder falsch?		
	a	DKIM verwendet digitale Signaturen, um die Integrität und Authentizität von E-Mails zu gewährleisten.		
	b	DKIM prüft die IP-Adresse des sendenden Servers, um sicherzustellen, dass sie mit den von der Domain autorisierten Servern übereinstimmt.		
	c	DKIM erfordert, dass ein Domaininhaber DNS-Einträge erstellt, um öffentliche Schlüssel zu veröffentlichen.		
	d	DKIM kann sicherstellen, dass eine E-Mail vollständig vor Spam geschützt ist.		
2		Welche der folgenden Aussagen zu SPF und DMARC sind richtig oder falsch?		
	a	SPF ermöglicht es dem Domaininhaber, eine Liste von IP-Adressen zu veröffentlichen, die berechtigt sind, E-Mails im Namen der Domain zu versenden.		
	b	DMARC baut auf SPF und DKIM auf und bietet eine Richtlinie, die festlegt, wie E-Mails behandelt werden sollen, wenn sie die Authentifizierungsprüfungen nicht bestehen.		
	c	SPF überprüft die digitale Signatur der E-Mail, um die Authentizität des Absenders zu bestätigen.		
	d	SPF, DKIM und DMARC können sicherstellen, dass eine E-Mail vollständig vor Spam geschützt ist.		
3		Welche der folgenden Aussagen sind richtig oder falsch im Kontext von Autorisierung und Zugriffskontrolle?		
	a	Autorisierung bestimmt, welche Ressourcen ein authentifizierter Benutzer zugreifen darf.		
	b	Nicht-Abstreitbarkeit stellt sicher, dass weder der Absender noch der Empfänger leugnen können, dass eine Kommunikation stattgefunden hat.		
	c	Vertraulichkeit schützt übertragene Daten vor Abhörern.		
	d	Authentifizierung überprüft eine behauptete Identität, zum Beispiel durch ein Passwort.		
4		Welche der folgenden Aussagen sind richtig oder falsch im Kontext von Access Tokens?		
	a	Access Tokens werden verwendet, um den Zugriff auf geschützte Ressourcen zu gewähren.		
	b	Access Tokens haben eine lange Lebensdauer und werden selten ablaufen.		
	c	Access Tokens werden in der Regel im Authorization Header bei API-Anfragen gesendet.		
	d	Access Tokens enthalten in der Regel Informationen über die Benutzeridentität und Zugriffsrechte.		
5		Welche der folgenden Aussagen sind richtig oder falsch im Kontext von Refresh Tokens?		
	a	Refresh Tokens werden verwendet, um ein neues Access Token zu erhalten, wenn das aktuelle abläuft.		
	b	Refresh Tokens haben eine kürzere Lebensdauer als Access Tokens.		
	c	Refresh Tokens sollten sicher auf dem Client-Gerät gespeichert werden.		
	d	Refresh Tokens können verwendet werden, um direkt auf geschützte Ressourcen zuzugreifen.		

b) (4P) Bei TOTP (Time-based One-time Password), beantworten Sie wer welche Daten generiert oder übermittelt (Benutzer, Server). Über welchen Kommuikationsweg wird ein Secret übermittelt? Hinweis: TOTP(secret, time) wie folgt definiert ist: truncate(HMAC-SHA-256(secret, time)).

Ein Secret wird normalerweise generiert durch:

Ein Secret wird normalerweise übermittelt von:

Ein Secret wird normalerweise übermittelt an:

Ein Secret wird normalerweise über diesen Kommunikationsweg übertragen:

c) (1P) Sie verwenden den folgenden JWT-Token mit korrekter Signatur (nicht abgebildet), bekommen jedoch eine Fehlermeldung. Was stimmt mit diesem Token nicht?

Header

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

Payload

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1720709401,
  "exp": 1720709400
}
```

Fehler:

Aufgabe 3: Protocols (5 Punkte)

a) (5P) Kreuzen Sie Zutreffendes an.

Bitte beachten Sie, dass pro Teilaufgabe 1-5 die Fragen (a-d) richtig beantwortet werden müssen. Ist eine Antwort bei (a-d) falsch, gibt es für die jeweilige Teilaufgabe 0 Punkte.

		Frage	True	False
1	Welche der folgenden Aussagen sind richtig oder falsch im Kontext der Schichten in Netzwerkprotokollen?			
	a	Die physikalische Schicht ist für die Wegwahl und das Routing der Datenpakete über das Netzwerk verantwortlich.		
	b	Die Transportschicht stellt sicher, dass Datenpakete in der richtigen Reihenfolge und ohne Verluste ankommen.		
	c	Die Netzwerkschicht ist für die Wegwahl und das Routing der Datenpakete über das Netzwerk verantwortlich.		
	d	Die Sicherungsschicht verschlüsselt die Daten, um sie vor unbefugtem Zugriff zu schützen.		
2	Welche der folgenden Aussagen sind richtig oder falsch im Kontext von TCP (Transmission Control Protocol)?			
	a	TCP ist ein verbindungsloses Protokoll, das für schnelle und unzuverlässige Datenübertragung verwendet wird.		
	b	TCP stellt sicher, dass Daten in der richtigen Reihenfolge und ohne Verluste beim Empfänger ankommen.		
	c	TCP verwendet eine dreifache Handshake-Methode, um eine Verbindung zwischen Sender und Empfänger herzustellen.		
	d	TCP unterstützt keine Flusskontrolle, um die Überlastung des Netzwerks zu vermeiden.		
3	Welche der folgenden Aussagen sind richtig oder falsch im Kontext von UDP (User Datagram Protocol)?			
	a	UDP ist ein verbindungsloses Protokoll, das keine Garantie für die Zustellung von Datenpaketen bietet.		
	b	UDP verwendet eine dreifache Handshake-Methode, um eine Verbindung zwischen Sender und Empfänger herzustellen.		
	c	UDP ist geeignet für Anwendungen, die eine schnelle und effiziente Datenübertragung erfordern, wie z.B. Videostreaming und Online-Spiele.		
	d	UDP stellt sicher, dass Datenpakete in der richtigen Reihenfolge ankommen.		
4	Welche der folgenden Aussagen sind richtig oder falsch im Kontext von QUIC im Vergleich zu TCP+TLS?			
	a	QUIC kombiniert die Funktionen von TCP und TLS und läuft über UDP.		
	b	QUIC bietet schnellere Verbindungsaufbauzeiten im Vergleich zu TCP+TLS, da es die TLS-Handshakes optimiert.		
	c	QUIC ist ein verbindungsloses Protokoll, das im Gegensatz zu TCP+TLS keine Zuverlässigkeit bietet.		
	d	QUIC benötigt weniger Round Trips im Vergleich zu TCP+TLS für die Verbindungsherstellung.		
5	Welche der folgenden Aussagen sind richtig oder falsch im Kontext von Flow Control und Congestion Control in Netzwerken?			
	a	Flow Control stellt sicher, dass ein Sender die Übertragungsgeschwindigkeit an die Empfangsfähigkeit des Empfängers anpasst.		
	b	Congestion Control verhindert, dass zu viele Datenpakete gleichzeitig in ein Netzwerk gesendet werden und dadurch Überlastungen entstehen.		
	c	Flow Control und Congestion Control sind identische Mechanismen, die beide die Überlastung eines Netzwerks verhindern.		
	d	Congestion Control bezieht sich auf die Kontrolle des Datenflusses zwischen zwei direkt verbundenen Geräten.		

Aufgabe 4: Containers and VMs (5 Punkte)

a) (5P) Kreuzen Sie Zutreffendes an.

Bitte beachten Sie, dass pro Teilaufgabe 1-5 die Fragen (a-d) richtig beantwortet werden müssen. Ist eine Antwort bei (a-d) falsch, gibt es für die jeweilige Teilaufgabe 0 Punkte.

		Frage	True	False
1		Was ist der Hauptunterschied zwischen virtuellen Maschinen (VMs) und Containern?		
	a	VMs bieten eine vollständige Virtualisierung der Hardware, während Container nur die Betriebssystem-Ebene virtualisieren.		
	b	Container benötigen in der Regel mehr Ressourcen als VMs, da sie vollständige Betriebssysteme enthalten.		
	c	VMs sind in der Regel schneller zu starten als Container.		
	d	Container bieten vollständige Hardware-Isolation, während VMs dies nicht tun.		
2		Wie funktioniert Docker bei der Implementierung von Containern?		
	a	Docker verwendet einen Hypervisor, um Container zu erstellen und zu verwalten.		
	b	Docker nutzt OS-Level-Virtualisierung, um Container zu erstellen und voneinander zu isolieren.		
	c	Docker erfordert eine spezielle Hardware zur Ausführung von Containern.		
	d	Docker-Container kommunizieren über direkt zugängliche Hardware-Kanäle.		
3		Welche Best Practices sollten beim Einsatz von Docker beachtet werden?		
	a	Verwenden Sie grosse Basisimages wie Ubuntu oder Debian, um mehr Funktionalität zu gewährleisten.		
	b	Setzen Sie Dateisysteme und Volumes nach Möglichkeit auf schreibgeschützt.		
	c	Lassen Sie Container immer als Root-Benutzer laufen, um Zugriffsbeschränkungen zu vermeiden.		
	d	Überprüfen Sie Ihre Docker-Images regelmässig auf Sicherheitslücken.		
4		Was ist Docker Compose und wofür wird es verwendet?		
	a	Docker Compose ist ein Tool zur Erstellung von Docker-Images.		
	b	Docker Compose ermöglicht die Verwaltung und Orchestrierung mehrerer Container.		
	c	Docker Compose wird ausschliesslich zur Überwachung von Docker-Containern verwendet.		
	d	Docker Compose ist nur für den Einsatz in Produktionsumgebungen geeignet.		
5		Welche der folgenden Aussagen sind richtig oder falsch im Kontext des Unterschieds zwischen Kubernetes, Docker und Docker Compose?		
	a	Kubernetes ist ein Container-Orchestrierungstool, während Docker ein Tool zur Containerisierung von Anwendungen ist.		
	b	Docker kann nur in Verbindung mit Kubernetes verwendet werden.		
	c	Docker ist eine Plattform, die nur in der Cloud funktioniert, während Kubernetes sowohl in der Cloud als auch On-Premises verwendet werden kann.		
	d	Docker Compose ist ein Ersatz für Kubernetes und bietet die gleichen Funktionen zur Container-Orchestrierung.		

Aufgabe 5: Load Balancing (12 Punkte)

a) (5P) Kreuzen Sie Zutreffendes an.

Bitte beachten Sie, dass pro Teilaufgabe 1-5 die Fragen (a-d) richtig beantwortet werden müssen. Ist eine Antwort bei (a-d) falsch, gibt es für die jeweilige Teilaufgabe 0 Punkte.

		Frage	True	False
1		Welche der folgenden Aussagen beschreibt korrekt den Zweck von Load Balancing?		
	a	Load Balancing verteilt die Arbeitslast über mehrere Server, um die Verfügbarkeit und Zuverlässigkeit zu erhöhen.		
	b	Load Balancing ist ein Verfahren zur Datenbankreplikation, um Datenintegrität sicherzustellen.		
	c	Load Balancing reduziert den Speicherbedarf eines Servers durch Datenkomprimierung.		
	d	Load Balancing wird verwendet, um Daten sicher zwischen verschiedenen Netzwerken zu übertragen.		
2		Welche Load Balancing-Methode verteilt Anfragen basierend auf der Anzahl der aktiven Sitzungen?		
	a	Round Robin		
	b	Least Connections		
	c	Weighted Round Robin		
	d	Hash-basierte Verteilung		
3		Welche Aussage trifft auf Layer-7 (L7) Load Balancer zu?		
	a	L7 Load Balancer arbeiten auf der Netzwerkschicht und verteilen den Datenverkehr basierend auf IP-Adressen.		
	b	L7 Load Balancer terminieren TLS-Verbindungen und können den Datenverkehr basierend auf HTTP-Headern und -Inhalten verteilen.		
	c	L7 Load Balancer sind ressourcenintensiver als Layer-4 (L4) Load Balancer.		
	d	L7 Load Balancer verwenden DNS-Round-Robin zur Lastverteilung.		
4		Welche der folgenden Aussagen sind richtig oder falsch im Kontext von Load Balancing und JWT-basierter Authentifizierung?		
	a	Ein Layer-7 Load Balancer kann den eingehenden Datenverkehr basierend auf dem Inhalt von JWTs verteilen, um Benutzeranfragen an spezialisierte Server zu leiten.		
	b	JWTs müssen auf jedem Load Balancer validiert werden.		
	c	Load Balancer können JWTs verwenden, um die SSL/TLS-Entschlüsselung direkt auf dem Load Balancer durchzuführen und die Entlastung der Backend-Server zu gewährleisten.		
	d	JWTs bieten eine eingebaute Funktion zur Lastverteilung, indem sie Benutzeranfragen automatisch an verschiedene Server weiterleiten.		
5		Welches der folgenden Beispiele beschreibt eine typische Anwendung eines Layer-4 (L4) Load Balancers?		
	a	Verteilung des eingehenden Datenverkehrs basierend auf IP-Adressen und TCP/UDP-Ports.		
	b	Verteilung des Datenverkehrs basierend auf HTTP-Headern und -Inhalten.		
	c	Verwaltung und Verteilung von Datenbankabfragen.		
	d	Erstellung von virtuellen Maschinen zur Lastverteilung.		

b) (3P) Sie haben eine dockerisierte Webapplikation (Frontend und Backend) entwickelt und sehen bei Ihrer Applikation die folgende Fehlermeldung. Was läuft auf Port 8080 und was auf Port 5000? Wie können Sie dieses Problem beheben?

```
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.
```

Port 8080:

Port 5000:

Lösung des Problems:

c) (4P) Sie haben die Wahl, bei Ihrer dockerisierten Webapplikation die Frontend-Konfiguration entweder in einer Konfigurationsdatei zur Build-Zeit (z.B. .env) oder über einen Konfigurationsendpunkt (z.B. global_config) zur Laufzeit zu hinterlegen. Nennen Sie jeweils einen Nachteil.

Nachteil einer Konfigurationsdatei (z.B. .env):

Nachteil eines Konfigurationsendpunkts (z.B. global_config):

Aufgabe 6: Bitcoin / Ethereum (7 Punkte)

a) (5P) Kreuzen Sie Zutreffendes an.

Bitte beachten Sie, dass pro Teilaufgabe 1-5 die Fragen (a-d) richtig beantwortet werden müssen. Ist eine Antwort bei (a-d) falsch, gibt es für die jeweilige Teilaufgabe 0 Punkte.

		Frage	True	False
1		Welche der folgenden Aussagen sind richtig oder falsch im Kontext von Bitcoin?		
	a	Bitcoin ist vollständig peer-to-peer und erfordert keine zentrale Entität.		
	b	Die kleinste Einheit an Bitcoin wird als "Satoshi" bezeichnet.		
	c	Bitcoin-Transaktionen werden durch den Nachweis des Einsatzes (Proof of Stake) validiert.		
	d	Da das Bitcoin-Mining erhebliche Rechenleistung erfordert, wird dabei auch viel Strom verbraucht.		
2		Welche der folgenden Aussagen sind richtig oder falsch im Kontext von Ethereum?		
	a	Ethereum verwendet ein Konto-basiertes System im Gegensatz zum UTXO-Modell von Bitcoin.		
	b	Ethereum wurde im Jahr 2009, gleichzeitig mit Bitcoin, veröffentlicht.		
	c	Ethereum ermöglicht die Ausführung von Smart Contracts, die Turing-vollständig sind.		
	d	Ethereum verwendet derzeit den Proof-of-Stake-Mechanismus zur Validierung von Transaktionen und zur Sicherung des Netzwerks.		
3		Welche der folgenden Aussagen sind richtig oder falsch im Kontext von 51%-Angriffen?		
	a	Ein 51%-Angriff tritt auf, wenn ein Angreifer mehr als 50% der Netzwerk-Hashrate kontrolliert.		
	b	Ein erfolgreicher 51%-Angriff ermöglicht es dem Angreifer, doppelte Ausgaben (Double Spending) durchzuführen.		
	c	51%-Angriffe sind in Proof-of-Work-Systemen wie Bitcoin unmöglich.		
	d	Ethereum ist aufgrund seines Proof-of-Stake-Mechanismus gegen Double Spending Angriffe geschützt.		
4		Welche der folgenden Aussagen sind richtig oder falsch im Kontext von Transaktionsvalidierung in Bitcoin?		
	a	Bitcoin verwendet das UTXO-Modell (Unspent Transaction Output) zur Verfolgung von Guthaben.		
	b	Alle Bitcoin-Transaktionen werden privat zwischen den beteiligten Parteien gehalten und nicht im gesamten Netzwerk verbreitet.		
	c	Bitcoin-Transaktionen werden durch den Proof-of-Work-Mechanismus validiert, der eine partielle Hash-Kollision erfordert.		
	d	Jeder Bitcoin-Transaktionsausgang kann nur einmal ausgegeben werden.		
5		Welche der folgenden Aussagen sind richtig oder falsch im Kontext der Vorteile und Nachteile von Bitcoin und Ethereum?		
	a	Ethereum hat keine Skalierungsprobleme und kann unbegrenzt viele Transaktionen pro Sekunde verarbeiten.		
	b	Ethereum erlaubt komplexere Transaktionen und Smart Contracts im Vergleich zu Bitcoin.		
	c	Ein Nachteil von Bitcoin ist der hohe Energieverbrauch durch den Mining-Prozess.		
	d	Ein Vorteil von Bitcoin ist die einfache Berechnung der Transaktionsgebühr, die nur abhängig von der Transaktionsgrösse ist.		

b) (2P) Beschreiben Sie, wie ein 51%-Angriff auf eine Kryptowährungsbörse ablaufen könnte.

Ablauf: