Semesterprüfung HS24/25
Studienstandort Rapperswil

NAME: _____ **VORNAME:**_____

MATRIKEL-Nr.: _____

STUDIENGANG: _____

Modulcode:	**M_BLCH**
Modulbezeichnung:	**BLOCKCHAIN**
Modulowner:	**INFORMATIK**
Modulverantwortung:	Thomas Bocek
Prüfungsverantwortliche/r:	Thomas Bocek
Datum/Zeit:	**Montag, 27.01.2024,** 14:10 – 15:10 Uhr

erreichte / max. Punktzahl: _____/60 **Prüfungsnote:** _____

Korrektur: Thomas Bocek / _____ ____

(Name/Unterschrift)

Nr.	Aufgabe	Max. Punkte	Erreichte Punkte
1	Blockchain Basics	16	
2	Decentralized Finance (DeFi) Basics	18	
3	Stablecoins / Wallets	10	
4	Bloom Filter	6	
5	Solidity / Ethereum	10	

Total 60

Hinweise allgemein:

- Zeit: 60 min.
- Zuerst diese Hinweise, dann die Prüfungsteile ganz durchlesen.
- Diese Prüfung ist **"Closed Book".**
- Taschenrechner ist nicht erlaubt.
- Es 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 ab.
- Nach Prüfungsende: Drehen Sie Ihre Prüfung um und warten Sie, bis die Prüfung eingesammelt wird. Bleiben Sie dann sitzen bis die/eine Aufsichtsperson die Prüfungen gezählt hat und ein Zeichen zum Verlassen des Raums gegeben hat.

Aufgabe 1: Blockchain Basics (16 Punkte)

a) (10P) Kreuzen Sie True/False für die jeweilige Aussage an. Es können mehrere Aussagen richtig oder falsch sein. Pro Aufgabenblock (1-5): 2 Punkte für alles richtig, 1 Punkt für einen Fehler, 0 Punkte für mehr Fehler.

		Statement	True	False
1	Welche der folgenden Aussagen zu Proof of Attendance Protocol (POAP) sind richtig?			
	a)	Verifizierung von Blockchain-Transaktionen		
	b)	Nachweis der Teilnahme an Veranstaltungen		
	c)	Basiert auf einem non-fungible Token (NFT)		
	d)	Können als Nachweis für Engagement in bestimmten Communities dienen		
2	Welche der folgenden Aussagen beschreiben die Eigenschaften einer Layer 2 Lösung?			
	a)	Eine separate Blockchain, die ihre eigene Sicherheit gewährleistet		
	b)	Ein Protokoll, das Transaktionen ausserhalb der Hauptkette verarbeitet und die Sicherheit des Layers 1 nutzt		
	c)	Ein System zur Skalierung von Blockchain-Transaktionen		
	d)	Eine neue Version der Ethereum-Blockchain		
3	Welche Aussagen über MetaMask sind richtig?			
	a)	MetaMask hat einen integrierten Ethereum Node, um mit der Ethereum Blockchain zu kommunizieren		
	b)	MetaMask kann einen lokalen Ethereum Node nutzen, um mit der Ethereum Blockchain zu kommunizieren		
	c)	MetaMask injiziert eine JavaScript-Bibliothek in den Browser, die den Zugriff auf Smart Contracts ermöglicht		
	d)	MetaMask kann mit Ethereum Mainnet kommunizieren, nicht mit Testnets		
4	Welche Aussagen über DAO-Governance sind richtig?			
	a)	Entscheidungen werden ausschliesslich von den Gründern getroffen		
	b)	Alle Vorschläge müssen von einer zentralen Stelle genehmigt werden		
	c)	Token-Inhaber können über Vorschläge abstimmen und diese ausführen lassen		
	d)	Wenn der DAO Smart Contract entsprechend implementiert ist, können Änderungen am Smart Contract per Abstimmung durchgeführt werden		
5	Welche der folgenden Aussagen trifft auf das Bitcoin Netzwerk zu?			
	a)	Es ist ein zentralisiertes Zahlungssystem		
	b)	Transaktionen im Bitcoin Netzwerk sind privat und nur für Sender und Empfänger sichtbar		
	c)	Es wird von einer einzelnen Organisation kontrolliert		
	d)	Es benötigt Banken zur Transaktionsvalidierung		

b) (2P) In Ethereum sind Transaktionen unveränderlich (immutable). Dennoch gibt es Möglichkeiten Smart Contract Code zu aktualisieren. Beschreiben Sie einen Ansatz in max. 2 Sätzen.

Ansatz:

c) (2P) Wie unterscheidet sich der Test eines Smart Contracts in einer lokalen Remix VM von einem Test im Testnet? Beschreiben Sie zwei wichtige Unterschiede in je 1 Satz.

Unterschied 1:

Unterschied 2:

d) (2P) Welche Operationen sind in Ethereum Smart Contracts besonders gas-intensiv (teuer)? Nennen Sie eine teure Operation und erklären Sie kurz warum. Begrenzen Sie Ihre Antwort auf max. 1 Satz.

Teure Operation:

Warum:

Aufgabe 2: Decentralized Finance (DeFi) Basics (18 Punkte)

a) (10P) Kreuzen Sie True/False für die jeweilige Aussage an. Es können mehrere Aussagen richtig oder falsch sein. Pro Aufgabenblock (1-5): 2 Punkte für alles richtig, 1 Punkt für einen Fehler, 0 Punkte für mehr Fehler.

		Statement	True	False
1	Was sind Merkmale von State Channels?			
	a)	Sie benötigen für jede Transaktion eine On-Chain-Bestätigung		
	b)	Sie ermöglichen private Zahlungskanäle zwischen Parteien		
	c)	Sie sind nur für NFT-Transfers geeignet		
	d)	Sie erfordern keine On-Chain-Transaktionen für Zwischenzustände		
2	Welches der folgenden Merkmale trifft auf Liquidity Providing in DeFi zu?			
	a)	Liquidity Provider müssen immer einen festen Betrag einzahlen		
	b)	Provider erhalten Gebühren proportional zu ihrem Anteil am Pool		
	c)	Provider können nur eine einzelne Kryptowährung bereitstellen		
	d)	Die Rendite ist unabhängig von der Marktvolatilität		
3	Was passiert beim "Price Impact" in einer DEX?			
	a)	Der Preis ändert sich nur bei kleinen Trades		
	b)	Grosse Trades haben keinen Einfluss auf den Handelspreis		
	c)	Je grösser der Trade, desto stärker die Preisauswirkung		
	d)	Der Preis bleibt immer konstant		
4	Welche Rolle spielen Arbitrage-Bots in DeFi?			
	a)	Sie verlangsamen das Netzwerk unnötig		
	b)	Sie helfen, Preise zwischen verschiedenen DEXes auszugleichen		
	c)	Arbitrage-Bots koennen auch zwischen DEXes und CEXes Preise ausgleichen		
	d)	Sie werden nur von zentralen Börsen eingesetzt		
5	Welche der folgenden Merkmale trifft auf eine dezentrale Börse (DEX) zu?			
	a)	Handel ohne zentrale Vermittlungsstelle		
	b)	Verwahrung der Vermögenswerte durch die Börse		
	c)	Verwendung von Smart Contracts zur Abwicklung von Trades		
	d)	Unterstützung ausschliesslich für Fiat-Währungen		

b) (4P) Erklären Sie "Flash Loans" und "Overcollateralized Loans" in DeFi und nennen Sie jeweils einen typischen Anwendungsfall. Begrenzen Sie Ihre Antwort auf je 1 Satz.

Flash Loan:

Anwendungsfall Flash Loan:

Overcollateralized Loans:

Anwendungsfall Overcollateralized Loan:

c) (2P) Was versteht man unter "Impermanent Loss"? Begrenzen Sie Ihre Antwort auf 2 Sätze.

Impermanent Loss:

d) (2P) Wie findet die Preisfindung in einer Order-Book-basierten Börse und in einer Constant Function Market Maker (CFMM)-basierten DEX statt? Begrenzen Sie Ihre Antwort auf je 1 Satz.

Order-Book:

CFMM:

Aufgabe 3: Stablecoins / Wallets (10 Punkte)

a) (10P) Kreuzen Sie True/False für die jeweilige Aussage an. Es können mehrere Aussagen richtig oder falsch sein. Pro Aufgabenblock (1-5): 2 Punkte für alles richtig, 1 Punkt für einen Fehler, 0 Punkte für mehr Fehler.

		Statement	True	False
1	Was charakterisiert einen algorithmischen Stablecoin?			
	a)	Er wird durch Fiat-Währungen besichert		
	b)	Die Stabilität wird durch Smart Contract Audits gewährleistet		
	c)	Die Preisstabilität wird durch externe Orakel garantiert		
	d)	Das System erstellt oder vernichtet die Gegenwährung um den Preis stabil zu halten		
2	Was passierte beim Kollaps von Terra/UST?			
	a)	Die Besicherung durch USDC ging verloren		
	b)	Es kam zu einer Liquiditätskrise, die das algorithmische System destabilisierte		
	c)	Die Fiat-Reserven waren nicht ausreichend		
	d)	Die Smart Contracts wurden gehackt		
3	Welche Aussagen zu einer HD-Wallet sind richtig?			
	a)	Eine HD-Wallet kann nur Bitcoins verwalten		
	b)	Eine HD-Wallet generiert alle Keys aus einem Master Seed		
	c)	Eine HD-Wallet benötigt für jede generierte Adresse einen eigenen Seed		
	d)	Eine HD-Wallet funktioniert nur mit Hardware Wallets		
4	Welche Aussagen zu Seed-Phrase (BIP-39) sind richtig?			
	a)	Der Seed-Phrase kann als Backup dienen		
	b)	BIP steht für Bitcoin Improvement Proposals und deshalb funktionieren Seed-Phrases nur im Bitcoin System		
	c)	Der Seed-Phrase wird zur Generierung des Master Keys verwendet		
	d)	Der Seed-Phrase besteht immer aus 12 Wörtern		
5	Welche Aussagen zu "hardened" Key Derivation (BIP-32) sind richtig?			
	a)	Sie verhindert Key-Ableitung nur mit Public Keys		
	b)	BIP steht für Bitcoin Improvement Proposals und deshalb funktionieren Key Derivations nur im Bitcoin System		
	c)	Bei der Key-Ableitung wird der Private Key verwendet statt des Public Keys		
	d)	Der Prozess benötigt zwingend eine Internetverbindung zur Validierung		

Aufgabe 4: Bloom Filter (6 Punkte)

Die folgende Tabelle zeigt das Alphabet a-c mit den Werten 0-2. Ihr Bloom Filter hat eine Länge von 4 Bits und Sie verwenden 2 Hashfunktionen: die erste Hashfunktion multipliziert die ersten beiden Buchstabenwerte, und addiert das Ergebnis mit dem dritten Buchstabenwert. Die zweite Hashfunktion addiert die ersten beiden Buchstabenwerte, und multipliziert das Ergebnis mit dem dritten Buchstabenwert. So hat z.B. der String «bba» mit der ersten Hashfunktion den Hash (1*1)+0=1, mit der zweiten Hashfunktion (1+1)*0=0.

a	**b**	**c**
0	1	2

a) (2P) Wie sieht Ihr Bloom Filter aus wenn Sie die folgenden Strings hinzugefügt haben: «bba», «aba», «bcb»

Bit 0	Bit 1	Bit 2	Bit 3

b) (2P) Welche Aussage können Sie über den Bloom Filter aus der Aufgabe a) treffen für alle möglichen Kombinationen des Alphabets a-c. Begrenzen Sie Ihre Antwort auf max. 2 Sätze.

Aussage:

c) (2P) Sie bekommen den folgenden Bloom Filter, überprüfen Sie ob die folgenden Strings enthalten sind: «bbb», «cab»?

Bit 0	Bit 1	Bit 2	Bit 3
1	0	1	1

Antwort:

bbb:
cab:

Aufgabe 5: Solidity/Ethereum (10 Punkte)

Das folgende Code Snippet eines Ethereum Smart Contracts zahlt Guthaben ein und aus:

```
pragma solidity ^0.8.0;

contract VulnerableContract {
    mapping(address => uint256) public balances;

    // Funktion, um Einzahlungen vorzunehmen
    function deposit() public payable {
        balances[msg.sender] += msg.value;
    }

    // Funktion, um Guthaben abzuheben
    function withdraw(uint256 _amount) public {
        require(balances[msg.sender] >= _amount, "Insufficient balance");

        // Auszahlung des Betrags
        (bool sent, ) = msg.sender.call{value: _amount}("");
        require(sent, "Failed to send Ether");

        // Aktualisierung des Kontostands
        balances[msg.sender] -= _amount;
    }
}
```

a) (2P) Was könnte das Problem in diesem Code sein? (Hinweis: der Syntax ist korrekt). Und was könnte die Lösung sein?

Problem:

Lösung:

b) (4P) Ein Gold-basierter Stablecoin "GLD" soll den Wert von einem Kilogramm Gold (ca. 100'000$) stabil halten. Das System verwendet physisches Gold als Sicherheit, und nutzt bei der Begleichung von Forderungen zunächst den Verkauf von ETH, bevor auf die Goldreserven zurückgegriffen wird. Gegeben ist folgendes Szenario:

- Der GLD Smart Contract hält derzeit 100 ETH (Preis: 2000$ pro ETH) und sie haben 4kg physisches Gold im Keller als Reserve
- Es sind 5 GLD Tokens im Umlauf
- Das System ist damit aktuell 120% überbesichert: (100 ETH × 2000$ + 4 Gold × 100'000$) / (5 GLD × 100'000$) = 1.2

Ein Händler möchte seine 3 GLD in ETH tauschen. Beschreiben Sie den Vorgang in max. 3 Sätzen mit den folgenden Börsen in diesem Szenario: eine Decentrarlized Exchange (DEX) wo man GLD gegen ETH tauschen kann, eine Centralized Exchange (CEX) wo man USD gegen ETH tauschen kann und einen physischen Handelsplatz (z.B. New York Mercantile Exchange - NYMEX) wo man Gold in USD tauschen kann.

Vorgang:

c) (3P) Wie sieht das Szenario nun bezüglich ETH auf dem Smart Contract, physischem Gold im Keller und GLD Tokens im Umlauf aus?

Smart Contract ETH:

Physisches Gold im Keller:

GLD Tokens im Umlauf:

d) (1P) Gehen Sie von dem neuem Szenario c) aus. Der ETH-Preis fällt. Beschreiben Sie wie sich dies auf die Besicherungsquote auswirkt.

Besicherungsquote wenn ETH Preis fällt: