Semesterprüfung HS23/24
Studienstandort Rapperswil

NAME: _____ **VORNAME:**_____

MATRIKEL-Nr.: _____

STUDIENGANG: _____

Modulcode:	**M_BLCH**
Modulbezeichnung:	**BLOCKCHAIN**
Modulowner:	**INFORMATIK**
Modulverantwortung:	Thomas Bocek
Prüfungsverantwortliche/r:	Thomas Bocek
Datum/Zeit:	**Mittwoch, 31.01.2024,** 10:30 – 11:30 Uhr

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

Korrektur: Thomas Bocek / _____ ____

(Name/Unterschrift)

Modul Blockchain (BlCh)
Prüfung HS23/24

Nr.	Aufgabe	Max. Punkte	Erreichte Punkte
1	Blockchain Basics	18	
2	Decentralized Finance (DeFi) Basics	18	
3	Algorithmen	10	
4	Atomic Swaps / HTLC	6	
5	Solidity / Ethereum	8	
		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 (20 Punkte)

a) (10P) Kreuzen Sie Zutreffendes an.

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

	Statement		True	False
1	Welche Aussage über Smart Contracts ist korrekt?			
	a)	Smart Contracts können nur in der Sprache Solidity geschrieben werden		
	b)	In Ethereum sind Smart Contracts immer deterministisch		
	c)	Smart Contracts benötigen manuelle Bestätigung von einem Netzwerkadministrator		
	d)	In Ethereum werden Smart Contracts ausserhalb der Blockchain gespeichert		
2	Welche Hauptfunktion erfüllt ein Orakel in einer Blockchain?			
	a)	Erzeugung von Kryptowährungen		
	b)	Bereitstellung von externen Daten für Smart Contracts		
	c)	Verschlüsselung von Transaktionsdaten		
	d)	Verwaltung von Wallet-Adressen		
3	Was ist die Hauptfunktion und/oder Ziele von Layer-2-Skalierungslösungen?			
	a)	Erhöhung der Sicherheit der Blockchain durch zusätzliche Verschlüsselung		
	b)	Die Auslagerung von Transaktionen von der Haupt-Blockchain		
	c)	Durch Layer-2-Skalierungslösungen werden die Transaktionskosten erhöht, sodass nur wichtige Transaktionen bestätigt werden		
	d)	Durch Layer-2-Skalierungslösungen wird die Transaktionsdurchsatzrate erhöht, sodass mehr Transaktionen bestätigt werden können		
4	Was ist der Hauptzweck von Proof of Attendance Protocol (POAP)?			
	a)	Registrierung der Teilnahme an physischen und virtuellen Veranstaltungen		
	b)	Nachweis des Besitzes einer bestimmten Kryptowährung		
	c)	Das Ziel ist das Sammeln und Tauschen von POAPs, um möglichst viele unterschiedliche POAPs zu besitzen		
	d)	Überprüfung der Identität der Teilnehmer an einer Blockchain-Transaktion		
5	Was beschreibt am besten eine Decentralized Autonomous Organization (DAO)?			
	a)	Eine Organisation, die vollständig von einer zentralen Autorität gesteuert wird		
	b)	Eine Gruppe von Minern, die zusammenarbeiten, um die Hash-Rate zu erhöhen		
	c)	Eine Organisation, die auf Smart Contracts basiert und autonom ohne zentrale Führung operieren kann		
	d)	Ein Konsortium von Banken, das die Entwicklung der Blockchain-Technologie fördert		

b) (3P) Beschreiben Sie den Prozess der Seed-Erzeugung gemäss BIP39 in 3 Schritten. Welche Schritte sind involviert, um von einer zufälligen Zahlengenerierung zu einer Mnemonic Phrase zu gelangen? Erklären Sie die Schritte mit je einem Satz.

Schritt 1:

Schritt 2:

Schritt 3:

c) (2P) Wie kann man überprüfen, ob eine Mnemonic-Phrase (Seed-Phrase) bei der Eingabe oder Wiederherstellung eines Wallets korrekt eingegeben wurde, um sicherzustellen, dass der Zugriff auf die Blockchain-Assets nicht verloren geht? Erklären Sie das Vorgehen in max. 2 Sätzen.

Vorgehen:

c) (3P) Beschreiben Sie einen Unterschied zwischen «Hardened» und «Non-Hardened» Schlüsseln / Keys in der BIP32 Hierarchie. Welche Auswirkung hat es, wenn ein «Non-Hardened» Public Key öffentlich bekannt ist?

Unterschied Hardened / Non-Hardened:

Non-Hardened Public Key öffentlich bekannt:

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

a) (10P) Kreuzen Sie Zutreffendes an.

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

		Statement	True	False
1	Was ist ein Flash Loan in der DeFi-Welt?			
	a)	Ein Kredit, der innerhalb einer einzigen Transaktion aufgenommen und zurückgezahlt wird		
	b)	Ein langfristiger Kredit, der über Smart Contracts vergeben wird		
	c)	Ein Kredit, der nur für Flash-Transaktionen auf zentralen Börsen verfügbar ist		
	d)	Ein Kredit, der innerhalb von max. 2 Transaktionen aufgenommen und zurückgezahlt wird		
2	Was kennzeichnet eine Decentralized Exchange (DEX) im Gegensatz zur Centralized Exchange (CEX) aus?			
	a)	DEXes erfordern persönliche Identifikationsinformationen für den Handel		
	b)	DEXes werden von einer zentralen Behörde betrieben und überwacht		
	c)	DEXes ermöglichen den Peer-to-Peer-Handel ohne zentrale Autorität		
	d)	DEXes unterstützen unter anderem Krypto-zu-Krypto-Handelstransaktionen		
3	Wie unterscheiden sich langfristige Loans von Flashloans im DeFi-Bereich?			
	a)	Langfristige Loans erfordern keine Sicherheiten und müssen innerhalb einer einzelnen Transaktion zurückgezahlt werden		
	b)	Flashloans erfordern umfangreiche Bonitätsprüfungen und haben eine Laufzeit von mehreren Monaten oder Jahren		
	c)	Langfristige Loans sind für einen längeren Zeitraum ausgelegt, erfordern meist Sicherheiten über die Laufzeit des Loans		
	d)	Langfristige Loans sind meistens overcollateralized, was bedeutet, dass sie mehr Sicherheiten erfordern als der ausgeliehene Betrag		
4	Was ist Arbitrage im Kontext von DeFi und wie wird sie üblicherweise durchgeführt?			
	a)	Der Kauf und sofortige Verkauf einer Kryptowährung auf demselben Markt, um von Preisunterschieden zu profitieren		
	b)	Die langfristige Investition in eine Kryptowährung, um von zukünftigen Preisanstiegen zu profitieren		
	c)	Der gleichzeitige Kauf und Verkauf desselben Vermögenswerts auf verschiedenen Märkten, um Preisunterschiede auszunutzen		
	d)	Das Ausleihen von Vermögenswerten, um sie in volatilen Märkten zu einem höheren Preis zu verkaufen und später zurückzukaufen		
5	Warum ist Arbitrage für das Funktionieren von Decentralized Exchanges (DEX) wichtig?			
	a)	Arbitrage Bots helfen, Preisunterschiede zwischen DEXes und anderen Märkten auszugleichen.		
	b)	Arbitrage dient der Identifizierung von Sicherheitslücken in Smart Contracts, und Arbitrage-Bots werden eingesetzt, um diese Schwachstellen zu testen		
	c)	Durch Arbitrage werden die Märkte effizienter. Es stellt sicher, dass die Preise der Assets ihre tatsächliche Nachfrage und ihr Angebot widerspiegeln		
	d)	Arbitrage spielt keine wesentliche Rolle auf DEXes; Arbitrage-Bots werden hauptsächlich für Marketingzwecke eingesetzt		

b) (4P) Wie wird der Preis bei einer Centralized Exchange (CEX) bestimmt? Und wie wird der Preis bei einer Decentralized Exchange (DEX) bestimmt? Erklären Sie die Preisbestimmung mit je 2 Sätzen.

Preis bei CEX:

Preis bei DEX:

b) (2P) Was verstehen Sie unter «Impermanent Loss» bei einer DEX? Erklären Sie «Impermanent Loss» in 2 Sätzen.

Impermanent Loss:

c) (2P) Was verstehen Sie unter «Slippage» bei einer DEX? Erklären Sie « Slippage» in 2 Sätzen.

Slippage:

Aufgabe 3: Algorithmen (10 Punkte)

a) (10P) Kreuzen Sie Zutreffendes an.

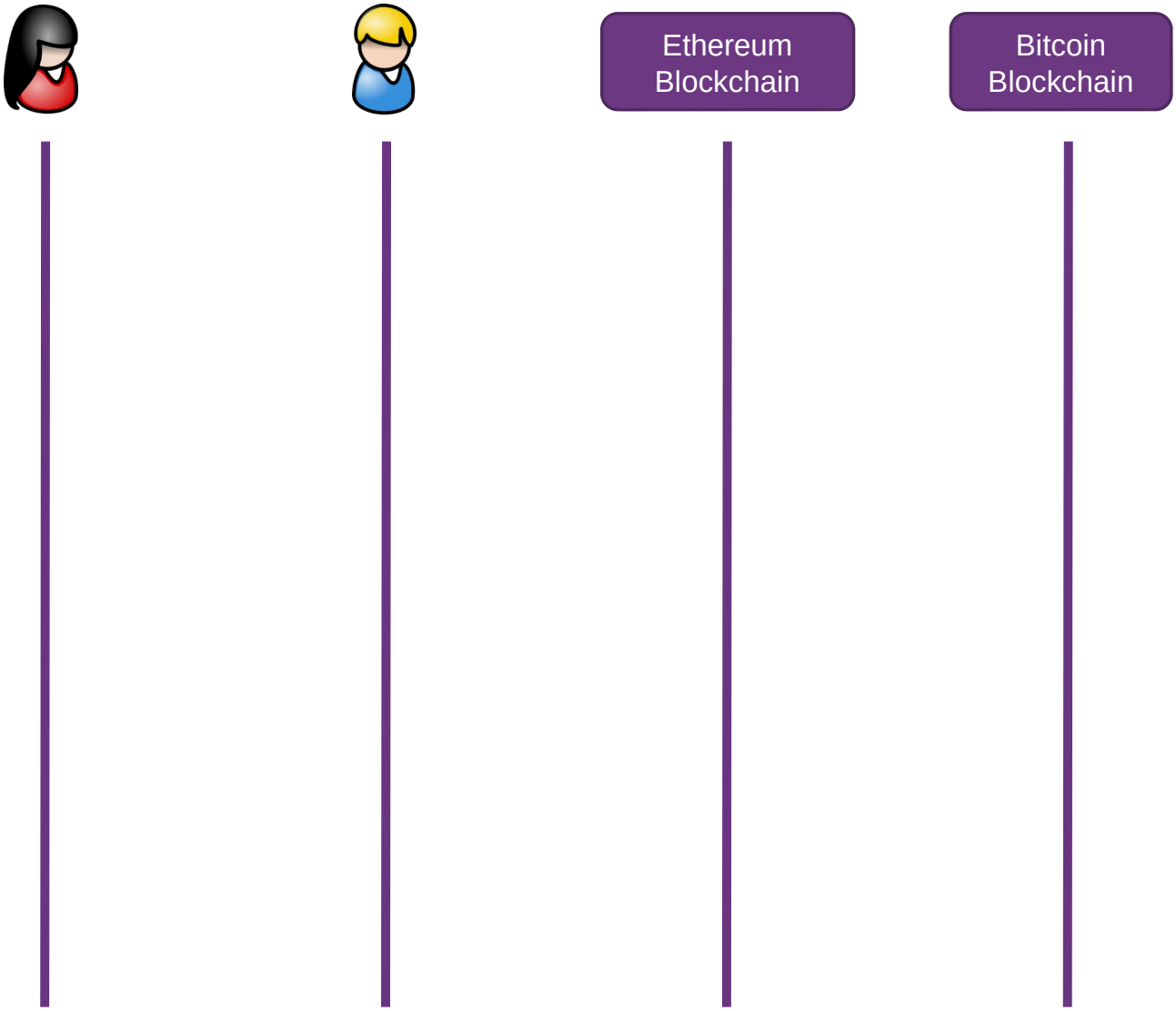
Bitte beachten Sie, dass **keine** Punkte für ein falsch gesetztes Kreuz abgezogen werden.

		Statement	True	False
1	Was beschreibt einen Bloom Filter am besten?			
	a)	Ein Datenstruktur, die schnelle Mitgliedschaftstests ermöglicht		
	b)	Eine Form der Datenverschlüsselung in der Blockchain		
	c)	Ein Protokoll für den sicheren Austausch von Kryptowährungen		
	d)	Ein Algorithmus zur Erzeugung von Merkle Trees		
2	Was ist ein Vorteil eines Bloom Filters?			
	a)	Ermöglicht das Rückgängigmachen von Transaktionen		
	b)	Bietet eine 100%ig genaue Mitgliedschaftsbestätigung		
	c)	Ermöglicht platzsparende Mitgliedschaftstests		
	d)	Unterstützt direkte Datenextraktion und -manipulation		
3	Was ist ein Merkle Tree?			
	a)	Eine Methode zur Verschlüsselung von Transaktionen in einer Blockchain		
	b)	Ein baumähnliche Struktur, die zur Zusammenfassung und zum effizienten Nachweis von Daten in einem Block verwendet wird		
	c)	Ein Algorithmus zur Erstellung von Smart Contracts		
	d)	Mit einem Merkle Tree kann die Zugehörigkeit eines Datenblocks zur gesamten Datenmenge überprüft werden		
4	Welchen Hauptvorteil bieten Merkle Trees in Blockchains?			
	a)	Reduzierung der Blockgrösse, da nicht mehr alle Transaktionen gespeichert werden müssen		
	b)	Vermeidung von Doppelausgaben		
	c)	Die Zugehörigkeit eines Datenblocks zur gesamten Datenmenge kann überprüft werden, ohne alle Daten vollständig herunterzuladen		
	d)	Automatisierung von Transaktionen		
5	Wie wird in einem Merkle Tree der Merkle Root berechnet?			
	a)	Durch das Summieren der Hashes aller Transaktionen		
	b)	Durch das paarweise Hashen von Transaktionshashes und das wiederholte Hashen bis zum Root		
	c)	Durch Auswahl des Hashes der ersten Transaktion im Block		
	d)	Durch zufällige Auswahl eines Transaktionshashes		

Aufgabe 4: Atomic Swaps / HTLC (6 Punkte)

Bob hat 12 ETHs und Alice hat 1 BTC. Bob möchte mit Alice 1 BTC für 12 ETHs tauschen. Wie kann Alice und Bob die ETHs und BTCs mit einem Atomic Swap und Hashed Time Lock Contracts (HTLC) austauschen?

(6P) Wer sendet welche Transaktionen an die entsprechenden Blockchains? Vervollständigen Sie die folgende Grafik eines erfolgreichen Austausches. Gehen Sie davon aus, dass die HTLC Smart Contracts und Adressen bereits existieren (Ethereum) resp. beiden bekannt sind (Bitcoin). Bob initiiert den Prozess.



Aufgabe 5: Solidity/Ethereum (8 Punkte)

Das folgende Code Snippet eines Ethereum Smart Contracts teilt ein Guthaben auf:

```
// Funktion, die einen Betrag in zwei Teile aufteilt:
// einen Prozentsatz des Betrags z.B., 75% und den Restbetrag z.B., 25%.
// Bei beiden Rückgabewerten (percentageAmount, remainingAmount) wird
// nie mehr als der tatsächliche exakte Betrag zurückgegeben.
function splitFunds(uint256 totalAmount, uint256 percentage) public pure returns (uint256 percentageAmount, uint256 remainingAmount) {
  // Berechnet den Anteil basierend auf dem gegebenen Prozentsatz
  percentageAmount = (totalAmount * percentage) / 100;

  // Berechnet den verbleibenden Betrag
  remainingAmount = totalAmount - percentageAmount;

  // Rückgabe der berechneten Beträge
  return (percentageAmount, remainingAmount);
}
```

a) (4P) Was könnte das Problem in diesem Code sein? (Hinweis: der Syntax ist korrekt). Und was könnte die Lösung sein?

Problem:

Lösung:

b) (4P) Für die Entwicklung einer neuen Finanzapplikation, die sowohl Sicherheit als auch Effizienz in der Verarbeitung von Transaktionen gewährleisten soll muss eine Blockchain verwendet werden. Welche Blockchain-Plattform würden Sie wählen? Sie haben die Wahl zwischen Bitcoin, Monero, und Ethereum. Bitte nennen Sie 3 Gründe Ihre Wahl.

Blockchain Wahl:

Grund 1:

Grund 2:

Grund 3: