



OST

Eastern Switzerland
University of Applied Sciences

Blockchain (BlCh)

Admin

Thomas Bocek

24.11.2024

BlCh 2024: Plan

Nr	Date	Lecture*	Lecturer
01	17.09.2024	Admin (lecture and challenge task), Repetition DSy (part 1) - no exercises	Bocek
02	24.09.2024	Repetition DSy (part 2), Introduction Blockchain, Ethereum Components / Architecture	Bocek
03	01.10.2024	Solidity	Bocek
04	08.10.2024	1st hand-in, Fungible Tokens, Stablecoins	Bocek
05	15.10.2024	DeFi, DEX	Bocek
06	22.10.2024	DAO, Non-Fungible Tokens	Bocek
07	29.10.2024	2nd hand-in, Wallets and Seed Phrases, POAP	Bocek
08	05.11.2024	HTLCs, Cross-chain Atomic Swaps, Payment Channels, DAI	Bocek
09	12.11.2024	Algorithms/Mechanisms for Fully Distributed Systems	Bocek
10	19.11.2024	3rd hand-in, Gai, Polkadot	Bocek
11	26.11.2024	Interview, Exam Preparation, Security Considerations, Layer 2	Bocek
12	03.12.2024	Final hand-in, Challenge Task Presentations, part 1	you
13	10.12.2024	Challenge Task Presentations, part 2	you
14	17.12.2024	Q&A and Challenge Task Award Winner Announcement - no exercises	Bocek

* topics may change

Exercises

- Do not use Sushiswap, use these:
 - Uniswap Ethereum Contract Deployments [\[link\]](#)
 - SwapRouter02
 - QuoterV2
 - UniswapV3Factory
- Interface: `exactInputSingle`
 - WETH:
0xfff9976782d46cc05630d1f6ebab18b2324d6b14

The image shows a web interface for the `exactInputSingle` function and a MetaMask transaction confirmation overlay.

Function Interface:

- Function: `exactInputSingle (0x04e45aaf)`
- exactInputSingle: 0
- params (tuple):
 - tokenIn: 0x36f438d47bb0285f90dc4b84d8d272a564cf72f9
 - tokenOut: 0xfff9976782d46cc05630d1f6ebab18b2324d6b14
- fee: 100
- recipient: 0x0CbdF580c4E117619631bA4b97dC0d439ADAbD88
- amountIn: 10000000000
- amountOutMinimum: 0
- sqrtPriceLimitX96: 0

MetaMask Confirmation:

- Extension: (MetaMask) - MetaMask — M...
- Network: Sepolia
- Account 1: 0x3bFA4...A...
- Transaction: 0x3bFA4...Ae48E : EXACT INPUT SINGLE
- Details: DETAILS | HEX
- Estimated changes:
 - You send: - <0.000001 (0x36F43...f72fc) Not Available
 - You receive: + <0.000001 (0xfff99...d6B14) Not Available
- Estimated fee: 0.00032364 (0.00032364 SepoliaETH)
- Market: -60 sec | Max fee: 0.00032406 SepoliaETH
- Buttons: Reject, Confirm

Presentations

- 1 group already handed-in, 1 group will present next Tuesday
- Available slots:
<https://rally.co/invite/xLbrSjsLEYY9>

Nr	Name 1	Name 2	Name 3	Project Idea + Repo
1	Noah F.	Tim E.		✓✓✓ (react/solidity)
2	Mino P.	Lukas A.		✓✓✓✓ (zeus token)
3	Corsin S.	Roman W.	Cedric C.	✓✓✓ (ccr token)
4	Dario B.	Dejan B.	Fabrice-Ronny B.	✓✓✓ (rutlicoin/react)
5	Matthias H.	Simon D.		✓✓✓ (Awec)
6	Matteo G.	Marco S.	Philipp H.	✓✓✓ (gold price)
7	Tom S.	Micha H.	Nico F.	✓✓✓ (wti-stablecoin)
8	Yannick S.	Sylvester H.	Roman C.	✓✓✓ (golang/solidity)
9	David H.	Andri J.	Davor L.	✓✓✓ (roesticoins)
10	Anja F.	Patrick S.		✓✓✓ (xoxo-taylor-coin)
11	Simon H.	Livio M.	Luca K.	✓✓✓ (co2coin)
12	Leonardo R.	Tobias K.		✓✓✓ (bidenbuck)
13	Tseten E.	Simon P.	Isaia B.	✓✓✓ (flipcoin)
14	Valerio F.	Eric H.		✓✓✓ (francoin)

Exam

- Last year HS 2023

Modul Blockchain (BICH) 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.