

This exercise sheet will be discussed in tutorials
from July 11 to July 15, 2022

Prof. Dr. Ali Sunyaev
sunyaev@kit.edu

AI: Internet Computing

Summer 2022

Exercise Sheet 5

Exercise 1: Distributed Ledger Technology

- Briefly describe a use case of your own choosing for the use of blockchain or DLT.
- Explain why the use of DLT makes sense in your use case. Consider essential attributes of DLT such as tamper resistance, data integrity, availability, decentralization, and disintermediation (minimization of trust and third parties).
- Differentiate between the terms blockchain and distributed ledger technology using the appropriate terminology.
- Differentiate between the different types of DLT (private/public and permissioned/unpermissioned). Which is most appropriate for your use case?

Exercise 2 (Excursus): Proof of Work

Take a look at the code in our repository¹ (especially the *startMining* method in *App.java* located in the *src* folder) and follow the instructions in the README. Try to understand the role of the nonce and the relationship between hash target (or difficulty) and execution time.

¹ <https://git.scc.kit.edu/tf2000/pow>

Exercise 3: Consensus Mechanisms

- a) In the context of DLT, what is a consensus mechanism? How does it differentiate from Proof of Work?
- b) What are the key differences of Proof of Stake and Proof of Work? What do they have in common?

Exercise 4: Smart Contracts

- a) What is a smart contract?
- b) Explain how a smart contract works within the Ethereum blockchain.
- c) Remix (<https://remix.ethereum.org/>) is an IDE² for smart contracts. Copy the code from the provided text file "TransactionDemo.txt" into Remix; test and understand the functions³. Please also try to specifically use arguments for the provided methods that cause errors.

Exercise 5: Adoption of Bitcoin

PayPal has announced the adoption of Bitcoin. Users in the US will be able to buy, sell, and hold selected cryptocurrencies⁴. What possible implications do you see (e.g., for society, technology, etc.)?

² IDE stands for Integrated Development Environment

³ Visit <https://remix.ethereum.org/> and create a file under "File Explorers". Paste the sample code into it. You can then compile the code in the Solidity compiler and deploy the compiled smart contract under "Deploy & Run Transactions". Under "Deployed Contracts" you can see all instances; you can expand them and call functions on them.

⁴ See <https://www.paypal.com/us/smarthelp/article/cryptocurrency-on-paypal-faq-faq4398>