Übungsklausur Web3 / Digitale Währungen & Blockchain Technologie 2022

1. Grundlagen zur Blockchaintechnologie

1.1. Distributed Ledgers / Verteilte Logbücher

Unter welchen Umständen ist die Nutzung von verteilten Logbüchern im Vergleich zu zentral verwalteten Logbüchern aus Ihrer Sicht empfehlenswert?

*Die Nutzung von verteilten Logbüchern im Vergleich zu zentral verwalteten Logbüchern ist empfehlenswert, sofern es keine nutzbare zentrale Instanz gibt, der jetzt und in Zukunft uneingeschränkt vertraut werden kann.*

Was ist für Sie das revolutionär Neue an der Blockchaintechnologie?

*Die Blockchaintechnologie hat eine neue Epoche in der Gestaltung des Internets eingeläutet. Nach*

*Web1(statische Webseiten mit Links – in den frühen 90ern) kam mit der Erfindung von Javascript… das*

*Web2 (dynamische Webseiten) – und danach mit der Erfindung der Blockchaintechnologie… das*

*Web3 (decentralized / distributed web)*

*Ich finde es weiterhin faszinierend, dass – durch die Nutzung von Konsensalgorithmen – die Notwendigkeit für zentrale Instanzen wegfällt und dass*

1.2 Einwegfunktionen

Welche Einwegfunktion spielt im Bitcoin System eine wesentliche Rolle bzw. zwei wesentliche Rollen? Bitte erläutern Sie dies in ca. 4 Sätzen.

1.3 Asynchrone Verschlüsselung / Public Key Verschlüsselung

Bitte beschreiben Sie ein Szenario, in welchem Alice an Bob eine vertrauliche Nachricht senden möchte und Bob sicher sein möchte, dass die Nachricht tatsächlich von Alice kommt. Hilfestellung: Was wird wann mit welchem Key verschlüsselt / entschlüsselt?

Inwiefern spielen digitale Signaturen bei Cryptowährungen wie Bitcoin & Ether eine wesentliche Rolle? Bitte erläutern Sie das knapp in 2 – 3 Sätzen

1.4 Datenstrukturen

1.4.1 Bloomfilter

Angenommen Sie nutzen einen Bloomfilter mit einem Bitset der Länge 11 mit den Bloombits 0 bis 10 sowie den folgenden Einwegfunktionen zur Belegung der Bits:

*h1(x)=(x \* 2)%11*

*h2(x)=(x \* 3)%11*

*h3(x)=(x \* 4)%11*

Wie sieht das Bitset jeweils nach dem Hinzufügen der folgenden Zahlen aus?

*const exampleArray = [6, 9, 14]*

--> Bitset nach dem Hinzufügen der 6:

--> Bitset nach dem Hinzufügen der 9:

--> Bitset nach dem Hinzufügen der 14:

Würde der Bloomfilter für die folgenden Zahlen jeweils einen false positive liefern?

*const entriesToBeValidated = [11, 3, 6]*

Bitte erläutern Sie mindestens einen Anwendungsfall von Bloomfilters.

1.4.2 Merkletrees (4 Punkte)

Bitte erstellen Sie einen Merkletree für die Einträge im untenstehenden Beispiel Array unter Nutzung der darunter stehenden Einwegfunktion:

const exampleArray = [2,4,8,1]

*h(x)=(x \* 2)%11*

Angenommen jemand behauptet im Beispielarray wäre eine 9 (anstelle der 1) enthalten. Welche Nodes innerhalb des MerkleTrees würden sich dadurch wie ändern?

Bitte erläutern Sie mindestens einen Anwendungsfall von Merkletrees.

1.4.3 Tries (2 Punkte)

Bitte skizzieren Sie einen klassischen Trie sowie daneben einen PATRICIA Trie für die folgenden Buchstabensequenzen:

Bitcoin, Ether, Blockchain, Blockheader

1.5 Konsensalgorithmen

Bitte erläutern Sie die Notwendigkeit von Konsensalgorithmen im Kontext verteilter Logbücher bzw. verteilter Anwendungen wie z.B. dem Ethereum System.

Aus welchen Gründen plant Vitalik Buterin & Friends aus Ihrer Sicht den Umstieg von Proof of Work auf Proof of Stake?

Bitte erläutern Sie wie ein "51% Angriff" auf die Bitcoin Blockchain gestaltet werden könnte und wie ein potentieller Angreifer davon beispielsweise profitieren könnte.

2 Anwendungsgebiete der Blockchaintechnologie

2.1 Digitale Währungen

Was sind für Sie die Hauptunterschiede zwischen einer Central Bank Digital Currency und einer Cryptowährung wie Ether? Was halten Sie von der potentiellen Einführung von Central Bank Digital Currencies? (ca. 7 Sätze)

Was halten Sie davon, dass Richard Nixon 1971 den Goldstandard aufgehoben hat? Warum?

Der folgende Smart Contract soll eine Währung namens QuinoaCoin mit den folgenden Eigenschaften definieren:

1. Nachkommastellen: 18

2. Gesamtzahl an Tokens (fixed supply): 2000000

Bitte streichen Sie fehlerhafte Zeilen und ersetzen Sie diese durch korrekte Anweisungen:

*// SPDX-License-Identifier: GPL-3.0*

*pragma solidity >=0.8.0 < 0.9.0;*

*import "https://github.com/OpenZeppelin/openzeppelin-contracts/blob/release-v4.4/contracts/token/ERC20/ERC20.sol";*

*contract QuinoaCoin is ERC20 {*

*constructor () ERC20("QuinoaCoin", "QNC") {*

*\_mint(msg.sender, 2000\*10\*\*17);*

*}*

*}*

Wie gehen Sie vor wenn Sie diesen Smart Contract z.B. auf dem Ropsten Test Netzwerk der Ethereum Blockchain oder auf dem Ethereum Mainnet deployen möchten?

Durch welche Handlungen könnten Sie als Eigentümer all dieser neu von Ihnen "geminteten" Coins auf dem Ethereum Mainnet dafür sorgen, dass sich andere Menschen für genau diese Coins interessieren und dafür vielleicht sogar etwas Fiat Geld wie z.B. Euro ausgeben würden, um Einheiten Ihrer Währung zu erwerben?

2.2 Decentralized Finance

Was verstehen Sie unter dem Begriff Decentralized Finance? Wie schätzen Sie die zukünftige Entwicklung von Decentralized Finance ein und warum?

2.3 Decentralized Governance

Was verstehen Sie unter dem Begriff Decentralized Governance? Bitte Erläutern Sie in diesem Kontext den Begriff "Decentralized Autonomous Organisations".

2.4 Decentralized Web (2 Punkte)

Angenommen Sie möchten eine HTML Seite unter einer bestimmten Domain im Internet veröffentlichen. Nehmen wir weiterhin an der Inhalt dieser Seite ist aus Ihrer Sicht derart wertvoll für die Menschen, dass Sie sicherstellen möchten, dass diese Seite für immer unter dieser Domain erreichbar sein wird.

Wie gehen Sie dazu vor?

2.5 Kunst / Collectibles / GamingAssets

Welches Smart Contract Template bzw. welche Smart Contract Templates würden Sie wählen, sofern Sie NFTs oder semi fungible tokens per Ethereum Blockchain gestalten und anbieten möchten?

3 Utilities & Aspekte

3.1 On-Chain / Off-Chain Verbindungen

Welche Browserextension können Sie z.B. für google chrome nutzen, damit Besucher Ihrer dApp mit Smart Constracts der Ethereum Blockchain interagieren können? Bitte nennen Sie eine Alternative zu dieser Browserextension.

Welches Deno Modul hilft Ihnen dabei ein zentrales - bei Ihnen lokal serverseitig ausgeführtes - in TypeScript geschriebenes Programm mit Smart Contracts der Ethereum Blockchain zu verbinden? Bitte erläutern Sie grob welche Rolle das ABI des zu verbindenden Smart Contracts dabei spielt.

Wie würden Sie die Funktion von infura.io in diesem Kontext ihren Freunden erläutern?

3.2 Airdrops

Wozu werden Airdrops typischerweise genutzt?

- [ ] Denial of Service Angriffe durchführen

- [ ] Distributed Denial of Service Angriffe durchführen

- [ ] Währung deployen

- [ ] Voting Power verteilen

- [ ] NFTs deployen

- [ ] Early Adopters belohnen

Welche Informationen und Module benötigen Sie wenn Sie einen Airdrop für Ihre Early Adopters gestalten möchten, welchen Sie über ein TypeScript Programm lancieren?

3.3 Smart Contracts

Wie würden Sie im Allgemeinen das Konzept „Smart Contracts“ Ihren Freunden beschreiben? Inwiefern kann ein Smart Contract als smarte Vereinbarung bezeichnet werden?

Angenommen Ihr Smart Contract soll alle Funktionen des „Ownable“ Smart Contracts (siehe Import 1) beinhalten. Bitte ergänzen Sie den untenstehenden Teil des Smart Contracts so, dass dieser das tut. (1 Punkt)

```

*import "https://github.com/OpenZeppelin/openzeppelin-contracts/blob/release-v4.4/contracts/access/Ownable.sol"*

*import "https://github.com/OpenZeppelin/openzeppelin-contracts/blob/release-v4.4/contracts/token/ERC1155/ERC1155.sol";*

*contract WWI19SEBSEMIFUNGIBLENFTS is ERC1155 {*

```

3.4 Wallets

Vergleichen Sie Custodial Wallets vs. Non-Custodial Wallets und nenne Sie dabei mindestens ein Beispiel für ein non-custodial wallet.

Vergleichen Sie Paperwallets und Browserwallets? In welchem der beiden würden Sie eher eine sehr große Summe an Ether speichern? Warum?

3.5 Stable Coins

Was verstehen Sie unter einem Stable Coin? Auf welche Arten können Stable Coins implementiert werden? Kennen Sie Beispiele?

3.6 Exchanges / Börsen

Was sind für Sie Unterschiede zwischen zentralen Exchanges (e.b. binance.com, coinbase.com etc.) und dezentralen Exchanges (e.g. uniswap.org)?

3.7 Mining

Wofür steht die Abkürzung "ASIC" im Bezug auf Mininghardware?

- [ ] Asynchronous Security Implementation Community

- [ ] Asset Specific Integrated Circuit

- [ ] Application Specific Integrated Circuit

- [ ] Altcoin Specific Integrated Circuit

- [ ] Alternative System for Improved Control  
- [ ] Application Specific Initial Coin

3. 8 Layer 2 Scaling

Inwiefern kann / wird Arbitrum aus Ihrer Sicht die Adoption der Ethereum Technologie beschleunigen?

4. Kreativteil

Bitte beschreiben Sie eines Ihrer Lieblingsthemen oder Lieblingsprojekte im Blockchain Space. Bitte achten Sie darauf dieses auf eine wissenschaftlich wertvolle Art zu beschreiben – kein Stammtischtalk mit 1.5 Promille ☺ - sondern eher eine Erläuterung auch im Hinblick auf einige der im Rahmen dieser Vorlesungsreihe erkundeten Aspekte / Konzepte.