Musterlösungen –

Digitale Währungen Klausur 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 weiterhin Konsensalgorithmen revolutionär. Mit Bitcoin und Ether sind mittlerweile weitgehend verteilte, digitale Assets vorhanden, so dass Proof of Stake eine gute Alternative zu Proof of Work darstellt.*

*Im Hinblick auf die Datenspeicherung finde ich auch den Paradigmenwechsel von CRUD Operationen hin zu CR Operationen bemerkenswert – kein update – kein delete.*

*Im Hinblick auf die kulturelle Dimension finde ich es bemerkenswert, dass die Blockchaintechnologie eine der wenigen digitalen Technologien ist, bei der Akteure mit besonderer Marktmacht keinen oder kaum einen unfair advantage haben (als Kontrast dazu nenne ich die Deep Learning Technologie, welche von Oligopolisten (AWS, Google, …) viel besser genutzt werden als von common peoples…).*

1.2 Einwegfunktionen

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

*Im Bitcoin System wird die SHA256 Funktion als wesentlicher Bestandteil des Konsensalgorithmus Proof of Work genutzt. In die Erstellung des SHA256 Blockhashes - als Arbeitsnachweis (PoW) - gehen die folgenden Input Parameter ein:*

*1. Die Bitcoin Versionsnummer*

*2. Der vorherige Blockhash*

*3. Der Merkle Root Hash aller - dem aktuellen Block zugeordneten - Transaktionen*

*4. Der Zeitstempel (wann hat das hashing stattgefunden?)*

*5. Der aktuelle Schwierigkeitsgrad*

*6. Die Nonce (number used once – um einen Hash zu finden, der den aktuellen Kriterien entspricht)*

*Wer den Blockhash gefunden hat, darf den Block der Blockchain hinzufügen. Die längste Chain gewinnt.*

*Zusätzlich spielt die SHA256 Funktion beim Signieren von Transaktionen und bei der Walletgenerierung eine wesentliche Rolle.*

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?

*Alice verschlüsselt die Nachricht mit ihrem Private Key. Das Ergebnis verschlüsselt sie mit dem Public Key von Bob. Das Ergebnis sendet sie an Bob. Bob entschlüsselt die Nachricht mit seinem privaten Schlüssel. Das Ergebnis entschlüsselt Bob mit dem öffentlichen Schlüssel von Alice.*

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

*Digitale Signaturen ermöglichen es sicherzustellen, dass eine Transaktion tatsächlich von einem bestimmten Sender (Besitzer des Private Keys) getriggert wurde.*

*Die Sign Funktion wird genutzt um eine Nachricht / Transaktion mit Hilfe des Private Keys zu signieren.*

*Die Verify Funktion wird genutzt um die Authentizität einer Nachricht / Transaktion mit Hilfe des Public Keys des Senders zu überprüfen.*

1.4 Datenstrukturen

1.4.1 Bloomfilter

Angenommen Sie nutzen einen [Bloomfilter](https://deno.land/x/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: *0 1 1 0 0 0 0 1 0 0 0*

--> Bitset nach dem Hinzufügen der 9: *0 1 1 1 0 1 0 1 0 0 0*

--> Bitset nach dem Hinzufügen der 14: *0 1 1 1 0 1 1 1 0 1 0*

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

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

*für die 11: nein*

*für die 3: ja – false positive*

*für die 6: nein – zwar positive – jedoch nicht false positive*

Bitte erläutern Sie mindestens einen Anwendungsfall von Bloomfilters.

*Bloomfilter können genutzt werden, um Netzwerk Traffic zu reduzieren. Das ist insbesondere in verteilten Netzwerkarchitekturen besonders lohnenswert.*

*Beispielsweise wenn es darum geht zu prüfen ob ein bestimmer Eintrag bereits in einem Ledger auf einem Server gespeichert ist - ohne das Ledger mitsenden zu müssen UND ohne durch Bloomfilter leicht vermeidbare Calls in Richtung des Servers zu generieren.*

1.4.2 Merkletrees

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*

Diagram

Description automatically generated

ob addition oder concatenation der hashwerte genutzt wurde, ist für die Bewertung egal – beides gilt

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

*Der rechte Ast / Zweig bis hoch zum Root Hash 🡪 7, 4, 3*

Bitte erläutern Sie mindestens einen Anwendungsfall von Merkletrees.

*Merkletrees können genutzt werden, um zu prüfen bzw. sicherzustellen, dass spezifische Elemente einer Liste (z.B. Transaktionen innerhalb eines Blocks) an einer bestimmten Position enthalten sind. Wird auch nur eine einzige Transaktion modifiziert oder ihre Position geändert, ändert sich der Root Hash – siehe auch Bitcoin’s simplified payment verification chapter 8 whitepaper.*

1.4.3 Tries

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

Bitcoin, Ether, Blockchain, Blockheader

Diagram

Description automatically generated

1.5 Konsensalgorithmen

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

Da jeder Miner grundsätzlich neue Transaktionen und Blocks zur Blockchain hinzufügen kann - und dadurch natürlich sehr schöne Transaktionen für jeden Wallet Besitzer vorstellbar sind… - braucht es einen Mechanismus der darüber entscheidet ob die neu hinzugefügten Transaktionen und Blöcke legitim sind.

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

*Beim proof of work beweist derjenige, der einen neuen Block hinzufügt, dass er sehr wahrscheinlich viel Arbeit (Rechenleistung) erbracht hat, um einen passenden Blockhash zu finden. Sofern dieser Akteur einen Betrugsversuch unternehmen würde, wäre es extrem wahrscheinlich, dass die von ihm erbrachte Arbeit unnötig erbracht wurde und er z.B. keinen Block Reward erhält. Dadurch haben Miner im PoW ein Anreizsystem sich integer zu verhalten.*

*Da es nun mit Bitcoin und Ether weitgehend anerkannte, verteilte digitale Assets gibt ist eine Umstellung auf Proof of Stake möglich. Anstelle von Arbeit sorgt der Stake (Pfand) für die entsprechende Anreizstruktur. Das erspart sehr viel „unnötig“ zu erbringende Rechenleistung, was vor allem aus ökologischer Perspektive wertvoll ist.*

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

*Sofern ein Angreifer mehr als 50 % der Rechenleistung besitzt, kann dieser mit einer hohen Wahrscheinlichkeit dauerhaft die longest chain maintainen. Dadurch kann er Transaktionen & Blocks hinzufügen, welche zuvor hinzugefügte Blocks invalidieren. Das lässt sich auf viele Arten ökonomisch ausnutzen. Die Einfachste und diejenige bei welcher der Angreifer (gleichzeitig der bewusste Nutznießer des Angriffs) schwer zu identifizieren wäre, ist jene die Währung zu shorten, da ein Bekanntwerden einer erfolgreichen 51 % Attack sehr sicher zu stark fallenden Preisen führen würde.*

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)

*Eine CBDC wird zentral durch politische Machthaber gesteuert.*

*Cryptowährungen basieren auf Algorithmen und werden m.E. weitgehend durch demokratisch organisierte Blockchain Node Betreiber gesteuert.*

*Mitarbeiter bzw. Lenker zentraler Institutionen sind häufig conflict of interest Situationen ausgesetzt – bewusst oder unbewusst. Das führt häufig zu Korruption, Vetternwirtschaft, Insidertrading & Co.*

*Zentrale Institutionen haben in der jüngeren Vergangenheit häufig versagt – siehe BaFin Skandal rund um Wirecard (unangebrachtes short selling verbot…) …, die Wallstreetbets 🡪 Gamestop 🡪 „RobinHood“ Affäre (illegale zentrale Marktintervention durch „RobinHood“ und andere) …*

*Eine CBDC ist wahrscheinlich ein Traum für jeden Diktator, da mit einer CBDC der Überwachungsstaat auf ein extremes Level kommt.*

*Wer die Freiheit liebt sollte sich m.E. Ländern entziehen, welche eine CBDC nutzen möchten oder die Weichen stellen, dass CBDCs scheitern.*

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

*Kurzfristige egoistische Interessen konnte Richard Nixon dadurch bedienen. Viele langfristige Auswirkungen stehen uns eventuell erst noch bevor, sobald die einzige Antwort von Zentralbanken auf Krisen – nämlich die Geldmenge zu erhöhen (durch Leitzinssenkungen, Quantitative Easing, …) – nicht mehr funktioniert.*

*Dies kann passieren, sobald wir nicht mehr lediglich eine enorme Asset Inflation sondern auch eine enorme Konsumgüterinflation bekommen, weil dies dazu führen kann, dass viele Menschen ihr Geld z.B. nicht mehr durch den gelegentlichen Kauf von Immobilien vor der Inflation schützen sondern durch die massive Flucht aus bestimmten Fiatwährungen und aus Ländern insgesamt deren Fiatwährungen kaum mit einem „handfesten“ Asset wie Bitcoin, Ether, Gold etc. gedeckt sind. Falls die Zentralbanken dann die Leitzinsen erhöhen möchten, sorgt dies für sehr viele private und kommerzielle Insolvenzen. Dies scheint mir eine Art Deadlock zu sein, welcher auch durch die Aufhebung des Goldstandards… zustandekam.*

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);~~*

*\_mint(msg.sender, 2000000\*10\*\*18);*

*}*

*}*

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?

*Ich öffne remix.ethereum.org, implementiere den Smart Contract dort als .sol (solidity) Datei und kompiliere diesen. Danach stelle ich sicher, dass mein Browserwallet mit dem gewünschten Zielnetzwerk connected ist (z.B. Ropsten oder Mainnet). Danach deploye ich den Smart Contract via remix…*

*Um zu prüfen ob alles geklappt hat, gehe ich auf etherscan.io (bzw. ropsten.etherscan.io) und schaue nach der entsprechenden Transaktion…*

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?

*Ich erzeuge einen Liquidity Pool bei via uniswap.org und statte diesen mit ordentlich Liquidität aus – z.B. für das Trading Pair ETHQNC.*

*Des Weiteren habe ich hoffentlich ein cooles Projekt mit einer vielversprechenden Value Proposition hinter dem QNC Coin definiert. Dann kann ich dieses Projekt entsprechend promoten…*

2.2 Decentralized Finance

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

*DeFi bezeichnet Financial Services welche ohne zentrale Institutionen (Banken, Versicherungen, Exchanges) – stattdessen smart contract basiert - bereitgestellt werden.*

*Ein wichtiger KPI für das DeFi System ist der Total Value Locked – vergleichbar mit dem im CeFi häufig genutzten „Assets under Management“ Indikator.*

*Der Automatisierungsgrad ist per Definition im DeFi System viel höher, was regelmäßig eine höhere Effizienz erwarten lässt….*

*DeFi ersetzt m.E. in Teilen oder revolutioniert allmählich das zentrale Finanzsystem (CeFi).*

2.3 Decentralized Governance

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

*DAOs sind m.E. eine revolutionäre Organisationsform, welche in gewisser Hinsicht mit Aktiengesellschaften vergleichbar sind. DAOs sind diesen gegenüber viel leichtgewichtiger und leicht zu implementieren. Wie bei Aktiengesellschaften gibt es Beteiligungs- und Mitbestimmungsmöglichkeiten. Um diese Beteiligungs- und Mitbestimmungsmöglichkeiten zu gestalten nutzen wir oft Governance Tokens für eine dezentrale Steuerung der Organisation / des Projektes…*

2.4 Decentralized Web

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?

*Ich registriere eine Domain via ens.domains, speichere die Seite (index.html…) in ipfs.io, trage den IPFS Hash in ens.domains als content link ein und teste ob es funktioniert – danach verbrenne ich ggf. meinen private key – je nach Ernsthaftigkeit und Kritikalität des Anwendungsfalls.*

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?

*NFT: ERC721*

*SFT: ERC1155*

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.

*metamask.io*

*alternative: brave.com (wallet schon im browser integriert)*

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.

*Das* [*https://deno.land/x/web3*](https://deno.land/x/web3) *Modul.*

*Im ABI sind die Funktionen des Smart Contracts dokumentiert, mit welchem ich interagieren möchte. Mein TypeScript Programm weiß dadurch welche Funktionen es mit welcher Parametrisierung & Typisierung aufzurufen hat.*

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

*Infura bietet Entwicklern, die z.B. keine eigene Blockchain Node betreibern eine Verbindung zur Blockchain an. Vergleichbar mit Internetprovidern – Infura ist ein Blockchain Access Provider für viele.*

3.2 Airdrops

Wozu werden Airdrops typischerweise genutzt?

- [ ] Denial of Service Angriffe durchführen

- [ ] Distributed Denial of Service Angriffe durchführen

- [ ] Währung deployen

- [x] Voting Power verteilen

- [ ] NFTs deployen

- [x] 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?

*Smart Contract Adresse der Airdrop Assets – z.B. Governance Token- / Coin- Contract (z.B. als ERC20)*

*Application Binary Interface (ABI) des Smart Contracts*

*Eine Provider URL oder eine eigene Node für die Verbindung zur konkreten Blockchain*

*Adresse der Empfängerwallets*

*Adresse und Private Key des Senderwallets*

*Web3 Modul*

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?

*Smart Contracts sind Programme, welche auf einer Blockchain gespeichert und ausgeführt werden. Sie sind insofern smarte Vereinbarungen, als dass ihre Erfüllung automatisiert sichergestellt ist. Das ist vergleichbar mit einem Getränkeautomaten am Bahnhof – auch mit diesem können wir eine smarte Vereinbarung haben, welche z.B. lautet: „Schmeiß Du mir 2 Euro rein, dann schmeiße ich Dir eine Flasche Wasser raus.“ Solche Verträge werden regelmäßig eingehalten, ohne dass es Anwälte braucht und ohne dass Rechtsverdreher eine Chance hätten das Recht zu verdrehen – unter der Annahme, dass die Smart Contracts und das System in diesem Sinne fehlerfrei und integer sind.*

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.

```

*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 , Ownable {*

*}*

```

3.4 Wallets

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

*Bei einem non-custodial wallet bin ich selbst für die Verwaltung meines Private Keys zuständig*

*Bei einem custodial wallet übernimmt ein Hüter (custodian) die Verwaltung meines Private Keys*

*Beispiel für non-custodial wallet = metamask.io*

*Beispiel für custodial wallet = BitGo*

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

*Paperwallets gehören in die Kategorie der „Cold Wallets“ (nicht mit dem Internet verbunden…) und sind im Wesentlichen ein Stück Papier mit eine Public Key + Private Key Pair. Sie sind im Vergleich zu Browserwallets (metamask.io etc.) m.E. besser geeignet um große Summen an Ether & Co. „aufzubewahren“. Einlaminiert im Wald vergraben halte ich Paperwallets momentan für eine der sichersten Varianten um Geld aufzubewahren. Es gibt viele sophisticated scams rund um metamask, auf welche sogar recht erfahrene Crypto Insiders schon reingefallen sind…*

3.5 Stable Coins

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

*Im Wesentlichen gibt es*

*1. Algorithmic stable coins (z.B. DAI, UST) und*

*2. Fiat “backed” “stable” coins (z.B. USDT – likely a scam)*

*Hybridformen halte ich eigentlich nicht für erwähnenswert.*

*Bei algorithmic stable coins wird der stabile Wechselkurs (z.B. 1 zu 1 zum US Dollar) wie der Name sagt durch Algorithmen – hier Smart Contracts erreicht. Im Detail gibt es erkundenswerte Unterschiede im Hinblick auf diese Algos z.B. zwischen UST (stark von einer zumindest aktuell künstlich erzeugten Nachfrage abhängig) und DAI (der m.E. solideste Stable Coin atm).*

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)?

*Zentrale Exchanges haben fragwürdige Anreizstrukturen in Richtung Marktmanipulation, da sie weniger auf Transparenz und mehr auf unfair advantages gegenüber den Tradern / Marketmakern basieren. Zentrale Systeme neigen oft zu Korruption, Vetternwirtschaft, Insidertrading und Co.*

*Dezentrale Exchanges wie uniswap basieren auf smart contracts, welche für jeden einsehbar sind.*

*Insbesondere uniswap hat m.E. eine Innovationskraft (Uniswap V3 Liquidity Pools etc…), welche mit dafür sorgen wird, dass zentrale Exchanges – wenn überhaupt – bald nur noch als Fiat On-Off Ramps genutzt werden.*

*Sofern wir dann noch Aggregators wie* [*1inch.io*](https://1inch.io/) *einbeziehen wird klar, dass die Qualität der dezentralen exchange services für zentrale exchanges nicht mehr zu toppen ist. In diesem Sinne wurden zentrale Exchanges Opfer ihres eigenen Erfolges…, da dieser wahrscheinlich alle von ihnen träge, korrupt und unfair gemacht hat.*

3.7 Mining

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

- [ ] Asynchronous Security Implementation Community

- [ ] Asset Specific Integrated Circuit

- [x] 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?

*Arbitrum ist meines Erachtens momentan die vielversprechendste Layer 2 Scaling Solution. Viele Projekte - z.B. uniswap.org bieten ihre services bereits auch auf dieser chain (arbiscan.io). Dadurch sind viele Geschäftsprozesse, welche früher auf dem Ethereum Mainnet gemacht wurden und mit hohen Kosten für die Gas Fees einhergingen, nun auch auf Arbitrum möglich. Die Arbitrum Bridge ist leicht bedienbar…. Aus diesen Gründen glaube ich, dass Arbitrum die Adoption massiv beschleunigen kann.*

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.

*Eines meiner Lieblingsprojekte im Blockchainspace ist ens.domains. Durch dieses Projekt ist ein dezentrales Domain Name System am Start. Die entsprechenden Domains können nicht nur als Web Adressen genutzt werden, um Web Apps via Browser leicht zugänglich zu machen, sondern sie können ebenso als Crypto Wallet Adressen Aliase genutzt werden, um es den Sendern von Crypto Assets sehr leicht zu machen eine Transaktion an den gewünschten Adressaten zu triggern.*

*Das Projekt hat im Rahmen eines Airdrops an seine early Adopters & Supporters dafür gesorgt, dass sich diese leicht in den Governance Prozess einbringen und das Projekt auch durch Mitbestimmungsrechte mitgestalten können.*

*In Verbindung mit einem dezentralen Dateisystem wie z.B. ipfs.io ist es durch ens.domains möglich beispielsweise das page provisioning komplett dezentral zu gestalten.*

*Mir ist bewusst, dass es weitere ähnliche Projekte gibt, gleichzeitig glaube ich, dass ens.domains hier dauerhaft eine Pionierrolle spielen wird.*