Konzept und Funktionsweise von Blockchains - Erwartungsbild

1 Eigenschaften der Blockchain

1.1 Erläutere die Eigenschaft der Dezentralität einer Blockchain. Gib dazu auch an was geschieht, wenn ein Client im Netzwerk ausfällt.

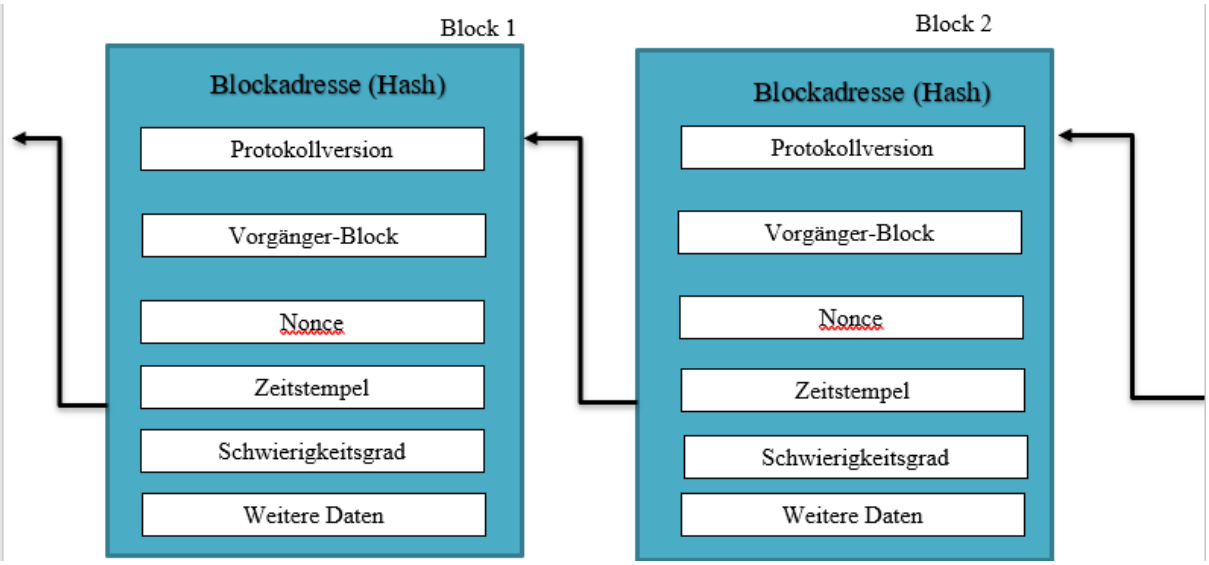
In einer Blockchain werden die Daten nicht auf einem einzigen Server gespeichert. Alle Clients erhalten eine Kopie aller Daten auf ihren Geräten, also werden sie bei allen gespeichert.

Wenn ein Client im Netzwerk ausfällt, arbeitet die Blockchain normal weiter, da alle NutzerInnen selbst als Server funktionieren.

1.2 Erkläre mit Hilfe der Eigenschaften der Blockchain, wodurch ein Manipulationsversuch an der Kette aufgedeckt werden kann.

Eine Blockchain ist Transparent. D.h. alle Clients können jederzeit die Daten auf ihr einsehen. Versucht jemand die Daten zu manipulieren, würden alle Nutzer die Änderung mit ihrer eigenen Kopie vergleichen und merken, dass die Liste bei dem Angreifer nicht stimmt. So würde der Manipulationsversuch durch die Transparenz und die Dezentralität auffallen.

2 Aufbau einer Blockchain



2.1 Erkläre die Funktionen der einzelnen Bestandteile der Blockchain.

- In der Blockadresse (dem Hash) steht der eindeutige Name des Blockes drin.
- Die *Protokollversion* gibt das Regelwerk an, unter dem der Block erstellt wurde.
- Die *Nonce* (*number used once*) ist eine Zahl, mit dessen Hilfe die Blockadresse errechnet wird. Mit ihrer Hilfe soll der Proof-of-Work erfüllt werden.
- Der *Zeitstempel* bildet den genauen Zeitpunkt ab, an dem der Block erstellt wurde.
- Der *Schwierigkeitsgrad* gibt an, mit welcher Schwierigkeit der Block erstellt wird.
- In *weiteren Daten* kann alles Weitere geschrieben werden, was gespeichert werden soll. Je nachdem, wofür die Blockchain genutzt wird.

2.2 Gib einen möglichen Vorteil davon an, dass jeder Block jeweils auf seinen Vorgänger verweist. Begründe deine Antwort.

Wenn eine Änderung in einem alten Block durchgeführt werden würde, würde sich dessen Blockname verändern. Das hätte zur Folge, dass beim nächsten Block der Vorgänger nicht mehr stimmen würde. Alle Nutzer würden dies schnell merken und könnten entsprechend einen Manipulationsversuch verhindern.

3 Blockerstellung mit dem Proof-of-Work

3.1 Erkläre in eigenen Worten wie die Blockerstellung mit Hilfe des Proof-of-Work funktioniert.

Beim Proof-of-Work müssen alle Teilnehmenden im Netzwerk ein mathematisches Rätsel lösen. Wer das am schnellsten schafft, erhält eine Belohnung und das Recht einen neuen Block zu erstellen.

3.2 Gib alle Elemente an, die für den Nutzer, bei der Blockerstellung mittels Proof-of-Work, gegeben sind.

Es sind gegeben ein Hash, die Protokollversion und der Schwierigkeitsgrad.

3.3 Erkläre, welche Funktion der Schwierigkeitsgrad genau bei dem Proof-of-Work erfüllt.

Der Schwierigkeitsgrad gibt an, wie viele Nullen am Anfang der Blockadresse stehen müssen.

3.4 Gib eine Methode an, mit welcher die Nonce ermittelt werden kann.

Die Nonce kann nur durch Ausprobieren ermittelt werden.

3.5 Angenommen ein Team besitzt insgesamt über 50% der gesamten Rechenleistung des Blockchain-Netzwerks. Erläutere die Folgen, die sich daraus ergeben würden.

Wenn ein Team über die Hälfte der gesamten Rechenleistung besitzt, sind sie dazu in der Lage am aller schnellsten möglichst viele Zahlen für die Nonce auszuprobieren. Damit haben sie die höchste Chance, einen neuen Block zu erstellen. Alle anderen NutzerInnen bräuchten viel Glück, um noch einen erstellen zu können.

4 Blockerstellung mit dem Proof-of-Stake

Ermittle den Vorgang zur Erstellung eines Blockes, beim Proof-of-Stake. Beantworte dafür die folgenden Aufgaben.

4.1 Erläutere die Funktion des Wallets beim Proof-of-Stake und wie der Stake (Einsatz) damit zusammenhängt.

Im Wallet können Einheiten der Kryptowährung hinterlassen werden. Diese können dann nicht mehr ausgegeben werden. Die Einheiten im Wallet werden Stake genannt.

4.2 Gib an, inwiefern der Schwierigkeitsgrad und das Wallet zusammenhängen.

Je höher der Einsatz im Wallet ist, desto niedriger ist der Schwierigkeitsgrad für das zu lösende mathematische Rätsel.

4.3 Erkläre das Zustandekommen der Belohnungshöhe bei erfolgreicher Blockerstellung.

Wenn man einen Block erfolgreich erstellt, erhält man dafür eine Belohnung. Je höher der Einsatz für das Rätsel war und je länger dieser im Wallet lag, desto höher fällt der Betrag der Belohnung aus.

5 Chancen und Risiken der Blockchain

Diskutierte den Nutzen und mögliche Gefahren der Blockchain. Beurteile dazu, ob Du selbst die Blockchain nutzen würdest und begründe deine Antwort.

Dadurch, dass die Blockchain im Nachhinein nicht manipuliert werden kann, bleiben Daten auf ihr dauerhaft gespeichert und können nicht gelöscht werden. Das hat z.B. den Vorteil, dass niemand meine persönlichen Daten manipulieren könnte. Ich kann immer eindeutig beweisen, wer ich bin bzw. was ich gespeichert habe. Allerdings bedeutet das auch, das veraltete oder auch unvorteilhafte Informationen für immer gespeichert sind. Das kann zu Problemen führen.

Ein Nachteil könnte auch die große Datenmenge sein, die ich speichern muss. Mit jeder Operation und jedem zusätzlichen Teilnehmenden erhöht sich auch die Datenmenge, die auf meinem Gerät liegt, wenn ich Teil des Blockchainnetzwerks sein will.