Universität des Saarlandes
FR Informatik

Kurt Mehlhorn und Antonios Antoniadis **WiSe 2019/20**

Übungen zu Ideen der Informatik

https://www.mpi-inf.mpg.de/departments/algorithms-complexity/teaching/winter19/ideen/

Blatt 14 Abgabeschluss: Keine Abgabe nötig.

Aufgabe 1 (*10 Punkte*) Teilnehmer bei dem Bitcoin/Blockchain Protokoll die versuchen die mathematischen Rätsel zu lösen, und damit den nächsten Block an der Blockchain bestimmen zu dürfen, nennt man auch *Miner*. Wie in der Vorlesung besprochen, darf ein Miner auch eine Transaktion in den Block setzen bei der er zur Belohnung einen festen Betrag an Bitcoins bekommt. Am Anfang, in 2008, waren das jeweils 50 Bitcoins. Jedes mal wenn die Blockchain um 210000 Blocks gewachsen ist, was circa alle 4 Jahre passiert, wird dieser Betrag halbiert. So liegt dieser gerade bei 12.5. Da die kleinste Denomination des Bitcoins $1/10^8$ beträgt (ein Satoshi), wird man irgendwann den Betrag nicht mehr halbieren können und der Betrag der Belohnung wird dann auf Null gesetzt. Wann wird das etwa passieren? Wie viele Bitcoins werden dann im Umlauf sein?

Lösung: Circa 2110-2140 wird der Betrag auf 0 fallen. Die menge der Bitcoins in Zirkulation wird dann circa 21 Millionen sein.

Aufgabe 2 (*10 Punkte*) Die Anzahl der Nullen, mit der die Ausgabe der kryptographischen Hashing-Funktion anfangen muss, wird so bestimmt, dass sich die Blockchain etwa jede 10 Minuten um einen Block verlängert (siehe Vorlesung). Dieser 10-Minuten-Takt wurde dabei als Kompromiss ausgewählt.
Geben Sie jeweils einen Vorteil für die Wahl eines kürzeren bzw. längeren Zeitabstandes als 10 Minuten an.

Lösung: Vorteile für kürzere Abstände:

- In der Regel kleinere Wartezeiten, bis eine Transaktion „sicher“ ist.
- Weniger Varianz bei der Auszahlung von Miners. (Kam in der Vorlesung nicht vor.)

Vorteile für längere Abstände:

- Benötigt viel mehr Kommunikation
- Da die neuere Version der Blockchain weniger Zeit hat, um alle Teilnehmer zu erreichen, wird es mehr „Aufspaltungen“ geben.

Aufgabe 3 (*10 Punkte*) Digitale und dezentrale Währungen sind eine relativ neue und revolutionäre Entwicklung. Dabei ist es noch weit offen wie diese sich entwickeln werden. Wie schätzen sie die Wahrscheinlichkeit ein, dass Bitcoin oder eine ähnliche digitale Währung zu einer etablierten Währung wird? Könnten Sie sich vorstellen in fünf oder in zehn Jahren im Supermarkt mit Bitcoins einkaufen zu gehen? Was wären Vor- und Nachteile davon? Diskutieren Sie auf circa einer halben Seite.

Bitcoins und Blockchains war spannend ☐ okay ☐ langweilig ☐
schwierig ☐ okay ☐ einfach ☐

Bitcoins und Blockchains war spannend ☐ okay ☐ langweilig ☐
schwierig ☐ okay ☐ einfach ☐