Aufgabe 5.1 a-e

Aufgabe 5.2

a b c

Aufgabe 5.3

1. Ändern des Nonce-Feldes
Beschreibung: Das Nonce-Feld ist ein 32-Bit-Feld, das Miner bei jedem Versuch ändern können. Es bietet 4.294.967.296 mögliche Werte.
Kosten: Gering. Das Ändern des Nonce-Feldes ist sehr billig, da es sich nur um eine einfache Zählung handelt.
2. Ändern des Zeitstempels
Beschreibung: Der Zeitstempel des Blocks kann innerhalb eines gewissen Bereichs angepasst werden. Miner können den Zeitstempel geringfügig erhöhen oder verringern, um unterschiedliche Hash-Werte zu erzeugen.
Kosten: Gering. Die Anpassung des Zeitstempels ist auch kostengünstig und wird häufig verwendet, wenn das Nonce-Feld ausgeschöpft ist.
3. Ändern der Coinbase-Transaktion
Beschreibung: Die Coinbase-Transaktion ist die erste Transaktion im Block und enthält eine einzigartige Coinbasestruktur, die vom Miner erstellt wird. Der Extra Nonce-Wert (ein zusätzlicher Nonce-Wert) und die Coinbasestruktur können geändert werden.
Kosten: Gering bis mittel. Es erfordert geringfügig mehr Aufwand als das Ändern des Nonce oder Zeitstempels, aber es ist immer noch eine sehr effiziente Methode.
4. Ändern der Reihenfolge der Transaktionen
Beschreibung: Miner können die Reihenfolge der Transaktionen innerhalb des Blocks ändern, um den resultierenden Hash zu verändern.
Kosten: Mittel. Das Ändern der Reihenfolge der Transaktionen erfordert mehr Rechenaufwand, da die Merkle-Root neu berechnet werden muss. Dies ist jedoch immer noch eine praktikable Methode.
5. Hinzufügen von Dummy-Transaktionen
Beschreibung: Miner können Dummy-Transaktionen (zusätzliche, aber gültige Transaktionen) hinzufügen, um den Hash des Blocks zu ändern.
Kosten: Mittel bis hoch. Das Hinzufügen von Transaktionen erhöht den Blocksize und den Rechenaufwand zur Erstellung und Validierung der Merkle-Root.
6. Ändern der Transaktionsstruktur
Beschreibung: Miner können die Struktur von bestehenden Transaktionen ändern, indem sie z.B. die Reihenfolge der Inputs und Outputs ändern, solange die Transaktionen gültig bleiben.
Kosten: Hoch. Dies erfordert umfangreichere Änderungen und ist komplizierter, da jede Änderung an einer Transaktion überprüft und neu validiert werden muss.

Aufgabe 5.4

Anreize für Mining:

Transaktionsgebühren: Zusätzlich zur Blockbelohnung erhalten Miner die Transaktionsgebühren, die Nutzer zahlen, um ihre Transaktionen priorisiert in einen Block aufnehmen zu lassen. Diese Gebühren sind besonders wichtig, wenn die Blockbelohnung durch das Halving sinkt und langfristig

zur Hauptquelle der Einnahmen für Miner werden.

Sicherung des Netzwerks und Wettbewerbsvorteil:

Netzwerksicherheit: Durch das Minen tragen Miner zur Sicherheit und Dezentralisierung des Bitcoin-Netzwerks bei. Ein hohes Maß an Rechenleistung (Hashrate) macht das Netzwerk resistenter gegen Angriffe wie 51 Prozent-Attacken.

Wettbewerbsvorteil: Miner konkurrieren weltweit darum, den nächsten Block zu finden und die damit verbundenen Belohnungen zu erhalten. Dies erfordert kontinuierliche Investitionen in leistungsfähige Hardware und effiziente Betriebsbedingungen, was den Wettbewerb innerhalb der Mining-Community antreibt und gleichzeitig die Sicherheit des Netzwerks erhöht.

Anreize für Full Nodes: Netzwerksicherheit und -integrität:

Überprüfung von Transaktionen und Blöcken: Full Nodes spielen eine entscheidende Rolle bei der Überprüfung und Validierung von Transaktionen und neuen Blöcken. Sie stellen sicher, dass nur gültige Transaktionen in die Blockchain aufgenommen werden, was die Integrität des gesamten Netzwerks schützt.

Schutz vor Manipulation: Full Nodes bewahren eine vollständige Kopie der Blockchain und können eigenständig die Korrektheit aller Transaktionen überprüfen. Dies schützt das Netzwerk vor Manipulationen und gewährleistet eine vertrauenswürdige und dezentrale Struktur.

Erhalt der Dezentralisierung und Unabhängigkeit:

Dezentralisierung des Netzwerks: Durch die Teilnahme als Full Node tragen Nutzer zur Dezentralisierung des Bitcoin-Netzwerks bei. Ein stark dezentralisiertes Netzwerk ist widerstandsfähiger gegen Zensur und zentralisierte Kontrollversuche.

Unabhängigkeit und Eigenverantwortung: Full Node-Betreiber sind nicht auf Drittanbieter angewiesen, um die Korrektheit der Blockchain-Daten zu überprüfen. Sie können Transaktionen direkt und unabhängig validieren, was ihnen mehr Kontrolle und Vertrauen in das Netzwerk gibt.

Aufgabe 5.5

1. Miner sind verantwortlich Transaktionen zu validieren und neue Blöcke zur Blockchain hinzuzufügen. Dies erfordert erhebliche Rechenleistung und damit verbundene Kosten.

Transaktionsgebühren bieten einen zusätzlichen finanziellen Anreiz für Miner, um weiterhin Transaktionen zu validieren, besonders wenn die Blockbelohnung im Laufe der Zeit abnimmt.

2. Ohne Transaktionsgebühren könnten böswillige Akteure das Netzwerk leicht mit einer großen Anzahl von unnötigen oder Spam-Transaktionen überschwemmen, was das Netzwerk verlangsamen und legitime Transaktionen behindern würde.

Transaktionsgebühren stellen sicher, dass jede Transaktion einen gewissen Wert hat und es für Angreifer kostspielig wird, das Netzwerk zu überlasten. Dies trägt dazu bei, die Integrität und Effizienz des Netzwerks zu schützen und sicherzustellen, dass Ressourcen für legitime Nutzer verfügbar bleiben.