universität innsbruck

### VU Prinzipien von Blockchain-Systemen

# Übungsaufgaben zur Klausurvorbereitung

Sommersemester 2020

16. Juni 2020

## 1 Verwaltung eines virtuellen Gutes

Betrachten Sie ein System mit Fungibilität mit 4 Teilnehmern ($A$, $B$, $C$, $D$) und einem virtuellen Gut, das sich in 7 Einheiten aufteilen lässt. Zustände sind so kodiert, dass zu jedem Teilnehmer die Anzahl der in seinem Besitz befindlichen Einheiten beschrieben wird. Dazu wird je Teilnehmer eine 3-Bit-Zahl verwendet, was dem Besitz von 0 bis 7 Einheiten entspricht.

Beachten Sie folgende Notationen: $A \xrightarrow{1} B$ bedeutet, dass $A$ eine Einheit an $B$ übergibt. Ein Zustand wird in Bits entsprechend der alphabetischen Reihenfolge der Teilnehmer kodiert: $(000, 110, 000, 001)$ würde bedeuten, dass A und C keine Einheiten besitzen, B sechs Einheiten besitzt und D eine Einheit besitzt.

a) Wie hoch ist die Anzahl der kodierbaren Zustände? Wie hoch ist die Anzahl der gültigen Zustände?

b) Welche Transaktionen in Abbildung 1a lassen sich paarweise vertauschen, sodass weiterhin alle Transaktionen gültig sind? Begründen Sie welche Transaktionen nicht vertauschbar sind.

c) Geben Sie für die Transaktion $B \xrightarrow{1} C$ und den Ausgangszustand $(000, 100, 011, 000)$ den Zielzustand an.

d) Geben Sie für die Transaktion $A \xrightarrow{1} B$ die Anzahl der gültigen Ausgangszustände an. Beschreiben Sie den Rechenweg.

e) Markieren Sie in Abbildung 1b den Zielzustand für die Transaktion ...

   i) $B \xrightarrow{1} C$ unter Annahme des Ausgangszustands $(000, 100, 011, 000)$.

   ii) $A \xrightarrow{1} B$ unter Annahme des Ausgangszustands $(001, 100, 011, 000)$.

   iii) $A \xrightarrow{1} B$ unter Annahme des Ausgangszustands $(000, 100, 011, 000)$.

f) Nehmen Sie nun unter den gleichen Bedingungen (7 Einheiten, 4 Teilnehmer) ein alternatives System ohne Fungibilität an. In einem solchen System kodieren wir einen Zustand, indem wir zu jeder Einheit des Gutes den Besitzer beschreiben. Wie viel Bit sind je Einheit des Gutes nötig, um den Besitzer eindeutig zu beschreiben?

g) Wie hoch ist die Anzahl der kodierbaren Zustände in dem alternativen System ohne Fungibilität? Wie hoch ist die Anzahl der gültigen Zustände in dem alternativen System ohne Fungibilität? Welchen Unterschied stellen Sie zu einem System mit Fungibilität fest? Was ist Ihre Schlussfolgerung daraus?

h) Sind die Menge der Ausgangszustände und die Menge der Zielzustände einer Transaktion immer disjunkt? Kommt es dabei auf die Fungibilität an? Begründen Sie.

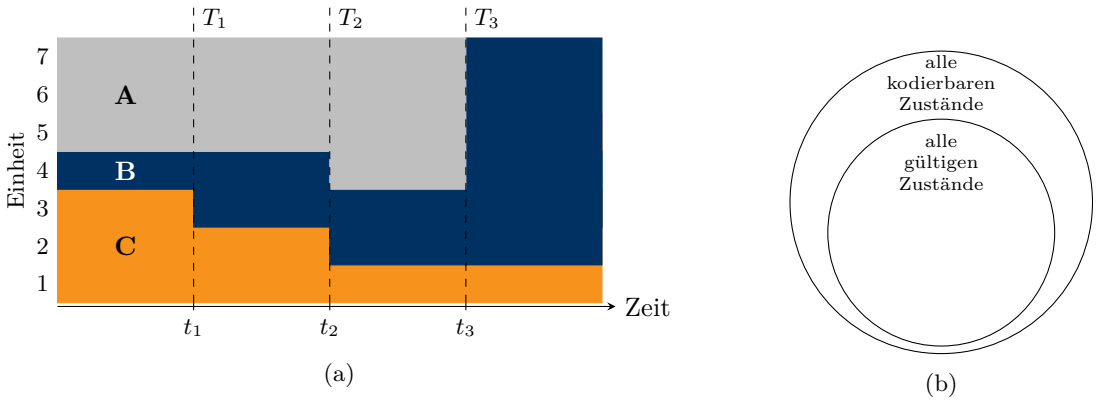


Abbildung 1: Transaktionen als Zustandsübergänge

## 2 Verständnisfragen zur Infrastruktur

a) Nennen Siei die zwei voneinander abzugrenzende Aufgaben, welche der Arbeitsnachweis bei typischen Blockchain-Systemen erfüllt.

b) Das „s“ bei *leadership selection* war bewusst grau gefärbt. Handelt es sich bei Bitcoin eher um eine Abstimmung (*election*), Auswahl (*selection*) oder kann das Verfahren durch einen ganz anderen Begriff treffender beschrieben werden? Begründen Sie Ihre Antwort.

c) Warum werden bei Bitcoin empirisch weniger ganz kurze Blockintervalle beobachtet als theoretisch vorhergesagt?

d) Welche Aspekte der besprochenen Infrastruktur könnten einfacher gestaltet bzw. komplett weggelassen werden, wenn Knoten feste Identitäten hätten?

## 3 P2P-Angriffe

Ein dezentrales System benötigt ein entsprechendes Overlay-Netz. Das macht es anfällig für bestimmte Angriffe. Informieren Sie sich ausgehend von der Einleitung des Papers von A. Singh, T. W. Ngan, P. Druschel und D. S. Wallach, „Eclipse attacks on overlay networks: Threats and defenses“, *Proceedings of the 25th IEEE International Conference on Computer Communications*, Barcelona, 2006, S. 1–12.

a) Was ist ein Sybil-Agriff? Erstellen Sie dazu eine Skizze und erklären Sie den Angriff anhand dieser.

b) Was ist ein Eclipse-Angriff? Erstellen Sie dazu eine Skizze und erklären Sie den Angriff daran.

c) Welcher der Angriffe ist kostengünstiger durchzuführen? Warum?

## 4 Double-Spending

In der vorherigen Aufgabe haben Sie sich mit P2P-Angriffen beschäftigt. Nun wollen wir deren Anwendung im Kontext dezentraler Währungssysteme genauer beleuchten.

a) Belesen Sie sich zu Double-Spending und erklären Sie das zugrundeliegende Konzept.
(Bedenken Sie, dass wir abweichend von vielen Autoren dieses Konzept bewusst nicht zur Motivation herangezogen haben.)

b) In der ersten Vorlesung wurden die drei Schritte der Verifikation von Transaktionen präsentiert:

- Prüfung der syntaktischen Korrektheit
- Prüfung, ob aktueller Systemzustand in $A$ enthalten ist
- Ermessensspielraum des (ersten) Prüfers

Ordnen Sie die Abwehr von Double-Spending einem der Schritte zu und begründen Sie (ggf. durch Ausschluss der Alternativen) Ihre Wahl.

c) Angenommen, Sie haben erfolgreich einen Eclipse-Angriff durchgeführt. Erklären Sie schrittweise, wie Sie darauf aufbauend einen Double-Spending-Angriff durchführen können.

d) Warum ist ein Double-Spending-Angriff trotz Eclipse-Angriff schwierig, wenn das Opfer mehrere Blöcke abwartet bevor es auf eine eingehende Zahlung reagiert?

# 5 Cluster-Heuristiken

Betrachten Sie die unten angegebenen Blöcke und die darin enthaltenen Transaktionen entsprechend der in der Vorlesung verwendeten Notation.

a) Bestimmen Sie zusammengehörende Entitäten nach der Multi-Input-Heuristik. Betrachten Sie dazu lediglich die Blöcke bis einschließlich Block 105.

b) Bestimmen Sie zusammengehörende Entitäten nach der Wechselgeld-Heuristik. Nehmen Sie an, dass die Wallet nie mehr Inputs verwendet als nötig und dass die Reihenfolge der Outputs randomisiert ist. Betrachten Sie dazu lediglich die Blöcke bis einschließlich Block 105.

c) Bestimmen Sie zusammengehörende Entitäten nach beiden Heuristiken. Betrachten Sie dazu lediglich die Blöcke bis einschließlich Block 105.

d) Betrachten Sie nun auch Block 106. Ändert sich etwas an Ihrer Zuordnung von Adressen zu den Entitäten? Warum (nicht)?

BLOCK 1
$T_1 = ((50), ((50, \boldsymbol{t}_\mathrm{A})), ())$

BLOCK 2
$T_2 = ((50), ((50, \boldsymbol{t}_\mathrm{B})), ())$

⋮

100 leere Blöcke (nur Coinbase-Transaktionen)

⋮

BLOCK 103
$T_3 = ((50), ((50, \boldsymbol{t}_\mathrm{A})), ())$
$T_4 = ((T_{1,1}), ((12, \boldsymbol{t}_\mathrm{C}), (12, \boldsymbol{t}_\mathrm{D}), (12, \boldsymbol{t}_\mathrm{E}), (12, \boldsymbol{t}_\mathrm{F}), (2, \boldsymbol{t}_\mathrm{G})), (\boldsymbol{s}_\mathrm{A}(T'_4)))$
$T_5 = ((T_{2,1}), ((12, \boldsymbol{t}_\mathrm{H}), (12, \boldsymbol{t}_\mathrm{I}), (12, \boldsymbol{t}_\mathrm{J}), (12, \boldsymbol{t}_\mathrm{K}), (2, \boldsymbol{t}_\mathrm{L})), (\boldsymbol{s}_\mathrm{B}(T'_5)))$

BLOCK 104
$T_6 = ((52), ((52, \boldsymbol{t}_\mathrm{A})), ())$
$T_7 = ((T_{4,2}, T_{5,2}), ((20, \boldsymbol{t}_\mathrm{M}), (3, \boldsymbol{t}_\mathrm{D})), (\boldsymbol{s}_\mathrm{D}(T'_7), \boldsymbol{s}_\mathrm{I}(T'_7)))$
$T_8 = ((T_{4,3}, T_{5,3}), ((20, \boldsymbol{t}_\mathrm{N}), (3, \boldsymbol{t}_\mathrm{O})), (\boldsymbol{s}_\mathrm{E}(T'_8), \boldsymbol{s}_\mathrm{J}(T'_8)))$
$T_9 = ((T_{4,4}, T_{4,5}), ((13, \boldsymbol{t}_\mathrm{P}), (1, \boldsymbol{t}_\mathrm{A})), (\boldsymbol{s}_\mathrm{F}(T'_9), \boldsymbol{s}_\mathrm{G}(T'_9)))$
$T_{10} = ((T_{5,4}, T_{5,5}), ((13, \boldsymbol{t}_\mathrm{R}), (1, \boldsymbol{t}_\mathrm{B})), (\boldsymbol{s}_\mathrm{K}(T'_{10}), \boldsymbol{s}_\mathrm{L}(T'_{10})))$

BLOCK 105
$T_{11} = ((50), ((50, \boldsymbol{t}_\mathrm{A})), ())$
$T_{12} = ((T_{7,2}), ((2, \boldsymbol{t}_\mathrm{R}), (1, \boldsymbol{t}_\mathrm{A})), (\boldsymbol{s}_\mathrm{D}(T'_{12})))$

nur für Aufgabenteil (d) relevant:

BLOCK 106
$T_{13} = ((51), ((51, \boldsymbol{t}_{\mathrm{A}})), ())$
$T_{14} = ((T_{4,1}, T_{7,1}, T_{8,1}, T_{8,2}, T_{9,2}, T_{10,2}), ((1, \boldsymbol{t}_{\mathrm{H}}), (2, \boldsymbol{t}_{\mathrm{P}}), (1, \boldsymbol{t}_{\mathrm{R}}), (12, \boldsymbol{t}_{\mathrm{Q}}), (12, \boldsymbol{t}_{\mathrm{S}}), (13, \boldsymbol{t}_{\mathrm{T}}), (15, \boldsymbol{t}_{\mathrm{X}})),$
$(\boldsymbol{s}_{\mathrm{C}}(T'_{14}), \boldsymbol{s}_{\mathrm{M}}(T'_{14}), \boldsymbol{s}_{\mathrm{N}}(T'_{14}), \boldsymbol{s}_{\mathrm{O}}(T'_{14}), \boldsymbol{s}_{\mathrm{A}}(T'_{14}), \boldsymbol{s}_{\mathrm{B}}(T'_{14})))$