Blockchain and Cryptocurrencies - Exercises

Riccardo Salvalaggio

June 24, 2021

Contents

1 Sheet 1 - Hash Functions **3**

1.1 Question 2: Collision 3

2 Sheet 3 **3**

3 Sheet 4 **3**

4 Sheet 5 **3**

5 Sheet 6 **3**

6 7 **4**

7 8 **4**

1 Sheet 1 - Hash Functions

1.1 Question 1: One-way function construction

Construct a function that is a one-way function if the factoring problem for natural number is difficult to solve.

1.2 Question 2: Collision

Let S_3 be the set of permutations on the set 1,2,3. For each $\pi \in S_3$ let e_π be the corresponding bit permutation on B_3 . For each $\pi \in S_3$, determine the number of collisions of the compression function $h_\pi(x) = e_\pi(x) \oplus x$ where $x \in B_3$.

$$S_3 : 123, 231, 312, 213, 132, 321$$

$$B_3 : 000, 001, 010, 011, 100, 101, 110, 111$$

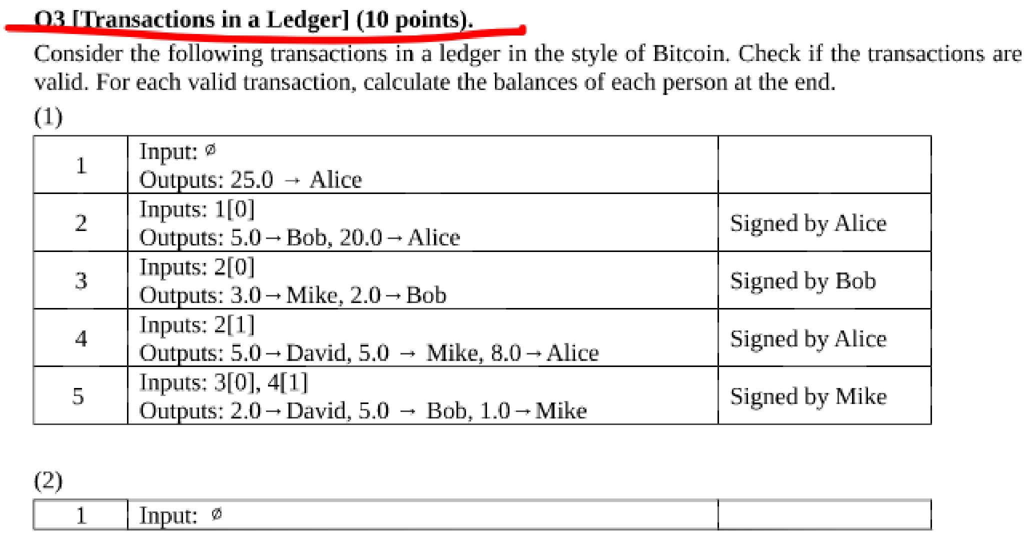
$$e_{123} =$$

2 Sheet 3

3 Sheet 4

4 Sheet 5

5 Sheet 6



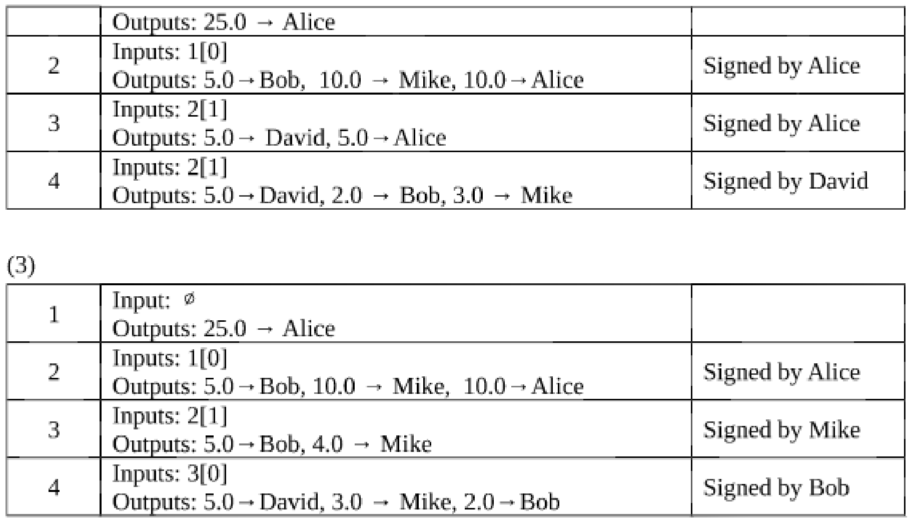
Q3 [Transactions in a Ledger] (10 points).

Consider the following transactions in a ledger in the style of Bitcoin. Check if the transactions are valid. For each valid transaction, calculate the balances of each person at the end.

(1)

1	Input: ∅ Outputs: 25.0 → Alice	
2	Inputs: 1[0] Outputs: 5.0 → Bob, 20.0 → Alice	Signed by Alice
3	Inputs: 2[0] Outputs: 3.0 → Mike, 2.0 → Bob	Signed by Bob
4	Inputs: 2[1] Outputs: 5.0 → David, 5.0 → Mike, 8.0 → Alice	Signed by Alice
5	Inputs: 3[0], 4[1] Outputs: 2.0 → David, 5.0 → Bob, 1.0 → Mike	Signed by Mike

(2)



1	Input: ∅ Outputs: 25.0 → Alice	
2	Inputs: 1[0] Outputs: 5.0 → Bob, 10.0 → Mike, 10.0 → Alice	Signed by Alice
3	Inputs: 2[1] Outputs: 5.0 → David, 5.0 → Alice	Signed by Alice
4	Inputs: 2[1] Outputs: 5.0 → David, 2.0 → Bob, 3.0 → Mike	Signed by David

(3)

1	Input: ∅ Outputs: 25.0 → Alice	
2	Inputs: 1[0] Outputs: 5.0 → Bob, 10.0 → Mike, 10.0 → Alice	Signed by Alice
3	Inputs: 2[1] Outputs: 5.0 → Bob, 4.0 → Mike	Signed by Mike
4	Inputs: 3[0] Outputs: 5.0 → David, 3.0 → Mike, 2.0 → Bob	Signed by Bob

1)

1. Ok 2. Ok 3. Ok mm 4. Ok 2 lost 5. Ok
Alice: 10 Bob: 7 David: 7 Mike: 1

2)

1. ok 2. ok 3. ok 4. mmm
Alice: 5 Bob: 7 David: 0 Mike: 3

3)

1. ok 2. ok 3. ok lost 1 4. ok
Alice: 10 Bob: 2 David: 5 Mike: 8

6 7

7 8