Learning to simulate a blockchain to understand its processes from a top level view

Introduction

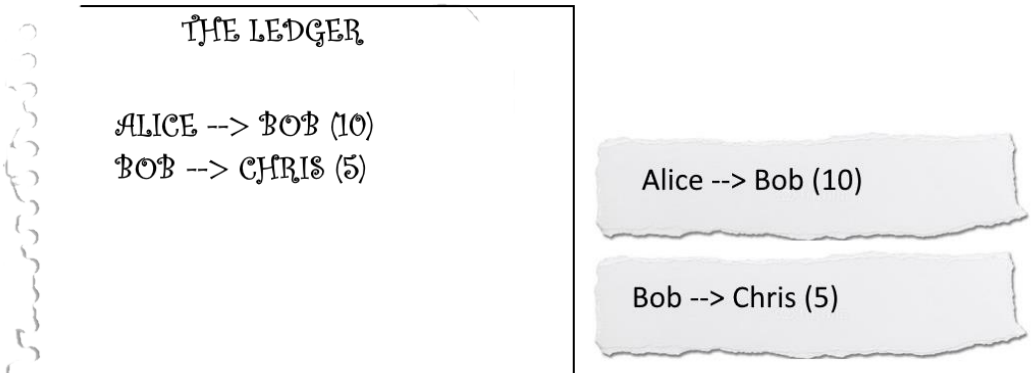
We have earlier learned that the double spending problem can be resolved by using a decentralized ledger. Here we will explore the issues related to it, and examine suggestions to resolve issues with it.

Assessment: Submit a report as a group with answers to the questions raised here.

1. Centralized Trust

Time: 10 mins
Players: users and 1 central authority
Each user starts with $10 and is listed on the ledger

Central authority maintains a new ledger of all transactions



Flow:

1. Users write on a slip of paper a transaction: A->B (Amt)
2. Transactions are sent to the central authority one at a time, with no rush.
3. The authority writes them to the ledger and verifies them.

Questions:

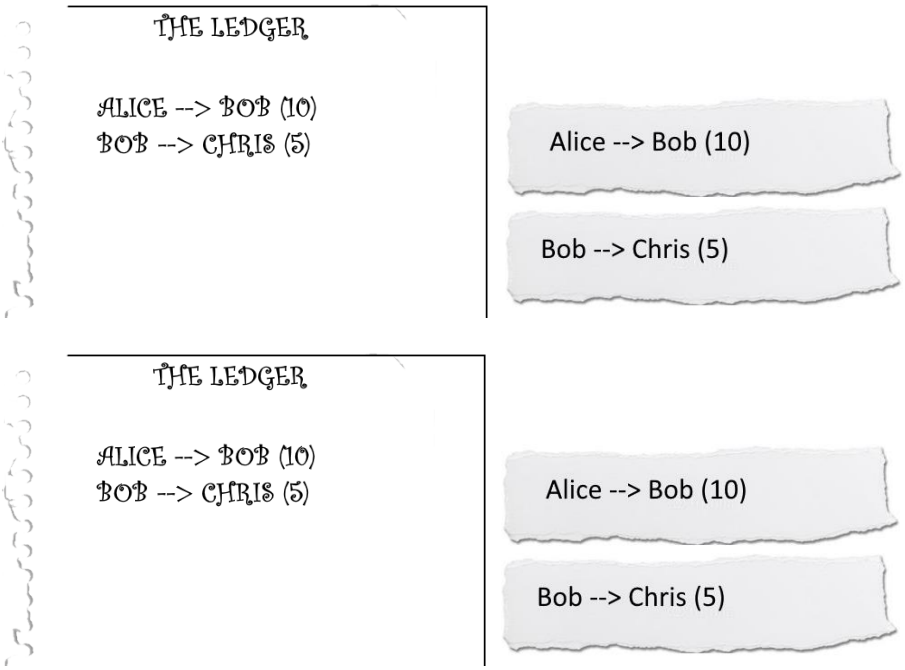
1. Are there any issues with a central authority?
2. Where is the opportunity to commit fraud (cheat)? List all of them down.

2. Multiple P2P Centralized Trust

Time: 20 mins

Players: users and N central authority
Each user starts with $10 and is listed on the ledger

Central authority maintains a new ledger of all transactions and there are multiple authorities.



Flow:

1. Users write on a slip of paper a transaction: A->B (Amt). Do 5 or 6 transactions.
2. Transactions are sent to all authorities one at time (no rush).
3. Each authority writes the transactions to their ledger in the order received and at the same time verify them.

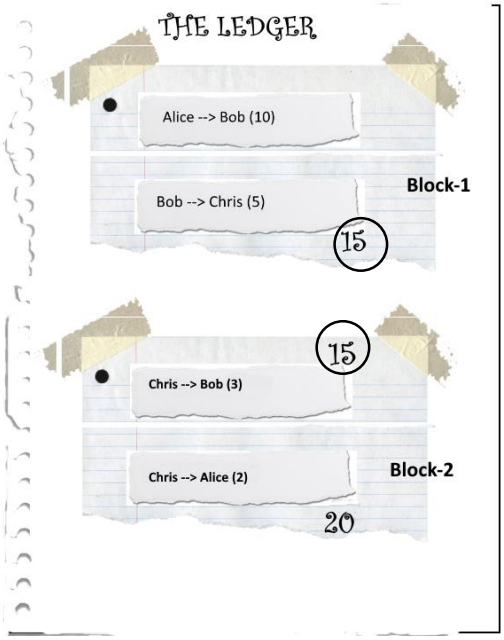
Questions:

1. Is this better than having a single authority?
2. Are there any issues with multiple central authorities?
3. How do we synchronize the ledger?
4. Where is the opportunity to commit fraud (cheat)? List all of them down.

3. Centralized Trust with Immutable Ledger

Time: 30 minutes.
Players: users and 1 central authority
Each user starts with $10 and is listed on the ledger

Central authority maintains a new ledger of all transactions and the ledger is immutable



Immutability is simulated the taping (or staple) of the block to the ledger. The running totals (eg. 15) creates a link between all blocks. Removing or altering one of the blocks would require changing the running total. We assume that the altering of the running total on the blocks would be noticeable.

Flow:

1. Users write on a slip of paper a transaction: A->B (Amt)
2. Transactions are sent to the central authority one at a time.
3. The authority group 2-3 transactions into a bundle (block). The transaction sum is noted down.
4. The transaction bundle is stapled or taped together (see image).
5. Central authority verifies them and insert in the blockchain.

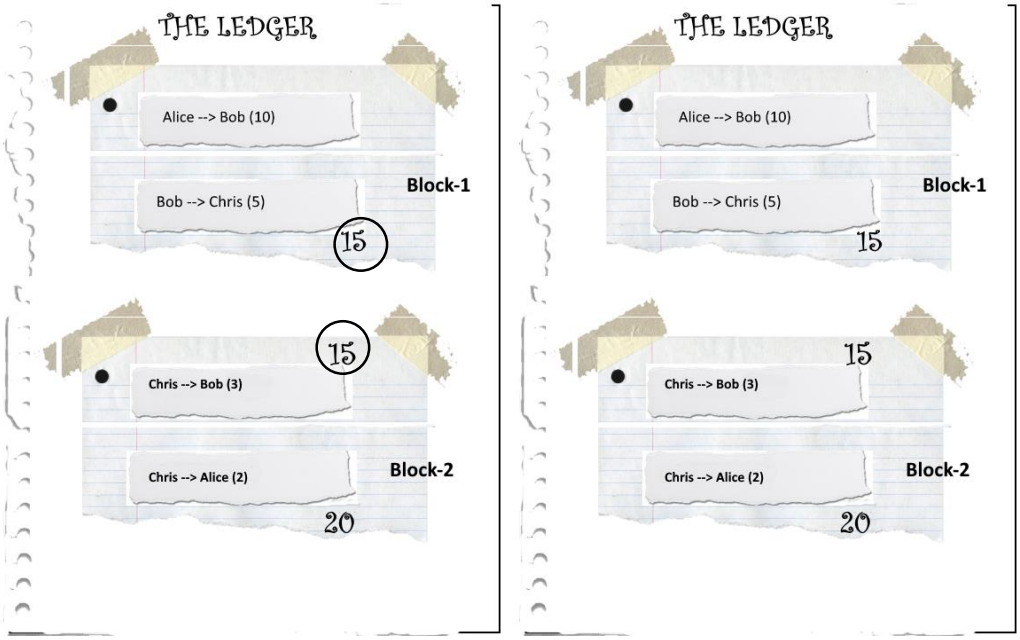
Questions:

1. Are there any issues with such a scheme? List as many as possible
2. Where is the opportunity to commit fraud (cheat)? List all of them down

4. Multiple Centralized Trust with Immutable Ledger with Blocks

Time: 30 minutes.
Players: users and N central authority
Each user starts with $10 and is listed on the ledger

Central authority maintains a new ledged of all transactions and is immutable



Immutability is simulated the taping (or staple) of the block to the ledger. The running totals (eg. 15) creates a link between all blocks. Removing or altering one of the blocks would require changing the running total. We assume that the altering of the running total on the blocks would be noticeable.

Flow:

1. Users write on a slip of paper a transaction: A->B (Amt)
2. Transactions are sent to all central authorities one at a time
3. The authority group 2-3 transactions into a bundle (block) according the order received. The transaction sum is noted down.
4. The transaction bundle is stapled or taped together (see image).
5. The authority verifies them and insert in the blockchain.

Question:

1. Are there any issues with such a scheme? List them down.
2. Where is the opportunity to commit fraud (cheat)? List all of them down

5. Multiple Decentralized Trust with Immutable Ledger

Time: 30 minutes.
Players: users and N decentralized authority
Decentralized authority maintains a new ledger of all transactions and the ledger is immutable.
Each user starts with $10 and is listed on the ledger

Example of a puzzle to solve: How many animals can you see?

Flow:

1. Users write on a slip of paper a transaction: A->B (Amt)
2. Transactions are sent to all authorities one at time.
3. While transactions are ongoing, each authority will attempt to solve a puzzle independently
4. If the puzzle is solved, he will raise his hands and every authority checks his answer.
5. The first authority who solved the puzzle will group 2-3 transactions into a bundle (block), verify it as before. The transaction bundle (block) is stapled or taped together (as usual). This block is copied by all other authorities.

Questions:

1. Does this approach solve the previous scheme's issues? What are those issues and how are they solved?
2. What are other issues with the approach?
3. What is the function of the puzzle solving? [This is an important question]
4. Can this be called trustless? Why or why not?
5. Does this solve the double spending problem?
6. What are the opportunities to commit fraud with this method? Or how to subvert this scheme.