COMP 189: Homework 9

Assigned April 1, 2022
Due midnight April 8, 2022
45 points total

Technical Exercises

For each problem, show all your work (required for credit). For answers requiring written answers, while no more than five or six sentences are expected, sufficient justification must be given for any position, opinion, or perspective taken.

1. The Blockchain (20 pts)

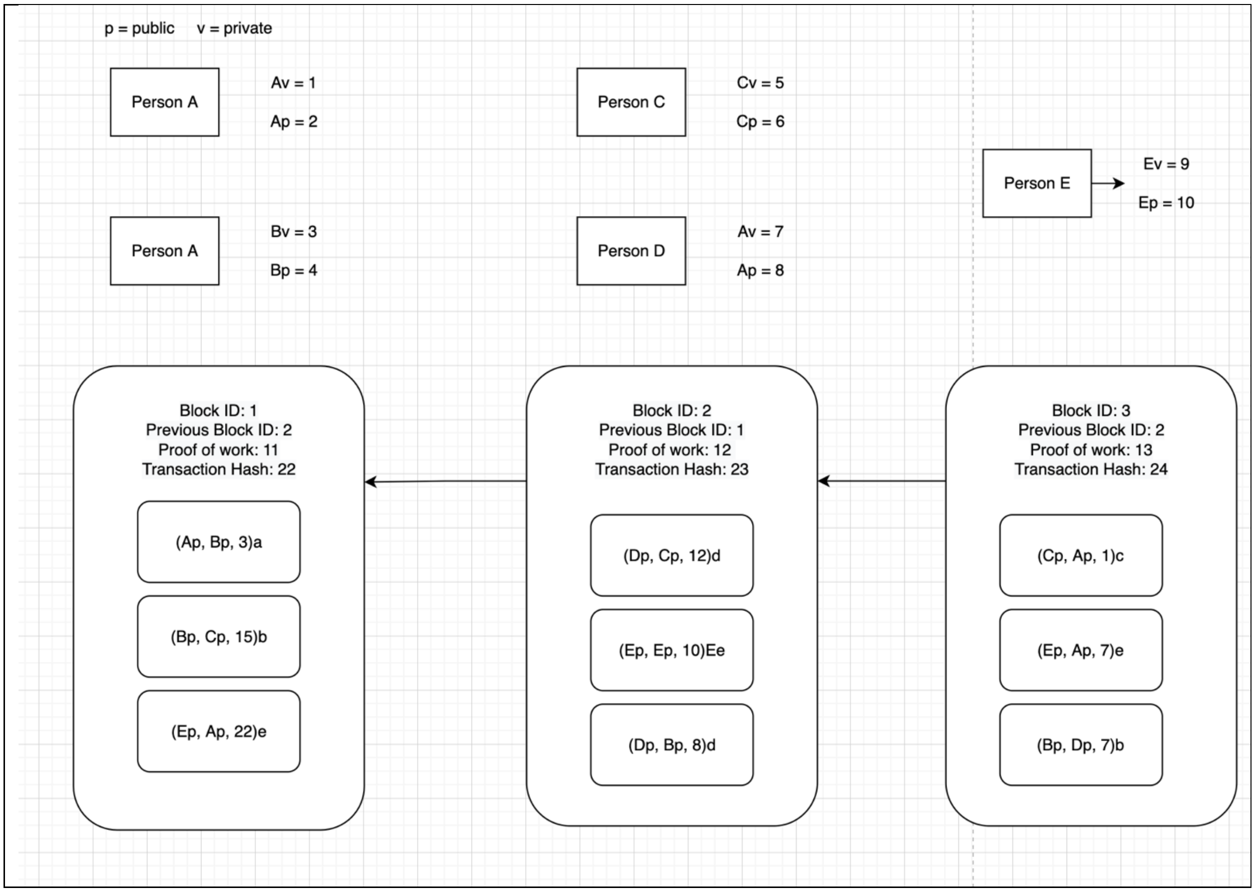
Diagram a blockchain consisting of three blocks, each containing 3 transactions. Represent the transactions, showing their contents and structure. The transactions will involve 5 entities: A, B, C, D, E. Each entity has their own keypair (e.g., <Ap,Av>). For the purpose of this problem, you can just invent any hash values you need – with each hash value being a number between 1 and 100.

Each block should include the following information:

- Block ID (a hash "generated" from all the data below)
- Previous Block ID
- Proof of work
- Transaction hash ("generated" from the transactions)
- Transactions

Populate your blockchain with the following transactions (listed in order from oldest to most recent):

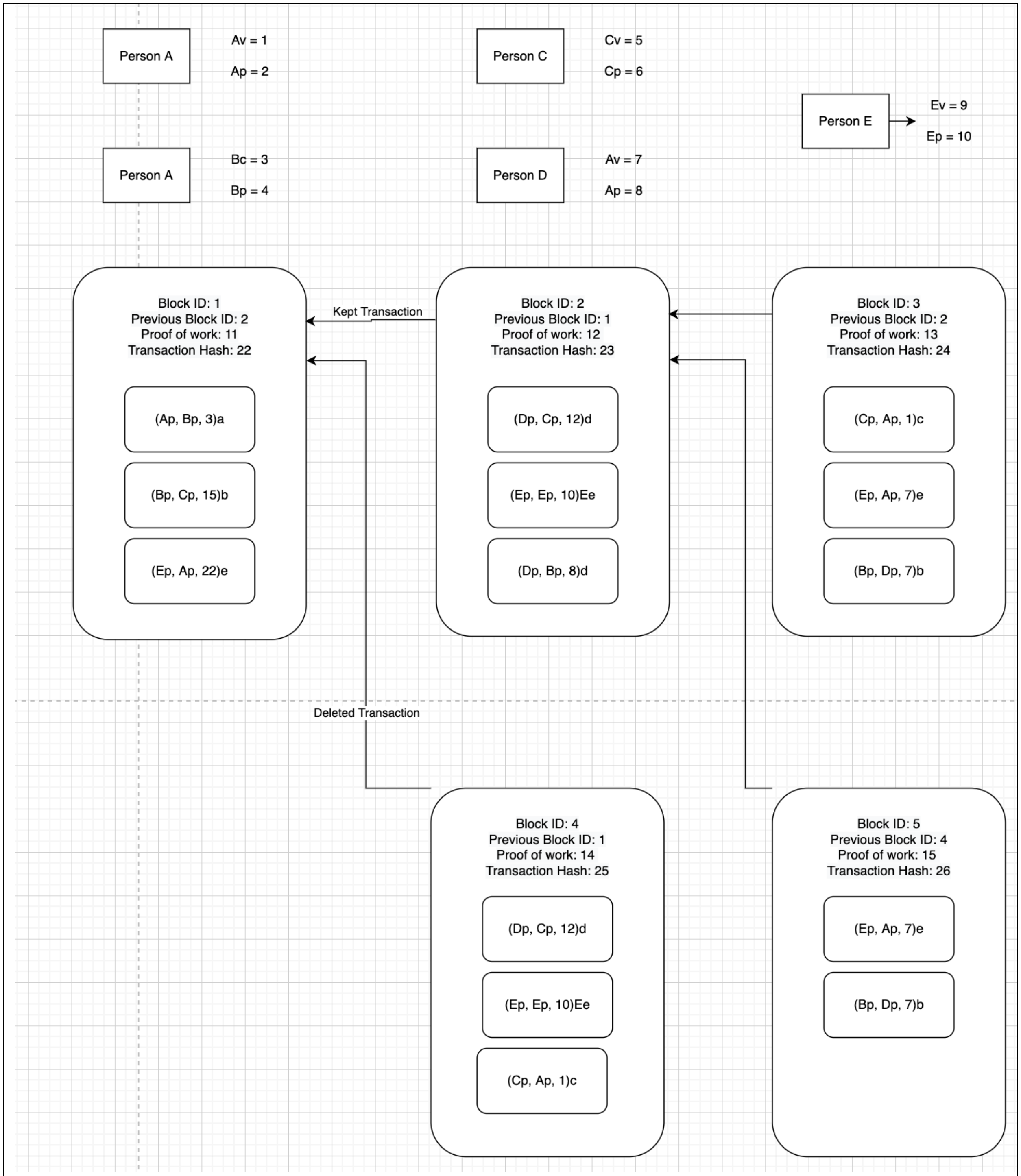
1. A gives $3 to B
2. B gives $15 to C
3. E gives $22 to A
4. D gives $12 to C
5. E gives $10 to E (this is not a typo)
6. D gives $8 to B
7. C gives $1 to A
8. E gives $7 to A
9. B gives $7 to D



2. Proof of Stake (10 pts)

You want to remove transaction 6 from the system. Diagram the alternative blockchain that is created as a result (using the conventions above)

Why is it unlikely that you will be able to pull this attack off and rewrite the blockchain?



It is unlikely for this attack to be pulled because it takes a lot of computing power to solve these hard math puzzles to rewrite the blockchain. Take the scenario written above where we remove transaction 6 and rewrite block with block ID 2 to the block with block ID 4; then creating a new block with block ID 5 and calculating all the hashes must be done faster than the previous blockchain since it's still calculating the next blocks.

In other words, the user trying to pull the attack off must have more computation power than the system or else it won't be able to rewrite the block.

3. Proof-of-Stake (15 pts)

Answer each question below in four sentences or less.

1. Explain the difference between proof-of-work and proof-of-stake.

Proof-of-work and proof-of-stake are both the main components when verifying a cryptocurrency transaction. Proof-of-stake needs participants to add cryptocurrency as security (in other words stake their cryptocurrency) so they can have the opportunity to do transactions. The investor with the most amount of invested crypto for the longest amount of time is rewarded. Proof-of-work, on the other hand, is a more secure way of doing cryptocurrency transactions since it avoids forgery. It requires the investor to solve a math puzzle to update the blockchain with their transaction. Proof-of-work was the first verification system and takes much more energy since it requires more computing power to enable people to do transaction and is being replaced with the newer proof-of-stake which does not require as much energy.

2. Why are proof-of-stake blockchain systems less wasteful than those that use proof-of-work?

Proof-of-work as briefly mentioned above requires a lot of computing power which utilizes energy to do so. The reason it needs computing power is because block chains that use proof-of-work are secured and verified by virtual miners and people are competing to solve a math puzzle to do their transaction as fast as possible. Proof-of-stake bypasses this computing requirement by allowing investors to put their investments as stake instead for a chance to validate their transaction. Doing so removes the need for massive amounts of electricity and resource computation.

3. How does proof-of-stake create a risk of centralization of block validation?

The idea behind proof-of-stake is that it replaces the more secure proof-of-work which uses a lot of “work” (computing power) with “stakers”, people who stake their investments for a chance to do their transaction. The proof-of-stake system favors people with higher amounts of tokens, more than those with less amounts like mentioned above. People who can stake more end up with larger profit margins and can use their coins to increase the production ability allowing them to grow faster.

Now, block chains using proof-of-stake risk being more centralized because the amount of validators participating in mining new blocks is very small. This allows only a select few to manipulate and collaborate on the network which makes it unreliable and defeats the purpose of decentralization.