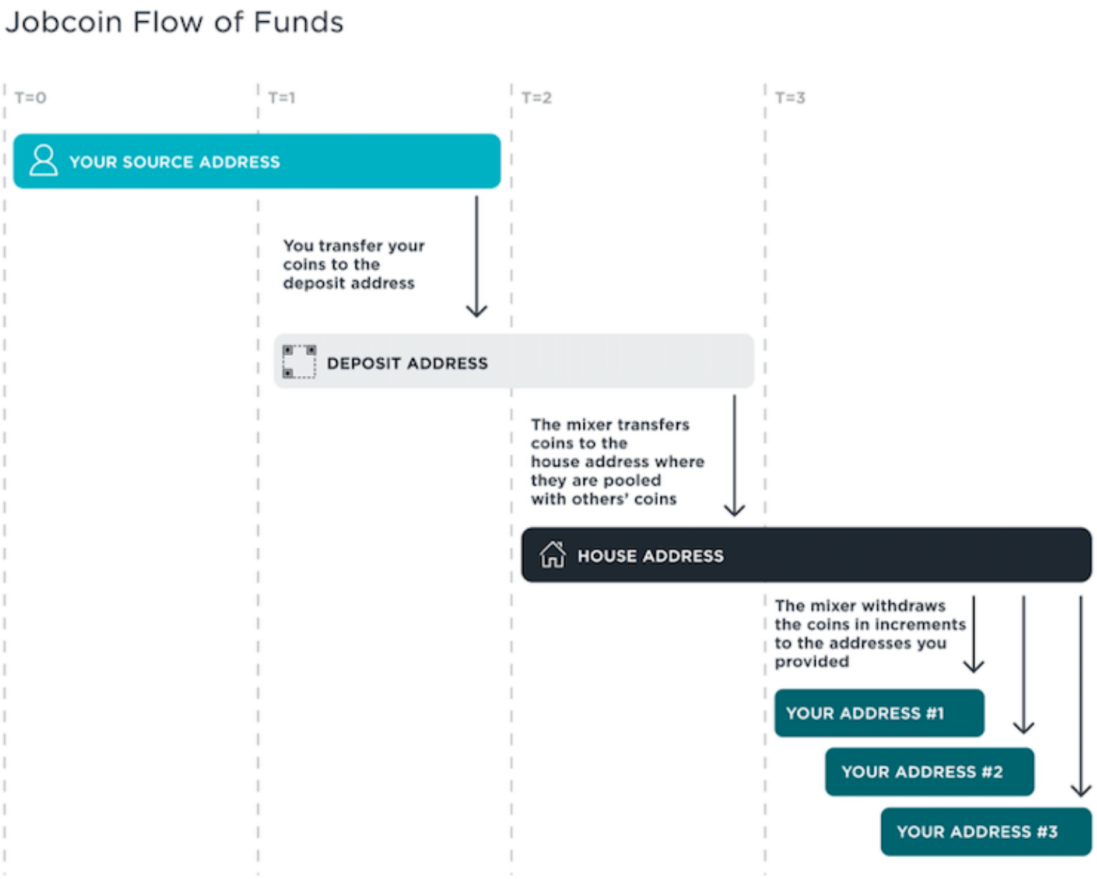
Coin Mixer Challenge

Despite some media reports, Bitcoin is not an anonymous protocol. Instead, it's often referred to as a pseudonymous system. All transactions to or from any Bitcoin address are publicly available, so Bitcoin's “anonymity” hinges on not knowing which addresses belong to which people. For instance, if your salary gets paid to the same Bitcoin address every two weeks, and if you buy your morning coffee using that address, it would be fairly easy for your barista to look up your previous transactions and figure out how much money you make.

Making new Bitcoin addresses is trivial, however, using a set of addresses rather than a single address does not solve the problem by itself. If an analysis of the transaction flow indicates that a set of addresses is controlled by a single entity, then that is no better than a single address. Using what is known as a ‘mixer’ would be one of the many ways to introduce obfuscation into transaction flow and maintain your privacy on the Bitcoin network.
The diagram below illustrates a user’s interaction with a simple ‘mixer’:



And a written explanation of the diagram:

User Flow for Simple Mixer

1. You provide a list of new, unused ‘withdrawal’ addresses that you own to the mixer;

2. The mixer provides you with a new ‘deposit’ address that it owns;

3. You transfer your bitcoins to that ‘deposit’ address;

4. The mixer will detect your transfer by watching or polling the P2P Bitcoin network;
5. The mixer will transfer your bitcoin from the deposit address into a big “house account” along with all the other bitcoin currently being mixed; and

6. Then, over some time the mixer will use the house account to dole out your bitcoin in smaller discrete increments to the ‘withdrawal’ addresses that you provided, possibly after deducting a fee.

Bitcoin can be a difficult protocol to work with, especially for a newcomer to cryptocurrencies, so this challenge is to design a mixer for a much simpler virtual currency, *Jobcoin*.

1. In Jobcoin an “address” is just an arbitrary string (no public key cryptography)

2. There’s no mining, no blocks, and no transaction signing (no digital signature

   cryptography).

3. Anyone can create units of Jobcoin out of thin air on the Jobcoin website.

4. Transfers between addresses can be accomplished using the website or the API.

Instructions

Please design a Jobcoin mixer, analogous to the Bitcoin mixer described above. You may collect a fee for your mixing service if you wish.

We are primarily looking for you to demonstrate an understanding of the problem above and decompose it into a well structured solution. There is no right answer, and where the prompt is underspecified or ambiguous, you’re welcome to make your own decisions. We understand that you have time constraints; feel free to time box yourself, and note where you bounded your work.

During your interview, you will be asked to present: (a) how you would complete this project, if tasked with it (b) how you would, in the role of a technical leader, assist your team in architecting a solution.

Your presentation of your solution can be entirely verbal, although it may assist you and the interviewer to have some supporting materials, such as diagrams, notes, or even code. Your interviewer will want to understand your interpretation of the specification, how you decompose the problem, as well as the gist of the algorithmic parts within the specification. You should also consider aspects such as testing, a QA plan, unit testing, and or integration testing and be prepared to speak to those.