

Programming Project #3

Due: 11:59pm on **Mon., Nov. 26, 2018**

Submit via Gradescope (each answer on a separate page) code: **9RZGVZ**

In this assignment, you'll use Solidity and web3.js to implement a complex decentralized application, or DApp, on Ethereum. You will write both a smart contract and the user client that accesses it, learning about 'full-stack' development of a DApp. To save you time, please read the whole assignment - especially the notes section - before you start development.

1 Blockchain Splitwise

We want to create a decentralized system to track debit and credit - a blockchain version of Splitwise. If you haven't heard of the app, it's a simple way to keep track of who owes who money within a group of people (maybe after splitting lunch, groceries, or bills). To illustrate the application, consider the following scenario:

Alice, Bob and Carol are all friends who like to go out to eat together. Bob paid for lunch last time he and Alice went out to eat, so Alice owes Bob \$10. Similarly, Carol paid when she and Bob went out to eat, and so Bob owes Carol \$10.

Now, imagine Carol runs short on cash, and borrows \$10 from Alice. Notice that at this point, instead of each person paying back their 'loan' at some point, they could just all agree that nobody owes anyone. In other words, whenever there is a cycle of debt, we can just remove it from our bookkeeping, making everything simpler and reducing the number of times cash needs to change hands.

We will build a decentralized way to track who owes what to who, so that no trusted third party has to be relied upon. It will be efficient: it won't cost an exorbitant amount of gas to store this data. No value will get transferred 'on the blockchain' using this app; the only ether involved will be for gas.

Because it's on the blockchain, when Carol picks up the check for her and Bob's meal, she can ask Bob to submit an IOU (which he can do using our DApp), and she can verify that he indeed has. The public on-chain storage will server as a single source of truth for who owes who. Later, when the cycle illustrated above gets resolved, Carol will see that Bob no longer owes her money.

As part of this, we will also build a user interface that computes useful information for the user and allows non-programmers to use the DApp.

2 Getting Started

1. Install the prerequisite software: you'll need to download and install Node.js from <https://nodejs.org/en/>. Choose the LTS version (the one on the left).
2. Run `npm install -g ganache-cli` to install the Ganache CLI, which we will use to simulate a real Ethereum node on our local machines. Then, run `ganache-cli` to run the node. You

can stop the node at anytime with Ctrl-C.

3. Download and extract the starter code from the course website.
4. Open <https://remix.ethereum.org> in your web browser. In the ‘Run’ tab, set the environment to ‘Web3 Provider’, click ‘Ok’ when prompted, and then set the ‘Web3 Provider Endpoint’ to <http://localhost:8545> - this should be the default. This is where you will develop your smart contract (which you will write in Solidity).
5. Open the `index.html` file in your web browser (you should see a page titled ‘Blockchain Splitwise’). It’s very helpful to also open your browser’s JavaScript console, so that you can see error messages (there’s a link on how to do this at the end of this document). If everything so far is working, you should see no errors in the console (you will probably see a warning; this is fine, see the the notes at the end for more details).
6. Open the starter code directory in your favorite IDE or text editor (something like Sublime Text, Atom, or Visual Studio Code works nicely). You’ll be modifying `script.js` to build the client, but looking at the other files may help. There are places marked with functions to modify - please do not modify any of the other code. Feel free to add helper functions.
7. Peruse the starter code, the web3.js API, and the Solidity documentation. Think carefully about the overall design of your system before you write code. What data should be stored on chain? What computation will be done by the contract vs. on the client?
8. Implement code for the requirements outlined below. When you have your contract, deploy it, and then **update the contract hash and ABI** in `script.js`. The ABI can be copied to the clipboard from the ‘Compile’ tab, and the contract hash can be copied from the ‘Deployed Contracts’ panel in the ‘Run’ tab. Note that the contract hash is *not* the transaction hash of the transaction that created the contract.

Note on OSs: All of the above steps should work on Unix-based systems and Windows. The commands we ask you to execute will work in a standard Unix terminal and the Windows Command Prompt.

3 Requirements

The project has two major components: a smart contract, written in Solidity and running on the blockchain, and a client running locally in a web browser, that observes the blockchain using web3.js and can call functions in the smart contract. For more information on how web3.js works, watch the section video from November 2nd.

3.1 Functions in the client

1. `getUsers()`: Returns a list of addresses. You can have this return either: ‘everyone who has ever sent or received an IOU’ OR ‘everyone currently owing or being owed money’. You may find this useful as a helper for other functions.
2. `getTotalOwed(user)`: Returns the total amount that the given `user` owes.

3. `getLastActive(user)`: Returns a UNIX timestamp (seconds since Jan 1, 1970) of the last recorded activity of this user (either sending an IOU or being listed as 'creditor' on an IOU). Returns `null` if no activity can be found.
4. `send_IOU(creditor, amount)`: Submits an IOU to the contract, with the passed `creditor` and `amount`. Doesn't return anything. **See note about resolving loops below.**

3.2 Functions in the contract

1. `lookup(address debtor, address creditor) public view returns (uint32 ret)`: Returns the amount that the `debtor` owes the `creditor`.
2. `add_IOU(address creditor, uint32 amount, ...)`: Informs the contract that `msg.sender` now owes `amount` more dollars to `creditor`. It is additive: if you already owed money, this will add to that. The amount **must** be positive. You can make this function take any number of additional arguments. **See note about resolving loops below.**

You are welcome to write more helpers for either the client or contract. The client can call contract functions with `BlockchainSplitwise.functionname(arguments)`. Remember that the client functions will be written in JavaScript, and the contract functions will be written in Solidity.

4 Resolving Loops of Debt

It's helpful to think of the IOUs as a graph of debt. That is, say that each user is a node, and each weighted directed edge from A to B with weight X represents the fact 'A owes \$X to B'. We will write this as $A \xrightarrow{X} B$. We want our app to 'resolve' any cycles in this graph by subtracting the minimum of all the weights in the cycle from every step in the cycle (thereby making at least one step in the cycle have weight '0').

For example, if $A \xrightarrow{15} B$ and $B \xrightarrow{11} C$, when C goes to add $C \xrightarrow{16} A$, the actual balances will be updated to reflect that $A \xrightarrow{4} B$, $B \xrightarrow{0} C$, and $A \xrightarrow{5} B$.



Similarly, if C goes to add $C \xrightarrow{9} A$, the actual balances will be updated to reflect that $A \xrightarrow{6} B$, $B \xrightarrow{2} C$, and $C \xrightarrow{0} A$.



The requirement is that if any potential cycles are formed when you are about to add an IOU using the client (`send_iou`), you must ‘resolve’ at least one of them. You **do not** need to worry about complex cases involving multiple loops, or optimizing which path to take (something like max flow) in those cases. You can assume that as a precondition to both contract functions (`add_iou` and `lookup`), there are no cycles in the graph. Finally, you can also assume that any cycle found will be somewhat small (say, less than 10).

We provide you with a breadth-first search algorithm in the code - to use it, pass in a start and end node, and a function to get the ‘neighbors’ of any given node. You are free to not use this implementation as well.

It’s up to you to implement this resolution securely. It should not be possible for a malicious client to somehow ‘wipe away’ their debt once it is posted.

We can now illustrate exactly how you can pay back an IOU in this system. Say Alice borrowed \$10 from Bob; now, she wants to pay Bob back in cash. When Alice gives Bob \$10 in cash, Bob will add an IOU for \$10 with the creditor as Alice. This will create a cycle: specifically, $A \xrightarrow{10} B$ and $B \xrightarrow{10} A$. By the cycle resolution requirements above, this will end with $A \xrightarrow{0} B$ and $B \xrightarrow{0} A$.

5 Overall Requirements

You are welcome to write your contract in any way you like, as long as it has the specified `lookup` and `add_IOU` functions. Your goal is to write a contract that minimize the amount of storage and computation used by both contract functions. This will minimize gas costs.

You can assume that the transaction volume is small enough that it’s feasible to search the whole blockchain on the client, but you should not assume that the only users are the ones in your wallet - in other words, `web3.eth.accounts` does not contain every possible user of the system.

6 Submitting your code

We will be using Gradescope for submission. Your submission will be graded on whether it correctly answers queries and whether it incurs a reasonable amount of gas. **Before submitting, please make sure to copy and paste your contract’s Solidity code from Remix into `mycontract.sol`.**

7 Notes

We will be posting an up-to-date listing of all clarifications and advice on Piazza. Please follow that post to get the latest information as we work any issues with the assignment.

7.1 System Architecture

- You should decide on what data structure(s) will be stored on the blockchain first. Think carefully about what information you need to provide to the client. You don't need to use any particularly fancy data structures. Your decision may make the implementation more difficult, so you should be okay with going back and changing your architecture.
- We have not mentioned what to do in the case of a cycle formed between just two people. We recommend designing your system so that this is not a special case - when the debtor has 'paid back' the creditor, the creditor simply attempts to add an IOU in the opposite direction, triggering cycle resolution and ending with both owing 0 to each other. We also recommend that you avoid any concept of 'negative' debt, as this can overcomplicate things.
- Remember when optimizing for gas cost that functions run on the client are free - they incur no cost.
- We suggest that after designing your system, you start by writing and thoroughly debugging the contract in Remix. You can call functions in the lower right panel, and switch accounts using the 'Account' selector in the top right. To copy the addresses to your clipboard, you can click the copy icon next to the selector. Once you're certain the contract works as intended, then you should start writing the client.
- You don't need a massive amount of code to complete the assignment. Our solution is about 40 lines of Solidity and about 70 new lines of JavaScript (not including the ABI).

7.2 Practical Development & Debugging

- Since JavaScript handles integers in a strange way, your calls to `BlockchainSplitwise.lookup` will return a JavaScript object; specifically, a `BigNumber` with `c`, `e`, and `s` properties. To convert this to a normal integer, call `bn.toNumber()` where `bn` is the returned `BigNumber`. You will probably want to do this with every call you make to `BlockchainSplitwise.lookup` on the client.
- To debug client-side code, make liberal use of `console.log`. You should see the results of the calls and the line number they originated from in your browser's JavaScript console.
- Warnings about synchronous `XMLHttpRequest` are fine to ignore. Errors about not connecting to `localhost:8545` are usually because you don't have `ganache-cli` running.
- Solidity has a very useful function `require` that will allow you to check preconditions
- If you want to just debug your contract, you can use the 'JavaScript VM' Web3 Provider and then press 'Debug' on the transaction that is failing. Make sure to switch back after so that you can run the client side code.

8 References

- You can read about how to open the JavaScript console of your browser *here*.
- The API for `web3.js` is *here*.