

Open Freelance hub

Technical Manual

Dean Lynch & David Weir

Table of Contents

- 1. Introduction
 - 1.1 Overview
 - 1.2 Glossary
 - 1.3 Initial Design Vs Final Application
- 2. System Architecture
- 3. High Level Design
 - 3.1 Architectural Overview Diagram
 - 3.2 Component Diagram
 - 3.3 Data Flow Diagram
 - 3.4 State Diagram
- 4. Problems and Resolutions
- 5. Installation Guide
- 6. Future Work

1. Introduction

1.1 Overview

The goal of Open Freelance Hub is to create a more open and transparent marketplace for freelance or casual work transactions. This application allows users to trade Ether, a cryptocurrency, for some amount of work completed. For example, a proofreader could be paid by a student for completing an analysis of their dissertation. With the growing popularity of blockchain based technologies, this application is a showcase of how blockchain "decentralised applications" can be used in place of commonly used applications.

1.2 Glossary

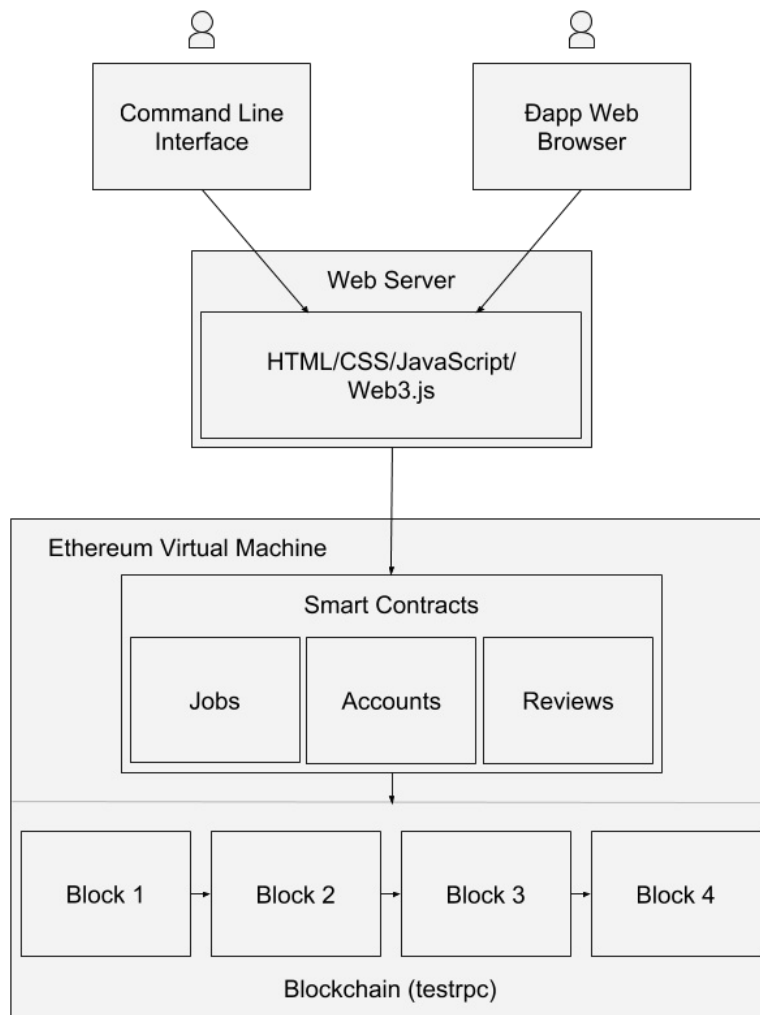
- **Blockchain:** A distributed digital public ledger that records transactions across multiple computers to prevent transaction history from being altered.
- **Smart Contracts:** Self-executing programmable contracts that allow for the transfer of currencies on the blockchain, and the updating of the public ledger.
- **Ethereum:** An open platform that allows for the development of decentralised applications.
- **Ether:** The common cryptocurrency used in the Ethereum environment.
- **Dapp:** An app consisting of a user interface and a decentralised backend built on the the Ethereum blockchain.
- **Gas Price:** The price paid to process a contract or transaction onto the Ethereum blockchain.
- **Solidity:** The language used to program smart contracts for the Ethereum blockchain.
- **web3.js:** A JavaScript API compatible with the Ethereum blockchain.
- **MetaMask:** A browser plugin for Chrome and Firefox which allows you to browse Dapps without running a full Ethereum Node.

1.3 Initial Design Vs. Final Application

The application that was developed achieves the minimum viable product that was outlined as part of the functional specification. Registered users have the ability to post jobs, browse both all jobs and all open jobs, apply to relevant jobs as a worker, and search for jobs based on job title and description.

Time was spent in an attempt to develop a chat functionality using the Whisper protocol, in hindsight this time was wasted as we discovered that the Whisper protocol is still heavily in development and severely lacking documentation, and therefore it would not be possible to integrate a chat functionality in time.

2. System Architecture



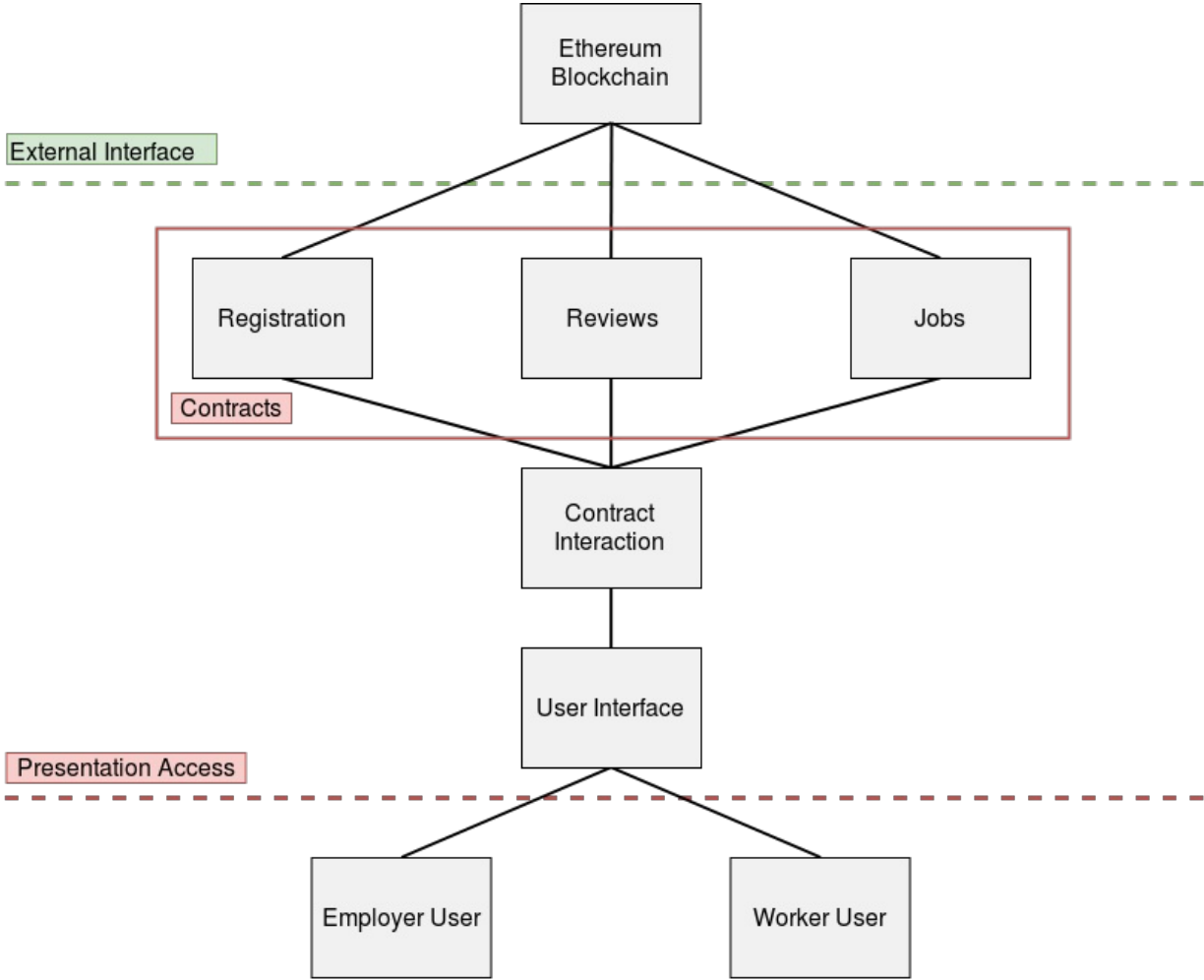
The Dapp web browser or Ethereum enabled browser is a browser capable of interacting with the Ethereum blockchain through web3js. Development took place primarily on Chrome with the MetaMask extension. The Mist browser is also another option to interact with the Ethereum blockchain.

The front end of the application is written in HTML, CSS, & JavaScript, using Bootstrap and AngularJS. The content for the front-end is populated using web3js, a JavaScript library specifically used for interacting with smart contracts stored on the Ethereum blockchain. Ideally in a fully decentralised application, you would not use a web server; you would use a service called 'swarm' which can provide the front end via a peer-to-peer network. This was not used for this application as 'swarm' is still too early in development.

The smart contracts contained on the Ethereum blockchain are where the data for the application is stored. Written in Solidity, they perform the transactions necessary for completing a piece of work and store the relevant data for our users and their jobs.

3. High Level Design

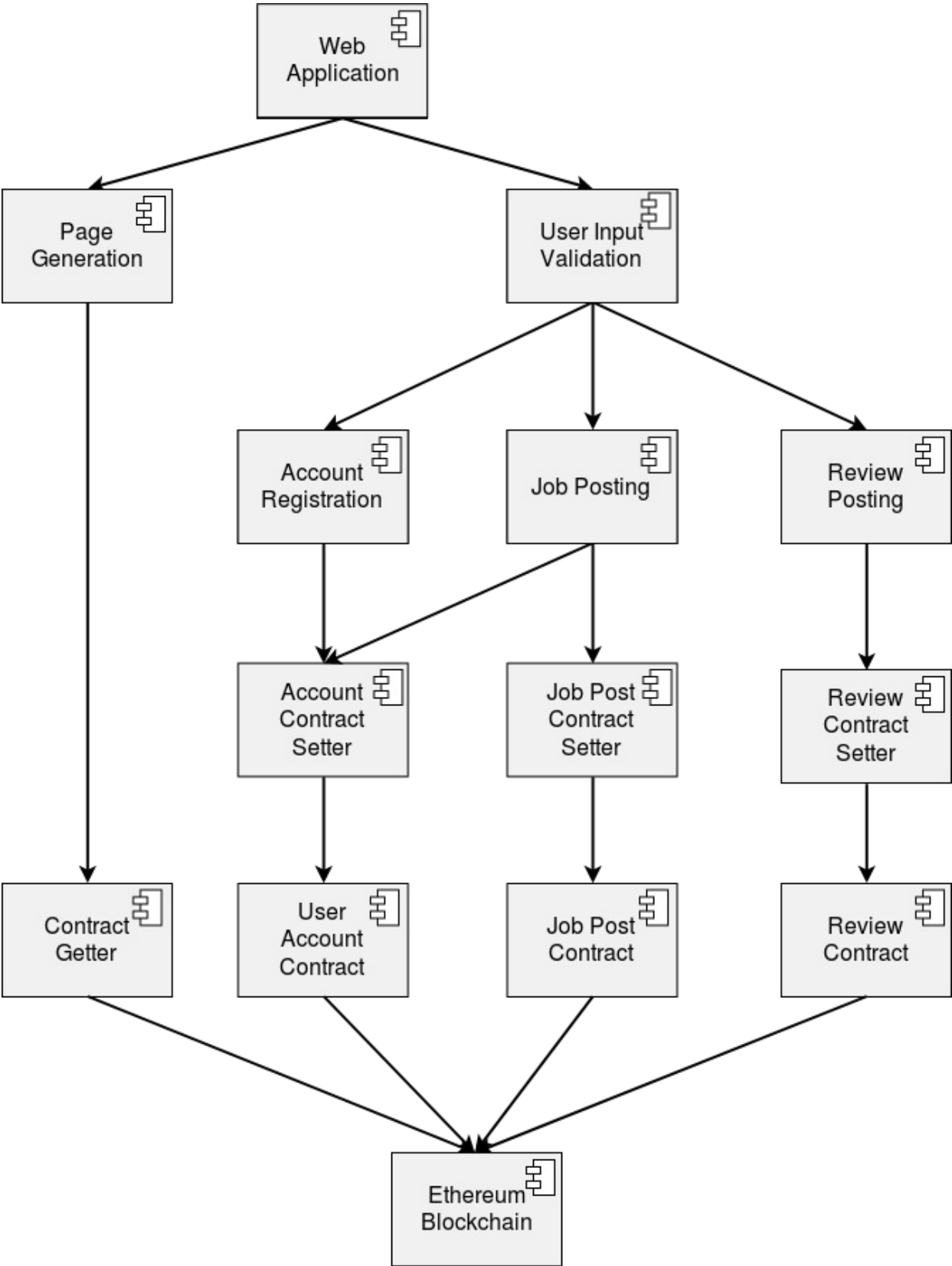
3.1 Architectural Overview Diagram



Note: Each of the users shown in the architectural overview diagram can collectively be one user. For example, the employer user for one job could be the worker user for a different job at the same time, and an unregistered user could become an employer user after they register their Ethereum account and post a job.

The A.O.D. is a high-level shared vision of the architecture and scope of the proposed application. It explores and evaluates alternative architectural options and enables early recognition and validation of the implications of the architectural approach. It helps to provides a conceptual understanding of the system. As shown in the diagram, the user interface interacts with a contract interaction section which will complete the main functionalities on the site using the smart contracts stored on the Ethereum blockchain.

3.2 Component Diagram

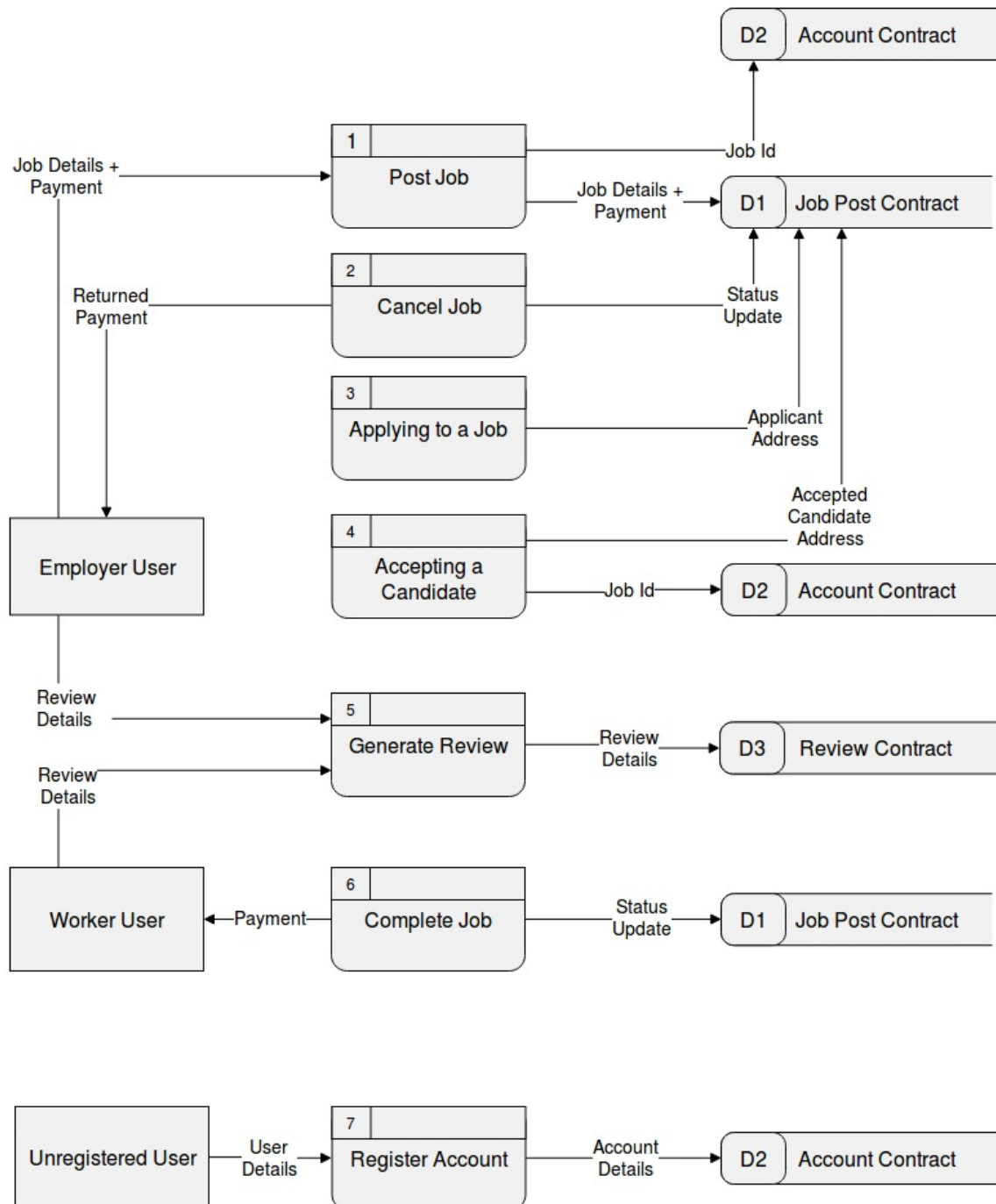


The component model is used to illustrate at a high level how components will interact within a system. The component diagram can be viewed as a lower level version of the architectural overview diagram. The different sections of the architectural overview diagram are displayed as

components. Components are functionalities in the system that complete a certain task.

For instance, the user interface section is broken down into page generation, user input validation and the different functionalities for the application. The contract interaction section is broken down into the various setters for the contracts and the contract getter used to populate the dynamic page generation.

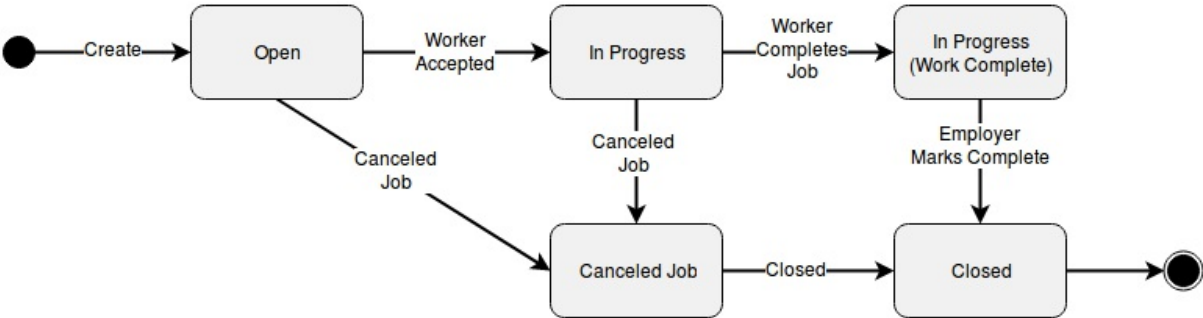
3.3 Data Flow Diagram



Note: As in the architectural overview diagram, the two employer and worker users can be one user.

A data flow diagram shows the flow of information for each process in our system.

3.4 State diagram



A state diagram describes the behaviour of a system.

This state diagram displays the different possible states for a job as it is completed by users on the application.

4. Problems and Resolutions

Profanity in the application

- **Problem:** It was mentioned at our project proposal demonstration that we should be wary of the use of profanity by users in our application. As the storage for this application is on a blockchain, traditional moderation would be extremely difficult.
- **Solution:** We developed a profanity filter with 3000+ profane words. These words were gathered by scraping a number of online profanity lists and compiling our own list of the unique words. Much of these words are slight variations of the same word. In the filter we strip the words of any special characters in order to catch attempts to circumvent the filter by appending special characters.

Dynamically creating unique webpages

- **Problem:** Each job created and account registered would need to have a unique webpage for displaying the information related to it. Accounts need to display user information, and jobs need to display the title, description of the work and payment amount for completing the work. Similarly, it was necessary to generate a page of search results dynamically based on the search input.
- **Solution:** Passing the job ID's and account addresses as part of the URL for the webpages. This information is parsed when generating the page and it pulls the relevant information from the blockchain.

Note: This had the added benefit of allowing our users to share links with one another, as the data for generating each page would be parsed from the URL they shared.

Deploying to a live network

- **Problem:** There are many conflicting tutorials on how to deploy certain applications to the Ropsten test network, most of which did not work for our application. Deploying to a test network allowed us to see how our application would act on a live network.
- **Solution:** After trial and error, our application was deployed to the Ropsten test network. We created a tutorial as part of our blog in order for us to remember how to deploy our application to the test network.

Returning an array of values from a contract

- **Problem:** Solidity does not allow you to return an array of struct type, instead you must return a single struct as an array of multiple types. This was necessary in order for us to display lists of jobs (including all job details).
- **Solution:** It was beneficial to keep a count of all jobs in the job contract, and allow easy access using a getter function. This meant we could retrieve this total and get each job

between 0 and total individually in a loop.

Lack of documentation

- **Problem:** Solidity, Truffle and many Ethereum based technologies are still in active development, this means that there is very little official documentation for many of the technologies we used. Of the documentation that is available, quite a lot of it is deprecated or conflicts with other documentation.
- **Solution:** We became members of public forum sites such as Ethereum Stack Exchange, Ethereum.org forum and Gitter chatrooms for some of the technologies used in this project. The Gitter chatrooms were particularly useful as in some cases we could interact with some of the open source developers of the projects.

Updating smart-contract ABI's for JavaScript interaction

- **Problem:** When interacting with smart contracts on Ethereum using JavaScript you must include the ABI of the contracts you are interacting with. When developing the application we had to generate a new ABI whenever any changes were made to the contracts in any way. Each JavaScript file that interacts with the contracts must have access to this ABI and the address of the contract on the blockchain.
- **Solution:** In order to prevent us having to edit every JavaScript file whenever a change was made to one of the contracts, we centralised these ABI's and contract addresses. Each contract ABI and address is stored in a file called *contractInfo.js* which every JavaScript file has access to.

Creating a "fuzzy search"

- **Problem:** Originally, we had planned to search for jobs purely by keyword but we decided later on that it was best to implement a "fuzzy search" to allow our system to return jobs or users that are spelled similarly to the search input. Fuse.js is a JavaScript library which provides a "fuzzy search", however it is a node module which means that it cannot be run by the browser on our site.
- **Solution:** In order to allow the use of fuse.js by the browser we had to bundle the *search.js* file using a tool called browserify.

Populating pages using angular js and smart-contract calls

- **Problem:** The angular js used to populate pages would complete before many of the calls to get data from the contracts on the blockchain had returned, resulting in a blank page or an error.
- **Solution:** Once the data had been returned from the contracts we had to force angular to update any relevant variables using *\$apply*.

Job List scalability

- **Problem:** As a larger number of jobs were added to the application, the job list & open job list slowed down greatly as initially every job posted on the application would be retrieved from the blockchain in order to display them all in one page.
- **Solution:** Modified job list and open job list to display jobs in a series of pages rather than on one page. The page information is passed as part of the URL similarly to the dynamic creation of webpages mentioned previously.

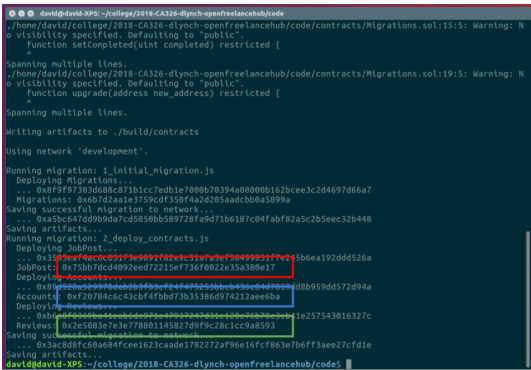
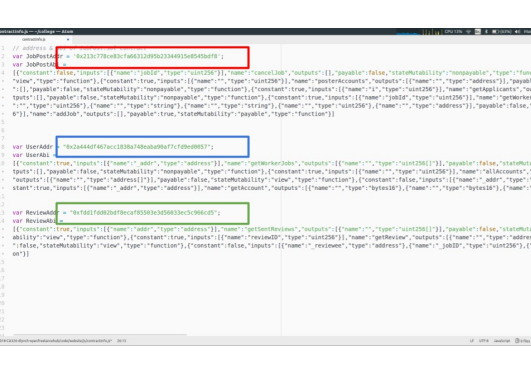
5. Installation Guide

5.1 Local Installation

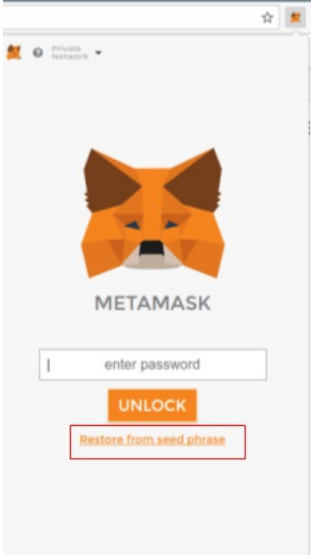
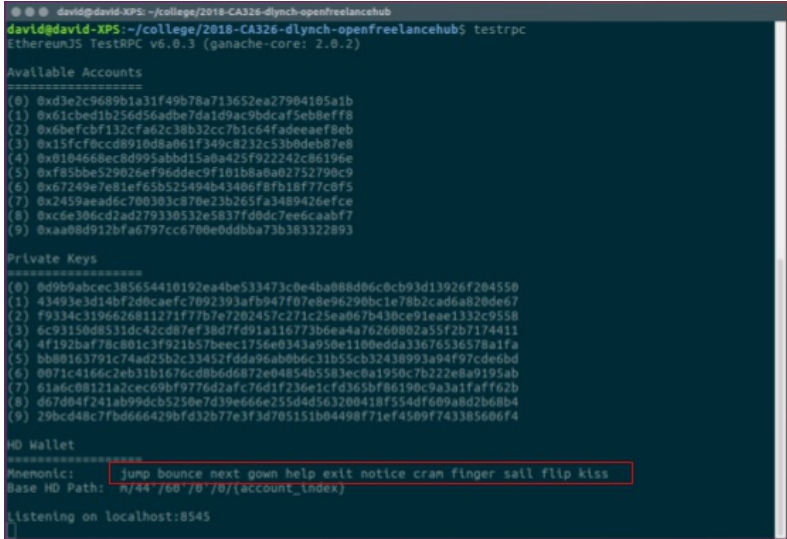
These steps will function as a walkthrough for deploying the application for use on a private blockchain on a local machine. All users will have to use the same machine when interacting with the site.

Requirements: testrpc, truffle framework, chrome with MetaMask extension, lite-server node module

- Run testrpc in a terminal instance using the command *testrpc*. This will run a local instance of the blockchain.
- In a different terminal instance enter the code directory of this project, run the command *npm run dev*. This will run lite-server to host the website frontend.
- In another terminal instance, in the same directory, run the command *truffle migrate*. This will post the smart contracts to the local instance of the blockchain running with *testrpc*.
- Copy the addresses of each of the contracts, which are returned by the *truffle migrate* command, and place them into the *contractInfo.js* file in the js directory.

truffle migrate result	contractInfo.js file
	

- Open chrome, choose *Restore from seed* in the MetaMask extension, copy the 12 word mnemonic from the *testrpc* terminal window into the popup and create a password.

MetaMask restore from seed	testrpc mnemonic
 <p>The screenshot shows the MetaMask extension interface. At the top, there's a fox logo and the text 'METAMASK'. Below that is a text input field with the placeholder 'enter password'. Underneath the input field is an orange 'UNLOCK' button. At the bottom, there is a red-bordered button labeled 'Restore from seed phrase'.</p>	 <pre> david@david-XPS: ~/college/2018-CA326-dlynch-openfreelancehub\$ testrpc EthereumJS TestRPC v6.0.3 (ganache-core: 2.0.2) Available Accounts ----- (0) 0xd3e2c9689b1a31f49b78a713652ea27904185a1b (1) 0x61cbcd1b256d56adbe7da1d9ac9bdcaf5eb8eff8 (2) 0x6befcbf132cfa62c38b32cc7b1c64faddeaf8eb (3) 0x15fcf8ccd8910d8a061f349c8232c53b0deb87e0 (4) 0x0104668ec8d995abbd15a0a425f922242c86196e (5) 0xf85bbe529026ef96ddec9f101b8a8a02752790c9 (6) 0x67249e7e81ef65b525494b43406f8fb18f77c0f5 (7) 0x2459aeaddc700303c870e23b265fa3489420efce (8) 0xc6e306cd2ad279330532e5837fd0dcfee6caabf7 (9) 0xaa00d912bfa6797cc6700e0ddbba73b38332893 Private Keys ----- (0) 0d9b9abcec385654410192ea4be533473c0e4ba088d06c0cb93d13926f204550 (1) 43493e3d14bf2d0caefc7092393af947f07e8e96290bc1e78b2cad6a820de67 (2) f9334c3196626811271f77b7e7202457c271c25ea067b430ce91eae1332c9558 (3) 6c93150d851d42cd87ef38d7f091a116773b6ea4a76260802a55f2b7174411 (4) 4f192ba778c00c3f921b57bec1756e0343a950e1100edda3676536578a1fa (5) b009163791c74ad23b2c3432fdda96ab006c31b55cb32438993a94f97cde0bd (6) 0071c4166c2eb31b1676cd8bd60872e04054b583ecba1950c7b222e8a9195ab (7) 61a6c08121a2ccc60bf9776d2afc76d1f236e1cf365bf86190c9a3a1faf62b (8) d67d04f241ab99dcb5250e7d39e666e25d4d563200418f554df609a8d2b60b4 (9) 29bcd48c7fbd666429bf632b77e3f3d705151b04490f71ef4509f743385606f4 HD Wallet ----- Mnemonic: jump bounce next gown help exit notice cran finger sail flip kiss Base HD Path: M/44'/60'/0'/0'/[account_index] Listening on localhost:8545 </pre>

- The application can now be used in chrome, at *localhost:3000*.

5.2 Ropsten Deployment

These steps will function as a walkthrough for deploying the smart contracts to the Ropsten network. The front end can be hosted either locally using *npm run dev* as in this walkthrough or a server for public users to access it. Similar steps have also been outlined on our project blog.

Requirements: geth (Ethereum implement using go), truffle framework, chrome with MetaMask extension, lite-server node module

- Run geth using the following command in a terminal window: *geth --testnet --syncmode "fast" --rpc --rpcapi db,eth,net,web3,personal --rpcport 8545*

geth running in terminal

```
david@david-XPS: ~/college/2018-CA326-dlynch-openfreelancehub/code
david@david-XPS:~/college/2018-CA326-dlynch-openfreelancehub/code$ geth --testnet --syncmode "fast" --
rpc --rpcapi db,eth,net,web3,personal --rpcport 8545
INFO [03-06|12:49:05] Starting peer-to-peer node                               instance=Geth/v1.7.3-stable-4bb3c89d/li
nux-amd64/go1.9
INFO [03-06|12:49:05] Allocated cache and file handles                             database=/home/david/.ethereum/testnet/
geth/chaindata cache=128 handles=1024
INFO [03-06|12:49:05] Initialised chain configuration                             config="{ChainID: 3 Homestead: 0 DAO: <
nil> DAOSupport: true EIP150: 0 EIP155: 10 EIP158: 10 Byzantium: 1700000 Engine: ethash}"
INFO [03-06|12:49:05] Disk storage enabled for ethash caches                       dir=/home/david/.ethereum/testnet/geth/
ethash count=3
INFO [03-06|12:49:05] Disk storage enabled for ethash DAGs                         dir=/home/david/.ethash
count=2
INFO [03-06|12:49:05] Initialising Ethereum protocol                             versions="[63 62]" network=3
INFO [03-06|12:49:05] Loaded most recent local header                             number=270 hash=3355cf...ce001a td=275302
312
INFO [03-06|12:49:05] Loaded most recent local full block                         number=270 hash=3355cf...ce001a td=275302
312
INFO [03-06|12:49:05] Loaded most recent local fast block                         number=270 hash=3355cf...ce001a td=275302
312
INFO [03-06|12:49:05] Loaded local transaction journal                             transactions=1 dropped=1
INFO [03-06|12:49:05] Regenerated local transaction journal                       transactions=0 accounts=0
WARN [03-06|12:49:05] Blockchain not empty, fast sync disabled
INFO [03-06|12:49:05] Starting P2P networking
INFO [03-06|12:49:07] UDP listener up                                           self=enode://eb77337aff4dd75128be82b0cf
e0db337517d5a80348a021e0d19d5f72d74b60d2739c91ba59a02cb83f4e4ee21d2dfc5ec769b3adc48e158c02f2e30c36eb42
@[::]:30303
INFO [03-06|12:49:07] RLPx listener up                                          self=enode://eb77337aff4dd75128be82b0cf
e0db337517d5a80348a021e0d19d5f72d74b60d2739c91ba59a02cb83f4e4ee21d2dfc5ec769b3adc48e158c02f2e30c36eb42
@[::]:30303
INFO [03-06|12:49:07] IPC endpoint opened: /home/david/.ethereum/testnet/geth.ipc
INFO [03-06|12:49:07] HTTP endpoint opened: http://127.0.0.1:8545
```

- In a separate terminal instance run the truffle console using: `truffle console --network ropsten`
- In the truffle console run: `web3.personal.unlockAccount(web3.eth.accounts[0], "-PASSWORD-HERE-")`
- Now run `migrate` in the truffle terminal to deploy the contracts to the ropsten network.
- To run the front end simply run `npm run dev` in a terminal as specified in the local installation steps above.

6. Future work

- Ability to add to the profanity filter based on a report system.
- Allow users to update their biography through the application after registration has completed.
- Whisper chat functionality between an employer and an applicant.
- Swarm hosting of the application front-end to allow a fully decentralised deployment.