Fake Product Identification System

CPTS 427 Final Project Report

Brenden Nelson

I. Abstract:

This project is about designing a web application which will utilize the Ethereum blockchain to store data blocks containing information about authentic shoe products accessible by a QR code. The main task was to implement data storage on the blockchain in order to utilize the security aspects of the transparent chain of data that makes up the blockchain. Due to the cost of implementing an online publicly accessible blockchain where anyone scans a QR code, I have implemented an offline version of this with an offline private blockchain on my local machine. This is technically an online blockchain server although only I have access and it is for development/testing purposes only. This allows me to demonstrate all the features and functionality of the project without needing to spend money on launching a fully online ledger which would be a working first version of the end application. Towards the end of the document, I will describe how this project can be implemented in a public online manner and describe the structure of what an online blockchain would look like.

The end product would allow for a user to purchase shoes that contain a QR code imprinted somewhere on the shoe or the tag. This QR code, if valid and authentic, would take the user to the private blockchain database and allow them to view all the relevant information concerning their recent purchase. This would allow users to verify the authenticity of their purchase with just a simple scan of a QR code which can be done on any recent smartphone with a camera. This would be a very secure method of verifying the authenticity of products due to the transparent nature of the blockchain ledger. In the event that the QR code does not link to a shoe in the database, users would be made aware that their products authenticity cannot be verified, although this does not necessarily mean the product is fake.

II. Background Description:

Consumers can have a real problem with purchasing fake or knock off items under the impression that these items are authentic. This is unfortunately all too common with expensive shoes and the current methods of detecting fake products and verifying authenticity are unreliable and based on visual comparisons which are susceptible to human error. This can lead to many consumers spending large amounts of money on a potentially fake product without a safe way to verify the authenticity of their purchase. My intention with this project is to create a way for consumers to be able to securely verify that the product they purchased is authentic.

There are existing solutions such as mine that are being discussed and worked on, however no such working model currently exists. One company which is trying to implement a similar process utilizing the blockchain ledger to store authentic shoe data is Nike. They are attempting to implement this on a small scale in Australia using a blockchain tool called VeChain. This attempt has been a small success on all accounts although the product is not ready for mass deployment at the moment. This has inspired me to research this topic and attempt to create my own solution to this problem.

III. Tools:

For this project, I used a variety of tools and languages to attempt to get a working version of this offline blockchain ledger. Firstly, I used Truffle, which is a development framework for Ethereum containing a bunch of handy tools. These features of truffle are there to manage blockchain contracts and provide a sample framework for creating a development blockchain server.

Inside of my application, I used the json library to load the file contract information in order to grab the contract information. I also used the Web3 library to create a client interface for the truffle blockchain address. Another tool that I used was a QR code creator which links some QR codes to an online PDF which would contain authentic shoe information (currently fake info).

I then used the PIL python module to import the Image function. This was needed to convert the QR codes into readable files that I could decode. These were decoded using the pyzbar.pyzbar python library and importing the decode function. This returned some results about the QR code, of which I was able to pull out the website data and can link the user to the appropriate website containing the correct shoe information.

I also used the python hashllib library to access the SHA-2(256bit) hash function with my completely offline and local blockchain ledger I created.

IV. Methodology:

The very first step of this project was to research the current status of the available solutions to the problem I am attempting to address. This led me to believe that a new solution was needed more than ever. Next, I continued my research with a focus on what possible frameworks or tools I could use to be successful in completing this application. After deciding on the set of tools described above that would allow me to build an online blockchain, I had to research how to go about doing this. Basically, my entire milestone 1 was research and determining the tools and architecture of this application. This led to me using the tools above to try and create a virtual blockchain application perfect for simulating and testing blockchain applications.

Shortly after milestone 1, I began developing a script which created an offline blockchain using a SHA-2(256bit) hashing algorithm to simulate the process of how a blockchain operates in a completely offline environment. This included creating classes for the Blockchain ledger and the individual blocks. I wrote a function to initialize the hash values with the previous block hash value, current transaction data, current block data (current block concatenated with previous block hash value), and the current block hash value. The Blockchain class has functions to add blocks to the chains current ledger and to display all transactions from the current ledger. This application also included a few examples blocks that were added to an example chain and then displaying the entire ledger to the user. I gained a significantly better understanding of how the blockchain works by implementing this offline version. This showed me how changing a single aspect of a block would then invalidate the entire chain due to it causing the rest of the chain to contain different hash values. This is what leads to the advanced security aspect of a blockchain technology to store data which is not very likely to be tampered with. It is this system integrity that drew me towards using the blockchain to store data in the first place.

The next steps I took was to begin development of the Truffle application. This started with looking at the architecture and learning the basics of solidity so that I could write the contracts I needed for my application. The first version was a very small test that just connected to an online virtual development blockchain server and demonstrated the ability to compile contracts and migrate them to the online server. The purpose of this test was to familiarize myself with not only the truffle framework and all its uses, but also solidity and how to write effective code in that language.

Once I felt comfortable with the basic application of truffle framework and writing basic code with solidity, I began to once again delve into some research about how truffle could further assist my development of the online version of this blockchain. This led to a slight adjustment with the code pertaining to the blockchain address. I instead made the address my localhost so that I could connect with the server easier as I was having some troubles with using an online virtual truffle server. This allowed my application to run smoother and thus I could work more towards development rather than debugging problems with my connection to the online virtual blockchain. This offline application and the virtual online test application along with my research on the frameworks and other various topics thus far made up the majority of milestone 2.

After milestone 2, I began working to develop the QR code hashing functionality and adding that to my offline blockchain. This took slightly more time than anticipated, although I did finally manage to add this functionality to my offline blockchain application. This included 4 QR codes, 3 of which would link the user to authentic shoe purchases and display the information in the form of a pdf, and 1 of which is a fake QR code that informs the user that their purchase is unverifiable to be authentic. These were included as images inside of my application and upon scanning them, the user would be taken to the appropriate information. To simulate this for my demo, I just included the pdfs as well so that I could display the functionality, although the QR codes are functional and do work in taking the user to the information associated with the code.

The Final steps were an attempt to incorporate the logic and contract information from the offline blockchain in blockchain.py into the application I developed that interacts with the virtual blockchain. This turned out to be much harder than I originally anticipated and thus I was not able to complete this task. This is shown below in the "challenges encountered" section of this document. Due to the challenge of getting an online and virtual blockchain application working through truffle which could include the functionality I stated in my proposal and milestones, I decided to only move forward with the offline blockchain application self-contained within "blockchain.py".

This python script includes all the blockchain security features as well as QR code functionality which is the main logical implementation of my project. I also talk below about the steps that could be taken towards moving this application into an online version of this. I believe this would require much more time or the use of more advanced software which requires payment to be implemented correctly on an online public blockchain which is what the commercial version of this project would need.

V. Final Status of Project:

The final version of this project is an offline blockchain application that demonstrates examples of users interacting with the blockchain through QR codes to view the information regarding their recent purchase. This will be contained in a zip file which is the offline blockchain application as well as all necessary attachments and files needed to run my test example the same as in my demo.

The python script will create an offline blockchain and add example blocks (bogus shoe data) to the ledger. These blocks will be identifiable through a QR code which the script will use to link the user to a website containing the shoe information.

VI. Challenges encountered:

This project was very challenging, and I ran into many issues, some of which I was able to overcome and others that I was not. The first challenge that I ran into when designing this application was when trying to get my test virtual blockchain application online. At first, my test truffle address was not working properly, and I could not make progress with the application for a little bit. After trying many solutions, I finally determined that I would need to run the server on my localhost server so that I could just move on with the project and not be stuck trying to connect to the virtual online server forever. This worked and I was able to quickly develop the rest of the test application after this fix. The next and final challenge I ran into was incorporating the logic of the blockchain.py offline example into my virtual blockchain test to combine the features and complete the project. I had trouble in the beginning with the contract function not working properly and thus when migrating contracts to the server, there would be errors and the information would not be added properly. This was overcome by simplifying the application and the features into the final version which is just the ability to connect to a virtual blockchain server and add information blocks to the chain. The QR codes were included as part of the data on the block which would link to the block itself. This, I was only able to complete in my offline blockchain application due to encountering difficulties when trying to link the user to a webpage inside of my application which connects to my localhost and a virtual blockchain application.

VII. Future improvements:

This project, although implemented in a virtual manner, can easily be brought to a fully public online blockchain assuming the user can afford to host the server. This was the biggest challenge I ran into was the paywall to launch an actual blockchain ledger server.