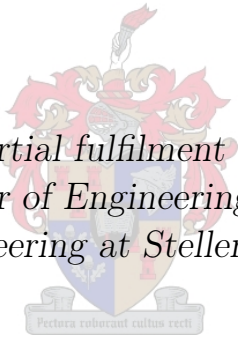
Bitcoin payment framework on a social media platform

by

Wessel Wessels



Thesis presented in partial fulfilment of the requirements for the degree of Master of Engineering (Electronic) in the Faculty of Engineering at Stellenbosch University

Department of Electrical and Electronic Engineering,
University of Stellenbosch,
Private Bag X1, Matieland 7602, South Africa.

Supervisor: Prof. G. van Rooyen

December 2015

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: 2015/12/10 .....

Abstract

Bitcoin payment framework on a social media platform

W. Wessels

Department of Electrical and Electronic Engineering,
University of Stellenbosch,
Private Bag X1, Matieland 7602, South Africa.

Thesis: MEng (E&E)

December 2015

English abstract to be written

Uittreksel

Bitcoin betalingsraamwerk op 'n sosiale media platform

("Bitcoin payment framework on a social media platform")

W. Wessels

Departement Elektries en Elektroniese Ingenieurswese,
Universiteit van Stellenbosch,
Privaatsak X1, Matieland 7602, Suid Afrika.

Tesis: MIng (E&E)

Desember 2015

Afrikaanse uittreksel wat nog geskryf moet word

Acknowledgements

I would like to express my sincere gratitude to the following people and organisations ...

Dedications

Hierdie tesis word opgedra aan ...

Contents

Declaration **i**

Abstract **ii**

Uittreksel **iii**

Acknowledgements **iv**

Dedications **v**

Contents **vi**

List of Figures **viii**

List of Tables **ix**

Nomenclature **x**

1 Introduction **1**
1.1 Background 1
1.2 Related Work 1
1.3 Objectives 1

2 Background **2**
2.1 History 2

3 System Design **3**
3.1 Framework 3

4 Detail Design **7**
4.1 Back-end 7
4.2 Social Media Platform 7
4.3 WeChat Wallet Design 11

5 Tests **12**
5.1 Quantative 12

5.2 Qualitive 12

6 Conclusion **13**
6.1 The Conclusion 13

Appendices **14**

A No appendices yet **15**

Bibliography **16**

List of Figures

3.1 Summary of Framework 4

4.1 Interaction with WeChat 8
4.2 Gamebook Database Table 10

List of Tables

Nomenclature

No nomenclature yet.

Chapter 1

Introduction

Bitcoin [1] is a peer-to-peer decentralised payment mechanism

1.1 Background

1.2 Related Work

1.3 Objectives

Chapter 2

Background

2.1 History

Chapter 3

System Design

3.1 Framework

In this project we test the viability of a payment framework on a mobile social media platform. The framework will consist of several independant but connected pieces:

- REST API for payments
- Wallet Application
- Bitcoin Interface
- Use-case Application

A summary of what is required from the system can be seen in figure 3.1.

3.1.1 REST API for payment management

A REST (Representational State Transfer) API [2] was chosen for the main interface for developers to use Bitcoin without running a Bitcoin node or having experience with Bitcoin. REST was chosen because it is a commonly used architecture, it is easy to use and understand and it does not constrain the user's choice of programming langauge or environment.

The purpose of the REST API is to let developers make payment requests and check if a payment has been made, without dealing with the low-level Bitcoin transactions directly. Thus, our system should generate a new Bitcoin address on request.

Our requirements from the REST API are:

- New Bitcoin address for each payment
- Verify payment

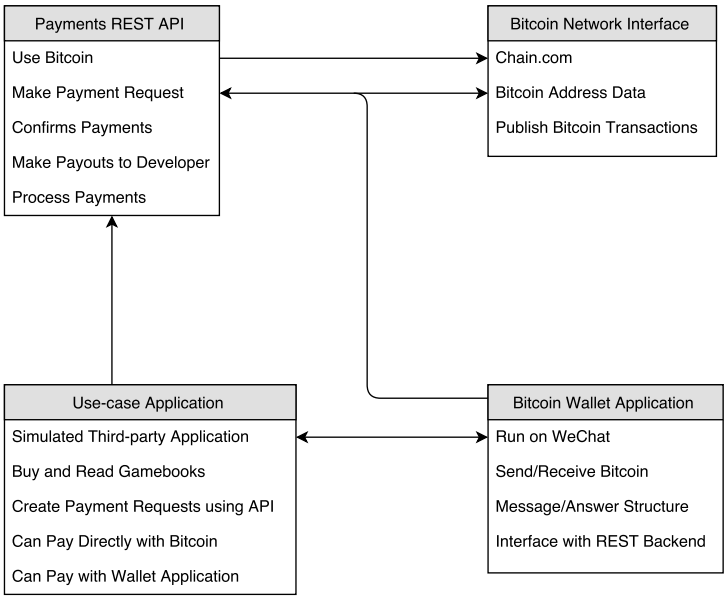


Figure 3.1: Summary of Framework

- Check total balance of developer
- Witdraw available Bitcoin of developer

3.1.1.1 The concept of the Bitcoin payment

This is a high-level explanation of how to receive verifyable payments with Bitcoin. With Bitcoin, unlike a traditional bank account, you don't have a single "account" where people can make payments to and you can verify that the payment came from them. With Bitcoin it is trivially easy to make a new Bitcoin address, and it can be generated without being connected to the Internet or the Bitcoin network.

Since the entire Bitcoin blockchain is public, a single address is not sufficient to receive multiple payments. With a single address, it is not easy to verify that a spesific person has made a payment, since there may be several payments of the same amount happening in short succession.

The sollution to the problem is generating a new address for every payment, and requesting that the user make the payment to that address. Since the newly generated address is not yet present on the blockchain, when a payment to that address of the requested amount occurs, we can be certain that the person in question made the payment. When the payment is complete, the Bitcoin in that address can be transferred to a central address, and the original address can be discarded.

From our requirements for the REST API, we clearly require (at least) the following methods:

- A “payment” method
- A “balance” method
- A “payout” method

3.1.1.2 The /payment method

The /payment method is the core of the REST API. It is used to make a payment request with a specified amount of Bitcoin and a description of the transaction. The /payment method returns a Bitcoin public address and a payment ID.

The user can then pay to the Bitcoin address using any standard Bitcoin payment method, or can pay directly from the Bitcoin wallet that will run on WeChat and will be connected to the payment infrastructure.

3.1.1.3 /payment/{PUBLIC_ADDRESS} and /payment/{ID}

These two methods are conceptually the same, but they take in two different arguments. The one takes the Bitcoin address to be queried, and the other takes the payment ID. The method returns all the data about the transaction, including the status of the transaction.

The main purpose of this method is to verify that a transaction has been completed by the user. It can also be used to give the payment details to to user again.

3.1.1.4 /balance

The /balance method gives the developer the balance of all the available Bitcoin from all the received transactions. The method also returns a flag that says if there is enough Bitcoin to make a payout.

3.1.1.5 /payout

The /payout method is used by the developer to transfer all of the available Bitcoin to a specified Bitcoin address.

3.1.2 Wallet Application

The Wallet Application is a Bitcoin wallet implemented on the WeChat platform. The WeChat platform uses a simple message-answer structure. A user sends a message in the Wallet Application. The message is then sent to WeChat that sends it to a third party server controlled by the developer. The server then sends a reply to WeChat that is then forwarded to the user.

In this manner, a fully functional Bitcoin wallet is realised. The third party server stores the private keys and processes the Bitcoin transactions on commands from the user.

The advantage of using the WeChat platform is the security built in to the platform, as well as an existing userbase.

The Wallet Application will be directly connected to the back-end of the REST API. Thus, payment requests will be referable directly from the Wallet Application without needing to reference the Bitcoin Address. It will be able to reference the request using the payment ID mentioned in 3.1.1.2

3.1.3 Bitcoin Interface

To connect to the Bitcoin peer-to-peer network, a Bitcoin client is needed. The standard way of doing this is running the Bitcoin open source software on a server. This is very network and processor intensive. For development and testing, it will be quite expensive to run the Bitcoin software. Thus, an alternative is required for interfacing with the Bitcoin network. Fortunately, there are services that provide access to most of the Bitcoin operations using their API's.

We require the following from such a service:

- Get the balance from an address,
- Get unspent outputs from an address,
- Post a signed Bitcoin transaction to the network,
- It must be able to use the Testnet

The details of the chosen service is covered in chapter 4.

3.1.4 Use-case Application

To use the payment framework, a Gamebook application is created to read Choose Your Own Adventure style books on the WeChat platform. User-created books can be sold by using the Bitcoin payment framework and the author can potentially earn Bitcoin.

For each sale, the Gamebook application creates a payment request using the REST API. The user can then pay using the Wallet Application or any Bitcoin payment mechanism. The Gamebook application can the query the API to confirm that the payment is received.

Chapter 4

Detail Design

4.1 Back-end

To implement the payment framework, we need a back-end server and a back-end web framework.

4.1.1 Back-end Server

We chose an Amazon Elastic Cloud Computing (EC2) instance for the back-end server. EC2 gives us access to a virtual machine (VM) where we can run our own software, including a publicly accessible website. The micro instance is deployed in Singapore in the Asia Pacific region. The reason for this is to have the server as close as possible to the WeChat servers in China, since our servers must connect to WeChat's servers.

4.1.2 Back-end Web Framework

We decided to use XAMPP (Apache, MySQL, PHP and Perl) for the back-end development environment. XAMPP is a full stack development environment. It includes an HTTP server (Apache), a database server (MySQL) and a scripting language (PHP). XAMPP is free and easy to deploy, and is also used because the author is familiar with it.

4.2 Social Media Platform

We chose WeChat for our social media platform. WeChat works on most smartphones, already has a userbase and it has a third-party API with a development sandbox feature.

On WeChat, a third-party application is known as an "Official Account". We registered for a sandbox Official Account that only allows 20 users and is not searchable on WeChat.

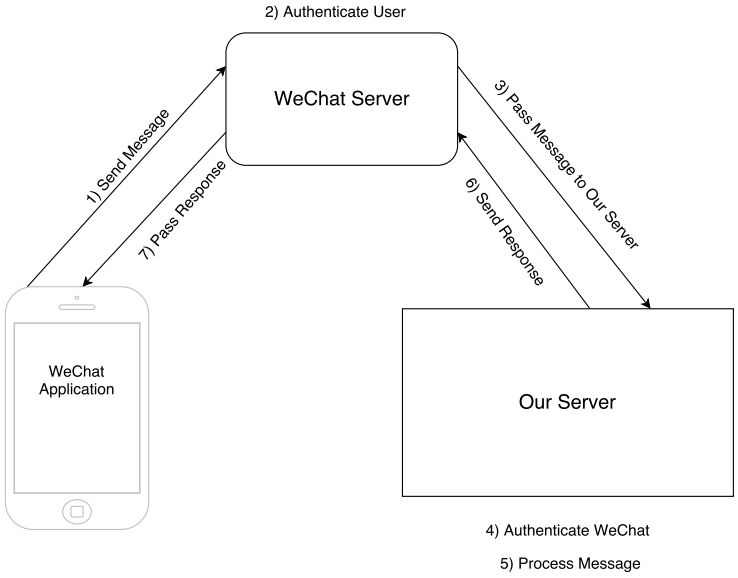


Figure 4.1: Interaction with WeChat

WeChat acts as an intermediary between the user and our server as seen in figure 4.1.

4.2.1 WeChat Security

WeChat uses a shared token hashing scheme to authenticate itself on our server. We provide WeChat with a unique string to use for authentication purposes. That string is then used in every request that is made to our server. WeChat uses the string we provided, a random nonce and the UNIX timestamp to create a signature. It sorts the string, timestamp and nonce and forms a single string from these three values. This single string is then hashed using the SHA256 hashing algorithm to generate a signature. When a request is made to our server, WeChat provides the nonce, the timestamp and the signature The message does not contain the unique string. Since we know the unique string, we can use the nonce and timestamp to also generate a signature. If the message comes from someone that possesses the same unique string, the signature that is provided must match the signature that we calculated.

Thus, we can be reasonably certain that any request that is made to our server with a signature that is verified comes from WeChat and not an attacker. If our unique string is compromised somehow, someone will be able to make false requests to our server that appear valid. If this would happen, we can give WeChat a new unique string.

4.2.2 WeChat Interface

The WeChat Official Account interface works on a message-answer basis. Any message that the user sends in the Official Account dialog is forwarded to our server. When we configure our Official Account, we provide WeChat with a URL that points to the script that handles all messages from and to Wechat. This script verifies any incoming messages as described in section 4.2.1.

The incoming message is in XML format. It contains a unique identifier for every subscriber to the WeChat Official Account. It is important to note that the unique identifier is only unique for the spesific Official Account. The identifier is not a global unique identifier for the entire WeChat platform. Thus, the same user will have two different identifiers in two different Official Accounts. This is important to remember, since we will be using two seperate Official Accounts.

The messages that are received must be interpreted and responded to accordingly. Since we will have applications that rely on previous messages and results, we need something to keep track of the user's current state. A state machine is required to look at the current state the user is in, look at the message they sent and accordingly determine what to reply and to what state to move to.

To keep track of the user's state, we will use a MySQL database as described in section 4.1.2. Thus, for each message received, we will read the user's current state from the database and apply the state machine logic to their message. We will then update their state in the database and reply with the message that the state machine determined.

4.2.3 Gamebook Design

The use-case application we chose to demonstrate the payments framework is a Gamebook application. A Gamebook is a non-linear book that tells a story based on the user's input. In physical books, this is done by giving the user a choice and then telling them what page to go to based on their choice. In the digital realm, we can simply provide the user a choice and give them the corresponding text. The software keeps track of what options links where.

In a dedicated Gamebook reader, a common method of generating a Gamebook is using a scripting language like ChoiceScript [3]. Since WeChat doesn't have any client-side scripting, using a scripting language like this is not possible.

We decided to create our own system of storing and reading Gamebooks. We use the MySQL database as the method of storing and organising the Gamebooks.

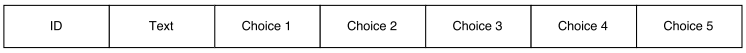


Figure 4.2: Gamebook Database Table

4.2.3.1 Gamebook Database Design

Every book in our design is a table, and every page is an entry in the table. Each entry has a unique id, the text of the page and then the references of each of the choices from that page. We chose five to be the maximum amount of choices on each page. The database resembles a linked list, where each entry has pointers to the next corresponding entry. The design of the Gamebook table is seen in figure 4.2.

The values of the fields choice 1 - 5 will have the corresponding ID's of the "page" they link to. If an entry only has two choices, the rest of the options will have the value null to indicate that it is not a valid choice.

We chose this method of storing the Gamebooks, because it is easy to implement, easy for a writer to visualise and allows us to have sircular stories and also allows us to visit multiple branches of the story.

We will also need two more tables: one to store a list of all the books available and another to keep track of books purchased by individuals.

4.2.3.2 Gamebook Author Platform

As stated in section 4.2.3, we are not going to use a scripting language to write the Gamebook in. It doesn't fit the design of the application that we are building, and has a learning curve for people that want to start writing books and are not familiar with scripting languages. We decided to use a Graphical User Interface for writing the Gamebooks.

We decided to use a website as the author platform. We used commonly used web technologies to build the platform. For the front-end, we used HTML, JavaScript with jQuery, and Twitter's Bootstrap CSS framework.

Using AJAX, we connect the front-end with the back-end PHP scripts that connects to the MySQL database. We also decided to use an OAuth login mechanism to facilitate logins, rather than writing our own login system. A big motivation for doing this is the authors desire to get experience with OAuth. We decided to use Google's OAuth platform, because it widely used and well documented. By using OAuth, we are enabled to have unique, secure logins without having to design all the security measures to protect the user. It also makes it easier for the user, because they can log in with a single click.

Since the Gamebook resembles a tree, we decided to display the tree using an organisational chart. We used Google's JavaScript Chart API to map the Gamebook. The Chart API is free, simple, powerful and well documented. To display the story as a tree makes it easier for the writer to navigate through the book and to get a bigger picture of the story.

4.3 WeChat Wallet Design

As stated before, the WeChat Official Account doesn't allow us to run client-side code. This means that the WeChat Wallet will have to be a hosted Bitcoin wallet, with the Official Account interfacing with the hosted wallet.

To have a WeChat wallet, we need a Bitcoin address. When hosting a Bitcoin wallet, there are two main method of keeping addresses. The first method is where a user gets a single address or adresses and these addresses are used only by the single user. The user may or may not have access to the private key, but the wallet is associated with only that user. This allows the user to verify the balance and transactions by checking the blockchain.

The second method is where the user has an account, and can have a receiving address, but the user is not directly in control of the address. The users' balance is not verifiable by using the Bitcoin blockchain. This is because the server keeps track of the balance of the user, and makes a payment from other addresses when a user wants to make a payment.

We chose the first method of storing the address, because it is simpler and has a more direct feeling for the user that he is using a real Bitcoin wallet, and not just something that arbitrarily keeps track of the balance.

4.3.1 Bitcoin PHP Library

Thus, we need to generate a Bitcoin address for each user. To do this, we use a a popular open-source PHP Bitcoin library called bitcoin-lib-php. One of the features of Bitcoin is that generating a Bitcoin wallet can be done locally. That means that the bitcoin-lib-php library generates a Bitcoin address on our server without connecting to the Bitcoin network. This has many advantages, including it doesn't use network bandwidth, it is fast and the private key never leaves our server.

We chose bitcoin-lib-php as our library, because it satisfies our requirements perfectly, it is open-source (and thus verifiable) and is decently documented.

As mentioned in section 4.3, by creating an address for each user, the user can more directly monitor his funds and transactions since it can be independently verified by using any software that is connected to the Bitcoin blockchain.

The Bitcoin library allows us to create an address, create a Bitcoin transaction and sign a transaction. These are the core functions of Bitcoin. However, a transaction can't be created without information about the address or addresses that want to create the transaction. This information is called "unspent outputs" and, as the name suggests, are previously received transactions that are not yet spent. These unspent outputs contain all the information to build a transaction, including the value of the output, the transaction hash and the script type etc.

Chapter 5

Tests

5.1 Quantative

5.2 Qualitive

Chapter 6

Conclusion

6.1 The Conclusion

Appendices

Appendix A

No appendices yet

Bibliography

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Consulted*, pp. 1–9, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] Oracle.com, "What Are RESTful Web Services?" [Online]. Available: https://docs.oracle.com/javaee/6/tutorial/doc/gijqy.html

[3] C. o. G. LLC, "Introduction to ChoiceScript." [Online]. Available: https://www.choiceofgames.com/make-your-own-games/choicescript-intro/