

Department of Computer Science

University of Hong Kong

Final Year Project

Topic:

FYP18003

Blockchain and Smart Contract Application

Project Plan

Author: LAU Siu Ming, Alex
YAM Mei Ki, Vanessa
Date: September 30, 2018
Reference: fyppros.010
Issue: 1.0

Distributions: *FYP students*
FYP supervisors
FYP portal

Revision History

Issue	Date	Author	Description
1.0	29/09/2018	LAU Siu Ming, Alex YAM Mei Ki, Vanessa	First issue

Table of Contents

1. Introduction	3
1.1 Project Background	3
1.2 Project Objective	4
1.3 Project Methodology	5
2. Scope & Limitation	7
2.1 Major features	7
2.2 Scope of following releases	7
2.3 Limitation	8
3. Project Organisation	9
3.1 Team	9
3.2 Division of work	9
4. Project Schedule	10
5. Reference	12

1. Introduction

1.1. Project Background

Throughout the last decade, social media platforms have rapidly emerged and become a crucial part of our lives. People rely on Facebook in making connections, Instagram in sharing of photos and videos, Twitter in spreading of news... All of these platforms with their popularities share a common trait — centralization, and it is part of the reason that makes concept of ownership on the internet unconceivable. Content that one shared, regardless of the effort one put in, ultimately is being ran and managed by a centralized authority, and it is often difficult for people that are used to such scheme of platform to question their ownership rights in what they have contributed. Consequently, the nonexistence of concept in property right on the internet also leads to a lack of protection on original work or ideas. Even if one wishes to trace back to the author of a piece of content, it is difficult with the ever-changing nature of the internet.

There is no guarantee in ownership nor originality to the content that one shared in the current media sharing platform, yet blockchain technology can change this. With the development of Bitcoin in 2008, increasing number of blockchains is being built and utilized in different aspects such as finance and game industry. It introduces a relatively less familiar concept to the public, a transparent and decentralized way of record storing. By making use of the blockchain technology, it is hoped that the ownership and originality of artwork published online can be better protected through this project.

1.2. Project Objective

This project aims to provide a secure media sharing platform via the means of blockchain technology.

The intermediate goal for this project is to develop a demo website platform which will allow users to upload their creative artworks underlying the crypto-method of blockchain. The target is to explore possible ways of implementing a secure prototype that can ensure each contribution, artworks and derivative works included, is being recorded in the blockchain.

The ultimate goal is to develop an application which will ensure artwork sharing under the protection of blockchain record and that the users' copyrights and property rights can be preserved. Whenever an artwork is uploaded or downloaded by the user, it will be recorded by the application into the blockchain. And it is immutable. With this feature, the derivative work can be traced back along the blockchain to locate the original content creator. Furthermore, it encourages the community to produce derivative work and to share their concepts of creative art under this secure media sharing platform as well as helping users to generate values from their works by listing the price with Ethereum.

As the project is to provide a trustworthy platform that allows users to share their own content to the public, the target users will mainly be artists on the Internet, and they can publish their artworks and creative paintings through this online sharing platform.

1.3. Project Methodology

This project will be constructed as a Single Page web application, with a hybrid approach of cloud service database and blockchain technology for its back-end development.

Blockchain technique

For data processing with the use of blockchain, it is necessary to select an approach that is most suited to our need among various type of blockchain that are available in the market. Ethereum will be used to facilitate the back-end development of this project, for its already well established cryptocurrency — Ether, and its better supported flexibility. Comparing Ethereum to other popular blockchains such as Bitcoin, it offers a better degree of customization to users via Smart Contracts. While Bitcoin was built with predefined operations that support transaction type of activities, Ethereum was built as “*a meta-protocol on top of Bitcoin*”[1], with its Smart Contract allowing storage of any executable codes. This type of blockchain could secure not just values or records but any type of functionalities, such as storing of image and interaction with users info that are required in this project. While there are also other built blockchains, such as Stratis and EOS, that can support similar flexibility and even offer higher transaction rate, Ethereum has been the most popular platform to be used to build decentralized applications with the availability of Ethereum Virtual Machine that offers powerful computing power and adaptability to different programming languages to better support the construction of this project. Furthermore, such popularity also makes its cryptocurrency — Ether widely adopted, hence beneficial to users that wish to use this platform as a market to generate financial value from their artworks.

While option of building an original blockchain can offer tailor-made functionality for the project without any restriction of existing cryptocurrency and faster transaction rate with further development, these features are considered less crucial as compared to the advantages from using Ethereum. Even though building our own blockchain would eliminate the restriction of significant low transaction rate from Ethereum, it would require extra effort in implementing the wallet and mining technology that are already extensively developed in Ethereum. Taking into account that this application need not be real-time to be able to operate, the benefits of a well-established platform from Ethereum outweighs the advantage of performance and flexibility from a customized blockchain.

Hybrid approach on data storage

Storage will be one of the concern in this project since there are images and uploading information to be recorded after each sharing is performed on the platform. These two data sets will be handled with separate approaches. The uploaded information consists of the identity of the user and the link to the image, which will be stored using blockchain. The uploaded image will then be stored in the cloud server, accessible only by the private key secured in the blockchain.

This hybrid approach aims to minimize the cost and processing time in handling a large amount of workload on image uploading as storing the entire image with Ethereum is costly.

In fact, processing a large file such as an image is too expensive to be done on blockchain as it has to analyze the data set pixel by pixel, which slows down the transfer rate for creating a block in the blockchain. Hence, using cloud service for storing the uploaded image will increase cost effectiveness and maximize resources utility. The approach is to create a hash function to store the image link into the blockchain, in which the hash is used to verify the content of the image that is still valid in the cloud server. Once the connection between record on blockchain and cloud server is established via the hash function, the image can be stored in a secure address with the protection of blockchain, it can also utilize the usage between blockchain and cloud service.

Cloud Service selection

There are several cloud server hosts such as Azure from Microsoft, Google cloud and Amazon Web Services. They are the major competitors in the market nowadays[2]. These are the powerful cloud services to be considered since they also offer other external functions such as image recognition from AWS that could enhance image filtering for detecting inappropriate media when users uploaded an image.

During the starting phase of the project, the selection of the cloud service will be one of the task to be managed. After picking up suitable cloud service, the implementation of the cloud service API will be one of the major task in the back-end development of the application. It is essential to facilitate the image uploading functionality successfully to the cloud while saving its address on the blockchain.

Website

Performance of the website is always a priority for this project. Processing speed matters while considering the type of web application to be constructed. The website will be implemented as a Single Page Application (SPA), as it aims to improve content sharing experience. SPA provides a responsive site that allows users to browse different content in an efficient way. The advantage of a SPA is to enhance the interaction on the website. The application will be faster while less bandwidth is used[3]. Considering the website is a media sharing platform which is going to include a lot of message and file exchanging, a swift and responsive website should be ideal.

A Single Page Application requires server communication and involves JavaScript frameworks, Ajax, Websockets, Data transport(XML,JSON,Ajax) which will be used for client-server side communication. For front-end implementation, there are numerous frameworks to be selected from, such as AngularJS, Ember.js, React, etc. AngularJS, Ajax or React will be taken under the consideration for website development as they provide a clearer structure for the construction of the web application and the learning curve is relatively mild, it should be convenient to explore the suitable framework to develop a better user experience.

2. Scope & Limitation

2.1. Major features

FE1: For users to create accounts on the Website.

FE2: For users to manage their Profiles that are being displayed to others.

FE3: For users to upload artwork on to the website.

FE4: For users to modify the previous artwork by downloading and publishing a new one.

FE5: For users to be able to track the derivative and origin of an artwork.

FE6: For users to have the option in pricing their artwork.

FE7: For users to exchange ideas by giving comments.

FE8: For users to get tokens for giving contribution, such as artwork publishing and commenting in the community.

2.2. Scope of following releases

The following table outlines the scope of the initial release, which are features to be published for this FYP, and scope of future releases, which are features that are being hoped to be established in the future.

Features	Scope of this FYP	Scope of subsequent releases
FE1: Account creation	Fully implemented	-
FE2: Profile Management	Simple modification of user information should be included	To include more information that is useful for enhancing the transparency of the community
FE3: Artwork uploading	Only limited to imagery form of work, such as file format of JPEG, PNG, BMP...etc	To be extended to other formats of work, such as text and video
FE4: Artwork downloading	Fully implemented for downloading the uploaded image one by one	To be extended to download multiple artworks at once for convenience
FE5: Artwork tracking	Fully implemented	-
FE6: Artwork selling	Fully implemented	-
FE7: Commenting	Only available under each individual artwork	To be available under user profile, and with the option of private or public comment
FE8: Token generating	Token is represented as an internal point system	Token can be exchanged into cryptocurrency

2.3. Limitation

Artwork selling with external wallet technology

The wallet will be implemented with the external wallet API MetaMask as a common cryptocurrency wallet. Since it is not built and designed by our own, it may restrict the selling features as trading regulation under the wallet API is applied for successful cryptocurrency transaction.

Filtering of uploaded artwork

The content of uploaded artwork will require filtering, supported by the following reasons:

- 1) Inappropriate image sharing is one of the risk that happens on all media sharing platform. The viewers will receive improper message and content while browsing the website. The sensitive content should not be viewed by the adolescent.
- 2) Content-less image uploading should also be considered since users may spam meaningless content to get token as contribution reward. The action will harm the ecosystem of the community by making the exchanges of ideas worthless.

With the above problems, a content filtering function is needed to improve the quality of the community.

3. Project Organisation

3.1. Team

The size of team is in two people for this project. Hence, the division of work is about half for each person. As the project is a web application, both front-end and back-end developments are involved.

3.2. Division of work

#	Tasks	Alex	Vanessa
T1	Background research	E	E
T2	Requirement Specification	E	E
T3	Use Case design	E	E
T4	Blockchain architecture design	A	L
T5	Cloud service analysis	L	A
T6	User Interface design	A	L
T7	Blockchain construction	E	E
T8	Front-end implementation	A	L
T9	Cloud services intergration	L	A
T10	System intergration	L	A
T11	Unit testing	E	E
T12	Integration & System testing	E	E

E - Equally Responsible

L - Leader

A - Assistant

4. Project Schedule

The following is a tentative timeline of the project:

#	Milestones	Sept 18	Oct 18	Nov 18	Dec 18	Jan 19	Feb 19	Mar 19	Apr 19
Requirement									
M1	Background research								
M2	Requirement Specification								
Design and Analysis									
M3	Use Case design								
M4	Blockchain architecture design								
M5	Cloud service analysis								
M6	User Interface design								
Implementation									
M7	Blockchain construction								
M8	Front-end implementation								
M9	Cloud services intergration								
M10	System intergration								
Testing									
M11	Unit testing								
M12	Integration & System testing								

Project Plan

With the following deliverables:

Time	Deliverable	Corresponding Milestones
Sept	Project Plan	M1 - M2
	Project Website	
Jan	First presentation	M3 - M8
	Interim Report	
	Demo application	
Apr	Finalized implementation	M8 - M12
	Final report	
	Final presentation	

5. Reference

[1] Buterin V. A next-generation smart contract and decentralized application platform [Internet]. 2014 [cited 2018 Sep 28]; Available from: <https://github.com/ethereum/wiki/wiki/White-Paper>

[2] Caylent [Internet]. Cloud Services Comparison: AWS Vs. Google Vs. Azure; [updated 2018 May 30; cited 2018 Sep28]. Available from: <https://caylent.com/aws-google-azure-cloud-comparison/>

[3] Angular University [Internet]. Angular SPA: Why Single Page Applications?; [updated 2018 June 18; cited 2018 Sep 28]. Available from: <https://blog.angular-university.io/why-a-single-page-application-what-are-the-benefits-what-is-a-spa/>