FYP Proposal

Stable Coin For HKD

By

Lo Kai Man and Zhou Haihui

Supervised By

Dr Yuen John

Department of Computer Science

The Hong Kong University of Science and Technology

2020 - 2021

Date of Submission: 3rd Oct 2020

Table of Contents

1 Background

1.1 Cryptocurrency

Cryptocurrency as a digital currency that can be transacted across the world has been long desired. According to the CoinMarketCap[1], there are over 6000 cryptocurrencies by september 2020 and carrying a total market value over $334 billions.

The first cryptocurrency, Bitcoin, was created in 2009. Undergone rapid growth, Bitcoin has significant influence on both the virtual and physical world. For example, people could use it to purchase hotels, games and gold[2].

There are several general advantages of cryptocurrency, it is transparent, decentralised and immutable. It is because cryptocurrency is implemented with blockchain technology. Blockchain is the foundation of cryptocurrency. A block contains digital data and the hash value of it, and a newly added block has a hash pointer pointing to the previous block with the previous block's hash value. In this way, they form a chain. The digital data are all digitally signed and therefore everyone can use the public key to verify the transaction. Anyone who wants to tamper with the transaction records will need to deal with the blocks connecting to it as well and makes this dishonest action computationally impossible. Moreover, the blockchain data is decentralized, that is every user's computer has a copy of it, so this requires the attacker to attack half of the users to make the fake transaction valid and that is adding another layer of protection as well.

With so many reasons to adopt Bitcoin, the drawback that is stopping shops from accepting Bitcoin as a payment method is also clear, that the value is highly volatile. Stablecoin then is designed to oppose this volatility and aim at providing cryptocurrency with price stability.

1.2 Stablecoin

There mainly are two kinds of Stablecoin, either pegged with fiat currency or exchange-traded assets like gold. A good example will be Tether, also known as USDT, is one renowned stablecoin that pegged with USD. It is issued with a promise that the value will always be stable at a 1:1 ratio between USDT and USD.

However, how to issue the coins or tokens to the user and make sure the exchange rate remains stable? That is the key role the smart contract is going to play.

1.3 ERC20 ICO Contract

Ethereum was initially described in a white paper by Vitalik Buterin in 2013. It proposed a new blockchain system (ETH Chain) and development platform. This network is account-based which allows one address to hold all the transactions so that it is more user friendly for new blockchain users. Since it is more user friendly, ethereum is now a popular blockchain platform and well developed.

ERC20 is a technical standard for Ethereum Network Smart Contract. It provides a list of rules for the tokens to follow the structure of ERC20. A Smart Contract can be deployed in the Ethereum Network by broadcasting the contract written in Solidity. ERC20 has become the dominant standard for a long time and by October 2019, the number of tokens that adopt ERC20 exceeds 200,000[3]. ICO is a technical standard of Smart Contract which is proposed for all newly initiated coins or tokens.

Following the standard structure, a crypto wallet is then developed to maximize user experience with the new currency.

1.4 Cryptocurrency Wallet

Trading digital currencies means there needs to be an application for buying, selling and transferring the coins. Therefore a digital wallet for cryptocurrency is developed, which can be interpreted as a bank account. Different crypto wallets applications may implement different features.

Beside basic functions, the main point is about securely storing the private key on the physical device. If the private key is leaked, others can easily steal the money. Since the private key is the only authentication method, once the physical device is broken, the money can never be recovered. Thus, some digital wallets have a wallet seed as well. The seed can be a set of words or alphanumerics that can be used to generate the private key, therefore it needs to be kept safe by the user or a leakage leads to financial loss.

2 Motivations

Hong Kong has a lot of useful payment methods, such as Octopus Card, Wechat Pay, Credit Card, PPS, but currently seldom companies or individual customers are using cryptocurrencies as their major payment method. The main reason could be the fluctuating value of cryptocurrencies, such as Bitcoin. The value of Bitcoin may have more than 3000 USD variance in three month. With the use of Stable Coin, cryptocurrency can now be one of the payment methods, but it only supports USD, EUR, CHN and XAU. Thus, this project is going to promote another Stable Coin HKDT and carry out a new payment method in Hong Kong.

3 Objectives

3.1 Stable Coin For HKD (HKDT)

This proposal proposes a new stablecoin that provides 1:1 exchange ratio with HKD and therefore can be used as a substitute for HKD in trading. Since HKDT is sticked on the blockchain system, whatever the trading amount, the transaction fee will be the same. The blockchain system runs automatically and carries out real time transactions. Thus, it is going to serve as a new cashless payment with lower transaction fee at any time anywhere.

3.2 HKDT Wallet

A mobile application that can provide services related to HKDT is another goal of the project. The application provides an easy-to-use interface for the blockchain system and transaction of HKDT can be achieved with a few manual steps. With the use of the mobile app, users can use the HKDT without prior knowledge on blockchain. The mobility nature would facilitate shops making transactions with the HKDT. The application is also the essential platform for HKDT and HKD exchange.

4 Methodology

4.1 ERC20 ICO Contract

Fiat-backed Stable Coin is the cryptocurrency that every coin is backed with reserved fiat money. That makes an obvious difference with the basic cryptocurrencies such as Bitcoin or Ether as it should not allow mining actions or the Stable Coin cannot provide reserved fiat money as rewards to the miners. Thus, fiat-backed Stable Coin should always be done as a smart contract in the blockchain system to adjust the value when needed.

There are many smart contracts widely used for Fiat-backed Stable Coin. This project chooses the ERC20 standard and ICO Smart Contract. The basic function is it allows users to purchase the token by sending the coin to the ICO Smart Contract and the token issuing is handled automatically. Using ICO Smart Contract gives the potential for users buying the HKDT with cryptocurrencies and a potential payment alternative in the future. In addition, ICO also provides real time payment and a more secure method since this does not involve any personal information such as credit card or bank account.

4.2 NodeJs Library

After the ICO Smart Contract is built, a library is required to provide all the functions related to the HKDT Stable Coin in the Ethereum Chain and it would need a lot of network communication and cryptographic functions. Building such a whole library all the way from the network layer will be time consuming. Therefore Web3 is adopted, which is a Node Core Module Library that allows the user to connect with Ethereum Network and use the service in the blockchain system. We are going to build a higher level api which uses the proposed HKDT ICO Smart Contract with the help of Web3.

4.3 React Native Application

While building the Smart Contract, Figma and Material UI will be used when designing the graphic user interface. Figma is a powerful UI design tool that can easily construct an interactive user interface and Material UI is a popular React UI Design Framework that provides common components and features that facilitate UI development.

After the UI design is confirmed, it will be implemented through React Native as the development language, because React Native allows developers to develop cross-platform applications that run on both IOS and Android with one code base. For better code management, React Redux will be used as the React Framework and would facilitate the development.

4.4 API server

To ensure trading function in the application is valid, an API server will be built for APIs required for the react native application and provide functionality of real time payment system which allow the trading between HKDT and HKD.

Also, the API server works as a third party between the trading of HKDT when users are using our application platform as trading tools. The API server will record the validated transaction in the database and handle the unhonest transaction for the HKDT market.

5 Schedule

Deliverables of Phase 1   Oct 04 2020

1. Project Planning
2. WebPage

Deliverables of Phase 2   Jan 24 2021

1. NodeJs Library
2. Application Prototype
3. Smart Contract Prototype

Deliverables of Phase 3   Apr 18 2021

1. React Native Application
2. HKDT ICO Smart Contract
3. API Server

Time Table

		Phase 1	Phase 2	Phase 3
Project Planning	Proposal	🟩		
WebPage	Webpage About FYP	🟩		
React Native Application	UI Design	🟩		
	Basic UI	🟩	🟩	
	Apply NodeJs Library		🟩	
	Balance Checking Function		🟩	
	Trading between HKDT		🟩	🟩
	Buying HKDT with HKD			🟩
	Buying HKDT with ETH		🟩	
	Selling HKD			🟩
	Providing Security			🟩

HKDT ICO Smart Contract	Trial of Smart Contract	🟩		
	ICO Smart Contract	🟩	🟩	
	HKDT ICO Smart Contract		🟩	🟩
NodeJs Library	Web3 Application		🟩	
	API server API			🟩
API Server	HKD to HKDT Trading API			🟩
	HKDT Transaction			🟩

6 References

[1] Cryptocurrency Market Capitalizations. (2020). Retrieved September 12, 2020, from https://coinmarketcap.com/

[2] What Can You Buy With Bitcoin? | CoinMarketCap. (2020). Retrieved September 12, 2020, from https://coinmarketcap.com/alexandria/article/what-can-you-buy-with-bitcoin

[3] Investopedia. 2020. *What Is ERC-20 And What Does It Mean For Ethereum?*.
[online] Available at:
<https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/>
[Accessed 27 September 2020].