DAB

Decentralized Autonomous Bank

August 3, 2017

v0.1

Tao Feng

***Abstract*—**

CONTENTS

I. INTRODUCTION

A. A Call for Monetary Liberation

A bank is a financial institutionthat pools social resources to make events. However, the existence of the bank must have its value and significance. In a way, banking system helps promote economic prosperity and assures safety of assets by pooling social wealth and resources: providing starting capitals for start-ups and entrepreneurs, at the same time generating interest for other deposit users by obtaining interest from the loan. But most business banks are regulated and controlled by central banks of authorized governments, thus rendering a hierarchical system. Moreover, traditional banks hold a large share of the profit except their employees' salaries, which should have belonged to both deposit users and loan users. Besides, People are not contented with this centralized administration because of its low efficiency and manifold restrictions. Thus, a call for balance between monetary liberation and banking functions maintenance arises.

B. Beyond an Age of Old

With the advent of new technologies, structure of the society and how it works have become to reform. The block chain technology is created to eliminate the highly centralized administrations like banks. Traditionally, banks provide two main types of service for customers:

- Deposit spare cash to obtain steady interest;
- Withdraw money from the bank account for living expenditure;
- Loan money for urgency and pay it back with extra interest.

However, the service procedures take numerous risks assessment and audit work. These complicated and repetitive operations increase unnecessary costs both in labor and in material, adding to difficulties of loaning without avoiding possibilities of bad debts. Therefore, an assumption is proposed that banking systems are transplanted on the block chain. The functions of the systems are retained, but all the profits that banks would have gained now belong to the users, thus increasing a higher deposit interest rate and meanwhile lowering users' loaning interest rates. Based on the distributed general ledger technology, this assumption needs a certain type of digital money as a substitute for real money to circulate and function. Although bitcoin is the first successfully encrypted currency, there is only one account book that records each transaction. As the currency with the largest market and community, Ethereum supports smart contract, enabling individuals to publish their own tokens on the platforms. That is what makes Ethereum the best choice for the establishment of our decentralized autonomous bank. With the emergence of block chain technology, data of transactions generated by users can be recorded more accurately, and at the same time the records on the block

chains cannot neither be modified nor be checked by anyone. To realize the decentralized autonomous bank, we transform the traditional abstract concept of "credit" into measurable units for new asset class of "tokens" that are typically issued in Initial Coin Offerings (ICOs for short) through smart contracts. Credit is an abstract concept yet a medium for banks and individuals to safely trade with each other. Yet it itself is not a tradable commodity, but an attribute of a certain individual, organization or institution. Once credit becomes measurable and negotiable GeneralizedCredit Token, a credit market will come into being and thus the value of credit will be guaranteed. Therefore, a credit-authorization-simplified yet credit-security-guaranteed banking system, a decentralized autonomous bank, DAB for short, is proposed.

II. What is Decentralized Autonomous Bank?

On platform of DAB, not only can users gain profits through depositing, but they can enjoy relatively lower interest of loaning service provided accordingly. These functions of DAB are mainly realized by a main contract and four types of tokens. The main contract contains two sub-contracts, which is responsible for depositing and loaning, respectively. As regards with the tokens, DPT (Deposit Token) is for depositing function, while CDT (Credit Token), SCT (Sub-credit Token) and DCT (Discredit Token) are collectively referred to for loaning as a joint name, Generalized Credit Token.

A. Contracts

- **Depositing Sub-Contract**: contract for deposit reserve fund for deposit user. It can automatically adjust the reserve rate of the deposit contract according to the amount of the deposit point outside the contract, and calculate the price of the corresponding deposit point.
- **Loaning Sub-Contract**: contract to deposit credit point reserve of credit users. It can guarantee the value of the credit point. The price of the credit spot calculates the price of the credit according to the reserve amount, the reserve ratio and the current amount of credit points (including the credit point, the secondary credit point and the break point). And be able to open up the credit spot.

B. Tokens

- **Deposit Token (DPT for short)**: a token in accordance with the ERC20 standard and a negotiable unit of depositing behavior.
- **Credit Token (CDT for short)**: a token in accordance with the ERC20 standard and a negotiable unit to measure users' credit and their loaning allowance. It can be cashed from the contract without any fees.
- **Sub-Credit Token (SCT for short)**: a token in accordance with the ERC20 standard and an non-negotiable secondary form of CPT when it is used for loaning. If the loaning is paid back in time, SCT will be transformed back to CRT by the depositing sub-contract; if not, it will be destroyed and users will lose the value of their credit.
- **Discredit Token (DCT)**: a token in accordance with the ERC20 standard and as alternative form of SCT when users do not have the ability or are not willing to pay back their loans. Users have to actively transform SCT into DCT through the contract, or the overdue SCT will be destroyed. It cannot be cashed, but can circulated with a certain number of fees.

C. Operations

Users have the following four operations on the platform of DAB.

- Deposit money in accordance with the depositing sub-contract. According to the contract, users deposit Ethereum into the depositing sub-contract bank and enjoys interest from it. Moreover, the deposit can be cashed at any time.
- Loan money in accordance with the loaning sub-contract. According to the contract, users can establish an Ethereum loaning agreement with an appointed user. First, users who want to loan money have to exchange their CDTs to the sub-contract bank for equivalent value of Ethereum and prepay a certain amount of interest based on their loaning time. The prepaid interest will be used for issuing new CDTs at four times of the price of ICO and then the new CDTs will be rewarded to the users who have paid the interest previously. At the same time, by loaning sub-contract, the exchanged CRTs will be transformed into equal numbers of SCTs back to the users. Finally, the users have to return the SCTs and the loan principal to the contract in a given period of time, which will trigger the transformation of SCTs back to CRTs. Besides, users gain bonus CRTs as mentioned above. But if not returned timely, the SCTs will be further degenerated into DCTs, the number of which will reduce as the time goes. The loss of DCTs means the loss of equal number of CRTs or SCTs.
- Be a guarantor of someone's loaning operation in accordance with the loaning sub-contract. According to the contract, a user can establish a new loaning agreement as a guarantor of another user who is in debt. The slight difference from the general loaning operation above is that the guarantor takes the risks.To be specific, it is the guarantor's CRTs that will be transformed into SCTs in this transaction, while the equivalent Ethereum (a net of deductions for the prepaid interest) will be given to the user in debt. Moreover, the CRT reward for retuning will be divided evenly for these two users. That is to say, the guarantor needs to secure the loaning agreement. If the user in debt cannot make an repayment in time, the guarantor shall undertake the repayment obligation.
- Found lending companies based on the third operation. If a user has adequate CDTs, he/she can offer loaning services with lower interest for other users. In this way, users in lending company can not only enjoy higher

profit than that of the depositing sub-contract, but also gain bonus CDTs in this transaction.

D. For users who loan

Users can not loan money unless they have equivalent CRTs. To obtain CRTs, one has three ways: purchase some from the market, borrow some from a friend or entrust a third party with the loaning. Unlike traditional loaning services, DAB substitute CDTs for laboursome supervision and time-consuming examination, thus lowering cost for management and interest of a loan, which is mainly dynamically determined by the market and gross lending. Annual interest rate can be close to 4% at a lower level of gross lending, and may reach 10% at a higher level. However, it does not imply that the interest rate will grow without any limits. The lending will be inhibited at two thirds of the reserve level. With the help of a friend or a third party, a user without CRTs is also able to loan: commissioning the friend or the third party to loan money for the user. This relies on a creditable hypothesis that users with CRTs is likely to gain profits using their idle CRTs. Once their friends have needs of loaning, they will be willing to help: using their CRTs to loan and paying the corresponding interest. In this way, as long as the user obeys the loaning agreement, both he/she and his/her friend or the third party can also gain bonus CRTs out of it. Compliance with credit is beneficial to all. Through these operations, circles of loaning and lending have gradually come into being, users of which pass idle CRTs on to their trusted friends. Thus, the healthy mode will eventually lead to an increase in the number of CRT issuance and loaning reserve, and a gradual expansion of the market. The market will not get too large in the presence of users' withdrawals.

III. Implementation

The realization and implementation this decentralized autonomous bank have to illustrated separately according to different stages and operations.

A. Modeling and Operations

As shown in the figure, the blue curve represents the functional relation between **Cash Reserve Ratio (CRR)** and **Negotiable DPTs**. a, b, l, d in the figure serve as parameters to adjust the shape and the position of the CRR curve (formula (4)); the purple curve represents the functional relation between **Issue Price of DPT (IP)** and **CRT Issuance Number** (formula (**??**)); the green curve represents the functional relation between **Withdraw Price of DPT (WP)** and **DPT Issuance Number Before Activation,** x (withdrawal of DPTs is limited before activation, so $DPTIssuanceNumber = NegotiableDPTs$) (formula (8). CRR(DPT, x) represents the reserve ratio of the depositing sub-contract, meaning that *users' deposits (Ethereum)* are deposited by CRR (DPT, x) into the depositing sub-contract bank and serve as the depositing reserve. Meanwhile, CRTs with equivalent value will be issued. The remaining $1 - CRR(DPT, x)$ *users' deposits* are used as the loaning reserve, issuing equivalent CRTs.

$$CRR(CDT) = 3 \tag{1}$$

$$Issue(CDT) = \frac{1 - CRR(DPT, x)}{2 * Price(Initial)} \tag{2}$$

B. Mintage and Credit

B.1) Before Depositing Sub-contract Activation: The two contracts are inactivated in the beginning. In this stage, users deposit Ethereum into depositing sub-contract to obtain DPTs and CRTs (their initial prices are 1000 DPT/ETH and 1000 CDT/ETH, respectively), and to control the deposit withdrawals, the monetary issue of DPTs and CRTs are the exactly the same. The issue price of a DPT is calculated dynamically through **formula (3)**, while that of a CRT remains unchanged. The issuance of CRT is based on the **formula (7)**. According to **formula (5)**, the reserve-loaning ratio is 3. As issuance of DPTs increases, the price of one will rise, thus tokens gained by the same amount of deposit will be accordingly reduced. With the increase in the overall issuance number of DPTs, CRR (DPT) will decrease, thereby increasing the issuance of CRTs. The issuance number of both DPTs and CRTs are calculated through the overall issuance number. In a lower issuance number of DPTs, reserve-deposit rate CRR (DPT) is high (close to *a*), the issuance number of DPTs *x* is large, and that of CRTs is small. When the issuance number of DPTs increases, the deposit reserve increases accordingly, and then the reserve-deposit rate CRR (DPT) reduces (until to *b*), the issuance number of DPTs decreases, and that of CRTs increases. The blue curve in the figure represents the change in CRR(DPT) as the overall issuance number. The green curve represents the change in the price of a DPT as x changes. When $x = x_0$ DPTs are issued, the area bounded by the blue curve, the x axis, the y axis, and the line $x = x_0$ represents the reserve in the depositing sub-contract, and the current DPTs issuance ratio represents the instantaneous reserve rate at $x = x_0$. The area of the blue curve, the $y = 1$ axis and the line of $x = x_0$ represents the reserve fund in the loaning sub-contract. The reserve-loaning rate is 3 (more than 1), so when issuing CRTs, each ETH into the loaning sub-contract corresponds to $\frac{1-CRR(DPT,x)}{3Price(Initial)}$ CRTs. But in order to ensure the issuance of CRTs, **formula (7)** is set as the implemented regulation of CRTs issuance. Before activation, users purchase each DPT at a lower price earlier yet they gain less CRTs as well, while users who purchase later have to cost more on each DPT yet they gain more CRTs than the early birds . Hence, depositors benefit no matter they are an early participant or not.

B.2) After Depositing Sub-contract Activation: There are only two stages, which are before the activation and after of activation. Commonly, the contract has no termination. The contract can continue to issue new CRTs and DPTs when the deposit are allowed to be withdrawn. The profit of issuing new DPTs and CRTs is larger as long as no DPTs is left in the deposit sub-contract. But this does not imply that users can issue new tokens as they wish, for the withdrawal behavior will not exchange all he DPTs in the contract. This rule can

prevent the issuance of unnecessary new DPTs and CRTs. The issuance number of DPTs is entirely determined by the market, which has no upper limit. Once a DPT is issued, it can not be destroyed. The green curve in the figure is the relationship between the price of DPT and the issuance number of it before activation. In order to suppress excessive market deposits, the price of DPTs increases slower and even decreases as the issuing price increases. The amount of each single deposit and withdrawal has its maximum limit, and higher fees for higher amount of deposits or withdrawals are set to avoid malicious behaviors by some users. The price of withdrawing CRTs is commonly a fixed value, in which $CRR(CDT) = 3$.

$$Balance(CDT) = 2 * Supply(CDT) \tag{3}$$

In formula (3), the reserve for CRTs is two times the amount of its issuance. The issuance of a CRT is mainly accompanied by the process of mintage. But a CRT can be destroyed when users who hold CRTs by simple cash withdrawals or violating the contract. New CRTs can also be issued when the loaning operations expand. A complete loaning and successful transaction will reward CRTs equivalent to the value of a quarter of interest prepaid at the initial issuance price back to the user who obey the contract, after returning the principal and interest.

C. Depositing and Withdrawal

C.1) Before Depositing Sub-contract Activation: Before the contract is activated, any cash withdrawal operation can not be satisfied. But the transfer operation of DPTs are not restricted.When the issuance number of DPTs exceeds the Issuance activation limit *l* or the projected activation time is up, users can withdraw their DPTs to cash.

$$CRR(DPT, x) = a * \frac{1}{1 + e^{(\frac{x-l}{d})}} + b(0 < b < a < 1) \tag{4}$$

$$Price(Initial) = 1/1000 \tag{5}$$

$$IssuePrice(DPT) = \frac{1}{CRR(DPT, x)} * Price(Initial) \tag{6}$$

$$Issue(DPT) = IssuePrice(DPT) \tag{7}$$

Before the activation, anyone can deposit within the upper limit 1000 ETH, which ensures the stability of DPT's price and the CRR(DPT) not to change dramatically. In this way, the situation where users benefit from large withdrawals afterwards are avoid. The issuance price of DPTs is calculated in accordance with the formulas above. Small impact on CRR of each transaction ignored, the larger a single deposit is (within the limit), the greater the user can benefit.

C.2) After Depositing Sub-contract Activation: After the activation, user can withdraw the tokens into Ethereum immediately. Each withdrawal operation will transfer the corresponding DPTs to an address in the contract. As long as there are some DPTs left in the contract, other users who deposit will first use those DPTs instead of issuing new ones. The projected activation time is two weeks long. Once the deposit reserve is higher than $l + 2 * d$ within two weeks, the sub-contract will be immediately activated. If the reserve does not reach $l + 2 * d$ but l within two weeks, the contract will be activated as projected. If the reserve does not reach l but $l - d$ within two weeks, the activation time will be extended another two weeks. If the reserve is less than $l - d$, that means the contract activation fails and a refund interface will be opened for users to redeem their initial capital (through a non-negotiable record called **Issuer Token**, either for refund after the activation failure or as commemorative coins after success). Once the activation succeeds, the contract runs on line. The price of DPTs withdrawal is calculated by formula (8. x represents the negotiable numbers of DPTs, which equals the subtraction of the issuance number of DPTs and the number of DPTs in the contract. The price fro withdrawal is always lower than its issuance price so as to protect the interest of all the depositors from excessive dilution of the depositing reserves.

$$WithdrawPrice(DPT) = \frac{Balance(DPT)}{Supply(DPT) * CRR(DPT, x) * Pric} \tag{8}$$

C.3) Mechanisms: After the activation, mechanisms for calculating the price of depositing and withdrawing DPTs are as followed: Under Sufficient DPTs Principles and Rules The price of a DPT is expected at a rather higher level in calculation so that users get less DPTs than they do in reality. The market price of a DPT after depositing behavior should be slightly lower than that when depositing in calculation. The price rises after depositing behavior, so $Price(Low) = Price(Before)$;$Price(Before) < Price(After)$; reserve increases; reserve ratio drops. The difference between the calculation value and the real value of CRTs users gaining acts as fees for all the CRT holders. Procedures

- Assuming that a user deposits d ETH: $Deposit(Max) = \frac{d}{Price(Low)}$, calculate the maximun DPTs are needed for the depositing users.
- Calculate the amount of the reserve after depositing: $b + d$.
- Calculate the minimum reserve ratio: $f(s + Deposit(Max))$, among which s represents negotiable DPTs outside the contract.
- Calculate the maximum price of a DPT: $Price(High) = \frac{b+d}{s*f(s+Deposit(Max))}$.
- Calculate the actual price: $Price(Actual) = Price(High)$.
- Calculate the actual number of DPT for depositing users: $Deposit(Actual) = \frac{d}{/fracb+ds*f(s+Deposit(Max))}$.

Under Insufficient DPTs Principles and Rules When the deposit point in the contract is not enough. It involves not only the deposit, but also the status of the contract entering into the state of specie and credit after the remaining deposit points in the contract have been used up. So the entire deposit of the ether workshop is divided into two parts, considered separately. For the remainder of the deposit point in the exchange contract, the principle is that the price of the deposit point is calculated as high as possible, and that the portion of the funds used by the user for the deposit will be less than the actual amount. This part of the calculation is consistent with the deposit point in the contract. Therefore, the price of the deposit point after the user deposits should be slightly lower than the price of the deposit point calculated at the time of deposit. After the user deposits, the deposit point price increases, so the $Price(Low) = Price(Before); Price(Before) < Price(After);$ reserves increase, and the reserve ratio drops. However, a portion of the user's funds will be used for specie and credit. The user receives less than the actual point of deposit, as a fee and a mint fee paid to all deposit point holders and developers. Therefore, the opposite question of the original question is that the remaining deposit points in the contract can reach at most how much the user will deposit in the etheric square. Then, through the user's actual savings, the portion of the money that is offset from the deposit point is the etheric square where the user should be used for coins and credits. On the one hand, coinage increased reserves, on the other hand lowered reserve ratio, but also increased the amount of deposit point circulation. Therefore, the impact of the middle is very complex, when the deposit point circulation is very large, the reserve rate is not obvious, but the growth rate of circulation is unchanged, so the behavior of coinage reduces the price of the deposit point instead. The location of the change is somewhere around (l+4d). This mechanism rapidly diluted the value of the deposit point, and also rapidly increased the total amount of the credit reserve fund, and to some extent inhibited the market over coinage and credit. The deposit point will be higher than the issue price of surplus exchange deposit contract in deposit price point, because many coins with credit, but the user may face higher the fee (deposit and credit points, each pay 30% of the fee).

Procedures

- At first, the contract did not know whether the deposit point was adequate, so it was assumed that it was sufficient. By using the method described above, $Deposit(Actual)$ is calculated to be in the current calculation if it is greater than the remaining deposit point sin in the deposit contract.
- By the initial calculation, we know how much DPT can be increased. $Deposit(Max) = Deposit(Actual)$, because in fact, the higher the cost of coinage, so in fact, the deposit point circulation increased less than $Deposit(Max)$.
- Calculate the largest deposit reserve: $b + d$.
- Calculate the minimum deposit reserve rate: $f(s + Deposit(Max))$.
- Calculate the maximum price of the deposit point: $Price(High) = \frac{b+d}{s*f(s+Deposit(Max))}$.
- Most of the users in the calculation Ethereum: $Price(High) * si$.
- Calculate the surplus should be used for coins of the ether workshop: $d - Price(High) * si$.
- If the square of the coin used is less than 0, the contract has not crossed the gap of the coin, and the remaining deposit point in the contract is given to the user. If it is greater than 0, the new deposit point and credit point are issued to the user by using the coinage method. The user gets the credit points of the $si + Issue(DPT, d - Price(high) * si)$ and $Issue(CDT, d - Price(High) * si)$.

D. Loaning and Repaying

D.1) Before Loaning Sub-contract Activation: The projected activation time of loaning sub-contract is due at the end of the second week after the activation of the depositing sub-contract activated. Before the activation, neither CRTs can be withdrawn, nor loaning behaviors are allowed. But the transfer behavior of CRTs is not restricted. When the loaning subcontract is successfully activated, users can immediately withdraw their CRTs and conduct loaning operations.

D.2) After Loaning Sub-contract Activation: After the activation, the number of tokens in the depositing subcontract basically meet the demand of the market, so the loaning operations can then be allowed to conduct by users. On the one hand, CRTs can be withdrawn into Ethereum from the loan contract. On the other, loan of Ethereum can be obtained by pledging CRTs from the loan contract. By withdrawing, CRTs will be destroyed and the negotiable number of it decreases. By loaning, users enjoy relatively lower interest rates and meanwhile gain bonus CRTs. Certainly, if a user exceeds the repayment time, the collateral credit point will be destroyed at a certain rate. Even if the user returns the principal and interest afterwards, he/she can not get the same number of CRTs as he/she owned before.

ACKNOWLEDGMENTS