# Decentralized Autonomous Bank (DAB)

# Abstract

# Introduction

## A Call for Monetary Liberation

A bank is a financial institution that 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.

## 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:

1. Deposit spare cash to obtain steady interest;
2. 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 Generalized Credit 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.

# What is Decentralized Autonomous Bank?

On platform of DAB, not only will users gain profits through depositing, but they can also enjoy the relatively low interest of loaning service provided accordingly.

These functions of DAB are mainly realized by the following main contract and four types of tokens, which are DPT (Deposit Token), CDT (Credit Token), SCT (Sub-credit Token) and DCT (Discredit Token). Among those, the main contract contains two sub-contracts, which is responsible for depositing and loaning, respectively. As to tokens, CDT, SCT and DCT are collectively referred to as a joint name, Generalized Credit Token.

## Contracts

* Depositing 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 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.

## 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.

## Operations

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

1. Deposit money in accordance with the depositing contract. According to the contract, users deposit Ethereum into the depositing sub-contract and enjoys the interest from it. Moreover, the deposit can be cashed at any time.
2. Loan money in accordance with the loaning contract. According to the contract, users loan Ethereum from a certain user via the loaning sub-contract. First, users who want to loan money have to exchange their CDTs to the contract for equivalent value of Ethereum and prepay a certain amount of interest. The prepaid interest will be initiated as new CDTs which have four times of the price of ICO and then 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.
3. Be a guarantor of someone's loaning operation in accordance with the loaning contract. According to the contract, a user can establish a new loaning agreement as the guarantor of another user who is in debt. The slight difference from the general loaning operation is that the guarantor takes the risks. In this transaction, it is the guarantor's CRTs that will be transformed into SCTs, and 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 to the 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.

# Implementation

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

## Mintage and Credit

### 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 an CRTs (the 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 accordinglly 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 X0 DPTs are issued, the area bounded by the blue curve, the X axis, the Y axis, and the line X=X0 represents the reserve in the depositing sub-contract, and the current DPTs issuance ratio represents the instantaneous reserve rate at X=X0. The area of the blue curve, the Y=1 axis and the line of X=X0 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 (1-CRR(DPT，x))/(3\\*Price(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.

### 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) (8)

In the **formula (8)**, 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.

## Depositing and Withdrawal

### 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.

Formula

CRR(DPT, x) = a\\*1/(1+e^((x-l)/d))+b (0<b<a<1) (1)

Price(initial) = 1/1000 (2)

IssuePrice(DPT) = 1/CRR(DPT, x)\\*Price(initial) (3)

Issue(DPT)=IssuePrice(DPT) (6)

Before the activation, anyone can deposit within the upper limit 1000ETH, 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.

### After Depositing Sub-contract Activation

合约顺利激活后，合约上线运行。**存款点的提现价格通过公式（4）计算。x是存款点的流通量，即存款点的发行量减去存款合约中的存款点的数量。**可以发现，存款点的提现价格始终低于存款点的发行价格，这个价格差是为了保护所有已经持有存款点的人的利益，避免存款合约中的储备金被过度稀释。

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 lwithin 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 (4)**. 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) = Balance(DPT)/(Supply(DPT)\\*CRR(DPT, x))\\* Price(initial) (4)

## Loaning and Repaying

### 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.

### After Loaning Sub-contract Activation

通过贷款的方式使用信用点，用户享受较低的利率获得贷款，同时在一个贷款周期内通过额外支付一定的利息可以没有损失的赎回信用点。如果用户超出还款时间，那么质押的信用点就会按照一定的速率被销毁，用户即使再还上本息，也无法获得与质押前一样多的信用点。

After the activation, the number of tokens in the depositing sub-contract 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.

Generalized credit points are divided into three types: credit point, secondary point and break point. The user gets credit and credit loan contract is equal to the number of points from the etheric square, is the credit loan ratio is 1:1, the user selects a different way of loan, the first half period, one year, pay different rates of interest. Pay the interest according to the credit of four times the issue price of the issuance of new credit to users' (if the user as lenders, to the user; if the user as a guarantor, the new credit points to the guarantor and the guarantor).

There are two main forms of borrowing.