Digital Demand-Supply Network: A New Implementation of Value Exchanging Platform and Decentralized System

Leo Y.C. Liu

leo19900723@gmail.com

2018/5/2

Abstract. Since the very first Bitcoin service has announced and activated from 2009, the whole environment called blockchain has been discussed and modified for many purposes. This system revealed a new page of human history to reconsider the possibilities of digital currency. However, the design of Bitcoin is too narrow and impractical for the long-term future. One of the most major problems of Bitcoin algorithm is that it lacks the most fundamental view of economic knowledge and it cannot change the financial system of the whole world. Our new design, on the other hand, perfectly solve the economic problem of humans. Digital Demand-Supply Network is designed to retire every monetary structure on this planet based on the belief that every asset or commodity must follow the very rule of demand-supply chain and the elementary equation: PQ=VM. The data structure must follow three major rules: decentralized, distributable, reclaimable. The whole system must serve one solemn purpose- transacting values and make this procedure convenient. We introduce a new system structure, focusing on redesigning the data structure and providing a new method of calculating the cryptocurrency. As to the data structure, an Account-Wise Ledger structure, which features account-oriented attribute, is revealed in order to achieve decentralized, distributable, and reclaimable. Replaced the Gold-Mining algorithm with the Job-Hiring program issued by any nodes to alleviate the waste of CPU time and the natural energy. For the values exchanging, we introduced the concept of UPN, which provides the very unique number for every commodity, including money. Everyone can document all of their own goods, assets, and money on DDSN. Through the power of the UPN and Account-Wise Ledger, one can have his or her own assets list online completely. Everyone can trade his or her own goods anywhere and anytime. The system has built-in monetary policy algorithm, which uses the deposit rate and lending rate to prevent the unreasonable money-issuing problem also works as an incentive to every participant. The monetary policy algorithm, which based on the demand-supply evaluation model, the network itself, through neural network technology, can balance the inflation and deflation phenomenon by calculating factors within a single task. The purpose of this research is ensuring the permanence and the acceptability of value transaction via cyber-based coin. Independence, freedom, low cost, justice, and more importantly: an easier way to exchange values are the contributions that we will implement in this theory. The Digital Demand-Supply Network is not just a cryptocurrency system, it is the most fundamental structure of value exchanging platform on this planet.

Keywords: decentralize, blockchain, distributed ledger, cryptocurrency, exchange rate, neural network, inflation, deflation, value exchange

1 Introduction

The Bitcoin service has been established almost a decade. Myriad discussions, theses or even imitations announced to show how popular it is. The main idea of the invention of Bitcoin is using a completely new data structure called blockchain to solve the double spending issue with decentralization financing network [1]. This approach, however, has its new problems: how to issue the money fairly, how to evaluate the true price of Bitcoin and how can cryptocurrency, like Bitcoin, be accepted by the real world financial community? A recent study has indicated that the dramatic fluctuation of Bitcoin has been the tremendous obstacles to the real-world financial community to accept cryptocurrency as genuine exchange medium [2]. Another study has confirmed that the exchange rate of Bitcoin has the positive reaction to the real world economic indicator, such as GDP, inflation and interest rate [3]. In addition, the same research has confirmed that the total number of Bitcoin in use and transaction would influent the exchange rate of Bitcoin. This conclusion has indicated that a new cryptocurrency system can be designed more stable by using factors as the volume of how many coins that the network issue and how the system reflect its own earning capabilities. The more stable financial environment that the cryptocurrency is, the more acceptable for the financial group in the real world.

Another flaw of current Bitcoin network design is the principle of proof-of-work. By original design, the proof-of-work was designed as mainly incentive to participants in the network to help complete the money transaction. Also, such design was the only approach to issue the money. There are many related problems have come out. First, a fixed principle of money issuing would lead to great inflation or deflation of money value. Second, by the greedy mind of humankind, every participant would do his or her best to solve the proof-of-work mathematic puzzle in order to gain the block generating reward. This “greedy action” may lead to great energy wasted on our planet with no actual contribution to our society. In April 2018, the latest power consumption of

Bitcoin mining is 62 TWh per year globally and the trend is still climbing[1]. The problem of how to change this wasted activity to a true value exchange chain is the main purpose of this project.

The blockchain, as its design, is a distributed ledger, which contained every money transaction record in a single, giant data chain. Such design, which depends on the owner's private key that mainly is used to sign every transaction, would have one major flaw: the private key is generated randomly, failing to reclaim the account if loss of private key such as the malfunction of owner's hard drive [4]. In order to prevent such tragedy, an account based new structure is a requisite. Also, we combine the biometric info of an individual such as fingerprint as private key and account name to ensure that one may have extremely low possibilities to lose his or her money.

The problems mentioned above regarding the Bitcoin and blockchain are all tiny. The most crucial flaws of this design are that it lacks the most fundamental knowledge of economic and it cannot change the environment of the finical world. The reason is clear and simple: the design of Bitcoin cannot allow people to exchange values directly. Namely, the Bitcoin can only record the transaction of digital currency. However, this design cannot record the exchange of every valuable asset, like people's properties or even knowledge and labor resources. In our new design, we considered this problem as our solemn target. A new value-concerned platform must be revealed.

Digital Demand-Supply Network (DDSN in short), which is our new design, serves only one purpose with three major rules: an online system can transact the values of everyone with a decentralized, distributable, and reclaimable data structure. In order to achieve this goal and solve many flaws that the original blockchain had, we introduced the concept of UPN (Universal Permanent Number), invented by Hugh Ching [5], as the very base of our monetary system. To be more specific, UPN has the power to give every commodity, including money, a unique number. By the power of UPN, everyone can digitalize his or her assets, all with unique UPN. People can trade any good, including houses, cars, even their knowledge, services, and labor resources, that they had anywhere and anytime. DDSN served as a new value-centered system, which is far beyond the concept of simple cryptocurrency.

The DDSN provides a new data structure: Account-Wise Ledger. The Account-Wise Ledger can restore everyone's transaction record, ordered by every individual account. By the power of Account-Wise Ledger, the whole data structure can be divided, distributed, and decentralized. Every member of the community has to restore some parts of the whole data only. The average data usage of each individual can be controlled under a specific amount. The design of Account-Wise Ledger can solve many potential

[1] The data is calculated and emulated by Digiconomist: https://digiconomist.net/bitcoin-energy-consumption

fraud issues, including double spending, sender and receiver collusion, and 51% attack. The solutions we put into DDSN and the new technique that we utilized lead the system to become a stable, trustable, and independent value exchanging platform.

2 Account-Wise Ledger

The traditional blockchain is designed as a single line that contains every transaction between different nodes. The blockchain needs to be fully copied to every participant to ensure the validity of the whole system. Every individual can acquire his or her remaining balance and transaction history via browsing the whole chain. The blockchain cannot be broken and modified (except adding new entity). This design may lead to data booming problem that the whole blockchain may be too large to be stored by any individual. Rather than mix everyone's transaction data together to form the blockchain, we categorize every transaction by account, which we called it as the *account-wise ledger*. A single ledger could be a huge block that contains basic info of the account and the blockchain of transactions that only related to the specific account. A basic ledger would at least contains following info: account number, private key lock, transaction chain, latest-operators' signature.

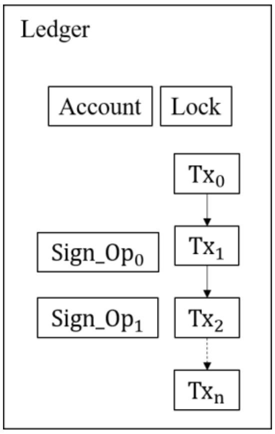

Figure 1 Basic Ledger Structure

This account-wise ledger design allows every individual to acquire his or her transaction history much faster and more efficient than original blockchain designed. Furthermore, every ledger is an isolated unit which can be stored by "some" members of the network (node) rather than "every" node compared to the traditional designed. Every ledger can be treated as an indivisible atom though may have different size due to the different amount of individual's transaction history. Because of this separated atom-liked attribute, nodes can be grouped respect to the system design also; every ledger can be grouped and stored by different sets of nodes, which means the environment may allow every node not to have a full copy of entire data. Through this ledger design, the whole internet can perform as a huge, RAID-like system, which allows an individual node can save more space compared to traditional blockchain design and make a single account to be reclaimed possibly.

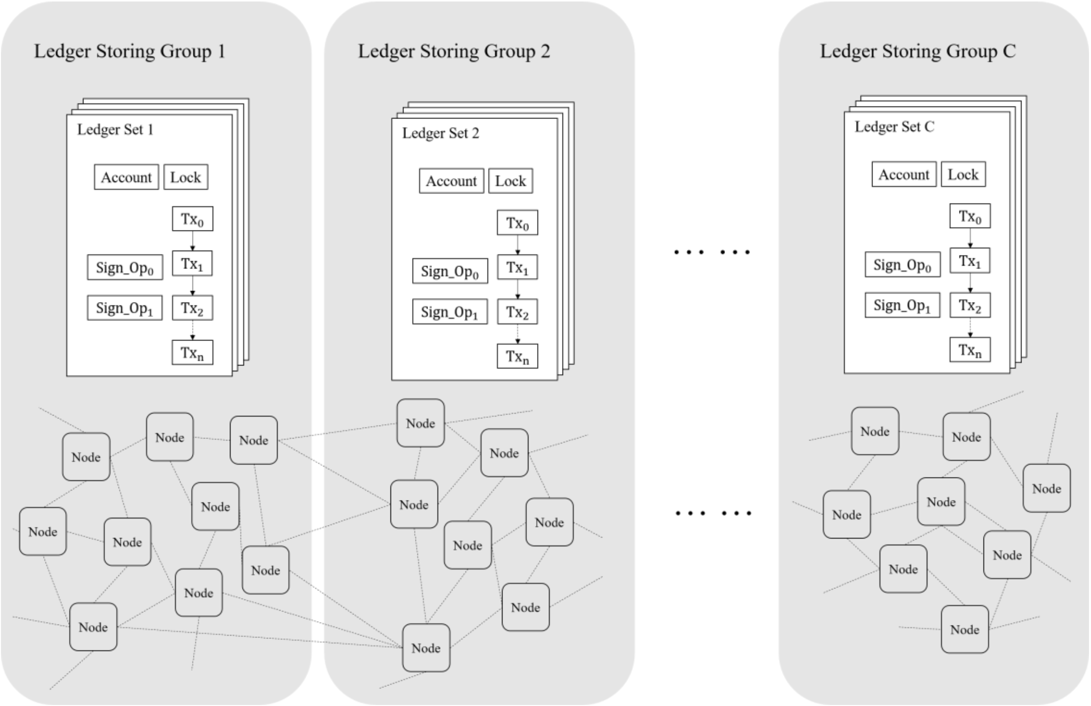

Figure 2 Separated Storing Model

To be more specific, set a network has N nodes and there exist M accounts (the numbers of total ledgers is equal to the numbers of existing accounts, which is M in this case). Also, set C as the numbers of groups of nodes. The numbers of nodes of every sub-set should be $\frac{N}{C}$ and the number of distributed ledgers that a single sub-set member has to store should be $\frac{M}{C}$ which means account-wise ledger design would cost less disk space to a single node compared to the traditional one. Furthermore, the possibility P of complete data loss from the whole environment should be $P = \prod_{n=0}^{\frac{N}{C}} Q_n$, where Q is denoted as the possibility of a single crash; $0 \leq Q \leq 1$. If the number of sub-set nodes is large enough, the possibility P would be extremely small which means the larger the network is, the more secure the environment should be.

The RAID-like system can also be dynamically distributed by network automatically. For instance, a single ledger storing group can detect the disk space usage of every node to determine whether the ledger storing group need to be divided into two separated sub-ledger storing group or not. The usage of the disk space of a single node can be controlled under a certain limited number.

2.1 Transactions

To fit the new account-wise ledger structure, the transaction algorithm must be modified. First, we canceled the mining rule, which means there will be no block-creating bonus at all. The only incentive of block creating is the transaction fee. The reason for setting such rule is trying to reduce the waste of CPU time, unfair and/or meaningless competition and energy. Therefore, the encryption difficulty, whose primary object is preventing the DDOS attack, info spam, and Byzantine Generals' Problem, of the block hashing would be limited under a certain level. Base on this design, there will be no miner anymore. Instead, because the job of creating blocks is making the transaction actually happened, like a role of the bridge, we prefer to call those block creator as an *operator*.

Secondly, to initiate the transaction task, similar to Nakamoto's method [1], the sender needs to create a transaction instruction called the *action* with his or her digital signature, asymmetric encryption of hash of action and the sender's private key. Once the creation of transactional task is done, the sender needs to broadcast the task to the network's task chain to wait for any operator. The operator who accepts this task needs to check: 1. Using sender's account (public key) to verify the validity of the task. 2. Check the sender's balance through his or her ledger's transaction chain to verify whether he or she is qualifying to proceed such transaction or not. After the check, the operator will create the transaction block for sender and receiver then the job may consider as complete.

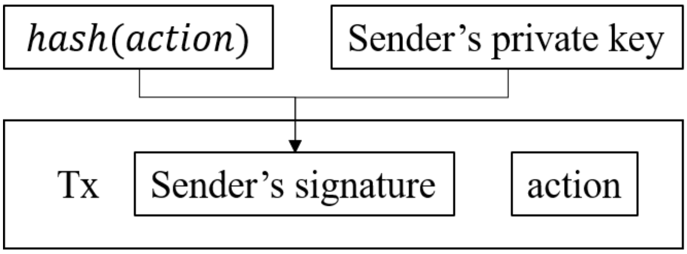

Figure 3 the structure of the transaction task block

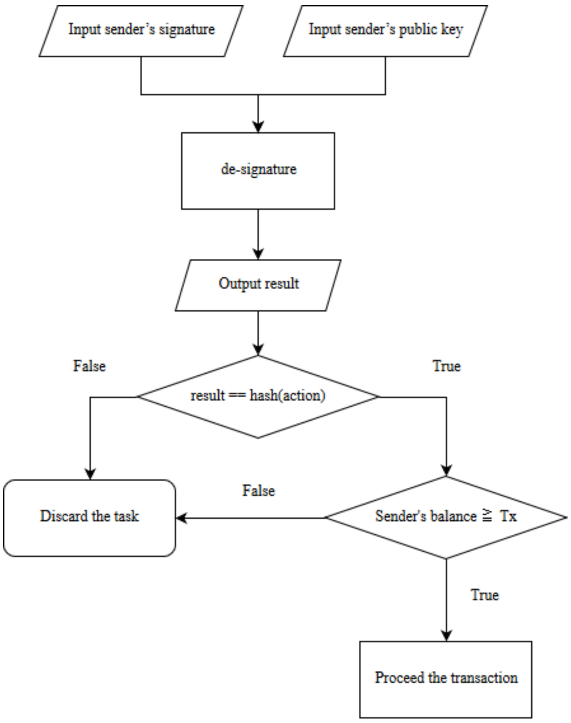

Figure 4 the diagram of task validation

After the task verification is determined as valid to the operator, due to the distributed storing feature of account-wise ledger system, every single transaction of the money sender to the receiver need to be created twice for both sender's ledger and receiver's. The operator creates a sender side block, which includes the previous hash of sender's transactional block and the hash of task block, and a receiver side block, which includes the previous hash of receiver's transactional block and the hash of sender's transactional block, simultaneously. To simplify the block, the transactional request can only be asked as a one-to-one model (one sender versus one receiver). If there has any request need to perform as one-to-many, the system will separate this single task as many one-to-one tasks. Once the transaction complete, the operator will sign the sender's and receiver's ledger and tag the task chain as completed by the operator.

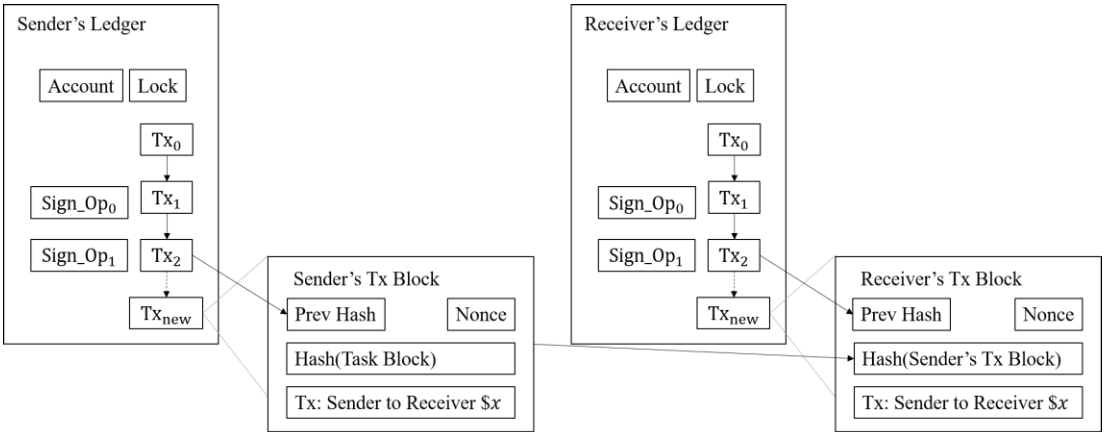

Figure 5 new transactional bock creation

2.2 Task Chain

The task chain is a data storing method which mainly contains every transaction request that any sender initiated. Task chain is a simple blockchain design that waits for operators to handle. Everyone in the network might have a 100% full copy of task chain to make sure that everyone can recognize the same environment. The problem of the task chain versus the account-wise ledger is that if the task chain is designed as one chain, mix with everyone's request, the operator may not determine which task can or cannot handle due to some network delay. Therefore, task chain designed should be changed to an account-oriented structure as well. To be more specific, a single sender announces his or her sending request by creating a task block which contains the latest block's hash info of his or her own task chain to the network. Once the task has handled by operators, operators will tag the specific task block (we called the action as the *handling tag*) that he or she just handled and broadcast to the network.

The duplicate works problem may occur due to some network delay which is some operators may work on the same task block because he or she has not detected the handling tag by someone else yet. In order to solve this issue, we introduce a function named *operator-signing principle*. As many formal tasks have been performed in the real world, the one who in charge of task solving needs to sign his or her name in sender's and receiver's ledger in order to prove his or her work. The tricky part of this principle is that the action "signing" is not performed by the operator itself. Once the block is created by the operator, the operator needs to send back to the sender to ensure the content of transactional action is match with the task required. If correct, the sender will sign the operator's name (account/public key) in his or her own ledger, and then broadcast to the whole network to approve the work. For the receiver side, the receiver will match the operator-signature, broadcast by the sender, and the operator's name. The operator-signing principle asks that a single transaction should be signed by two different operators at least when the task is considered done, but the principle does accept more than two operators as an endorsement. Actually, the more endorser of a single transaction, the more security that the network would be. The transaction fee will be distributed with an equal amount to every operator.

Since the task chain is designed as account-oriented too, it should be no "the longest path to solve the forking path" problem. The transaction request must have its "queuing attribute" which means that none of any two or more transactions can be asked for exactly the same time. If an operator discovers any transactional task chain forks exist, all of the task blocks, attached in forks, will be dropped and reported as fraud.

Task chains can compress or wipe out some old, handled histories in order to save more disk space because the transaction can be recognized as formal only by tracing sender's and receiver's ledger. However, the task chain still needs to keep at least a consistent amount of blocks to prevent attackers to recreate a dishonest chain.

2.3 Reclaiming Account and Privacy

Every member needs to remember his or her account in order to reclaim his or her balance info. To prevent and lower the risk of lost account, every member would be asked to use his or her biometric data, such as fingerprint, as a private key. The account, which is a public key, can be generated from the private key through a certain function. Once an individual changes his or her devices, facing the hard drive broken tragedy or else, a certain individual can log in with his or her fingerprint info. The working flow would be: 1. The devices will use the transferring program to gain the account through biometric data. 2. The devices will start to join the network, ask for the copy of task chain and ledgers. 3. The devices will match the individual's account (public key) from the network, which stored by other members, to reclaim the transaction and balance.

Since nearly everyone has a full copy of others' ledgers, the ownership is not determined by who has such ledger's copy but by who has an authority to initiate a transactional task, as a sender, from such account. The problem can be solved by the transactional task designed that described in section 2.1 Transactions: the sender needs to create a transaction instruction called the action with his or her digital signature, asymmetric encryption of hash of action and the sender's private key that is derived from user's biometric info. Accordingly, the only one who has the private key has such authority.

Although the whole system became the account-wise structure, the anonymous attribute has still remained. Everyone can only realize that a certain account tries to transfer his or her money to another one. None of any can actually know who they truly are in real life. Furthermore, as account-wise ledger design, we can do much more than anonymous. We treated any ledger as a huge block or object which allow us to implement some object-oriented interfaces to ensure the data privacy. For example, we can only provide *account.checkAffortable(taskBlock)* Boolean function for operators to check whether a certain sender can afford the transaction or not without allowing any operator to browse every transiting history. On the other hand, only the person who has private key can use *account.getBalance(privateKey, taskBlock)* function to claim his or her full details of the balance.

3 Environment Economic

A cryptocurrency, in some point of view, is a true currency that has its own exchange rate against other currencies. As long discussions, bitcoin kind of cryptocurrency cannot be accepted by the real world financial group due to its tremendous fluctuation and hardly evaluation [2]. In our theory, we are not presenting a valuation model but the policy that slightly controls the interest rate of cryptocurrency and the true value in every customer's mind.

3.1 Proof-of-Work

According to the traditional cryptocurrency system, the only way that issue the money is releasing currencies by miners who dedicated themselves to solve the proof-of-work, a series of mathematical puzzles. The policy worked perfectly in the beginning. However, as the inherently greedy nature of human being, more and more miners did their best to build better computers in order to triumph others and gain the cryptocurrency reward. The situation even getting worse that many resources, money, equipment and human resources, were clustering together to build up more powerful mining factories named mining pool [6]. As more and more nodes clustered together to get powerful calculating abilities, some of these mining pools become majorities of Bitcoin network, making the whole Bitcoin network vulnerable under the threat of so-called 51% attack [6] [7]. Even though many previous studies tried to increase the difficulty or disincentive to lower the interest of the mining pool, the situation can only be called as being "alleviated" but "annihilated" by the method.

Trying to solve the inherently greedy nature of humankind is nearly impossible to everyone, therefore we need to change the policy. Increasing the difficulty is not fine enough; we plan to remove the mining-reward policy entirely. The only benefit of transactional block creating is transferring fee. This situation is perfectly fitting with the real world model and the post-Bitcoin era.

However, it does not mean that we canceled the original proof-of-work policy entirely. Instead, we lower the difficulty of proof-of-work calculating through the number of zero that the system required as valid. The new difficulty may cost a computer, generally, one to two minutes to find the result. This basic requirement may, at least, prevent the DDOS attack, info spam or hacker, and Byzantine Generals' Problem.

3.2 Money and Universal Permanent Number

A rational economy needs a rational money system. The invention of UPN (Universal Permanent Number) based on completely automated UPS (Software). All the current money types are not really suitable for permanent money, which is guaranteed to last permanently, even when governments or even the earth perish. The best example of permanent money is gold, but the fatal defect of gold to be used as money is its limited supply, while UPN is unlimited, controlled by the monetary policy algorithm that the DDSN had. Fundamentally, Money must satisfy three conditions:

1. $\mathrm{PQ} = \mathrm{VM}$ $(\mathrm{Price} \times \mathrm{Quantity} = \mathrm{Velocity\ of\ Circulation} \times \mathrm{Money\ Supply})$,
2. $\mathrm{Rate\ of\ Return} > \mathrm{Interest\ Rate} > \mathrm{Inflation\ Rate}$, and
3. Have permanent intrinsic value.

For example, fiat money can satisfy 1 and 2, gold can satisfy 3, and only UPN can satisfy 1, 2, and 3 [5]. Since the most solemn purpose of this research is to establish a new system which allows everyone exchanges their asset or value without barriers. We use UPN for two functions: 1. a special sequence of UPN acts a role as genuine money. 2. other sequences of numbers are treated as a unique ID for every good that registers into DDSN. The power of UPN allows everything to be documented. People can set any price for their asset and host an audition for the goods that they want to sell through the DDSN.

The usage of UPN denoted to genuine money and goods has fundamental benefits that traditional cryptocurrency would never have: everything in this world is exchangeable. Everyone's asset, no matter cars, houses, clothes, or even labor resources, can be opened to sell online. The price details and the ownership of every good can be recorded in the Account-Wise Ledger related to every single person. By tracking the transaction chain that the specific person had, one can realize the total money and assets that the person had. Thus, the Digital Demand-Supply Network is not just a cryptocurrency system, it is the most fundamental values of exchanging platform on this planet.

3.3 Monetary Policy

Without block-mining reward, the alternative way of issuing money will be, in our design, set as giving a certain amount money when an individual register his or her account at the very first time, we called it as a *beginning deposit*. The reason for our policy, according to Federal Reserve Act Section 16[2], is that if an organization try to

[2] Federal Reserve Act Section 16. Note Issues:

issue its own money, it should have correspondent physical assets to support the action. However, as to the decentralized cryptocurrency network, there is no centralized, government-like, authority to hold an amount of physical asset to ensure the monetary issuing. Therefore, we assume that every individual's personal asset can act as his or her voucher. Therefore, the next problem would be how to set the amount beginning deposit. According to the online statistic service, provided by Statista, the average purchasing price of the personal computer is 629 U.S. dollars in 2017[3]. We assumed that the initial exchange rate of our cryptocurrency to U.S. dollar should be nearly 1:1. Also, we assume that any individual, who joins our network, has one personal computer at least, regarding as the first investment to the network. Base on the assumption above, our system will give 600 coins as a beginning deposit.

The value of a currency should be dynamic. Different from the real world money, without centralized government, there is no robust, specific connection between cryptocurrency and real-world money. Every participant, however, as a blood-flesh genuine human being, can realize the true value of cryptocurrency currently. To be more specific, one can realize the true value of cryptocurrency through participants' behavior. As a simple demand-supply model, the price of goods in a certain market will come to equivalent when the demand and supply curve cross with one single point [8]. Base on this policy, our system can calculate a situation that, with the same type of good as index, if the price of equivalent point rises through times, the system may consider the situation as inflation; on the other hand, if the price of equivalent point falls, the system may consider the situation as deflation. The whole system can only accept 3% price grow or down within a year. If the equivalent point goes beyond the limitation, the system will initiate the interest rate control to ameliorate the phenomenon. The system will use the average price of the whole past year as a new standard price for the following year on Jan 1st.

https://www.federalreserve.gov/aboutthefed/section16.htm

[3] Statista's study: Average selling price of personal computers (PCs) worldwide from 2015 to 2019, in actual and constant currency (in U.S. dollars) https://www.statista.com/statistics/722992/worldwide-personal-computers-average-selling-price/

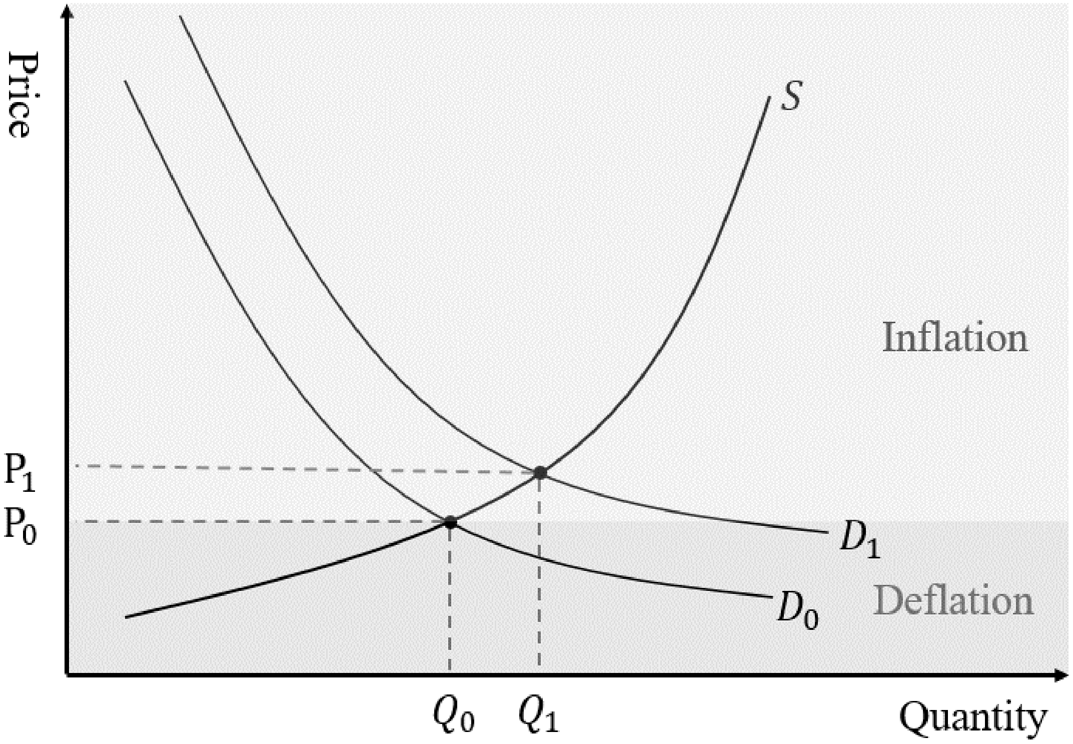

Figure 6 A simple demand and supply model

To implement the interest rate control, without a central government, only three rates that the system can use as controlling factor: transaction fee, deposit rate, and lending rate. First, to ensure the operators' incentive, the transaction fee will be set as fix payment for operators (3 coins, share by every operator for a single transaction). To the sender side, however, transaction fee can be dynamic in order to control the inflation or deflation situation. For example, if an inflation situation occurred, the standard transaction fee may increase by the system. The difference between new transaction fee and three coins that operators receive will "evaporate", vanishing from the whole network entirely to decrease the total amount of circulating currencies in the network. Once the transaction fee rise, the numbers and the willing of the transaction may decrease due to the cost increase. Every customer may tend to deposit his or her own money rather than spend. The share value of each coin rises due to rarely transactional activity. The phenomenon called the paradox of thrift may occur [9]. As to this situation, the whole environment would become deflation rather than inflation. The system may lower the transaction fee, even under three coins, to galvanize the transferring activity. The difference between new transaction fee and three coins, a fixed reward to operators, can be considered as issuing new money by the system. Accordingly, an economic cycle, an inflation and deflation interaction, performs automatically.

In addition, if the system acknowledges that a deflation or even the paradox of thrift is occurring, the system can increase the deposit rate, designed as an annual reward, that galvanize more people to participate the network and willing to spend. In short-term view, people may think they have earned more money without doing anything further, just like buy stocks and wait for its annual dividend. In the long-term view, as the number of circulating currencies increases, an inflation phenomenon has been created by the system to solve the previous deflation trap. If the over inflation occurs, the system would cancel the deposit rate to zero in order to stabilize the environment.

The network provides lending service. However, there is no bank-like center for people to borrow the money. In order to accomplish such service, the lending process is a unique task request to everyone in the network that everyone can choose whether he or she is willing to lend his or her own money to this complete stranger to expect the lending rate as rewards, considering it is an investment. If the deflation occurs, as the solution suggested by the Keynes in order to solve the paradox of thrift, the system will try to galvanize the will of investment which is increasing the lending rate for the lender side. As to the debtor, the system may lower the lending rate that he or she will not have to pay a higher amount of interest. The difference between two interests will be paid by the system, considering as a way of issuing the money. Once the money issuing increase, the whole environment will head to inflation then the currently deflation situation may be soothed. For the inflation situation, the same concept is applied; the difference between two interests will evaporate from the network.

Actions	Inflation	Deflation
Transaction Fee	Increase. The difference evaporates.	Decrease. The difference is paid by the system.
Deposit Rate	Decrease to zero.	Increase.
Lending Rate	Decrease to the lender. Increase to the debtor. The difference evaporates.	Increase to the lender. Decrease to the debtor. The difference is paid by the system.

Table 1 Interest rate controlling method

The most daunting part of adjusting interest rate should be how to determine the index and how to calculate the equivalent price. To make this approach practical, we introduced a special kind of task that a human resource hiring program, which can be put on the task chain. The working flow of the hiring program is the requester initiates a job with details, like locations, working period, hourly wage, gender limit, the number of workers and the job description. For instance, anyone can broadcast a request like pick up requester’s cat from the pet salon, and then sent it to the owner’s home. The program makes the cryptocurrency connects to the real-world life more possible. More importantly, with the task data, the system can build a neural network learning model, using locations, working period, gender limit, the number of workers, the number of how many people have applied and who, with which condition etc, has been chosen by the requester as parameters. The output of the neural network model is dealing hourly wage, which is the equivalent point. The model will rebuild every two weeks. If the latest predicting general equivalent price is higher than the standard price, the average-dealing wage of the previous year, the situation will be considered as inflation.

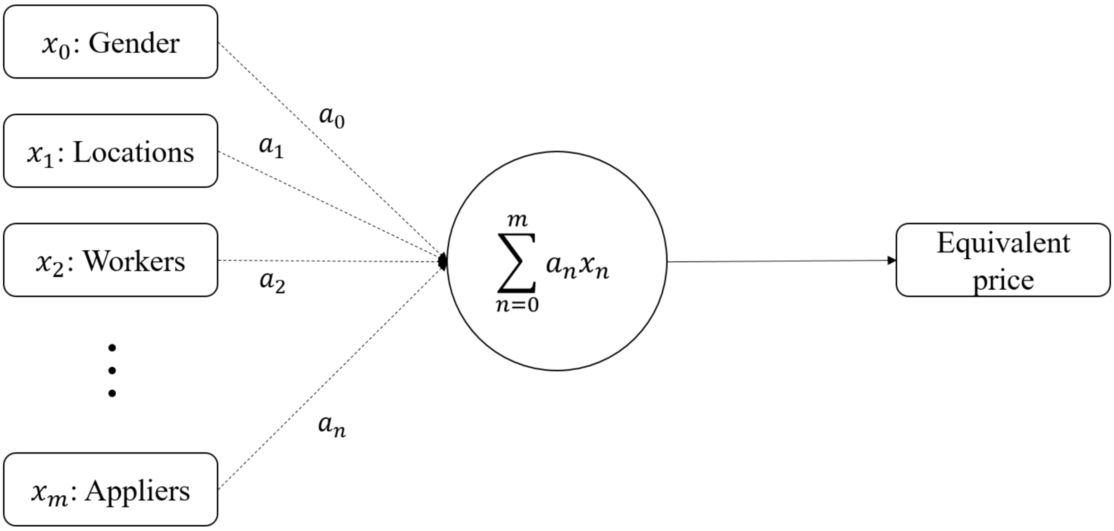

Figure 7 A simple neural network model for calculating the equivalent point of the network

For the very beginning of the network, the whole environment can be considered as a deflation society. Therefore, according to the Table 1, the system will use a series galvanizing methods to encourage the growth of the network. In addition, there is no standard price of the first year. The whole network is expected as a stable growing network year by year. As this attribute, to the real-world financial group, the digital demand-supply network can be considered as a reliable, self-adjusted financing society without any center.

4 Fraud and Risk

As the new structure, account-wise ledger, has introduced, some risk that traditional blockchain designed to solve needs to be reconsidered. Two major problems have been discussed within the decentralized network is: double spending issue and 51% attack.

4.1 Double Spending Issue

Since account-wise ledger system does not have a single, long blockchain, the double spending problem cannot be solved by the “longest chain determination” method. We have another solution to handle the double spending problem accordingly. The basic concept of determining whether the sender is cheating on double spending or not is that the operator needs to finish two checking job: 1. Trace the sender's balance to make sure that the sender is capable to afford the transaction. 2. Trace the whole sender's task chain (queue like design) to make sure that there is no further or previously unfinished transactional task may make the sender into a deficit situation. Once the checking failure occurred, the operator will drop the task and then report/broadcast to the network to announce every unfinished queueing task related to the sender is fraud.

However, the major challenge of the double spending problem in decentralizing network is the time delay of synchronizing every node of the network. According to the operator-signing principle, every operator needs to sign his or her unique signature to the sender's and receiver's ledger in *Sign_Op* slot in order to prove the work is done. The system requires at least two different operators to finish the same task and sign to the ledger in order to announce the transaction as valid. If the transaction result is different among operators, the transaction would be considered as invalid and withdraw from the sender's or receiver's ledger.

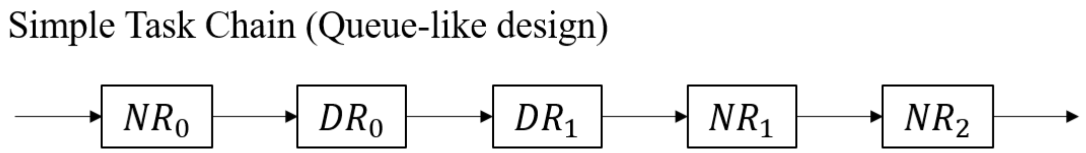

Figure 8 A pair double spending tasks in task chain

To be more specific, consider a double spending condition as Figure 5 shows, NR denoted as a normal task, DR denoted as double spending task. The simplest situation is that DR_0 and DR_1 are both invalid due to the insufficient balance of the sender. Both of these two tasks would be dropped by any operator. Therefore, the most tricky part of double spending question should be solving the puzzle of the valid transaction DR_0 and the invalid transaction DR_1, when DR_0 is complete, vice versa. To solve such question, we need to break down this big problem into four sub-questions in order to fit four situations: 1. DR_0 is handled by the first group of operators but neither has the following operator notice that the sender's ledger being updated or signed nor has the following operator notice that DR_0 being handled by someone else due to the network delay. 2. DR_0 is handled by the first group of operators. The following operator acknowledges the update of sender's ledger by the first group, but do not notice the task chain handling tag by them due to the network delay. 3. The opposite of Condition 2, the following operator does not notice the update of sender's ledger by the first group due to the network delay but do acknowledge the handling tag by them. 4. The following operator does acknowledge both latest operators' signatures of sender's ledger and task handling tag update. Both tag and operators' signatures are the same.

Considering the Condition 1, because the following operator does not acknowledge the change, he or she would consider themselves as first group operators. The operator will solve DR_0 task, sign to ledgers and broadcast the task tag. Because, according to the operator-signing principle, the system accepts operators' signature more than two, the action, handling DR_0, that the following operator took is valid. DR_1 is still waiting for someone else to handle. As to Condition 2 and 3, because the following operator notices the difference between task chain's handling tag and latest operators' signatures of both side ledgers, the following operator would realize that his or her task chain and/or ledger copy is not the latest version. The following operator will start the synchronizing function and wait until every info is consistent (to become Condition 4). For Condition 4, because the following operator considering DR_0 is complete, he or she will start to handle DR_1. At this moment, the following operator would realize that DR_1 cannot proceed due to the deficit situation of the sender. DR_1 will be recognized as a fraud.

Conditions	Task chain is synced	Task chain is NOT synced
Transaction chain is synced	Condition 1: Handle DR_0.	Condition 2: Listen to the network. Wait to be condition 4
Transaction chain Is NOT synced	Condition 3: Listen to the network. Wait to be condition 4.	Condition 4: Notice the deficit status of the sender. Drop the task and report.

Table 2 double spending conditions and related solutions

If the sender cheats on broadcasting inconsistent tasks to different groups of operators in order to achieve double spending fraud, different groups of operators will take the same valid, latest transaction block as the previous hash resource then create a new transaction block. In this case, the sender's transaction chain exist fork, which is not allowed. Any operator who acknowledges the fork will report the transaction as a fraud. Also, there exists another way to determine the inconsistent broadcast cheat. Any operator needs to announce his or her own handling tag if the job is complete. If a certain operator received a handling tag which does not exist in his or her copy of task chain, the operator will initiate the synchronizing job again. The operator will finally notice that the sender is cheating due to the different version of task chain co-exist in the network. The operator will report to the network of this fraud then everyone would only hold the consensus part of each copy.

4.2 Collusion and 51% Attack

Many previous studies have confirmed that if the decentralized network has any majority, the whole environment will become much more vulnerable than it used to be [6] [7]. The root cause of this weakness is the will of collusion through every node. As to Bitcoin kind cryptocurrency, the mining reward becomes the most valuable incentive for everyone to stick together in order to have a much powerful calculating ability to win the prize. In our system design, however, we cancel the mining reward, which does not only solve the unreasonable money-issuing problem but also alleviate the intention for everyone to stick together. For example, consider a simple model; two people try to collude with each other. One person creates a fraud task which he or she wants his or her partner can handle the case. However, when the network is growing large enough, with M nodes, the possibility of his or her partner can take the case should be $\frac{1}{M}$, which is extremely small. The transaction fee has a high possibility $\frac{M-1}{M}$ to be taken by the third party and without the mining reward as compensation. Under this circumstance, in the long-term view, the sum of total assets of these two will decrease, leaving no reason for them to work together any longer.

In addition, according to operator-signing principle, at least two different operators' signature is required. The action is performed by the sender rather than operators, meaning that no random hackers can duplicate or fake a transactional block without discovering by the ledger's owner. Therefore, the weakness is coming back to the collusion problem, the sender and the operator collude together, which is highly unlikely presented in this new system.

Considering a worst case, if there do exist a clustering majority in the network, actually, the successful possibility of fraud should be $(\frac{K}{M})^n$, where n denoted as the number of operators who handling a single task and K denoted as the number of nodes that collude together, $n \geq 2$. The whole system can increase the index of security by increasing the requirement of the least number of operators' signature. By doing so, however, may increase the general difficulty and processing time per tasks.

5 Conclusion

We have proposed a new way to implement the value exchanging platform and decentralized network. The new system can document every asset or good, which is valuable for humans, in order to allow everyone to exchange their properties. The whole system, with the neural network algorithm, can predict and emulate the wage trend which can reflect the current economic status in the real world. Also, the DDSN can solve the storage problem, data lost, and CPU calculating waste perfectly by respecting the very rules: distributable, decentralized, and reclaimable. Furthermore, the DDSN is not only a new implement of cryptocurrency but a new concept of the network which allow everyone to transact or exchange their value. With the power of DDSN, everyone can trade their properties directly, peer-to-peer, by the effort of intermediated handlers. There is no central authorities or government involved, which indicated the system is independent, free, and justice. The interest rate controlling function is also proposed. The economic control is performed by a 100% reasonable AI and the global tendency of every participant. With this design, the cryptocurrency value can be controlled by the system itself to build a more stable value exchanging platform.

Reference

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] W. J. Luther and L. H. White, "Can Bitcoin Become a Major Currency?," George Mason University Department of Economics, 2014.

[3] X. Li and C. A. Wang, "The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin," *Decision Support Systems,* pp. 49-60, 2017.

[4] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, Inc., 2015.

[5] H. Ching, "Universal Permanent Number," Post-Science Institute, [Online]. Available: http://upn4.com/.

[6] I. Eyal and E. G. Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable," Wayback Machine, 2016.

[7] M. Bastiaan, "Preventing the 51%-Attack: a Stochastic Analysis of Two Phase Proof of Work in Bitcoin," University of Twente, 2015.

[8] A. Marshall, "Principles of Economics," Macmillan, London, 1890.

[9] J. M. Keynes, The General Theory of Employment, Interest and Money, Palgrave Macmillan, 1936.