FOUNDATION@RCTOKEN.COM

VERSON 0.4.5

# REFERENCE & CERTIFY TOKEN

# Contents


1 *Background and Concept of Design* 4

2 *Our Mission And Team* 8

2.1 *Our Mission* 8

2.2 *Team* 8

3 *Innovation of the RCT Project* 10

3.1 *Review of Consensus Mechanism* 10

3.1.1 *Proof of Work* 10

3.1.2 *Proof of Stake* 11

3.1.3 *Proof of Importance* 11

3.2 *Blockchain Design* 12

3.3 *Incentive Mechanism* 12

3.3.1 *Proof of Importance (PoI) and "Random Walk" Algorithm* 12

3.3.2 *Difficulty Calculation* 13

3.4 *Serialization* 14

3.4.1 *Principles* 14

3.4.2 *Cases* 15

4 *Possible Attacks and Solutions* 17

*4.1 Sybil Attack* 17

*4.2 Loop Attack* 17

*4.3 Low-value Works* 17

*4.4 Retrospecctive Difficulty* 18

*4.5 Block Generation Time* 18

5 *Commercialization Program* 19

*5.1 Circulation of RCT* 19

*5.2 RCT Allocation Program* 19

*5.3 Milestones for the RCT Project* 20

6 *Possible Applications* 21

*6.1 Monetizing Social Media Importance* 21

*6.2 Patent Monetization and Rapid Pricing of Scientific Research Products* 21

*6.3 Research Paper/We-media/Blog/Network Literature* 22

*6.4 Online Forums* 22

*6.5 Ranking System for Universities, Electronics, Services* 22

7 *Summary* 24

# 1 Background and Concept of Design

The popularity of the Internet and smart phones has brought us into the era of We-media. For example web content analytics have shown that in the blog and microblogging space alone, more than 200 million new accounts are created per day. We live in a time when everyone with a computer or cell-phone can take place in the participation and sharing of media. With little more than a beautiful photo or witty phrase, one can become a temporary star or reach social media infamy.

However one drawback to the rapid-fire dissemination of information arises in the issue of intellectual property protection. The reproducibility of Internet files speeds up the dissemination of information, while also increasing the difficulty of property right protection. Internet content will soon be spread by other and oftentimes it is difficult to find the original author of the work. This is not only an infringement of intellectual property rights and damage to the original author's rights and interests, it also dampens the authors' enthusiasm and incentive to further improve upon their original uploads and submissions. We envision an information system that not only gives the creator a reward corresponding to the influence of his/her work, but simultaneously preserves integrity of authorship. Such a program will ignite the passion of innovation and promote the continuous integrity and a flourishing culture in the We-media era.

In the world of scientific and academic publishing, the internet has been used to address some of the issues related to authorship attribution and relevance/importance quantification. Example databases include ArXiv, SCI, and Ei Compendex, along with impact measurement techniques including *h*-index, or impact factor. Despite their relative success, these techniques and platforms are fraught with issues and difficulties. For example the *JIF* (journal impact factor) of a journal is interpreted as the mean count of citations pointing to any given article accepted to the journal in question. A problem with this is the skewed distribution of citation count per article within a journal. In most cases the majority of the citations are concentrated a small number of articles in any given issue of the journal, and many at the bottom are cited very little, sometimes not

at all. To make matters worse, the method used to compute the *JIF* is proprietary and unknown to the public. This is a result of Thomson Reuters, a private entity which is responsible for publishing and maintaining the *JIF* list, which makes money by selling access to the Web of Science (a collection of inter-disciplinary databases). In general there is much documented dissent and criticism of the *JIF* as a measurement of impact and importance, which some have claimed is no better than guesswork.

For measuring the importance of individual uploads, the most commonly used approach is the *h*-index. An *h*-index of 70 is best interpreted as having *at least* 70 citations on 70 different papers in your career. It is a generally accepted measure of a scientist's success, by taking into account both the quality and the quantity of their output. However it is not without its drawbacks: The *h*-index does not take the context of the author's field into account. For certain fields (mathematics in particular), an important work may have very few citations if any. *h*-factor has been shown in an empirical study by Yong [1] to have nearly the same capacity to measure impact as simply counting the number of citations.

[1] Alexander Yong, Critique of Hirsch's Citation Index: A Combinatorial Fermi Problem, Notices of the American Mathematical Society, vol. 61 (2014), no. 11, pp. 1040–50

With open-source databases such as ArXiv, one encounters a new set of pros and cons. A positive feature of ArXiv is the fact that it is open source, version controlled, and free to upload and view. However, there is no mechanism for authorization to prevent "junk science" from appearing on the network, or any system of valuation to measure impact. An alternative to the open source option is to publish on a centrally maintained database such as SCI or Ei Compendex. These databases solve issues such as authorization, and have an automated system of impact measurement, but they cost money to access, and because they are privately run, they are susceptible to cheating and manipulation, as the methods used to calculate value and importance are often opaque and privately maintained. For example the Web of Science was recently sold to various private interests in a multi-billion dollar transaction. The presence of multiple private stakeholders makes it increasingly difficult to prevent corruption and abuses of the citation system.[2]

[2] http://www.the-scientist.com/?articles.view/articleNo/46558/title/Web-of-Science-Sold-for-More-Than–3-Billion/

The birth of blockchain technology points to a natural and elegant solution to preserving the value of original authorship while circumventing all of the problems listed above that are intrinsic to a centralized document repository system: Blockchain was initially proposed in an October 2008 whitepaper by Satoshi Nakamoto entitled "Bitcoin: A Peer-to-Peer Electronic Cash System"[3]. Blockchain is a smart peer-to-peer network used to identify, transmit, and record information on a distributed database. The security of the database is ensured by an ensemble of cryptographic methods, time series data, and a Byzantine-fault tolerant consensus mechanism, all of which ensure the continuity and persistence of the nodes in the distributed database. In addition, this is all done through

[3] Nakamoto, Satoshi (October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System" bitcoin.org. Retrieved 28 April 2014.

open source software, guaranteeing that the information that can be verified and traced back to its origin immediately. This results in records that are tamper-proof and intrinsically transparent, resulting in a secure, shared, registery of value. [4]. The system is also known as the Internet of Value, which can transmit virtual currency, implement smart contracts automatically, host autonomous corporations etc. without requiring third party participation and review of any centralization agency. Since its inception, the value of the blockchain technology itself has been discovered and recognized continuously [5] [6] . In In the case of Bitcoin, for example, the first transaction recorded was by a programmer named Laszlo Hanyecz in the United States bought two pizza with 10,000 BTC on May 22, 2010. By May 22, 2017, the same amount of Bitcoin was valued at about $ 22.89 million, appreciating by about 1 million times.

[4] Iansiti, Marco; Lakhani, Karim R. "The Truth About Blockchain". Harvard Business Review (Harvard University). January 2017 [2017-01-17].

[5] Popper, Nathan (2016-05-21). "A Venture Fund With Plenty of Virtual Capital, but No Capitalist". New York Times. Retrieved 2016-05-23.

[6] Morris, David Z. (2016-05-15). "Leaderless, Blockchain-Based Venture Capital Fund Raises $100 Million, And Counting". Fortune. Retrieved 2016-05-23.

The developers at RCT realized that citations themselves are a form of transaction. In most cryptocurrencies a transaction is thought of as an arrow connecting two nodes on a graph, and a time stamp is allocated for each transaction event and recorded permanently and indelibly on the blockchain. In the citation chain, we adopt this transaction model to represent citations and references between entities. In other words by citing another author you are performing a transaction, and in the citation economy, authors with many citations are rewarded, just as they would be in a traditional economy. The power and beauty of blockchain's consensus network allows this to become a possibility. With this "citation-as-transaction" insight driving our technology, we adopted the following features in the design of our network:

- The proof chain uses the limitless range of virtual address space to cover every component of each author's content. In the RCT network, each submitted document, such as a microblog, a blog, a picture, music, video, an academic paper, a patent, etc., can get a wallet address for its unified resource locator (URL) through Hash coding. The key to the wallet belongs to the creator himself to ensure his ownership.
- The proof chain uses the "transaction history" of the blockchain to record the citation relationship between the works. The creator adds "reference" in the process of making the wallet address, namely, listing the wallet address of other works that are quoted, reproduced, and forwarded in creating the work to establish the proof network. The records that have been repeatedly confirmed in the blockchain will be difficult to overturn, and the difficulty and the number of confirmations will increase exponentially, which will ensure the reliability of the proof relationship.
- The blockchain adopts the unique PoW + PoI consensus mechanism to award RCT tokens for excellent works. For RCT tokens of each block, 60% will be given to miners and 40% will be given

to the excellent works according to the influence of the work in the proof relationship network. This ensures that the creator as "intellectual exporter" and the miner as "technical service exporter" have a considerable income to encourage creators to create more influential works.

- The proof chain, relying on the open and transparent features of the distributed account books of the blockchain, makes it possible for the public to supervise the miners and creators. The transactions and proof relationship in the proof chain are stored on different nodes in the form of blockchains, so everyone can go back and check the historical records.

The value and impact of the blockchain on modern life is no longer a topic of dispute. Nearly 10 years out from the inception of this incredible technology, we are seeing an oncoming wave of blockchain and cryptocurrency innovation which experts have compared to the impact of the World Wide Web in the late 90's. Our intention is to participate in this singular, world-historical event by implementing the power of the blockchain to provide an entirely new alternative to existing academic document repositories and media hosting databases.

# 2 Our Mission And Team

## 2.1 Our Mission

***Protect each and every intellectual creation, encourage innovation and creation and help everyone realize his dream through creation.***

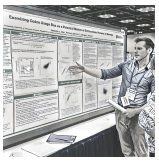
The popularity of the Internet and mobile Internet enables everyone to become a good creator. The team of the proof chain is committed to using blockchain technology to help each creator protect the results of intellectual labor, help each creator to benefit from his work, encourage every creator to create better works and ultimately help each creator to achieve his dream through innovative creation.

## 2.2 Team

Table 2.1.

Table 2.1: Team Members

*Kevin Lopez*
a Ph.D. candidate at Yale University. He used to be an experienced software developer for several years and took responsibility of algorithm design and advanced framework solutions. He has also studied blockchain technology for years and contributed to cryptocurrency development.



*Alexander Cope*
Ph.D. He is an engineer and developer with deep knowledge in computational models, database development and algorithm design. He has experience in developing integrated and high performance computational systems at oak ridge national laboratory (ORNL). Regarding blockchain as the next revolution, Alex started to get involved in cryptocurrency ecosystem and joined the team to launch blockchain platform based on innovative consensus algorithm.

*Jason Lian*
Ph.D. Works in oak ridge national laboratory (ORNL), biophysics and datamining. He is a cryptocurrency & blockchain enthusiast. As a former Senior Data Mining Engineer at Holaverse, he worked on mobile internet big data datamining and recommendation algorithm design. He was involved in blockchain field since 2013 and joined RCT in 2017, responsible for the development of the infrastructure and smart contract of RCT blockchain.

*Stephen Grady*
Ph.D. With five years of experience in graph algorithms, applications and implementations, Stephen brings a wealth of consensus algorithm development knowledge to the RCT project. He has a strong track record working with advanced computation solutions in algorithm design, modeling, simulation and product development.

*Yaojin Sun*
Ph.D. As an experienced developer, he participatd in projects related to blockchain at oak ridge national laboratory (ORNL). Yaojin manages the technical aspects of the RCT project including consensus algorithm, framework design and the development of the project's information. He is cryptocurrency enthusiast, blockchain developer with background in advanced computation technology and machine learning algorithm design.

*Harrison Hicks*
a Ph.D. candidate at UTK. He Works in Deep Learning Architecture. Strong background in Applied Statistics. Passionate about the potential of cryptocurrency and blockchain.

# 3 Innovation of the RCT Project

## 3.1 Review of Consensus Mechanism

Consensus mechanism is the heart of blockchain project. Since different nodes follow the same consensus algorithm, it is possible for most honest people join the network and contribute to the network. In other words, the consensus algorithm is the reason why value can be built in a private network and why serialization is feasible to be constructed. For the past several years, researchers and computation scientists have already created several famous consensus mechanisms. When it comes to the blockchain world, Proof of Work (PoW) proposed by Satoshi Nakamoto is the most famous one. Apart from PoW, researchers bring new ideas like Proof of Stake, Proof of Storage, Proof of Importance and the like to the blockchain technology. We will discuss the pros and cons for some famous consensus algorithms and explain why we bring Proof of Importance (PoI) and Proof of Work (PoW) together to RCT project.

### 3.1.1 Proof of Work

According to Bitcoin whitepaper, "...The proof-of-work also solves the problem of determining representation in majority decision making..." From a technical point of view, mining process is an operation of inverse hashing: it determines a number (nonce), so the cryptographic hash algorithm of block data results in less than a given threshold. Because of successful Bitcoin story, many (or even most) blockchain projects have used this consensus mechanism as their core part of serialization methods.

The main advantage of PoW is that this consensus algorithm has been tested by different platform and proved to be safe and secure. However, PoW is not perfect. Miners need to spent huge amount of computation power and electricity to maintain this network. Someone may argue this costs are necessary but energy cost itself is a big issue in blockchian network.

### 3.1.2 *Proof of Stake*

The idea of Proof of Stake (PoS) is proposed on the bitcointalk forum in 2011 and applied in Peercoin in 2012. In short, it means the rich one would be richer. Unlike the proof-of-Work, where the algorithm rewards miners who solve mathematical problems with the goal of validating transactions and creating new blocks, with the proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth (or Stake).

It has also been proved to be successful. Actually, the Ethereum project is currently alternating its consensus mechanism from Proof of Work to Proof of Stake. And the energy efficiency itself is a big advantage compared with Bitcoin.

For both PoW and PoI, if someone wants to apply Sybil attack, the evil node may need to control 50% of computation power (PoW) or 50% of circulation tokens (PoS). At that time, the node itself has become the biggest part of the system.

### 3.1.3 *Proof of Importance*

Proof of Importance (PoI) was first applied in the New Economy Movement (NEM). Because the transaction information for each account is public to the entire network, a large transaction matrix can be constructed based on past transaction history. Each account is calculated with a corresponding importance score, and an account with a high importance score is more likely to gain the reward of the next block. By introducing the NCDawareRank algorithm, the importance score of the eligible account in the network is calculated.

In the blockchain network, there may be tens of millions of accounts with the number of transactions even in billions. An algorithm based on similar PageRank and NCDawareRank results in an exponential rise in the consumption of computer memory. However, NEM bypasses the problem of computer memory consumption by increasing the filtering conditions, for example, the amount of transaction must be large enough; the blocked generated in the past 30 days will be calculated in the blockchain, etc. By adding filtering conditions of the account, there are only a few hundred accounts that are included in the calculation.

The application of NEM is feasible in the algorithm, but it is problematic for the evaluation of the value based on "citation network". Due to the limit of the amount of the transaction, the account balance itself can also affect the academic value of the work. This is contrary to the idea of decentralization.

## 3.2 Blockchain Design

Since the RCT project aims to revolt the way how to value creator's work, we would set Proof of Importance (PoI) as core part of the consensus algorithm. At the same time, to make sure the network is safe and secure, we would also bring Proof of Work into the consensus algorithm to make sure miners would contribute to maintain the RCT project. The decentralized assessment method based on the blockchain can help us assess your works continuously.

In RCT network, we want to expand the definition of "citation". The work will not be limited in terms of the format and form, and it can be an academic article, a picture, a video or even just a passage. And "citation" refers not only to the index relationship between academic papers, it can also be a citation to the author of the work, and even citation of each of the pictures by an article. In the blockchain, we use "Transaction" to bear "citation".

Intuitively ,the citation of the work embodies the value of the work itself. A work cited by more accounts shows that it has a higher value. Similarly, a work cited by another work with a higher value also represents a higher value. This idea is widely used in activities such as page rankings.

## 3.3 Incentive Mechanism

### 3.3.1 Proof of Importance (PoI) and "Random Walk" Algorithm

The citation network would involve millions of accounts and billions of transactions. Just as mentioned in previous section, the "account" is the way how to prove ownership of creator and the "transaction" is the way to hold citation information.

Given the citation network with huge amount of accounts and citing information, it is close to be impossible to run matrix calculation which is the essential step of NCDwareRank or PageRank algorithm. In order to solve both the problem of decentralization and computer memory consumption, we introduce the mathematical model of "Random Walk" in order to balance the value judgment and the normal operation of the blockchain network.

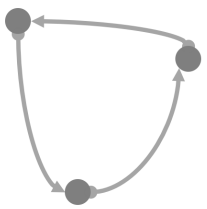


Figure 3.1: Circular citation

Inspired by PageRank algorithm, a way to organize random walk of various lengths, we introduce the simulation/modeling of "random walk" to avoid the matrix computation and validation.

The problem that Random Walk intends to solve is to achieve value judgment based on the citation relationship between the accounts entirely without significantly increasing memory consump-

tion. The figure 3.3 shows a hypothetical academic citation network. In the blockchain, the concept of “citation" is more flexible than the current generic concept, and may not be limited to time. If a drunk jumps and walks randomly in the network with one jump every time, the direction of jump must be the direction of citation. With limited steps, the place where the drunk finally stays is the location that has significant value for this network.

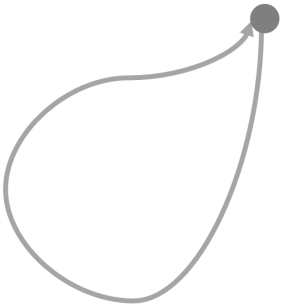


Figure 3.2: Self-citation

Because the implementation of "citation" in RCT network is neither limited to time nor limited to works, we may observe "self-citation" (figure 3.3.1) and "circular citation" (figure 3.3.1). In the case of circular citation and self-citation, the Random Walk Model is easily used by miners to reduce the difficulty of searching, but cannot achieve the reward for high-value works. For this type of problem, we add a restrictive condition that each account in the Citation Chain can appear at most once. In this case, the search difficulty will be maintained in a relatively stable degree.

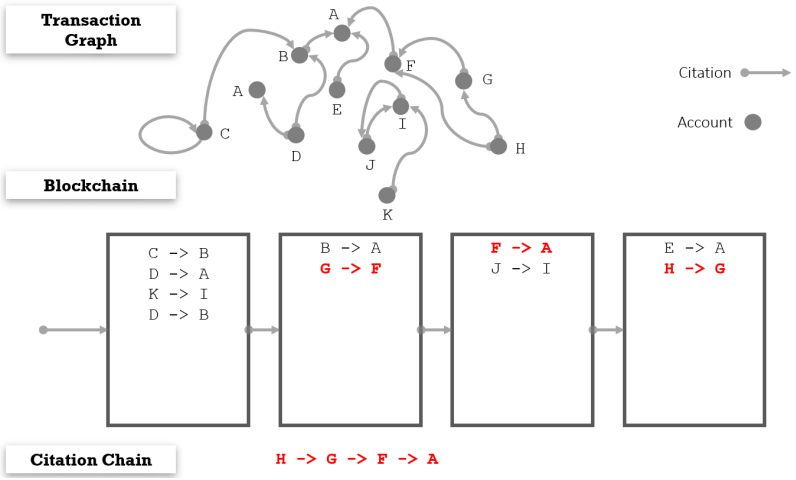



Figure 3.3: Transaction graph, blockchain and citation chain

The storage and computation on the blockchain are very valuable and expensive. And too many steps in Random Walk will not be accepted; otherwise the corresponding block size will increase significantly, even increased to the extent that no miners have enough time to verify. The current number of Random Walk is at most 8 steps and at least 1 step. In the figure 3.3, the citation chain generated by Random Walk contains 3 steps.

### 3.3.2 *Difficulty Calculation*

In order to encourage miners to carry out Random Walk operations as much as possible (i.e., to find the most valuable works in the blockchain), the number of Random Walk will have impact on the difficulty of the whole block.

$$f(x) = 1 - \frac{1}{2(1 + e^{\bar{x}-x})}$$

- $\bar{x}$: the average number of steps of Random Walk in past blocks
- $x$: number of steps for Random Walk in the current block
- $f$: current difficulty coefficient

In most cases of blockchain application, the difficulty coefficient is only utilized to regulate the time for generating a certain block. Since the generation time for one block is related to the security of that block, the difficulty level has to be managed frequently and carefully.

In RCT project, the function of difficulty coefficient calculation would be applied not only for managing block time but also as a key incentive. Intuitively, the level of difficulty coefficient would not only be determined by previous block, but also the PoI the miner has applied in the latest block. The reason why we introduce this mechanism inside RCT project is that we want to encourage miners to search whole blockchain database over and over again to make sure the rewarded work is the work with high value.

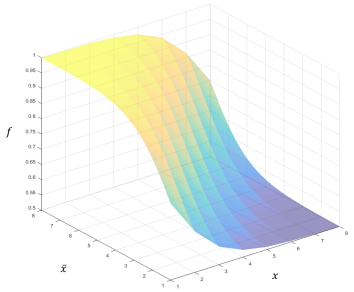



Figure 3.4: The surface of $f(x)$

## 3.4 Serialization

### 3.4.1 Principles

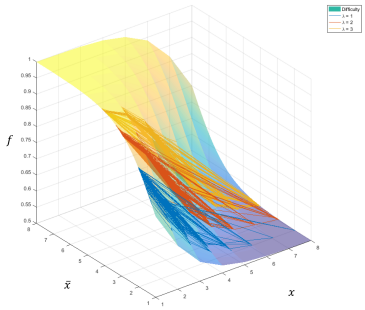



Figure 3.5: The surface of $f(x)$ with simulation results

Bitcoin and other mainstream currencies are mainly based on PoW for the construction and confirmation of the block. We will combine PoI and PoW to achieve double protection for miners and content providers.

In the previous section, we have been able to get a difficulty coefficient through random walk algorithm. In the new block confirmation, the portion of the PoW still utilize the hash code calculation (e.g. SHA256 algorithm to calculate the zero character matching the times), and the second part, the specific hash value must be greater than the difficulty coefficient f. We note that after the introduction of the Random Walk Model, if no Random Walk is attempted (i.e., the number of steps is 1), the difficulty coefficient will be close to 1, and if the number of steps of the citation chain reaches 8, the difficulty coefficient $f$ will be close to 0.5. The two corresponds to about 50% of the calculation of the difference.

For an honest miner, he will, as far as possible, *go back to the entire block as much as possible and find all possible citation chains to*

*reduce the corresponding difficulty coefficient*. With the increase in the number of blocks, the difficulty of search will increase. When the difficulty of the search increases to a certain extent, the miner will give up the search (he will search only 1 corresponding step in extreme cases) and turn into PoW calculation. This result will reduce the average length of the citation chain, and in this case the advantage of search is explored again, and the miner will search more blocks to obtain a reduction in the difficulty coefficient.

After each block is confirmed, there will be a certain amount of reward provided. The total award is divided into two parts: the first part is the miner (60%) who completed the current block, and the second part is the final account (40%) cited by the citation chain, which is identified as a work with important value in the current block.

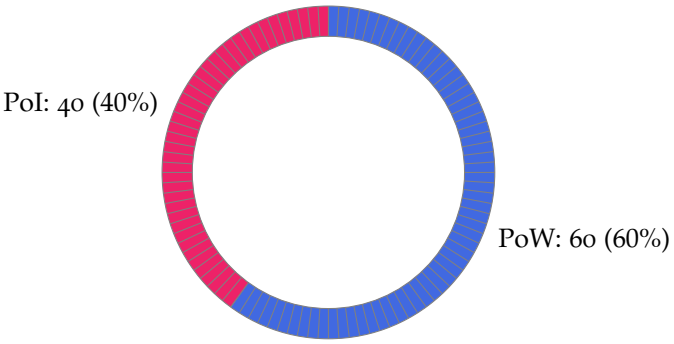



Figure 3.6: Consensus mechanism. (Unit: Percent)

### 3.4.2 *Cases*

In this section, we would provide several cases of serialization.

*[Genesis]*

The genesis is defined as the very first block. In genesis, we would include detailed information collected from Initial Coin Offering (ICO) and initial investments. You will find detailed information from chapter of commercialization.

We pre-define all necessary information for serialization purpose. All of these information will include but not limit to allocation details, average steps and initial value of difficulty and random block selected. For making a complete block, a miner need to solve several key problems. These questions and procedures include but not limit to verication of all transactions generated from father block, the number of average steps for the whole RCT network, identification of the random block number generated by the father block, finding the longest citation chain (no more than eight steps) and generate a new random number for next block.

*[Random Block]*

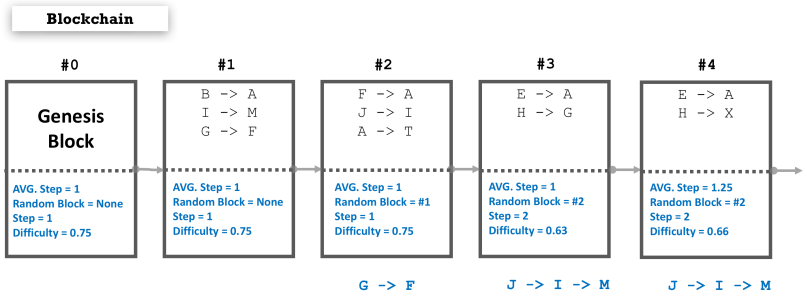



Figure 3.7: Case 1

There is one possible way to attack the network by copying the "correct answer" from previous blocks. It means that the miner does not search through the RCT network but just copy the answer (given a citation chain with eight steps) from before. That's cheating and not accepted by our consensus mechanism. The solution is bring randomness to the whole blockchain. For each block, the first transaction of citation chain must be picked from the block that has already determined by previous block. Given the case of figure 3.8, the block #121 also generated a random number which points the block #61, so the miner of block #122 must find a citation chain with first citation in block #61.

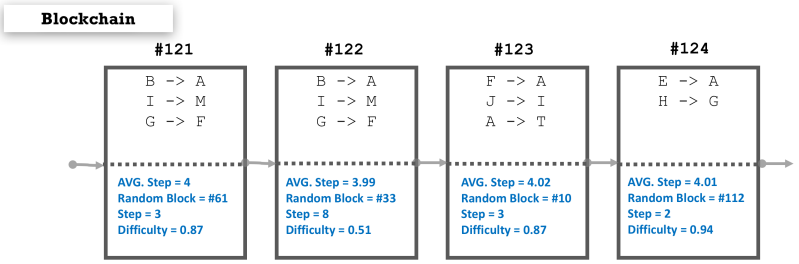



Figure 3.8: Case 2

*[No Citation in A Certain Block]*

It is possible that miners cannot find even one citation in a certain selected block determined by previous block. Since all the other nodes in the RCT network cannot identify whether this behavior is on purpose or not, they can only regard this situation as a search with one step. Then, the miner of this block would reward the account that has been rewarded in the previous block. (figure 3.4.2)

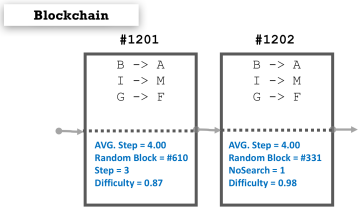



Figure 3.9: Case 3

# 4 Possible Attacks and Solutions

## 4.1 Sybil Attack

Sybil Attack is the most common problem in blockchain design. For a completely PoW-based Bitcoin and other blockchain system, the premise of a witch attack is the grasp more than half of the computing power of the entire network. In the RCT, sybil attack for a certain block not only needs have sufficient computing power, but also requires the ability to trace back the entire blockchain. Because the starting position of the Random Walk is randomly determined by the previous block, the corresponding attack difficulty is no less than the PoW-based blockchain network.

## 4.2 Loop Attack

Another pattern of attack is to build "loop attack". Figure 4.2 has illustrated a simple situation. An evil node is able to create four accounts with four transactions to connect them. In a real-world situation, the evil node could build a big circle to operate this kind of attack. It means that no matter which citation has been identified, one of his accounts would also be picked. Figure 4.2 provides a more complicated situation. Our solution is still to bring RANDOMNESS. By adding restrictions to the transaction/citation, the citation counted for building citation chain would be much less than before. However, the normal citation would not be affected because this randomness would be applied to all users. For the evil nodes and their accounts, the cost of applying similar attack would be much huger than before.

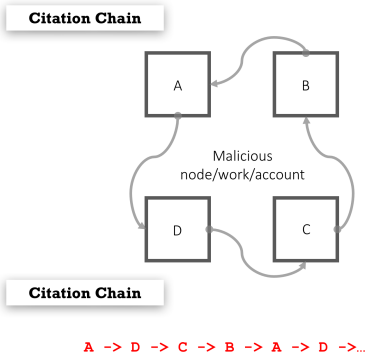



Figure 4.1: Loop Attack (Simple)

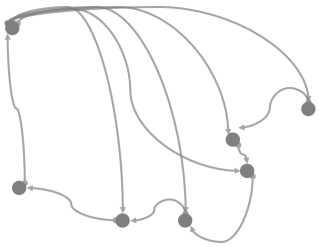


Figure 4.2: Loop Attack (Complex)

## 4.3 Low-value Works

Assuming the existence of a completely worthless work, the author, by generating a large number of accounts, continuously cites the worthless work in order to deceive the reward of each block. This type of problem is the challenge of all the value judgment sys-

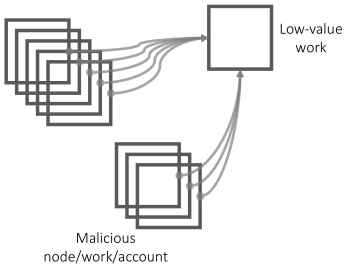



Figure 4.3: Low-value Work. We regard "loop attack" as a subset of "Low-value work" attack.

tems based on mutual citation. The performances of Random Walk Model and PageRank, NCDawareRank are basically the same, and they all avoid the massive storage consumption of decentralization. On the other hand, every citation is not completely free and the fee will be significantly higher than the general transaction. The current citation fee we set is equivalent to more than twice the normal transaction, and the amount of money transferred must be greater than or equal to the current transaction fee. In this case, for a malicious node, the number of citation cannot be too much, otherwise the deceived block award cannot make up for the fee resulting from citation itself.

## 4·4 *Retrospecctive Difficulty*

Bitcoin's blockchain network generates about 50GB of data reach year and the size of our blockchain network will not significantly exceed this figure in early stages. For such a large data, the time consumed to search once will not be more than a few seconds. The honest miner can have the calculation difficulty greatly reduced only by complete search. The search difficulty should be in logarithmic growth without having a huge impact on the Random Walk Model itself.

Our goal is to bear all citation information of the academic journals and to award the outstanding works. When the amount of citation information of the block is quite large, the time for a single search may be extended to ten seconds or more. In this case, the miner will be likely to conduct only the first search (namely, find the location of the previous block, constant time consumption with the retrospective step being 1). In this case, PoL and corresponding Random Walk Model will offer incentives for the search in terms of difficulty to attract the miners to re-search in the entire blockchain.

## 4·5 *Block Generation Time*

Compared to other digital currencies, the changes of the generation time of new block from the previous one will reach 50% at most. But this is in a very extreme situation, and in most cases, the generation time will not exceed 10%.

# 5 Commercialization Program

## 5.1 Circulation of RCT

The English for RCT program token is *Reference and Certify Token* abbreviated as RCT with a total circulation of 420 million. The generation speed of the blockchain is 1m/block and the initial amount of block incentive is 50 tokens/block regularly halved. The consensus mechanism is PoW + PoI accounting for 60% and 40% respectively.


Figure 5.1: The logo of Reference & Certify Token

## 5.2 RCT Allocation Program

The initial source of funding for the implementation of the project is mainly dependent on the support of ICO and early investors as well as public sale of the part of early investors. In the early stage of project implementation, this part of funds raised will be invested into model validation and network construction. Nearly one third of the 420 million tokens will be provided by the miners (give rewards in proportion according to PoW and PoI mechanisms). In the stage of promotion, 10% of all flows will be used to finance academic research institutions and enterprises to participate in RCT network.

During the operation of the project, the creator needs to pay a certain RCT as a fee to establish a reference relationship (in order to prevent malicious establishment of the garbage reference). Once the reference relationship is established, 40% of the RCT awarded will be rewarded to the "works" (wallet address) in the past block according to the its influence to encourage more people to join the citation chain and encourage creators to create more influential works. ICO and early investors can either choose to transfer RCT to others, or convert their works into a wallet address for others to cite to claim more RCT earnings.

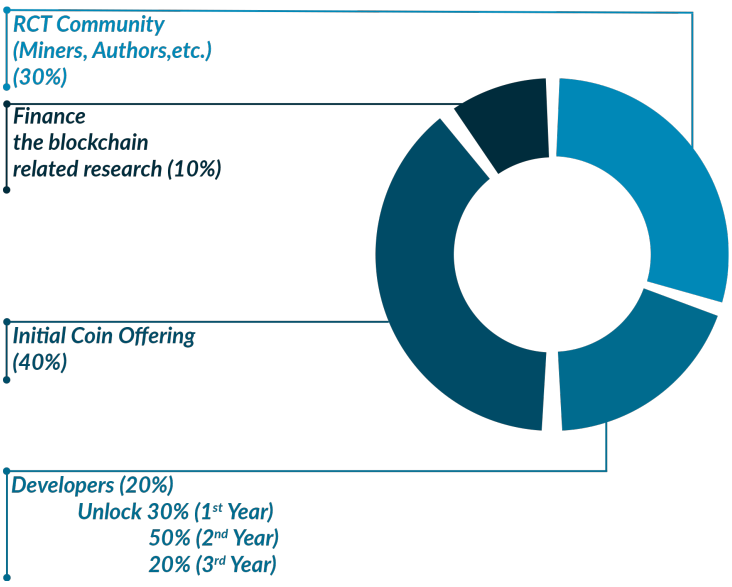



Figure 5.2: Allocation

## 5.3 Milestones for the RCT Project

Please refer figure 5.3.

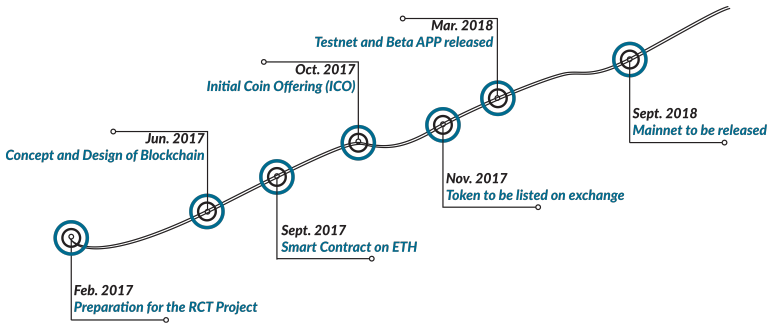



Figure 5.3: Roadmap

# 6 Possible Applications

## 6.1 Monetizing Social Media Importance

In many social media platforms, the accounts and content are not yet monetized. With RCT, any account on social media can be hashed and given an address on the blockchain, and any content produced by an account can be hashed and addressed as well. Storing this on the RCT can allow users to monetize social media content, by committing a citation/transaction as a proxy for "liking", "subscribing", "clicking", "retweeting", "upvoting" etc. social media content.

On traditional social media, content-interaction is indirectly monetized through centralized systems like Google AdSense, which and determined by advertisers and views. RCT will replace this as the primary revenue stream for content creators on social media, and eliminate the middleman from the process of valuing social media content.

## 6.2 Patent Monetization and Rapid Pricing of Scientific Research Products

In traditional research, peer review can be used to conduct a pricing study of a class of products to reflect the status of the research results throughout the research community. On the citation chain network, value judgments are based entirely on peer review and records are impossible to change once committed to the blockchain. When a work is introduced into the citation chain network, an account that has a higher reward in the industry (for example, an account that is constantly referenced in all previous nodes and has a high importance score) can be made simple for "reference", you can achieve the endorsement for the value of this product. One of the consequences of this is that the credit of the account becomes an important criterion for judging pricing and at the same time, the value of the work can be accounted for by the entire network.

## 6.3 Research Paper/We-media/Blog/Network Literature

The Internet is constantly reducing the cost of piracy, and authors of we-media/network literature and other original contents need to face the challenges of copyright infringement and other challenges without sufficient income. Although the citation chain network cannot achieve the task of recording the content itself, copyright verification is relatively simple for the works existing in the entire network own hash value. This feature has also been proven by other blockchain networks.

## 6.4 Online Forums

A very popular form of online discussion and interaction is an online forum. One of the primary forums is Reddit or 4chan. Account-holders post comments and various other media to the forum and interact via comments or "upvotes". If we think of these as transactions, we can stack the forum structure on top of the citation network, and create the appropriate security features to make sure that it cannot be abused. This kind of network would intrinsically reward users whose comments generated a lot or were upvoted.

## 6.5 Ranking System for Universities, Electronics, Services

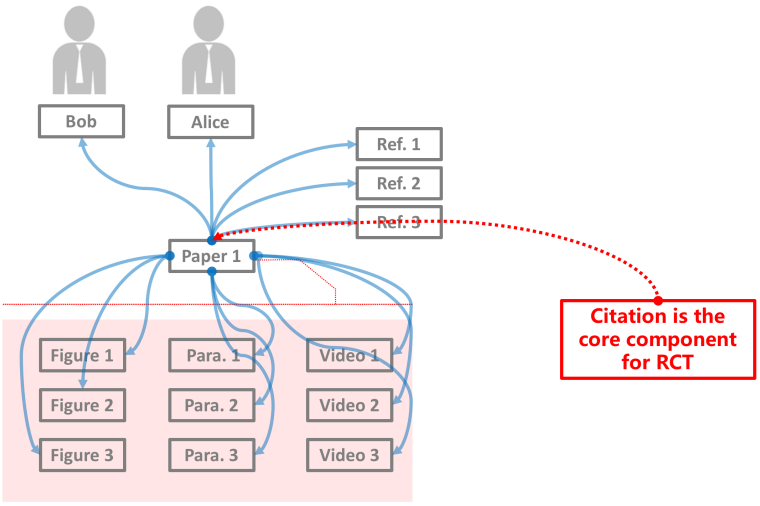



Figure 6.1: An example of RCT application

One significant feature of the citation chain network differing from other blockchain networks is that systematic and scientific calculation has been done in terms of the awards of the original content of the network. Most of the modern social networks have cited the incentive mechanisms of "praise" and "opposition", and

some platforms even judge the value of the entire work through the praise and opposition. But one of the challenges to this behavior is that a malicious node can generate massive virtual users in a short period of time to continually "praise" or "oppose" the work, thus affecting the platform's judgment of its value. The citation chain network, based on "citation" , conduct the value judgment, which on the one hand, costs the honest users a little for every "citation" with only a few transaction costs. But for a malicious node, if you want to deceive the network to obtain rewards, you need to generate massive users to repeat the "citation", so the income cannot even cover the required fee.

The author of the original works of the network can provide information such as the hash value, account address and other information in the website, social media, or the network platform we recommend to attract other authors to make a simple reward or more formal academic reference. For an original author, the cost of the above act is almost negligible, but it can be a lot of money by virtue of the value of his work.

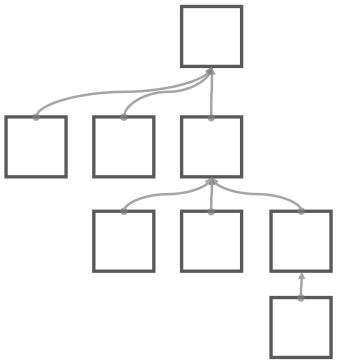


Figure 6.2: Tree Citation: The way we recommend for citation structure.

# 7 Summary

- RCT can be used to create trustworthy value evaluation and transmission network;
- RCT network can bear all forms of creative works;
- The application of timestamp enables RCT network to realize property rights protection and copyright tracking effectively;
- By introducing an importance proof mechanism based on citation (PoI), RCT can judge the value of any work in a short period of time;
- The development of RCT project includes community construction, technical verification, token issuance and final network publishing;
- ***Our goal is to protect all intellectural property, reward and maintain the rights of global creators;***