# A Proposed Currency System for Academic Peer Review Payments Using the BlockChain Technology

515030910620 陈晋进

May 27th, 2018

Partners: 515030910622 陈泓宇
515030910590 吕枝钖

**Abstract**

Peer review of scholarly papers, as a critical step in the publication of high quality outputs in reputable journals, may face problems such that few incentives for researchers drive them to conduct suitable reviews in a timely fashion and in some cases unscrupulous practices are occurring as part of the production of academic research output. This report is based on a proposed currency system using the BlockChain as its basis and finds a particular solution for the system.

## 1 Introduction

Almost every research academic is aware of the current environment in which both institutions and individuals are subject to some form of assessment and a considerable proportion of the scoring is often weighted on the production of scholarly outputs, typically as papers in reputable journals. Apart from the obvious authors and readers, these journals typically have a small number of editors who do most of the day-to-day management of the intellectual material; there might also be a larger editorial pool from the discipline who oversee the journal, and then there are those people who take on the role of reviewers which could include all of the previously listed groups of people. The production of a journal also include publishers who publish for profit or publish through a non-profit entity such as a learned society. Irrespective of the details of the process, the production of an academic journal is an economic system and like any such system the publishing process presents a number of intended and unintended incentives.
Due to the anonymous nature of peer review, people seem to have lesser incentive to carry out this part of the publication process. Although some journals will list those that have carried out reviews on its behalf, it is more difficult to provide

a measure of the number, quality and timeliness of those reviews. The paper considers how it might be possible to provide a greater incentive to carry out peer review and to raise the quality of those reviews using some of the currently available internet-based technologies. The proposal also provides a mechanism to track the review process and has the potential for wider application within the academic publishing environment as an alternative metric to those used at present.

# 2 Proposed System

## 2.1 Blockchain

The incentive to improve the peer review process might to be to pay the reviewers some real money but obviously it's not a good option here for there are potential conflicts of interest. Instead, the technology of BlockChain allows for alternative currency exchange mechanisms, and we can found a new exchange system using the cryptourrency similar to bitcoin (caledl r-coin in the paper referred to 'ReviewCoin')
The BlockChain has the advantages:

- It is a distributed accounting system not owned by any specific organisation. No one has the only right to modify the system.
- It is difficult to corrupt and transactions are anonymous, which means that it is difficult for 'bad guys' to modify the review due to interfere the publication of a paper.

## 2.2 R-coin system

In order for this exchange system to work, authors need to register an ID using a system such as ORCID to confirm their identifications and then submit their ID to the journal or through Publons when doing a peer review. Then they are paid with r-coins. The exchange mechanism will be talked at next part.
The new journals needs a registration process to join the r-coin currency in case of unscrupulous people from setting up publications that do not conform to the rules agreed by the community. Also, a lot of journals, are not so fabulous that should be excluded from participating. A body that decides which journals were acceptable is needed.
Finally, the r-coin is just 'present' for review. The r-coin system only provides a "right to publish" mechanism. It couldn't be access to the 'real' money transaction.

## 2.3 Transaction Mechaisms

### 2.3.1 Pay for one publication

The author should pay some r-coin to require a peer review, but this will have many conditions. When multiple authors are involved in submitting a paper, then should the cost be shared equally, or only the corresponding author pay or the authors could decide their own r-coin contribution that could be a reflection of their contributions to the paper.
The cost of submitting a paper to a journal would need to be agreed and whether that cost was the same for all journals or journals could set their own price.

### 2.3.2 Earn from review

The participant will only earn the r-coins from review. However, the payment of the amount of r-coin could also be related to timeliness where less r-coin is paid if a review is late. The reviewers would be paid more r-coins per review the more reviews that were completed.

### 2.3.3 Expansion of currency pool

There are two ways to expand the r-coins pool.

**New registration.** An author would be given a certain amount of r-coin during the ID registration process. Every new author will have an initial r-coin budget so that they can then start submitting papers to journals. This also resolve the lack of budget for a new research.

**Review** The r-coin is paid once an editor accepts the review in terms of meeting the journal's quality requirements. But the payment of the amount of r-coin can be changed in each transaction(review) which depends on the factors mentioned above, thus the r-coins that an author pay is not equal to the total of what the reviewers receive. In this method, the pool expand and it also encourage peer review.

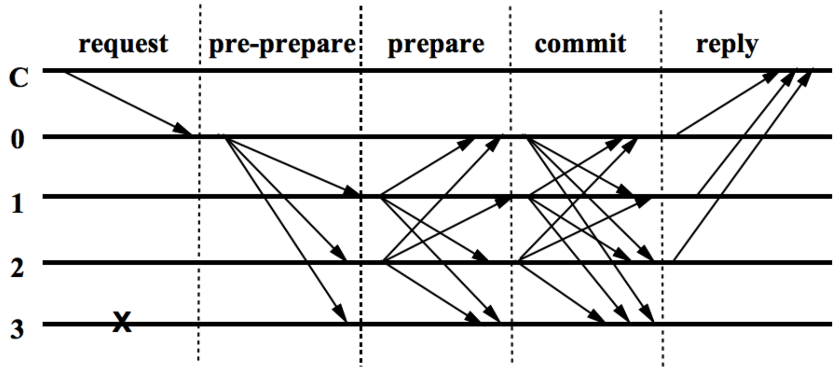
# 3 My work

My work is on the consensus.

## 3.1 Practical Byzantine Fault Tolerance

We assume an asynchronous distributed system where nodes are connected by a network. The network may fail to deliver messages, delay them, duplicate them, or deliver them out of order.
We assume $R \geq 3n + 1$ nodes, where $n$ is the maximun for nodes that may be faulty. In every consensus, the system will choose one node as the primary and the others become the backips.
The algorithm works roughly as follows:

- A client sends a request to invoke a service operation to the primary
- The primary multicasts the request to the backups
- Nodes execute the request and send a reply to the client
- The client waits for 1 replies from different replicas with the same result; this is the result of the operation.



The step of node execute the request can be divided in three parts.

**Pre-prepare** The primary assigns a sequence number, $n$, to the request, multicasts a pre-prepare message with$m$ piggybacked to all the backups, and appends the message to its log. The primary tells the backups a protocal is arosen.

**Prepare** The backups get the message from the primary and check the message is legal. They will multicast to all other replicas and adds both messages to its log. Otherwise,it does nothing. The nodes will accept at least $n + 1$ non-faulty messages (the same as itself) . Then they will go to the commit part or just stop here.

**Commit** The nodes calculate the new block and multicast the new block. If any node in the chain receive at least $n + 1$ blocks as a same block. This block will be written on it blockchain.

## 3.2 Delegated BFT

The disadvantages of PBFT is that all the nodes are static, so if $\frac{1}{3}$ of the nodes is offline, the system is breakdown. The PBFT also have the problem that if the number of the nodes is large. The time cost may be very big. Actually, it's better to used in a system with a few nodes.
Learned from DPOS(Delegated proof of stake), Neo Smart Economy give a

variation of dBFT(Delegated Byzantine Fault Tolerance).
The dBFT randomly divided the nodes as two parts - only one part of them in 'congress' can vote for the new block but the other one can also record the information but have no right to vote. But the division of the congress and the other is always changing.
Then the algorithm works roughly as follows:

- Using a ramdom number to decide who is in the congress and suppose that there are $R = 3n + 1$ nodes in the congress, where the $n$ is the maximum of faulty nodes.
- A client multicasts a request of transaction and the every node in the congress log this transaction.
- Once the new block is to be written, the primary multicasts the request to the backups in the congress.
- Nodes execute the request also like what PBFT do, at last they multicast the new block to all the node in the network. Every node, receive the new block and wirite it to its own chain.
- If the primary is accused of being faulty, the primary lose its right. After a certain time (or even just change the congress every time we reach the consensus), the division of the two parts of nodes will also alter.

### 3.3 Changes in this System

Now we talk about the division of the congress.
At the beginning, I want to divide the users as two parts- one is of researcher and the other one is for the press. The press users has more right and possibilty to be one of the congress in the system. However it will reduce the difficulty to attack the system- hackers can achieve an attack by controling less nodes that in the press users.
This part is about what I plan to do.
The computation won't tell the lies. So we will use a ramdom number to decide the division. Like the proposed Algorand, which use a random number to dicide the vertifiers (those in the congress). Every node calculate the random value with its private key by a random function which is defined with the current block at last proposal. If anyone is satisfied with some conditions, It becomes the vertifier and multicast the information. All the nodes regards the node of the least random value as the leader in this proposal. After a new block is written, a new random functions with the information of the new block forms and every node in the network calculate the new random value. In this case, the hackers can never succeed to predict who is the next leader or the vertifiers.

## 4 Future Work

We have done the simulation (referring to my partners' report). The future work, we first complete the consensus and then try to implement our model on the Hyperledger .

## References

[1] Michael Spearpoint. A Proposed Currency System for Academic Peer Review Payments Using the BlockChain Technology

[2] Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance. Third Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999

[3] NEO- DBFT Whitepaper

[4] Algorand- Jing Chen, Silvio Micali