Chapter 10
Scientific Paper Peer-Reviewing System With Blockchain, IPFS, and Smart Contract

Shantanu Kumar Rahut
East West University, Bangladesh

Razwan Ahmed Tanvir
East West University, Bangladesh

Sharfi Rahman
East West University, Bangladesh

Shamim Akhter
https://orcid.org/0000-0003-1408-9133
East West University, Bangladesh

ABSTRACT

In general, peer reviewing is known as an inspection of a work that is completed by one or more qualified people from the same profession and from the relevant field to make the work more error-free, readable, presentable, and adjustable according to the pre-published requirements and also considered as the primary metric for publishing a research paper, accepting research grants, or selecting award nominees. However, many recent publications are pointing to the biasness and mistreatment in the peer-review process. Thus, the scientific community is involved to generate ideas to advance the reviewing process including standardizing procedures and protocols, blind and electronic reviewing, rigorous methods in reviewer selection, rewarding reviewers, providing detailed feedback or checklist to reviewers, etc. In this chapter, the authors propose a decentralized and anonymous scientific peer-reviewing system using blockchain technology. This system will integrate all the above concern issues and eliminate the bias or trust issues interconnected with the peer-reviewing process.

DOI: 10.4018/978-1-5225-9257-0.ch010

INTRODUCTION

In general sense, peer-reviewing is known as an inspection of a work that is completed by one or more qualified people from the same profession and from the relevant field to make the work more error free, readable, presentable and adjustable according to the pre published requirements. Peer-reviewing is considered as the primary metric for publishing a research paper, accepting research grants, or selecting award nominees. However, many recent publications are pointing question to the biasness and abuse in peer-review process including author conflictions, authors from less prestigious institution, awarding women author, negative studies, idea stealing etc. Thus, scientific community is involved to generate ideas to advance the reviewing process (despite abandoning it) including standardizing procedures and protocols, blind and electronic reviewing, rigorous methods in reviewer selection, rewarding reviewers, providing detailed feedback or checklist to reviewers, and etc. In this chapter, we are proposing a decentralized and anonymous scientific peer-reviewing system using Blockchain technology with modified cryptocurrency (as reputation points) method. The system will integrate all the above concern issues, and able to eliminate the bias or trust issues interconnected with peer-reviewing process using decentralized authorities or without intermediaries, but improve reliability, transparency, and streamlining in the entire process. Publishing a research paper takes several steps from start to finish. Peer-reviewing process is one such step where a proposed article or work is evaluated or scrutinized by other experts in the matching subject to ensure quality of research contribution and to increase credibility. Experts play an important role in this process and help to validate a research, evaluate the method, establish the strengths and weaknesses and finally provide a reasonable judgment to publication. However, many recent publications are pointing question towards the biasness and abuse in peer-reviewing process including authors conflicts of interests, authors from less prestigious institution, awarding women author, negative studies, idea stealing etc. As a consequence, peer-reviewing is very successful in many instances however it also has few fail instances. Abandoning peer-reviewing may cause unreliability and less navigability in scientific article publication, and thus scientific community is involved to generate ideas to improve the reviewing process despite abandoning it. In this chapter, we will inspect different peer reviewing processes, applications, technological advancements, and drawbacks or challenges in existing peer reviewing system. Thereafter, we will propose an innovative decentralized and anonymous scientific peer-reviewing system using Blockchain, IPFS, cryptocurrency and smart contact technology.

EXISTING PEER REVIEWING SYSTEM, DRAWBACKS AND CHALLENGES

It is assumed that the first peer- reviewing process was archived in a book named “Ethics of the Physician”, written by a Syrian physician, Ishap bin Ali Al Rahwi (CE 854–931). Back then, other physicians used peer-reviewing on a given prescription to the patients to see if they are being treated according to the standards (Spier, 2002) or not. The idea of peer-reviewing was started from here. Later, many media, and literature societies started practicing the peer-reviewing system for their own development and improvement of knowledge. The societies submitted their works to the committee where the committee reviewed papers, accepted or recommended for any changes (kronick, 1990). In 1731, the Royal Society of Edinburgh instigated the peer-review system in Scholarly publication with a bunch of peer-reviewed

medical papers. But the publication of articles was decided almost 100 years later after (Shema, 2014). In 1831, William Whewell of royal society of London proposed the *Proceeding of the Royal Society* where the new papers were included. That's where the real peer-reviewing was started (INFOGRAPHIC). At first, the single blind review was adopted, where the reviewer was anonymous, but the author name was known to the reviewer. This process was garbage as the papers were not well reviewed and most of the time the reviewer was biased (Csiszar, 2016). "Editor plus two referees system" became quite popular among the scholars for peer-reviewing. Then "Double-blind" peer-reviewing was adopted to avoid bias (Rowland, 2002). This process is now used to review most of the scientific papers with some updates which will be discussed later.

Currently peer-reviewing is the "most standard" process for any scholarly publication. Researchers are relying on the peer-reviewing process which they found most useful for a better research paper. Almost 90% scientist recommends peer reviewing is effective for the development and improvement in technological areas (Mulligan, Hall & Raphael, 2012). Researchers and Scholars are getting their works reviewed by peers, which is helping them to work further and gives them the room for improvement. The papers which are being accepted is adding values to the scientific inventions and technological advancement. Papers which are being sent back to the author for a correction are getting a second chance to remove their lacking.

As the history says, the peer review started at the medical sectors, still the medical journals use peer reviewing which helps to get more realistic results in different sectors in medical science. Besides journals for Computer science, Biotechnology, Genetics, Physics, Mathematics also use peer reviewing system (omicsonline).

When a scientific paper is submitted for peer -reviewing, it goes through several steps. After finishing the research work, at first, the author submits his paper to journal. Here comes a journal editor, who reviews the paper if it meets the criteria of the journal. Not all the journals follow the same pattern for accepting a paper, some journal may have different criteria than traditional approach. The Editor makes sure of the paper submitted has met all the criteria and it can proceed further. But if the paper does not stand up to the mark of the journal, the editor informs the author that his paper was rejected. In next step, when the paper has passed the test and has met all the requirements of the journal, it is sent to the reviewers, who are eligible to review the paper. The reviewers are also known as the referees. After the paper has reached to the reviewers, they examine the paper thoroughly. They mark every detail and evaluate the papers methodology or proposed models; how much they can contribute or there is any error or corrections in the paper. They also determine the originality of the work. The references are also checked by them. The reviewers write a report on the findings from the submitted paper and give it to the editor.

What editor does is, he checks the reports from the reviewers. If there is no error, the paper gets accepted. But if the reports recommend any major or minor correction in the paper, the editor notifies the author to make changes and then resubmit. After updating the paper as per the recommendation, the paper is again sent to the editor who hands them to the reviewer again. If this time everything is fine by the report of the reviewer, the paper is accepted and published in the journal. The papers also can be rejected if the report is negative from the reviewers.

Not all the journals follow the same pattern for accepting a paper; some journal may have different criteria than traditional approach. Different journal uses different type of peer-reviewing system. There are a few forms of peer-reviewing that are currently being used by the journals. Here are some common types of peer-reviewing systems:

- **Single Blind Peer Review:** Author does not know who will evaluate the paper; the identity of the reviewer is unknown to the author of the paper. On the other hand, reviewer will know the authors identity.
- **Double Blind Peer Review:** In this system, author and reviewer, both sides are not disclosed to each other's identity.
- **Open Peer Review:** There is no hiding in this system. Author and reviewers are well aware of opposite side's identities. When the final paper is published, reviewers comment as well as authors response can be published in this system.
- **Collaborative Peer Review:** Most of the time reviewer's identity is hidden which is disclosed at the time of publication. Authors and reviewers are given a platform where they can discuss about the improvement sides of the paper.
- **Third Party Peer Review:** Before approaching to any journal, author does a review by an independent peer reviewing source. After getting review from there, author submits it to the journal.
- **Cascading Peer Review:** Various journals have target readers. If the submitted paper is not for those particular readers, the paper can be rejected after review. In that case the journal may suggest the author to submit the paper to another journal. Most of the time the journal gets published in the next one.
- **Post Publication Peer Review:** After the paper is published, it is available in a platform where others can read the paper and comment of their perspective and thoughts about the paper.

In the peer-reviewing system, no paper can get through easily without going through a several stages. Those have to go through the heavy guard of the reviewers who have their own field of expertise. These reviews are called as the "Gatekeepers" of science (Hojat, Gonnella & Caelleigh, 2003). They have a vital role on the inventions and research areas. They always keep their guard on when it comes to the paper reviewing, as it can make a huge difference in science and belief. Though peer-reviewing is the most used process among the scientific community, it faces much criticism. Even with so much popularity, the process has many drawbacks. The accusations on the process are like these:

- **Poor Evaluation:** Sometimes the reviewers are not so careful about evaluating the paper with full consciousness. The mistakes are not always found by the reviewers. The reviewer may not even read the paper and the paper gets through the journal. A few times the reviewers overlook the errors and the paper gets published. This type of carelessness can create a mislead idea on the particular topic.
- **Personal Conflict:** In peer reviewing system, there can be a conflict between author and reviewer, as the identity is known. In that case, if the editor sends the paper to the reviewer who has internal conflict with the author, can willingly give bad reviews about the paper submitted. As a result, the paper can be rejected by the journal despite of having quality content.
- **Gender Biasness:** The gender discrimination is a worldwide problem. In every sector, gender biasness exists. The cases are found like when the editor is male; he refers the paper to a male reviewer. Same thing happens when the editor is female (Stoye, 2017). Again, the acceptances of the paper submitted by the female authors are more likely to be accepted than the male authors. But a smaller number of females are invited by the journals to review papers (Lerback & Hanson, 2017).

- **Manipulated Priority:** When a paper is submitted under a particular journal or in any conference, if the author who submitted the paper is related to that situation, the publishers tend to prioritize their paper to be submitted and get published.
- **Conformity Bias:** The reviewer's point of view can be different from the authors. In that case, reviewer can give negative feedback about the paper that has not matched his view to that. This does not mean the submitted paper has misconception. The paper can be disqualified even if the editor does not agree with the concept of the paper. These decisions can put important inventions to danger (Mahoney, 1977).
- **Professional vs. Newbie:** In almost every aspect of life, people tend to prioritize the professionals and who is well recognized to people rather than a newcomer who may have the potential to serve something good. In this peer reviewing system, editors and reviewers try to make the known author's paper published rather than the newcomers. This is known as the "Matthew Effect" in scientific arena (Sharp, 1990), which is a tendency to highlight the high profiled author more than the low profiled ones.
- **Reviewer's Background:** A submitted paper can be reviewed by a number of reviews. Each reviewer has their expertise in their own field. There can be a different number of opinions from the reviewers, which can lead to the rejection of the paper. Even the journals can reject a paper based on the reviewer's feedback. It is not rare that a paper has been reviewed by a professional from another field. It makes a biasness form the reviewer's own expertise field.
- **Journal Policy:** Many journals can have their own hidden policies by which most papers submitted cannot go through. These journals are not often public about their policies. So, it is hard to tell if a journal will be published or not in a particular journal (Hojat et al, 2003).
- **Manuscript Fraud:** It is possible that the author can change some parts of the original paper and submit another paper as a new one. This can happen when the paper is rejected at the first place. Sometimes the reviewers can also steal an idea from the paper and make the idea as his own.

So, despite of being so popular among the science area, the peer-reviewing process has many challenging sides. From all the above problems, we can see that the biasness between author and reviewer gets the most focus. Most of the problems are related to the reviewer's opinion about the author, relation between them, competitiveness, point of view etc. In many cases there are accountability problem, the people in power which are editors and reviewer are doing as they want without being accountable to anyone. Conflict of interest also has a huge impact on this peer-reviewing system. These problems can be misleading for anyone who is related to science. It can take the new scientists to a wrong path. Science has its own risk with the peer-reviewing system. These identified problems should be solved as soon as possible to make sure the science to not go to a wrong direction. For the welfare of the science, a new concept of paper reviewing should be adopted. Thus, in the current peer-reviewing system, a journal holds the control of the whole system of peer-reviewing if the paper should be published or not. If we can have a system that the review system is not centralized; not only one person handles the whole process, but everyone has the ability to justify the process, the biasness in the system can be reduced. Both the editor and reviewer would be accountable for their deeds, also the author. Everything would be transparent so that the others can make sure the right thing has been done. In this platform, everyone would get a chance to participate in the development of the future of science with transparency.

In these recent years, Blockchain technology has emerged which can bring transparency in any system where it is implemented. We will have a detail discussion on Blockchain in next section. This technol-

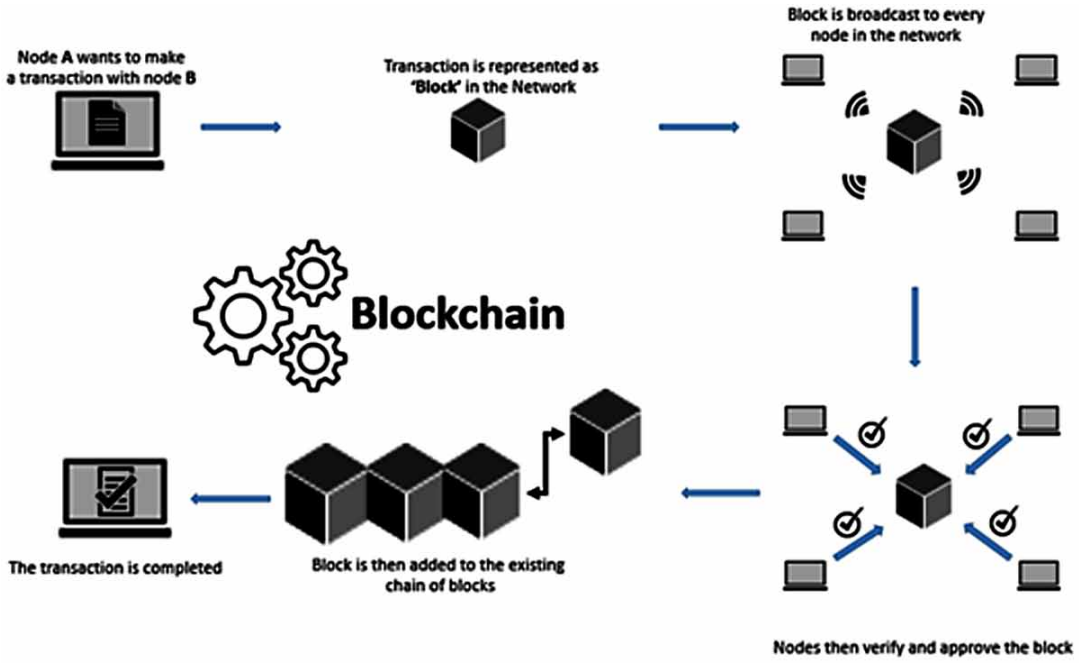
ogy can make sure of the proper reviewing of a paper in many extend. If we can make a platform where Blockchain technology is implemented, the distribution of the paper can be safe and secured as it will have node to node encryption system, so there is no possibility to go the paper in wrong hand. Without this, the system has an approval option for all the nodes, so it is not possible for a single human to spread anything wrong. Besides, the Blockchain system is decentralized, so there is no chance for manipulation of the paper in case of any biasness. If the file uploaded is manipulated somehow, the encryption of both ends will not work. So, this Blockchain technology can bring a change when it comes to the transparency of the scientific paper peer-reviewing system.

BLOCKCHAIN AND OTHER REQUIRED TERMINOLOGIES FOR PROPOSED PEER REVIEWING SYSTEM

Blockchain

In general, Blockchain is a digital ledger of transactions that are continuously updated and broadcasted within a distributed network. Every node in this network has an exact copy of that ledger or accounting book. Each and every transaction between the nodes is echoed in that distributed ledger. By storing the same ledger across the network, Blockchain cannot be controlled by any single authority and it has no single point of failure. For every successful transaction, a block is appended to the existing chain of blocks by a secure and strong cryptography and the updated ledger is shared among the distributed network. To ensure every node in the network has identical version of the ledger. Proof of Work (PoW)

Figure 1. Mechanism of blockchain



mechanism integrates a system of collective consensus and verification through mining to certify that no conflicting versions of that ledger is emerged. This mechanism also ensures the immutability of the stored data in a block without having a central authority.

The uniqueness in Blockchain technology lies in the distinctive properties of this system. Some of its protocol features are listed below:

- **Replication:** The data on the Blockchain is stored on every node that is a part of the network. So, the ledger is replicated and kept on each computer connected to the network.
- **Immutability of Data:** The blocks are linked with one another, storing the previous node's hash. So, if a node is edited then the hash of that node is also changed. Therefore, the hash stored on the next block will not match with the changed hash of the edited block. Thus, if one node is edited then all the blocks after that will be unverified. By this, the immutability of the data on Blockchain is reserved.
- **Irreversibility of Transactions:** Once a transaction is recorded on Blockchain then there is no way to reverse, hide or alter that transaction. Only a new transaction should be done to retract the effect of that transaction. Say, user A accidentally made a transaction of 5 units to user B. Then there is no way to reverse this transaction unless B makes a transaction of 5 units back to A.
- **Distributed System:** The Blockchain ledger is distributed to all the individual nodes on the network. The ledger is maintained by the users of the network.
- **No Central Authority:** No central authority can govern the network. All the nodes are part of the decision and this is ensured by the consensus among the nodes of the network.
- **No Single Point of Failure:** As the ledger is distributed all over the network, there is no central point of failure in Blockchain. Everyone has the copy of the exact same ledger.
- **Resilient:** Blockchain network utilizes the consensus model to resolve the changing state of the ledger. By a consensus algorithm, the ledger accepted by the network always reflects the exact scenario of transactions. A ledger will be accepted if 51% or more nodes have the exact same ledger. This ensures the resiliency of the network.
- **Anonymity:** Bitcoin – is built on Blockchain technology. Bitcoin only uses public-private keys to identify a user. The user needs not to provide any other information like name, address, age, gender etc. (BLOCKCHAIN COUNCIL). So, in another words, Blockchain technology provides anonymity.

The usage of Blockchain is excitingly increasing nowadays. Various applications have been seen in recent years which rely on Blockchain mechanism. The application domain of the Blockchain Technology (BCT) is vast and expanding. Presently, Blockchain technology is mostly used in the field of Finance, Healthcare (Ekin & Unay, 2018) (Zhang, Walker, White, Schmidt & Lenz, 2017), Gaming, File Transfer (Kiyomoto, Rahman & Basu, 2017), Security, IoT (Chen, Ma, Ye, Zheng, & Zhou, 2018) etc.

Blockchain has shown a new path to the gaming industry. By using crypto-currency the players can transact their unique avatar and all. (CryptoKitties, 2018) is considered the most successful Blockchain based game. The player of the game can make transactions using smart contract on Ethereum Blockchain. There are other games based on Blockchain such as (CryptoCelebrities, 2018), (Etherbots,2018) etc. E-voting system is emerging to provide transparency to the voting system. The inherit properties of Blockchain technology provides transparency to any system. Nowadays the E-voting is gaining attention.

Various models of E-voting based on Blockchain (Hjalmarsson, Hreioarsson, Hamdaqa, & Hjalmtysson, 2018; Kshetri&Voas, 2018) are proposed. Even, government information can be stored in Blockchain because of the immutability, which is very important especially for government information.

CRYPTO-CURRENCY

One of the fields where Blockchain is being currently used is crypto-currency. The "crypto" in the word crypto-currency stands for cryptography which is a technology that keeps information safe from unauthorized access. So, crypto-currency is a cryptographically secured digital exchange. This peer-to-peer digital exchange system requires the distributed verification of transactions as this system has no central authority. In 1983, eCash (Chaum, 1997) was developed by Chaum which is an anonymous electronic money exchange system. But unlike crypto-currencies, the eCash was centralized and controlled by banks. PayPal (Valenta & Rowan, 2015) is also an online Money Transfer System which issued to send and receive money from each other. These systems do not have their own currency. But crypto-currency has its own currency. In 2008-09, Bitcoin (Nakamoto, 2015), the first crypto-currency, was implemented by Satoshi Nakamoto. And after that various crypto-currency systems came into existence like Ethereum (Wood, 2014), Litecoin (Litecoin, 2018), Ripple (Schwartz, Youngs & Britto, 2014), Namecoin (Kalodner, Carlsten, Ellenbogen, Bonneau & Narayanan, 2015) etc. But the functionality of all the crypto-currency systems is somewhat similar. A user of a crypto-currency has a wallet address which is a public key of that user. That public key has a private key. Public and private key are together known as Public-Private Key pair. The private key is used to sign the transactions the user makes. The ownership of a coin is given to the person who has in possession of the private key of the public/private key pair. The user sends money to other users' address which is the payees' public key and signs the transaction using his (sender) private key. Then the transaction needs verification by the miners. These are the steps which need to be performed to exchange currency in any crypto-currency exchange systems. The key pairs are stored in a file named 'wallet.dat' which is the most important file as if any user loses or has the file stolen, and then he will lose the ownership of those coins. Through decentralization, the control of the network is given to the users of the network. So, everyone is responsible for the security of their files. There are different types of crypto-currency at present. Bitcoin, Litecoin, Ether etc. are the most used crypto-currency.

SMART CONTRACTS

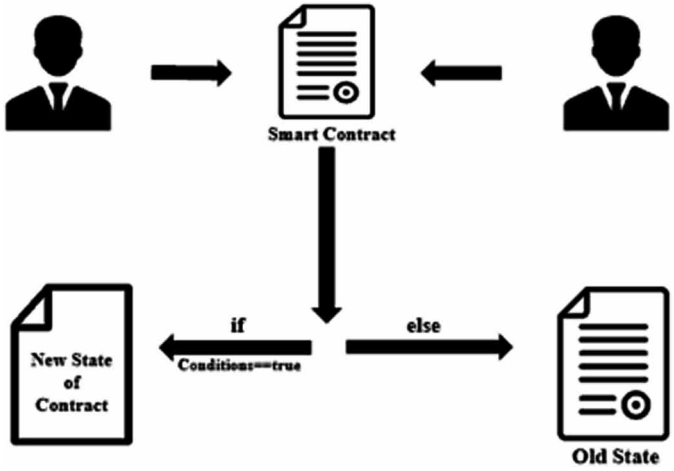
American cryptographer Nick Szabo described smart contract in 1996, long before the development of Blockchain. Szabo described a contract as – 'a set of promises agreed to in a "meeting of the minds", is the traditional way to formalize a relationship.' In the article on smart contracts (Szabo, 1996), according to Szabo, smart contracts are set of rules for transferring information that automatically execute, when the conditions of the contracts are met. Back at 1996, this definition did not mean much to that time, because required technologies like distributed ledger were absent at that period. After the appearance of Bitcoin, the first crypto-currency, the distributed ledger was implemented by Blockchain technology and that is how a new era for smart contracts started. Though Bitcoin only allow that the information of the transaction must be in the block. So, still smart contracts were not useful with Bitcoin.

Smart contract can be considered a sophisticated Blockchain network's node that can store procedures to be called under some specific rules. It provides features to eliminate intermediaries from a contract happening between two or more parties. This is a computer or computer program which is used to enlist the terms of the contracts in "if-then" form when two parties agree to the contract's terms, then the encrypted code is securely replicated to the decentralized ledger which ensures the transparency. If the conditions stated in the contracts are met, then the code autonomously executes the transaction. After every execution of a smart contract, the states of that contract are changed. By 'state' here it means the data that smart contract stores in a certain point of time. The autonomous execution and surety of the agreement remove third party interference on the contracts. Smart contract provides services to exchange money, goods or other assets which have some value. So, smart contracts can be applied to make transactions on a variety of use cases.

Below a simple visualization of how smart contracts work is depicted.

Smart contract is now being implemented to solve wide range of problems. Healthcare, Finance, Elections, E-commerce, Taxation and many more sectors are using the services of smart contract along with Blockchain. In the health care sector, faster data sharing is important and related to the chance of recovery of any patient. Blockchain is also integrated with IoT (Dey, Jaiswal, Sunderkrishnan & Katre, 2017) to store health data in Blockchain to provide faster medical response. Considering the privacy of medical data, Blockchain and smart contract are helping to provide security for medical data. In finance or in business, the use of smart contract is rapidly increasing. The supplier role automation in the electricity supply (Thomas, Long, Burnap, Wu, & Jenkins, 2017) was developed based on the smart contract. In business the trading and the privacy of the users can be ensured by the smart contract (Niya, Shupfer, Bocek, & Stiller, 2018) which make trading reliable and flexible. Blockchain and smart contract have opened a new possibility of developing a transparent E-voting system (Hjalmarsson et al, 2018) and (Kshetri&Voas, 2018). These E-voting systems based on Blockchain and smart contract provides the reduced chances of fraud and increase voter access. Everyday new use cases are designed utilizing the possibilities of smart contract and Blockchain. Various new innovations (Ahram, Sargolzaei, Sargolzaei, Daniels &Amaba, 2017) are a matter of time now which will be implemented by smart contract and Blockchain based systems.

Figure 2. Working mechanism of smart contract



Pros and Cons of Smart Contract

Pros

- **Reliability:** As smart contract works with Blockchain, the data stored in Blockchain cannot be altered or modified. So, alteration of contract's conditions is impossible. So, smart contract provides the reliability.
- **Speed:** Smart contract does not have any personal involvement. Thus, its execution is faster which saves huge amount of time. It eliminates the time delay of the completion of contract objectives which serves faster transaction and contract completion.
- **Low Cost Execution:** Smart contract serves its services with minimal cost as it removes the third-party interference in the contract. The operational cost is thus reduced.
- **Accuracy:** All the conditions of the contract are inspected by the contract program automatically which provides higher accuracy than human inspected contracts.
- **Independence**: Smart contract eliminates the involvement of third party in a contract. The trust issues are handled by programming. So, the integrity is ensured by the contract itself.

Cons

- **Immutability:** Smart contract is inherently immutable that is, no one can alter any part of a contract. So, if the parties want to alter or modify the condition after forming the contract, they must need to create a new separate contract. So, immutability is providing the security, but this may cause problem when parties want to modify the contract.
- **Lack of Knowledge:** General people lack the knowledge of Smart Contract and Blockchain. This throttles the rapid development of application backed by these technologies.

IPFS TECHNOLOGY

Inter Planetary File System or IPFS is a protocol and a network. It has been designed to create a content-addressable, peer-to-peer storing and sharing hypermedia in a distributed file system (Finley, 2016).

IPFS will be used for a user to submit article for reviewing through the system. Some peer-to-peer systems like P2P sharing software (Ratnasamy, Francis, Handley, Karp &Schenker, 2001) use hash of the content to address it. Other technologies such as Git use complex Merkle-Linked Structures (Loeliger & McCullough, 2012). IPFS integrates both the use of complex Merkle-Linked structure with the data-addressability of P2P file sharing systems. The content is distributed over a peer-to-peer network (Tenorio-Fornés, Hassan & Pavón, 2018). So, IPFS is a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files. In some ways, IPFS is similar to the World Wide Web, but IPFS could be seen as a single BitTorrent swarm, exchanging objects within one Gitrepository. In other words, IPFS provides a high-throughput, content-addressed block storage model, with content-addressed hyperlinks (Allison, 2016). IPFS combines a distributed hash table, an incentivized block exchange, and a self-certifying namespace. IPFS has no single point of failure, and data transit cannot be tampered with (IPFS is the Distributed Web, 2018). Distributed Content Delivery saves bandwidth and prevents DDoS attacks, which HTTP struggles with (Cointelegraph, 2017).The

file system can be accessed in a variety of ways, including via FUSE or "File system in User space" (Filesystem in Userspace, 2018) over HTTP (Allison, 2016). A local file can be added to the IPFS file system, making it available to the world. Files are identified by their hashes, so it is cached-friendly. They are distributed using a BitTorrent-based protocol. Any user who downloads the file also serves the file to the other users of the network. IPFS has a name service called IPNS, a global namespace based on PKI, serves to build trust chains, is compatible with other NSes and can map DNS, onion, bit, etc. to IPNS (Ipfs/README.md, 2018).

TECHNICAL CHALLENGES OF BLOCKCHAIN

There are several technical challenges in adapting Blockchain. Many researchers identified different challenges of using a Blockchain technology. These are discussed below:

- **Throughput:** As for now, Bitcoin network can process only seven (7) transactions per second which is very few in compare to other money transferring networks like VISA and Twitter. So, the big scale implementation of Blockchain is a challenge.
- **Latency:** In Bitcoin Blockchain, all the transactions are verified by the miner nodes to ensure that no one can spend one coin more than once which is known as Double-spending. So, to ensure valid transactions Blockchain has to verify all the block added in the Blockchain every time a transaction occurs. This makes latency a great problem for the Blockchain technology.
- **Security:** Current Blockchain is vulnerable to 51% attack. 51% attack is an attack where only one party has the power over the majority of the network's mining hash-rate. Thus, he can manipulate the Blockchain. This issue is one of the big risk factors of a Blockchain based application.
- **Usability:** Nowadays, implementing Blockchain based application is hard because of the complex usage of the Blockchain API. More sophisticated yet easy-to-use technology should be developed to ensure usability of the features of the Blockchain technology.
- **Wasted Resource:** Huge energy is wasted to mine Bitcoin. Proof-of-Work causes this wastage of energy. There are also some alternatives to Proof-of-Work like Proof-of-Stake. Proof-of-Stake is used by the industrial applications to reduce the energy consumption. Proof-of-Work depends on the work done by the miner but on the other hand, Proof-of-Stake depends on the amount of Bitcoin the miner holds. So, different approaches need to be introduced to increase resource utilization by the Blockchain network.
- **Size and Bandwidth:** The size of the Blockchain grows with the usage of the network by its users. As of June 2018, the size of the Bitcoin Blockchain is 173gigabytes which is increasing since the creation of Bitcoin crypto-currency in 2009. If Blockchain is used by the mass people, the Blockchain size would be a problem. So, size of the Blockchain is a challenge which needs to be solved for the usability of the system.
- **Scalability:** The main issue of scalability problem in Blockchain is that every transaction in the network must be verified by the mining nodes (Mitra, 2017). Ethereum does 20 transactions per second and Bitcoin does only 7. So, obviously the scalability of these systems must be improved to compete with the existing transaction speed of money transfer systems. Presently the scalability problem of Blockchain is being addressed to make this technology useful for big scale imple-

mentations. There are several approaches to solve the scalability problem like Bitcoin Lightning Protocol (Hay, 2018), Ethereum Sharding (Jordan, 2018), DPoS Solution by EOS (Arora, 2018).

- **Privacy:** All the transactions in the Blockchain network are broadcasted to public. Transparency in the Blockchain network is ensured by the flow of information to all parties. But public can only see the transactions not the senders' and receivers' identities (Nakamoto, 2008). Around 24% studies of recent researches are on the anonymity issue of the Blockchain network (Yli-Huumo, Ko, Choi, Park, &Smolander, 2016). Centering on the ownership of the Bitcoin (Meiklejohn & Orlandi, 2015), presents a definitional model of anonymity. Again, various researches are based on the evidence that the Bitcoin Blockchain lacks the anonymity of its users (Koshy, Koshy & McDaniel, 2014) (Valenta& Rowan, 2015). To solve this anonymity problem many researchers proposed numerous solutions. Transaction mixing technique is applied to increase anonymity in the network. (Valenta and Rowan, 2015) has modified the Mix Coin protocol to prevent the address mapping of the receivers and senders.

PROPOSED BLOCKCHAIN BASED PEER-REVIEING SYSTEM

Generally, a peer-review process can be divided into three steps. First step is the authors will submit papers in the hope to get it reviewed and published. Second stepis the editorwill distribute the submitted paper to eligible reviewers. Third step is the reviewers will accept and review the submitted paper and send their reviews to the editor, and then editor will forward their reviews to the specific author.

The proposed method integrates all these steps with Blockchain technology and creates a decentralized platform for peer-reviewing process. Our proposed decentralized method of peer-reviewing system is also divided into three (3) different steps and presented in three (3) different sections. Section 1.4.1 includes information on how authors will submit their articles to the system for reviewing, how the system will find eligible reviewers, and how the submitted articles will be distributed among the reviewers with the help of IPFS. Section 1.4.2 includes information on how the reviews will be verified as a good, authentic and valid review. Section 1.4.3 includes information on the idea of crypto-reward system. It also utilizes smart contract for creating transactions. These transactions are used for passing information and selecting eligible reviewers, distribute papers for reviewing and etc. These transactions are affiliated with costs and that needs to be paid through Crypto-Currency. This section will examine all details of these implementations.

ARTICLE DISTRIBUTION

For distributing article through Blockchain for peer-reviewing process, the first step is to submit the article for reviewing through the system. The users of our proposed system can act on three (3) different types of roles-

1. Author
2. Primary Reviewer
3. Secondary Reviewer

If a user submits an article for the peer-reviewing process, he is an author or author node. He is denoted as #Author. If a user reviews an article, he acts as a primary reviewer or primary reviewer node, and denoted as #PR. If a user reviews the review of a primary reviewer, he is a secondary reviewer or secondary reviewer node, and denoted as #SR.

For reviewing each article, the system will find out and enlist Eligible Reviewers or #ER through TAG matching and Ranking Process. First three (3) of the enlisted #ERs who accept the proposal of reviewing an article, will be selected as #PR. After all, three (3) #PRs submit their reviews, there will be a similar enlisting process to enlist #SRs, first two (2) #ER from the list who accepts the proposal of reviewing the reviews given by the #PR on the submitted article will be selected as #SR. More details on TAG matching and Ranking Process will be given later.

Submitting Article: Use of IPFS Technology

Current Blockchain technology supports transfer of large amount of data in a single transaction but is very costly. So, our framework takes the help of IPFS for sharing large amount of data at low cost. The idea is simple. Upload something using IPFS. IPFS then provides a download link. The link is then shared with another user of Blockchain using a single transaction.

So, how does one user can share his file or article or paper through the system with the help of IPFS?

Let's look at the figure 3, #Author wants to submit an article or paper through the system. First, he/she puts the article in his/her directory and then tells the IPFS system that he wants to upload it. Then the IPFS system takes the address of the article and generates a hash that can be shared with anyone on the same network.

This process lacks the security of the submitted article as anyone could read it. But with Blockchain, in our proposed system the security will be assured. For better understanding let's look at the figure 4.

First, he/she puts the article in his/her directory and then tells the IPFS system that he wants to upload it. Then the IPFS system takes the address of the article and generates a hash that will be shared with anyone on the same network. Then the system encrypts the hash with the public key of #PR (who the author wants to share the article with). As it was encrypted with #PR's public key, only #PR could decrypt the hash and collect the submitted article using that decrypted hash as only he has the associated Private Key.

So, this is how #Author will submit his/her article or paper through the proposed system for peer-reviewing process, in a secure manner, with the help of IPFS.

Figure 3. Submitting article through IPFS

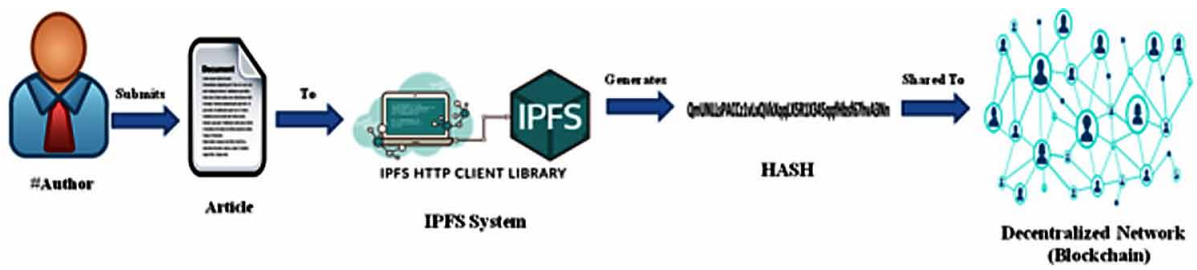
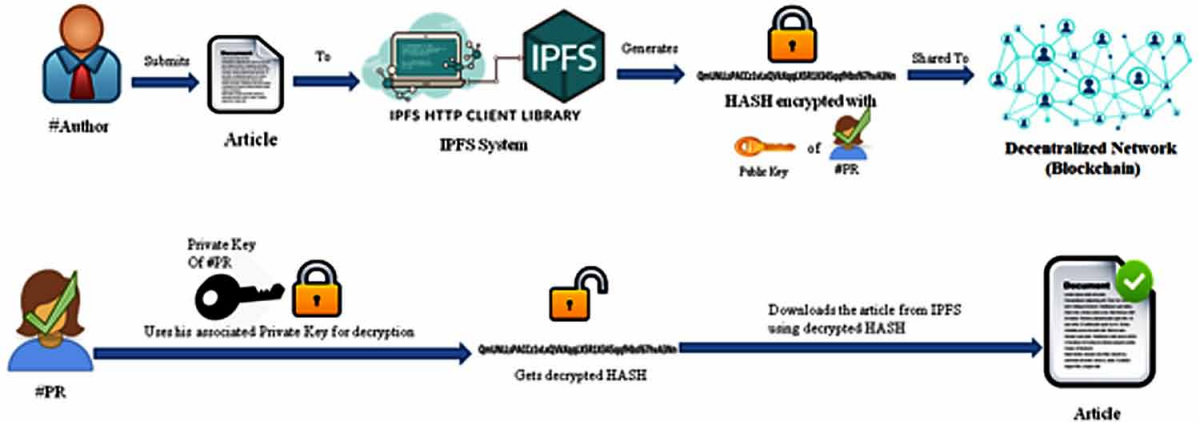


Figure 4. Submitting article through IPFS used with Blockchain (i.e. proposed system)



Whom to Ask for Reviewing?

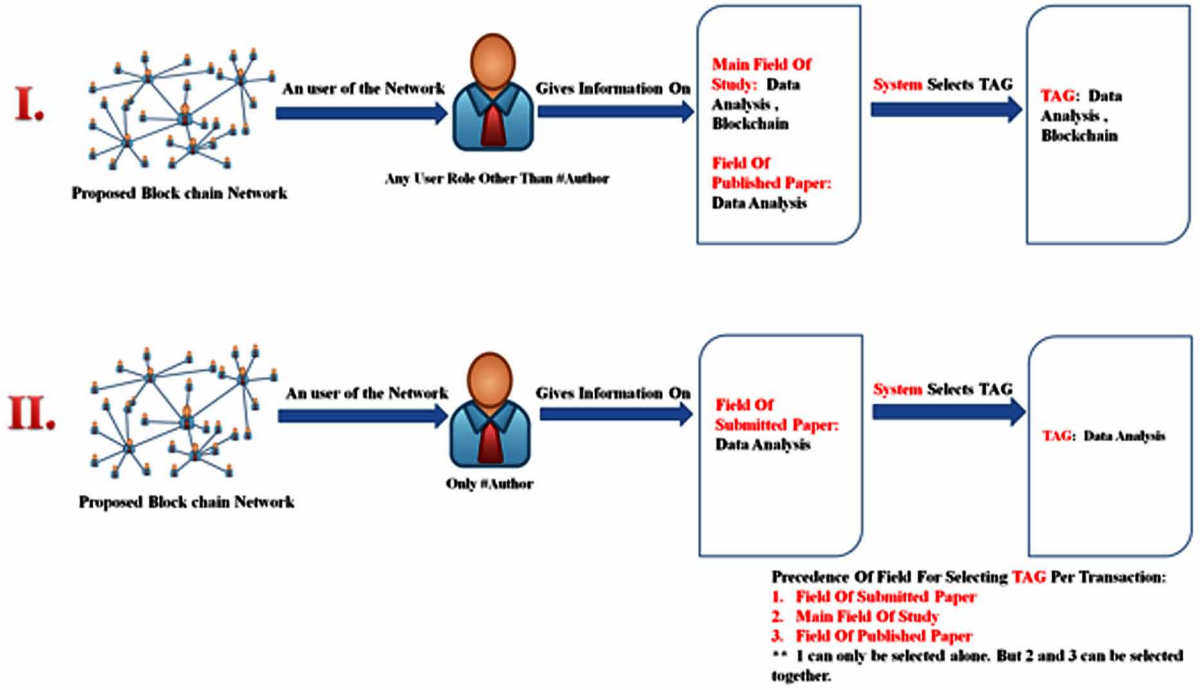
One of the most important parts of a peer-reviewing process is to send or distribute the submitted article to the perfect reviewers. A reviewer must be eligible enough to review that paper and needs to accept the job of reviewing the paper. A reviewer can be assumed eligible if he has sufficient knowledge about the field of study of the submitted article. It is presumable that a PhD holder from social science does not have sufficient knowledge to review an article submitted from the field of Data analysis. To review a paper related to Data analysis a reviewer should have sufficient knowledge regarding the study of Data analysis.

A reviewer can be assumed to be willing to accept the offer of reviewing the article if he explicitly agrees to do so. When asked if a reviewer wants to review a particular paper or not, he must answer "yes" or "no", and if the answer is "yes" it can be safely assumed that the reviewer is willing enough to accept the proposal of reviewing the paper submitted for peer-review. The proposed system solves the issue of selecting eligible reviewers and distributes submitted paper to the peer review process in a decentralized and anonymous manner.

Tag Based Field of Study Matching System: For Finding Eligible Reviewers

TAG is a text-based label attached to the users of the proposed system for the purpose of their identification or to give other information. When a person becomes a user of this system, he/she must provide some information so that it can be ensured that the person is authentic. She/he along with his/her other details must provide the area of research interest (or Field of study). Whenever, one of his papers gets published, she/he will be mentioned the field related to that published paper in his account. Every update in the account or related activity of a user will be treated as a transaction. Every transaction that happens in a decentralized system is kept as a record. During each transaction the system will automatically check the record and select TAGs for each user. From the figure 5 we can see a clear view of how the TAG selection process for a user works. When a user includes his/her field of study or the field of his/her published paper in his/her account, a transaction happens, and that field is saved as that user's TAG. If

Figure 5. TAG selection process



someone submits a paper through the system for reviewing, it is treated as a transaction and the field of that submitted paper is also saved as a TAG for that user. So, the system can select TAG for a particular user from three (3) different sources –

1. **Field of Submitted Paper:** The field of study related to the submitted article by #Author. #Author will give the related field name while submitting the article. (Source #1)
2. **Main Field of Study:** Main area of interest or field of study of a user. A user will give his/her main area of interest or field of study while opening an account on the system. He can always update the information when he/she wants. (Source #2)
3. **Field of Published Paper:** The field of study related to a published paper of a user. If he/she published it elsewhere he/she could just fill in the information in his/her account. If the paper was first submitted and then published in the proposed system, the system will automatically collect the field of the published paper from the previously given TAG while it was in submission phase (Source #1).For example, if a user submits an article or paper on Data Analysis, he/she includes the field of his/her submitted paper. If the article is published on the system, then the previously given field of submitted paper will be automatically collected by the system and it will be saved as the field of published paper. (Source #3)

The TAGs are selected from these three (3) sources while maintaining a special kind of precedence. If (Source #1) is found, then the system won't look for (Source #2) or (Source #3). If (Source #1) is not found, then the system will use (Source #2) and (Source #3) both as sources. The TAGs will be non-repeated and cumulative for each transaction.

So, in this way, a user who's Field of study is Data analysis (Source #2) and has some published works in the field (Source #3) will have TAG of Data analysis. If a user submits a paper related to Data analysis (Source #1) as an author, then he will also have a TAG of Data analysis. These TAGs will be selected, updated, modified and saved at each transaction in every user's block. Every user's account will always accommodate his TAG information so that the system causes the information whenever needed.

Now let us look at the figure 6for a better understanding of how the eligible reviewers are selected for article distribution.

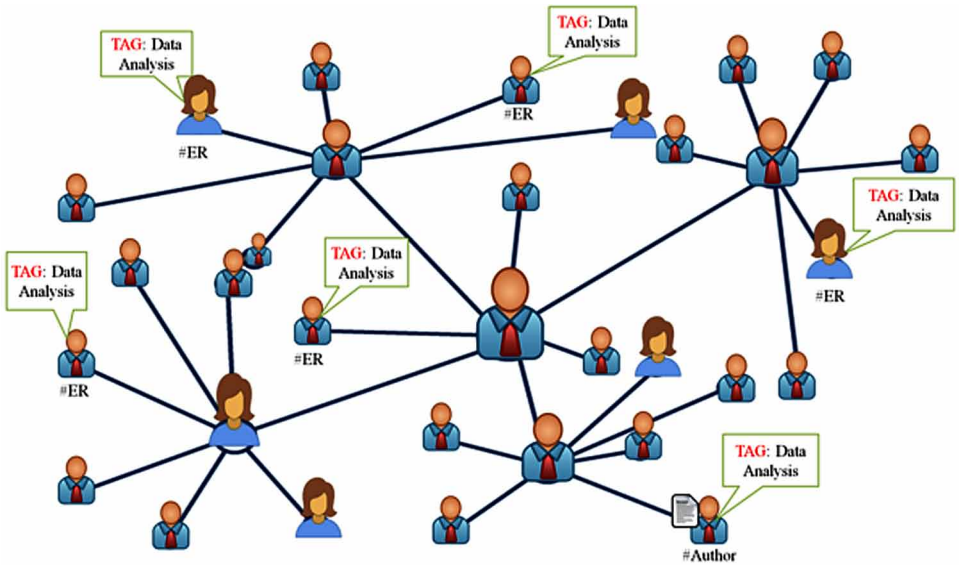
So far, the system has collected or selected some words based on TAGs from three (3) different fields. The TAG represents two (2) things-

1. The related field of a paper that was submitted for peer-review process
2. The field of expertise of a user

If both fields match that means a user's field of expertise matches with the field of the paper which was submitted for review. So, from the figure 6, a user who's Field of study is Data analysis (Source #2) and has some published work in the field (Source #3) will have a TAG of Data analysis. If a user submits a paper related to Data analysis (Source #1) as an author, then he will also have a TAG of Data analysis. The system matches the TAG of the author with the TAGs of other users to find the eligible reviewers for reviewing a paper submitted by the author whose TAG is Data analysis.

When a user acts as #Author node and submits his/her paper for peer-review process through the system, the user must mention the name of the field related to the submitted paper which will be used as the TAG. After he/she submits the paper through his/her machine, a request will be automatically generated. This request can be perceived as a "Hello" message. Every block in the system receives this request, asking them if anyone has the same TAG as the #Author. In each node, a string matching algorithm matches the TAG of the #Author with the TAG of the node. And if the TAG matches, then a reply is generated automatically, that can be perceived as something like "I have the same TAG as you!"

Figure 6. Eligible reviewer selection process



Every block or node that sends reply message to the #Author is enlisted as an eligible reviewer by the system. If there is a situation where no block is sending reply, there can be two (2) possible reasons-

1. There is no available user with same TAG
2. The reply was sent but was somehow lost

To solve this problem the #Author node will continue to send request automatically after an interval, until the node gets at least two (2) replies. The system will only start enlisting users as eligible reviewers only if there are at least three (3) replies.

There is not limitation on the number of users that can be selected as eligible reviewers. Any number of users can be selected as eligible reviewers by the system if the criteria of having the same TAG meet.

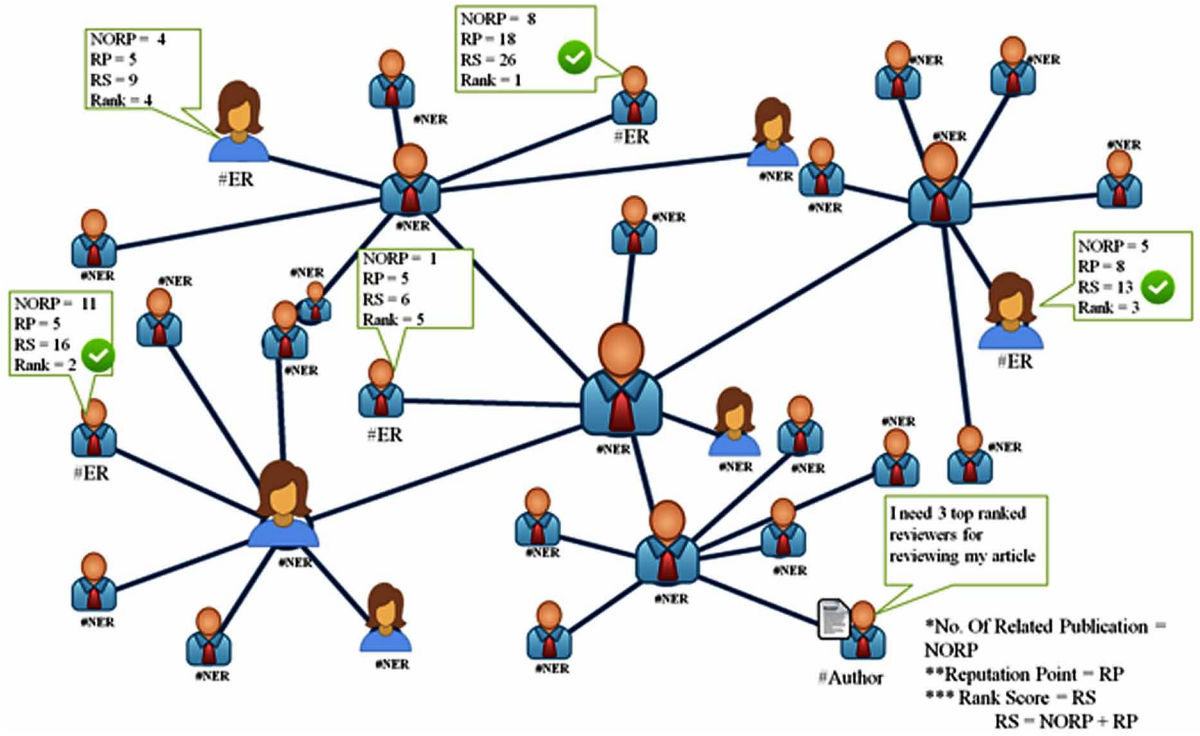
Reputation Point Based Ranking System: To Rank the Reviewers

After finding eligible reviewers through TAG matching process, the system will automatically rank those reviewers based on their reputation points and no. of published papers. Reputation points will be automatically generated by the system and given to a user if he/she successfully completes task as a review.

For better understanding of the Ranking procedure, let's take a look at figure 7.

Only the users who were found eligible by the TAG matching process will be enlisted for probable review process as an eligible reviewer. They are denoted as #ER or Eligible Reviewer. The users who

Figure 7. Ranking of eligible reviewers based on rank score



were not enlisted will be denoted as #NER or Not an Eligible Reviewer. After finding all available #ER, the system will try to give them rank through a simple process. Every #ER will get his own Rank Score after every time an enlisting process is completed. This Rank Score will be determined on the basis of two (2) different criteria-

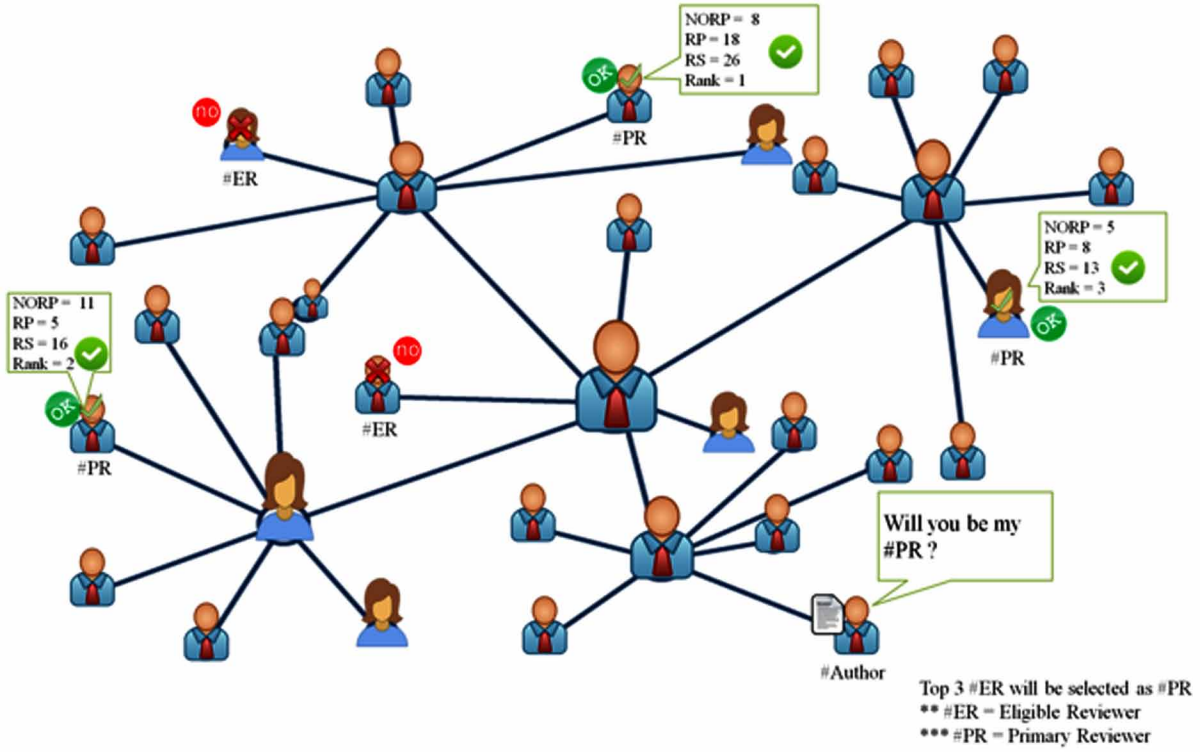
1. No. of related publications
2. Reputation Points

So, Rank Score = No. of related publications + Reputation Points; where No. of related publications indicates the number of published papers of a user on the same field as the submitted article.

No. of published papers will indicate the capability of the user as a researcher and reputation points will indicate the reputation of a reviewer. More will be discussed on Reputation Point (RP) in the next section.

Now, let's look at figure 8. All #ER that has been ranked based on their Rank Scores will be asked by the system if they want to accept the proposal of reviewing the submitted article or paper. An #ER has to explicitly agree to this proposal for becoming a primary reviewer or #PR of that submitted paper. There can be at least two (2) and at most three (3) #PR for reviewing one paper. After the criteria is met, the system will close the process of reviewing and until the review process is completed, selected #PR will not show up in TAG Selection or Reviewer Selection process for other submitted papers. In another word, #PR busy with one review process will not be bothered with new review proposals until the completion of his current job.

Figure 8. Top Three #ER getting selected as #PR after accepting proposal



After review process is completed by a #PR, he/she will give one of the below four ratings to that article-

- Accepted (A)
- Major Revision (MAR)
- Minor Revision (MIR)
- Rejected (R)

The submitted paper and the review decision of that paper together will be sent to the secondary reviewer as a part of two-step verification process. More on this process will be discussed in the next section.

If the submitted paper gets any other review decision than Accepted, it will be sent back to the #Author. If "Accepted", then the submitted paper will get published in the system. Here, publishing refers to adding the accepted paper to the Blockchain and becomes a part of an open access and eternal journal.

Transaction Using Smart Contract: Keeping Records

It has been said earlier that every update in the account or related activity of a user will be treated as a transaction. In this case Transaction is an exchange of information and may or may not be recorded for ever and may or may not be added to the Blockchain. The core infrastructure of Blockchain requires transaction to happen between two users in each time. And for one Blockchain based system, all transactions should carry same type of information. This framework utilizes smart contract to create all kinds of transactions.

Submitting an article or requesting reviewers, sending information about user's TAG, accepting review proposal, sending hash of the article to the selected reviewer etc. can be done through transaction. The figures given below could help us to understand more about how the transactions will occur in the system while distributing the article. These transactions should be similar to the nature of smart contracts (Szabo, 1996).

Transaction during TAG matching process could be as shown in Figure 9.

Figure 9. Transaction during TAG matching

Transaction during reviewer ranking process could be as shown in Figure 10.

Transaction during a #ER accepting review request and becoming a #PR could be as shown in Figure 11.

And transaction during #Author sending file hash to #PR could be as shown in Figure 12.

Each transaction happens between two (2) users at a time and is validated by every user on the system other than the two who did the transaction. So, when not reviewing a particular article, a user of the system will act as a potential block validation node by default, for the system of validating the transactions regarding that article. This is how article submitted through the proposed Blockchain based peer-review system will be getting distributed to the most capable reviewers for peer-reviewing process.

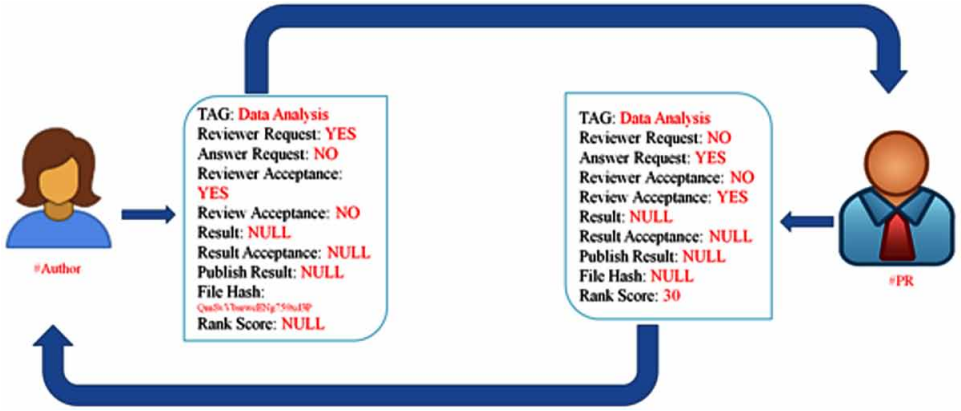
ARTICLE REVIEW VERIFICATION SYSTEM

After #PR or primary reviewer gives review of the submitted article, there remains a question whether the review was authentic or not. A #PR could just not review the submitted article and gives "Accepted" rating to it. This could pave a path for what the system tries to avoid, biasness and corruption in peer-

Figure 10. Transaction during eligible reviewer ranking process

Figure 11. Transaction during an #ER becoming a #PR

Figure 12. Transaction during #Author sending hash of his article to #PR



reviewing. To avoid this situation, the system proposes what it can be called as "Two-step verification process".

As it has been mentioned earlier there could be three (3) different roles a user can play –

- Author (#Author)
- Primary Reviewer (#PR)
- Secondary Reviewer (#SR)

Here, a #Author submits an article for peer-reviewing. #PR reviews the article. Any user other than #Author and #PR will go through the previously mentioned TAG matching process and Reviewer ranking process. Top ranked reviewers will get the proposal of reviewing the review of #PR. First two (2) users that accept the proposal will be selected as #SR. #SR will then review the reviewing or rating submitted by #PR.

This way there will be a two-tier or two-step peer-reviewing and if the submitted article should be published or not, gets verified through this two-step verification process.

Primary Review: Review of the Submitted Article

After #PR is selected through TAG matching and Reviewer selection process described earlier, #Author can see the list of three (3) finally selected #PRs who accepted the request of reviewing the article.

IPFS then takes the address of the article can create a hash. The system then encrypts the address hash with the public key of a #PR. Then #Author share the encrypted hash with the #PR. #PR decrypts the article with his private key (see figure: 13). After decrypting he uses the decrypted address hash to download the article from IPFS. This process is repeated for all three (3) selected #PRs.

#Author will initiate a transaction with the #PR to send the hash of the article.

This transaction happens each time #Author sends a hash of his article to a #PR. After #PR gets the hash, he then decrypts the hash using his private key. After the decryption, he gets the hash that is generated from the address or location of the article in #Author's directory by IPFS that #Author wants him to review. He then uses it to download the file through IPFS.

Figure 13. #Author sending Article to #PR using IPFS

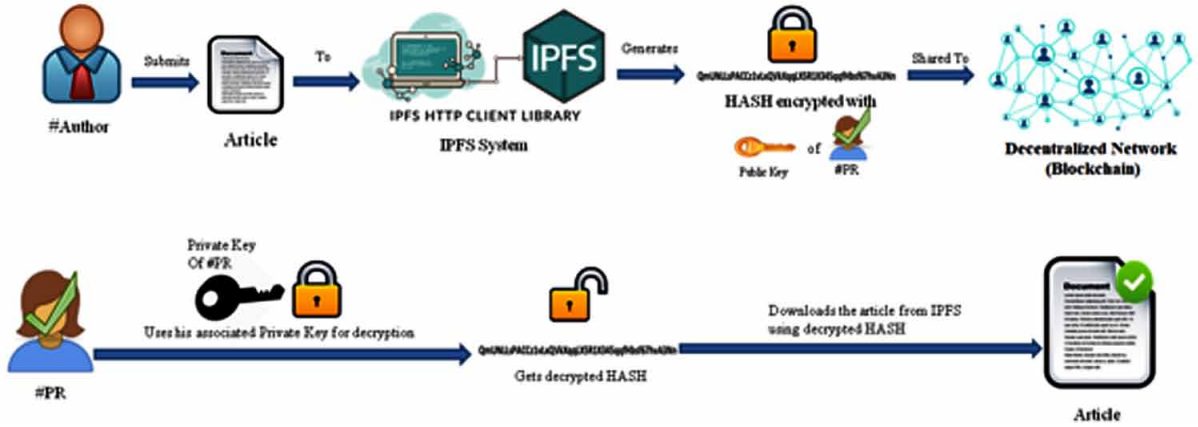
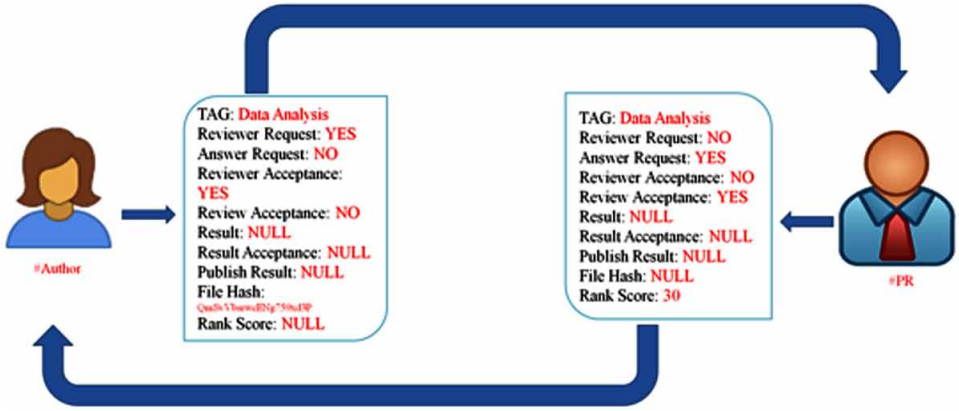


Figure 14. #Author sending hash of the article created by IPFS to #PR within a transaction



After reviewing the article #PR creates a file that includes the rating decision (A/MAR/MIR/R) and comments regarding the submitted article. This review file is then sent to #SR with the main submitted article.

Secondary Review: Review of the Primary Review

The job of a secondary reviewer is to make sure that the primary reviewer completes his job correctly. Secondary reviewer or #SR is selected from the users excluding the #Author and three #PR. #SR selection process is the same as the selection process of #PR. At first, TAG is matched. Then eligible reviewers are ranked based on their rank score. After that they are asked to be #SR based on their rank on a descending manner. The user with best rank score is asked first, then second best, then third best and so on. This process is same as the #PR selection process described above.

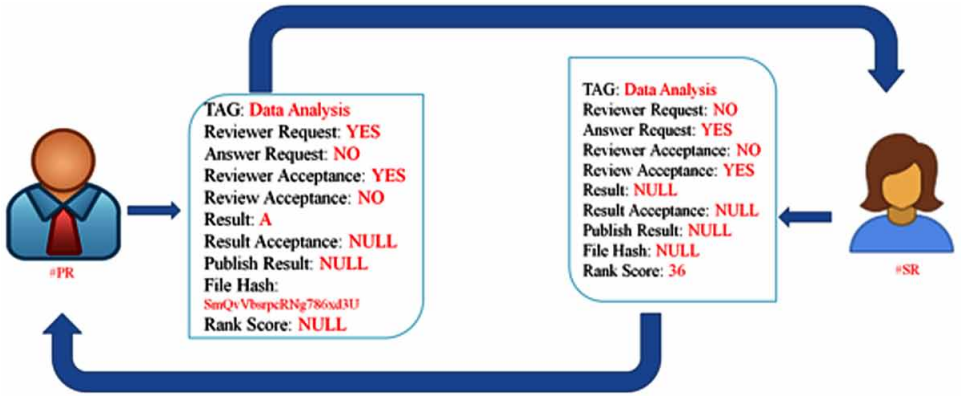
First two (2) eligible reviewers who agree to the review request become secondary reviewer or #SR.

After #PR downloads, decrypts and reviews the article submitted by the #Author; he writes down his review, comments and the rating (A/MAR/MIR/R) he has given to the submitted article and creates

a doc file or pdf file. Then he keeps both his review file and the submitted article in a folder. Then #PR uploads the folder to IPFS. IPFS then generates a hash of the address of this folder. Then the system encrypts the hash with the public key of a #SR. Then the encrypted address hash of the folder is shared with the #SR. This process is repeated for both #SR. #SR then decrypts the encrypted address hash, and then he uses the decrypted hash to download the folder from IPFS. After downloading is completed he collects both file; the submitted article and the review file. For better understanding please see figure 15.

After collecting both files #SR will review the primary review and the article. Then he will produce

Figure 15. #PR sending hash of the combined article and review file created by IPFS to #PR within a transaction



a binary decision, the primary review is TRUE, or the primary review is FALSE. The decision being TRUE means, the review of the primary reviewer is accepted, if FALSE it means the review of the primary reviewer is rejected. As there will be two #SR, a primary review will be considered true only if both #SR gives the decision "TRUE". And a primary review will be considered false only if both #SR gives the decision "FALSE".

There can be three possible situations-

1. If the primary review was "A" meaning "Accepted" and the secondary reviewer gives the binary decision TRUE, then the submitted article will be published.
2. If the primary review was "MAR" or "MIR" or "R" and the secondary reviewer gives the binary decision TRUE, then the author will be notified and the submitted article won't get published at that time.
3. If the secondary review is "FALSE" then the primary review will become void. The primary reviewer will be notified, and his reputation point will decrease as a penalty for being biased, unethical and unprofessional. The whole process will re-initiate automatically until the review process is completed rightfully.

For better understanding of how the decision will be sent as transaction, take a look at figure 16.

Once, #PR gives "A" rating to the submitted article and #SR gives the decision "TRUE"; the submitted article will get published and added to the proposed system.

Figure 16. #SR sending final decision to #Author

This two-step verification process ensures that the submitted article is being reviewed correctly without any kind of biasness. It does so because of following reasons-

1. All of three (3) primary reviewers don't know the #Author. It will be a blind review process.
2. None of the primary reviewers will be sluggish and give wrong or biased review of the submitted article because their review will be reviewed by the #SR. And if any primary reviewer gives wrong review, his reputation point will be decreased as penalty.
3. There will be two (2) #SR and the final decision will be taken only if both of the #SR gives the same decision. So, there is no chance that the final decision will be biased or wrong.

REPUTATION POINT - BASED ON THE IDEA OF CRYPTO CURRENCY

Reputation Point or RP can be denoted as a form of reward gained each time a reviewer successfully completes a review process. RP cannot be used as any form of currency, it cannot be transferred; however, one can earn RP through completing an authentic and correct review of a submitted paper. If the review is rejected because of its questionable character, then the primary reviewer that made the review will lose RP because of his/her questionable reviewing on the submitted paper. Thus, Reputation Point acknowledges a researcher's expertise as a reviewer.

Primary reviewers will earn RP by giving authenticate review of Author's submitted paper. Secondary reviewers will earn RP by reviewing the reviews previously given by the primary reviewers.

So, a high-ranking reviewer (primary and secondary) will have a high number of published works as well as a high number of Reputation Points indicating the reviewer's expertise as a reviewer.

Reputation Point: Crypto Reward

Reputation Point or RP plays a vital role in the proposed system. It is a variation of crypto currency which holds only abstract value. It has no monetary value.

Primary reviewer (#PR) and Secondary reviewer (#SR) both get selected on the basis of the number of publication and Reputation Point or RP.

This Reputation Point will act as a token of gratitude. The information of total amount of Reputation Point a user has will always be public. The more Reputation Points reflects a better reviewer. This can also be viewed as a certificate given by publishers to the reviewer. Unbiased, authentic and rightful or fair review will earn a reviewer some Reputation Points. Failing to do so will result in penalty and Reputation Point will be deducted from the reviewer.

Whenever, a #PR completes an authentic and rightful article review process, he will be rewarded with, for example 10 Reputation Points. This Reputation Points will be awarded to the #PR for giving an authentic review by the system itself.

#SR will be reviewing the primary review produced by the #PR. For completing the secondary review process, #SR will be awarded with, for example 5 Reputation Points.

For better understanding of matter, please see figure 17.

If a #PR gives a review that is biased, wrong or unethical; then, for example 6 Reputation Point will be reduced as a penalty from his current amount of Reputation Points. #SR will not lose any Reputation Points because he will only be reviewing the primary review that #PR produced. And also, as the final decision will be taken only when both of two #SR agrees on the decision, the secondary review, has a very less chance of being biased. This is why #SR won't be penalized here.

#SR will have a very little amount of Reputation Point gain from the review process, but there is no penalty for him. #PR will have a much higher gain of Reputation Point than the #SR but will be penalized if found guilty of giving wrong review.

For better understanding of matter, please see figure 18.

As it can be observed that there is a strong relation between review and Reputation Point. Higher amount of Reputation Points indicate that the user is a good reviewer who is unbiased and does rightful reviews of scientific articles. Lower amount of Reputation Points indicate that the user is not up to par as a reviewer. That means, the more Reputation Points a user has, the more eligible and better reviewer he is. It should be mentioned here that; higher and lower amount is relative. Having 15 Reputation Points

Figure 17. Gaining reputation points in case of primary and secondary reviewer

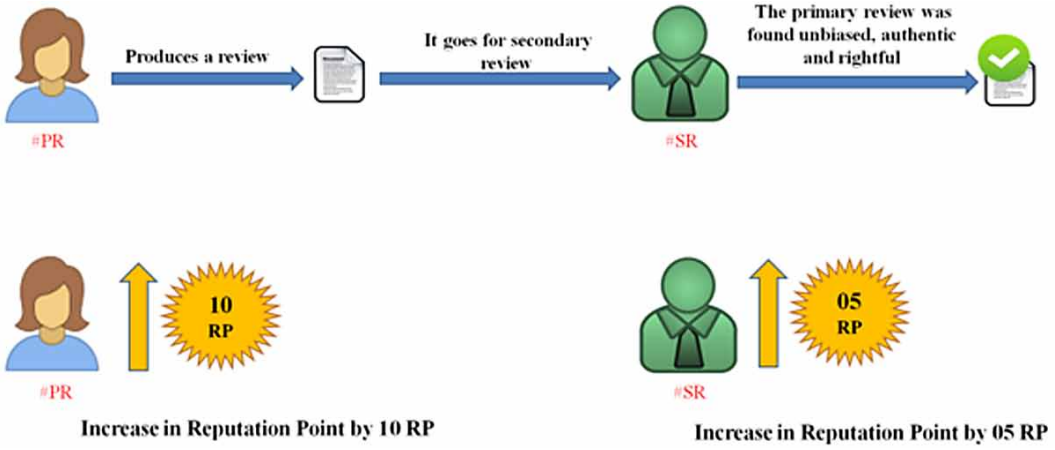
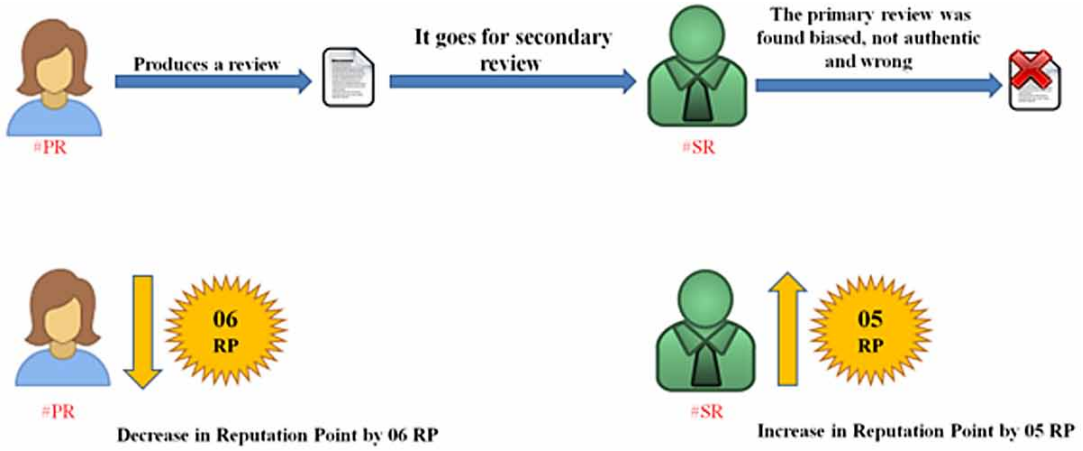


Figure 18. Loosing reputation points in case of primary reviewer



can be considered as high amount, if other users of the system have lower than 15 Reputation Points. On other hand, having 100 Reputation Points can be considered as a lower amount if others have more than 100 Reputation Points.

Validating Transactions: Another Use of Reputation Points as Crypto Reward

There is a fourth role a user of the system can act on. This role is not a part of the whole review process but a part of the Blockchain who will act indirectly to maintain the reliability of the system.

In existing Blockchain based systems, there is a type of users called miner. Miners deal with validating transactions and building new adding new block to the Blockchain (Ellervee, Matuleviˇcius & Mayer, 2017). Fundamentally, a Blockchain operator is a miner, because miner's tasks in a Blockchain environment are to create new blocks, sign them, validate them and submit them to the Blockchain (Ellervee et al., 2017). Usually mining a block gets a miner some crypto currency that he can spend. But as all of our users will be from scientific and researcher community, there is a significant amount of probability that the miner validating the blocks of the proposed peer-reviewing system based on Blockchain will also come from the same community. As in the proposed system infrastructure, a miner is helping the review process by validating the transactions, he will be rewarded with a minimal amount of Reputation Point for his contribution.

Reputation Point, in all means will not act as a traditional crypto currency; but a crypto reward based on the idea of crypto currency. As Reputation Point holds no monetary value and cannot be transferred from one account to another, there is a less chance of bribery and corruption. But as it holds an abstract value, it will help identifying a user as a better reviewer and a better contributor to the field of research.

Challenges of Integrating Blockchain and Smart Contracts in Scientific Paper Peer Reviewing System

There are several challenges of implementing the proposed system along with the limitations of Blockchain technology discussed in earlier section. The challenges are discussed below.

- **Human Interaction:** As it is sure that there is no sufficient technology which can review or evaluate a scientific paper, therefore, this proposed system must have some interaction with human. This brings a possibility that can potentially corrupt the system. But, as the system integrates smart contracts that control the behavior of the stakeholders of the system, the possibility is less and also any aberrant behavior can be traced back through the data stored on the blockchain. However, this system still struggles to maintain human interaction with the system.
- **File Storage:** Authors will submit their paper through IPFS, and other reviewers are supposed to download and seed the file. But it is imminent that no one wants to waste their storage for seeding other files. This makes a challenge for the proposed system that how the file will be stored. Initially, the author must seed his own file. But to circulate the file efficiently through system it is necessary that some other users also seed the same file. This problem can be eliminated through offering rewards or crypto-currency to store files. Already, Filecoin is in its development phase which provides the user with some crypto-currency to host other people's files.
- **Proper Reviewing Rules or Criteria:** As there are no ground rules for reviewing a paper, it sometimes may get confusing whether a paper is reviewed correctly or not. Though the secondary review process is integrated into the system, it is not sure that the quality is impeccable. However, if this system is maintained by an organization that sets some ground rules then this problem may not exist.
- **Implementing the Flow of Cryptocurrency:** Another important fact that should not go unnoticed that the flow of reputation point, and cryptocurrency play a big role to the system. Though, it is also a debatable topic that whether a reviewer should get crypto-currency in exchange of his or her review. This problem can also be eliminated if a single organization adopt the system and set ground rules for biasfree reviewing of scientific papers.
- **Immutability of Smart Contracts:** Smart contracts are immutable by definition. This system cannot assure that the rules will remain same forever. So, it is challenging to maintain or upgrade smart contracts. Though, there are ways to upgrade a smart contract by using an intermediate contract where the active smart contract's address will be saved. There are some security risks to upgrade smart contracts that cannot be overlooked. So, this is also a challenge to maintain smart contracts of the proposed system.

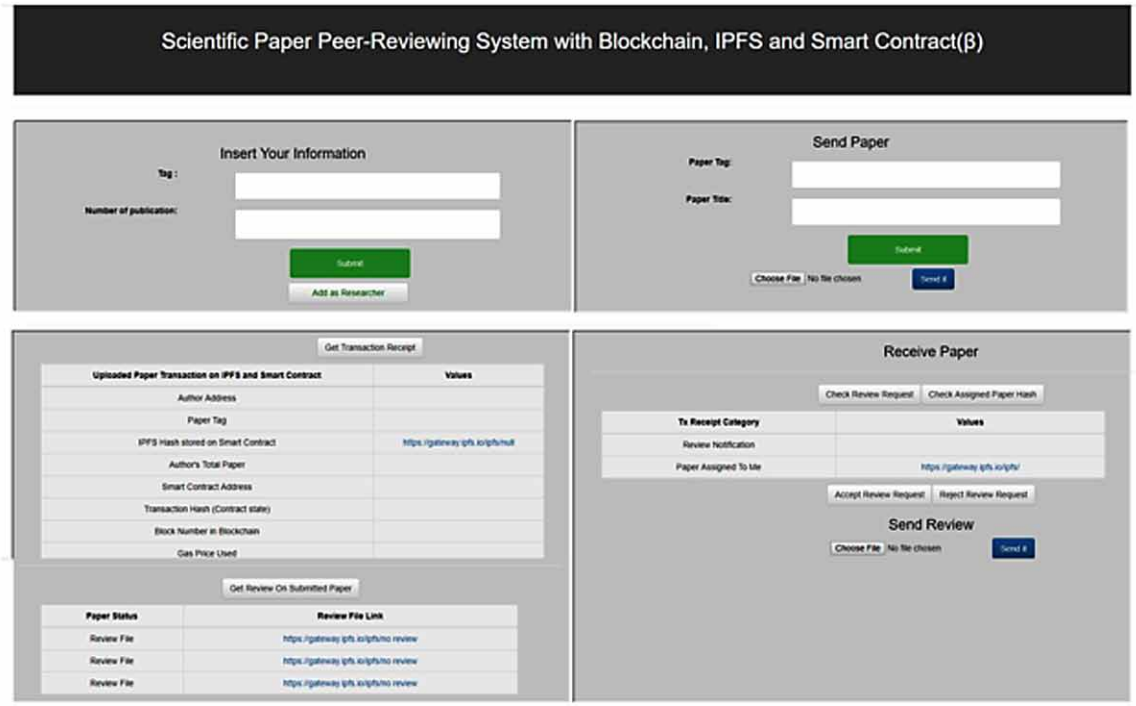
IMPLEMENTATION

A prototype has been prepared to validate the above given proposed system. Distributions of article using IPFS, finding eligible reviewers, giving review – these parts have been successfully implemented. The system was implemented using Ethereum's test network. Backend was developed using Solidity and frontend was developed with ReactJS. Currently "Two-step verification" and "Reputation Point" are being worked on and will be added to the system as soon as possible.

SIMILAR WORK

Recently, Digital Science and Katalysis have launched a pilot project to implement blockchain technology to test the peer review process. This project aims to discover the practical solutions to enhance distributed

Figure 19. Implemented parts of the proposed system



registry and smart contracts which are the elements of Blockchain technology. The initiative is divided into three (3) parts namely Pilot Phase, Minimal Viable Product Phase and Advanced Development. Participation is almost closed for the first phase as of Feb 01, 2019. (Blockchain Peer Review Project)

CONCLUSION

Recently, the decentralized applications (DApp) based on Blockchain technology are gaining attention to the developer and researcher communities. In this paper an anonymous scientific paper reviewing system based on Blockchain and IPFS technology has been proposed. However, the scalability of this system is needed to be observed. Researches can improve the scalability of this system.

Reputation Point of this system does not hold any monetary value. The integration of monetary system in peer reviewing system is a debatable topic. So, researches in this area could unearth whether peer reviewing should be done by exchanging cryptocurrency or not. Again, access to the published paper could also be monetized. This system presently does not integrate any monetary system. So, feasibility of integrating money exchange in this system needs more study.

Design of the smart contracts can be of different forms, so more precise contracts formation may emerge. So, the evaluation of different contracts can be analyzed and ensure efficiency of this system.

In this proposed system, the users of the network store the files, but they are not provided anything in return. So, to ensure that the published papers are held by maximum number of users, cryptocurrency can be provided to the holders of scientific papers in the network.

REFERENCES

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). *Blockchain technology innovations. In 2017 IEEE Technology & Engineering Management Conference*. TEMSCON. doi:10.1109/temscon.2017.7998367

Allison, I. (2016, October 13). *Juan Benet of IPFS talks about Filecoin*. Retrieved October 27, 2018, from https://www.ibtimes.co.uk/juan-benet-ipfs-talks-about-filecoin-1586122

Arora, J. (n.d.). *How EOS can solve the Blockchain scaling problems*. Retrieved August 5, 2018, from https://itsblockchain.com/eos-scaling/

Blockchain Council. (2018, July 10). *How is blockchain verifiable by public and yet anonymous?* Retrieved January 29, 2019 from https://www.blockchain-council.org/blockchain/how-is-blockchain-verifiable-by-public-and-yet-anonymous/

Blockchain on AWS. (n.d.). Retrieved October 26, 2018 from https://aws.amazon.com/blockchain/

Blockchain Peer Review Project. (n.d.). Retrieved February 01, 2019 from https://www.blockchainpeer-review.org

Chaum, D. (1997). David Chaum on Electronic Commerce How much do you trust Big Brother? *IEEE Internet Computing*, *1*(6), 8–16. doi:10.1109/MIC.1997.643931

Chen, W., Ma, M., Ye, Y., Zheng, Z., & Zhou, Y. (2018). IoT Service Based on JointCloudBlockchain: The Case Study of Smart Traveling. *2018 IEEE Symposium on Service-Oriented System Engineering (SOSE)*. 10.1109/SOSE.2018.00036

Crypto Celebrities. (n.d.). Retrieved October 29, 2018, from https://cryptocelebrities.co/

CryptoKitties. (n.d.). Retrieved October 29, 2018, from https://www.cryptokitties.co/

Csiszar, A. (2016). Peer review: Troubled from the start. *Nature*, *532*(7599), 306–308. doi:10.1038/532306a PMID:27111616

Dey, T., Jaiswal, S., Sunderkrishnan, S., & Katre, N. (2017). HealthSense: A medical use case of Internet of Things and blockchain. *2017 International Conference on Intelligent Sustainable Systems (ICISS)*. 10.1109/ISS1.2017.8389459

Ehsani, F. (2016, December 21). *Blockchain in Finance: From Buzzword to Watchword in 2016*. Retrieved October 26, 2018 from https://www.coindesk.com/blockchain-finance-buzzword-watchword-2016/

Ekin, A., & Unay, D. (2018). Blockchain applications in healthcare. *2018 26th Signal Processing and Communications Applications Conference (SIU)*. doi:10.1109iu.2018.8404275

Ellervee, A., Matuleviˇcius, R., & Mayer, N. (n.d.). *A Comprehensive Reference Model for Blockchain-based Distributed Ledger Technology.* Retrieved October 27, 2018, from http://ceur-ws.org/Vol-1979/paper-09.pdf

Etherbots. (n.d.). Retrieved October 29, 2018, from https://etherbots.io/

Feld, S., Schönfeld, M., & Werner, M. (2014). Analyzing the Deployment of Bitcoins P2P Network under an AS-level Perspective. *Procedia Computer Science*, *32*, 1121–1126. doi:10.1016/j.procs.2014.05.542

Filesystem in Userspace. (2018, October 22). Retrieved October 27, 2018, from https://en.wikipedia.org/wiki/Filesystem_in_Userspace

Finley, K. (2016, June 20). *The Inventors of the Internet Are Trying to Build a Truly Permanent Web*. Retrieved October 26, 2018 from https://www.wired.com/2016/06/inventors-internet-trying-build-truly-permanent-web/

Hay, S. (2018, January 02). *What is the Bitcoin Lightning Network? A Beginner's Explanation*. Retrieved October 26, 2018 from https://99bitcoins.com/what-is-the-bitcoin-lightning-network-a-beginners-explanation/

Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjalmtysson, G. (2018). Blockchain-Based E-Voting System. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. doi:10.1109/cloud.2018.00151

Hojat, M., Gonnella, J. S., & Caelleigh, A. S. (2003). Impartial Judgment by the "Gatekeepers" of Science: Fallibility and Accountability in the Peer Review Process. *Advances in Health Sciences Education: Theory and Practice*, *8*(1), 75–96. doi:10.1023/A:1022670432373 PMID:12652170

Hyperledger: Blockchain collaboration changing the business world. (n.d.). Retrieved October 26, 2018 from https://www.ibm.com/blockchain/hyperledger

Infographic. (2018, October 4). *A history of academic peer review*. Retrieved October 26, 2018 from https://www.editage.com/insights/a-history-of-academic-peer-review

IPFS is the Distributed Web. (n.d.). Retrieved October 27, 2018, from https://ipfs.io/#how

Ipfs/README.md. (n.d.). Retrieved October 27, 2018, from https://github.com/ipfs/ipfs/blob/master/README.md#who-designed-it

Jordan, R. (2018, January 10). *How to Scale Ethereum: Sharding Explained – Prysmatic Labs – Medium*. Retrieved October 26, 2018 from https://medium.com/prysmatic-labs/how-to-scale-ethereum-sharding-explained-ba2e283b7fce

Kalodner, H., Carlsten, M., Ellenbogen, P., Bonneau, J., & Narayanan, A. (2015). *An empirical study of Namecoin and lessons for decentralized namespace design*. Retrieved October 26, 2018, from http://randomwalker.info/publications/namespaces.pdf

Kiyomoto, S., Rahman, M. S., & Basu, A. (2017). On blockchain-based anonymized dataset distribution platform. *2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA)*. doi:10.1109era.2017.7965711

Koshy, P., Koshy, D., & McDaniel, P. (2014) An Analysis of Anonymity in Bitcoin Using P2P Network Traffic. In Lecture Notes in Computer Science: Vol. 8437. Financial Cryptography and Data Security. Springer. doi:10.1007/978-3-662-45472-5_30

Kronick, D. A. (1990). Peer Review in 18th-Century Scientific Journalism. *Journal of the American Medical Association*, *263*(10), 1321. doi:10.1001/jama.1990.03440100021002 PMID:2406469

Kshetri, N., & Voas, J. (2018). Blockchain-Enabled E-Voting. *IEEE Software*, *35*(4), 95–99. doi:10.1109/MS.2018.2801546

Lerback, J., & Hanson, B. (2017). Journals invite too few women to referee. *Nature*, *541*(7638), 455–457. doi:10.1038/541455a PMID:28128272

Litecoin. (n.d.). Retrieved October 26, 2018, from https://en.wikipedia.org/wiki/Litecoin

Loeliger, J., & McCullough, M. (2012). *Version control with Git*. Sebastopol, CA: OReilly.

Mahoney, M. J. (1977). Publication prejudices: An experimental study of confirmatory bias in the peer review system. *Cognitive Therapy and Research*, *1*(2), 161–175. doi:10.1007/BF01173636

Meiklejohn, S., & Orlandi, C. (2015). Privacy-Enhancing Overlays in Bitcoin. In M. Brenner, N. Christin, B. Johnson, & K. Rohloff (Eds.), Lecture Notes in Computer Science: Vol. 8976. *Financial Cryptography and Data Security. FC 2015*. Berlin: Springer. doi:10.1007/978-3-662-48051-9_10

Merton, R. K. (1968). The Matthew Effect in Science: The reward and communication systems of science are considered. *Science*, *159*(3810), 56–63. doi:10.1126cience.159.3810.56

Mitra, R. (2017, December 4). *Lightning Protocol &The Raiden Network: A Beginner's Guide*. Retrieved October 26, 2018 from https://blog.springrole.com/lightning-protocol-the-raiden-network-a-beginners-guide-c9d7bc702748

Mulligan, A., Hall, L., & Raphael, E. (2012). Peer review in a changing world: An international study measuring the attitudes of researchers. *Journal of the American Society for Information Science and Technology*, *64*(1), 132–161. doi:10.1002/asi.22798

Nakamoto, S. (n.d.). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved October 26, 2018 from https://bitcoin.org/bitcoin.pdf

Niya, S. R., Shupfer, F., Bocek, T., & Stiller, B. (2018). Setting up flexible and light weight trading with enhanced user privacy using smart contracts. *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*. doi:10.1109/noms.2018.8406112

Peer Reviewed Medical Journals. (n.d.). Retrieved October 26, 2018 from https://www.omicsonline.org/peer-reviewed-medical-journals.php

Ratnasamy, S., Francis, P., Handley, M., Karp, R., & Schenker, S. (2001). A scalable content-addressable network. *Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications - SIGCOMM 01*. doi:10.1145/383059.383072

Rowland, F. (2002). The peer-review process. *Learned Publishing*, *15*(4), 247–258. doi:10.1087/095315102760319206

Schwartz, D., Youngs, N., & Britto, A. (2014). *The Ripple Protocol Consensus Algorithm*. Retrieved October 26, 2018, from https://ripple.com/files/ripple_consensus_whitepaper.pdf

Sharp, D. W. (1990). What Can and Should Be Done to Reduce Publication Bias? *Journal of the American Medical Association*, *263*(10), 1390. doi:10.1001/jama.1990.03440100102015 PMID:2304218

Shema, H. (2014, April 19). *The Birth of Modern Peer Review*. Retrieved October 26, 2018 from https://blogs.scientificamerican.com/information-culture/the-birth-of-modern-peer-review/

Spier, R. (2002). The history of the peer-review process. *Trends in Biotechnology*, *20*(8), 357–358. doi:10.1016/S0167-7799(02)01985-6 PMID:12127284

Stoye, E. (2017, June 19). *Studies flag signs of gender bias in peer review*. Retrieved October 26, 2018 from https://www.chemistryworld.com/news/studies-flag-signs-of-gender-bias-in-peer-review/3007593.article

Szabo, N. (1996). *Smart Contracts: Building Blocks for Digital Markets*. Retrieved October 26, 2018, from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution how the technology behind Bitcoin is changing money, business and the world*. Portfolio/Penguin.

Tenorio-Fornés, A., Hassan, S., & Pavón, J. (2018). Open Peer-to-Peer Systems over Blockchain and IPFS. *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems - CryBlock18*. 10.1145/3211933.3211937

The Linux Foundation. (2015, December 17). *Linux Foundation Unites Industry Leaders to Advance BlockchainTechnology* [Press release]. Retrieved October 26, 2018 from https://www.linuxfoundation.org/press-release/2015/12/linux-foundation-unites-industry-leaders-to-advance-blockchain-technology/

Thomas, L., Long, C., Burnap, P., Wu, J., & Jenkins, N. (2017). Automation of the supplier role in the GB power system using blockchain-based smart contracts. *CIRED - Open Access Proceedings Journal, 2017*(1), 2619-2623. doi:10.1049/oap-cired.2017.0987

Valenta, L., & Rowan, B. (2015). Blindcoin: Blinded, Accountable Mixes for Bitcoin. In M. Brenner, N. Christin, B. Johnson, & K. Rohloff (Eds.), Lecture Notes in Computer Science: Vol. 8976. *Financial Cryptography and Data Security. FC 2015*. Berlin: Springer. doi:10.1007/978-3-662-48051-9_9

Wood, G. (2014*). ETHEREUM: A Secure Decentralized Generalized Transaction Ledger EIP-150 REVISION.* Retrieved October 26, 2018, from https://gavwood.com/paper.pdf

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology? A Systematic Review. *PLoS One*, *11*(10), e0163477. doi:10.1371/journal.pone.0163477 PMID:27695049

Young, J. (2016, September 24). *IPFS Protocol Selects Ethereum Over Bitcoin, Prefers Ethereum Dev Community*. Retrieved October 27, 2018, from https://cointelegraph.com/news/ipfs-protocol-selects-ethereum-over-bitcoin-prefers-ethereum-dev-community

Zhang, P., Walker, M. A., White, J., Schmidt, D. C., & Lenz, G. (2017). Metrics for assessing blockchain-based healthcare decentralized apps. *2017 IEEE 19th International Conference on E-Health Networking, Applications and Services (Healthcom)*. doi:10.1109/healthcom.2017.8210842

Zhao, J. L., Fan, S., & Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*, *2*(1), 28. doi:10.118640854-016-0049-2