doi:10.20944/preprints202007.0665.v1

Theory of the Academic Blockchain

M. Keith Wright, Ph. D
University of Houston Downtown
wrightm@uhd.edu
https://orcid.org/0000-0002-7463-6920

This article integrates existing theory from distributed computing and cryptology with anecdotal material from the cryptocurrency industry, to provide a comprehensive description of the minimum requirements of the hypothetical academic blockchain. The paper argues that such a community could significantly reduce the biases and misconduct that now exist in the academic peer review process. Theory suggests such a system could operate effectively as a distributed encrypted telecommunications network where nodes are anonymous, do not trust each other, and there is minimal central authority. To incentivize the academic community to join such a proposed community, the paper proposes a pseudo-cryptocurrency called litcoin (literature coin). This litcoin-based system would create economic scarcity based on proof of knowledge (POK), which is a synthesis of the proof of work (POW) mechanism used in bitcoin, and the proof of stake (POS) mechanism used in various altcoin communities. The paper argues that the proposed POK system would enable the academic community to more effectively develop the research it finds valuable.

Key words: cryptography, timestamping, cryptocurrency, proof-of-knowledge, proof-of-work, proof-of-stake, proof-of-authority, litcoin, bitcoin

doi:10.20944/preprints202007.0665.v1

Biases in academic peer review. Most laymen assume the process of academic peer review is robust, anonymous, and impartial. However, as many researchers would probably agree, it is often none of these. The Internet revolution has been a double-edged sword for academic publishing. While the average cost of journal publication has plummeted, the number of journals of dubious quality has spiraled. While the probability of plagiarism is now much higher, articles with minor text reuse can be easily mistaken as plagiarized. While virtually any published work is now freely available to subscribers, filtering such work for quality and originality is now more complex.

Most of us probably agree that academic authors and reviewers make honest mistakes. However, as this article will evidence, not all the behavior of academic community members is honest. For instance, Fang, et.al. (2012) examined 2,047 retractions in biomedical and life sciences journals and found 88 % were attributed to either error or misconduct. This raises the issue of review validity.

A quite common review experience is three radically different reviews for the same paper: one recommending acceptance, one requesting major changes, and one recommending rejection. Hanley (2013) and Starbuck (2003) indicated that reviewer dissensus often causes top journals to reject high quality papers, while accepting low quality ones (Lodahl & Gordon 1972; Pfeffer 1993).

Article review mistakes can have serious negative consequences. For examples, Andrew Wakefield's flawed study of the measles, mumps, and rubella vaccine (Deer, 2014) and Hwang Woo-suk's fraudulent study of cloning (Sang-Hun, 2009) have had major negative repercussion. (Yong, 2012). Sage Publications recently retracted sixty papers from one of its journals. In one such case, a reviewer used a phony name to give a glowing review to his own work. Furthermore, according to a 2011 report in the *Journal of Nature Reviews Drug Discovery*, the results of two-thirds of sixty-seven key studies analyzed by Bayer researchers from 2008-2010 could not be reproduced.

The prestigious Proceedings of the National Academy of Science once published a paper entitled "Female Hurricanes are Deadlier than Male Hurricanes" (Jung et. al. 2014). because of the following excerpt from organization's own submission guidelines:

> "The review process is conducted anonymously for all submissions, except NAS members' own contributions, where the reviewers are known to the author and their names are published…."
> https://www.pnas.org/page/authors/reviewers

In other words, if you are a NAS member, you may be able review your own paper or those of people you know. In 2002 and 2010, two papers published in those proceedings claimed that a pesticide called atrazine was causing sex changes in frogs. Both papers had the same prestigious editor, who was a colleague of the paper's lead author. The author preselected his editor, and both papers were published without a review of the data on which the paper was based. The Environmental Protection Agency (EPA) could not reproduce the results of either paper (Campbell, 2013).

Heuristic criteria related to authors' social relations, writing style, doctoral origins, and current affiliations can play major roles in review bias, because such heuristics can be used to avoid the difficult burden of deeply evaluating an article (Yong, 2012). To demonstrate this, Ceci & Peters (1982) identified several papers published by faculty from prestigious departments. Next, they copied and resubmitted the papers to the same journals, but with phony author names and affiliations. Of the nine papers not deemed plagiarized, eight were rejected by sixteen of eighteen reviewers. There is also evidence of a "complex language bias" in journal article reviewing. In the best-known study of this issue, faculty from three prestigious universities evaluated passages from previously published research [1]. The investigators rewrote the articles in two different versions, one with straightforward language, the other with more complex language. Reviewers rated the complex language versions more highly. Mahoney [20] presents evidence that reviewers tend to favor research that does not deviate very much from prevailing wisdom.

> Michael Eisen, a biologist at UC Berkeley, and a founder of the *Public Library of Science*, was quoted in the following *Wall Street Journal* article (Campbell, 2013).

> "We need to get away from the notion, proven wrong on a daily basis, that peer review of any kind at any journal means that a work of science is correct. What it means is that a few (1-4) people read it … and didn't see any major problems. That's a very low bar in even the best of circumstances"

That same WSJ article (Campbell, 2013) also quotes Professor Larry Wasserman, of Carnegie Mellon University,

> *"The peer review system that we currently use … is a centralized, secretive system that allocates scarce resources (reviewers' time) by fiat. We need to scrap the whole system and build a new one that recognizes that science is first and foremost a marketplace of ideas. We should replace pre-publication peer review with post publication open review. All papers (except for obviously terrible papers screened out by the editor) should be posted online. Authors should be required to also post their data, …details of experimental procedures, and … how the data were analyzed. Consumers, i.e., scientists and interested parties, could download the data, do their own analyses, ask questions and challenge assumptions … Important papers would naturally attract more scrutiny, thus leading to a more efficient allocation of resources."*

In summary, major deficiencies in the traditional academic peer review process in the Internet age are now well documented. However, the recent advances in cryptography and distributed computing have made it possible to address the aforementioned challenges. These advances are sometimes known as *blockchains*.

Blockchain technology and bitcoin. The word "blockchain" means different things to different people. Computer scientists see it as either an efficient distributed computing protocol, a shared data structure, or a peer-to-peer network protocol. Business people see it as an immutable electronic ledger of financial transactions. However, to a layman, it means nothing if not the mysterious engine that underlies the bitcoin community.

Anyone can join the bitcoin community by paying a cash fee. These fees become their initial bitcoin balance stored in their local PC's "wallet". Members can then conduct virtually untraceable business transactions with other community members using only bitcoins. At any time, community members can buy more bitcoin, or exchange theirs for cash at the open market exchange rate. All these transactions are stored in an immutable blockchain, which establishes the global order of transactions. Because there is no central authority such as a bank, bitcoin is a true cash-equivalent cryptocurrency. A few lucky people have made millions from bitcoin speculation.

The *litcoin* blockchain. The concept of a blockchain community can be generalized to include any type of anonymous community, such as our proposed *litcoin* network. (Note that *litcoin* is not to be confused with litecoin *(https://litecoin.org)*, a cryptocurrency that competes with bitcoin.) The author proposes that anyone could subscribe to the *litcoin* community freely as a reader or reviewer. Because reviewing would earn litcoin, a sufficient litcoin balance would lead to the permission to become an author. It would not be possible to "buy" litcoin with cash or trade it for any other tangible asset. Its value would be derived indirectly through influence in the academic community. Thus, litcoin should be properly considered only a pseudo-cryptocurrency. All litcoin transactions, such as subscription, submission, and review, would be appended to the immutable litcoin blockchain. The dataflow in the proposed network is shown in figure 1.

Identity management in the *litcoin network*. To ensure members' anonymity, and to avoid a central authority to manage their identities, the authors propose that the litcoin protocol use an encryption key to locate and identify a members' network node. This is what the bitcoin

doi:10.20944/preprints202007.0665.v1

protocol does. These "addresses" would be the public portion of a public-private key pair as proposed by Merkle (1980). Chaum et.al (1988) is credited with the idea of using such keys as network node identities. The author also proposes that any litcoin content submitter could create aliases any time simply by generating new pair of public-private keys. However, doing so would dilute their influence in the network. Further, litcoin nodes would not need to inform other nodes when it creates aliases. However, any single transaction would require one and only one of a node's respective addresses.

For example, in a litcoin community when Alice wishes to submit content such as an article or review, her network node would use one of her public addresses to digitally sign a transaction containing that content. Her node would then broadcast that transaction to all litcoin nodes. Bob, a validator node (See Figure 2.), would later commit the valid transaction to a block in the chain. Although the address of blockchain transactions would be encrypted, most payloads (e.g. the articles), would be plain text. Thus, any subscriber node would have read access to all articles in the blockchain. In summary, all litcoin transactions could be done effectively with neither Alice's nor Bob's true identity. Only if a local node is compromised, could the true identity of the community member be revealed and/or their litcoin stolen. All litcoin members would be responsible for securing their PC's.

Articles and reviews would comprise most of the transactions on the academic blockchain. However, the litcoin consensus protocol could generate occasional endogenous transactions to periodically adjust blockchain parameters. Given that such a litcoin protocol could be developed, the academic community could operate without a central authority, such as a chief editor. The possibility of developing such a protocol is demonstrated by the popularity of bitcoin.

Behavior on the academic blockchain would be rewarded or punished in litcoins, which would accrue to reviewers, authors, validators, and to the content itself. Although the data flow in a litcoin blockchain community can be described as the simple process shown in figure 1, the computer science would be complex (Narayann, et. al. 2016).

The origins of blockchain science were papers by Haber and Stornetta (1990, 1997) who envisioned a “digital notary” service. The central themes in that literature are computationally efficient mechanisms to establish an absolute immutable global order of transactions. This would be the chief advantage of the academic block chain compared to traditional methods of academic review.

Time stamping, digital signatures, and hash pointers. Time stamps are crucial elements of any cryptocurrency, and especially for the litcoin community, where authors wish to assert that their ideas were created at a certain point in time, no later; and readers want assurance that ideas were created at a certain point in time, no earlier. Time stamping was central in the original Haber and Stornetta papers. There, documents were constantly being created, broadcast, and modified. The creator of each document asserted a time of creation and then digitally signed the document, its timestamp, and the immediately previous broadcast document. Because the previous document creator had digitally signed his own predecessor, the signatures formed a long chain with pointers backwards in time.

A digital signature has the following three properties:

1. it can’t feasibly be forged, even if the adversary has seen many examples of the signer’s signature;
2. any node on the network can efficiently verify that the signature is valid; and

3. the signature is unique to a specific document. Thus, it cannot be cut from one document and pasted onto another.

More formally, a digital signature can be produced by the following three types of algorithms (Narayanan & Clark, 2017).

1. (sk, pk) = *generateKeys*(keysize), where sk and pk are the secret and public keys, respectively.
2. Signature = *sign* (sk, document. The secret key is used to sign a document,
3. isValid = *verify* (pk, document, signature). Valid signatures must evaluate to true, and anyone with the public key can efficiently verify the signature's authenticity.

Due to potentially very long bit strings in a litcoin transaction, a *hash pointer* to the document would be signed rather than the document itself. A hash pointer points to an address where a document and its hash are stored. This gives software modules both an efficient way to find content, and to verify its integrity.

An effective cryptographic hash function has the following properties (Narayanan et. al. 2016):

- its input can be any bit string
- it produces a specified size output string
- it is efficiently computable (If n is number of bits in the input, then its hash computation has a running time that is O(n), which means that the hash time function is linear in n.)
- it is extremely unlikely to produce any two identical outputs
- given the hash output, there is no feasible way find the input; and
- puzzle friendliness

For the academic blockchain, the author suggests using the ECDSA algorithm (Elliptical Curve Digital Signature Algorithm). It is an update to DSA and is a U.S. government standard. Breaking this algorithm would have running time comparable to guessing a 128-bit encryption key by brute force It is cautioned that, when implementing this algorithm, a good source of randomness be used. Otherwise, the secret key used to sign a document could leak, making forgery feasible.

The root hash pointer at the tail of the blockchain prevents members from secretly altering any transaction, because doing so would require altering the entire upstream chain of transactions. Thus, any arbitrary litcoin node, given a single trusted transaction at time *t*, could trust the entire chain's integrity and chronological order up to time *t*. Thus, such a technique would assure members that litcoin transactions are at least as old as they claim to be.

To improve numerical efficiency, Haber and Stornetta later proposed grouping transactions into time intervals called "blocks", that were represented by “Merkle trees” (Merkle, 1980). A Merkle tree is a binary tree where the leaf nodes are the data (transactions) and the other nodes are pairs of hash pointers. Merkle's original goal was a digest for a public directory of digital certificates. For example, when a website presents a digital certificate, it can also present a short proof that the certificate appears in the global directory. Another network node can efficiently verify that proof if they know the root hash of the Merkle tree. This efficiency turned out to be one of the most important features of a distributed blockchain. It is also the core of the recently implemented Certificate Transparency System (Laurie (2014). In the litcoin blockchain, the leaf nodes of a block would be the block's transactions, and all other tree nodes would be pairs of hash pointers. The root node would be a hash pointer to the next block in the chain.

In summary, blockchains have two important properties. First, the root hash of the latest block acts as a digest of the entire blockchain. Thus, any network node given only the *last trusted* root hash value of the chain, could compare it to the *present untrusted* hash, and if equal, trust the integrity of the entire chain without downloading and inspecting it. Secondly, any network node can efficiently prove to any other node that a particular transaction is in the chain by transmitting only small number of other transactions. This ability to efficiently prove inclusion of transactions is very important in bitcoin, and would also be for litcoin, but to a lesser extent because a litcoin network would probably be smaller than the bitcoin network, and the fraud incentive less.

Fault tolerance. Another requirement of the litcoin protocol is that it be tolerant of network faults, including *Byzantine faults* (Narayanan & Clark, 2017). Byzantine fault tolerance is the network's ability to reach consensus even when faults are random and not easily reproducible. Such faults include nodes going offline forever or sending outdated messages. Note that a weakness of many such fault tolerant systems is their assumption that most network nodes are both honest and reliable. While this may be a dubious assumption in the bitcoin community, it would be less so in the litcoin community where litcoin will *not* be exchangeable for actual cash.

In review, the paper has thus far concentrated on how linked timestamps can help achieve distributed consensus with virtually no central authority. However, litcoin will need more than linked timestamps to prevent *blockchain forks*. Forks can occur when multiple blocks are generated at nearly identical times by an adversary or by multiple nodes unaware of each other's block. In this case two different nodes could mistakenly think they are working with the latest block. If not prevented, such a condition would cause the blockchain to split along different paths, destroying the chain's integrity. In peer-to-peer network protocols, this problem is known as the distributed *state replication* problem (Narayanan & Clark, 2017). Any solution to the forking problem requires that a set of nodes reach identical states each time they apply the same transactions. The fault-tolerance literature describes many such solutions, including the proof of work (POW) scheme that underpins the bitcoin network (Narayanan et. al., 2016). That solution assumes that the largest local block is the latest global block. The authors suggest that this rule be used in the litcoin blockchain.

Proof of Work. Although Nakamoto (2008) was the first to use POW to generate a cryptocurrency, Dwork & Naor (1992) proposed a POW scheme. The goal there was to deter email spam. In that design, email recipients would process only those email messages that were accompanied by a "friendly" one-way hash function (also called a "puzzle"). The solution to the puzzle was to "invert" the hash function, or to discover what its input must have been. Furthermore, the hash had to be unique to the email and to the recipient. If the message recipient can solve the puzzle in less time than the sender used to create it, then the recipient was said to have "proved" that the sender had done some work. Thus, to send a large number of messages, a spammer would have needed enough hardware power to quickly discover a friendly hash function. Otherwise, a spammer could send multiple messages to the same recipient, or the same message to multiple recipients, for a cost identical to that of one message to one recipient. Likewise, a message recipient would need significant hardware power to "prove" the work of large numbers of messages. This is the case with bitcoin, where the compute power needed to prove work is the economic scarce resource. Proving such work is known as bitcoin *mining*.

Dwork and Naor's 1992 POW scheme, however, was not suitable for bitcoin, nor would it be for litcoin, because it required a "trap door" or a secret known only to a central authority. If this super-user were compromised by an adversary, such an adversary could prove non-existent work. An idea very similar to that of Dwork and Naor (1992) called *hashcash* was independently published by Back (1997). Although it did not require a trap door, it did not prevent double spending, so never became a popular cryptocurrency.

Bitcoin and proof of work. Nakamoto, creator of bitcoin, claimed to have completely solved the problem of distributed consensus without a central authority, and thus the problem of POW (Nakamoto, 2008). In bitcoin, this trial and error POW scheme is performed by highly rewarded users called *miners,* who compete with other miners for newly minted bitcoin. A miner who "proves" the most work (aka solves enough puzzles) during a time interval gets to contribute the next block of transactions to the chain. As a reward for performing this service, a miner who contributes a *valid* (proven) block is rewarded with newly minted bitcoin. If a miner includes an unproven transaction in their block, it will be ultimately be rejected by most other miners who contribute subsequent blocks. If so, the reward for the invalid block is erased. Thus, miners incentivize each other to be honest.

Bitcoin is a true liquid currency and can be exchanged for cash. To control inflation, its POW scheme varies the number of *bitcoins* rewarded per block. This fluidity is accomplished by making the amount of compute power needed to "prove" a block proportional to the current total global mining power. Thus, the most successful miners are those with the largest fraction of the network's computing power. Note that this has caused a dangerous concentration of influence in the *bitcoin* network: a cabal of dishonest bitcoin miners could execute double-spend transactions, and secretly alter the blockchain. Although *bitcoin* seems to be working reasonably well in practice, its theoretical underpinnings are not well understood, and its future viability for legitimate business transactions is anything but certain. However, bitcoin remains quite notable because it is thought to have been the first cryptocurrency to prevent double spending, and to quickly generate a significant network effect, also called bootstrapping.

Bootstrapping a blockchain community is difficult because it involves a circular dependence among the following three ideas. First, a valuable currency is necessary to attract enough community members. Second, sufficient member work is needed to prove the work that creates the currency and deters double spending. Third, deterring double spending is necessary to support the value of the currency. Given these three conditions, a significant network effect could also occur for the proposed academic blockchain.

The litcoin community and proof of knowledge (POK). Because litcoin could not be directly exchanged for any tangible asset, the litcoin network is best thought of as an anonymous voting and reputation management system that leverages the wisdom of the crowd to evaluate content and authors. The reputation of litcoin community members would be measured by their litcoin holdings. The value of an article in the community would be measured by its review *endorsements* weighted by the reviewers' *litcoin* holdings (See figure 3, transaction types). Any cryptocurrency scheme requires a mechanism that allocates scarce economic resources. In *bitcoin* that is POW, and the scarce resource is compute power. For the litcoin community the author proposes a mechanism called proof of knowledge (POK), where the scarce resource is applied knowledge. POK is a variant of the schemes proposed for the altcoins, Steem [31], and Ethereum https://github.com/ethereum/wiki/wiki/White-Paper?source=post_page---------------------------.

Via POK, a litcoin network could leverage many of the same cryptographic concepts the paper has discussed. POK could deter spam, denial of service attacks, and "Sybil" attacks (Douceur, 2002). (A sybil attack tries to overwhelm a network by creating fake accounts).

Validators, validation and rubrics. The central challenge in an academic blockchain is a distributed consensus protocol for incentivizing individual contributions that is fair, unbiased, and resistant to manipulation by dishonest community members. Widespread abuse of the incentive system would destroy community members' faith in the fairness of the economic system, the value of the currency, along with any network effects.

Accordingly, in a litcoin network, there would be two kinds of transaction validators, gatekeepers and *supervisors* (See figure 2, membership types). After any submission, a supervisor’s node would compare its payload to the appropriate rubric and, if valid, include it in their next block of transactions. Any litcoin member could become a supervisor if they accumulate enough litcoin. Supervisors would be responsible for adding only "valid" articles and reviews into a block on the chain. A transaction would be a valid if it satisfies the rubric for its type of content. For example, to evaluate a review, a rubric like this would be used:

- “Does the review identify the reviewer?”
- “Does the review assess the empirical evidence on which the article is based?”
- “Does the review assess the article’s readability and organization?
- “Does the review assess the central contributions of the article?”
- “Does the review include a positive (or negative) endorsement?”
- etc.

Note that validating an article, or review would not be the same as evaluating their worth.

To evaluate an article, the reviewer would follow a rubric such as this:

- “Does the article identify it’s author?”
- “Does the article present the empirical evidence on which it is based?”
- “Is the article organized well organized?”
- “What new knowledge does the article contribute?”
- “Is the article written in clear language?”
- “Would you endorse this article, thereby recommending it to colleagues?”
- etc.

Valid content would be simply that which adheres to its rubric. Rubrics would be established by submissions that are the consensus of the litcoin community. Only the most senior and knowledgeable litcoin community members would become and remain litcoin supervisors.

Community members would elect supervisors via a *vote* transaction (See figure 3, transaction types.). This voting mechanism could be like that proposed by the creators of the altcoin, Steem. Accordingly, votes would be weighted by the voter's litcoin holdings. To prevent excessive concentration of power, the author recommends that one such member represent *all* the runner-up candidates.

If a supervisor repeatedly ignores transactions from a particular network node, censorship could be occurring. This would be of great concern to a litcoin community, which would need a mechanism to control it. To deter censorship, it is proposed that transaction validation be done in a finite number of "rounds", as in Steem. In each round, a sequence of supervisors would sequentially validate transactions, and the sequence would be shuffled each round. This would reduce the probability that the same supervisor could repeatedly refuse to validate the same transaction.

Validators would also be rewarded based on their *vested* interest in the long-term health of the academic community. In a sense, supervisors would use their accumulated litcoin as collateral to vouch for a block. If a block is later deemed invalid by consensus, litcoin would be subtracted from that node. Over time, articles, authors, and reviewers would distinguish themselves by the amount of litcoin they have accumulated. It is likely that a litcoin network could operate effectively without more elaborate controls on validator behavior. This is because a litcoin network would be relatively much smaller in size than those imagined by true cryptocurrency communities. Furthermore, litcoin community members would have less incentive to behave dishonestly on the network. As you may imagine, such a litcoin based protocol system could effectively shift the emphasis in academic review from "who" to "what" and "when."

Reviewing and endorsing. To promote fairness in a litcoin network, it is proposed that the review include either a positive or negative *endorsement* of the article (See figure 3, transaction types). Prior to reviewing an article, a reviewer should not be permitted to read others' reviews of it. Doing so could bias their initial impression of the article. Then, at some later point, litcoin nodes would request a summary of an article's endorsements to determine the marginal amount of litcoin to be ascribed to the author and the article. The weight of the endorsement would the reviewer's prior litcoin balance. Furthermore, if a review later became the consensus of the community, reviewers could be rewarded additionally in proportion to the ultimate reward ascribed to the article. This would incentivize the production of diligent reviews and valuable articles.

Any litcoin community member could become a reviewer, and some could become elite. However, such elite reviewers could potentially endorse their own articles, and an article with an unusually large number of positive endorsements could indicate concentration of power among collusive groups of elite but dishonest reviewers. Thus, the litcoin protocol would need a mechanism to deter this. The author proposes that negative, in addition to positive, endorsements be implemented for this purpose. Dishonest litcoin reviewers considering this kind of collusive behavior, would face what is known as the N-person prisoner's dilemma (Voneuman & Morgenstern, 1953). In the extreme case of this, if every litcoin reviewer endorsed only themselves, then no litcoin would be distributed to anyone, which could destroy the community network effect. Yet if only one reviewer defected, then that reviewer could win unearned litcoin which could cause inflation. This would also weaken the network effect. Negative endorsements could attenuate the effects of collusive dishonest litcoin reviewers.

Vesting and voting. Besides incentives for authoring, reviewing, and validating, there should be incentives for *sustained* valuable contributions. Thus, the author proposes that all content creators who make sustained positive contributions be awarded additional litcoin proportional to their *vested* litcoin holdings. This is like what Steem does (See figure 3, transaction types.). Vesting periods could be determined by some specified threshold of sustained valuable contribution. Each node could *vote* for the node producing the most work during the period. These votes would be weighted by that node's litcoin holdings. To control inflation, there would be some periodically determined maximum number of litcoins distributable during that period. At the end of each vesting period, the litcoin available for the period could be divided among members proportionally according to their total number of votes. Ideally the most *vested* nodes would have the most influence on how to reward litcoin to other nodes. Nodes with greatest vested interest in the community would have the most to lose by attempting to game the system. Thus, vesting would be an additional incentive for members to behave in a way that maximizes their litcoin's future value.

Litcoin inflation control. As mentioned earlier, the litcoin protocol would have a network effect only if content attracts new community members and keeps them engaged. To accomplish this, currency inflation control would be needed. For this, the author proposes that block production be capped at a defined rate. Furthermore, the author proposes that, of the supply of litcoin minted each year, the majority would go to authors, articles, and reviewers; with a lessor amount going to validators.

Changing the rules of the academic blockchain. Another issue to consider for the academic blockchain is a fair way to change the community rules embedded in the software. Because cryptocurrency software is freely available in the open source repository, *Github*, litcoin development could begin as a "fork" of one of these projects. Forking an open source code repository allows developers to freely experiment with and vote on proposed software changes. Because developers would be inherently very powerful community members, it would be vital that all other members of the litcoin community have an equal opportunity to vote whether to accept a proposed fork.

Bootstrapping the litcoin network. In the litcoin network, each new subscriber would be granted reader access to all articles on the blockchain. Readers wishing to become reviewers would apply for a temporary reviewer license, which would expire unless they are productive. Although unproductive reviewers would be demoted to reader access, productive reviewers would be paid litcoin, and temporarily promoted to author status; during which time they must be productive. Although unproductive authors would lose litcoin and be demoted to reviewer status, productive authors would be paid litcoin. Any productive community with enough litcoin could become a validator. Although unproductive community members could attempt a Sybil attack, there would be relatively little incentive to do so, because litcoin would not be redeemable for cash. The final step in successfully bootstrapping the academic blockchain community will be establishing a significant network effect. This would require convincing enough initial members to join. Although the challenges of establishing a large network effect for a true cryptocurrency are daunting, our proposed, much smaller, litcoin community might not face equivalently large challenges.

Transactions. In review, transactions on the proposed academic blockchain would include, at a minimum: subscription, submission, validation, vote, and payment (See figure 3, Transaction Types.). Some transactions would be initiated by community members, and others would be endogenous to the software. Yet all would be immutable parts of the blockchain. Note that there would be no litcoin "cash out" transaction. That is to say that litcoin could not be exchanged for any tangible asset. *Litcoin* would have value only by the influence in the community it represents.

Summary and Conclusions. In summary, this paper argued why and how academia might now completely rethink the concept of academic peer review. The paper presented evidence that dishonest members of the academic community can often gain unfair advantage, sometimes at the expense of the pace of scientific discovery. Then the paper reviewed the literature that suggests how existing cryptography could address these challenges. Our proposed system combines ideas from cryptography, distributed computing, economics, and cryptocurrency projects such as Bitcoin, Ethereum, and Steem.

We introduced a hypothetical pseudo-cryptocurrency called *litcoin (*for literature coin) which could present opportunities to reviewers and authors not seen today. An individual would join a litcoin community because they adhere to a set of academic values, which would include both self-interest and community interests. These values would be developed by anonymous consensus, rather than by fiat. Community members could vote how to shape and reinforce those values. Litcoin would be the reward for contributions to the academic community. The paper argued that a well-developed such mechanism could enable authors and reviewers to earn fair rewards proportional to an objective determination of the value of their academic contributions. Although such rewards would not have direct monetary value, community members with the most litcoin would wield the most power in the academic community.

In a litcoin community, the correct amount of litcoin payments would be determined by a peer-to-peer telecommunications network protocol like that used in bitcoin and various altcoins. Such a protocol should include incentives for behaving honestly on the network. Economic scarcity would be created via proof of knowledge (POK), which is a proxy for the proof of work (POW) scheme used in bitcoin.

The proposed litcoin network would employ a blockchain as its immutable public ledger of transactions, which would include, at a minimum: article submission, article review, content validation, and payment. (See figure 3.) The blockchain would ensure the exact order in which valuable contributions are enshrined. Thus, an author would always be able to point to the public ledger for proof of proper attribution.

Such a litcoin network would face fewer technological challenges than those of bitcoin and altcoin networks, because litcoin would not be pegged to any actual currency and could not be traded on any exchange. Litcoin would not be bought, only earned. Thus, there would be relatively less incentive for community members to behave dishonestly.

Ideally, there would eventually be a *single* litcoin community covering most academic disciplines. More probably, such a community would begin when a few prominent university departments include litcoin in their evaluation of faculty performance, or when a few prominent journals incorporate an academic blockchain in lieu of a chief editor. It is hard to imagine how the size of any future litcoin network would ever approach the size that Nakamoto (2008) imagined for his bitcoin network. Thus, scalable

doi:10.20944/preprints202007.0665.v1

performance would be less of a concern for the academic blockchain.

Limitations. The author realizes that the proposed litcoin technology as described would not eliminate the double spending problem, nor would it ensure that community members are completely anonymous, as Nakamoto (2008) claimed to have done: the ecosystem that grew around the bitcoin community, such as the wallet and exchange industries, do not make anonymity their priority. None the less, bitcoin is now seen as an effective vehicle for untraceable business transactions, including criminal ones. It is difficult to predict how the ecosystem to emerge around the academic blockchain would affect the anonymity of its members.

Another limitation is that, when community members are known only by their public encryption keys, there is no provable way to efficiently route messages to the correct local nodes. (Narayanan et.al. 2016). However, in the case of litcoin, the author feels that anonymity and the lack of central authority are far more important than scalable performance.

It is likely that some readers of this paper may feel the system described herein is overengineered and that its aims could be more practically addressed by the following:

1. better screening of reviewers

2. better quality control

3. implementing blind review.

However, more effective ways of dealing with items one and two are not known to the author, and there is now sufficient reason to believe that item three is now, in the internet age, virtually impossible to enforce via traditional means. Studies dating back forty years ago suggested that around one third to one half of blind reviewers could deduce authors' names and affiliations just from information in the text and bibliography (Rosenblatt & Kirk,1980; Ceci &

doi:10.20944/preprints202007.0665.v1

Peters, 1984; Yankauer, 1991) Note that these studies were conducted years before there was LinkedIn, Facebook, and Google. It seems likely that most of us would now agree that, with only a little internet sleuthing, a reviewer can determine the identity of most authors.

The other possible objection to this paper is that bootstrapping such a community would be very difficult and the few attempts to do so have thus far failed. For example, https://projectaiur.com/, or https://deip.world/.

Other's might criticize the paper on the grounds that the probability is quite low that a community, such as the one described herein, will be built, or that a description of such is no longer newsworthy. However, even if these beliefs are true, the author feels the underlying arguments are straw men. The intent of this paper is only as to be a rigorous theoretical review of the minimum requirements for such a technology. The author feels that judging the probability of it being implemented or judging its newsworthiness are for readers not the author. Readers will likely react to it quite differently according to their unique experience.

Finally, to some, it may seem ironic that the author chose to submit this paper to a traditional, albeit prestigious, peer reviewed journal. Unfortunately, a more effective means of connecting with top reviewers and readers is unknown to the author.

Future research. Perhaps the most pressing research area for blockchain networks are low-level role-based security protocols. The paper conjectured that such roles could be based on litcoin balances, and that roles such as "subscriber", "gatekeeper", "author", and "reviewer" would be needed as a minimum. This issue is complicated if members' transactions are identified only by a public encryption key, especially if they use more than one such "address". How could a member's total litcoin holdings be computed while maintaining anonymity? Could it be periodically derived and stored in the blockchain? If so, how would it be identified?

Perhaps it could be derived only at run-time by "wallets" stored on the local PC. If so, what recourse would a member have they lost their PC? The mechanisms used in Steem could help point the way here. For example, the Steem "posting" role allows "accounts" to post content, review other's submissions, and endorse them. The "active" role adds the permission to administer the "posting" role. An "owner" role has permission to administer itself and the previous two roles. Finally, the "master" role adds the permission to select certain third-party services to prevent transmission of improper keys. Another beneficial line of research would be how to integrate the academic blockchain with text reuse detection tools such as *Ithenticate* and *Turnitin*. This could help the *litcoin* community validate the true order of scientific discoveries.

In conclusion, the author firmly believes that an academic blockchain community as proposed herein can and will eventually be developed by academic leaders, perhaps with the help of cypherpunks. The author hopes this paper will stimulate their thinking.

References

Armstrong, JS (1980) Unintelligible management research and academic prestige. *Interfaces*, ***10***(2): 80–86.

Ashton, RH (1980) A review and analysis of research on test-retest reliability of professional judgment. *Journal of Behavioral Decision Making*, (13): 277–294.

Back, A (1997) A partial hash collision-based postage scheme. http://www.hashcash.org/papers/announce.txt

Campbell H (2013) The corruption of peer review is harming scientific credibility. *Wall Street Journal*, Eastern edition (July 13), file:///C:/Users/keith/Dropbox/Research/BlockChain/Paper/ISR/The_Corruption_of_Peer_Review_Is_Harming.pdf.

Ceci, SJ, Peters D (1984). How blind is blind review? *American Psychologist, 39*(12): 1491–1494. https://doi.org/10.1037/0003-066X.39.12.1491 Accessed 6/21/20.

Chaum D, Fiat A, Naor M (1988). Untraceable electronic cash. *Proc Crypto '88: Advances in*

Cryptology. (IBM Almaden Research Center, 650 Harry Road, San Jose, CA), 319-327.

Cummings LL, Frost, PJ (1985). Reflections on the experiences in an editor's chair: an analysis of reported experiences of journal editors in the organizational sciences, Cummings & P. J. Frost, eds. *Publishing in the organizational sciences:* Sage Publications, Thousand Oaks, CA., London, New Delhi, 379–468.

Deer, B (2011) The Medical Establishment Shielded Andrew Wakefield from Fraud Claims. *The Guardian* (January 12), https://www.theguardian.com/science/blog/2011/jan/12/andrew-wakefield-fraud-mmr-autism.

Douceur JR. (2002) The sybil attack. Peter Drushel, M. Frans Kaashoek eds. *Proc IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems. 2002.* (Springer-Verlag, Berlin, Heidelberg). https://dl.acm.org/citation.cfm?id=687813. 251-260.

Dwork C, Naor M (1992) Pricing via processing or combatting junk mail. Ernest F. Brickell EF, eds. *Proc* CRYPTO '92: Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. https://dl.acm.org/citation.cfm?id=705669.1992 (Springer- Verlag, Berlin) 139–147.

Ethereum. White paper. Accessed June, 17, 2020, https://github.com/ethereum/wiki/wiki/White-Paper?source=post_page---------------------------.

Fang F. Steen RG, Casadevall A (2012) Misconduct accounts for the majority of retracted scientific publications., Thomas Shenk eds 2012 *Proc of the National Academy of Sciences*. 2012 https://doi.org/10.1073/pnas.1212247109 (Princeton University Press)17028-17033.

Haber S, Stornetta, WS (1990) How to timestamp a digital document, *Proc Theory and Application of Cryptography Conf* https://link.springer.com/chapter/10.1007/3-540-38424-3_32 *.1990* Springer-Verlag, New York (1993).]437-455.

Haber S, Stornetta WS (1997) Secure names for bit strings. *Proc 4th ACM Conference on Computer and Communications Security 1997 Proc 4th ACM conference on Computer and communications security* https://doi.org/10.1145/266420.266430 (Association for Computing Machinery**,** New York, NY) 28–35.

Hanley T (2013) The problematic nature of peer review, *Counselling Psychology*. 28(1).

Henderson M. (2010) End of the peer review show? *British Medical Journal*, 340 (7749):738–740.

Jung K, Shavitt, S, Viswanathan M, Hilbe JM (2014) Female hurricanes are deadlier than male hurricanes. Fiske, ST, eds. *Proc of the National Academy of Sciences Conf. 2014* https://doi.org/10.1073/pnas.1402786111 (Princeton University Press, Princeton, NJ) 8782-8787.

Just, M. (1988) Some timestamping protocol failures, *1988*. *Proc NDSS*. 1-9.

Laurie, B. Certificate transparency (2014). *Acmqueue https://queue.acm.org/detail.cfm?id= 2668154.* (12)8:1-9.

Lodahl, JB, Gordon, G (1972) The structure of scientific fields and the functioning of university graduate departments. *American Sociological Review*. 37(1): 57–72.

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

Merkle, RC (1980) Protocols for public key cryptosystems. *Proc IEEE Symposium on Security and Privacy*. http://www.merkle.com/papers/Protocols.pdf. (Institute of Electrical and Electronics Engineers, Washington, DC) 122-134.

MILLER, C (2006) Peer Review in the Organizational and Management Sciences: Prevalence of Effects of Review Hostility, Bias, and Dissensus. *Academy of Management Journal* 49(3):425–431.

Narayanan N. Bonneau J, Felten E, Miller A, Goldfeder (2016) *Bitcoin and cryptocurrency technologies,* (Princeton University Press, Princeton, NJ).

Narayanan N, Clark J (2017) Bitcoin's academic pedigree, 2017; *Communications of the ACM*. 60(12):37-38.

Nakamoto, S. Bitcoin (2008) A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

Peters DP, Ceci SJ (1982) Peer-review practices of psychological journals: the fate of published articles submitted again. *Behavioral and Brain Sciences***.** 5(2):187–255.

Pfeffer, J (1993) Barriers to the advance of organizational science: paradigm development as a dependent variable.; *Academy of Management Review***,** 18(4):599-620.

New York Times (2009) Disgraced cloning expert convicted in South Korea. *New York Times*. https://www.nytimes.com/2009/10/27/world/asia/27clone.html. (Oct. 26).

Rosenblatt A, Kirk SA (1981) Recognition of Authors in Blind Review of Manuscripts Journal. *Journal of Social Service Research* 3(4):383-394, 1981.

Starbuck WH (2003) Turning lemons into lemonade: where is the value in peer reviews? *Journal of Management Inquiry***.** 12(1):344–351.

Starbuck, WH (2005) How much better are the most prestigious journals? the statistics of academic publication, 2005; *Organization Science***,** 16(2):180–200.

Steem (2018) An incentivized, blockchain-based, public content platform. *https://steem.io/steem-whitepaper.pdf*.

Van Rooyen S, Godlee F, Evans S, Black N, Smith R (1999) Effect of open review on quality of reviews and on reviewers' recommendations: a randomized trial. *British Medical Journal*, 318:23.

Von Neumann J, Morgenstern O (1953) *Theory of games and economic behavior*. (Princeton University Press, Princeton, NJ).

Yankauer (1991) How blind is blind review? *American Journal of Public Health* https://doi.org/10.2105/AJPH.81.7.843. Accessed 6/21//20.

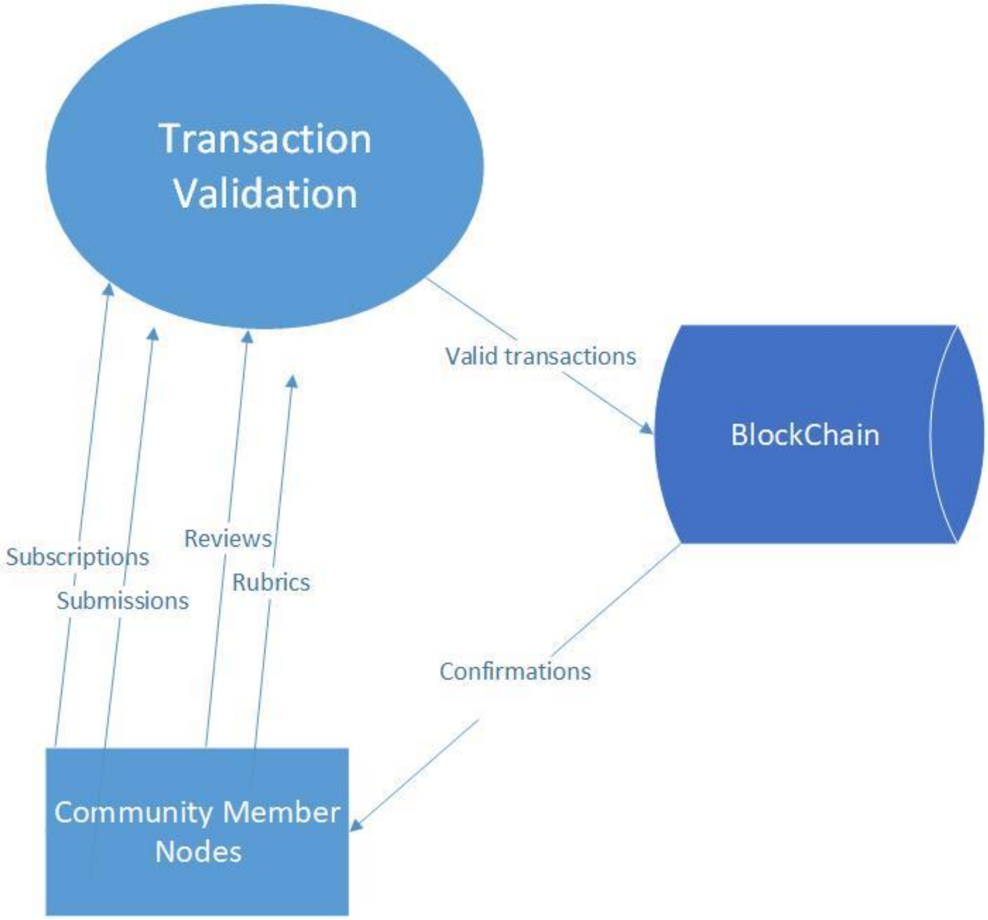
Yong, E. (2012) Why a new case of misconduct in psychology heralds interesting times for the field, *Discover: The Magazine of Science, Technology and the Future*; http://blogs.discovermagazine.com/notrocketscience/2012/06/26/why-a-new-case-of-misconduct-in-psychology-heralds-

doi:10.20944/preprints202007.0665.v1

interesting-times-for-the-field/#.XU8VJuNKi2w

Zuckerman H (1988) The sociology of science. Smelser NJ eds. *Handbook of sociology***,** (Sage Publications, Los Angeles, London, New Delhi, Singapore, Washington DC and Melbourne) 511–571.

Figure 1
Litcoin Network Data Flow



doi:10.20944/preprints202007.0665.v1

Figure 2
Community Member Types

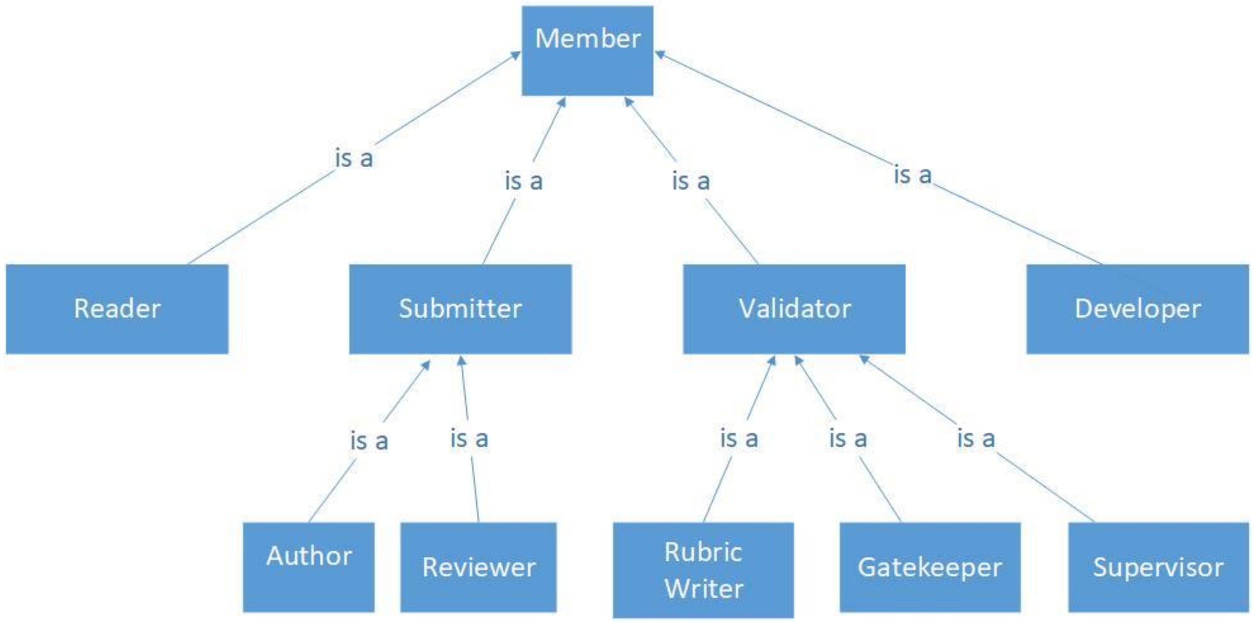
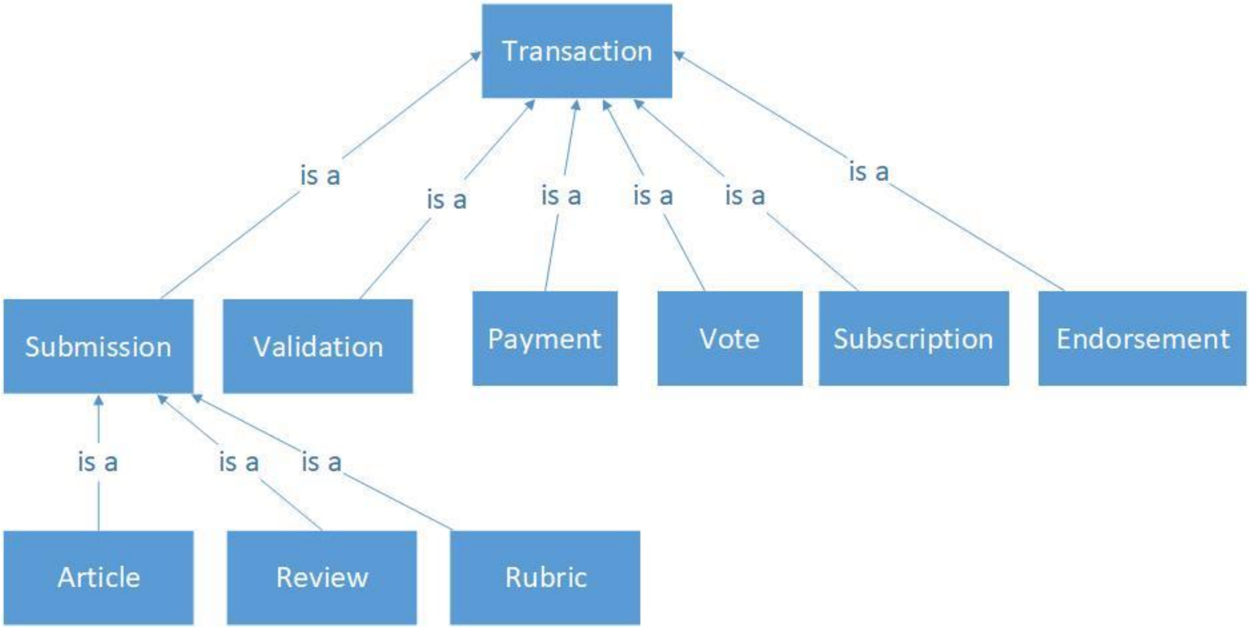


Figure 3
Transaction
Types


Transaction
is a
is a
is a
is a
is a
is a
Submission
Validation
Payment
Vote
Subscription
Endorsement
is a
is a
is a
Article
Review
Rubric