Blockchain in Academia: A Literature Review

James Pearce
james@jpearce.net

January 2019

1 Introduction

Blockchain technology was invented in 2008 by Satoshi Nakamoto. The idea of a distributed immutable ledger enabled the creation of a decentralised cryptocurrency known as Bitcoin. The growth of blockchain technology's popularity has greatly increased over the past few years; the ability to prove the existence of data at a specific moment in time has piqued the interest of many industries. This paper is a literature review of work currently being done in the field of blockchain technology, with a focus on applications of the technology in academia.

2 Academic Applications

Blockchain technology has had interest from the academic industry. Chen, Xu, Lu and Chen (2018) identify several promising applications for further research.

One such application is a system for educational reward. This could be used to create a permanent record of students' credentials in the form of a transcript, as well as a method to reward students for their work. Sharples and Domingue (2016) describe a system for educational reward which they call Kudos. Kudos is a concept for a universal academic reputation system. Participants in the system are awarded an initial amount of the Kudos currency based on current academic achievements such as citations and published author rankings, this currency is used as a metric to measure an individual's academic credibility. The currency can be transferred to individuals or institutions to increase their reputation, for example a university may transfer some of their Kudos to a student upon completion of a course.

A disadvantage to Kudos may be that it requires a central authority to control access to the blockchain, as well as to issue the initial currency. Schaub, Bazin, Hasan and Brunie (2016) explain that centralisation in this manner could leave a blockchain based reputation system open to abuse; they go on to define a completely decentralised system for use in e-commerce. A hybrid of their trustless privacy-preserving reputation system and Kudos might be an ideal solution for use in academia.

Chen et al. (2018) discuss the features of data committed to a blockchain, they note that "data recorded on blockchain are more specific, authentic, and anti-theft." These features could have implications wider than uses in academic evaluation and assessment, a system could be developed for the purpose of enforcing academic integrity. If data on the blockchain is timestamped and immutable then it could be

used to prove the originality of work in the academic field. Gipp, Breitinger, Meuschke and Beel (2017) outline a system for academic peer review which includes such features.

Chen et al. (2018) identify the need for security and privacy when committing information to the blockchain. They propose that potential privacy issues could be mitigated by using ID numbers, in place of users' real identities. Using ID numbers carries the risk of a user being linked to their blockchain identity, at which point all of a user's data would be viewable by anyone with access to the ledger (Filippi, 2016). Henry, Herzberg and Kate (2018) discuss how blockchains are open to attack by people seeking to de-anonymise users on the network. They say that privacy researchers have developed powerful heuristics, which are able to link transactions to real world users. Chen et al. (2018) say that information committed to an educational blockchain could be protected by a user's private key. This would however, defeat the purpose of having a publicly verifiable ledger in the first place.

3 Peer Review

Research is being conducted into the use of blockchain technology for the peer review process. The peer review process can involve papers being submitted online, for review by several individuals or boards. Researchers outline how blockchain technology could be used to prevent tampering and prove originality as papers are submitted.

Gipp et al. (2017) propose CryptSubmit, a blockchain based system for automating the academic peer review process. CryptSubmit aims to alleviate current weaknesses in arbitrary manuscript review systems used by journals. The authors state that current systems are open to influence by involved individuals with dishonest intentions. Several examples are cited in which work was plagiarised during the review process itself. The examples are used to justify how a blockchain based peer review system could help authors to prove ownership of their work in the event that it is plagiarised.

Whilst using blockchain technology to achieve secure time stamping, CryptSubmit does not implement it's own blockchain. CryptSubmit is a third party hosted system, it uses the Bitcoin blockchain to store timestamped file hashes through a service called OriginStamp. There are inherent security problems with a system which is not truly decentralised, as described by Schaub et al. (2016). It is possible that a malicious individual within the organisation running CryptSubmit could tamper with the data.

CryptSubmit is a complete concept for a manuscript review system which uses the Bitcoin blockchain to store immutable timestamps of work at the point of submission. The concept could be used to deter those may plagiarise the work within the review process itself. While a solid foundation, the system is open to potential tampering due to its reliance on a centralised system, as well as a third party API. Further research into this field could result in a completely decentralised review process or document time stamping system. Such a system could alleviate any trust related concerns.

Emmadi, Padmaja Maddali and Sarkar (2019) propose a MaRSChain, a decentralised manuscript review system. Similar to CryptSubmit by Gipp et al. (2017), MaRSChain aims to allow authors to prove the originality of their work after it has been submitted for review. Unlike CryptSubmit, MaRSChain is designed to operate in a completely decentralised manner; the authors assert that this can guarantee fairness for all involved parties.

Like CryptSubmit the MaRSChain implementation utilises a third party blockchain, in this case

Hyperledger. While used to demonstrate their proof of concept, the authors say that a third party blockchain is not necessary for their framework. Hyperledger allows for additional features that the Bitcoin network (as used by CryptSubmit) does not (Emmadi et al., 2019).The authors explain the advantages of these features over a network designed to handle monetary transactions.

Emmadi et al. (2019) go on to explain the advantages of using a permissioned blockchain, that is a blockchain that allows a central authority to define who is allowed to access certain features. The authors show how this can be used to manage a decentralised review system, an example being the ability to link pseudonymous identities to original identities. The ability to control which data is accessible by specific entities in a permissioned blockchain could address issues in the concepts outlined by Chen et al. (2018), where an obfuscated ID number was the privacy solution.

MaRSChain is designed to function in a completely decentralised manner, with only the access permissions being defined by a single entity. The fact that all of the processing is carried out peer-to-peer has significant advantages over other systems which also use a blockchain, the transparency that this affords means that any involved party can be assured that no data has been tampered with.

Spearpoint (2017) presents a concept for a blockchain based currency for researchers. The currency is aimed at providing potential peer reviewers with a non-monetary incentive to review papers. They state that the currency could be used as a metric to measure an individual's academic credibility, similar to how the number of authored journal publications and citations are used today.

Like Gipp et al. (2017), Emmadi et al. (2019), Spearpoint is critical of the current academic review process, he cites the lack of incentive to review a paper in a timely manner as the reason for lengthy peer review times. The lack of transparency is also criticised, he proposes a mechanism to track the review process as a part of the system. According to Spearpoint:

> "The (current) review process exhibits various forms of bias, including a sometimes arbitrary outcome as to whether a paper gets rejected or not." (Spearpoint, 2017)

Spearpoint does not provide a direct solution to potential reviewer bias in his concept, but implies that the transparency of the blockchain based system would deter it.

The research currency described by Spearpoint (2017) is comparable to the Kudos educational reward currency presented by Sharples and Domingue (2016). Both systems offer a blockchain based metric to measure academic credentials. Spearpoint (2017)'s system is created specifically for the review process with mechanisms to aid it. For either system to experience widespread adoption, a feature necessary for a distributed blockchain based system to be secure (Lin & Liao, 2017), the intended purpose of the system should be as generic as possible. A hybrid of both concepts to form a unified academic reward and credibility system might be pertinent.

4 Academic Transcripts

Several institutions are conducting research into the possibility of blockchain technology being applied to academic transcripts. This is the idea that members of academic institutions can have their qualifications and credentials committed to a blockchain. Such a system would make this information immutable and independently verifiable (Jackson, 2018).

Jackson (2018) outlines developments in the field of blockchain for academic transcripts. The article cites several academic institutions, identifying issues pertaining to fraudulent diplomas. Jackson explains that the frequency that the University of Washington finds fraudulent diplomas is representative of academic institutions nationwide; most universities will have people attempting to forge credentials from them. In addition to traditional transcripts being relatively easy to forge in comparison to a blockchain based solution, Jackson explains that traditional transcripts suffer from other issues; the student who owns the transcript may find it difficult to obtain a copy for example.

Jackson asserts that a blockchain transcript could be used to provide students "immediate access to their own data in a secure manner." It is not clear from this statement whether the credentials themselves are assumed to be secure, or the process of accessing the data itself. While data on the Blockchain can be assumed to be secure provided that there are enough nodes to maintain integrity, any user with access to the blockchain is able to access all other records (Filippi, 2016); in this sense student credentials would be immutable but not private.

Several institutions are identified which have already implemented, or are in the process of developing a blockchain based academic transcript solution. Stanford University is identified as one such university with an implementation, although specific details are not expanded upon. Central New Mexico Community College is another institution which is shown to be making advancements in the field, with digital certificates available to students. Jackson states that the college is looking to implement a blockchain solution in the near future.

Jackson outlines how institutions are looking to include student behavioural information on transcripts, including disciplinary notations. This has possible ethical implications due to the permanent nature of blockchain transactions, further research may be appropriate.

Overall Jackson provides a good summary of current developments in blockchain transcript technology. Several institutions are cited and the need for blockchain transcripts is sufficiently justified. Jackson does not discuss the potential ethical implications of what is effectively a permanent, immutable student record. As it is possible for items on a transcript to be erased or modified, two processes which the blockchain is specifically designed to prevent, it would have been pertinent for the author to discuss this.

Jirgensons and Kapenieks (2018) present a report on the potential of blockchain technology for assessment and credential management in education. They claim that a blockchain based educational credential management system can reduce administrative costs for both the student and the institution, this is supported by AACRAO (2018). They find that the cost for a student to obtain a copy of their transcript could be as high as 100 US Dollars.

Similar to Jackson (2018), Jirgensons and Kapenieks (2018) explains how a blockchain-based transcript could benefit from inherent security and immutability. They go further to say that the traditional transcript is too limited; it could include descriptions of skills achieved for example. Digital badges are identified as a potential alternative, or supplement to the traditional transcript.

The authors cite Mozilla's open digital badges as the current digital standard for online credentialing. Open badges was designed to allow students to share their achievements on different social networks, with a goal to increase student motivation (Santos et al., 2013). Jirgensons and Kapenieks (2018) explain how digital badges suffer from a lack of security; if badge issuing institutions cease hosting of their public keys then there would be no way to verify that the badge is authentic. This would render the badges

invalid.

The authors discuss how a blockchain based credentialing solution could solve the issue of badges becoming invalid over time. They say that the blockchain could be used to create redundant copies of the badges. MIT Media Lab's Blockcerts is identified as a potential blockchain based credentialing solution. Blockcerts is a certificate verification platform which is designed to match the specifications of Mozilla's open badges as closely as possible (Jirgensons & Kapenieks, 2018). Blockcerts is based on the Bitcoin network, a network designed for the exchange of monetary value. This is not ideal, as using Bitcoin for purposes other than exchanging the currency is against the best practices and may even be considered spam (Bitcoin Community, 2016). Further work could be done to implement a similar system on a purpose-built network.

5 Conclusion and Further Study

This paper has evaluated the current state of academic uses for blockchain technology; several such uses have been identified. Sharples and Domingue (2016) found that blockchain technology has the potential to motivate students as they earn a currency. The concept of an academic currency was also used by Spearpoint (2017), who showed that their research coin could be used to provide an incentive to peer reviewers, as well as a metric to measure academic credibility.

The need for a permanent and immutable record of academic credentials was identified by both Jackson (2018) and Jirgensons and Kapenieks (2018). Jirgensons and Kapenieks (2018) proposed that the blockchain could enhance traditional academic transcripts with extra information about the learning experience. This could be relevant to colleges and employers.

All of the literature attempts to show how the digitisation of established processes can speed them up. They show how the blockchain can provide security and an element of trust. It is possible that trust in a service could be misplaced if a blockchain implementation is not sufficiently secure. Lin and Liao (2017), Henry et al. (2018) describe how heuristics could be used to compromise privacy on a weak implementation. According to Wust and Gervais (2018):

> "In general, using an open or permissioned blockchain only makes sense when multiple mutually mistrusting entities want to interact and change the state of a system, and are not willing to agree on an online trusted third party." (Wust & Gervais, 2018)

Therefore while developing systems which contain potentially sensitive data, it is important that blockchain technology is implemented and used correctly, and only when necessary. Use of the blockchain for certificates or badges for example, would require a high degree of public verifiability and transparency. This however comes at the cost of privacy (Wust & Gervais, 2018), which is important to take into consideration.

If a blockchain network is to be successful then it must be robust. This is accomplished with many nodes, which can help a network resist attack (Lin & Liao, 2017). For a system to experience widespread adoption it must be targeted towards a large enough audience. Further work should be carried out to create a generic system which is capable of performing enough tasks to guarantee this security.

Additional further work could be carried out to resolve security issues when trusting public keys

over a network. In a Public Key Infrastructure (PKI) it is not possible to know for sure who you are communicating with, without manually verifying keys (Ellison & Schneier, 2000). Technology developed for the purpose of verifying academic credentials should have a mechanism to confirm that any names associated with keys are genuine.

References

AACRAO. (2018). Official transcript types, cost and volume: Results of the aacrao may 2018 60-second survey.

Bitcoin Community. (2016). Spam transactions - bitcoin wiki.

Chen, G., Xu, B., Lu, M. & Chen, N.-S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments; Heidelberg*, *5*(1), 1–10.

Ellison, C. & Schneier, B. (2000). Ten risks of pki: What you're not being told about public key infrastructure. *Computer Security Journal*, *16*(1), 1–7.

Emmadi, N., Padmaja Maddali, L. & Sarkar, S. (2019). Marschain: Framework for a fair manuscript review system based on permissioned blockchain. *Euro-Par 2018: Parallel Processing Workshops*, 355–366.

Filippi, P. D. (2016). The interplay between decentralization and privacy: The case of blockchain technologies. *Journal of Peer Production*, *7*.

Gipp, B., Breitinger, C., Meuschke, N. & Beel, J. (2017). Cryptsubmit: Introducing securely timestamped manuscript submission and peer review feedback using the blockchain. *2017 ACM/IEEE Joint Conference on Digital Libraries (JCDL)*, 1–4.

Henry, R., Herzberg, A. & Kate, A. (2018). Blockchain access privacy: Challenges and directions. *IEEE Security & Privacy*, *16*(4), 38–45.

Jackson, N. M. (2018). Transcripts transformed: Incorporating blockchain to verify academic credentials. *University Business*, 27.

Jirgensons, M. & Kapenieks, J. (2018). Blockchain and the future of digital learning credential assessment and management. *Journal of Teacher Education for Sustainability*, *20*(1), 145–156.

Lin, I.-C. & Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *IJ Network Security*, *19*(5), 653–659.

Santos, J. L., Charleer, S., Parra, G., Klerkx, J., Duval, E. & Verbert, K. (2013). Evaluating the use of open badges in an open learning environment. *European Conference on Technology Enhanced Learning*, 314–327.

Schaub, A., Bazin, R., Hasan, O. & Brunie, L. (2016). A trustless privacy-preserving reputation system. *IFIP International Information Security and Privacy Conference*, 398–411.

Sharples, M. & Domingue, J. (2016). The blockchain and kudos: A distributed system for educational record, reputation and reward. In *Adaptive and adaptable learning: Lecture notes in computer science* (pp. 490–496). Cham: Springer International Publishing.

Spearpoint, M. (2017). A proposed currency system for academic peer review payments using the blockchain technology. *Publications*, *5*(3), 19.

Wust, K. & Gervais, A. (2018). Do you need a blockchain. *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 45–54.