Blockchain-based Micro-credentials: Design, Implementation, Evaluation and Adoption

Shohil Kishore
The University of Auckland
s.kishore@auckland.ac.nz

Johnny Chan
The University of Auckland
jh.chan@auckland.ac.nz

Udayangi Perera Muthupoltotage
The University of Auckland
u.muthupoltotage@auckland.ac.nz

Nick Young
The University of Auckland
nick.young@auckland.ac.nz

David Sundaram
The University of Auckland
d.sundaram@auckland.ac.nz

Abstract

This study examines a blockchain-based micro-credential system implementation with a particular focus on understanding user perceptions. While blockchain technology has become increasingly popular, its applications extend far beyond finance and cryptocurrency. In particular, blockchain enables the generation and management of verifiable digital certificates which possess several system-level advantages when compared to current solutions. Still, does the utilisation of blockchain add value to the issuers and recipients of micro-credentials? Applying a design science approach, we design, implement and evaluate a blockchain-based micro-credential management system within a business school's executive education unit. Qualitative evaluation reveals that such systems can decrease the overall cost and administrative workload. While issuers perceive the implementation as useful and low risk, the general knowledge regarding blockchain and its advantages, especially in the context of micro-credential management, is insufficient. We discuss this amongst other challenges that must be addressed before widespread adoption of blockchain-based micro-credentials can be achieved.

1. Introduction

While it has been argued that the performance of cryptocurrencies has been underwhelming [1], the underlying blockchain technology has gained popularity for its vast applicability in areas such as smart contracts, smart property and online content distribution [2]. At its core, a blockchain represents a decentralised data structure which contains layers of cryptographically linked transactions [3]. This creates a trust minimising environment where information can be stored and verified online which opens several implementation opportunities and avenues for future research.

One implementation opportunity involves online micro-credentials. Continuous learning is a prerequisite for our current and future workforce, and micro-credentials represent a growing area of interest as it enables recipients to highlight specific courses or projects and easily communicate this information to a broad audience [4]. However, distributing and verifying micro-credentials proves to be challenging as they are likely to be generated at a higher frequency than conventional credentials such as college degrees [4].

Utilising a blockchain to store and verify credential information is already a reality, with projects such as Blockcerts providing an open standard to build applications that can issue and verify blockchain-based records [5]. However, research on designing, implementing, evaluating and adopting blockchain-based micro-credential systems, particularly from a design science perspective, is limited. Therefore, the objectives of this study are two-fold:

1. To design and implement an independently managed blockchain-based, micro-credential system within a university.
2. To evaluate the implementation from the perspectives of the certificate issuer and recipient.

To carry out this study, we adopt the Design Science Research Methodology (DSRM) [6]. DSRM is a popular approach to conduct design science research which involves six key steps: (1) Problem

URI: https://hdl.handle.net/10125/71442
978-0-9981331-4-0

Identification and Motivation, (2) Definition of Solution Objectives, (3) Design and Development, (4) Demonstration, (5) Evaluation, and (6) Communication of Results.

As the primary issues and motivation are identified above, the rest of the article is organised as follows. Section 2 explores blockchain-based applications and micro-credentials in education with a focus on blockchain. Section 3 discusses the overall requirements, system design and implementation. Section 4 summarises the preliminary qualitative findings and Section 5 presents our conclusions.

2. Related Work

2.1. Applications of Blockchain

In the context of finance, blockchain-based applications have the potential to dramatically decrease transaction costs among all participants in the economy [7]. Multiple parties can establish contracts, execute transactions and transfer value without the costly involvement of financial intermediaries [7, 8]. Beyond the financial sector, applications of blockchain technology are growing in areas such as governance [9], digital identity management [10], e-voting [11], energy [12] and education [8, 13, 14].

2.2. Micro-credentials in Education

Digital learning, also known as e-Learning, has revolutionised the contemporary education landscape [15, 16]. As technology-based learning has grown in popularity and demand, so has the need to recognise achievements through micro-credentials [15]. Micro-credentials, such as digital credentials and badges [17], allow the individual to customise their learning and development experience which, in turn, offers more control over their online representations [18].

The advantages of micro-credentials have been explored from the perspective of professionals as well as students. One study, for instance, states that utilising micro-credentials adds value to workplace learning as development opportunities can be personalised to help meeting professional requirements [18]. Another study suggests that students can be motivated, both intrinsically and extrinsically, to engage in e-Learning to earn micro-credentials [19]. Therefore, micro-credentials are likely to have a positive impact on learning engagement, particularly in the context of education.

While credentials play a valuable role in learning and workforce development, verifying credentials poses a difficult challenge. A key disadvantage of some online credentials is that they require manual verification or long-term storage by a third-party [20]. Issuing non-verifiable credentials reduces the administrative workload but that makes forgery and falsification easier to take place [21]. Falsely claimed educational credentials is a significant problem [22], with one study declaring that 6% of Bachelor's degrees and 35% of Associate's degrees were falsely claimed in the United States [23].

A potential solution to this problem could involve blockchain technology [20, 24]. The cryptographic data structure of blockchain allows blockchain records to be virtually tamper-proof and provides a foundation to build applications where credentials can be distributed without compromising integrity [25]. As abovementioned, open standards such as Blockcerts [5] possess the potential to dramatically reduce costs associated with verification [26]. While the applications of blockchain technology appear promising, there is little research on blockchain-based micro-credential management systems [27]. Therefore, evaluating technological awareness and adoption from the perspectives of the issuer and recipient proves to be valuable.

3. Design and Demonstration

3.1. Participating Organisation

The organisation participating in this study is a business school's executive education unit. This unit currently uses a micro-credential system to certify a large cohort of professional short-course participants. While the feedback from certificate recipients is generally positive, each of these certificates carries significant administrative overhead for the unit. For example, if a certificate is lost or requires verification, one of the executive education team members must manually generate a new certificate or check online records to verify the legitimacy of a certificate. Over time, this process has become a significant issue.

To help overcome these issues, we apply the DSRM to implement a blockchain-based micro-credential management system. As the unit intends to use the system long-term with minimal interference from IT or the researchers, we will have access to staff and student recipients regularly using the system. This provides us with a source of regular feedback throughout the design and demonstration process, enabling a clearer understanding of user perceptions regarding blockchain-based micro-credentials.

3.2 Implementation Design

The implementation design is based on MIT's Blockcerts open source project, an open-standard which enables trust minimising credential verification through blockchain technologies [5]. While these credentials are practically tamper-proof and simple to share online [28], they also reduce the administrative workload associated with distributing and verifying certificates manually [26]. Credential verification through Blockcerts requires minimal human interaction as the credentials can be verified securely through a four-step digital verification process using information stored on a blockchain. Since blockchains are immutable, any credential tampering would result in the verification process to fail. Also, even though credential information is stored on a blockchain, Blockcerts has implemented features to allow the issuer to revoke, cancel or set an expiry date on a certificate which would also cause the verification process to fail within a few hours of the transaction occuring.

When attempting to implement the Blockcerts project, we realised that the current project had a notable flaw: certificates could only be generated through a set of command-line procedures. Without a user interface, long-term adoption proved to be unlikely. To simplify the credential generation process, we utilised design science to guide the iterative development of cert-manager (i.e. a flask-based web application) to orchestrate the entire blockchain credential generation workflow (Figure 2). In our implementation, cert-manager works as a web form used by the issuer to input details such as certificate title, description, logo, and a file containing a list of recipients (Figure 1).

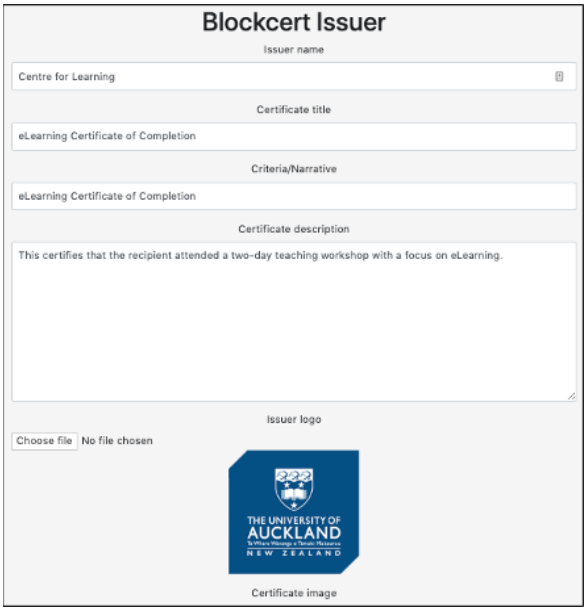

Figure 1: Screenshot of the cert-manager web form

This information is collated and then communicated to another module named cert-tools which generates a certificate for each recipient. At this stage, however, the certificates are unverifiable. To enable verifiability, cert-issuer creates a certificate hash, a string which uniquely identifies the certificate, and issues the certificate by broadcasting a blockchain transaction from the issuer to the recipient [29]. The certificates are then made available publicly online through cert-viewer which is used to display and verify certificates [29]. Finally,

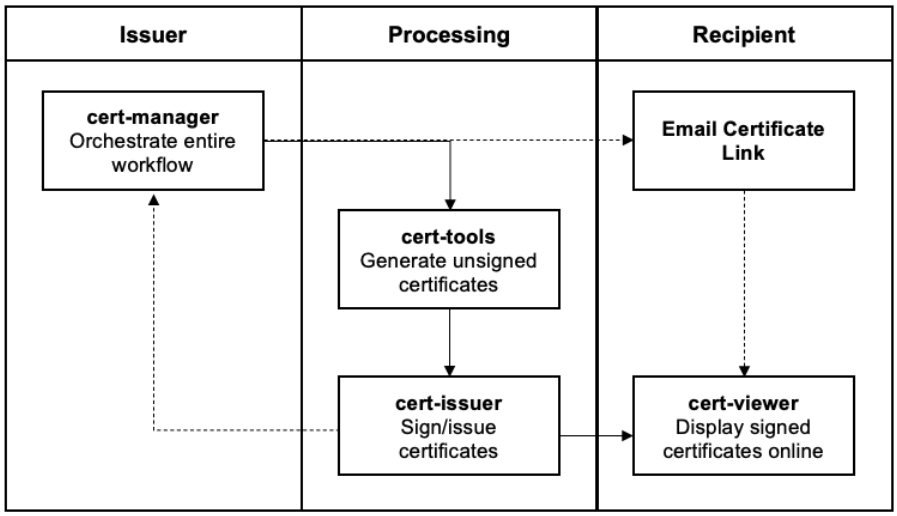

Figure 2. Credential generation process

as each certificate possesses a unique URL, these URLs are distributed to the respective recipients via email through cert-manager. The recipient could be the student of the course, current or future employers, or another educational institution.

3.3 Implementation Feedback

During the iterative requirements gathering, design and implementation processes, we found that certain factors had a persistent impact on the perceptions of team members throughout the unit. While the initial system implementation was viewed as highly useful (as it reduced overall administrative cost) and low risk (as the unit had an interest in adopting blockchain technologies), ease of use was critical in enabling adoption. Initial meetings suggested that if the system was difficult for the managers to use or understand then unit-wide implementation would not proceed. In fact, the fundamental characteristics of blockchain were discussed with the unit on many occasions. This demonstrates that blockchain, as well as blockchain-based applications, were weakly understood by the team initially despite their interest in them.

As the level of blockchain-specific knowledge increased, questions concerning risk and ease of use decreased. Interestingly, additional blockchain knowledge which was not relevant to the micro-credential management system also eased managerial concerns. Technical personnel continued to ask questions throughout the iterative implementation process, but their overall confidence in the blockchain-based implementation was higher when their perceived risk was lower. In summary, managerial confidence and support decreased perceptions of risk during the implementation. These dynamics are illustrated in Figure 3.

Figure 3. The Knowledge-Confidence-Risk nexus

4. Initial Evaluation

A qualitative approach was adopted to evaluate the system. Interviews were conducted with students (i.e. recipients) who were awarded a digital credential, and course administrators (i.e. issuers) who generated the credentials. While data collection continues, we present the initial results from three semi-structured interviews (two recipients and one issuer) and five survey responses (five recipients).

To identify potential interview questions, we focused on potential adoption concerns with blockchain-based technology. Literature as well as implementation feedback further guided the development of the questionnaire.

Contrary to the usual undergraduate cohort, all student participants were full-time professionals who were working in the sales and financial sector which is generally representative of the population studied. In order of collecting data, the first female participant (hereto referred to as S1) was 28 years old and had worked in a retail sales organisation for three years at the time of interview. The second female participant (hereto referred to as S2) was 30 years old and worked in the sales division of a tertiary education organisation for over four years. She was familiar with provisioning of micro-credentials. The third and fourth participants (hereto referred to as S3 and S4) were males who were respectively 30 and 31 years old and worked in finance-related positions. The last female participant (hereto referred to as S5) was 38 years old and also worked in the retail sales sector.

The issuer (hereto referred to as I1) was a female employee at the issuing institution. She was 28 years old and had started working at the issuing organisation a few months before system implementation began. Managing the digital micro-credential provision was one of her first duties. She had prior experience with the pre-established process of managing paper-based qualification distribution.

The student participants were sourced from courses which ran from June 2019 onwards. The interviews were conducted either face-to-face or via video conference and lasted approximately 30 minutes each. All interviews were carried out in English. The audio recordings were then transcribed, coded and thematically analysed with NVivo 12.

The first cycle of the coding process started with reading through each transcript and assigning descriptive codes [30] which enabled understanding, summarising and constructing a core index of the key concepts within the data. The codes were then categorised based on underlying patterns, thus using thematic analysis for further analysis of the

descriptive codes. Some significant themes identified during thematic analysis are discussed below.

4.1 Effortless Use

It was evident from the interviews that 80% of the student participants did not possess a high level of technical knowledge. The participants admitted that they had a basic understanding of blockchain technology and were in fact caught off guard when they were provided with a blockchain-based online credential. S1 admitted that:

"My current understanding is that it's (blockchain) a way of linking information, a lot of different stages of information, to an item like a contract or currency as well. It's my understanding that it can also show the history of the transactions or the movements of that information. I didn't realise the email sent to us with a certificate was on the blockchain" (S1).

However, both S1 and S2 agreed that once they received the email certificate, they were able to quickly identify how to use the system and access the credential. S2 stated "*What was interesting was that even though there was no history, it was pretty straightforward and user-friendly. Like it was easy enough to go through it"*. S2 went on to state that she was expecting "*something to come out in the post 30 days after training"*. She also elaborated on how she used the system by saying:

"When I got it, I thought there would be more than that, oh, okay. If that's how they are doing it, you know, at least it has arrived was more the thing. So I just went into the email and I had to read and downloaded and printed it out. I think I've also saved the actual documents on my computer as well as a personal copy to my personal email address" (S2).

The issuer (I1), who was generating the certificates, also agreed that the system was *"very easy to use"* and went on to elaborate that only two issues had been brought to her attention regarding *"operating glitches"*. One of the issues involved some students claiming that they did not receive the email containing the link to the certificate. This was later revealed to be due to the firewall settings on the recipient's end and not relevant to the system's operations. The second issue involved errors being generated when verification requests were sent. The development team were notified of this and addressed the issue immediately. I1 went to state that the system *"was up and running again within a few hours"*. Therefore, we can conclude that our initial design objective of providing ease of use has been achieved and has led to an increased intention to use the credential management system. This finding, however, did contrast with the some of the other themes that emerged.

4.2 Perceived Short-Term Benefit vs. Perceived Long-Term Value

The responses received from all students who were interviewed indicated a prominent perception that the verifiable credential lacked long-term value. However, all of the participants agreed that receiving a certificate online had certain short-term benefits. One of the participants (S2) had experience working with physical certificates before as an issuer. She stated:

"What this would mean is that you wouldn't have to print and post to people, you know, like you're printing this stuff and you're posting and sometimes the postman is not always on time and then the certificates get damaged in the post or they don't ever get there. You know, or the person that's receiving it for some reason changes location or changes jobs and address you might have listed for them is no longer current" (S2).

This eloquently describes the administrative benefits of the technology over traditional paper-based certificates, as recognised in the literature [14].

S1 was quick to identify the benefit of being able to authenticate a qualification quickly by saying *"But it would be easier for me to correlate that information to get it quickly to an employer because I wouldn't have to go through that process of getting it certified by someone else"*. The participant went on to add that as a person experienced in human resource management, she was well aware of the perils of qualification counterfeiting. Blockchain is recommended for its ability to provision a comprehensive system for recording, storing and retrieving educational information and enabling verifiability [31].

Other short-term benefits identified included the ability to easily store and access the qualification as well as reuse it. For example S4 stated "*having an e-cert is more convenient than paper, I know where it is and I won't lose it or forget it*".

Whilst benefits were perceived, all the participants, however, expressed reservations regarding the usefulness (long-term value) of the credential sent to them. For example, one participant (S1) mentioned that she would not be using the credential sent to her to provide evidence of qualification to a third party, saying *"I would be unsure as to their understanding of it. And so, it would depend on the knowledge of the technology that would affect whether or not I send it"* (S1).

S5 stated that *"other people I send this to would not understand what is verification. It needs to be explained to them"*. This indicates that a knowledge barrier could prevent the long-term adoption and use of the system and impact its perceived long-term value. This finding is in line with other studies where a lack of knowledge of the technology has frequently been cited as a potential deterrent for its continued adoption in business applications [32]. Another participant (S2) stressed that *"I don't think people have a very good understanding of what blockchain is so they may be surprised if I sent them a link saying they could verify my qualification through that" (S2).*

Furthermore, 60% of the participants dismissed the need for continuous use of the system. S1 stated that:

You know, at the end of the day, very seldom do they actually ask you when you do things or to actually bring in your hard copy certificate that was provided, and if they need very fine details they know and have the means and ways of doing it." (S1).

This comment clearly indicates that the participant did not perceive a need for the credential verifiability provided by the system nor its long-term value. While the students did not perceive the long-term value clearly, the staff member (I1) had a different viewpoint. The new system was seen to *"take less time and effort"* than the previous method that the issuing team had been using to generate certificates and the issuing team were keen to keep using the system. She went on to state that:

"I guess maybe there's about 40% less time spent with the blockchain one because the certificate is set up and ready to go. Whereas with the system we used (previously), you have to create the draft of each course. So, like the template for each certificate. And imparting dates and making sure that like names and all that is correct. Yeah, we would continue to use it, I think it's been pretty good" (I1).

The above comment clearly indicates how the ease of use of the system has generated an enhanced perception of its usefulness. The only concern that the staff member had regarding the long-term value of the system was that it would need to scale to handle a larger number of requests for generation and verification of certificates. She suggested *"having the capacity to have them be verifiable with a large number of students and not cause issues"* as a potential improvement to the current system. The differences in perception of value for the student and issuer is illustrated in Figure 4.

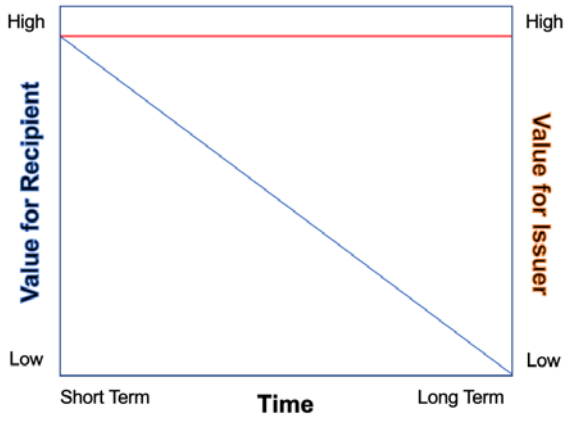

Figure 4. Value over Time for Recipients vs. Issuers

4.3 Security of Personal Data

A key consideration which emerged from the analysis of interviews is a conflict between the usefulness of the system and its security. All participants expressed concerns regarding how secure it was to store their information on the system and who had access to the system. Our participants also appeared to be concerned about the possibility of modification as well as unauthorised access. One participant (S2) said, *"So I'm thinking that there must be some IP and some code behind it to make sure that it (the certificate) doesn't go necessarily to the wrong person"*. During the interview, S1 attempted to understand the possibility of unauthorised modification by asking *"Is it possible that the information could get changed in anyway? I assume you must have taken what precautions you can for that"*.

Furthermore, one participant (S2) explicitly referred to the European General Data Protection Regulation (GDPR), and the necessity for any solution to be GDPR compliant in the following manner:

"Do you know about the GDPR? Yeah. So, we work with those rules and those policies and things like that. So, it's kind of like, okay, what systems are in place that my data is going to get collected and actually being put in the right place. Actually, who's actually got, you know, access to this information, I don't know. So that was kind of like, concerning, where does this actually land in, in the bigger scope of things?" (S2).

Indeed, we are in agreement that any blockchain-based application should carefully consider GDPR implications. It has been established that blockchain eliminates the necessity to trust a centralised authority in order to retain an accurate record of

activity and makes surveillance of activity difficult. The above comment made by the interview participant also indicates that the concerns that the participants raise regarding security could also be fuelled by a lack of knowledge regarding the technology.

The staff member (I1), on the other hand, did not perceive data security to be a pressing concern. She believed that the new system was *"as secure as the certificates we were using anyway"*. She believed that the responsibility for securing the credential data was as much with the receiver as with the sender elaborating that *"at the end of the day, all that data is going to be stored somewhere. Unless they share the link with someone. I don't see how we can be, they need to protect their own stuff" (I1).*

4.4 Need for Enhanced Knowledge

The apparent lack of knowledge and expressing a need for further knowledge about the system itself and the underlying technology in general was a recurrent theme within the student participant's narratives. The interview participants did have a basic understanding of blockchain technology and were accepting of the system in general. As mentioned previously, however, the perception of long-term value of the system was impacted by the perceived lack of knowledge about blockchain technology. Hence, all the participants suggested that certain initiatives should be taken for enhancing the current level of knowledge. One such initiative was to provide the students themselves with more information about the system in such a way that the information could be shared with a third-party. For example, one participant (S1) elaborated saying:

"…accompany this (the emailed certificate) with an instruction set saying here's why you have been sent this and here's what you could do with this. If you want to apply for any position or if you want to send this to somebody else your qualification for verification, here's what you need to do" (S1).

Another initiative recommended by the participants was to include instructions on exactly what could be done with the credential within the email sent across to them as well as to provide them with this information before the credential was issued so that they could opt to receive a paper-based certificate if required. When probed further to indicate why they might opt for a paper-based certificate again the reason provided was that *"Other people may not have the required knowledge" (S2)* to use the credential as it was *"meant to be used"(S1).* When these recommendations were discussed with the staff member who was a core member of the team which had interacted with the students regarding issuing and verification of certificates, she agreed that these recommendations were sensible from the student perspective. The issuing team had been provided training on the system and how to use it and therefore *"knew what this was all about" (I1).* The students on the other hand had only been provided with a *"5-minute talk" (S1)* on the new method of receiving certificates before their consent had been obtained. The staff member (I1) conceded that *"It would be good for them to know explicitly what the advantages are and how it is going to be useful for them. So, yeah, providing more information would be the key here" (I1).*

5. Conclusion and Limitations

Our current findings utilising the DSRM indicate that the system is well received by the stakeholders. Both the recipients and the issuers appreciate the ease of use provided by the system. The issuers also plan to continue using the system.

Most importantly, however, the current findings indicate potential concerns which may negatively impact the persistent adoption of a blockchain-based micro-credential management system and the issues which need to be addressed to allow for adoption. The recipients primary concerns revolved around perceived long-term value and security. This aligns with current research which identifies technology risks, data privacy concerns, lack of awareness and regulatory uncertainties as significant barriers to blockchain adoption [33, 34].

Lack of knowledge regarding blockchain technology in general, and our system in particular, decreased perceived usefulness and increased perceived security concerns. Providing clear prior information could be one approach to address the concerns of the recipients. The initiative to enhance the current level of knowledge and provide clear instructions should encompass not just the immediate recipients of a certificate generated by the system (the students) but also the end recipient who would use the system for verifying a certificate. This end recipient could be, for instance, a potential employer of the student who has received a certificate generated by the system and needs to verify its authenticity. This recommendation is further strengthened by the findings regarding the issuer. They were more knowledgeable due to training and exposure to the system, and therefore less concerned about security risk, and more aware of the system's usefulness.

Our study aligns with Iansiti and Lakhani [35] who define the four stages of blockchain adoption as

(1) single use, (2) localisation, (3) substitution, and (4) transformation. Our blockchain-based micro-credential management system is positioned in the third quadrant where we hope to replace well established and deeply embedded credential provisioning systems within educational institutions. Iansiti and Lakhani [35] also argue that blockchain is a foundational technology, and its widespread adoption is only possible after a complex set of issues spanning across technological, societal and organisational areas are resolved. This is in line with the findings from our interviews where the existence of societal and technological issues has been verified, indicating a need for further investigations.

The data collection process continues. We have not yet identified recipient concerns regarding system usability and usefulness. Furthermore, we are currently in the process of collecting quantitative data which attempts to evaluate the system's perceived ease of use, usefulness and risk, as well as their subsequent effects on long-term usefulness and adoption. We have received approval to approach over 7,000 participants to carry out this study. The results from this study will be made available in future publications.

6. References

[1] R. Farell, "An analysis of the cryptocurrency industry," University of Pennsylvania, Pennsylvania, USA, 2015.

[2] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?—a systematic review," *PloS One*, vol. 11, no. 10, p. e0163477, 2016.

[3] L. Luu, D. H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria, 2016: ACM.

[4] M. LaMagna, "Placing digital badges and micro-credentials in context," *Journal of Electronic Resources Librarianship*, vol. 29, no. 4, pp. 206-210, 2017.

[5] Blockcerts. (2019, 28/11/2019). *Guide*. Available: https://www.blockcerts.org/guide/

[6] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of management information systems*, vol. 24, no. 3, pp. 45-77, 2007.

[7] A. Tapscott and D. Tapscott, "How blockchain is changing finance," *Harvard Business Review*, vol. 1, no. 9, pp. 2-5, 2017.

[8] F. Casino, T. K. Dasaklis, C. Patsakis, and Informatics, "A systematic literature review of blockchain-based applications: current status, classification and open issues," *Telematics*, vol. 36, pp. 55-81, 2018.

[9] W. Reijers, F. O'Brolcháin, and P. Haynes, "Governance in blockchain technologies & social contract theories," *Ledger*, vol. 1, pp. 134-151, 2016.

[10] P. Dunphy and F. A. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 20-29, 2018.

[11] P. Boucher, "What if blockchain technology revolutionised voting," 2016.

[12] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," *Computer Science-Research and Development*, vol. 33, no. 1-2, pp. 207-214, 2018.

[13] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *European Conference on Technology Enhanced Learning*, Cham, 2016, pp. 490-496: Springer.

[14] A. Grech and A. F. Camilleri, "Blockchain in education," ed: Luxembourg: Publications Office of the European Union, 2017, p. 137.

[15] P. A. Lemoine and M. D. Richardson, "Micro-credentials, nano degrees, and digital badges: New credentials for global higher education," *International Journal of Technology and Educational Marketing*, vol. 5, no. 1, pp. 36-49, 2015.

[16] C.-S. Li and B. Irby, "An overview of online education: Attractiveness, benefits, challenges, concerns and recommendations," *College Student Journal*, vol. 42, no. 2, 2008.

[17] J. Clayton, R. Elliott, and J. Iwata, "Exploring the use of micro-credentialing and digital badges in learning environments to encourage motivation to learn and achieve," 2014: ASCILITE.

[18] C. Gamrat, H. T. Zimmerman, J. Dudek, and K. Peck, "Personalized workplace learning: An exploratory study on digital badging within a teacher professional development program," *British Journal of Educational Technology*, vol. 45, no. 6, pp. 1136-1148, 2014.

[19] S. Abramovich, C. Schunn, and R. M. Higashi, "Are badges useful in education?: It depends upon the type of badge and expertise of learner," *Educational Technology Research and Development*, vol. 61, no. 2, pp. 217-232, 2013.

[20] W. Gräther, S. Kolvenbach, R. Ruland, J. Schütte, C. Torres, and F. Wendland, "Blockchain for education: lifelong learning passport," in *Proceedings of 1st ERCIM Blockchain Workshop 2018*, Amsterdam, Netherlands, 2018: European Society for Socially Embedded Technologies (EUSSET).

[21] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, "Blockchain and smart contract for digital certificate," in *2018 IEEE International*

Conference on Applied System Invention (ICASI), Chiba, Japan, 2018, pp. 1046-1051: IEEE.

[22] A. Ezell and J. Bear, *Degree mills: The billion-dollar industry that has sold over a million fake diplomas*. Pyr Books, 2005.

[23] P. Attewell and T. Domina, "Educational imposters and fake degrees," *Research in Social Stratification and Mobility*, vol. 29, no. 1, pp. 57-69, 2011.

[24] J. Hope, "Issue secure digital credentials using technology behind bitcoin," *The Successful Registrar*, vol. 17, no. 11, pp. 1-4, 2018.

[25] A. Murali, "A blockchain-inspired design for a modern academic system," 2018.

[26] M. Jirgensons and J. Kapenieks, "Blockchain and the future of digital learning credential assessment and management," *Journal of Teacher Education for Sustainability*, vol. 20, no. 1, pp. 145-156, 2018.

[27] M. Oliver, J. Moreno, G. Prieto, and D. Benítez, "Using blockchain as a tool for tracking and verification of official degrees: business model," in *29th European Regional Conference of the International Telecommunications Society (ITS)*, Trento, Italy, 2018.

[28] Blockcerts. (2019, 28/11/2019). *FAQ*. Available: https://www.blockcerts.org/guide/faq.html

[29] MIT Media Lab. (2016). *What we learned from designing an academic certificates system on the blockchain*. Available: https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196

[30] J. Saldaña, *The coding manual for qualitative researchers*. Sage, 2015.

[31] M. Kirya, "Corruption in universities: Paths to integrity in the higher education subsector," Norway2019.

[32] G. R. White, "Future applications of blockchain in business and management: A Delphi study," *Strategic Change*, vol. 26, no. 5, pp. 439-451, 2017.

[33] B. Biswas, R. J. C. Gupta, and I. Engineering, "Analysis of barriers to implement blockchain in industry and service sectors," vol. 136, pp. 225-241, 2019.

[34] M. Kouhizadeh, S. Saberi, and J. J. I. J. o. P. E. Sarkis, "Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers," vol. 231, p. 107831, 2020.

[35] M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Business Review*, vol. 95, no. 1, pp. 118-127, 2017.