Rakibul Hasan Sayed

POTENTIAL OF BLOCKCHAIN TECHNOLOGY TO SOLVE FAKE DIPLOMA PROBLEM

UNIVERSITY OF JYVÄSKYLÄ
DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION SYSTEMS
2019

ABSTRACT

Sayed, Rakibul Hasan
Potential of blockchain technology to solve fake diploma problem
Jyväskylä: University of Jyväskylä, 2019, 71p.
Information Systems, Master's Thesis
Supervisor: Semenov, Alexander

Blockchain technology is a revolutionary technology for its potential to build systems where strangers can transact with each other without the need of any intermediary to oversee the transaction between the parties. In our traditional degree certificate system, employers need to trust the intermediaries e.g. certificate holder, teacher and university officials for the legitimacy of the certificate. Because of trust, there are vulnerabilities to fraudulent activities by the intermediaries to produce fake diplomas or fake degree certificates. Fake certificates cause significant damages to the society. In this research, using design science research methodology (DSRM) process model, we have developed a conceptual model of a blockchain-based certificate system where blockchain technology replaces the need of trust on intermediaries in the certificate system and prevent the fraudulent activities to produce fake or illegitimate certificates. Our conceptual model addresses the fraudulent activities which are not addressed by the existing blockchain-based certificate systems. Developed artefact- the conceptual model can be used for developing prototype and further research. This research also contributes to the research field of blockchain technology as a trust-free technology and fraud activities in degree certificate system.

Keywords: DSRM, blockchain, trust-free system, fake diploma, fake degree certificate

FIGURES

TABLES

ABBREVIATIONS

API	Application Programming Interface
DApp	Decentralized Application
DSRM	Design Science Research Methodology
ECTS	European Credit Transfer and Accumulation System
HEI	Higher Education Institute
ICO	Initial Coin Offering
IPFS	Interplanetary File System

TABLE OF CONTENTS

1 INTRODUCTION

Degree fraud has become a global phenomenon because of the rising demand of degree certificate in job market (Brown, 2006). There is a billion-dollar industry behind the credential frauds and no nation is immune from the problem (Ezell & Bear, 2012). Based on national data in US, 6% bachelor's degrees and 35% of associate degrees are fake (Attewell & Domina, 2011). Almost every employer has or will come across a degree certificate which is either produced through fraudulent activities by a student or officials in a legitimate institute or issued by a fake institute (Mir-Jabbar, 2017). As certification process and university's internal data system is not transparent to employers, employers need to trust the intermediaries such as students, teachers and university officials involved in the certification process for the legitimacy of the accomplishments claimed in the certificate. Because of this trust issue, there is always risk of error and fraud activities which leads to produce and present fake diplomas.

There is an emerging technology called Blockchain which promises to build trust-free and transparent systems where we do not need to trust any middleman or central authority to make and store transactions between two strangers (Beck et al., 2016; Gupta, 2017). Blockchain technology can help to develop a trust-free distributed digital platform through a peer-to-peer consensus network which is open for all to innovate their own trust-free business model (Asharaf & Adarsh, 2017). It establishes integrity and trust between strangers (Tapscott & Tapscott, 2016b). The first application of blockchain technology was Bitcoin based on the white paper by Satoshi Nakamoto in 2008 (Mattila, 2016). Satoshi demonstrated the possibility to transact electronic cash between two strangers without any intermediaries like bank (Nakamoto, 2008). People from different industries are using blockchain technology to build applications which enable trust-free transactions and protect the system and data from fraudulent activities (Banking Is Only The Beginning, 2018). For example, health care, insurance, and supply chain industries are implementing blockchain based solutions to make their business more efficient. In this research, we will use the potentials of blockchain technol-

ogy to make a trust-free certificate system where we don't have to trust the intermediaries such students, teachers and university officials, and which will prevent fraudulent activities in the certificate system.

1.1 Motivation

Academic certificate is an important piece of document which confirms that the certificate holder has achieved certain learning outcomes or accomplished certain course work before achieving this certificate. This certificate will lead the certificate holder to get some important role in the society, for example to become a doctor, engineer, or a teacher. If the certificate holder claims or present a certificate without proper studies being done, which is a fake certificate, it creates a significant damage to the whole society and economy.

The dean of the admissions at Massachusetts Institute of Technology (MIT), Marilee Jones, resigned after it was found that she had fabricated her own educational credentials and she did not have even an undergraduate degree. (Lewin, 2007). We live in a society where educational credential or certificate is very important. So, there will be always somebody to counterfeit it (Clifton et al., 2018).

A fake diploma or fake certificate refers to a counterfeit and substandard academic degree to give impression of real academic achievement (Grolleau et al., 2008). In our traditional certificate system, there are several actors. Teachers assess the course work to grade or give the credits to students. University officials or secretaries checks the completed courses and publish final certificate. Students present the paper copy or the digital copy of the certificate to employer. If any of these actors does any unscrupulous or fraudulent activity in their respective role, that could lead to produce a fake certificate. Details of the fraudulent activities by different actors have been explained in Fake Diploma section.

In most of the universities, a paper-based final degree certificate is given based on the students' completed courses recorded in the university's database. Although paper-based certificate has some built-in security features, still it is possible to make a counterfeit copy of the certificate outside of the institute. In some cases, student just add fake certificate in his or her resume without achieving the real certificate. In both cases employer's might just take the certificate at face value to avoid manual and lengthy activity to verify the certificate.

In case of digital certificates which are cryptographically signed requires much effort to secure the registry of the certificates and open standard for digital signatures for global verification. Even though the certificate is verified against the university register, employer can not verify that whether the teacher took any fee to give the passing grade or university officials took any fee to register illegitimate grade in the university database. In both cases, employers have to trust

teachers and university officials that they did not do any fraud activity or error during grading or registering certificate data.

Apart from trusting the human actors (teachers, university officials, and students) in the certificate system, employers have to trust the university's database where students' certificate data is stored. These traditional databases are not tamper-proof, which are prone to get hacked or can be changed by any internal officials. And it is not possible for an employer to detect the tampering in the university's database. Usually these traditional databases are on centralized server, not transparent to employer, and only accessed by the database admins. There is no way to trace or verify the certificate data directly on the university's database. So, employers have to blindly trust the study data management system of the university for the legitimacy of the certificate.

Blockchain technology is an emerging technology and offers features like decentralized, transparent, and tamper-proof data storage. It can be used to solve issues such as lack of trust, fraud, high transaction cost, sharing, privacy and evaluating trustworthiness of a potential actor in a transaction (Zhao et al., 2016). Therefore, blockchain technology is a promising technology to prevent the fraud activities in our current paper-based or digital certificate system.

Present blockchain applications in education are applying blockchain technology to support academic degree management and evaluation for learning outcomes (Chen et al., 2018). There is no application, research paper or projects which focuses on applying blockchain technology to prevent fraud activities in certificate system. But the researchers suggest that blockchain is ideal to prevent fraud activities in certificate system or to solve fake degree problem (Chen et al., 2018; Gräther et al., 2018). In this research, we want to make a contribution to fill-up this research gap by designing a conceptual model of a blockchain based certificate system to prevent fraud activities in certificate system.

1.2 Research objective and questions

The goal of this research is to design a blockchain technology based degree certificate system to prevent the fraud activities or the ways of making fake diploma. Our first objective is to find out the ways of making a fake degree, in other words what are the fraud activities in our traditional certificate system. Second objective is to check the existing blockchain based certificate systems and find out whether the existing systems are preventing or addressing these fraud activities. Finally, we will design a blockchain based system which will address fraud activities which are not addressed by the existing blockchain based systems.

Research Question:

> How to design a blockchain-based certificate system to solve fake diploma problem?

Sub-questions:

1. What are the ways of making fake diploma or fraud activities to make fake diploma?

2. How existing blockchain-based certificate or education systems prevents fraud activities?

3. How to design a blockchain-based certificate system to prevent fraud activities which are not prevented by the existing blockchain-based certificate systems?

1.3 Thesis structure

The structure of the thesis is as follows. The introduction section presents the motivation, research questions, summary of the result and contribution of the thesis. After that we will present the design science research methodology (DSRM) and application of DSRM in my thesis. Then we will do literature review in next four sections as preliminary work for my research. First, on fake diploma to list the fraud activities in degree certificate system. Second, on blockchain technology and its features. Third, what does trust-free means in blockchain technology. Fourth, existing blockchain-based systems and how they prevent fraud activities in certificate system. After literature review, following each section will represent the activities of our design science approach- Problem Identification,

Objectives of the Solution, Design and development, Demonstration and Evaluation. In the Discussion section, we will discuss about the results, implication to research and practice. Finally, we will conclude the thesis with limitations of the study and recommendations for further research.

1.4 Summary of the result

There are two types of fraud activities in certification system - 1) fraud activities done by university internals (teachers, university officials) 2) fraud activities done by students. Existing blockchain based systems prevent the fraud activities done by students, not the fraud activities which are done by university internals. If we change the traditional study data system which is based on centralized server and traditional databases to blockchain based study data system it will reduce the fraud activities by the university internals. Finally, we have designed an artefact, conceptual architecture of the university's internal study data system, which addresses the fraud activities which are done by university internals or happens inside the university. Through design and evaluation of the artefact, we have found that blockchain can take care of the trust issues or fraud activities in the certificate system by enforcing teachers, officials to act according to the regulations set in the smart contracts, and by recording their transactions or activities during certification process in immutable blockchain storage.

1.5 Contribution

This research has made novel contributions by identifying the fraud activities which have not been addressed by existing blockchain based certificate systems. Other blockchain based certificate systems have not addressed the fraudulent activities by university's internal officials or teachers in the study data system. We have developed a conceptual model of an improved blockchain based certificate system which will address the fraud activities which have not been addressed by existing blockchain based certificate systems.

2 RESEARCH METHODOLOGY

As the goal of our thesis is to develop a conceptual model of a blockchain based certificate system to prevent the fake diploma problem, design science research methodology (DSRM) is the best fit for our research. In design science, researchers create IT artefact to solve unsolved and important business problem and get understanding about the problem and the feasibility of the solution (Hevner et al., 2004). Through developing this artefact, we will try to prevent fraudulent activities which are not prevented by the existing blockchain based solutions and understand the potentials of blockchain technology to develop trust-free systems.

2.1 Design science research

Most of the research in Information Systems Science falls into two categories- behavioral science and design science (Hevner et al., 2004). In behavioral science research, researchers make research contribution by developing theories which predict or explain the phenomena related to the use of existing IT artefacts implemented in organizational context (Hevner et al., 2004).

In design science (DS) research, researcher makes research contribution by creating and evaluating Information Technology (IT) artefacts to solve an identified, unsolved and important business problem (Hevner et al., 2004). It enables the researcher to understand the problem and the feasibility of the solution (Hevner et al., 2004). The created IT artefact can be a construct, a model, a method or any designed object which is relevant to the solution of the identified problem (Hevner et al., 2004).

2.2 Definition of artefact

IT artefacts in IS research refers to the constructs, models, methods and instantiations which researchers develop or innovate through design science research to understand and solve problems. The problem can be improving the information system or the process of information systems development. The artefact can be used in development or use of information systems (Hevner et al., 2004). In general, IT artefacts are not production ready information systems (Hevner et al., 2004). But It holds/contains the knowledge achieved through design science research which improves the capability of designing, implementing, analysing or use of information systems (Hevner et al., 2004).

For example, an entity-relationship model, is an IT artefact, which is a set of constructs which helps to do system analysis and database design to develop the final information system for a specific problem. Additionally, this model can also be generalized to solve problems in similar problem domains. A method for building such model can also be another artefact (Hevner et al., 2004). (IS Artifact) Not exactly designing the solution to a problem or instance of problem, but the guidelines/ theories/ model/ methods/ concepts(constructs) to design the solutions to solve that kind of problems.

2.3 Design science research guidelines

Hevner et al. (2004) have established seven guidelines which can be understood as requirements for an effective design science research. They are 1) Produce an innovative and purposeful artefact 2) Artefact is purposefully developed to solve important and unsolved business problems 3) design artefact is evaluated 4) Verifiable research contributions 5) rigorous methods used in construction and evaluation of design artefact 6) Design artefacts as a search process utilizing available means 7) communicate the research to appropriate audiences.

2.4 Design science research methodology (DSRM)

To carry out a design science research, Peffers et al. (2007) have introduced a DSRM process model. DSRM process model has described seven activities which provides roadmap to conduct a DS research and a mental model about the characteristics of the research outputs (Peffers et al., 2007).

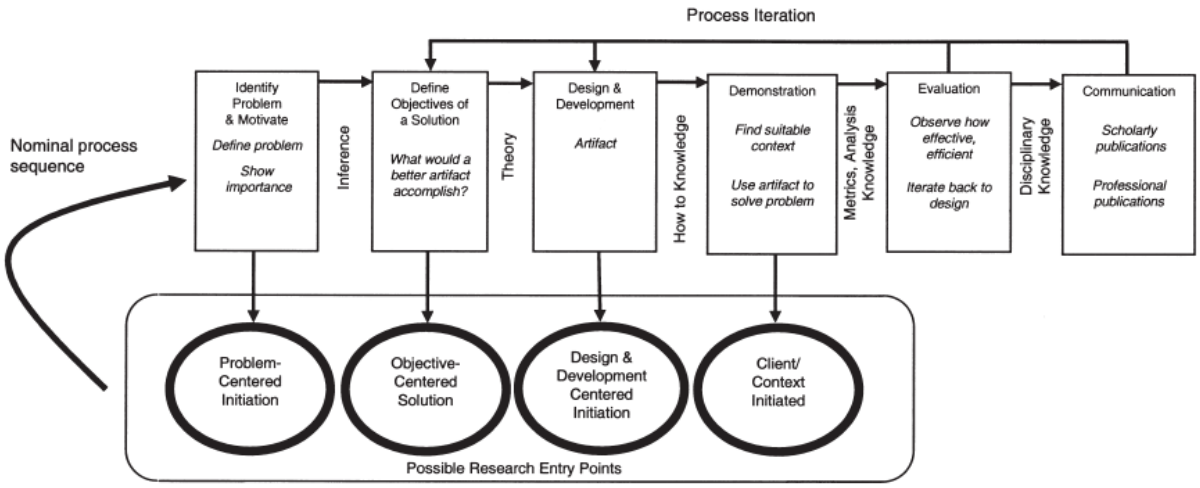

FIGURE 1 DSRM process model (Adapted from Peffers et al., 2007)

Activity 1: Identify Problem and Motivation. Define the problem and why we need a solution for it. Knowledge about the problem and the importance of the solution are the required knowledge for this step.

Activity 2: Define the objectives for a solution. The expected solution will solve a problem which was not addressed before, or the expected solution would be better than the existing solutions. Objectives for the artefact is not necessarily the direct solution of the problem, it can be partial or incremental solution of the identified problem. Knowledge about the problem, existing solutions and their efficacy are required knowledge in this step.

Activity 3: Design and development. Determine the expected functionalities and architecture of the artefact and design the artefact in which the research contribution is embedded (Peffers et al., 2007). Knowledge of theory which supports the design of the solution is the required resources for this activity.

Activity 4: Demonstration. Use the artefact in real environment or simulation or using case study to show that how the designed artefact solves the specified problem.

Activity 5: Evaluation. Evaluate how well the artefact have fulfilled the objectives of the artefact (Peffers et al., 2007). Evaluation methods depend on the artefact and nature of the problem (Hevner et al., 2004). Therefore, applying appropriate methods to evaluate the artefact is important (Hevner et al., 2004). Communicate the evaluation result or go back to redesign to increase the effectiveness of the artefact.

Activity 6. Communication.
Presentation of Design-science research emphasis on how the artefact will be effectively applied in the specific context by individual or organization (Hevner et Al., 2004).

2.5 Application of DSRM in this thesis

Our research will adopt problem-centered approach and will start with activity 1: problem identification and motivation. Because our idea for the research has started with the observation that existing blockchain based certificate systems do not prevent some of the fraud activities which are done by university officials and teachers. Therefore, we need an improved certificate system which will prevent those unaddressed fraudulent activities and make certificate more legitimate.

Activity 1: Identify Problem and Motivation. After literature review on fake diploma and existing blockchain based certificate systems, we have realised that existing blockchain based systems do not prevent fraud activities done by university teachers and officials. Without preventing all the fraud activities in the certificate system, we cannot have a valid degree certificate. More about the identified problems and motivation are described in Problem Identification section.

Activity 2: Define the objectives for a solution. Develop a conceptual model of a blockchain-based study data management system. Then integrate that model into complete certificate system. The conceptual models of the study data management system and complete certificate process model can be used to develop the actual prototype.

Activity 3: Design and development. Conceptual models of the study data system and complete certification system. Literature review in blockchain technology and features sections supports the design of the conceptual model.

Activity 4: Demonstration. There is no practical demonstration or prototype developed during this thesis. Because time and resources to develop such prototype is not possible within this thesis.

Activity 5: Evaluation. The conceptual model and list of fraud activities will be presented to blockchain researchers at blockchain laboratory at university of jyvaskyla for review.

Activity 6. Communication. In the discussion section the thesis contributions will be discussed.

3 FAKE DIPLOMA

Degree fraud has become a global phenomenon because of the rising demand of degree certificate in job market (Brown, 2006). This fake diploma problem is not only in the higher education sector, it exists in from high school to PhD level (Koenig & Devlin, 2012). Fake diploma creates significant damage to the whole society and economy. It directly negatively affects those universities whose degree has been faked, students who intentionally or unintentionally buying the fake degrees and the employers who is hiring that degree holder by having trust on those credentials (Koenig & Devlin, 2012). When counterfeit diploma is produced, it misrepresents the academic institute and as an impact it degrades the reputation of the institute.

A fake diploma or fake degree refers to counterfeit and substandard academic degrees to give impression of real academic achievement (Grolleau et al., 2008). A Degree Mill or Diploma Mill refers to the organization or person who sells or offers academic degrees or certificates for a fee without being proper studies or coursework done by the students (Grolleau et al., 2008). The institutions or the entity who does not have proper accreditation also called as degree mill. Fake degree also refers to the degree which is offered by a university or organization which is non-existent (Grolleau et al., 2008). Sometimes, fake degree holder, mention the degree in his job application or present the certificate which looks like genuine certificate, although he never attended in that institution.

Degree mills are very clever to play with the law of the country, and to make the students and employers fool to believe that their degrees are legitimate. One of the frequently used methods is making a fake work certificate or life experience and then convert that certificate into accredited university degree (Grolleau et al., 2008). In this case, prospective employer only verifies the degree or organisation, but not the fake work certificate which was the base of offering the degree. There are students who intentionally or unknowingly buy fake degree from them to get benefits of having a degree. Sometimes, a person falsely writes a degree qualification in his resume or application without completing or even attending to that degree. Sometimes, for applying in foreign countries, applicant intentionally use misleading translated copy of the real document (Koenig & Devlin, 2012). Fake certificate seller can make copy of almost any kind of certificate of secondary to higher education by using similar paper and special security features used in the original paper certificate ("Sharadeshe jal sonoder," 2015; Lancaster, 2017). So, there are several layers of verification is required to check the legitimacy of the diploma or just trust blindly some parties involved in the diploma process.

Only degree mills or fake institution do not offer fake certificates. There are also several ways that one can attain an illegitimate qualification from an accredited and well-known university. For example, when there are some corrupted

employees in the university registry office, they can be bribed to offer a real certificate without proper coursework done. Sometimes, teachers can be biased and can grade students without proper studies being done. (Brown, 2006)

Due to internet and current technology, modern universities have offered digital information systems for managing grades and certificates, and the online system to check their approved certificate through internet. There is also fear of making fake qualifications. Hackers can hack a university's system and do necessary changes in the data system and change the score of the student (Smith, 2015; Knox, 2017). Hackers can create a cloned university site where fake certificates are verified as real.

Based on national data in US, 6% bachelor's degrees and 35% of associate degrees are fake (Attewell & Domina, 2011). Most of these falsely claimed degree holders have attended the university in question and partly completed the coursework. But for some reason they could not completed the required studies (Attewell & Domina, 2011). Many employers just trust the word of job applicant that he or she has completed the degree. Other imposters buy the certificate from universities who are like diploma mills who sell fake diplomas. Attewell & Domina, (2011) did not describe how the educational imposters are able to get certificates from those universities by completing just part of their degree studies. As there is opportunity to get final certificate without completing the whole degree studies, we assume that there are possibilities where corrupt officials or teachers who support fraudulent activities to issue illegitimate certificate.

Although the fake certificate is a global problem, it is very challenging to find out that how the fraud syndicate or corrupt university officials manage to register or store the fake or illegitimate result in the official information system of an accredited university. I did not find any research paper where it is explained that how corrupt activities are done by the university officials. I have found local news articles, investigative reports by news reporters, and websites in Bangladesh where there is some information about corrupt activities done by university officials.

According to Global Integrity site, there are incidents of fraud activities in admission and grading process in accredited educational institute from primary to university levels where teacher and university officials are involved in corrupt activities in Bangladesh (Islam, 2009). One of the fraud activities is that the teacher is not teaching in class properly and unofficial payment or money is asked from the students to secure the passing grade in test and assignment (Coughlan, 2013; Islam, 2009). In some cases, teachers are biased and grade students without proper studies being done (Brown, 2006).

A website named Buy University Degrees claims that they can give degree certificate from a list of well reputed, accredited, verifiable and legal universities

in UK, US, and Australia ("Degree Overview," 2019). When I contacted through their Instant Chat service and asked them, what kind of difference will be apparent in the certificate achieved by someone who has studied properly and who has bought certificate from you. They replied "Your data will be present in the university database. So, it can be verified". Here also, we find that there could be corrupt officials who store the illegitimate certificate data into university database.

Along with diploma mills and fraud syndicate, there are corrupt personnel at university and education board who are involved in fraud activities to provide illegitimate certificate (Yusuf & Bijoy, 2016). Sometimes, the fraud syndicate have links with corrupt officials and bribes to register better score or grade in the system than the original performance in exam ("Sharadeshe jal sonoder," 2015). Higher the amount of money you pay, you get certificate from more reputed university and the certificate will be registered in the university's information system and so, later there will be no problem verifying the certificate's authenticity (Yusuf & Bijoy, 2016). The universities from which one can buy illegitimate certificates includes accredited private universities and also public university. The university is complying with the government laws and regulations, that's why it's accredited and approved by government. But there are corrupt officials who are involved in this kind of fraud activities which comes into public attention only when it is revealed by law enforcement agency or journalists ("Sharadeshe jal sonoder," 2015).

To provide a certificate without completing minimum required studies done from the accredited university, corrupt official of that university takes several actions to make it genuine (Ekushey Television – ETV, 2014). One method is that if your certificate is a four years degree, they will enrol you in the intake which started four years ago. Your class attendance, exam participation date and grade will be registered as a student as you started four years before. And they will provide you all credentials like university ID card, transcript, certificate. Attewell & Domina (2011) have categorized those students who cannot provide transcripts or other documents besides the certificate as fake. Therefore, fraud officials provide all the documents to make it genuine.

Another method is that fraud officials issue credits or certificates based on life experiences and fake work experience certificates or some fake training certificates (Lancaster, 2017; Ekushey Television – ETV, 2014). Although the officials know that these certificates are fake and student have not done appropriate studies, but because of a fee corrupt officials issue credits or certificates as coursework has been done. Student might take the other remaining courses as he or she likes and complete the required credits and get the final certificate.

Process of verifying the validity of the certificate is a challenging process. This process mostly depends on someone's experience of investigating credentials and trusted network of professionals around the world who have knowledge about verifying documents (Koenig & Devlin, 2012). In one hand, if the diploma is faked outside the legitimate institute or offered by a diploma mill, it is kind of straightforward to recognise the diploma mill with little investigation. But if the certificate is forged from a genuine institute, it is difficult to catch. In an institute, there are several actors, for example, students, teacher, registry office, different information systems who can be involved in producing illegitimate certificates. There is no easy way for outsiders and also sometimes for the insiders to verify each actor's inputs into the diploma process. Usually, when an employer wants to verify the authenticity of the job applicant, they send an email or contact the registry office. If illegitimate grades have been stored in the information system by some corrupt officials, the university registry office will give positive reply about the authenticity of the certificate. In some countries, recommendation letter from a teacher can be biased or based on personal relation. So, the problems are complexed. Therefore, trusting any party involved in the university degree process and checking all the achievements is a challenge for a potential employer and admission office.

By just verifying the transcript or final certificate, there is no assurance that student's certificate or credential is not illegitimate. Even though the certificate is valid against the information system of the university, but there is no assurance that the certificate and grade mentioned in the certificate is achieved by completing appropriate studies.

3.1 Fraudulent activities to make fake diploma

One of our research questions is that what are the ways of making fake diploma or fraudulent activities to gain a fake diploma. Based on the literature review on fake diploma in previous section, we have made a list of ways of making fake diploma. This list will be used to find out that how the existing blockchain based certificate systems addresses these fraudulent activities.

TABLE 1 Fraudulent activities to make fake diploma

	Fraudulent activities to make fake diploma	Actor(s)
Fraudulent Activity 1.	Student adds certificate to his/her CV although (s)he did not attend or complete the degree there (Grolleau et al., 2008).	Student
Fraudulent Activity 2.	Student makes a counterfeit paper copy of the original paper copy (Grolleau et al., 2008) by using similar paper and special security features used in the original paper certificate ("Sharadeshe jal sonoder," 2015; Lancaster, 2017).	Student
Fraudulent Activity 3.	Student buys certificate from non-accredited university or diploma mill (Phillips, 2014).	Student, diploma mill
Fraudulent Activity 4.	Student uses misleading translated copy of the real document (Koenig & Devlin, 2012)	Student
Fraudulent Activity 5.	Student hacks the university grading system and change grades (Smith, 2015; Knox, 2017).	Student
Fraudulent Activity 6.	Student uses work certificate or life experience and then convert that into academic credit (Grolleau et al., 2008) with the support of corrupt officials in accredited university degree (Lancaster, 2017; Ekushey Television – ETV, 2014).	Student, university officials (e.g., secretary)
Fraudulent Activity 7.	Corrupt teacher takes unofficial fee to assure the passing grade without submitting the assignments or required studies done (Coughlan, 2013; Islam, 2009).	Teacher
Fraudulent Activity 8.	Teachers are sometimes biased and grade students higher than their performance (Brown, 2006) such as on exam paper.	Teacher
Fraudulent Activity 9.	Fraud syndicate have links with corrupt officials to store fake certificate data in the university's database (Yusuf & Bijoy, 2016). Certificate seller e.g., "Buy University Degrees" website claims that the information of the certificate will be in the university's database ("Degree Overview," 2019).	university officials (e.g., secretary)
Fraudulent Activity 10.	Corrupt officials change the students' academic information like enrolment date, course completion date and grade in study data management system to prove the validity of the counterfeit certificate (Ekushey Television – ETV, 2014; Mir-Jabbar, 2017).	university officials (e.g., secretary)

4 BLOCKCHAIN TECHNOLOGY

Blockchain refers to the data storage which uses an innovative data structure, and blockchain technology refers to the mechanism or methods, computer programs, architecture, and network that maintain the blockchain (Cao et al., 2017; Mattila, 2016). In other words, Blockchain technology is a new way of storing data in a collective manner in a decentralised and distributed database. The technologies behind blockchain were existed in 1980's and 1990's, but the word blockchain has become popular after Satoshi Nakamoto's whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" in 2008 (Mattila, 2016). Even Satoshi did not use the word 'blockchain' in his paper. He proposed a distributed public ledger system to store the valid transactions into blocks which are cryptographically chained together based on computational proof to remove trust or the need of trusted third parties like financial institutions (Nakamoto, 2008). In our current financial system, financial institutions are working as trusted middle party to make mediation between parties who are willing to make transactions and a central authority is taking care to maintain those transactions.

The CEO of IBM, Ginni Rometty has stated that "What the internet did for communications, blockchain will do for trusted transactions" (Rapier, 2017). Understanding of the potential of blockchain is in very early stage. Marr (2017) has compared the current state of the development of blockchain technology with the internet technology as it was twenty years ago. There are very few practical implementations of blockchain technology now in the world, most of them are in development or experimental stage. Big tech giants like IBM, Microsoft, and Google, big accounting firms like KPMG and Deloitte are investing resources into research on blockchain potential (Bajpai, 2017).

Blockchain is the main technology behind the revolutionary digital currencies like Ethereum, Bitcoin, and Litecoin. The reason for using blockchain behind these cryptocurrencies is that the nature of the design of blockchain technology can replace the need of any intermediary such as bank to ensure trust and security in the transactions. It can verify the transactions, for example, double spending problem, impose the business rules through smart contracts, and store the valid transaction records in cryptographic chain of blocks in decentralised system. (Karame & Androulaki, 2016; Lindman et al., 2017).

4.1 How Blockchain technology works

Blockchain technology is a decentralised and distributed system, it requires a network of individual computers. A blockchain network is basically a network of computers or nodes over the internet who are incentivised for verifying and storing the transactions records into a block, approving and appending the block in the blockchain and storing the current copy of blockchain. A block can be created only when the computer or node in the blockchain network has accomplished the proof-of-work which refers to solving a cryptographic puzzle or problem. Then this node broadcast the newly created block to other nodes in the network. When other nodes in the network find the transactions in the block are valid, then they add the block to their copy of the blockchain. Figure 1 will simply outline how blockchain works.

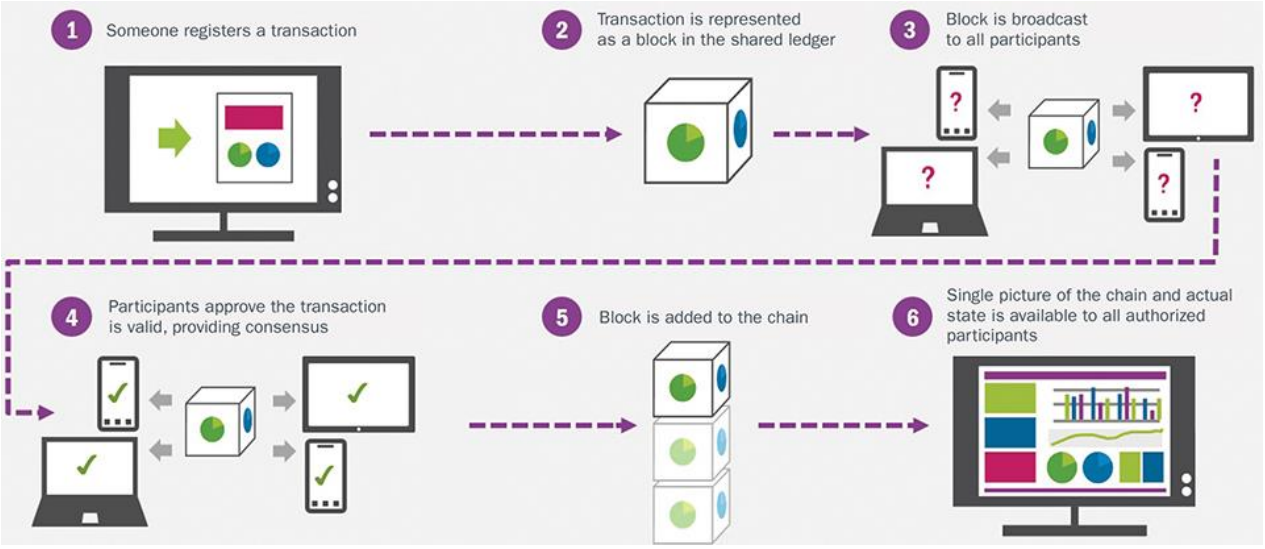

FIGURE 2 How blockchain works (Adapted from Canaday, 2017)

Blocks are chained or grow chronologically and cryptographically. Hash value of the previous block header is stored in the current block with the recent transactions. And this block header's hash value will be stored in the next block with the upcoming transactions (Nakamoto, 2008).

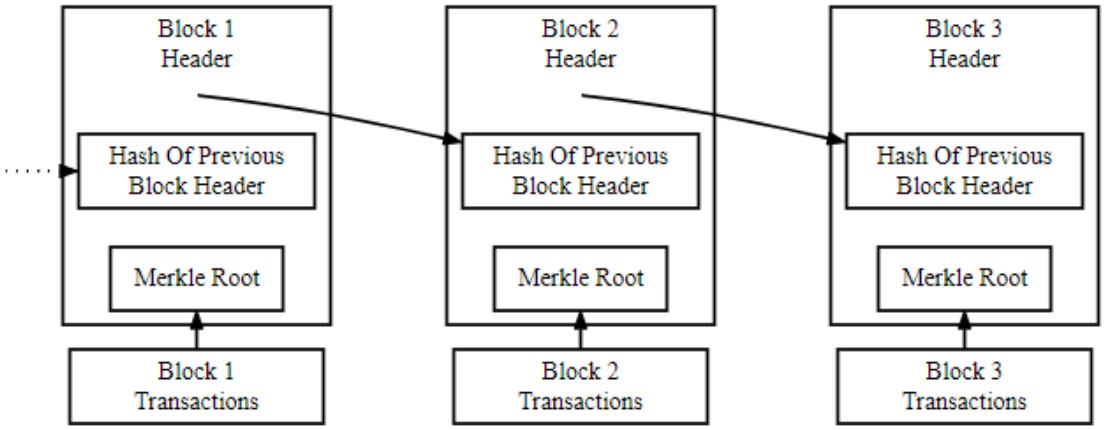

FIGURE 3 Blocks in Bitcoin Blockchain (Adapted from Harding, 2015)

Copy of this chain of blocks or blockchain is stored in distributed system over the network instead of in one server or computer. As it is practically impossible to reverse cryptographic hash and to exceed the computational power of existing honest nodes or computers in the network who are creating these blocks, therefore it is practically impossible to modify any record or transactions stored in the blockchain. So, we can verify the transactions computationally and securely store it in distributed systems over the network, which means that we don't need to trust or use any middle party to verify and store our transactions (Ølnes & Jansen, 2017).

4.2 Blockchain features

Researchers and practitioners from different industries are exploring ways to use blockchain technology to improve the traditional business models. Many industries have already improved their businesses significantly by using the key features of blockchain technology (Hooper, 2018). How these features work and provides benefits is important to understand for solving the fake diploma problem in our research.

4.2.1 Decentralized

In blockchain technology there is no centralized data storage or central authority over data management. In traditional data storage, there is data server and people who has authority to access to the data to manipulate. In blockchain technology, copy of blockchain or blockchain database is stored in all the computers over the blockchain network. If anyone destroy in any way one computer, there thousands of other computers in the network have the copy of the blockchain. If anyone become success to change any data in any block in longest chain of blocks, although which is practically impossible, the other computers in the network will

compare their copy of blockchain with the modified one. If it does not match with the majority or most of the network participants blockchain copy, blockchain network will disagree to take the modified copy of blockchain, and thereby modified copy of blockchain is lost from the network.

4.2.2 Transparent

Transparent information is a growing demand, but with our current economic and digital system it is not completely possible. But with blockchain technology it is possible to create highly transparent decentralised data storage. Any transaction between two users which is stored on the blockchain can be visible to all the users, although users can be anonymous if they don't share their public key. Anyone with access to the blockchain is able to see the data and its history. We know how Google doc works. Each participant is able to see who made what changes on what point of time. Similarly, in blockchain, all participants in the network can see all the changes made to the data (Marr, 2017). The blockchain is constantly being updated and each participant in the network has the access to the valid blockchain. In supply chain, blockchain technology can give the possibility to certify, track, and trace the origin of the goods. And all the information in these steps are transparent and confidently verifiable by the customer (Steiner, 2015).

4.2.3 High availability

The data which is stored in blockchain has very high degree of availability compare to our traditional technology. Because the copy of the blockchain database is stored in the thousands of nodes around the world and the nature of Collective maintenance of the data. Each node in the network works for the security and the integrity of the blockchain database. Even all the nodes in one geographical location lost their copy of blockchain, other nodes from another location will still have the copy of the blockchain. If an application is running on blockchain, for example a smart contract in Ethereum blockchain, it is guaranteed that it will have very high uptime until very long to the future (Buterin, 2015).

4.2.4 Immutable

Data in blockchain is temper proof, once the data is recorded in blockchain it is immutable (Coletti, 2015). If a single node or computer wants to that it will not change the data in blockchain, unless 51% nodes or computers in the blockchain network want to do that (Cao et al., 2017). But in practical, as blockchain network consists of vast number of nodes, it is not possible to change the mind of huge number of nodes to do dishonest tasks.

4.2.5 Anonymity

Blockchain technology gives the ability to make transactions or trade anonymously and does not need to trust each other (Cao et al., 2017). In blockchain, a participant is identified by his or her public key. Your personal information like name, email address, and user IDs are transformed into a cryptographic hash value. And this hash value is like a unique token and stored in blockchain. It is practically impossible to reverse the hash value to get the data. So, even your unique hash value is visible to everybody in blockchain, but you are anonymous to all participants in the blockchain (Perez, 2017). Your identity can be recognised if only you give your personal data that you used to make the hash value.

4.2.6 Trust service provider

Blockchain technology eliminates the need for a trust service provider in IT-enabled relationship. Using the proof-of-work methods blockchain technology create a truthful record (Pilkington 2015). If there is a scenario in digital world where dishonesty can damage the integrity of the information, blockchain technology can become a solution to prevent that dishonest action and keep the integrity of the information. Using blockchain technology, peer to peer transactions can be done completely trust free. Even there is no need to trust the nodes or computer in the blockchain network who are creating the blocks to store the data and storing the blockchain. (Cao et al., 2017; Mattila 2016). The only trust required is that the majority of the nodes in the network will not do some unethical thing in a coordinated manner (Asharaf & Adarsh, 2017).

4.2.7 Smart contract

A Smart contract is an application or computer program which handles to execute the terms of a contract when conditions are met (Tapscott & Tapscott, 2016b ; Szabo, 1996). When a smart contract runs on blockchain, it runs exactly as programmed without any possibility of fraud or third-party interference and downtime ("Build Unstoppable," 2017). In a normal contract, there is need of legal framework or rely on trust to ensure that each party in the contract will behave according to the terms. An intermediary party can cause accidental or intentional misleading behaviour to execute the contract. In smart contract, contractual clauses are transformed into computer script, this script run automatically when the conditions in contracts are met (Christidis & Devetsikiotis, 2016). If the conditions are not met, smart contract will not allow to behave or transact out of the agreement. Therefore, smart contract reduces the need of trusted intermediary or need of trusting any intermediary party to execute the process or tasks programmed in the smart contract.

Smart contract can be used in different situations like escrow agreement, voting, employment agreement, auction where an intermediary distributes the

assets based on the terms in the contract. For example, an escrow agent, as a third party, holds an asset on behalf of two other parties. When two parties fulfil the requirements agreed on the contract, escrow agent transfers the asset from one party to another party (Banton, 2019). So, we have to trust the escrow agent that they will do their job. Smart contract in blockchain can do the same thing as escrow agent. Smart contract holds the transaction until the respected requirements are met from both parties. The major difference is that the transaction and requirements fulfilment proof have to be digitally enabled or on the digital platform. As the smart contract is in blockchain system, nobody can tamper or change the code or execution rule of the contract. It will do its job when contractual requirements are met. So, you don't need to trust the smart contract which makes it trustless or trust-free system.

There are multiple blockchain platforms such as Ethereum, Bitcoin, and Hyperledger Fabric which support smart contract feature. Ethereum is the most widely used platform for creating complex decentralized applications with smart contracts (Mulders, 2018). In this research, when we refer to smart contract, we mean smart contract in Ethereum blockchain. In Ethereum platform, solidity language is used to write smart contracts. In a smart contract the conditions and data of a contract are written using solidity language to make it a software program in Ethereum platform. The format of a smart contract is like an object in an object-oriented language where actions are presented as methods and data is presented as variables. Then the smart contract file is compiled into Ethereum Virtual Machine (EVM) bytecodes. When the smart contract bytecodes or file is deployed into Ethereum blockchain, it has an account or blockchain address and is ready to receive transactions. Based on data state and defined condition, smart contract execute the methods to distribute the asset between parties. Each party involved in a smart contract is identified as a blockchain account. A human or another smart contract can be owner of this account.

5 TRUST-FREE SYSTEM

5.1 What is Trust

Trust is a difficult concept to define and measure to both practitioners and researchers (McKnight et al, 2002). There are diverse and inconsistent definitions of trust in different disciplines and lack of clarity about the dimensions of trust. But everybody agrees that trust is becoming more and more important. Most researchers have defined trust based on their own disciplinary perspective. Psychologist define trust as a tendency to trust others. Sociologist define trust as a component of the institutional environment.

According to Mayer et al. (1995) trust refers to,

> *"the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party."*

Here trustor refers to the party who grants trust, and trustee refers to the party who receives trust (Li et al., 2008). McKnight et al. (2002) have defined initial trust as when trustor and trustee are unfamiliar to each other. Then trustor takes other means to build trust on trustee.

5.2 Trust in IS

In most IS research, trust is discussed about trust on web vendor or virtual team members where trustee and trustor both are human or an organization of human (Li et al., 2008). In recent IS research, trust is discussed about trust on technological artefact or an information system. A trustee is either human or an information system, in both cases trustor behaviourally depend on trustee to do a task. For example, customer trust the online vendor that the given data will not be misused although there is vulnerability and risk of data misuse.

In e-commerce, researchers have defined trust as a belief in an attribute of the trustee or willingness to believe the trustee. Trust-related behaviours are actions that makes trustor dependent on the trustee (vendor) which makes trustor(customer) vulnerable to trustee(vendor) or increase his risk (McKnight et al., 2002). So, when there is trust, there is vulnerability and risk of misconduct.

5.3 Blockchain as a trust-free technology

The revolutionary design of blockchain technology makes it a trust-free technology (Beck et al., 2016). Because the data in blockchain is immutable, transparent and runs on decentralized network. Therefore, if a user(trustor) uses blockchain technology(trustee), and as it has no vulnerability to work otherwise than expected, and user can monitor what is happening to the data, which makes blockchain users free from trust concern.

In trust-based transactions, two strangers make transactions and middleman like bank work as a trustee for two strangers. In trust-free blockchain based transactions two strangers make transactions without any middleman like bank. Blockchain takes care of trust issues and frees us from the necessity to have middleman like bank or to implement a mechanism to convey trust (Beck et al., 2016). And Blockchain itself is trust-free technology, so the complete system becomes trust-free.

The Economist has said the blockchain is the trust machine ("The promise of." 2015). Which means that blockchain technology is not just itself a trust-free technology, but it can also give the possibility to create systems which are trust-free (Beck et al., 2016). Blockchain takes care of trust issues in that system. Most prominent example of such systems is Bitcoin cryptocurrency system. Bitcoin does not require any intermediary or middleman such as central bank to ensure trust, security, and monitor that no parties will do fraudulent activities in transactions. (Nakamoto, 2008). Blockchain takes care of the trust issues, and control, record and monitor each parties' activities during the transaction.

5.4 Trust-based certificate system

Our traditional certificate system is a trust-based system or economy where employer is a trustor, and student and university are trustees. When a student presents his certificate to an employer, if employer accepts the certificate at face value, then employer have trust on the activity of the student that student has presented valid certificate and student did not do any fraudulent activities to produce this certificate. As both student and employer are unfamiliar to each other because of initial trust (McKnight et al., 2002) theory, employer might contact university for the authenticity of the certificate. Here, employer trusts the university for the activity that university teachers and officials have recorded and assessed the students learning outcomes appropriately which is claimed in the certificate without any fraudulent activity. Therefore, in certificate system, there is trust issue or concern because employer does not have the ability to monitor or control the student's activity or university's activity, and vulnerable to the actions of students and university teachers and officials.

5.5 Trust-free certificate system

If there is an information system, where system controls the activities of trustees (student, university officials, teachers) in the certification process based on the agreed upon rules defined in smart contracts and records the activities of the trustees (student, university officials, teachers) in the certification process, then employer don't need to trust the trustees (student, university officials, teachers) for their activities. Rather, employer can monitor those recorded activities and knows what happened which makes the system free from trust concern or trust issues. Now, employer's trust has shifted from (student, university officials, teachers) to the information system for its ability to control and record the activities. Then this system is a trustee. If the system is enabled by blockchain technology which is a trust-free technology(Beck et al., 2016) for its security and ability to record and control the activities, based on the defined rules in smart contracts, of trustees (student, university officials, teachers) in certification process then the certificate system is free from trust issues, in other words trust-free certificate system.

6 EXISTING BLOCKCHAIN-BASED CERTIFICATE SYSTEMS

Blockchain in education is at the peak of Gartner Hype Cycle for Blockchain Business, 2018 and will take 5-10 years to reach plateau (Levy, 2018). There are few institutes who are developing and some already have developed blockchain based certificate systems to issue certificates using blockchain technology, such as, University of Nicosia, National University of La Plata, and Holberton School (Chen et al., 2018; Turkanović et al., 2018). But the descriptions of those projects are not publicly available. We have also searched for Initial Coin Offering (ICO) projects related to certificate system in education industry, if there is any white paper available where the details of such implementation can be found. But we did not find any ICO projects related to degree certificate system. Through google scholar and online search, we have found three projects related to certificate system where they have made the project details publicly available.

Only 'Blockcerts' project, initiated by Massachusetts Institute of Technology (MIT) and Learning Machine, have made their project open-source and shared their learning experiences. Two other projects, "EduCTX" and "Blockchain for Education" have developed prototype of blockchain based certificate systems and published their work as research paper.

6.1 Existing projects

We will review "BlockCerts", "EduCTX" and "Blockchain For Education" projects in details and understand their motivation, system architecture and services. This literature review will support us to find out whether these systems are addressing fraud activities in the certificate system or not.

6.1.1 BlockCerts

MIT Media lab have developed a set of open-source software tools, named Blockcerts, using blockchain technology and Open Badges specification that anyone can use to issue, share, display and verify digital certificates of academic and non-academic achievements (Schmidt, 2017). The system prevents fraud and supports to manage wide variety of achievements or certificates. MIT have already deployed this system to issue certificates for some achievements, for example, for the participants of MIT's Global Entrepreneurship Bootcamp.

Purpose

Authors have noticed that the current credential or certificate system is mostly for recognising the achievements in formal education. There is no standard or widely accepted system for certificating a person's achievements, accomplishments or ability to do something which have been recognised outside of the academy. The Open Badges specification guides to make a standard system for certificating or credentialing different kinds of achievements. But the challenge is how a person will store, manage and share her all different kinds of certificates or badges for her achievements throughout her life.

In the current certificate system to store, verify and validate certificates, we rely on third parties like universities and certificate issuer. University or certificate issuer keeps the registration of our certificates, provides official certificate document, and validate the copy of the certificate when asked. So, the student does not have much control on his/her certificate.

When an employer wants to verify a certificate presented by an applicant, usually it is slow and complicated process for both certificate issuer and employer which is one of the reasons behind the fake certificate issue.

System description

Blockcerts project have created three repositories or tools for their digital certificate system. They are Cert-schema, Cert-issuer and Cert-viewer. Cert-schema describes the necessary data fields or standards for the certificate document, based on the Open Badges specification, to be issued on blockchain by Cert-issuer. Cert-issuer creates the hash of the certificate document and make a bitcoin transaction from issuer's address to student's address and registers the hash of the certificate in Blockchain. Cert-viewer can display and verify the certificates (Nazaré, 2016).

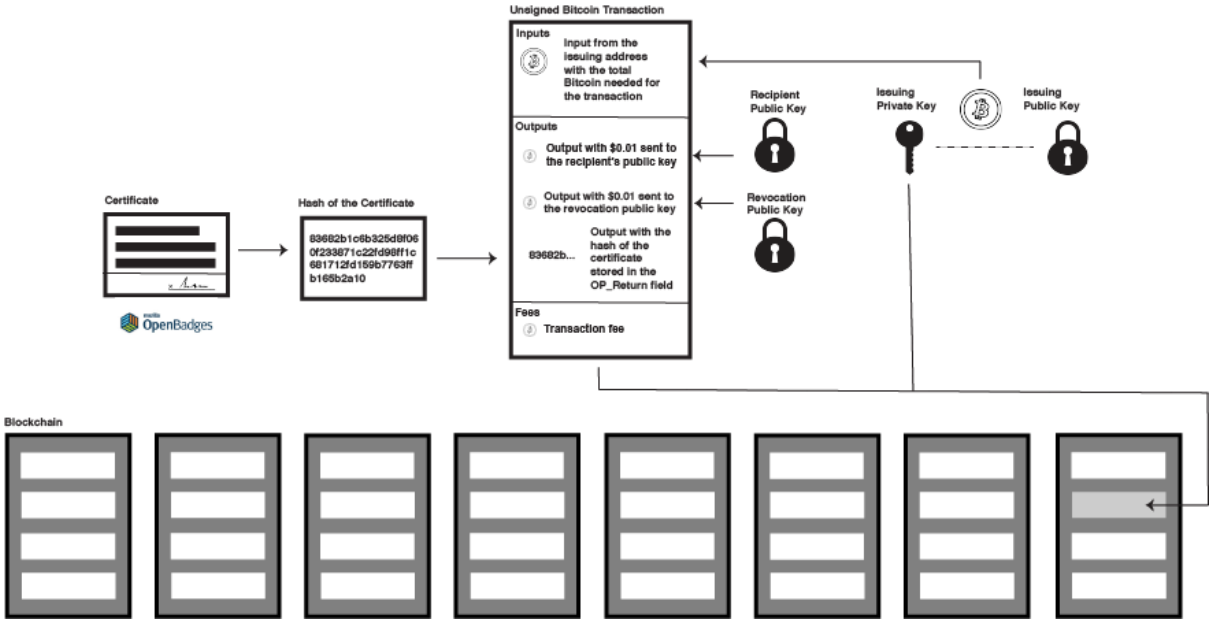

FIGURE 4 Overview of the digital certification architecture. (Adapted from Nazaré, 2016)

The workflow of the system is simple. At first, certificate issuer creates a digital file (digital certificate) with the basic information (e.g., recipient's name, issuer's name, issue date) structured in Open Badges standard. After that, the issuer cryptographically signs the digital file with their private key and append the signature to the digital file itself. In this stage, issuer can give a copy of the digital certificate to its student and student can store the digital copy in any of his digital devices and even can print it on paper. But the certificate is not in blockchain yet. In order to do that, certificate issuer creates a hash of the cryptographically signed digital file created in the previous step and store the hash in Bitcoin blockchain by making a bitcoin transaction using Cert-issuer tool. Now, student can share his digital certificate with employer and data needed to verify the legitimacy of the certificate is stored on the blockchain. Employer can use Blockcert system to verify or compare the hash of the presented digital certificate with the hash in the blockchain to verify the certificate content and check the cryptographic key used to sign the certificate correspond to the issuer's key to verify the issuer. (Schmidt, 2017). The steps happen to verify a certificate in Blockcerts system is depicted in figure 5, the screenshot, which is taken from one of the certificates issued by MIT's Global Entrepreneurship Bootcamp using Blockcerts system.

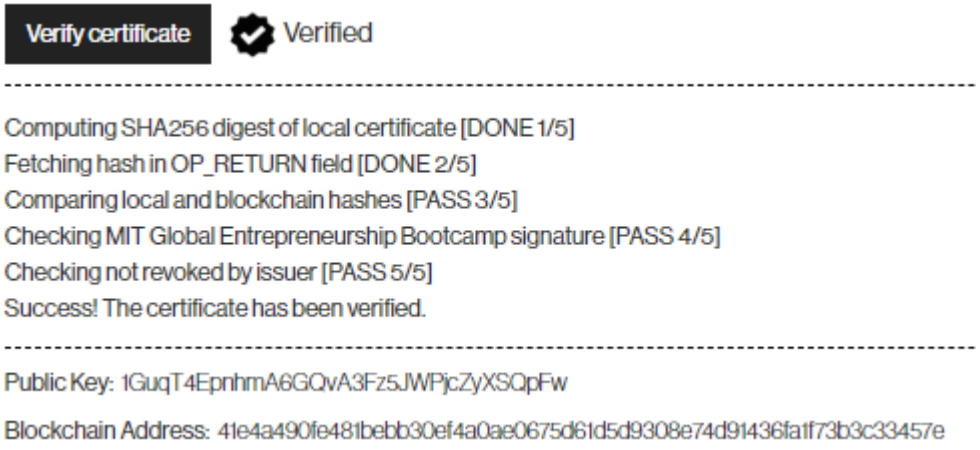

FIGURE 5 Verification steps in Blockcerts system (Adapted from "Digital Certificates," 2016)

The system also supports to register the certificates in Ethereum blockchain ("Verification Process," 2018). Issuing a batch of certificates is more efficient than issuing one certificate per Bitcoin transaction. So, issuer can build a Merkle tree of certificate hashes and store the Merkle root as OP_RETURN field in the Bitcoin Transaction ("Cert-issuer," 2019).

Services

With Blockcerts system, it is possible to store all different kinds of accomplishments and achievements in a decentralized, tamper-proof system permanently. The learners are able to share their certificates without depending on their issuer. When the learner is moving to another country, or the certificate issuer does not

exist anymore, still the learner can share the certificate. The employer independently can verify the authenticity of the presented certificate efficiently and with complete trust (Jagers, 2016).

Advantages

Blockcerts system allows to store all different kinds of accomplishments and achievements in blockchain whereas other projects or systems allow certain type of achievements, for example EduCTX supports only Higher Education accomplishments (Turkanović et al., 2018). Employer can verify the certificate manually or by using Blockcerts system (Nazaré, 2016).

Disadvantages

In Blockcerts system, I did not find anything which describes that how to verify that the certifier or certificate authority is genuine or not a diploma mill even though they are issuing their certificate on blockchain. In this system, employer can verify the authenticity of the certificate but not the authenticity of the certificate authority. Whereas, when the blockchain based certificate system (e.g. EduCTX) consists of network of certificate authorities, existing certificate authorities in the network ensures that only the genuine certificate authority can issue certificates (Turkanović et al., 2018).

6.1.2 EduCTX

Turkanović et al. (2018) have proposed a Blockchain-based global higher education credit platform and ecosystem, named EduCTX. It is based on the concept of European Credit Transfer and Accumulation System (ECTS). EduCTX system is using blockchain technology to create a globally trusted higher education credit assigning and recording system, by complementing the existing ECTS system, to shorten the shortcomings of the existing ECTS processes in organizations ("Welcome to EduCTX," 2019).

Purpose

Authors have recognised several issues in our current higher education credit assigning, recording and presenting system which they have tried to solve with EduCTX platform. In general, students' completed courses are recorded in a certain data structure in the databases hosted in the data centre of the Higher Education Institute (HEI) which raise several issues - interoperability, transparency, inaccessibility, and difficulty to share the records securely.

Students can view their full records in HEI's traditional online system as long they have the authorisation to log in to the system, although they can not share the records to prospective employer or other university directly from the system. Moreover, after completing the studies, student lose the access to the online records system. After that if the student loses his or her certificate, he or she have to apply again for a copy of the certificate which is costly and time consuming process.

When students want to transfer the studies to another HEI in another country, there are differences in language and standards of the recorded data which makes difficult to match and exchange records between HEIs. Because of the similar reasons when students apply for jobs in a foreign country, students have to translate and nostrificate the academic certificates which is a complex and time-consuming process. So, there is a need for standardization globally.

There is ECTS standards for academic credit and grading system for higher education across the European Union and other collaborating European countries. But there is a need to adopt and implement a global standard which requires a globally decentralized, trusted and secure platform.

System description

In the proposed solution, blockchain based EduCTX platform is the base of EduCTX initiative or ecosystem. In EduCTX, students' achievements or ECTS credits are defined as ECTX tokens. There are three types of stakeholders or users of the platform, 1) Student or individual who achieve ECTX tokens 2) Higher Education Institute(HEI), who rewards ECTX tokens 3) Employer or HEI, who wants to verify the presented ECTX tokens (Turkanović et al., 2018).

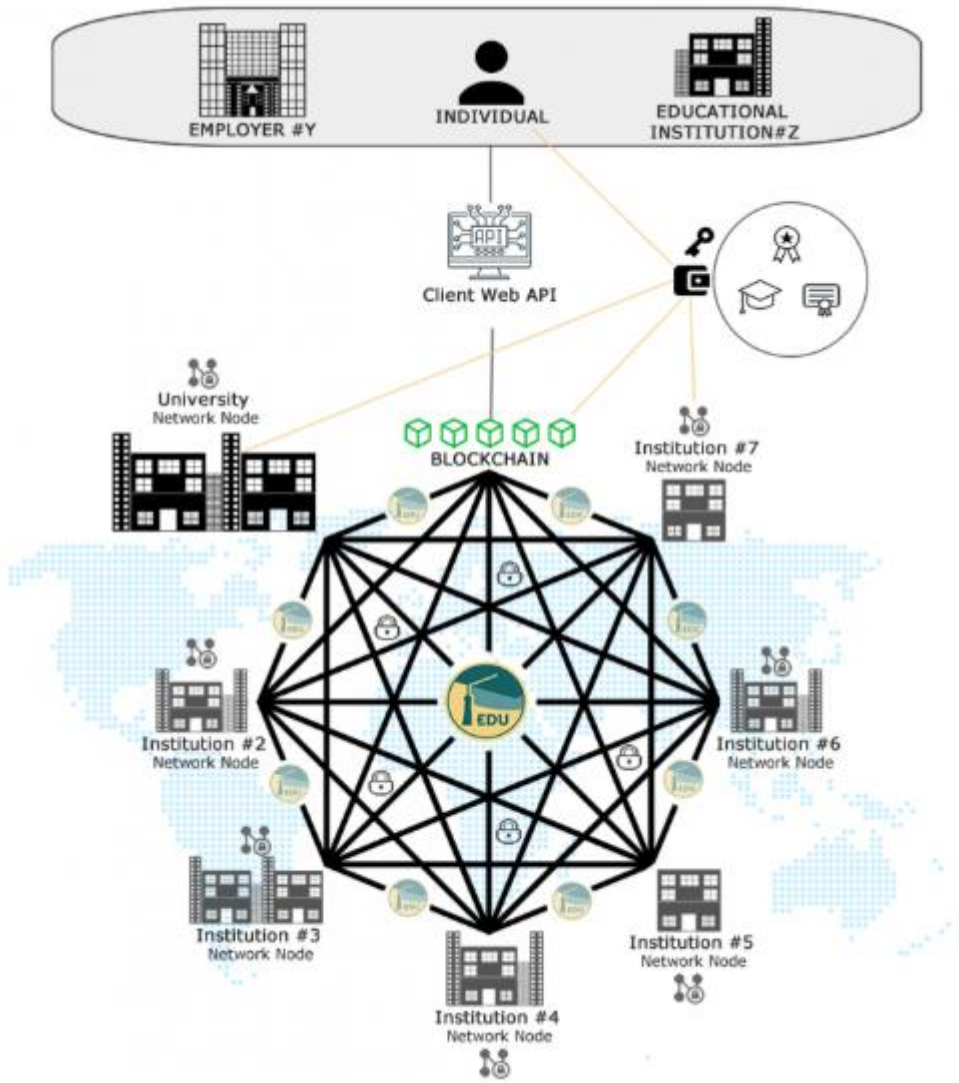

FIGURE 6 A high-level depiction of EduCTX platform. (Adapted from Turkanović et al., 2018)

They have chosen ARK Blockchain mainly because of it's open-sourceness and flexibility to support different programming languages to implement client apps (Turkanović et al., 2018). A Higher Education Institute (HEI) joins the EduCTX blockchain network with the support and recognition of an existing HEI member in the network and creates blockchain wallet and set up a network node. When a new student enrols in a HEI, a 2-2(Keys of HEI and Student) multi-signature wallet is created for the student. When a student successfully completes the course, the results or achieved ECTS credits information are stored in centralized database. Thereafter, professor or administration transfer appropriate number (same amount of ECTS credits) of ECTX tokens from HEI's wallet to student's 2-2 multisignature wallet. Because of the nature of the student's 2-2 multisignature wallet, student is not able to transfer ECTX tokens to other's wallet. When a student wants to present his or her completed courses, he or she sends the block-

chain wallet address and redeem script to prospective employer. Prospective employer use blockchain web API to check and verify student's academic credit achievements or the completed courses (Turkanović et al., 2018).

Services

EduCTX initiative will provide a transparent and globally unified view of the students' achievements or all the completed courses. Those Higher Education Institutes(HEIs) will join the EduCTX platform will be able to store the information of the students' completed courses (ECTX tokens) on blockchain(Tamper-proof distributed ledger system). The platform will also provide the possibility to detect and prevent fraud academic records (Turkanović et al., 2018).

Students can have access to their records or achievements even after the student have completed their studies at the institute, in contrast to traditional system where student can access the online grading system only when they are student of the institute (Turkanović et al., 2018).

Presenting completed courses globally will be easier for students as EduCTX platform will eliminate the language and administrative complications faced in traditional system. Students can easily share the information about their academic records with potential employers, and employers can verify the information in a transparent way without time consuming and manual process of obtaining information (Turkanović et al., 2018).

They are using Delegated Proof of Stake (DPoS) consensus protocol to register the information in the blockchain, which does not require computing power as in Proof-of-Work(PoW) protocol in bitcoin network, and no random peer(HEI) can join the network without the permission of existing peer which makes the network more secure (Turkanović et al., 2018).

There is no transaction fee or coin transfer (Turkanović et al., 2018).

Advantages

EduCTX system records the information of each completed courses, not just the final certificate, in the blockchain.

Disadvantages

They are using centralized database (traditional database, non blockchain system) to initially store the student's exam result. After that administration checks the amount of ECTS corresponding to that exam and student blockchain address from the centralised database, and then appropriate number of EduCTX tokens are transferred to the blockchain wallet address of the student. The process is not

fully automated and there is possibility of making mistakes to transfer wrong amount of EduCTX tokens, and therefore trust or reliability can be compromised. Using smart contract to compare the ECTS credits and transferable amount of EduCTX to make it more reliable and automated.

Although student can share the number of ECTS and corresponding courses, but there is no detail about how student will receive final certificate and which HEI will award it and how it will be presented to employers.

Sometimes it may happen that student does not want to share the full records (all the completed courses) to a prospective employer or sometimes it is unnecessary to share all the completed courses instead of sharing only the relevant completed courses. In EduCTX system, students share their blockchain wallet address and redeem script to prospective employer, so that prospective employer can check and verify student's academic credit achievements or all the completed courses using blockchain web API (Turkanović et al., 2018). In this process, student does not have control if he or she does not want to share some irrelevant courses or achievements.

The system is not flexible in terms of choosing from different credit or achievement recording system. For example, if any HEI wants to adopt some other credit or achievement recording system than for example currently proposed ECTS system. Because ECTX tokens are measured against ECTS in the proposed system.

6.1.3 Blockchain for Education

Gräther et al. (2018) have developed a prototype named Blockchain for Education as a solution for issuing, validating and sharing certificates. Their solution is mainly focused on the certificates issued by the educational institute who are under an accreditation authority.

Purpose

Gräther et al. (2018) want to use the potential of blockchain technology to increase the security and efficiency of the current certificate system. They have discussed about some disadvantages which exist in traditional paper and digital(non-blockchain) certificate system. When a third party or employer wants to verify the paper certificate, it is a time-consuming and expensive process. Certificate authorities need to maintain the registry system to store the certificates for long period. If the registry system is lost or the certification authority is no longer exist, it is a big issue to verify the certificate. If it is a digital certificate, securing the registry system and verification of certificate globally without an open standard for digital signatures are challenging issues. In the area of educational certificates,

there are different fraudulent activities in making fake degree and use of counterfeit certificates. Authors believe that with the support of blockchain technology above mentioned problems can be solved (Gräther et al., 2018).

Authors have said that blockchain technology based system should support three main activities in certificate system – creating and maintaining the identities of the certification authorities, issuing certificates, and verify the certificates by third parties like employer. The system should also support that the students can share the certificates with third parties.

System Description

Authors have identified three user groups in a blockchain based certificate system and elicited requirements or features for each user group. User groups are certification authorities, learners and employers. Certificate authorities are divided into three groups, in hierarchical order, Accreditation authority, Certification authority and Certifier. Certifier can issue and register the certificates on a blockchain and monitor the certificates. Students can share their certificates and have the control to decide which certificate to share with which employer and monitor that what the employers are doing with their certificates, e.g., reading or verifying. Employers can read and verify the certificates in a trustworthy way.

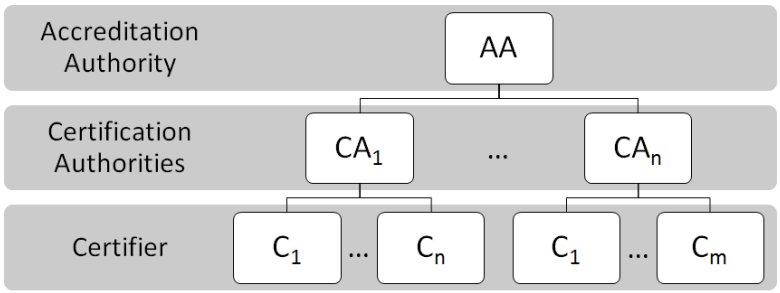

FIGURE 7 Identity hierarchy in Blockchain for Education platform. (Adapted from Gräther et al., 2018)

Blockchain for Education prototype consists of Ethereum blockchain, two smart contracts (IdentityMgmt and CertMgmt), Interplanetary File System (IPFS) and BSCW document management system. IdentityMgmt smart contract is used for managing the public keys of the certificate authorities and CertMgmt smart contract (CertMgmt) is used for managing the hashes or fingerprints of the certificates. IPFS is used for storing the profile information of the certificate authorities publicly. BSCW document management system where information about courses, participants and results are imported from legacy system and from these information certificates are generated. Fingerprint or hash of the certificate with a few attributes (e.g., status, issue date, expiration date) are registered in blockchain.

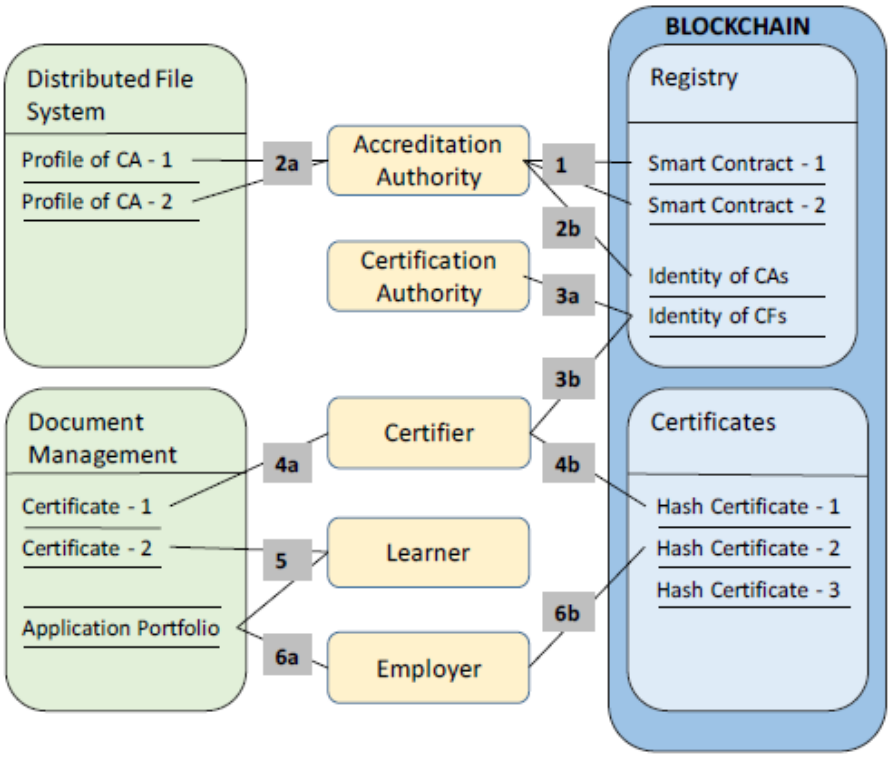

FIGURE 8 Conceptual architecture of Blockchain for Education platform. (Adapted from Gräther et al., 2018)

Accreditation authority store the public profile information of the Certificate authorities in Interplanetary File System (IPFS) and register the IPFS addresses and public keys of the Certificate authorities in IdentityMgmt smart contract's registry. Registered certificate authorities can then register the certifiers (e.g. employee of the institution) in IdentityMgmt smart contract. Registered certifiers can then prepare and sign the certificate and store it on the BSCW document management system. After that the certifier creates the fingerprint(hash) of the certificate from document management system and sends the fingerprint to blockchain using CertMgmt smart contract. When a learner registers in the document management system, he or she can create application portfolios with his/her selected set of certificates and share with potential employers. Employers can verify the presented certificate by entering the SHA256 hash value of the certificate or directly drag and drop the certificate document into the interface of verification service on BSCW document management system. There is also possibility to implement the verification service by the third parties.

Services

Blockchain for Education platform provides a decentralized immutable storage for storing digital certificates. Identities or profile information of the certificate authorities are stored in immutable and public storage. Blockchain for Education uses identity scheme or identity hierarchy and a smart contract for identity management which prevents illegitimate certificate authority or diploma mill to act

or appear like a legitimate certificate authority and so issuing certificates. Using CertMgmt smart contract, certificates authorities can manage (e.g. revoking or renewing) the certificates in the blockchain. BSCW document system allows students to share and monitor their certificates. Third parties, like employers, can verify the certificates easily in a trustworthy way avoiding time consuming and manual process.

Advantages

Blockchain for Education platform maintain the authenticity of the certificate authorities using identity scheme which allows that only accredited university can issue certificate and unaccreted university or diploma mill can not issue certificate. Blockchain for Education platform allows Students and Certificate authorities to automatically monitor the certificates. Certificate authorities can revoke and renew the certificates. Students can monitor what the employers are doing with their certificate, i.e. reading or verifying.

Disadvantages

In the current prototype, every time a certificate is registered in blockchain, it costs. In the future release they have some idea to reduce the cost using some refund technique. They should explore the potential of Merkle tree to register multiple certificates in one transaction to reduce the transaction cost in blockchain platform. Merkle tree supports to register multiple certificate or hashes in one transaction.

Accreditation authority is the single powerful root node in the identity scheme or hierarchy. It is solely accreditation authority's responsibility to ensure or check the authenticity of the certificate authorities before registering their identity to the blockchain. If there is compromise and an illegitimate certificate authority is registered in the platform, illegitimate certificate will be issued, which is unexpected.

6.2 Comparison between existing projects

To understand the existing implementations, system architecture, what problems they have solved and how they have designed the systems, we have made comparison based on the available description of the implementations. We have picked those systems for the comparison which have description of the system publicly. Table 2 can be an overview of the current blockchain based certificate systems and used as a reference to consider the things while designing a blockchain based certificate system.

TABLE 2 Comparison between existing blockchain-based systems

	Blockcerts	**EduCTX**	**Blockchain for Education**
In production or prototype	Production	Proposal/ Prototype	Proposal / Prototype
Key services	- Any certificate authorities can issue certificate - Open for any type of achievements - Open badges standard - Learners can share what do they want to share. - Employer can verify independently or using the Blockcerts system.	Each student will hold a dedicated EduCTX blockchain wallet, where he/she will collect ECTX tokens, i.e. the value of credits assigned by the HEI for his/her completed courses	- Identity Scheme, hierarchy of certificate authorities - Two Smart contracts, one for identity management and another for certificate management - Profile information of certification authorities and certifiers Distributed file system and verifiable through public keys in blockchain.
User groups	Student, Certificate issuer, Employer	Student, Higher Education Institute (HEI), Employer or another HEI	Student, Certificate authorities (accreditor, certificate issuer), Employer
Type of certificate or achievement	Any type of certificate, academic and non-academic; Formal and informal education	Obtained Credits for completed academic achievements, such as ECTS	Certificates from higher education or accredited institutions
Certificate issuer	Any type of institute; academic and non-academic; Formal and informal education.	Higher education institution those who follow ECTS standards and have joined the network.	Accredited institutions or member of an accredited board in the network.
Blockchain platform	Bitcoin, Ethereum	Ark	Ethereum
Use of Smart Contract	No	No	Yes, 2 smart contracts
Blockchain accessibility	Public	private/consortium network	Public
Consensus protocol	Proof of Work	Delegated Proof of Stake (DPoS), no computing power is required, no random peer can join the network	Proof of Stake
Requires transferring coin or fee	Yes, requires transferring minimal amount of bitcoin from issuer's bitcoin address.	Transaction costs are set up to zero, therefore no gas consumption.	Yes, transaction fee.

Components	1) Cert-schema 2) Cert-issuer 3) Cert-viewer	1)Ark Blockchain based EduCTX network, 2) Blockchain client API. 3) Wallets for transferring, storing and sharing Credits or ECTX coins.	1) IPFS Distributed file system for storing public and non-personal profile information 2) Two Smart contracts; IdentityMgmt for registering the public keys of the identities, and CertMgmt for registering the hashes of the certificates in the blockchain 3) Document Management system
Storage	Blockchain	Blockchain	- Blockchain - IPFS - BSCW Document Management System
Certificate representation	Digital certificate	ECTX token	Digital certificate
Stored data in blockchain	Hashes of the certificates (in one batch) combined in a Merkle tree. Merkle root is stored.	- ECTX token (course credit value) - course identification. - Sender (Institute) identity - Receiver (student) identity	- Hash of the certificates - Public keys of certificate authorities using smart contracts - Hash of the IPFS address of Profile information of certificate authorities
Certificate recovery if student's key is lost	Not mentioned	Yes	Not mentioned
Use of IPFS	No	No	Yes, certificate authorities' profiles are stored on the IPFS
Certificate revocation	Yes	Not mentioned	Not possible yet but in plan
System consists of network of Certifiers or a single certifier	Individual certifier	Network of certifiers	Network of certifiers

How to ensure that certifier is accredited	Individual certifier	With the support of an existing HEI/ certifier in the network	Accreditation board registers new certificate authorities in blockchain.
Privacy of personal information	Yes	Yes	Yes
GDPR	Obliged. Hash of the certificate in blockchain.	Obliged. Student's information is stored anonymously.	Obliged, no personal information stored in blockchain but the address of IPFS block.
Key Challenges	- Costly - For non-technical users, creating public-private keys for authentication process - Certificate revoking method	- The more nodes or HEIs in the network, it will reduce the security risk.	- Costly - If Private key of accreditation authority is compromised who is the single powerful root node. - Accreditation authority's responsibility to ensure the legitimacy of certificate authorities.
Future goals	- Track the views of certificate and creating Value out of it - Right to curation (which part of the history to share) - Wallet to hold credentials similar to wallet to hold and transact bitcoin	- Use Smart contracts - After finishing course, students will get tokens from the course address.	- Multi-signature scheme instead of single root private key of accreditation authority - Learner pay to authority and in refund transaction, certificate is submitted to blockchain

6.3 **Discussion**

Reviews on existing blockchain based certificate systems provide good knowledge about the current development status of the blockchain based certificate systems around the world. Although some of them are still in prototype and some have already deployed in real life and issued the certificates with their system.

Although these systems' goals or expectations are to same direction to make a digital certificate platform or ecosystem to make the certificate system more secure and efficient, but they have different approaches and focusses on issues to solve. In 'Comparison table' section, I have tried gather those similarities and dissimilarities.

Some projects or systems are storing only the fingerprint or hash of the certificate and some(Blockchain for Education) are storing some additional data for example the certificate authority or issuer's fingerprint in blockchain to verify the certificate issuer.

EduCTX and Blockchain for Education systems are supporting only Higher education certificates or credentials, and Blockcerts provides the ability to store all kinds of credentials or certificate- academic and non-academic.

Different systems are using different blockchains (Bitcoin, Ethereum, Ark) based on the design or requirements of the systems and features provided by the blockchain. Blockcerts support both Bitcoin and Ehtereum, BFE is using Ethereum, EduCTX is using Ark.

6.4 Challenges

In the current blockchain based systems, officials manually input or imports the data to prepare or collect the certificate data from legacy system. Before issuing final certificate in blockchain, officials can make mistake or compromise the integrity. Because when final certificate is issued on blockchain, it is important that the data in the certificate are same as teacher graded or in the legacy system. There can be multi-signature approval mechanism or use smart contract which ensures that the data in the certificate and source data are same before issuing certificate.

How to check the validity of the certifiers or certification authorities. How to prevent or detect that the certifier or certification authorities are not fake or illegitimate. Usability of the web API or interface or the process for certifiers, learners and employers to check the authenticity of the certificate. Students ability to control to share only the relevant certificates to an employer or a third party. Not everything what is in students blockchain address or wallet.

In blockchain based system, storing personal blockchain wallet data (public and private keys) safely and how to recover if stolen or lost is a critical issue (need reference). In EduCTX system, if Student loses his or her blockchain wallet data, student can apply again to his/her home HEI to get back his EduCTX tokens to his/her new wallet. There are also measures how to protect form being stolen (Turkanović et al., 2018).

6.5 Addressing fraud activities with existing projects

Before we develop our own solution to address the fraud activities in certificate system, we want review which of the fraud activities are addressed by the existing blockchain based certificate systems.

Existing blockchain based certificate systems have one thing in common that they issue the final certificate on blockchain and there are services for sharing and verifying the final certificates. But they don't use blockchain technology for recording and controlling transactions by teachers and officials, and they store study data in traditional database. Table 3 shows which of the fraud activities are addressed or not addressed by the existing solutions and reasons for that.

Fraudulent activities 1 to 3 are addressed by the existing solutions. Fraud activity 4 is out of the scope of certificate system. Fraud activities 5 to 10 are not addressed by the existing solutions.

TABLE 3 Addressing fraudulent activities with existing blockchain-based certificate systems

Fraudulent activities	**BlockCerts**	**EduCTX**	**Blockchain for Education**
Fraudulent Activity 1.	Addressed - Degree certificate is stored in blockchain. Certificate can be shared and verified using blockchain.	Addressed - Completed course credits are stored in blockchain. Certificate can be shared and verified using blockchain.	Addressed - Degree certificate is stored in blockchain. Certificate can be shared and verified using blockchain.
Fraudulent Activity 2.	Addressed - Digital certificate in blockchain which can be shared and verified using blockchain technology.	Addressed - Digital certificate in blockchain which can be shared and verified using blockchain technology.	Addressed - Digital certificate in blockchain which can be shared and verified using blockchain technology.
Fraudulent Activity 3.	Unaddressed - Any institute can issue certificate.	Addressed - Diploma mill can not join the proposed ecosystem to issue certificate.	Addressed - Diploma mill can not join the proposed ecosystem to issue certificate.
Fraudulent Activity 4.	Not within the scope of the certificate system.	Not within the scope of the certificate system.	Not within the scope of the certificate system.

Fraudulent Activity 5.	Unaddressed - Internal study data is stored traditional centralized server.	Addressed - Credits and grades are stored in block-chain system.	Unaddressed - Internal study data is stored in traditional centralized server.
Fraudulent Activity 6.	Unaddressed - Does not control or monitor based on what credit is awarded.	Unaddressed - Does not control or monitor based on what credit is awarded.	Unaddressed - Does not control or monitor based on what credit is awarded.
Fraudulent Activity 7.	Unaddressed - Does not control or record whether the assignment is submitted or not.	Unaddressed - Does not control or record whether the assignment is submitted or not.	Unaddressed - Does not control or record whether the assignment is submitted or not.
Fraudulent Activity 8.	Unaddressed - Does not control or record the exam paper.	Unaddressed - Does not control or record the exam paper.	Unaddressed - Does not control or record the exam paper.
Fraudulent Activity 9.	Unaddressed - Internal study data is stored in mutable and traditional database.	Unaddressed - Internal study data is partly stored mutable and traditional database.	Unaddressed - Internal study data is stored in mutable and traditional database.
Fraudulent Activity 10.	Unaddressed - Student's academic information or study data is stored in mutable and traditional database which is not transparent.	Unaddressed - Student's academic information or study data is stored in mutable and traditional database which is not transparent.	Unaddressed - Student's academic information or study data is stored in mutable and traditional database which is not transparent.

7 PROBLEM IDENTIFICATION

In "Fake diploma" Section, we have discussed about the fake diploma problem and created a list of ways of making fake diploma or fraudulent activities to make fake diploma. we have found that university officials and teachers are also involved in fraud activities in some cases. After reviewing existing blockchain based certificate systems, we have found that fraudulent activities 5 to 10 are not addressed in the existing systems. Most of them have focused on issuing and verifying the final certificate in the blockchain. They have mechanism to remove the need to trust on student but don't have mechanism to remove trust on university officials and teachers. They did not address the fraud activities which can happen before preparing the final certificate like grading process and recording the grades in the system based upon what the final certificate is issued. The fraud activities, as in table 4, which are not addressed by the existing blockchain based certificate systems, our proposed system will focus on to solve those problems.

TABLE 4 Fraud activities not addressed by existing systems

	List of fraud activities not addressed by existing blockchain based systems	**Actors**
Fraudulent Activity 5.	Student hacks the university grading system and change grades (Smith, 2015; Knox, 2017).	Student
Fraudulent Activity 6.	Student uses work certificate or life experience and then convert that into academic credit (Grolleau et al., 2008) with the support of corrupt officials in accredited university degree (Lancaster, 2017; Ekushey Television – ETV, 2014).	Student, university officials (e.g., secretary)
Fraudulent Activity 7.	Corrupt teacher takes unofficial fee to assure the passing grade without submitting the assignments or required studies done (Coughlan, 2013; Islam, 2009).	Teacher
Fraudulent Activity 8.	Teachers are sometimes biased and grade students inappropriately on their performance (Brown, 2006) such as exam paper.	Teacher
Fraudulent Activity 9.	Fraud syndicate have links with corrupt officials to store fake certificate data in the university's database (Yusuf & Bijoy, 2016). Certificate seller e.g., "Buy University Degrees" website claims that the information of the certificate will be in the university's database ("Degree Overview," 2019).	university officials (e.g., secretary)
Fraudulent Activity 10.	Corrupt officials change the students' academic information like enrolment date, course completion date and grade in study data management system to prove the validity of the counterfeit certificate (Ekushey Television – ETV, 2014; Mir-Jabbar, 2017).	university officials (e.g., secretary)

Even though the university is accredited or approved by the government, fraud officials or corrupt teachers inside the institute can contribute to issue certificate without appropriate studies being done by the student. Fraud activities can happen by any middlemen, e.g., university officials and teachers, in the certificate process. To ensure a valid education certificate we have to prevent the fraud activities in the whole certificate process, issuing and verifying the final certificate on blockchain is not enough. If we can prevent the fraud activities which are done by corrupt officials or teachers to register illegitimate academic achievements or credits based upon what the final certificate is issued then the certificate will have more credibility.

Blockchain stores the interactions or transactions in immutable and traceable storage and provides the mechanism to replace trust on middlemen. If we can store and trace the coursework, accomplishments, attendance in an immutable and easily verifiable information system, and replace the role of middlemen using blockchain, certificate will be more authentic.

Based on the reviews on existing blockchain based systems, we see that the current blockchain based certificate systems are issuing only the final certificate on the blockchain. But the information based on what the final certificate is prepared are using traditional web app and database to manage and store information about courses, degree programmes, student's personal data, grades. figure 9 shows that university's internal systems for study data management like managing course requirements, study modules, participants, grading, degree requirements are using traditional web app and traditional database.

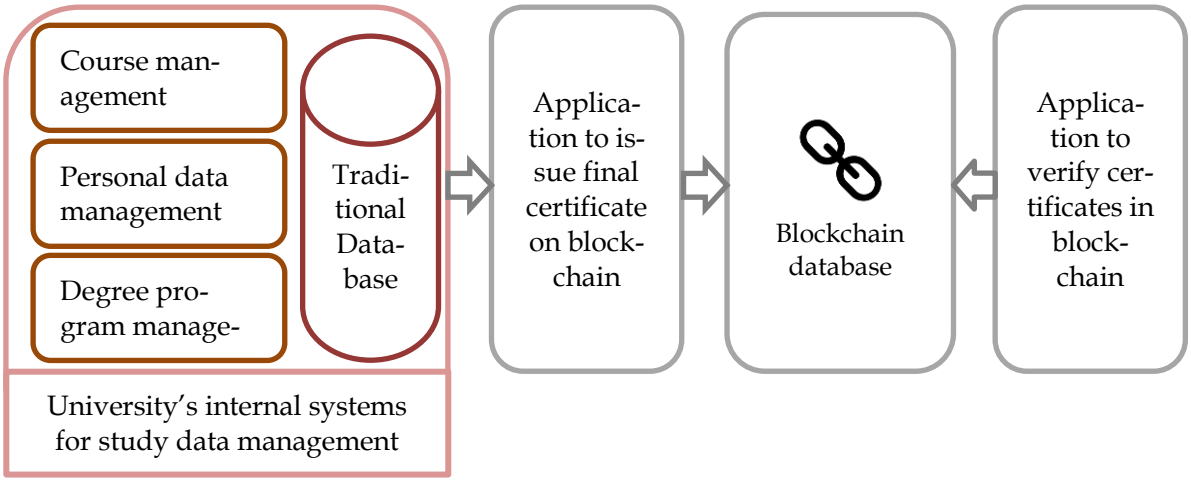

FIGURE 9 Certificate process in existing blockchain based systems

8 OBJECTIVES OF THE SOLUTION

The objective is to develop a conceptual model of a blockchain based certificate system which will prevent the fraud activities in certification process which are not addressed by the existing blockchain based systems. More specifically it will prevent fraud activities by the university officials and teachers by removing the trust on those middlemen who are involved in the certificate process. Using blockchain technology, it will develop a conceptual model of the study data system which is used by university officials, teachers and students to store study data such as student's academic and grading information. The new solution will prevent fraud activities in the whole certificate process. The conceptual models of the study data management system and complete certificate process model can be used to develop the actual prototype.

9 DESIGN AND DEVELOPMENT

We will develop a conceptual model of the blockchain based certificate system which will address the fraud activities which are not addressed by existing blockchain based certificate systems. Final diploma certificates are prepared based on the study data system which records students individual course completion, course description, degree programme etc. The conceptual model of the system will not focus on what already existing blockchain based system have accomplished like issuing and verifying final certificate on blockchain. This conceptual model will only focus on improving the current study data system. The current study data system consists of traditional web application and database in centralized server. Our goal is to design a blockchain based decentralized application which will be able to prevent fraud activities done by officials and teachers inside an accredited university.

9.1 Traditional web application and blockchain based application

There is a critical difference between decentralized applications (DApp) and traditional web applications. Traditional web applications run on centralized server or system whereas decentralized applications run on decentralized systems like Ethereum blockchain system. This difference makes the decentralized app superior to solve the identified problems over currently used centralized system at university. Front-end technologies could be same in both types of applications, but the backend of decentralized apps will use the technologies available in Ethereum decentralized system.

Traditional information systems or web applications for grading, keeping students' records, and course information at university, typically consists of front-end, backend application and database. Backend application and database stay in centralized server. Frontend interacts with backend app or business logic which allows to do the necessary changes in database.

FIGURE 10 Traditional web app

Ethereum blockchain based decentralized applications consists of also frontend and backend. In Ethereum blockchain platform, backend application or business logic refers to smart contract which is deployed on blockchain and also the data is stored in blockchain. The frontend can interact directly with Smart

contracts and each transaction in smart contract or data changes are stored in blockchain. A transaction does not mean only transferring blockchain currency or asset from one account to other, but also when data changes in smart contract or blockchain database also called a transaction. ("Decentralized applications," 2019).

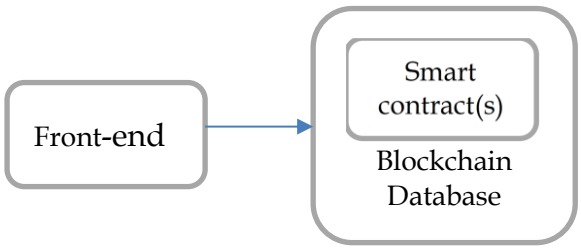

FIGURE 11 Decentralized app on Ethereum blockchain

The proposed solution will replace the backend of the traditional information system of university from centralized server to Ethereum blockchain platform and will use the features of Ethereum blockchain platform to solve many of the fake diploma problems identified in this research.

When the current application or information system runs on a decentralized blockchain system it gets the advantages of decentralized system over the application which runs on centralized system.

9.2 Possible blockchain solution for the problems

Our goal is to use blockchain features to address the fraudulent activities. We will discuss each fraudulent activity and how the possible blockchain features can address that fraudulent activity.

Solution for Fraudulent Activity 5:

For Addressing "Student hacks the university grading system and change grade (Smith, 2015; Knox, 2017)" we need an immutable or hack proof database system. Blockchain database is immutable which means that once the grade has been registered, it cannot be changed. Every transactions or data change happen to blockchain they are recorded in the blockchain database. Therefore, if we store the grades in blockchain database instead of traditional database, the hackers will not be able to change the grade.

Solution for Fraudulent Activity 6:

For addressing "Student uses work certificate or life experience and then convert that into academic credit (Grolleau et al., 2008) with the support of corrupt officials in accredited university degree (Lancaster, 2017; Ekushey Television – ETV, 2014)", first we have to check at the course completion methods predefined in the course management system. If work experience certificate is not accepted as a method to complete the course, officials should not be able to register the grade for that course. Instead of trusting the officials, if we create a smart contract for course management which will have the course completion methods or conditions and smart contract will check whether the work certificate is a valid method to award credits for it or not. If work certificate is a valid method to complete the course, smart contract will require proof of having a work certificate. University officials will store the digital copy of the certificate in Interplanetary File System (IPFS) and store the reference of the file in smart contract which can be verified later if someone wants. IPFS is a peer-to-peer distributed file system with no single point of failure, and nodes do not need to trust each other. Stored files are tamper-proof and get content-addressed hyperlinks (Benet, 2014).

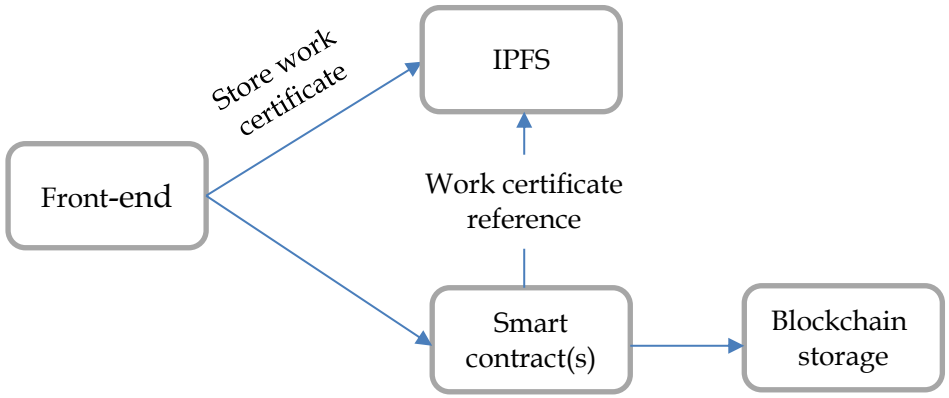

FIGURE 12 Registering course grade based on work experience certificate

Solution for Fraudulent Activity 7 and Fraudulent Activity 8:

"Corrupt teacher takes unofficial fee to assure the passing grade without submitting the assignments or required studies done (Coughlan, 2013; Islam, 2009)." and "Teachers are sometimes biased and grade students higher than their performance (Brown, 2006) such as on exam paper." are kind of similar type of fraud activity. In both cases, teachers are trusted for checking that students have completed his assignments and passed the exam. But there can be risk of making error. We can not completely replace trust on teacher as checking the exam answer and assignment requires human involvement. But we can minimize the risk of making error to check that whether the student have submitted his assignments and passed the exam. When the assignment is submitted from students blockchain account, smart contract will record that student has submitted the assignments. When teacher has evaluated the assignments and the score is registered through smart contract in blockchain, only after that smart contract will

allow to award the credits for that course or record the course completion in the blockchain database.

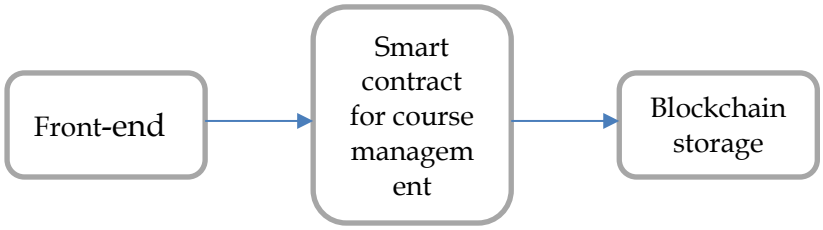

FIGURE 13 Registering course grade using smart contract

Solution for Fraudulent Activity 9 and Fraudulent Activity 10:

To address the corrupt activities done by corrupt officials, for example, storing fake certificate data in the university's database, and registering students' illegitimate academic information like enrolment date, degree programme, and study modules in study information management system to prove the validity of the counterfeit certificate (Ekushey Television – ETV, 2014; Yusuf & Bijoy, 2016), one smart contract to register student personal information and another smart contract to process student's degree application form. Only the authorize blockchain account can execute the smart contracts where the student data and course data are stored. As blockchain transactions are traceable, we can trace who changed what and what point of time.

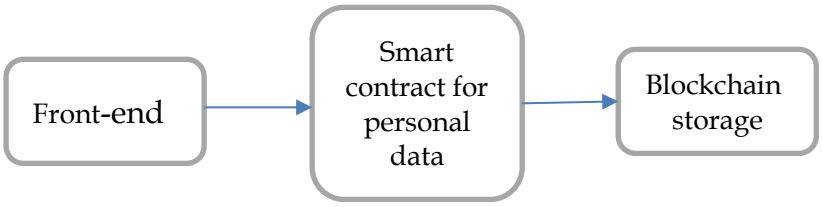

FIGURE 14 Registering personal data using smart contract

9.3 Design of smart contracts

Designing appropriate smart contracts for storing information like student's personal data and study modules in blockchain and executing tasks like submitting assignments, exam answers, assessing course completion, registering grade depends on the individual university's environment. Because study information and workflow vary from university to university. Based on the data and conditions set in the smart contract, smart contract will execute the tasks or transactions.

In our conceptual model, we have included four smart contracts (table 5) which can accommodate the most common and simple use cases that a university has. Based on the need of the university, they can add more smart contracts or include the information and tasks in these contracts.

TABLE 5 Smart contracts in study data management DApp

Smart contracts	**Description**
Course	Store data about the course (e.g. requirements for the course completion, credits) and register grade when students meet the requirements.
Degree programme	Store degree information and award degree when students meet the degree requirements
Student	Store student's personal data
Identity management	Store and authorize users to execute other smart contracts

These smart contracts will not store large data or long textual description, e.g., course description, degree programme objectives, but only what is required to execute the tasks or transactions in smart contract. In smart contracts, objects like other smart contracts, participants in the contracts are identified with their own blockchain address.

When a new course is launched there will be a new "Course" smart contract designed and deployed in blockchain for that course, and this contract will get its blockchain address. The Course contract will have data about course completion requirements, credits, participated students Ids or blockchain address.

"Degree Program" smart contract will store the address of each course contract required to complete the degree, enrolled students' addresses. When an enrolled student will have completed all the required courses, degree award function will be automatically executed without any intervention from the officials, and degree completion status will be stored in blockchain. Each time there will be transactions or data changes in the smart contracts it will be recorded in the blockchain.

"Student" smart contract will store data about student's personal information like his degree programme, enrolment year. For each student, one contract will be deployed.

"Identity Management" smart contract is a multisignature smart contract. To execute this smart contract, multiple officials and teachers' signature will be required. The reason for extra security for this smart contract is that it will register the users of the system and delegate who can execute other smart contracts and make changes data on blockchain.

9.4 Proposed blockchain-based study data system

The proposed study data system consists of blockchain, smart contracts and Interplanetary File System (IPFS) instead of traditional database and backend app running on centralized server. Our objective was to design a conceptual model for blockchain based study data system and reduce the trust on teachers and university officials or secretary. As the study data is the basis of final degree certificate, we want to prevent the fraud activities in study data system. We have designed the conceptual model of the blockchain decentralized app and used smart contracts to store and check the requirements to execute tasks like grading. Properly designed smart contracts will reduce the trust on actors (teachers, secretary) in the university study data system and each transaction or data changes will be recorded in a transparent and immutable storage. IPFS will be used for storing documents, like work certificate, assignment etc, which are required by the smart contract. When student will fulfil the requirements defined in the course contract, student will be awarded the credits.

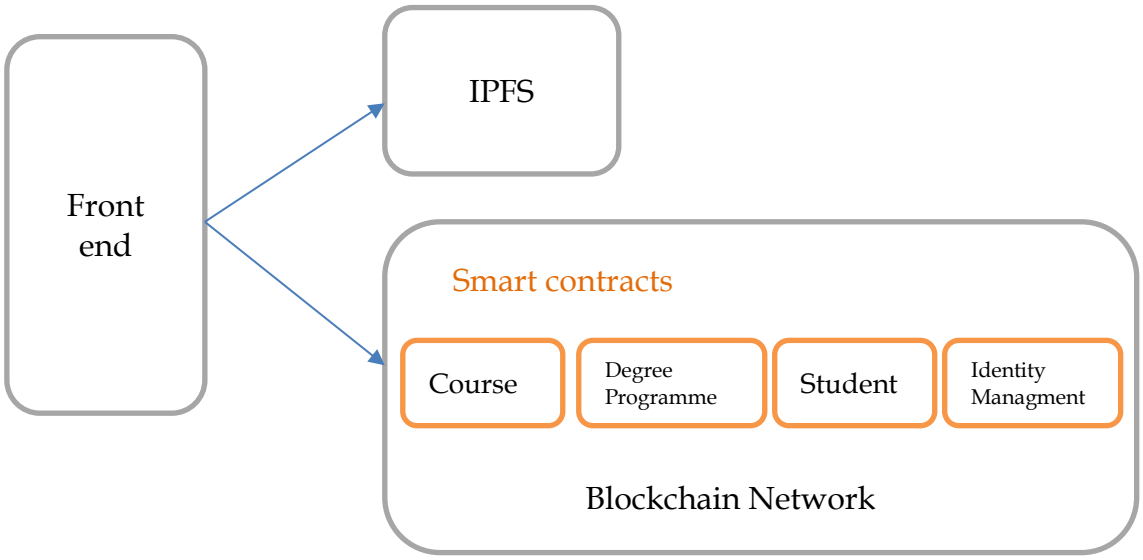

FIGURE 15 Conceptual model of the blockchain based study data management system

9.5 Proposed overall certificate system

Overall certificate system consists of four components as in figure 16. First component is the Ethereum blockchain based study data management system, which we have proposed, figure 15, in the previous section, which will store the study data records in blockchain using smart contracts. As the data is stored using smart contracts and in blockchain, system is more preventive to fraud activities. The second component is the application or front-end app to read the certificate data from blockchain based study data system and prepare the final certificate for displaying and sharing with employers or others. In this app, student can

choose what to share with employers, whether the whole academic achievements or part of the achievements and based on that student can retrieve data from the study data system. The third component is optional. The digital copy of the final certificate can be issued or stored in another blockchain network than university's study data system. Fourth component is the application to give verification service to employers.

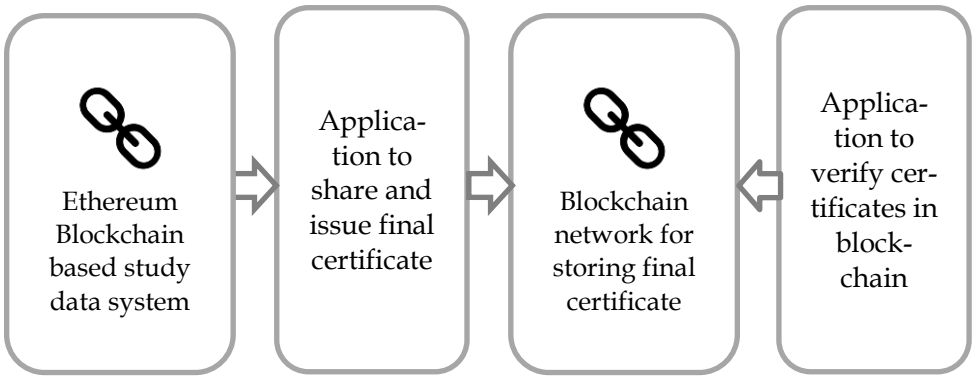

FIGURE 16 Conceptual model of the complete certificate system

10 DEMONSTRATION

Demonstration requires to use the artefact in experimentation to solve one or more of the identified problems (Peffers et al., 2017). Our artefact is a conceptual model or architecture which will guide to develop a blockchain based certificate system to address fraudulent activities in the certificate process. Developing a conceptual model of an application is the first step in designing the system.

To develop a prototype or proof of concept for a certificate system requires lot of effort. During this thesis, it is not possible to develop a prototype. Moreover, it will require a lot of collaboration with a university to develop and experiment such a system. That's why there is no practical demonstration done during this thesis. But there was a review on the conceptual model by the researchers at Blockchain laboratory at our university which has been described in evaluation section.

11 EVALUATION

The evaluation activity compares the objectives of the solution to actual observed results in the use of the artefact (Peffers et al, 2007). This evaluation can take different strategies based on the nature of the artefact (Peffers et al, 2007). Objective of our designed artefact is that it will address or prevent the identified fraudulent activities and support to develop actual prototype. We presented fraudulent activities 5 to 10 which are not addressed by existing blockchain based systems and conceptual model documents to the researchers at Blockchain Laboratory at University of Jyvaskyla.

In the beginning of the discussion, first we explained the model and we went through the fraudulent activities one by one. Blockchain Laboratory researchers gave opinion that whether the new system will address the identified fraudulent activities. In table 6, the summary of their comments on each fraudulent activity is described. They appreciated the concept as it will be a smart system. Fraudulent activities 5, 6, and 7 can be prevented. For fraudulent activity 8, it requires teachers to evaluate the exam paper or performance of the students which blockchain cannot control. If there is computer gradable exam and stored in blockchain then these fraudulent activities can be prevented. As there is human involved in checking the exam answers, there is always risk of making mistakes and frauds by human being. We have to wait until artificial intelligence is developed enough to assess the exam answers or assignments. For fraudulent activities 9 and 10, current design will provide some prevention but using multisignature feature will give stronger protection of the data. As a suggestion for improving the system, making exams computer-gradable, storing exam answers in blockchain, using multi-signatures smart contract could possibly make the probability of fraud less than the usual.

We also asked about to review the appropriateness and effectiveness of the model, and feasibility to develop such system. They have appreciated the figures to explain the conceptual model as it makes easy to understand the concept. And the figures are technically correct from blockchain technology perspective. It can be used as reference to communicate and design the actual prototype.

TABLE 6 Addressing fraudulent activities with the proposed solution

	Evaluator's comments	Description
Fraudulent Activity 5.	Addressed	As the grades will be stored in blockchain, it is not possible to hack or change the grade once it is stored in blockchain.
Fraudulent Activity 6.	Addressed	If a smart contract is used, it will force officials to give the cryptographic hash of the work certificate in IPFS distributed file system as a proof to award the course credits which will allow employer later to check the work certificate if needed.

Fraudulent Activity 7.	Addressed.	If a smart contract is used, it will not allow to grade until the assignment submission is done through smart contract.
Fraudulent Activity 8.	Addressed partly.	If assessment by a human teacher is must, block-chain cannot control personal judgment. Making exams computer-gradable or student-gradable could possibly make the probability of fraud less than the usual. Relying on Artificial in-telligence and evaluation by peers.
Fraudulent Activity 9.	Addressed, but can be improved	As the data is stored in blockchain and study data entry is controlled by smart contract, only from the delegated blockchain address smart contract can be executed and change the data. With multisignature, several teachers / faculty members need to sign the transactions, so a single fraudster cannot succeed with his plans.
Fraudulent Activity 10.	Addressed, but can be improved	Every transaction is timestamped and transparent. With multisignature, several teachers / faculty members need to sign the transactions, so a single fraudster cannot succeed with his plans.

12 DISCUSSION

Our first research sub-question was to find out the fraudulent activities in our traditional certificate system. Student is the one who is generally produce fake certificate by different means such as making counterfeit paper copy of the original certificate, hacking the university's study data system, and making wrong translated copy of the certificate. We have found that not only students who make fake certificate but also university teachers and officials contribute to make fake certificate. Unscrupulous teachers take bribe and sometimes biased when assessing the students course work, and award credits without proper studies being done by students. Dishonest university officials take bribe and change the academic records of the students and award final certificate.

Second research sub-question was to find out whether the existing blockchain-based certificate systems address all these fraudulent activities done by students, teachers and officials. First, we reviewed those existing systems whose implementation and description are available publicly. In our finding, existing blockchain based certificate systems address those fraudulent activities which are done by students only not which are done by university teachers or officials. In existing blockchain-based systems, universities prepare the final certificate based on the data stored in the university's internal study data system and then store the final certificate on blockchain, and employer can verify the certificate from blockchain. Therefore, student cannot change the final certificate once it is on the blockchain. So existing blockchain-based systems prevents the fraudulent activities of students. In other words, there is no trust concern in the transaction between employer and student; blockchain takes care of it. But university's internal study data system where the course data, assignment submission, course gradings are stored uses traditional database which is not temper proof or trust-free technology. Moreover, teachers' and officials' activities are not controlled or recorded by any system. The employer does not know whether the teacher or officials did any fraudulent activities during assessment or storing the grades and credits in the study data system. Employer just trust that the university teachers and officials did no fraudulent activities during the course evaluation or recording the grades. Thereby, existing blockchain based certificate systems does not address the fraudulent activities done by teachers and officials.

Third research sub-question was how to design a blockchain-based certificate system to prevent fraud activities which are not prevented by the existing blockchain-based certificate systems. Design Science Research method was applied to conduct the research. Through literature review on fake diploma and existing blockchain based certificate systems, we already found that existing blockchain based systems do not address the fraud activities done by university teachers and officials. Because existing systems uses blockchain only for issuing final certificate on blockchain and uses traditional database and centralized

server for study data management system. There was need for a blockchain based study data system which will address the fraud activities done by teachers and students. Our objective was to develop a conceptual model of the study data system using the potentials of blockchain technology. The conceptual model of the system was designed based on the research on blockchain technology features and existing blockchain based certificate systems. The proposed conceptual model explains how a blockchain-based study data management system can be designed to prevent fraudulent activities done by the university officials and teachers. Proposed conceptual model also explains how the complete certificate process should be designed using blockchain technology. After developing the conceptual model, we presented the list of fraud activities and conceptual model document to blockchain researchers at blockchain laboratory at University of Jyvaskyla. The conceptual model description and figures were effective to convey the design objectives and architecture was appropriate from blockchain technology. The proposed conceptual model addresses the fraudulent activities except where human intervention, such as evaluating exam answers, can not be captured with blockchain technology. They gave some suggestions which will make it more preventive to fraud activities.

12.1 Implications to research

In design science research, designed artefact must be innovative by solving problems which have not been solved before or improving the existing systems (Hevner et al, 2004). In this research, I have identified the problems or fraud activities which have not been solved by existing blockchain based certificate systems. After that I have developed a conceptual model of the system to address those unaddressed fraudulent activities. The research result, identified fraud activities and conceptual model of the improved system, will give new information to researchers who wants to design and develop blockchain based certificate system and also to researchers who will do research on developing such system.

Blockchain is the trust machine meaning that it can be used to develop trust-free systems ("The promise of." 2015). With the increasing development of blockchain technology such as smart contract feature, blockchain can be used in other areas than crypto currencies to develop trust-free systems (Beck et al, 2016). In this area of trust-free system and blockchain research, my designed artefact and evaluation result can be used as an example that how potential the blockchain technology is to transform trust-based systems into trust-free systems. As in our case, we have transformed trust-based certificate or study data system to trust-free certificate system. Although in our findings, it was not completely trust-free certificate system, as there are activities such as exam paper evaluation which is usually done by a human teacher in our current system.

12.2 Implications to practice

This research has made a novel contribution by identifying the fraud activities which have not been addressed by existing blockchain based certificate systems and developed a conceptual model of an improved blockchain based certificate system which will address the fraud activities which have not been addressed by existing blockchain based certificate systems. In my findings, no other blockchain based certificate systems have addressed the fraud activities by university's internal officials or teachers in the study data system. The list of identified fraud activities in university's internal study data system and conceptual design of the study data system will guide those who are involved in designing and developing certificate systems and researchers from other areas.

Blockchain in education is at the peak of Gartner Hype Cycle for Blockchain Business, 2018 and will take 5-10 years to reach plateau (Levy, 2018). This research is an important contribution in blockchain for education industry. My findings about the unaddressed problems in currently existing blockchain based certificate systems and the conceptual model to address those problems, specifically conceptual model of the university's study data register system is an innovation or first in its type. Identifying problems and conceptual model are typically the first documents and designed artefact in the design process of a system and gives high level abstract knowledge to develop a system. Conceptual model of the study data system and list of fraud activities inside the university will guide to design and develop a better and smart blockchain based certificate systems for the individual needs of universities or companies who are trying to develop blockchain based certificate system. The proposed architecture and set of smart contracts based on theoretical perspectives gives guidance to develop the actual smart contracts and how to use them.

13 CONCLUSION

Blockchain technology have the potential to create systems where people can make transaction in a verifiable manner and reduce the trust issues between parties in the system. The fraudulent activities in our education system to produce counterfeit credentials can be reduced using blockchain technology. Instead of trusting student, teachers, university officials to produce and issue legitimate credentials, using blockchain technology can enforce not to act wrongfully, and employer can check the recorded activities of those parties.

13.1 Limitations of the study

Developing an actual prototype and evaluating it in an actual university setting would have been the most proper to do it. But due to the fact that developing a prototype for such a system would require lot of technical skills and resources and collaboration with the university which is not possible during this thesis period.

Ezell and Bear (2012) has said that academic research on fake certificate or fraud activities in certificate system is very rare. Fraud activities in the certification process in details is rare in scientific paper and it cannot be generalized with every country, although Ezell and Bear (2012) have said no nation is immune from this problem. I had to collect some of the details of the fraud activities from newspaper and investigation reports by TV channels.

13.2 Recommendations for further research

The conceptual design of the blockchain based certificate system developed in this thesis can be used to develop a proof-of-concept with collaboration of a university and test the system. There can be research on developing an exam or assignment evaluation system based on blockchain technology and artificial intelligence instead of depending on human intervention to make the evaluation activities trust-free.

REFERENCES

Antonopoulos, A. M. (2015). Mastering Bitcoin. O'Reilly Media, Inc. Online edition. http://chimera.labs.oreilly.com/books/1234000001802

Apurv, S. (2018). Digital Certificates on Hyperledger Fabric. Retrieved March 02, 2019 from https://medium.com/coinmonks/digital-certificates-on-hyperledger-fabric-3d0ba1c36ecd

Asharaf, S. & Adarsh, S. (2017). Decentralized Computing Using Blockchain Technologies and Smart Contracts: Emerging Research and Opportunities. *IGI Global*. Retrieved from https://books.google.fi/books?id=rYMJDgAAQBAJ

Attewell, P., Domina, T. (January 2011). Educational imposters and fake degrees, *Research in Social Stratification and Mobility*, Volume 29, Issue 1, 2011, Pages 57-69, ISSN 0276-5624, https://doi.org/10.1016/j.rssm.2010.12.004.

Atzei N., Bartoletti M., Cimoli T. (2017) A Survey of Attacks on Ethereum Smart Contracts (SoK). In: Maffei M., Ryan M. (eds) Principles of Security and Trust. POST 2017. Lecture Notes in Computer Science, vol 10204. Springer, Berlin, Heidelberg

Bajpai, P. (2017, July 05) 'Big 4' Accounting Firms Are Experimenting With Blockchain And Bitcoin. Retrieved December 20, 2017, from http://www.nasdaq.com/article/big-4-accounting-firms-are-experimenting-with-blockchain-and-bitcoin-cm812018

Banking Is Only The Beginning: 30 Big Industries Blockchain Could Transform. (2017, August 25). Retrieved January 13, 2018, from https://www.cbinsights.com/research/industries-disrupted-blockchain/

Banton, C. (2019, April 19). Escrow. Retrieved May 01, 2019, from https://www.investopedia.com/terms/e/escrow.asp

Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain – the Gateway to Trust-Free Cryptographic Transactions. Twenty-Fourth European Conference on Information Systems (ECIS), Istanbul, Turkey.

Benet, J. (2014). IPFS - content addressed, versioned, P2P file system. *White Paper*

Brown, G. M. (2006). Degrees of Doubt: Legitimate, real and fake qualifications in a global market. *Journal of Higher Education Policy and Management*, Vol. 28, No. 1, pp. 71–79.

Build Unstoppable Applications. (2017, December 18). Retrieved from https://www.ethereum.org/

Buterin, V. (2015, April 13). Visions, Part 1: The Value of Blockchain Technology. Ethereum Blog. Retrieved from https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/

Canaday, H. (2017). Blockchain In MRO Could Happen Sooner Than You Think. Retrieved December 26, 2017 from http://www.mro-network.com/big-data/blockchain-mro-could-happen-sooner-you-think

Cao, S., Cao, Y., Wang, X., & Lu, Y. (2017). A Review of Researches on Blockchain. WHICEB 2017 Proceedings. 57

Cert-issuer. (2019). Retrieved March 27, 2019, from https://github.com/blockchain-certificates/cert-issuer/blob/master/README.md

Chen, G., Xu, B., Lu, M., and Chen N. S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*

Christidis, K. & Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things, *IEEE Access*, pp. 2292-2303, May 2016.

Clifton, H., Chapman, M., and Cox, S. (2018, January 16). 'Staggering' trade in fake degrees revealed. *BBC News*. Retrieved from https://www.bbc.com

Coletti, P. (2015, May 20). Bitcoin's baby: Blockchain's 'tamper-proof' revolution. *BBC News*. Retrieved from http://www.bbc.com

Coughlan, S. (2013, October 9). Corruption and bribery in the classroom. *BBC NEWS*, Retrieved from https://www.bbc.com

Decentralized Applications – dApps. Retrieved April 07, 2019, from https://blockchainhub.net/decentralized-applications-dapps/

Degree Overview. (2019, April 08). Retrieved April 08, 2019 from https://www.buyuniversitydegrees.com/degree-overview/

Digital Certificates Project. (2016). Retrieved March 27, 2019, from http://certificates.media.mit.edu/

Ekushey Television - ETV. (2014, April 11) *Private university Certificate Frauding*. Retrieved from https://www.youtube.com/watch?v=0edAvEZ8LOA

Ezell, A. & Bear, J. (2012) *Degree Mills: The Billion-Dollar Industry That Has Sold Over a Million Fake Diplomas* (Updated ed.). New York: Prometheus Books.

Faraj, S. & Sambamurthy, V. (2006). Leadership of Information Systems Development Projects. *IEEE Transactions on Engineering Management, 53(2),* 238–249.

Gräther, W., Kolvenbach, S., Ruland, R., Schütte, J., Torres, C., & Wendland, F. (2018). Blockchain for Education: Lifelong Learning Passport. In: W. Prinz & P. Hoschka (Eds.), Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies (ISSN 2510-2591), DOI: 10.18420/blockchain2018_07

Grolleau, G., Lakhal, T., & Mzoughi, N. (2008). An Introduction to the Economics of Fake Degrees, *Journal of Economic Issues*. 42(3): 673–693.

Gupta, V. (2017, March 06). The Promise of Blockchain Is a World Without Middlemen. *Harvard Business Review*. Retrieved from https://hbr.org/2017/03/the-promise-of-blockchain-is-a-world-without-middlemen

Hallak, J. and Poisson, M. (2007). Corrupt schools, corrupt universities: What can be done ?. International Institue for Educational Planning. UNESCO

Harding, D., A. (2015). Is it chain of headers rather than a chain of blocks? Retrieved December 26, 2017 from https://bitcoin.stackexchange.com/questions/35448/is-it-chain-of-headers-rather-than-a-chain-of-blocks

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*, Volume 29, Pages 50-63.

Hevner, A.R., March, S.T., & Park, J. (2004). Design research in information systems research. MIS Quarterly, 28, 1, 75–105.

Hooper, M. (2018). Top five blockchain benefits transforming your industry. Retrieved from https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/

Islam, S. (2009, May 8). Bangladesh: Making the Grade, or Making a Bribe?. Retrieved from https://www.globalintegrity.org/2009/05/08/post-393/

Jagers, C. (2016, June 3). Verifiable Credentials on the Blockchain. Retrieved March 26, 2019, from https://medium.com/learning-machine-blog/blockchain-credentials-b4cf5d02bbb7

Jagers, C. (2016, June 3). Verifiable Credentials on the Blockchain. Retrieved March 26, 2019, from https://medium.com/learning-machine-blog/blockchain-credentials-b4cf5d02bbb7

Karame, G. & Androulaki, E. (2016). Bitcoin and Blockchain Security. Norwood, MA: Artech House.

Knox, J. (2017, October 6). Student grades believed to be hacked at University of Regina Retrieved April 26, 2019, from https://globalnews.ca/news/3790701/student-grades-believed-to-be-hacked-at-university-of-regina/

Koenig, A. M., & Devlin, E. (2012). FIGHTING domestic and international FRAUD in the admissions and registrar's offices. College and University, 88(1), 18-33. Retrieved from https://search.proquest.com/docview/1239088196?accountid=11774

Lancaster, T. (2017, January 31). Everything you need to know about fake degrees and the 'universities' awarding them . Retrieved April 26, 2019, from http://theconversation.com/everything-you-need-to-know-about-fake-degrees-and-the-universities-awarding-them-71132

Lewin, T. (2007, April 27). Dean at M.I.T. Resigns, Ending a 28-Year Lie. *The New York Times.* Retrieved from https://www.nytimes.com

Lindman, J., Tuunainen, K., V., Rossi, M. (2017). Opportunities and Risks of Blockchain Technologies – A Research Agenda. Hawaii International Conference on System Sciences.

Marr, B. (2017, September 21). 14 Things Everyone Should Know About Blockchains. Retrieved from https://www.forbes.com/sites/bernardmarr/2017/09/21/14-things-everyone-should-know-about-blockchains

Mattila, J. (2016). The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures, The Research Institute of the Finnish Economy.

Mir-Jabbar, S. (2017, November 2). An Overview of Fraud and Degree Mills with Updates on the Axact Degree Mill Operation: November 2017 Newsletter. *The Association for International Credential Evaluation Professionals*. Retrieved from https://www.taicep.org/taiceporgwp/an-overview-of-fraud-and-degree-mills-with-updates-on-the-axact-degree-mill-operation-november-2017-newsletter/

Mulders, M. (2018, March 5). Comparison of Smart Contract Platforms. Retrieved from https://hackernoon.com/comparison-of-smart-contract-platforms-2796e34673b7

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Nazaré, J. (2016, June 2). What we learned from designing an academic certificates system on the blockchain. Retrieved March 26, 2019, from https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196

Ølnes, S. & Jansen, A. (2017). Blockchain Technology as s Support Infrastructure in e-Government. In: Janssen M. et al. (eds) Electronic Government. EGOV 2017. Lecture Notes in Computer Science, vol 10428. Springer, Cham

Orlikowski, W. J. & C. S. Iacono (2001). Research commentary: Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact. Information Systems Research 12(2) 121-134.

Panetta, K. (2016, August 19). 3 Trends Appear in the Gartner Hype Cycle for Emerging Technologies, 2016. Retrieved from https://www.gartner.com/smarterwithgartner/3-trends-appear-in-the-gartner-hype-cycle-for-emerging-technologies-2016/

Peng, Y.(2017, February 26) Ethereum: fueling the hype around blockchain? Retrieved from https://digit.hbs.org/submission/ethereum-fueling-the-hype-around-blockchain/

Perez, B. (2017, September 27) The three key things you need to know about blockchain technology. South China Morning Post. Retrieved December 23, 2017, from http://www.scmp.com/tech/enterprises/article/2112627/three-key-things-you-need-know-about-blockchain-technology

Phillips, G. A. (2014). Degree Mills: The Billion-Dollar Industry That Has Sold Over a Million Fake Diplomas by Allen Ezell, John Bear (review). *The Review of Higher Education*, vol. 37 no. 2, pp. 282-284. Project MUSE.

Pilkington, M. (2015). Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations, edited by F. Xavier Olleros and Majlinda Zhegu. Edward Elgar.

Rapier, G. (2017, June 21). From Yelp reviews to mango shipments: IBM's CEO on how blockchain will change the world. BUSINESS INSIDER NORDIC. Retrieved from http://nordic.businessinsider.com/ibm-ceo-ginni-rometty-blockchain-transactions-internet-communications-2017-6

Schmidt, P., J. (2017, April 24). Credentials, Reputation, and the Blockchain. Retrieved March 26, 2019, from https://er.educause.edu/articles/2017/4/credentials-reputation-and-the-blockchain

Sharadeshe jal sonoder sorasori : shokrio oshonkho jaliat chokro [Fake certificate syndicate across the country : many active fraud syndicates]. (2015, June 16). *Bhorer Kagoj*. Retrieved from http://www.bhorerkagoj.com/print-edition/2015/06/16/37541.php

Smith, E., K. (2015, April 24). Cheating student who hacked into university computer system to give himself a better degree is jailed. *Daily Mail Online*. Retrieved from https://www.dailymail.co.uk

Sommerville, Ian, and Pete Sawyer. 1997. Requirements Engineering: A Good Practice Guide. Chichester, England: John Wiley & Sons Ltd.

Steiner, J. (2015, June 19). Blockchain Can Bring Transparency to Supply Chains. Retrieved December 22, 2017, from https://www.businessoffashion.com/articles/opinion/op-ed-blockchain-can-bring-transparency-to-supply-chains

Sven, W. (2010). Design Science Research: Paradigm or Approach?" AMCIS 2010 Proceedings. 214. http://aisel.aisnet.org/amcis2010/214

Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. Retrieved December 26, 2017, from http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Tapscott, D. & Tapscott, A. (2016a). The Impact of the Blockchain Goes Beyond Financial Services. Retrieved July 27, 2018, from https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services

Tapscott, D. & Tapscott, A. (2016b). The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. pp. 72, 83, 101, 127. ISBN 978-0670069972.

The great chain of being sure about things. (2015, October 31). *The Economist*. Retrieved from https://www.economist.com

Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A Blockchain-Based Higher Education Credit Platform. *IEEE Access*, vol. 6, pp. 5112-5127. doi:10.1109/ACCESS.2018.2789929

Verification Process. (2018). Retrieved March 27, 2019, from https://github.com/blockchain-certificates/cert-verifier-js/blob/master/docs/verification-process.md

Welcome to EduCTX. EduCTX is an efficient, simplified, ubiquitous solution for a student's credit assignment. (2019, March 09). Retrieved from https://eductx.org/

Yusuf, Z., I. & Bijoy, S., I. (2016, October 25). Private porikhkhar arale certificate banijjo [Certificate business behind the private institutes]. *Jugantor*. Retrieved from https://www.jugantor.com/news-archive/protimoncho/2016/10/25/70962/প্রাইভেট-পরীক্ষার-আড়ালে-সার্টিফিকেট-বাণিজ্য

Zhao, J. L., Shaokun, F., and Yan, J. (2016). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation*