Cerberus: A Blockchain–Based Accreditation and Degree Verification System

3 authors, including:

Hina Binte Haq
National University of Sciences and Technology
7 PUBLICATIONS   **93** CITATIONS

Cerberus: A Blockchain-Based Accreditation and Degree Verification System

Aamna Tariq*, Hina Binte Haq [†] , Syed Taha Ali[‡]

School of Electrical Engineering and Computer Sciences (SEECS), National University of Sciences and
Technology (NUST), Islamabad, Pakistan.

* [†] contributed equally to the paper.

*atariq.msit16seecs@seecs.edu.pk, [†]hhaq.dphd18seecs@seecs.edu.pk, [‡]taha.ali@seecs.edu.pk

Abstract—**Credential fraud is a widespread practice that undermines investment and confidence in higher education systems and bears significant economic and social costs. Legacy credential verification systems are typically time-consuming, costly, and bureaucratic, and struggle against certain classes of credential fraud. In this paper, we propose a comprehensive blockchain-based credential verification solution, Cerberus, which is considerably more efficient, easy and intuitive to use, and effectively mitigates widespread manifestations of credential fraud. Cerberus also improves significantly upon other blockchain-based solutions in the research literature: it adheres closely to the existing credential verification ecosystem, it addresses a threat model informed by real-world fraud scenarios. Moreover, Cerberus uses on-chain smart contracts for credential revocation, and it does not entail students or employers to manage digital identities or cryptographic credentials to use the system. We prototype our solution and describe our attempt to design an online verification service with a rich feature set, including data privacy, transcript verification, and selective disclosure of data. We hope this effort contributes positively to towards alleviating the problem of fake credentials.**

Managerial Relevance Statement

There is widespread recognition that the blockchain can effectively combat the problem of fake credentials and significantly improve the credential verification process. There are several efforts underway in this domain, both in industry and ideas proposed in the research literature. However, to the best of our knowledge, what is most lacking is a rigorous effort to tailor these solutions to existing practices of credential fraud, and to mitigate usability issues on the part of users.

Our system will enable practitioners (universities, accreditation bodies, employers) to undertake the following: 1) to concretely visualize the workings and benefits of such a system and work towards integrating it into existing credential verification ecosystems, and 2) to adapt and customize the rich feature set of our solution to cater to their own requirements.

I. Introduction

The value of education to society cannot be overstated: education plays a pivotal role in enabling social mobility [1] [2], it contributes to economic uplift [3] [4] [5], and it promotes political stability and reform [6] [7] [8]. Education is also a critical factor for innovation to meet local and international challenges and opportunities [9]. For these reasons, education typically ranks near the top of government spending priorities in developed countries, and often absorbs over a fifth of total government spending in the public sector [10].

Corruption in the domain of education can have wide-ranging and detrimental effects. In 2013, in its global corruption report on education, Transparency International extensively documented various instances of such phenomena, particularly in developing countries where such fraud is pervasive and systemic. Corrupt practices range over a wide spectrum including bribery and nepotism in admissions and in examinations results, a culture of teacher absenteeism, deteriorating quality of education, misappropriation of funds, ghost schools existing only on paper, diploma mills which issue fake academic degrees, and compromised accreditation services [11].

In this paper, we specifically focus on the problem of fake academic credentials. With increasing social pressure to outperform peers in highly competitive job markets, many applicants misrepresent their qualifications to make their curriculum vitae more appealing to employers. An academic credential typically requires considerable investment in terms of time, effort, and funding, and in turn it confers a certain prestige on the bearer and opens new opportunities to them. Fake degrees essentially enable third parties a 'free ride' on these benefits [12].

Falsified credentials range from high school diplomas to doctorate degrees. There have been publicized instances where investigators have successfully procured fake degrees on behalf of pet cats [13] and dogs [14]. According to one study, over a third of potential candidates admit to falsifying or 'enhancing' their qualifications for a job application [15]. A professor in South Africa was recently assassinated for exposing a syndicate producing fake PhD degrees [16]. There is a marked scarcity of research on the scope of this problem, but a conservative estimate suggests that there are more than 5000 unrecognized universities and diploma mills operating worldwide, and issuing over 200,000 fake degrees annually with revenues in excess of $1 billion [17].

These unethical practices not only discourage individual investment in education but also damage the value, credibility and reputation of a higher education system. Moreover, there may be considerable social harm: apart from a compromised sense of ethics, a fake degree holder will likely not possess the requisite expertise in his field (achieved through rigorous training and evaluation), thereby posing a real danger in certain domains. For instance, subjects implicated in fake degree scandals include doctors, nurses [18] [19] , pilots [20] [21],

and even politicians and government ministers [22] [23] [24].

The traditional defense against fake credentials is stringent verification procedures. In certain countries, this task is undertaken at a national level by government bodies, such as the Academic Degrees and Graduate Education Development Center in China [25], the Higher Education Commission in Pakistan [26], and the Higher Attestation Commission in Russia [27]. In some territories, accreditation is overseen by non-governmental agencies, such as the Council for Higher Education Accreditation (CHEA) in the United States [28], and Tertiary Education Quality and Standards Agency (TEQSA) [29], Australia's independent national quality assurance and regulatory agency for higher education. There also exist wide-ranging international efforts such as the Hague Apostille Treaty of 1961, whereby citizens can have their credentials certified by a designated authority so that they may be recognized in 116 signatory countries [30]. Another facility is the IAU World Higher Education Database (WHED) which provides comprehensive information on accredited higher education systems and credentials around the world [31].

However, most credential verification mechanisms are opaque, cumbersome, time consuming, and costly. According to a survey, one in three employers in the UK do not request candidates for their degree certificates; and, of those who do, 76% of employers assume the certificates are legitimate and do not verify their authenticity [32]. Foregoing diligent background checks entails costs in terms of lost time, performance, and investment: in the US, the Department of Labour reports that forged credentials and doctored qualifications cost companies an average of $40,000 per bad hire [33].

In recent years, the blockchain has been promoted as a promising new technology for transparency and data integrity in a variety of domains, including payment settlements [34] [35], copyright protection [36] [37], data notarization [38] [39], digital government [40] [41] [42] [43], health care [44], [45], [46] [47], logistics and tracking [48] [49], and secure elections [50] [51]. Due to its distributed architecture and its reliance on cryptography, the blockchain offers strong guarantees on accountability, accessibility and data immutability, which is particularly suited to scenarios with multiple untrusted parties. Various efforts also advocate using the blockchain to combat the fake degree problem [52] [53] [54], but as yet there are few rigorous efforts [55] in this direction.

We attempt to address this deficiency. Our paper makes the following contributions:

1) We propose a comprehensive blockchain-based solution for easy and efficient verification of academic credentials. We describe a solution architecture which integrates seamlessly with typical credential management ecosystems and we devise a threat model informed by real-world fraud scenarios,

2) We prototype our solution and describe our attempt to design an online verification service with a rich feature set, including data privacy, transcript verification, and selective disclosure of data,

3) We propose a novel credential revocation mechanism. This is a distinct contribution in its own right. We sug-

gest a simple and practical on-chain revocation mechanism which leverages smart contracts.

We describe here briefly a representative scenario which motivates our solution: an Accreditation Authority operates and maintains a permissioned blockchain in partnership with universities and watchdog organizations. When a student, Alice, graduates, her university issues her a physical degree certificate and also add her details on the blockchain platform. This certificate also contains a QR code which allows Alice, or any other party, to verify her credentials in real-time from the blockchain using a smartphone app. This is similar to national visa verification services such as VEVO in Australia [56], the Employer Checking Service in the UK [57], and E-Verify in the US [58], which allow employers to check the visa status of job applicants via a Web portal. Alice can even paste a QR code on her resume, thereby enabling prospective employers to verify her details independent of the certificate. In case her degree is revoked, the university will make corresponding entries in the blockchain which will be revealed when Alice's QR code is scanned.

This solution has notable differences with prior work: first, our effort is on engineering a solution that preserves the existing ecosystem and maintains key security properties such as guarantees on data privacy, integrity, and revocation. Second, it approximates and improves upon the real world process flow for credential management and verification. Furthermore, we focus on usability: our solution is relatively easy to use since verification can be done by scanning a QR code and neither Alice nor her employer are required to personally interact with the blockchain or maintain secret keys.

The rest of this paper is organized as follows: in Section II Background, we discuss the ground realities regarding academic credential fraud throughout the world and also discuss the higher education Ecosystem specific to Pakistan. In Section III we discuss the architecture and flow of the Proposed System. In Section IV we enumerate implementation details of our prototype of the system. In Section V Discussion, we highlight and explain how our system achieves the various security properties. In Section VI we compare and contrast our endeavour with similar systems and related work. In Section VII we delineate future direction for research and conclude our discussion in Section VII.

II. BACKGROUND

A. The Varieties of Credential Fraud

Credential fraud has been around since at least the fourteenth century [17], and there is considerable evidence that degrees were widely sold in German universities in the 18th century [59]. However, this phenomenon gained rapid traction in the 20th century due to two main drivers: first, as Johnson convincingly argues, increasing global competition in job markets has given rise to a widespread culture of *credentialism*, with employers 'overly relying on degrees as proof of job competency', even for low-to-moderate skill positions. This practice likely contributes considerably to the black market for fake credentials [60].

Second, the 20th Century marked the ascendance of the "for-profit" education model in schools and universities, whereby academic excellence and integrity had to contend increasingly with economic and business interests. This situation was further complicated by rapid expansion higher education institutions in the form of distance learning programmes, flexible and distributed learning modes, branch campuses, franchising, and credit transfer schemes [61]. The distributed and transnational nature of these schemes makes it considerably more difficult to enforce independent checks on quality and integrity.

The result is a pervasive and thriving culture of credential fraud and a billion dollar industry [11]. Whereas concrete figures on credential fraud are not available [62], some investigations reveal the alarming scope of this trend [63]. For instance, in the US, home to the largest number of diploma mills in the world [64], Ezell et al. document that the number of fake PhD degrees purchased every year exceeds 50,000, outnumbering the 40,000-45,000 legitimate PhDs awarded by universities [65]. One diploma mill, operated by Americans with offices in Europe and the Middle East, has sold more than 450,000 degrees with revenues exceeding US $450,000,000. [66]

In Europe, the UK is believed to host the largest number of diploma mills [64]. A prominent example was the University of Wales, the second-largest university in the country with a 120-year history, which had 70,000 students enrolled in 130 colleges around the world. After multiple scams and administrative failures were uncovered, the registrar resigned and the university shuttered its highly profitable degree validation program, which accounted for nearly two thirds of institutional revenue [67] [68].

Fraud is also rampant in the developing world. According to one estimate an alarming half of all high school transcripts in overseas university admissions applications by Chinese students are falsified [62]. This problem is also very widespread in India [69] [70], and trafficking in fake certificates has been described as a 'pan-India' crime [71]. A 2015 study found that one in nine politicians in the lower house of the Russian parliament possessed a plagiarized or fake degree. In Indonesia, a task force was set up by the government in 2015 to crack down on fake degrees issued specifically to politicians [22].

Here we broadly classify various categories of credential fraud:

a) Document Fraud: typically involves illegal counterfeits, deceitful alteration of legitimate credentials (modification of name, signatures, degree, details, etc.), or complete fabrications (using fake logos, seals, and serial numbers) [72]. This category also includes doctored or misleading translations and evaluations of credentials.

A recent example is the case of degree shops that have recently sprung up on the Syrian-Turkish border, where merchants exploit desperate Syrian migrants and refugees by selling them forged documents on their way to Europe. A high school diploma reportedly costs USD $600, whereas a university degree can be as much as USD $2,500 [73].

b) Institutional Fraud: refers to the case where staff within institutions are compromised [67]. Such fraud may involve the university registrar or other officials who create an illegitimate credential which is retroactively appended in the official record of the university. This tactic is more reliable than document fraud because the credential itself is authentic and can usually withstand cursory scrutiny because it is backed by university records.

A prominent example is the case of Busoga University in Uganda which was investigated in 2016 for issuing more than 1,000 "premium-tuition" degrees to South Sudanese students, most of them military officers seeking easy degrees to secure government positions [74].

c) Diploma Mills: sell fake credentials from fictitious universities and lead the mass market in credential fraud. These bodies operate in a highly structured and sophisticated manner, with a corporate culture including a dedicated marketing and sales teams, and offer customised "products" to buyers. These mills often maintain immaculate websites for fictitious universities [75].

A recent example is the international scandal of Axact, widely considered the largest degree scam yet, where a Pakistan-based company that operated a web of more than 370 diploma mills which collectively earned millions of dollars in revenue by selling fake degrees and certificates of hundreds of fictitious universities to clients worldwide [75]. Axact have also been known to extort their customers for funds after making sales to them by threatening to reveal that their credentials were bogus [76].

d) Accreditation Fraud: refers to the case where the accreditation body that validates a credential as authentic may itself be compromised or fictitious. A very common strategy employed by diploma mills is to set up fake accreditation mills to legitimize the credentials they sell.

The Federal Investigation Agency in Pakistan, has probed several instances where regulatory bodies verified fake degrees of powerful officials without due diligence [77]. Recently a company investigating credentials of Chinese student applicants on behalf of prominent universities in the US had to withdraw from the project on charges that it engaged in widespread application fraud itself [78]. A Connecticut man who sold fake degrees operated a fictitious accreditation service in parallel, the National Distance Learning Accreditation Council to validate his degrees [79]. These practices pose highly complex challenges for employers who often have limited resources available to verify academic credentials.

B. Blockchain and Smart Contracts

Here we present a high-level overview of blockchain and smart contracts technology and highlight the security properties of this novel new paradigm.

A blockchain is a decentralized global ledger consisting of a continuously growing list of records, called blocks, arranged in chronological order. Users possess cryptographic credentials, namely a public/private key pair, which enables them to insert new records into this ledger. Individual blocks are coupled together using hash pointers such that data cannot be removed
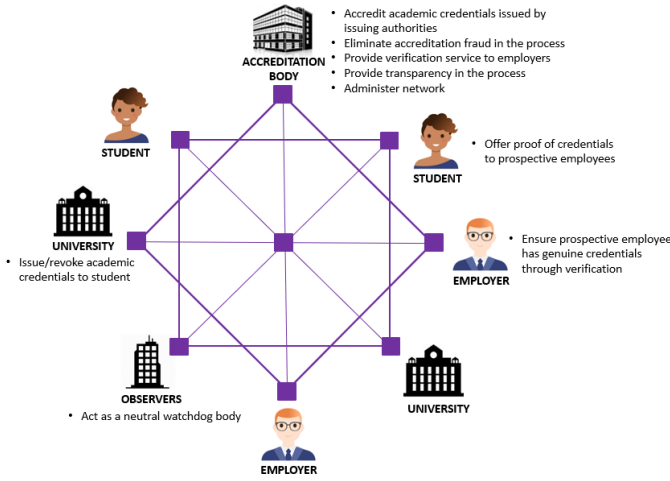
Figure 1: The ecosystem for credential verification

from the block nor added retroactively without detection by all the other parties. The synchronization and integrity of this ledger is assured by a distributed consensus protocol which periodically selects certain parties (miners) to append new blocks to the ledger.

The notion of smart contracts builds on this paradigm by envisioning the shared ledger as a public memory space, thereby extending the notion of verifiability from data to computations. The earliest cryptocurrencies, including Bitcoin, introduced limited support for scripts to govern the handling of transactions. Later platforms, notably Ethereum, provide powerful support to users to embed complex application logic into the ledger.

Various developers are using smart contracts to build sophisticated solutions which address real-world solutions in a secure and decentralized manner. These include applications such as trading securities and derivatives [80], optimize supply chains [81], remote healthcare [82], and prediction markets [83], etc.

Our credential verification solution uses a permissioned blockchain, i.e. one where peers in the ecosystem are assigned different roles and privileges. Smart contracts define the rules according to which credentials may be revoked.

C. Ecosystem and Threat Model

The ecosystem for credential verification typically consist of various parties as depicted in Fig. 1.

Universities award academic credentials in a field of study. A **credential** in this context refers to a diploma, degree, or certificate issued by a university to a **student** in lieu of successful completion of the requirements of a certain educational program. These credentials serve as proofs of qualification, considered essential for most jobs and various other life opportunities. Therefore, there is a considerable need among **employers** and others to ensure that degrees belonging to their workers are genuine.

Accreditation bodies are national-level or private entities which undertake the task of verifying and validating academic credentials issued by educational institutions. Certain accreditation authorities also issue certified translations of credentials

or prepare equivalence certificates. In our setup, accreditation bodies are also responsible for setting up and administering the Cerberus network.

A final party to this scenario could be **observers** such as citizen groups, activists, and watchdog bodies whose key role is to audit the operations of these different parties and maintain quality checks.

In our threat model, we assume that any of these entities may be malicious. For instance, a student may try to forge a credential or purchase one from a diploma mill. A university may sell fake degrees. An accreditation body may try to accredit fake degrees. Different malicious parties may even collude. As we've noted in §.II-A, these threats are realistic and there are abundant examples of each.

A credential verification solution should defend against the aforementioned attacks to the greatest possible extent. Here we list certain desirable security properties of such a system:

- **Authenticity** The system should serve as a secure and authentic repository which enables verification of credentials. All stakeholders should be able to view and audit the inner workings of this system and maintain checks on the behavior of other parties. Moreover, the system should integrate with existing credential management infrastructure.
- **Resilience:** In the ideal case, we should be able to detect credential fraud if there is at least one honest party participating on the blockchain network.
- **Privacy Preservation:** The system should not leak any data regarding students' credentials or personal information to third parties (such as employers) beyond any information the students may choose to reveal themselves. This includes student identities, grade transcripts, degree status, etc.

We also list here certain other features for a credential verification system that are desirable from a usability and efficiency perspective:

- **Real-time Online Verification:** A prominent property of blockchain solutions is disintermediation, i.e. decoupling the need for trusted centralized parties, and thereby immensely speeding up operations. The credential verification process is typically cumbersome and involves paperwork and communication with the awarding university. However, an online verification solution operating on top of a permissioned blockchain should enable real-time degree verification for users.
- **Third-party Verification:** The system should enable third parties to directly and independently verify credentials of a user without relying on intermediaries.
- **Selective Disclosure:** Users should be able to verify individual credential details in a piecemeal manner. This would enable students to share selective details with different parties. For instance, Alice could print her primary credential details on her curriculum vitae and on job applications, without revealing any other potentially sensitive data, such as national identification number or grades transcript. These could be disclosed in other situations that necessitate it.
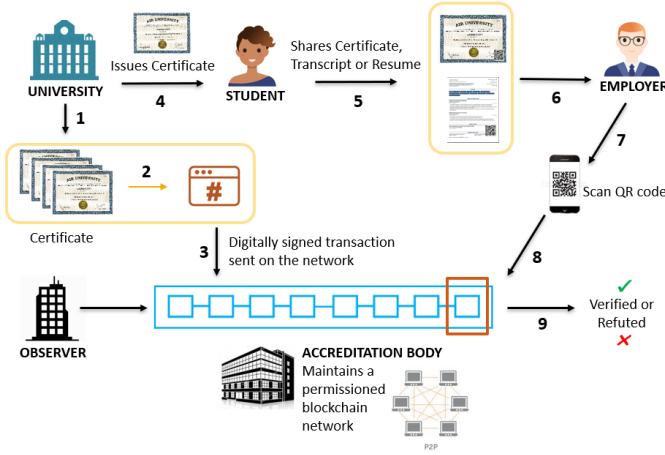
Figure 2: System Overview

- **Usability:** The system should be easy to use and not require significant technical sophistication on the part of users. Multiple studies also note that users face difficulty storing and handling cryptographic credentials [84][85].
- **Revocation:** If a credential is revoked, the revocation information should be efficiently and quickly disseminated to all stakeholders, without any room for ambiguity.

Credential verification solutions in certain countries are already adopting many of these features. Centralized online verification systems have recently been rolled out to combat widespread credential fraud in India [86] and Malaysia [87]. In later sections, we discuss how popular technologies such as smart phones and QR codes can be leveraged to further facilitate user experience.

III. The Proposed System: Cerberus

In this section we describe the inner workings of our proposed solution. We start with a high-level overview of the key steps in the life cycle of a **credential**. The process is depicted in Fig. 2.

An **accreditation body** operates and maintains a permissioned blockchain network in partnership with multiple parties including **universities** and **observer** entities, such as activist organizations and citizen groups. The **universities** circulate transactions containing validation information for credentials they issue to **students**. The **accreditation body** periodically collects these transactions and aggregates them into blocks which are then added to the blockchain. **Observer** parties audit every process in the system and maintain checks on integrity.

When a student, Alice, graduates, the **university** issues her a physical certificate of her academic degree and her transcript. The university administration also creates a transaction containing a digital fingerprint of Alice's **credential** details (alongside that of other graduating students). This transaction is digitally signed by the **university registrar** and propagated on the Cerberus network, where it is verified by nodes belonging to the **accreditation body**, mined into a block and added to the blockchain. This step corresponds to the issuance and accreditation of a **credential**.

The physical degree certificate issued to Alice by the **university** incorporates a QR code, for **credential** verification, printed on the front which facilitates verification of the information on her certificate. If an **employer**, Bob, wants to check if Alice's degree is genuine, he can scan the code with a smartphone app or use a web portal. These services retrieve validating information from the Cerberus network in real-time, verify the code, and inform Bob of the degree's authenticity. Alice can also print the credential verification code on her resume alongside her educational details so that any third party can verify her degree independently of the physical certificate.

If the **university** were to revoke Alice's degree, it would circulate a revocation transaction which the **accreditation body** would verify and add to the blockchain. Any party that checks Alice's credential verification code subsequently would be informed that the degree has been revoked (as explained in detail below).

In the detailed solution specification which follows we also describe additional features whereby additional data may selectively disclosed and authenticated using the blockchain (such as Alice's identity, the contents of her educational transcript, etc.). Solution developers can easily adapt these general techniques to different types of data as per their requirements.

A. Administering the Network

The **accreditation body** is responsible for initial configuration of the network and to maintain the blockchain and update the network as participants change over time. The **accreditation body** has to deploy multiple nodes itself to distribute and secure the network. These nodes should ideally be geographically spaced and secured as per industry standards.

The **accreditation body** also manages how other parties access and use the network. When a new **university** is listed, the **accreditation body** adds it to the network and certifies it's cryptographic keys. A **university** may also be removed from the network for various reasons (e.g. in case of fraud or if quality standards are not met) in which case it's address and keys are added to a blacklist. Keys that have been lost or compromised are also added to the blacklist and new keys are generated to replace them. The **accreditation body** also provides access to third party **observers** to audit the network.

The **accreditation body** may also update the network as per users' requirements by introducing new contracts, roles, and privileges to cater to evolving policies or changes in the ecosystem.

B. Issuance of the Credential

When an academic session concludes, the **university** prepares degree certificates for students in the graduating batch. Issuing the **credential** comprises three key steps as follows:

a) Preparing the Credential: Our solution enables verification of two sets of data: the first is data pertaining to the academic degree (denoted as *degree_info*), and second is more detailed data relating to the identity of the **student** and contents of her transcript (denoted as *id/transcript_info*). The **student** can choose to disclose these data items selectively for

verification. For instance, she can publicly circulate details of her degree on her resume or her social media profile, whereas transcript and detailed identity details may only be required by some **employers**.

The first data set, *degree_info*, typically contains the following information:

- name of the Student
- serial number of the degree
- title of the degree/program
- year the degree is awarded
- name of the University

The second data set, *id/transcript_info*, consists of the following data items:

- details of student's identity document (such as drivers license, citizen card, etc.). This can even be just a personal identification number.
- course codes, Titles, and credit hours for the study program
- grades earned by the student
- Grade Point Average and Cumulative Grade Point Average earned by the student

The items in both data sets are individually concatenated and uniquely fingerprinted using a hash function, *H()*, forming the *student-info* that constitutes a leaf. Popular hash functions, such as SHA2 or MD5 may be used for this purpose. The fingerprints are then input into a Merkle tree. Merkle trees, first proposed by Ralph Merkle, are hash-based data structures that allow authentication of data sets by computing a message digest (or *root*) over the data items using hash-and-concatenate operations to build a tree structure encompassing the entire set [88]. This arrangement significantly reduces the amount of verification data that needs to be put on the blockchain to verify large data sets.

In our solution, the tree is composed as depicted in Fig. 3. Each leaf node represents a **student's** data, and the root of the tree is computed over the entire graduating batch of **students**[1]. This Merkle root, denoted the *batch_Merkle_root*, can now be used to authenticate all data items in the original set, i.e. the degree, identity, and transcript information for all **students** in the batch.

b) Registering the Credential: The next step is to record the *batch_Merkle_root* computed by the **university**, on to the blockchain.

The **registrar** at the **university** creates a Cerberus transaction, addressed to the **accreditation body**, embeds the *batch_Merkle_root* in the data field of the transaction, signs the transaction with its private key, and circulates it on the Cerberus network where it is received by every party. As per the consensus rules, nodes belonging to the **accreditation body** check incoming transactions for correctness, verify the signatures, collect the transactions into a block and append it to the blockchain.

As we noted earlier in §.II-A, **university staff** themselves have been known to insert fake information into the student

---

[1]Merkle trees are binary, and therefore, if there are an odd number of students, the last hash will be duplicated once to create an even number of leaf nodes.
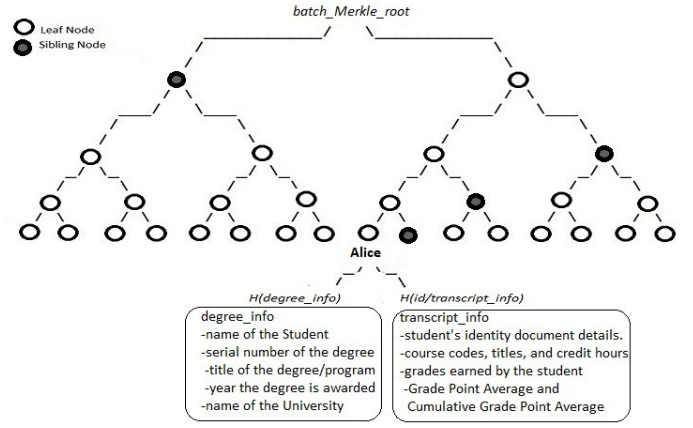

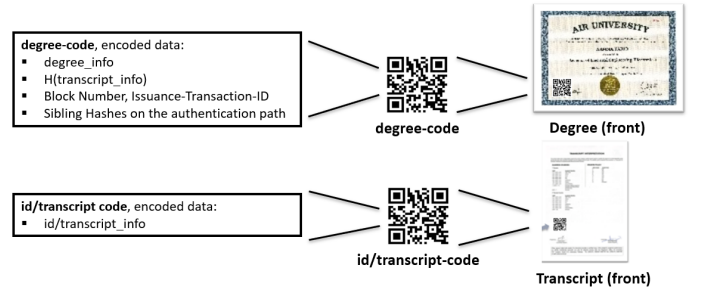Figure 3: Preparing the Credential

Figure 4: Issuance of Physical Certificates: degree-code and id/transcript-code

record. In our scheme, **universities** can institute further checks against insider malfeasance by deploying schemes like multi-signature wallets. This strategy requires the cooperation of additional personnel in different departments within the **university** to successfully create a valid transaction, for instance, the examination departments for the students' schools as well as the **university registrar**.

The insertion of the transaction in the blockchain serves as to accredit the **student credentials** with the **accreditation body**.

c) Issuance of the Physical Certificates: The physical certificates of the **credentials** and transcripts contain printed QR codes, enabling users to validate the information using the *batch_Merkle_root* on the blockchain.

Merkle trees have a useful property in that individual data items in the original set over which the tree is computed may be verified independently of the other data items if the 'authentication path' for the individual data items are available, i.e. those sibling nodes in the tree that share the same parent, on the path from the data item to the root. As an example, in Fig. 3, Alice's degree can be authenticated by hashing the contents of the degree, concatenating a hash of her transcript and identity documents, and then reconstructing the path up to the root, using the sibling nodes [2] (shaded in Fig. 3), and

---

[2]For illustration purposes, the figure shows, a Merkle tree of height 4 and the sibling hashes on the authentication path are also 4. The number of sibling hashes on the authentication path, are always equal to the height of the Merkle tree
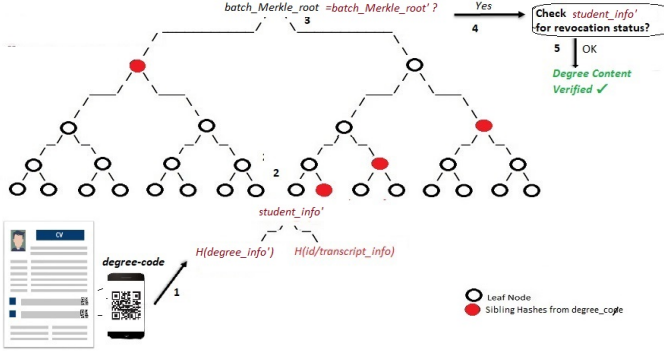
Figure 5: Degree content Verification

Figure 6: Rules Engine

then verifying that the signature on the transaction belongs to the **university**. All the information that a user requires to undertake this process is embedded in the QR codes imprinted on the degree certificate. We describe these next.

The first QR code, denoted *degree_code*, is used to verify the contents of the degree certificate, and encodes the following data:

- *degree_info*, i.e. text of student's name, serial number of the degree, title of degree/program, year of the award, and name of the university
- *H(id/transcript_info)*, i.e. a hash fingerprint of the data pertaining to the student's identity and transcript details, which is also necessary to reconstruct the authentication path for the *degree_info*
- the *block-number* and *issuance-transaction-ID* for the transaction that validates the specific degree
- the complete authentication path for the particular degree in the Merkle tree, i.e. all the *sibling-hashes* on the path leading up to the tree root

The second QR code, denoted *id/transcript_code*, can be used to verify the student's identity and the contents of her transcript, and encodes *id/transcript_info*, i.e. contents of student's identity document or identification number, and complete contents of her transcript. This code can be printed on the student's degree or transcript as per requirements.

We consider QR code specifications in detail in §. IV. Next we describe the verification process for students and **employers**.

C. Verification of the Credential

The verification process for contents of the degree and of the the identity and transcript data is very similar.

Contents of the degree are verified by scanning the *degree_code* using a verification app, imprinted on the physical copy of the degree or if embedded into a resume. The step-wise verification process is depicted in Fig. 5.

First, the user's app computes *degree_info'* using the plain-text degree contents information in the *degree_code*. *degree_info'* and *id/transcript_info* are then concatenated and hashed. The result is then repeatedly concatenated with the appropriate sibling nodes and hashed to reconstruct Merkle tree, i.e. *batch_Merkle_root'*. The app then queries the Cerberus blockchain (using the block number and transaction ID in *degree_code*) and checks if *batch_Merkle_root* matches *batch_Merkle_root'* which it has computed. If the match is positive, the contents of the degree are successfully verified.

Transcript contents are verified in a similar manner:

The **id/transcript_code** is scanned, and a **id/transcript_info'** generated by the app by hashing the plain-text transcript data in the code. Then the verifier manually enters the student's identity document number. These two items are concatenated and hashed to obtain a *H(id/transcript_info')*. If this regenerated *H(id/transcript_info')* matches the *H(id/transcript_info)* (used earlier when verifying the contents of the degree) then the transcript content is also verified.

D. Revoking a Credential

Now that we've discussed degree issuance and verification, we are in a position to describe the revocation process. In certain cases, universities or accreditation bodies may choose to revoke degrees. Cerberus implements efficient on-chain multiparty revocation using smart contracts. The revocation process involves two smart contracts, the *Rules Engine* which defines the precise rules according to which credentials may be revoked, Figure 6 and the *Implementation Engine*, which enforces these rules. These contracts are summarized in Fig. 7. The addresses of these contracts are explicitly embedded in the original transaction made by the university to register the credential as described earlier.

a) **Rules Engine***:*
- Only predefined nodes (belonging to the accreditation body and/or university) can execute this contract and participate in the revocation procedure. These nodes are listed in an *Authority-List*.

- Revocation must be approved by at least 2 nodes, in the Authority-List.
- The university and the accreditation body each have two pairs of keys. Revocation may be undertaken individually by the university or the accreditation body, or by both.
- A node in the Authority-List can only sign the revocation of a certificate once.
- Batch revocation is also possible in case the degree status of an entire batch of students needs to be revoked (may happened if the **university** fails to meet quality assurance criteria or if any irregularities are discovered by the **university** or **accreditation body**).

To revoke a credential, a node in the Authority-List initiates the revocation procedure, by invoking the Implementation Engine and providing the *student_info'*. In case of batch revocation, *(batch_Merkle_root)* is provided.

    b) **Implementation Engine***:*

- This contract verifies that *student_info'* matches one of the existing certificates on the blockchain.
- The contract then verifies that the node is listed in the Authority-List and issues a *process-hash* for the certificate, and increments a revocation counter.
- A second node in the Authority-List, using the *process-hash* generated in the previous step, also invokes the *Implementation Engine*.
- The *Implementation Engine* after verifying that the calling node is listed in the Authority-List, increments the revoke count again. It now stores *student_info* in a Revoke-List.

The verification process for the degree needs to be slightly modified to check for revocation status. In this case, the user's smartphone app invokes the *Implementation Engine* present in the transaction. This contract checks if **student_info'** is listed in the Revocation-list. If so, then it declares the **credential** as revoked.

IV. PROTOTYPE

The Accreditation Body and University nodes were run on desktop computers with the following specifications: CPU: Intel Core i7-3517U @ 1.90 GHz, Physical Memory: 4 GB DDR3 1600 MHz, OS: Ubuntu 13.04.e

The Students, Employers and Observers, can either use, a desktop computers, a laptop or even a smart phone. For our prototype we used one of each with the following specifications

- **Desktop** CPU: Intel Core i7-3517U @ 1.90 GHz, Physical Memory: 4 GB DDR3, OS: Ubuntu 13.04.e
- **Laptop** CPU: Intel Core i3-7100U @ 2.40 GHz, Physical Memory: 8 GB DDR3, OS: Microsoft Windows 10 Pro 10.0.17134
- **Smartphone** CPU: 1.2GHz dual-core Qualcomm Snapdragon 410, Physical Memory: 1 GB , OS: Android 4.4.4 (KitKat); Sense UI, Main Camera: 8 MP

We implemented our protoype on Parity, an Ethereum Client, Version 1.10.4-stable. Parity claims to be the fastest and most advanced Ethereum client [89]. Parity supports a

---

Contract Implementation Engine

Inputs: D_H, P_H
r = Rules Engine (adressRulesEngine)
Revoke Document (D_H):
call r.Rules (A.address)
if (r.Rules (A.address)=true):
    return (PH)
else
    terminate process
Confirm Revocation (P_H):
call r.Rules (A.address)
if (r.Rules (A.address)=true & Revoke count = requiredCount):
    call Revoke List (DH)
else
    terminate process
Revoke-List (D_H):
Revoke-List{} := D_H U Revoke List{}
Output: "PH", Revoke-List

D_H = Hash of Document P_H = Process Hash requiredCount = revocation count required for successful revocation

Figure 7: Implementation Engine

private blockchain network configuration, through a Proof-of-Authority consensus engine. Proof-of-Authority, a replacement for Proof-of-Work, uses a set authorities - nodes that are explicitly allowed to create new blocks and secure the blockchain. The transactions to become permanent record and included in the blockhain have to be signed off by the predefined Authority List. This makes it easier to maintain a private chain and keep the block issuers accountable. Ethereum Virtual Machine (EVM) is the runtime environment provided by Ethereum for the efficient execution of smart-contracts. Solidity Version 4.24, was used to code the smart contracts.

The data for all the students in a batch is input and converted to a JSON format file. These JSON files, are input to the Python program for data preparation. This program deploys SHA256 where ever a hash function is required, such as for fingerprinting the data, sibling hashes and merkle roots computation etc.

The required data for each QR code is input into an open-source QR code generator to create the QR codes to be printed on the credentials. Also an open source QR code reader was embedded into our Android app, and website interface.

A QR (Quick Response) Code consists of black modules arranged in a square grid on a white background, that offer a unique representation of data and can be read by an imaging device. There are various types of QR codes available, distinguished by the total number of black modules and the number of modules per unit area referred to as module density. The earliest and smallest QR code called version 1 was a 21X21 grid, while each subsequent version increases by 4x4. Other

distinguishing features include the level of error correction level achieved (through redundancy of data), the size of the QR Code, scanning distance, light and angle, and camera quality. It can encode numeric, alphanumeric and byte data. [90]. Each hash is 32 bytes long.

The amount of data in *degree_code* and *id/transcript_code* (for a batch of 100 students) is estimated to be around 800 alphanumeric characters, for which Table I shows the QR code specification and size. The equation for calculating the minimum size of the QR code is as follows: Minimum Size=(Scanning Distance/Distance Factor)x(Data Density/25) [90]. For our calculation the Distance Factor =10 was assigned.

Students in batch	Merkle Tree Height	Sibling Hashes (bytes)	degree_code Size (bytes)	Scanning Distance	QR Code Size (inches)
50	6	192 bytes	406 bytes	2" 4"	0.808" 1.616"
100	7	224 bytes	438 bytes	2" 4"	0.832" 1.664"
200	8	256 bytes	470 bytes	2" 4"	0.904" 1.808"
500	9	288 bytes	502 bytes	2" 4"	0.904" 1.808"
1000	10	320 bytes	534 bytes	2" 4"	0.936" 1.872"
2000	11	352 bytes	566 bytes	2" 4"	0.968" 1.965"
4000	12	384 bytes	596 bytes	2" 4"	0.968" 1.965"

Table I: Batch Size & QR Code Specification

V. DISCUSSION

In this section we discuss how our scheme counteracts common types of credential fraud described earlier in §.II-A and highlight its novel properties.

Cerberus safeguards Academic Credentials against modification and manipulation, undue access, while making them available to legitimate entities seeking to verify the existence of a record, and surety that it has not been altered or been revoked since. We separately reason how Cerberus prevents the occurrence of each type of Credential Fraud as defined previously in the II-A.

The permissioned blockchain architecture ensures strict separation of roles and privileges among the participating entities, preserves the integrity and chronological ordering of the credential record, and enables stakeholders to efficiently audit the operations of the system. If even one party on the network is honest, it can detect suspicious behavior by other entities and raise the alarm.

Counterfeit credentials and altered documents can easily be detected using this system. A fake credential will not have a corresponding record in the blockchain, whereas alterations of an original document will result in a different credential fingerprint which will not match the one on the blockchain.

However, our student, Alice, may bribe administrative staff in the university to falsify a credential on her behalf. Cerberus addresses this issue in two ways: first, due to the append-only property of the blockchain, even universities and accreditation bodies cannot insert backdated records into the ledger. Rewriting entire blocks to retroactively add data would require the university to actively collude with the accreditation authority, and this activity would be visible to all other parties on the blockchain.

At best, Alice, can influence staff members to insert a falsified record for her in the next upcoming batch on the blockchain. This concern may also be mitigated if the university were to define multi-signature policies for registering credentials on the blockchain. In this case, for example, creating a transaction would require the university registrar as well as administrative staff in the relevant department within the university to independently vet and sign the transaction. Alice would therefore have to bribe multiple disassociated parties to procure a fake credential, which will hopefully require considerably more effort.

Likewise, this solution would address the problem of diploma mills. Any new university wishing to join the network would first have to be thoroughly vetted by the accreditation body which would certify the university's public key, thereby allowing the university to make transactions. Non-approved entities such as fake universities, by default, would not be able to publish any data on the blockchain.

Combating fake accreditation agencies is more complex, as a resourceful attacker might set up an entire blockchain network himself to validate his fake credentials. In the context of a single nationwide or regional accreditation service, there should ideally be no confusion regarding which accreditation body is legitimate. In areas where accreditation services are privatized, the situation can perhaps be mitigated by requiring accreditation bodies to include legitimating information on the blockchain itself, such as a license to operate or a statement of authorization from relevant government ministries or reputed education watchdog bodies. The presence of reputed activist and watchdog bodies which have joined the network as observers will add to the legitimacy of the accreditation body.

Cerberus has other fundamental advantages over legacy credential verification solutions. First and foremost, the blockchain is integrated into the credential issuance process itself, thereby enabling *accreditation-by-default* in a sense. The verification process consists of only a simple lookup on the blockchain. This process dispenses with time-consuming and cumbersome paperwork that is typical in existing systems and can be undertaken in real-time using computers and smartphones. Students and employers can verify the provenance and authenticity of credentials themselves and at their convenience without relying on third parties or requiring specialized technical skills or maintaining cryptographic keys.

Privacy of student data is maintained since no actual data is put on the blockchain but only data fingerprints. These are computed using one-way hash functions thereby disassociating the process of validation of the data from the data itself. No third party is therefore able to deduce students' degree details or information from the blockchain alone without also

accessing the authentication path data that is printed on the physical certificates. Cerberus enables the student to exercise personal control over this data and share it with various parties to undertake verification.

Selective disclosure is also facilitated in that the student can share an individual data item (degree data or identification data and transcript contents) and it's authentication path with a third party without having to reveal to them all the original data items.

Cerberus also significantly improves on state-of-the-art blockchain-based credential verification solutions proposed in the literature. We discuss these next.

VI. Related Work

Legacy credential verification procedures typically rely on university databases and unique codes (pin numbers and hashing) and anti-counterfeiting technology to establish the credibility of a document [93], [94], [95]. Some solutions associate user profiles and education records with a single identity [96] [97]. These systems have numerous weaknesses: there is systematic redundancy, tedious paperwork, and cumbersome processes, resulting in extensive effort, cost, and delays. There is little standardization. Moreover loopholes for fraud and crime persist, as documented in §. II-A.

It is widely acknowledged that the blockchain can play a pivotal role in resolving many of these issues. Various startups and companies now offer **credential verification on the blockchain**, e.g. Appii [98], Gradba [99], Aversafe [52], Verify [100], Accredible [101], TrueRec [102], and Bcdiploma [103]. Efforts are also underway to build **blockchain-backed credential verification solutions at the national level** in Malaysia [104] and India [105].

Academic researchers have made significant contributions in this domain and have proposed various new features and optimizations. A pioneering effort in this regard was made by the **University of Nicosia (UNIC)** in 2015, when it became the first educational institution to issue academic certificates (for its Digital Currencies course) on the Bitcoin blockchain [106]. Since 2017, UNIC has issued all university diplomas on the Bitcoin blockchain. Their solution is to issue the student a digitally signed PDF file of the credential. The hash of this file is inserted in the OP_RETURN field of a Bitcoin transaction.

Another prominent example is **Blockcerts**, an initiative of the MIT Media Lab, which similarly inserted credential verification information in the Bitcoin OP_RETURN field and the Ethereum extraData field. Blockcerts also supported batch issuance of credentials using Merkle trees.

Blockcerts had two key shortcomings: first, it required students to maintain cryptographic keys, and, second, it maintained credential revocation lists on a centralized website which could theoretically be compromised. To resolve the second issue, researchers proposed **Hypercerts**, a distributed and trustless credential revocation mechanism, which relies on Ethereum smart contracts and the InterPlanetary File System (IPFS), a decentralized data storage solution [107].

Solutions that followed contributed further to developing scope, features, and application. For instance, **EduCTX** proposes a unified global higher education credit and grading system based on the European Credit Transfer and Accumulation System (ECTS), in which coins are transferred on the blockchain to signify academic study credits attained by students [54]. This solution, built on the ARK platform, also requires students to maintain cryptographic keys.

EchoLink stores user identities and academic credentials on-chain via smart contracts for a range of blockchain platforms, including Ethereum, AntShares, Metaverse, etc. [108] It's goal is to build a professional networking and recruiting platform, providing easy access to a pool of vetted candidates. EchoLink does not have a revocation mechanism.

UZHBC (University of ZuricH BlockChain) is a blockchain-based verification system, specifically for diplomas issued by the University of Zurich [109]. It uses the public Ethereum blockchain and employs a smart contract for both issuance and verification functions, and accepts a PDF of the credential as input. Likewise, **Blockchain for Education** also uses the public Ethereum blockchain and smart contracts for access control and certificate management [53]. The Interplanetary Filesystem supplements this system by providing users access to profile information of certification authorities.

These systems have various limitations: for instance, UNIC and UZHBC are limited in scope to their parent institution and EchoLink is only available to registered users. Most of these solutions do not incorporate accreditation bodies (with the notable exception of EduCTX and Blockchain for Education), which leaves open the issue of university staff falsifying records and the problem of diploma mills.

Most of these systems preserve privacy of student data. EchoLink is the notable exception since it is recruiting platform and offers viewing access to registered users.

The issue of scalability is only addressed by Blockcerts, which offers a batch issuance mechanism. Other systems rely on separate transactions per student which add to transaction costs and contribute to blockchain-bloat when deployed on public blockchains.

Moreover, the significant problem of certificate revocation, is only satisfactorily addressed by two systems: Hypercerts which relies on the InterPlanetary File System network, and by Blockchain for Education which claims to use smart contracts for revocation (implementation details are not provided).

In addition, many systems, notably Blockcerts, EchoLink and EduCTX, require students and verifiers to maintain cryptographic credentials or digital identities to participate in the ecosystem and avail the verification service. This complicates the user experience as has been documented in multiple studies in the literature.

We compare key properties of these solutions with our work in II. Cerberus makes significant new contributions: for one, our solution adheres closely to the established ecosystem and enables an extra layer of oversight by incorporating accreditation authorities and independent observer and watchdog bodies. This is an effective check against documented real-world problems such as that of corrupt university staff and the phenomenon of diploma mills.

Cerberus relies on batch issuance and is therefore scalable and can function as a university, consortium, or national-level solution. Our revocation scheme is also unique in that

Scheme	System Features			Security Features				Usability		
	Accreditation	Verification	Revocation	CounterfeitProtection	Privacy	Selective Disclosure	Transparency	UserExperience	No KeyManagement	Accessibility
UNIC[106]	-	◐		◐	●	-	●	●	●	●
Blockcerts*[55]	-	●	◐	◐	●	-	●	●	-	●
Hypercert[107]	-	●	◐	◐	●	-	●	●	-	●
Echo†[108]	-	◐		◐	-	-	●	◐	-	◐
UZHBC†[109]	-	◐		◐	●	-	●	●	●	●
EduCtx†[54]	●	◐		●	●	-	◐	◐	-	◐
Blockchain for Education†[53]	●	●	◐	●	●	-	●	●	●	●
Cerberus	●	●	●	●	●	●	●	●	●	●

●= provides property; ◐= partially provides property; - = does not provide property
†= has academic publication; * = end-user tool available

Table II: Summary comparison of various solutions

it is on-chain and is a multi-party scheme, making it harder to abuse. Cerberus also maintains privacy of user data and offers students the novel facility of selective disclosure of their verification information as per requirements.

A key advantage of Cerberus over prior solutions is in terms of usability. Verification is an intuitive process which simply requires scanning QR codes. Users do not have to maintain digital identities or cryptographic credentials. QR codes are easy and intuitive to use. Students can even distribute the codes on their resumes and circulate them publicly if they choose, enabling verification without the physical credential.

Finally, Cerberus is a private and permissioned system, which, in contrast to public blockchains, enables more streamlined management and enforcement of policy and rules, and the system can be upgraded to cater to the changing requirements of the ecosystem.

VII. Future Work

Here we describe possibilities for enhancing Cerberus and adding new features.

One straightforward addition is to link multiple credentials or qualifications undertaken by a student such that verifying the most recent one ensures that all her previous credentials are also genuine. This can be easily incorporated, by including hashes of the earlier credentials in the transaction for her recent credential. This would simplify the verification process in cases multiple qualifications in the candidate's history need to be verified.

Second, Cerberus is a private network, and as an additional integrity check, periodic snapshots of the Cerberus blockchain can be anchored to a public blockchain, such as Bitcoin, Ethereum etc. A convenient option for the snapshot would be the hash of the latest block. This provides security against malicious forks and history revision attacks if all parties in the network collude and insert data retroactively in the blockchain [117]. Blocks may only be considered part of the canonical record if they build on top of the most recent block snapshots.

Furthermore, as blockchain-based solutions permeate management and governance structures (as has been predicted [118]), we anticipate there will be solutions for various public records (e.g. identity-information, health, education, driving license, passport, criminal records, etc.). This may eventually give rise to overarching records management systems, which link multiple blockchains in the background as *sidechains* to a main chain, enabling them to securely and efficiently exchange information and present a unified and integrated platform.

A relevant example is IndiaChain, a high-level blockchain platform with which other sidechains are expected to interface [105]. Various sidechain protocols have been proposed to date [110] [111] [112] include prominent projects such as Rootstock [113] and Elements [114] that are sidechains linking to the Bitcoin network. This architecture introduces modularity in the system as well as obvious advantages of scalability and interoperability. Whereas interoperability protocols are still at a nascent stage in their development [115] [116], it would be interesting to devise integration solutions for Cerberus in a unified platform and investigate new features and opportunities of such a step.

VIII. Conclusion

Credential fraud is a widespread and pervasive practice that undermines confidence in educational institutions, impairs social development, and involves significant economic costs. Unfortunately, legacy credential verification systems are time-consuming, costly, and cumbersome. Moreover, they are not very effective against certain widespread corrupt practices, including fraud on the part of educational institutions and accreditation bodies.

In this paper we have proposed Cerberus, a comprehensive blockchain-based solution which counters widespread instances of fraud, as well as offers dramatic improvements over legacy systems in terms of usability and efficiency. Cerberus also offers distinct benefits over existing blockchain-based solutions proposed in the literature and in industry. Our solution

integrates effectively with the existing credential verification ecosystem, it includes a novel on-chain credential revocation mechanism, and does not require students or employers to maintain cryptographic credentials.

We hope this work contributes positively to ongoing and future efforts towards alleviating the phenomenon of credential fraud.

REFERENCES

[1] Haveman, Robert, and Timothy Smeeding. "The role of higher education in social mobility." The Future of children (2006): 125-150.

[2] Brown, Phillip. "Education, opportunity and the prospects for social mobility." British Journal of Sociology of Education 34, no. 5-6 (2013): 678-700.

[3] Hanushek, Eric A., and Ludger Woessmann. "Education and economic growth." Economics of education (2010): 60-67.

[4] Hanushek, Eric A., and Dennis D. Kimko. "Schooling, labor-force quality, and the growth of nations." American economic review 90, no. 5 (2000): 1184-1208.

[5] Coulombe, Serge, Jean-François Tremblay, and Sylvie Marchand. Literacy scores, human capital and growth across fourteen OECD countries. Ottawa: Statistics Canada, 2004.

[6] Schweinhart, L., and Z. Xiang. "Evidence that the High/Scope Perry Preschool program prevents adult crime." In American Society of Criminology Conference. 2003.

[7] Verba, Schlozman. "Brady 1995 Verba S., Schlozman KL, Brady HE Voice and Equality." (1995).

[8] Reimers, Fernando. "Citizenship, identity and education: Examining the public purposes of schools in an age of globalization." Prospects 36, no. 3 (2006): 275-294.

[9] Barro, Robert J. "Human capital and growth." American economic review 91, no. 2 (2001): 12-17.

[10] Cardenas-Denham, Sergio. "Corruption in Education: A Review of the Literature." PhD diss., Harvard Graduate School of Education, 2007.

[11] Transparency International. Global corruption report: Education. Taylor & Francis, 2013. Available: https://www.transparency.org/whatwedo/publication/global_corruption_report_education. [Accessed: 11- Sep- 2018].

[12] Grolleau, Gilles, Tarik Lakhal, and Naoufel Mzoughi. "An introduction to the economics of fake degrees." Journal of Economic Issues 42, no. 3 (2008): 673-693.

[13] "Cat Gets MBA Degree - Money News Story - WCAU | Philadelphia", Web.archive.org, 2019. [Online]. Available: https://web.archive.org/web/20071026103729/http://www.nbc10.com/money/3975070/detail.html. [Accessed: 19- Feb- 2019].

[14] "Education: Sending Degrees to the Dogs", TIME.com, 2019. [Online]. Available: http://content.time.com/time/magazine/article/0,9171 ,954229-1,00.html. [Accessed: 19- Feb- 2019].

[15] "Lying on your resume", Monster Career Advice, 2018. [Online]. Available: https://www.monster.com/career-advice/article/lying-on-your-resume. [Accessed: 28- Feb- 2018].

[16] D. Davis, "Unizulu professor's murder linked to fake PhD syndicate at university", Briefly, 2019. [Online]. Available: https://briefly.co.za/20375-unizulu-professors-murder-linked-fake-phd-syndicate-university.html. [Accessed: 19- Feb- 2019].

[17] Ezell, A. (2015, November 10). The "Axact" Scam and the Big Business of Credential Fraud [webinar]. American Association of Collegiate Registrars and Admissions Officers

[18] "Doctors fake degrees score reaches 38", Thenews.com.pk, 2019. [Online]. Available: https://www.thenews.com.pk/archive/print/248189-doctors-fake-degrees-score-reaches-38. [Accessed: 19- Feb- 2019].

[19] C. Turner, "NHS consultants and nurses accused of buying fake degrees online", The Telegraph, 2019. [Online]. Available: https://www.telegraph.co.uk/education/2018/01/16/nhs-consultants-nurses-accused-buying-fake-degrees-online/. [Accessed: 19- Feb- 2019].

[20] "24 PIA pilots held fake degrees, CAA informs SC | The Express Tribune", The Express Tribune, 2019. [Online]. Available: https://tribune.com.pk/story/1706726/1-24-active-pia-pilots-fake-degrees-caa-informs-sc/. [Accessed: 19- Feb- 2019].

[21] "Fake degree holders deserve no compassion: CJP | The Express Tribune", The Express Tribune, 2019. [Online]. Available: https://tribune.com.pk/story/1884489/1-sc-disposes-pia-fake-degrees-case/. [Accessed: 19- Feb- 2019].

[22] "Politicians, Fake Degrees and Plagiarism | Inside Higher Ed", Insidehighered.com, 2018. [Online]. Available: https://www.insidehighered.com/blogs/world-view/politicians-fake-degrees-and-plagiarism. [Accessed: 05- Dec- 2018].

[23] "Breaking down Russia's culture of fake degrees", Radio National, 2016. [Online]. Available: https://www.abc.net.au/radionational/programs/latenightlive/breaking-down-russias-culture-of-fake-degrees/7482698. [Accessed: 19- Feb- 2019].

[24] "SA MP resigns over fake degree", BBC News, 2019. [Online]. Available: https://www.bbc.com/news/world-africa-28745435. [Accessed: 19- Feb- 2019].

[25] "China Qualifications Verification", Chinadegrees.cn, 2019. [Online]. Available: https://www.chinadegrees.cn/en/. [Accessed: 19- Feb- 2019].

[26] "Degree Attestation System", Hec.gov.pk, 2019. [Online]. Available: http://hec.gov.pk/english/services/students/Degree%20Attestation%20System/Pages/Degree-Attestation.aspx. [Accessed: 19- Feb- 2019].

[27] Vak.ed.gov.ru, 2019. [Online]. Available: http://vak.ed.gov.ru/87. [Accessed: 19- Feb- 2019].

[28] "Home | Council for Higher Education Accreditation", Chea.org, 2019. [Online]. Available: https://www.chea.org/. [Accessed: 19- Feb- 2019].

[29] "Tertiary Education Quality and Standards Agency", Teqsa.gov.au, 2019. [Online]. Available: https://www.teqsa.gov.au/. [Accessed: 19- Feb- 2019].

[30] "Apostille Convention", En.wikipedia.org, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Apostille_Convention. [Accessed: 15- Sep- 2018].

[31] (IAU), "World Higher Education Database (WHED) Portal", Whed.net, 2018. [Online]. Available: https://whed.net/home.php. [Accessed: 15- Sep- 2018].

[32] R. Garner, "A third of employers never check job applicants' qualifications,", The Independent, 2014. [Online]. Available: https://www.independent.co.uk/news/education/education-news/a-third-of-employers-never-check-job-applicants-qualifications-survey-finds-9681286.html. [Accessed: 12- Sep- 2018].

[33] London, "Aversafe Meets Global Market Needs – Aversafe", Aversafe, 2018. [Online]. Available: https://blog.aversafe.com/aversafe-meets-global-market-needs-6a7489ef67fe. [Accessed: 12- Sep- 2018].

[34] "Ripple - One Frictionless Experience To Send Money Globally | Ripple", Ripple, 2019. [Online]. Available: https://ripple.com/. [Accessed: 19- Feb- 2019].

[35] "Stellar - Develop the world's new financial system", Stellar, 2019. [Online]. Available: https://www.stellar.org/. [Accessed: 19- Feb- 2019].

[36] "Binded: Copyright made simple", Binded.com, 2018. [Online]. Available: https://binded.com/. [Accessed: 15- Feb- 2018]

[37] "Artists & Creators | ascribe", ascribe, 2018. [Online]. Available: https://www.ascribe.io/. [Accessed: 15- Feb- 2018]

[38] "Bitcoin.com", Notary.bitcoin.com, 2018. [Online]. Available: https://notary.bitcoin.com/. [Accessed: 11- Jan- 2018]

[39] "Proof of Existence", Proofofexistence.com, 2018. [Online]. Available: https://www.proofofexistence.com/. [Accessed: 05- Dec- 2018].

[40] J. Young, "Sweden Officially Started Using Blockchain to Register Land and Properties", Cointelegraph, 2019. [Online]. Available: https://cointelegraph.com/news/sweden-officially-started-using-blockchain-to-register-land-and-properties. [Accessed: 19- Feb- 2019].

[41] "Blockchain | Smart Dubai", Smartdubai.ae, 2019. [Online]. Available: https://www.smartdubai.ae/initiatives/blockchain. [Accessed: 19- Feb- 2019].

[42] Ølnes, Svein, and Arild Jansen. "Blockchain Technology as s Support Infrastructure in e-Government." In International Conference on Electronic Government, pp. 215-227. Springer, Cham, 2017.

[43] Hou, Heng. "The Application of Blockchain Technology in E-Government in China." In Computer Communication and Networks (ICCCN), 2017 26th International Conference on, pp. 1-4. IEEE, 2017.

[44] Azaria, Asaph, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. "Medrec: Using blockchain for medical data access and permission management." In Open and Big Data (OBD), International Conference on, pp. 25-30. IEEE, 2016.

[45] Xia, Qi, Emmanuel Boateng Sifah, Kwame Omono Asamoah, Jianbin Gao, Xiaojiang Du, and Mohsen Guizani. "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain." IEEE Access 5 (2017): 14757-14767.

[46] Mettler, Matthias. "Blockchain technology in healthcare: The revolution starts here." In e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on, pp. 1-3. IEEE, 2016.

[47] Shae, Zonyin, and Jeffrey JP Tsai. "On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine." In Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on, pp. 1972-1980. IEEE, 2017.

[48] "Blockfreight, Inc. [BFT:XCPC]", Blockfreight, Inc. [BFT:XCPC], 2019. [Online]. Available: https://blockfreight.com/. [Accessed: 19- Feb- 2019].

[49] "Everledger | A Digital Global Ledger", Everledger.io, 2018. [Online]. Available: https://www.everledger.io/. [Accessed: 7- Jan- 2018]

[50] "Agora", Agora, 2019. [Online]. Available: https://www.agora.vote/. [Accessed: 19- Feb- 2019].

[51] "The Online Voting Platform of The Future - Follow My Vote", Follow My Vote, 2019. [Online]. Available: https://followmyvote.com/. [Accessed: 19- Feb- 2019].

[52] "Decentralized credential verification", Aversafe - Decentralized Credential Verification, 2018. [Online]. Available: https://www.aversafe.com/. [Accessed: 05- Dec- 2018].

[53] Kolvenbach, Sabine, Rudolf Ruland, Wolfgang Gräther, and Wolfgang Prinz. "Blockchain 4 Education." In Proceedings of 16th European Conference on Computer-Supported Cooperative Work-Panels, Posters and Demos. European Society for Socially Embedded Technologies (EUSSET), 2018.

[54] Turkanović, Muhamed, Marko Hölbl, Kristjan Košič, Marjan Heričko, and Aida Kamišalić. "EduCTX: A blockchain-based higher education credit platform." IEEE Access (2018).

[55] "Blockchain Credentials", Blockcerts, 2018. [Online]. Available: https://www.blockcerts.org/. [Accessed: 11- Jan- 2018].

[56] "Check visa details and conditions", Immi.homeaffairs.gov.au, 2019. [Online]. Available: https://immi.homeaffairs.gov.au/visas/already-have-a-visa/check-visa-details-and-conditions/check-conditions-online. [Accessed: 19- Feb- 2019].

[57] "Use the Employer Checking Service", GOV.UK, 2019. [Online]. Available: https://www.gov.uk/employee-immigration-employment-status. [Accessed: 19- Feb- 2019].

[58] "Home", E-Verify, 2019. [Online]. Available: https://www.e-verify.gov/. [Accessed: 19- Feb- 2019].

[59] Zaretskiy, Yury. "Fake Academic Degrees in the 18th Century?." (2016).

[60] Johnson, Creola. "Credentialism and the proliferation of fake degrees: The employer pretends to need a degree; the employee pretends to have one." Hofstra Lab. & Emp. LJ 23 (2005): 269.

[61] N. Clarke, "Understanding Transnational Education, Its Growth and Implications - WENR", WENR, 2018. [Online]. Available: https://wenr.wes.org/2012/08/wenr-august-2012-understanding-transnational-education-its-growth-and-implications. [Accessed: 11- Sep- 2018].

[62] S. Trines, "Academic Fraud, Corruption, and Implications for Credential Assessment", WENR, 2018. [Online]. Available: https://wenr.wes.org/2017/12/academic-fraud-corruption-and-implications-for-credential-assessment. [Accessed: 11- Sep- 2018].

[63] Mohamedbhai, Goolam. "The scourge of fraud and corruption in higher education." International Higher Education 84 (2016): 12-14.

[64] Cohen, Eyal Ben, and Rachel Winch. "Diploma and accreditation mills: New trends in credential abuse." Bedford: Verifile Accredibase (2011).

[65] Ezell, Allen, and John Bear. Degree mills: The billion-dollar industry that has sold over a million fake diplomas. Pyr Books, 2005.

[66] Bear, John. Degree Mills: The Billion-Dollar Industry That Has Sold Over a Million Fake Diplomas. Prometheus Books, 2012.

[67] Henry, "University of Wales abolished after visa scandal", Telegraph.co.uk, 2018. [Online]. Available: https://www.telegraph.co.uk/education/educationnews/8843200/University-of-Wales-abolished-after-visa-scandal.html. [Accessed: 04- Dec- 2018].

[68] G Altbach, P. (2012). Taking on corruption in international higher education. [online] University World News. Available at: https://www.universityworldnews.com/post.php?story=20120717134058780 [Accessed 28 Feb. 2019].

[69] "Degree certificate racket thrives in Bengaluru", The Hindu, 2018. [Online]. Available: https://www.thehindu.com/news/cities/bangalore /degree-certificate-racket-thrives-in-bengaluru/article19127959.ece?utm_content=buffer69bc3&utm_medium=Social&utm_source=twitter.com&utm_campaign=buffer. [Accessed: 04- Dec- 2018].

[70] Gitanjali, B. "Academic dishonesty in Indian medical colleges." Journal of postgraduate medicine 50, no. 4 (2004): 281.

[71] "Tomar's law degree is indeed fake, Smriti's case is different." 9 June. Available: http://www.rediff.com/news/report/tomars-lawdegree-is-indeed-fake-smritis-case-is-different/20150609.htm (Accessed 04- Dec- 2018).

[72] "CVC Nigeria - Committee of Vice Chancellors of Nigerian Universities.", Cvcnigeria.org, 2018. [Online]. Available: https://www.cvcnigeria.org/view.php?id=66. [Accessed: 04- Dec- 2018].

[73] D. Schemo, "Diploma Mill Concerns Extend Beyond Fraud", Nytimes.com, 2018. [Online]. Available: https://www.nytimes.com/2008/06/29/us/29diploma.html. [Accessed: 04- Dec- 2018].

[74] Barigaba, J. (2016). Uganda: Scandal - How Ugandan Varsity Awarded 1,000 Sudan Sudanese Degrees in Months. [online] All Africa. Available at: https://allafrica.com/stories/201611290869.html [Accessed 28 Feb. 2019].

[75] D. Asad, "Axact CEO, 22 others sentenced to 20 years in jail in fake degrees case", DAWN.COM, 2018. [Online]. Available: https://www.dawn.com/news/1418156. [Accessed: 04- Dec- 2018].

[76] Cheema, U. (2018). Axact fraud case: FIA report raises questions about FIA. [online] Thenews.com.pk. Available at: https://www.thenews.com.pk/print/277439-axact-fraud-case-fia-report-raises-questions-about-fia [Accessed 28 Feb. 2019].

[77] "FIA probing fake degrees attestation by HEC officials", Thenews.com.pk, 2019. [Online]. Available: https://www.thenews.com.pk/print/392649-fia-probing-fake-degrees-attestation-by-hec-officials. [Accessed: 20- Feb- 2019].

[78] Stecklow, S. (2017). Exclusive: Chinese firm withdraws from U.S. effort to fight college.... [online] U.S. Available at: https://www.reuters.com/article/us-usa-college-dipont-idUSKBN1521QT [Accessed 28 Feb. 2019].

[79] "Connecticut Man Pleads Guilty In Multi-Million Dollar Diploma Fraud", Justice.gov, 2019. [Online]. Available: https://www.justice.gov/usao-edpa/pr/connecticut-man-pleads-guilty-multi-million-dollar-diploma-fraud. [Accessed: 20- Feb- 2019].

[80] Mainelli, Michael, and Alistair Milne. "The impact and potential of blockchain on the securities transaction lifecycle." (2016).

[81] Kim, Henry M., and Marek Laskowski. "Toward an ontology-driven blockchain design for supply-chain provenance." Intelligent Systems in Accounting, Finance and Management 25, no. 1 (2018): 18-27.

[82] Griggs, Kristen N., Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson, and Thaier Hayajneh. "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring." Journal of medical systems 42, no. 7 (2018): 130.

[83] Clark, Jeremy, Joseph Bonneau, Edward W. Felten, Joshua A. Kroll, Andrew Miller, and Arvind Narayanan. "On decentralizing prediction markets and order books." In Workshop on the Economics of Information Security, State College, Pennsylvania. 2014.

[84] Eskandari, Shayan, Jeremy Clark, David Barrera, and Elizabeth Stobert. "A first look at the usability of bitcoin key management." arXiv preprint arXiv:1802.04351 (2018).

[85] Krombholz, Katharina, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl. "The other side of the coin: User experiences with bitcoin security and privacy." In International Conference on Financial Cryptography and Data Security, pp. 555-580. Springer, Berlin, Heidelberg, 2016.

[86] "DigiLocker - Online document storage facility | National Portal of India", India.gov.in, 2018. [Online]. Available: https://www.india.gov.in/spotlight/digilocker-online-document-storage-facility. [Accessed: 04- Dec- 2018].

[87] "Penerima Ijazah Kehormat dan Ijazah Kedoktoran di Universiti Malaysia / Honorary Degree and Doctorate (PhD) Holders at Malaysian Universities", 2018. [Online]. Available: http://waecdirect.org/. [Accessed: 04- Dec- 2018]. http://dohe.mohe.gov.my/award/

[88] Merkle, Ralph C. "A digital signature based on a conventional encryption function." In Conference on the theory and application of cryptographic techniques, pp. 369-378. Springer, Berlin, Heidelberg, 1987.

[89] "Parity Documentation - Parity Technologies", Wiki.parity.io, 2018. [Online]. Available: https://wiki.parity.io/. [Accessed: 29- Sep- 2018].

[90] Qrcode.com. (2019). Information capacity and versions of QR Code | QRcode.com | DENSO WAVE. [online] Available at: https://www.qrcode.com/en/about/version.html [Accessed 25 Jun. 2019].

[91] Dinh, Tien Tuan Anh, Ji Wang, Gang Chen, Rui Liu, Beng Chin Ooi, and Kian-Lee Tan. "Blockbench: A framework for analyzing private blockchains." In Proceedings of the 2017 ACM International Conference on Management of Data, pp. 1085-1100. ACM, 2017.

[92] Dinh, Tien Tuan Anh, Rui Liu, Meihui Zhang, Gang Chen, Beng Chin Ooi, and Ji Wang. "Untangling blockchain: A data processing view of blockchain systems." IEEE Transactions on Knowledge and Data Engineering 30, no. 7 (2018): 1366-1385.

[93] Sharma, Smita. "Certisafe, a novel Credential Authentication Process and System (CAPS)." U.S. Patent Application 14/349,363, filed March 12, 2015.

[94] Malkawi, Mohammad Isam. "Counterfeit Prevention and Detection of University and Academic Institutions Documents Using Unique Codes." U.S. Patent Application 15/594,615, filed December 7, 2017.

[95] Digital Credential Service | Parchment", Parchment, 2018. [Online]. Available: http://www.parchment.com/. [Accessed: 04- Dec- 2018].

[96] "Badgr", Badgr.com, 2018. [Online]. Available: https://badgr.com/. [Accessed: 04- Dec- 2018].

[97] "Open Badges Homepage", Openbadges.org, 2018. [Online]. Available: https://openbadges.org/. [Accessed: 04- Dec- 2018].

[98] "World's first blockchain career verification platform | APPII", APPII, 2018. [Online]. Available: https://appii.io/. [Accessed: 05- Dec- 2018].

[99] T. team, "Gradbase - Instantly Verify Qualifications", Gradba.se, 2018. [Online]. Available: https://www.gradba.se/en/. [Accessed: 17- Jan- 2018].

[100] Zabar, Ed Adi. "Verification System." U.S. Patent Application 14/231,852, filed October 9, 2014.

[101] "Home", Accredible, 2018. [Online]. Available: https://www.accredible.com/. [Accessed: 05- Dec- 2018].

[102] Tummuru, Nethaji, Surbhi Sheth-Shah, Michael Kunzmann, Sanjay Shirole, and Jun Meng. "Decentralized credentials verification network." U.S. Patent Application 15/385,479, filed March 22, 2018.

[103] BCDiploma", Bcdiploma.com, 2018. [Online]. Available: https://www.bcdiploma.com/. [Accessed: 05- Dec- 2018].

[104] A. Abas, "University consortium set up to authenticate degrees using blockchain technology", Nst.com.my, 2018. [Online]. Available: https://www.nst.com.my/news/nation/2018/11/429615/university-consortium-set-authenticate-degrees-using-blockchain. [Accessed: 27- Jun- 2019].

[105] Bansia, M., Murali, A., Murali, A. and Sen, S. (2019). India readies its biggest deep tech bet yet: a UPI-like blockchain platform | FactorDaily. [online] FactorDaily. Available at: https://factordaily.com/india-readies-upi-like-blockchain-platform/ [Accessed 27 May 2019].

[106] "Academic Certificates on the Blockchain", UNIC Blockchain Initiative, 2018. [Online]. Available: https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/. [Accessed: 10- Jan- 2018].

[107] Kim Hamilton Duffy, Learning Machine, Hypercerts: Blockcerts Revocation Improvements- By João Santos, Instituto Superior Técnico,

[108] Chen, S.X. and Team, E., Blockchain Based Professional Networking and Recruiting Platform.

[109] Gresch, Jerinas, Bruno Rodrigues, Eder Scheid, Salil S. Kanhere, and Burkhard Stiller. "The Proposal of a Blockchain-based Architecture for Transparent Certificate Handling."

[110] Androulaki, Elli, Christian Cachin, Angelo De Caro, and Eleftherios Kokoris-Kogias. "Channels: Horizontal scaling and confidentiality on permissioned blockchains." In European Symposium on Research in Computer Security, pp. 111-131. Springer, Cham, 2018.

[111] Kokoris-Kogias, Eleftherios, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ewa Syta, and Bryan Ford. "Omniledger: A secure, scale-out, decentralized ledger via sharding." In 2018 IEEE Symposium on Security and Privacy (SP), pp. 583-598. IEEE, 2018.

[112] Joseph Poon and Vitalik Buterin. "Plasma: Scalable Autonomous Smart Contracts" Available at: [https://plasma.io/]

[113] RSK - Smart Contract Platform Secured by the Bitcoin Network ", Rsk.co, 2019. [Online]. Available: https://www.rsk.co/. [Accessed: 30- Jun- 2019].

[114] "Elements", elementsproject.org, 2019. [Online]. Available: https://elementsproject.org/. [Accessed: 30- Jun- 2019].

[115] Deng, Liping, Huan Chen, Jing Zeng, and Liang-Jie Zhang. "Research on Cross-Chain Technology Based on Sidechain and Hash-Locking." In International Conference on Edge Computing, pp. 144-151. Springer, Cham, 2018.

[116] Kan, Luo, Yu Wei, Amjad Hafiz Muhammad, Wang Siyuan, Gao Linchao, and Hu Kai. "A multiple blockchains architecture on inter-blockchain communication." In 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), pp. 139-145. IEEE, 2018.

[117] Barber, Simon, Xavier Boyen, Elaine Shi, and Ersin Uzun. "Bitter to better—how to make bitcoin a better currency." In International Conference on Financial Cryptography and Data Security, pp. 399-414. Springer, Berlin, Heidelberg, 2012.

[118] ansiti, M. and R. Lakhani, K. (2017). The Truth About Blockchain. [online] Harvard Business Review. Available at: https://hbr.org/2017/01/the-truth-about-blockchain [Accessed 1 Jul. 2019].