Swiss EduChain Project Proposal

Christian Killer, Eder Scheid, Bruno Rodrigues, Geetha Parangi, Burkhard Stiller
Communication Systems Group CSG, Department of Informatics IfI,
Universität Zürich UZH, Binzmühlestrasse 14, CH-8050 Zürich
E-mail: [killer,scheid,rodrigues,parangi,stiller]@ifi.uzh.ch

***Abstract*—Diplomas, serving as official proofs for education, have a high importance in todays knowledge society. Unfortunately, the forgery of academic certificates has become frequent and evident. Normally, third parties (*e.g.* Employers) manually verify the documents by contacting the Issuers. In recent years, the emergence of immutable and decentralized public blockchains can offer a platform to create a new and efficient way to exchange and validate information. Thus, this proposal outlines a potential design of a Swiss EduChain system to simplify the process of the issuance and verification of academic certificates. While the initial use-case scope entails digital diplomas, the data structure should be data-agnostic, not restricted to academic certificates, but extensible to other structured data such as a Curriculum Vitae (CV), recommendation letters, scientific publications, attributions of attendance, including all forms of publicly verifiable data.**

I. Introduction

Academic certificates have major relevance in the labor market, signaling capability and the level of education and skills of the recipient. Unfortunately, recent years have seen an increase in fraud, ranging from inflating academic grades to fake diplomas. Several organizations focus on providing illegitimate academic degrees and diplomas (also called *diploma mills*. Globally estimating the number of individuals with fake diplomas is a hard task. In 2015, estimations indicated that about 41% of job applicants presented falsified information about their education in the US (United States) [11]. In 2017, it is estimated that about 500 fake doctoral diplomas are sold monthly in the US [12].

Thus, the release and verification of academic certificates is a known problem, tackled by academia [1], [3], [5] and also private companies. Public blockchains can be considered tamper-proof, transparent, without any centralized control, and they offer applications to a wide range of domains [2]. The main use-case applied to academic certificates is the Proof-of-Existence (PoE) *e.g.* by first generating a unique cryptographic hash digest of a certificate, and then publishing that hash to a public blockchain, effectively timestamping, thus proving the existence of the certificate, without leaking information about the contents of the data. Recognizing the potential benefits of such a blockchain-based approach, prior work presented the necessary the requirements for a solution at the University of Zurich (UZH) [7].

This document is structured as follows. Section II discusses related work. Section IV details a proposal design and architecture, while Section V includes open issues and outlines future work.

A. *First* Swiss EduChain *Workshop*

The first Swiss EduChain project workshop meeting occurred on the 7th of June of 2019 in the University of Zurich (UZH) at Binzmühlestrasse, 14, Zürich. The following institutions and companies were present at the workshop. From the side of the UZH, **Thomas Sutter**, *Chief Information Officer (CIO) of Zentrale Informatik* and **Dr. Maria Olivares** as *Leiterin Innovation, from Forschung Innovation und Nachwuchsförderung (FINF)* attended the workshop. Also from the UZH, Computer Science research groups, were represented by **Prof. Dr. Burkhard Stiller**, *Head of Communication Systems Group (CSG)*, and **Prof. Dr. Gerhard Schwabe**, *Head of Information Management Research Group (IMRG)*. Moreover, from the CSG, were present the Junior Researchers and Ph.D. students, **Eder John Scheid**, **Christian Killer**, **Geetha Parangi** and **Muriel Figueredo Franco**. Further, external stakeholders that were present are **Dr. Michael Hill** from the *Swiss National Science Foundation (SNF)*, **Ronnie Brunner**, *Co-Founder, Member of the Board, Netcetera AG*, and **Philipp Deangelis** from *Company Builder and Ventures, Swisscom AG*.

The main goal of the first workshop was to provide an overview of the current state of academic certificate verification using blockchains, and to raise discussions about the challenges and requirements from both the UZH and external stakeholders. As **Prof. Stiller** is leading the Swiss EduChain pre-project, he prepared the workshop agenda, and invited all participants. **Prof. Schwabe** is contributing to the Swiss EduChain pre-project with topics regarding Governance and Business Development. **Dr. Maria Olivares** is interested to hear from the project in the near future, especially the potential reduction of administrative burden is of interest.

Further, according to **Dr. Michael Hill**, representing the **SNF** does not focus on infrastructure, but rather focuses on the long-term orientation and strategy of Swiss EduChain. However, **SNF** wants to participate as *objective* spectator, because the interest in the legitimacy of academic certificates and official documents, in general, are highly important to **SNF**. **Netcetera** is naturally

interested in producing a business case that can benefit all parties involved. Thus, **Netcetera** has no specific requirements but is open to be a technology and implementation provider. Their approach is to create small deliverables, act fast, and try things out as fast as possible. Same as **Netcetera**, **Swisscom** is open to be a potential technology or implementation partner, focusing on providing infrastructure.

Further, **Eder John Scheid** presented the findings of prior work done at the CSG [7] and provided an overview of *Blockchain-Based Academic Certificate Handling*, indicating the overall stakeholders and the technical requirements. In addition to Eder's presentation, **Christian Killer** outlined a *Proposal of Requirements and Architecture*, which is outlined in Section III and Section IV, respectively.

In summary, the First Swiss EduChain Workshop ended on a positive note. It demonstrated, after discussions, that the points of view from all the stakeholders are aligned toward developing a complete ecosystem to support the verification of academic certificates, but also different types of certificates and documents that attest a qualification of individuals. All participants agreed that the importance of blockchains to support this ecosystem, due to their immutability and availability, is promising and should be further researched. Thus, this document supports the formalization of a project proposal, detailing the requirements, the foreseen architecture, and open challenges.

II. Related Work

Providing a trustworthy, decentralized, and publicly available data storage, public blockchains have become a disruptive technology that has seen interest across academia and industries alike. Many interesting projects (blockchain-based or not) have explored the possibility to digitally verify diplomas to counter-act the trend of fake degrees.

Blockcerts [9] is an initiative by the MIT (Massachusetts Institute of Technology) to create an open standard for issuing and verifying credentials on the Bitcoin blockchain. The system is now in use at MIT [8] and empowers graduates to use the service through a mobile app [6]. Similar to that approach, the National Research and Education Network of Greece (GRNET) [3] also persist diplomas hashes to a public blockchain. However, the GRNET project [3] differs from Blockcerts [9] because not only hashes of diplomas can be stored, but also the entire verification process. Therefore, verification requests, successful or unsuccessful proof and the forwarding of the result to its requester are steps that will be stored.

Another mentionable initiative is led by the Trust::Data Consortium [14] from MIT, aiming to provide for safe distributed computation, enabling privacy-preserving data sharing [14].

Further, BCDiploma [1], EduCTX [15] and UNIC (University of Nicosia) [16] initiated blockchain-based projects to issue and verify academic certificates. BCDiploma and EduCTX share the same goal towards a global certification network of higher academic institutions. However, UNIC aims to digitize and decentralize their internal processes issuing their first academic certificates as a Proof-of-Concept (PoC).

BADGR [4] and Mozilla Open Badges [10] are both unified solutions to ease the management of entire educational histories of students, by collecting digital certificates associated with one single user identity. While these solutions do not use public blockchain, they demonstrate multi-certificate integration with one single identity.

Generally, the same approach can be found in all most related and blockchain-based work of academic certification. Most projects only persist the hash of the certificate into the public blockchain, while the certificate data are then sent to the recipient, who can share them with others, such as an employer. The credentials can then be used to create the same fingerprint that can be found in the blockchain and thus verify its veracity. The amount of related work tackling the problem of academic certification highlights its necessity.

III. Requirements Elicitation

According to [7], the main requirements for the UZH are summarized in Table I derived from interviews with stakeholders.

While, Requirements (RQ) 1-4 relate to the Issuer (*e.g.*, UZH faculties), RQ5-6 define requirements for a Verifier (*e.g.*, a company that wants to verify diplomas). Most requests are coming from background check companies [7]. Finally, RQ7 is related to the delivery of the diploma in a digital form to the student.

TABLE I: Requirements for an certificate issuance and verification process at the UZH [7]

Issuer	
RQ1	Only authorized UZH departments are allowed to issue diplomas
RQ2	Diploma data should be confidential to its recipients
RQ3	Process of issuing and verifying diplomas should abstract technical complexities
RQ4	Multiple diplomas should be processable in batch
Verifier	
RQ5	Verification capabilities should be accessible to any company
RQ6	Diplomas should be verified autonomously
Recipient	
RQ7	Graduates should receive their diplomas in a digital format

A. Issuer

In the case of academic certificates, Issuers are official academic institutions . From the standpoint of this proposal, the main stakeholder is the UZH, which consists of seven faculties whereas each faculty includes many departments. According to [7], each of the seven UZH faculties is an Issuer. Also, different online certification institutes and private course institutes could profit from such a solution.

RQ1 defines that diplomas can only be issued by authorized Issuers (*e.g.* UZH faculties).

RQ2 addresses the confidentiality of student data, which should only be accessible by the student and potential verifiers. The "right to be forgotten" defined in the new General Data Protection Regulation (GDPR) declares that data of consumer (*i.e.*, students) cannot be permanently stored [17]. Hence, the diploma itself cannot be stored in a public blockchain.

RQ3 defines that technical details involved in the process of issuing diplomas must remain transparent to all involved stakeholders. Thus, the use of blockchain (or any other infrastructure) for issuing or verifying diplomas should not require any expert know-how from the users (*e.g.,* extracting the hash of a diploma at the verification process).

RQ4 relates to the scalability and the ease to create and verify multiple diplomas at once.

B. Verifier

A *verifier* is every third-party verifying the academic certificate of a recipient. According to [7], the most frequent requests are originating from background screening companies, which as of today, query the UZH manually. However, verifiers are not limited and include for example visa authorities, who might need to verify the academic certificate in the visa application process.

RQ5: allows anyone in possession of a diploma hash to verify its authenticity. As any company that receives a diploma from a graduate might want to verify its authenticity, this functionality has to be publicly accessible.

RQ6: describes an always available service with an automated response of the verification. If the diploma is authentic, the system has to recognize it, whereas tampered documents need to be rejected.

C. Recipient

A *recipient* holds the academic certificate and wants to easily distribute it to *verifiers*.

RQ7: graduates should receive their diplomas in a digital format. Physical diplomas can get lost or damaged, whereas digital diplomas are not affected by these problems.

IV. Preliminary System Design

The proposed architecture of the Swiss EduChain system is depicted in Figure 1. The architecture is divided into two environments, *(i) public* and *(ii) private*. These environments refer to the notion of *public* (*i.e.*, permissionless) and *private* (*i.e.*, permissioned) blockchains, which are defined in [19], and take into consideration the stakeholders defined in Section III.

In public blockchains, the data is transparent, and network participation is permissionless. This means that there is no restriction for a peer to be part of the network. Such public blockchains offer the benefits of *(a)* an append-only immutable data storage, and *(b)* high availability of the data, which makes them a perfect fit to publish publicly verifiable data (*e.g.*, certificate hashes). Although public blockchains provide these benefits, this deployment type requires a mechanism to secure that the data state is consistent throughout all peers. Thus, they employ consensus mechanisms (*e.g.*, Proof-of-Work (PoW) or Proof-of-Stake (PoS)) to ensure all the peers have the same copy of the blockchain and that new included transactions are valid.

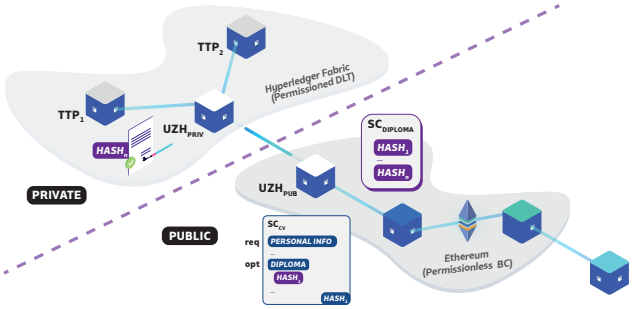

Fig. 1: Preliminary Architecture Overview

However, due to privacy and security concerns, not all data (in transit or at rest) should be public. For example, personal information of European citizens must be kept private and be processed inside European territory under the GDPR. Moreover, the blockchain technology was not conceived as a database, but rather a mean to exchange funds without the need for a Trusted Third Party (TTP). For this reason, the storage of data in public blockchains is expensive and limited, hindering the ability to store encrypted data to ensure privacy. Therefore, these aspects underline the necessity of private environments, where the data remains private, and the data storage and costs are not a limiting factor. In private environments, the deployment, *i.e.*, where the nodes are located, of a blockchain is restricted to a set of know authorities (TTP_1, TTP_2, TTP_n), which do not necessarily trust each other but trust in the blockchain technology. As the peers are previously defined, the consensus mechanism can be simplified and the access rights easily controlled, due to the presence of a central authority or consortium.

A. Access Control

The following Table II shows the read and write policies of the publicly verifiable academic certificates (*i.e.*, hashes published to the public blockchain). Different technical approaches can be used to realize this sort of access control. For example, Smart Contracts (SC) [2], or even the deployment of dedicated Parachains [18] can be considered. As indicated in Table II only *Issuers* should be able to write authenticated hashes. Only educational institutions (*e.g.*, UZH or ETH) should be allowed to issue diplomas or certificates. Consequently, *Recipients* and *Verifiers* must

only be able to read from the blockchain, allowing them verify the certificate.

TABLE II: Stakeholders and Access Rights

Stakeholder	Read	Write
Issuer	✓	✓
Recipient	✓	✗
Verifiers	✓	✗

B. Preliminary Process Flow

The process flow is depicted in Figure 2 and shows the different stakeholders interacting.

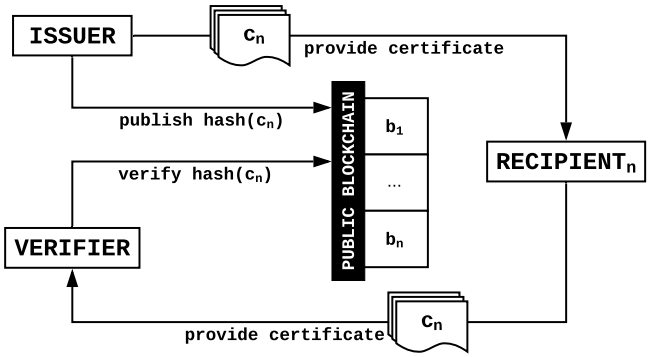

Fig. 2: Process Diagram

In a first step, the Issuer provides the certificate c_n to the recipient n and also publishes the $hash(c_n)$ to a public blockchain. The recipient may distribute the certificate to verifiers, who then are able to verify the $hash(c_n)$ without the need to contact the verifier. The $hash(c_n)$ is compared with all the hashes stored in the public blockchain. Using a SC-based approach, the hashes could be stored in a SC, also allowing the transparent revocation of academic certificates.

V. Open Issues

To further refine the proposed Swiss EduChain design and architecture, the following open issues need to be resolved. The issues are classified into Business, System, and Implementation Levels.

A. Business Level

The requirements identified in Section III need to be extended in detail. For instance, the demand for a private environment is a clearly defined requirement for the UZH faculties end-users, which is administrative personnel. Another stakeholder with diverging requirements is *e.g.*, the Zentrale Informatik, which provide operational services throughout all IT infrastructure of the UZH. Further, the Swiss EduChain project not only aims to provide a specific solution for the UZH, but rather to develop a generic and issuer-agnostic a solution. Thus, the requirements listed in [7] are only a starting point which lead to broader research on how to extend or generalize. Moreover, unrecognized and unaccredited institutions need to be prevented from issuing certificates.

B. System Level

To provide integrity of the publicly verifiable academic certificates, clearly defined authentication and authorization mechanisms are necessary, taking into consideration the different access controls listed in Table II. Data privacy issues must be critically discussed and evaluated. For example, GDPR compliance is important, because data removal from public blockchains is impossible, also, whether hashes can be considered personal data or not.

The data structure to formalize academic certificates should be defined and designed in a way that offer extensibility in the future. For instance, a possible extension could be the possibility to assemble Curriculum Vitae (CV) for recipients, using open-source standards (*e.g.*, JSON Resume [13]) which could then be verified in the same manner as academic certificates. Besides CVs, the data structure should be extendable to more use-cases which require independent and efficient verification mechanisms.

Moreover, Section II showed that each project operates in their own ecosystem and implementation, leading to a myriad of isolated projects, which are not able to communicate with each other. For example, if a certificate is issued and stored in project A, the *verifier* must use the tools provided by project A to check the document integrity, even if it already possesses access to the tools of project B. Currently, there is no mechanism that allows these two projects to seamlessly communicate or interoperate. Therefore, standards must be researched and developed to ensure that projects implement common functions and data types, allowing for agnostic data exchange.

C. Implementation Level

Further, the architecture and design need to find appropriate implementations and process definitions, which result in decisions to be taken aiming the success of the Swiss EduChain project. For example, once the architecture is defined, the stakeholders identified, and the information workflow detailed, the choice of which blockchain implementation (*e.g.*, Ethereum, HyperLedger) is able to address the requirements and provide underlying mechanisms, such as Turing-complete SCs, that aid in the implementation of verification functions and access control.

VI. Preliminary Conclusions

In conclusion, it can clearly be shown that all stakeholders involved can positively benefit from the use-case of academic certificate verification. Further, the possibility to extend beyond academic certificates, to any verification process, can help to improve and simplify document verification and support the mitigation of fraud. Thus, the open issues identified in Sec. V need to be tackled with more inter-disciplinary research efforts, combining the requirements of internal and external stakeholders.

References

[1] BCDiploma. Degrees Certified on the Blockchain. Accessed: 2019-07-01. [Online]. Available: https://bit.ly/2rp95qC

[2] T. Bocek and B. Stiller, "Smart contracts - blockchains in the wings," in *Digital Marketplaces Unleashed*. Springer, 2018, pp. 169–184.

[3] A. Castor. (2018, January) Cardano Blockchain's First Use Case: Proof of University Diplomas in Greece. Accessed: 2019-07-01. [Online]. Available: https://bit.ly/2DVsrYt

[4] Concentric Sky. Make your badges meaningful with Badgr. Accessed: 2019-07-01. [Online]. Available: https://bit.ly/2L271Ne

[5] A. T. Elizabeth Durant. (2017, Oct) Digital Diploma debuts at MIT. Accessed: 2019-07-01. [Online]. Available: https://bit.ly/2xPRWXC

[6] Google Play Store. Blockcerts Wallet. Accessed: 2019-07-01. [Online]. Available: http://bit.ly/blockcerts-wallet

[7] J. Gresch, B. Rodrigues, E. John Scheid, S. S. Kanhere, and B. Stiller, *The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling: BIS 2018 International Workshops, Berlin, Germany, July 18âĂŞ20, 2018, Revised Papers*, 01 2019, pp. 185–196.

[8] MIT Registrar's Office. Digital diploma. Accessed: 2019-07-01. [Online]. Available: http://bit.ly/mit-registrar

[9] ——. Digital diploma pilot program faqs. Accessed: 2019-07-01. [Online]. Available: https://bit.ly/2JYw4zT

[10] Mozilla. Open Badges. Accessed: 2019-07-01. [Online]. Available: https://bit.ly/2u7YS3n

[11] N. M. Musee, "An Academic Certification Verification System Based on Cloud Computing Environment," *PhD diss., University of Nairobi*, 2015.

[12] H. Park and A. Craddock. Diploma Mills: 9 Strategies for Tackling One of Higher Education's Most Wicked Problems. Accessed: 2019-07-01. [Online]. Available: https://bit.ly/2DoEeyu

[13] J. R. Team. The Open Source Initiative to Create a JSON-based Standard for Resumes. Accessed: 2019-07-03. [Online]. Available: https://jsonresume.org/

[14] Trust::Data Consortium - An initiative of MIT Connection Science. Accessed: 2019-07-01. [Online]. Available: https://www.trust.mit.edu/about

[15] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A Blockchain-based Higher Education Credit Platform," *IEEE Access*, 2018.

[16] University of Nicosia. Academic Certificates on the Blockchain. Accessed: 2018-04-02. [Online]. Available: https://bit.ly/2I5G3mj

[17] P. Voigt and A. v. d. Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 1st ed. Springer Publishing Company, Incorporated, 2017.

[18] G. Wood, "Polkdaot: Vision for a Heterogeneous Multi-Chain Framework," November 2016, Accessed: 2019-07-04. [Online]. Available: https://polkadot.network/PolkaDotPaper.pdf

[19] K. Wüst and A. Gervais, "Do you Need a Blockchain?" in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2018, pp. 45–54.