A Framework for Long-Term Revocable Credentials

Erbguth, Jorn

How to cite

ERBGUTH, Jorn. A Framework for Long-Term Revocable Credentials. Doctoral Thesis, 2022. doi: 10.13097/archive-ouverte/unige:160529

This publication URL: https://archive-ouverte.unige.ch/unige:160529
Publication DOI: 10.13097/archive-ouverte/unige:160529

A Framework for Long-Term Revocable Digital Credentials

Un cadre pour les certificats numériques révocables de longue durée

THÈSE

présentée à la Faculté des sciences de la société
de l'Université de Genève

par

Jörn Horst Erbguth

sous la direction de

prof. Jean-Henry Morin

pour l'obtention du grade de

Docteur sciences de la société
mention systèmes d'information

Membres du jury de thèse

Mme. Giovanna DI MARZO SERUGENDO, Professeure, présidente du jury

M. Pierre-Yves BURGI, Docteur, Directeur SI adjoint,
en charge du domaine fonctionnel "Recherche & Information Scientifique"

M. Dimitri KONSTANTAS, Professeur

M. Jean-Henry MORIN, Professeur, Directeur de thèse

M. Jean-Philippe WALTER, Docteur, Expert indépendant et
commissaire à la protection des données du Conseil de l'Europe

Thèse no 189
Genève, 21 février 2021

La Faculté des sciences de la société, sur préavis du jury, a autorisé l'impression de la présente thèse, sans entendre, par-là, émettre aucune opinion sur les propositions qui s'y trouvent énoncées et qui n'engagent que la responsabilité de leur auteur.

Genève, le 21 Février 2022

Le doyen

Bernard DEBARBIEUX

Impression d'après le manuscrit de l'auteur

Déclaration sur l'honneur

Par ma signature, j'atteste avoir rédigé personnellement cette thèse sans aide extérieure non autorisée, n'avoir utilisé que les sources et moyens autorisés, et mentionné comme telles les citations et paraphrases. Cette thèse n'a pas déjà été présentée devant une autre faculté.

List of figures

List of Tables

Résumé

Les certificats et justificatifs à long terme, comme les titres universitaires, sont de plus en plus utilisées sous forme numérique. Souvent, les diplômes en papier, sécurisés par du papier et des sceaux spéciaux, sont utilisés simplement numérisés mais pas sécurisés lors des communications en ligne. Cependant, il est facile de falsifier des numérisations non sécurisées de diplômes en papier, ce qui constitue un problème croissant. Une série d'approches différentes sont discutées dans la littérature scientifique et sont également partiellement disponibles sur le marché. Ces approches de sécurisation des justificatifs à long terme par des moyens cryptographiques présentent des forces et des faiblesses différentes en ce qui concerne une série d'exigences telles que l'authenticité et la facilité d'utilisation.

Cependant, les justificatifs à long terme révocables, tels que les diplômes universitaires, sont confrontés à un défi spécifique : Les justificatifs restent valables même lorsque l'institution cesse d'exister. Par conséquent, les titres doivent être vérifiables même lorsque l'institution n'existe plus, mais ils doivent également être révocables par l'institution qui les a délivrés en cas d'erreur ou plagiat. En même temps, les lois sur la protection des données donnent aux détenteurs de la crédence le droit à l'oubli. Comment un justificatif peut-il être vérifiable indépendamment de l'institution et en même temps révocable ? Comment s'assurer que l'avis de révocation ne se perdra pas lorsque l'institution pourrait cesser d'exister ? Dans le même temps, il convient de limiter l'accès au titre et, éventuellement, à la notification de révocation.

Dans la première partie, cette thèse évalue les approches ouvertes et propriétaires existantes, depuis les signatures électroniques qualifiées et les apostilles électroniques jusqu'aux certificats vérifiés pour les identités numériques souveraines.

La deuxième partie discute et définit un ensemble d'exigences pour un cadre qui répond aux besoins des certificats révocables à long terme. Une conception propose un cadre basé sur une combinaison de sceaux électroniques qualifiés, un smart contract sur une blockchain et un serveur en ligne. Un prototype est construit conformément à ce cahier des charges.

Enfin, l'approche choisie est évaluée en la présentant et en la discutant lors de plusieurs conférences dans des auditions gouvernementales, des organismes de normalisation et des établissements universitaires. Une série de questions sont apparues dans ce contexte et sont discutées dans la troisième partie de cette étude.

Il est conclu que la technologie des blockchains peut être un outil utile pour vérifier les titres de compétences à long terme qui restent valables même lorsque l'institution émettrice n'existe plus. Déterminer qui devrait avoir accès à l'info d'une révocation dépend du cas d'utilisation spécifique et de l'effet rétroactif des révocations. L'intérêt légitime des personnes qui doivent être informées d'une révocation doit être mis en balance avec le droit à l'oubli du détenteur du justificatif révoqué qui n'est plus utilisé. Les smart contracts sur une blockchain peuvent constituer un bon équilibre à cet égard, en fournissant les informations de révocation lorsque cela est justifié et en les masquant dans les autres cas. L'identité numérique souveraine (SSI) pourrait, en théorie, renforcer certains droits du détenteur du titre. Par exemple, le détenteur d'une carte d'identité pourrait prouver son identité sans divulguer son nom. Cependant, les portefeuilles SSI sont moins faciles à utiliser et ne sont pas encore largement utilisés.

En particulier, ils ne garantissent pas encore une identification fiable du détenteur du titre sans que son nom soit divulgué.

La solution proposée est une solution ouverte qui peut être adoptée par de nombreuses institutions émettrices en partageant un smart contract et qui peut offrir la possibilité d'une vérification croisée des titres avec une structure de gouvernance décentralisée minimale, comme c'est le cas, par exemple, de la blockchain académique Bloxberg.

Abstract

Long-term credentials like academic titles are increasingly being used in a digital format. Often, paper diplomas, secured by special paper and seals are used as unsecured scans when communicating online. However, forging unsecured scans of paper diplomas is easy and an increasing problem. A range of different approaches are being discussed in scientific literature and are also partially available on the market. These approaches to secure long-term credentials by cryptographic means offer different strengths and weaknesses regarding a range of requirements like authenticity and usability.

However, revocable long-term credentials like university diplomas face a specific challenge: Credentials remain valid even when the institution ceases to exist. Therefore, credentials need to be verifiable even when the institution no longer exists, but they also need to be revocable by the issuing institution in case of error or plagiarism. At the same time, data protection laws provide the credential holders with the right to be forgotten. How can a credential be verifiable independently from the institution and at the same time revocable? How can it be ensured that the revocation notice cannot get lost when the institution might cease to exist? At the same time, access to the credential and possibly its revocation notice needs to be limited.

In the first part, this thesis evaluates existing open and proprietary approaches ranging from qualified electronic signatures and e-apostilles to verified credentials for self-sovereign identities.

The second part discusses and defines a set of requirements for a framework to support revocable long-term credentials. A design proposes a framework based on a combination of qualified electronic seals, a smart contract on a blockchain and an online server. A prototype is being built according to that specification.

Finally, the chosen approach is evaluated by presenting and discussing it at several conferences at government hearings, standards organizations, and academic institutions. A range of questions occurred in that context and are discussed in the third part of this study.

It is concluded that decentralized ledger technology can be a useful tool to verify long-term credentials that remain valid even when the issuing institution does not exist anymore. Determining who should have access to the revocation information depends on the specific use-case and the retroactive effect of revocations. The legitimate interest of those who should be informed about a revocation needs to be balanced with the right to be forgotten by the credential holder of the revoked credential that is no longer used. Smart contracts on a blockchain can model a good balance here, provide the revocation information where justified and hide it in other cases. Self-sovereign identity (SSI) could – in theory – support some rights of the credential holder further. A credential holder could prove a credential without disclosing her name, for example. However, SSI wallets have less usability and are not widely used yet. Particularly they do not yet ensure reliable identification of the credential holder without the disclosure of the name of the credential holder.

The proposed solution is an open solution that can be adopted by many issuing institutions by sharing a smart contract and can provide the possibility of cross-

verification of credentials with a minimal decentralized governance structure as being found, for example, at the Bloxberg academic blockchain.

Acknowledgment

I would like to thank my parents, Sieglind and Horst Erbguth, who raised me and supported me in going on this journey by many means. Jean-Henry Morin has been a great teacher to me, particularly in Design Science, but his biggest support was his encouragement and inspiration for which I am very grateful. I like to express my gratitude towards Pierre-Yves Burgi who made it possible to have the prototype project at the University of Geneva and included the implementation of blockchain based certification in a bigger project on digital services provided by the University of Geneva, projet de loi PL 12767, that has been approved by the Geneva Grand conseil. I would also like to thank Omar Benkacem, Vincent Gessler and Sophie Huber among many others at the university who supported me when building the prototype, particularly in answering many questions regarding requirements and possible designs. I would like to thank André Camacho who built the web app of the system.

I would like to thank the thesis committee: Prof. Giovanna Di Marzo Serungendo, Doc. Pierre-Yves Burgi, Prof. Dimitri Konstantas and Doc. Jean-Philippe Walter for their insightful comments, support, and trust towards my work.

I would like to thank Alexandre Poltorak for his inspirational discussions about the spirit behind technology enabling decentralization. The evaluation was only possible by discussing it within many different communities. I am very thankful, to Katrin Kirchert who partnered in setting up the *Conference on Blockchain and GDPR* in Berlin, to Александр Чубурков, with whom I had a lot of discussions in the context of FG-DLT and SG16 at the ITU as well as in Russia, to Ismael Arribas who supported my discussions at the ITU and INATBA, to Javier Wenceslao Ibáñez Jiménez with whom I had many discussions at the ITU and who invited me to the Token World Conference, to Galia Kondova with whom I co-authored a paper on Self-sovereign identity on public blockchains and the GDPR, to Anik Kohli for co-authoring a paper for INATBA and the Climate Ledger Initiative, to Eva Stöwe, Todor Karaivanov, Max Jarvie and Samuli Pahalahti in the worbli governance group and so many others in the DIN SPEC 4997 group and the Bloxberg community. My thanks also go to Veronica Stivala for her expeditious proof-reading.

I dedicate this work to my son who I am so happy to have watched and supported growing up.

Chapter 1 Introduction

Who am I? Identity has become an increasingly important but also controversial topic in society. Belonging to a specific group depending on gender, ethnicity, family, school of thought, etc. increasingly determines our role and rights in society. Although Article one of the Universal Declaration of Human Rights states that *all humans are born free and equal in dignity and right*s, discrimination and anti-discrimination based on our identity do not grant us more equal but rather serve as the cause for more different treatment.

Since our identity has a strong impact on our life, there always has been a desire to change, disguise or fake it. Women that have been denied the right to perform an activity disguised themselves as men. Qualifications were faked so that those who were unqualified could perform a job. In a famous cartoon, *Peter Steiner*, as early as 1993, wrote “On the Internet, nobody knows you’re a dog” [1, p. 61]. Although using the Internet leaves many traces, hiding or forging our identity when communicating electronically is often easier than proving our identity. This leads to the question: What part of our identity are we allowed to hide and in which contexts and finally, who controls our identity?

One of the less controversial aspects of identity is education. In a knowledge society of lifelong learning, education and experience play an increasingly important role. Diplomas certify our qualifications. An increasingly digital and interconnected society requires us to use them online, when applying for a job or performing any other task for which that qualification is required.

While presenting fake credentials is not acceptable, individuals are generally granted the right to not disclose a qualification they do not want to disclose. The right to be forgotten, as declared by the European Court of Justice [2], for example, includes the right to hide airplane pilot qualifications when applying for a job at an organization that thrives to reduce carbon emissions.

Credentials for qualifications ensure that people have the knowledge required for performing a task and it is important for society that, for example, doctors or pilots are well skilled. Applying for a job is increasingly done electronically. In 2015, 45% of US-Americans had already applied for a job online [3, p. 9]. In Germany, in 2015, only 27% of companies preferred to receive job applications on paper, whereas 58% preferred online applications [4]. In 2018 the percentage of job applications on paper shrank to 17%, while only 1.5% of job applicants and 5% of larger companies preferred paper form [5]. However, most university degrees are still printed on paper. A scan of a printed university degree is not protected against tampering. In times of the COVID19 pandemic, 86% of companies are conducting interviews online [6]. In a physical interview, it is possible to ask job applicants to show the originals of their diplomas to verify their authenticity. Online interviews do not provide this possibility. Even when the original of a diploma is shown during an interview, the print quality of color laser printer is so good that it requires special skills to detect that an applicant is not

showing an authentic diploma. An additional form of proof of authenticity is required.

Forged diplomas are easy to create or obtain online [7]. Occasionally, fake diplomas are detected and the holders of fake diplomas face the consequences [8]. *Degree Mills* have sold more than a million of fake diplomas [9]. Given that many employers only require an unsecured PDF-document, forging diplomas can be done with readily available computing tools. There are generally three main ways diplomas are forged:

- A fake diploma for an existing university is created. Often, a copy of an existing real diploma is used as a template.
- A diploma for a non-existing university is created. Given the possibility to verifying the existence of university through a simple Google search, sometimes a website for a fake university is created.
- A real diploma is manipulated to modify the grades or achievements documented by the diploma.

Sometimes, authentic credentials need to be revoked. Credentials might have been erroneously issued or achieved through plagiarism. Some countries and universities have a system of trading in an existing diploma to use the credit points of a previous degree for earning a higher degree. Obviously, returning a digital credential cannot be done by sending back a copy of the file containing the credential.

Diplomas are credentials that accompany us during all of our – at least – professional lives. Practicing as a lawyer or a doctor might mean one relies on credentials earned decades ago regardless of how much the subject matter has advanced in the meantime. Credentials remain valid even when the institution that has granted them does not exist anymore.

The need for secure digital identification and digital credentials was already recognized more than 20 years ago. A range of standards have been created [10]. Laws regulating the recognition of digital signatures were enacted in 1997 in Germany (SigG) and in 2000 in Switzerland (ZertDV). Terms for digital signatures differ between legal systems. In Europe *electronic signatures* are data added to a document that is used to identify or authenticate the source of a document. Setting the name of a person in simple typed letters below a document, for example, serves as an electronic signature, because it indicates to the reader that this person has authored the document. An *advanced electronic signature* is a signature that proves that the signatory has signed the document. While the simple electronic signature does not prove that the name has been typed by the author, the advanced electronic signature offers this proof. A qualified electronic signature is an advanced electronic signature that is based on a regulated public key infrastructure. The UN, however, rather uses the US terminology in calling advanced electronic signatures *digital signatures* [11, p. 9]. This work uses the terminology used in Europe. When no reference to a public key infrastructure is made but only the technology of the signature is relevant, signatures that use

cryptographic methods are called cryptographic signatures. For further details on electronic signatures see chapter 4.3.1.

Discussions among legal scholars date back well before the introduction of these laws. However, adoption is slow. Laws have been modified to improve usability and acceptance. An EU-wide regulation, eIDAS, is mandating legal recognition of qualified electronic signatures in all EU member states. However, eGovernment services in Germany circumvent this regulation. Electronic communication with courts, for example, requires access to a specialized communication system, which is restricted to a proprietary ID. Electronic tax declaration needs to use a specialized system called ELSTER. Access to this system is restricted to taxpayers residing in Germany. The eIDAS regulation is not adopted in Switzerland, rendering Switzerland a digital island regarding the validity of their own, non-eIDAS-compliant qualified electronic signatures. A new law to introduce privately managed identification systems even for official purposes, has been heavily criticized [12] and was voted down in a referendum in March 2021 [13]. A new proposal based on the concept of self-sovereign identity has been announced for summer 2022 [14].

Qualified electronic signatures are based on certificates that have a limited validity of a maximum of typically 3 years. Any signature presented after the certificate has expired needs to be proved to have been created within the validity of the qualified certificate. Therefore, a timestamp is added to the qualified electronic signature to prove that it was not created after the expiration of the certificate. Since the timestamps used are also based on certificates with limited time validity, regular maintenance of the qualified electronic signature is required to maintain its legal validity. Techniques are described in ETSI SR 019 510 V1.1.1 [15].

While qualified electronic seals and qualified electronic signatures rely on a centralized and hierarchical trust chain controlled by the government, other, grass-roots models have emerged. *Pretty Good Privacy (PGP)* relies on a web of trust [16]. If somebody we trust knows the identity behind an account, we do not need a central authority to certify it. And if we trust the ID, somebody else that trusts us and our judgement, will also trust the ID. Another decentralized approach to securing data is *distributed ledgers*. Also known as blockchains, they allow data to be stored almost immutably. Since the time of the creation of the block is known, entries can also serve as timestamps. All entries also have to be signed by a private key which can serve as means of authentication.

This thesis studies long-term credentials and often refers to the use-case of university diplomas. The terminology used is the *issuing institution*, e.g., the university that creates the credential. The digital *credential* is – for example – the university diploma. The student who earns a diploma is called the *credential holder*. The person the credential is presented to, e.g. the employer or another university, and that should be able to verify it, is the *credential verifier*.

This work uses the design science methodology [17]. It is structured as follows: First the research question is narrowed down. Then the context and

background are discussed. The following chapter offers prior art regarding comparative analyses and existing systems to secure long-term credentials. This analysis leads to a definition of requirements. These requirements form the basis for the design of a framework which is then implemented in a prototype. This prototype is evaluated and discussed. The work ends with a conclusion and outlook to future work.

Chapter 2 Research problem description

This chapter defines the research question and introduces the chosen research methodology.

2.1 Research question

Digital long-term credentials, like university diplomas, face almost contradicting requirements. They must be able to be verified for a very long time, possibly during the entire life of the credential holder. They also continue to be valid even when the issuing organization no longer exists. However, under some conditions credentials might need to be revoked by the issuing institution. Also, the credential holder enjoys the right to be forgotten. This creates the need for a digital credential which is durable and legally valid, but which can be revoked. This digital credential needs to be verifiable autonomously, meaning independently from the issuing institution or a third party that might cease to exist but the information in the credential should not be public.

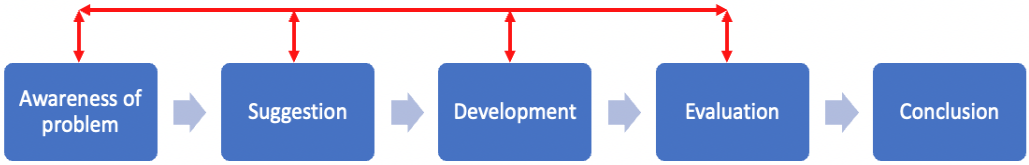
Technologies like online verification, cryptographic signatures or distributed ledgers are offering possible components of a solution that provide self-sovereignty of credential holders. Laws on data protection, identity and electronic signatures provide legal frameworks that are currently evolving. At the same time the solution needs to satisfy other requirements as well. It has to be secure, efficient, usable and sustainable.

The resulting research question is: How might we design a framework to certify and verify digital revocable long-term credentials?

Addressing this question requires a holistic design approach that bridges the almost contradicting requirements of a secure credential that is durable and autonomous but that is also revocable. This design needs to address technical and legal requirements, create trust and should be supportive of individual rights in a future digital society that do not create unnecessary dependencies on centralized actors.

2.2 Research methodology

The goal of this thesis is the design of a framework to secure revocable long-term credentials. The method chosen is Design Science Research [17, pp. 59–73] which is an adapted general design cycle. The red two-way arrows in Figure 1 indicate that this is an iterative and agile process that starts with an awareness of the problem. This results in a proposal from which a tentative design is created, developed into a design and which then leads to an artefact in the form of a prototype which is then evaluated, discussed, and from which a conclusion is drawn. The problem awareness includes an analysis of the state of the art where existing systems and approaches are evaluated. The process is agile and involves frequent iterations and revising assumptions that have been made before.



Source: Adapted from *Vaishnavi/Kuechler*

Figure 1: Design Science Research method [17, p. 59]

Chapter 3 Context & background

This chapter describes the context and background regarding technology and law. These are building blocks on which the following definition of requirements, design and discussion will be based. First, technology and regulation regarding **electronic signatures** are introduced. This is followed by **decentralized ledger technology**, the more general term for **blockchains**. **Smart contracts** based on decentralized ledger technology allow the programming of new transaction types on existing blockchains. **Data protection** protects natural persons in relation to the processing of their personal data. Data protection regulation sets conditions for the processing of personal data. **Self-sovereign identity** is an idea to maximize the control of individuals over the personal data that form their digital identity. These technological, legal and philosophical concepts will be referred to in the following chapters.

3.1 Electronic signatures

Electronic documents can be copied. There is no electronic "original" since the use of electronic document involves copying the document. The display of an electronic document involves reading it from a data store, copying it into working memory and then copying it from there into the display memory.

When it comes to computer software, copy protected media, dongles and *digital rights management* (DRM) have been used to prevent the copying and/or use of copied software or audiovisual licensed works. However, these kinds of copy protection tend to impact usability and user experience [18, p. 339]. For example, DRM often restricts the choice of hardware and/or software systems that can be used to view or listen to the licensed work. Switching platforms might result in a loss of access [19, p. 56]. Some systems are based on license servers running, so if the server stops running, access to the licensed work might also be blocked even if a perpetual license has been purchased. Fair use rights might be affected, and the licensor is also able to withdraw access as was seen with free licenses for the book “1984” on Amazon’s Kindle [20]. If pirated copies offer better user experience, DRM could be *hurting sales* [21]. While DRM tries to prevent copying, a credential should be copied and distributed to be used, for example, in the case of job applications. Identical copies are usually a desired side effect of digital credentials. Still, DRM-systems could also be used to verify the authenticity of a credential. However, for credentials the use of dongles and limitations to proprietary platforms are even less practicable than in the media industry.

Verifying digital credentials means that the author and the originality of the document can be verified and any tampering with the document can be excluded. Just like a manual signature, the verification of the signature does not verify the content of the document but merely the fact that it has been signed by the person or institution mentioned in the signature and that it has not been altered since.

Rivest/Shamir/Adleman introduced a public key encryption system [22] of a combination of a public and a private key to sign a document with a private key

and to verify this signature using the corresponding public key. The knowledge of the public key can securely verify that the document has been signed with the private key and has not been altered since. However, the knowledge of the public key does not allow the private key to be calculated. An electronic document cryptographically signed with a private key can be securely attributed to a party, if the corresponding public key can be securely attributed to that party and if it can be ensured that the party has exclusive knowledge of the private key. This type of electronic signatures requires a verification that the public key is attributed to a specific party and the confidentiality of the private key has not been breached. A qualified certificate electronically signed by a *trusted third party* (TTP) certifies that a public key belongs to the specific party. This authority is called a *qualified trust service provider* for qualified electronic signatures in eIDAS Article 3 nr. 20 [23], while it is called *certification authority* (CA) in X.509 the ITU/ISO standard used for website certificates and TLS [24, p. 4]. Furthermore, a qualified trust service provider verifies the validity of a qualified certificate by signing it herself. This *Public Key Infrastructure* (PKI) may consist of multiple levels of certificates that are signed by a superior trust service provider. This hierarchical trust chain finally requires trust only in the certificate from the *root certification authority* (root CA) and, of course, in the adherence to the protocol by the members of the trust chain.

The UN has created a model law to recognize electronic signatures based on the PKI principle [25]. Switzerland has enacted the SCSE/ZertES law that recognizes electronic signatures [26]. The EU has enacted the eIDAS regulation to recognize electronic signature systems throughout the European Union. However, a signature that is eIDAS compliant is not (necessarily) SCSE/ZertES compliant and vice-versa. Some providers like, for example Skribble [27] let users choose whether they want signed documents to be eIDAS or SCSE/ZertES-compliant.

Art 14.2bis of the Code of Obligations of Switzerland [28] specifies that a SCSE/ZertES-compliant qualified electronic signature is deemed equivalent to a handwritten signature. Besides qualified electronic signatures of its representatives, an institution can also apply an electronic seal – the equivalent to an institutional analogue seal. Although the requirements of an electronic seal are defined in the SCSE/ZertES, the complete legal equivalence is not yet stated in the law.

Qualified certificates have a limited lifespan and can also be revoked. The revocation, however, will not invalidate electronic signatures created before the certificate has been revoked. Therefore, every qualified electronic signature is required to be accompanied by a qualified electronic time stamp that allows one to determine whether the qualified electronic signature was created before the qualified certificate lost its validity. The qualified electronic time stamp itself is based on a certificate that also has a limited validity and could also be revoked. Therefore, the qualified electronic time stamp needs to be timestamped again before the end of the validity of its certificate is reached. Without regular application of new timestamps, the chain of timestamps is broken and the validity

as a qualified electronic signature including the legal equivalence to a handwritten signature might be lost. After a certificate has expired, it will no longer be revoked in the case of security breaches. Therefore, a broken chain of timestamps will also create a slowly increasing security risk.

The acceptance of qualified electronic signatures has been very slow in Switzerland. Besides bureaucratic hurdles for the university, the usability for students is limited. It seems impractical to renew time stamps on electronic diplomas on a regular basis. A different method of preserving time stamps should be preferred. Also, only the original digital document can be verified. Any non-identical copy, conversion into a different format, printout or scan from a printed document cannot be verified.

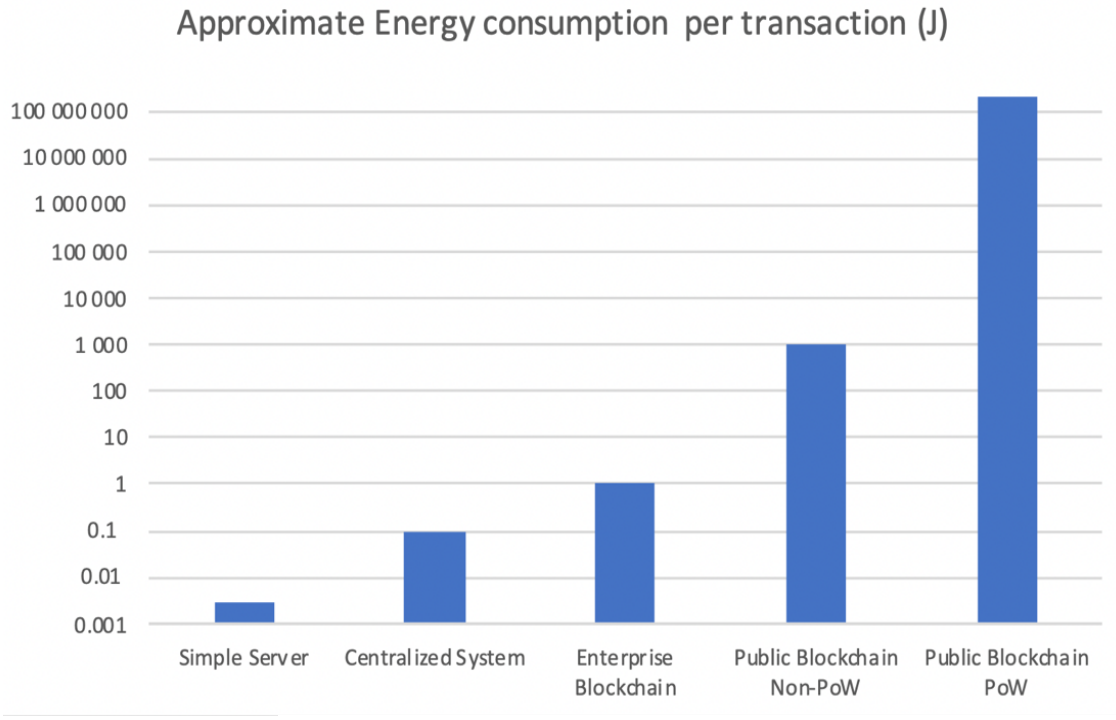
3.2 Decentralized Ledger Technology

Decentralized Ledger Technology (DLT) addresses the issue of digital trust. Our society is becoming increasingly dependent on digital records stored in databases. Analogue proofs are getting less common and increasingly easy to forge. Therefore, we need a way to ensure that these records are not manipulated by single actors. DLT offers decentralized trust that is much less dependent on central actors.

Blockchains started with the *Bitcoin*-paper [29], published under the pseudonym of *Satoshi Nakamoto*. Bitcoin incorporated then existing technologies like cryptographic hashes, cryptographic signatures and was built on prior ideas like *DigiCash* (using *Blind Signatures*) [30] and *Proof of Work* (POW) *Hashcash* [31]. The purpose of Bitcoin was to create a peer-to-peer version of electronic cash. Bitcoin was created in a community of crypto-anarchists that – after the crash of the financial markets in 2008 – did not trust the established monetary system and looked for an alternative that does not depend on centralized entities that could be corrupted or attacked. Crypto-anarchists came out of the cypherpunk movement [32] and wanted to use cryptography to reduce government influence by untampered communication and unstoppable systems. Characteristic for crypto anarchists is the Crypto Anarchist Manifesto [32, Ch. 16.4.2].

Blockchains are distributed ledgers where information is grouped in blocks and linked through hash values. There are also other distributed ledger systems, that are not organized in a chain. For, example, hashgraph [33] forms a more complex structure than a simple sequence. Since this distinction is not relevant in this thesis, both terms are use synonymously. Transactions are signed by cryptographic signatures of the private keys of the accounts the transaction fees are paid for and that will be the source of the funds to be transferred. Cryptographic signatures, however, cannot prove that Bitcoins are still under the control of the owner and have not already been spent. The Bitcoin blockchain solves the problem of *double spending* in an environment without a central actor. It creates a synchronized common copy of the truth through a decentralized consensus mechanism called *Proof of Work* (PoW). To reduce the risk of manipulations, like the removal of transactions, the version of the truth with the

most computing power will prevail. As an incentive to dedicate substantial computing power to this process called *mining*, the participation is rewarded with *mining rewards*. The probability to be able to create the next block corresponds to the fraction of the computing power of a *miner*. A new block is created on average every 10 minutes and is currently being rewarded with 6.25 Bitcoins – which corresponds to about 250'000 CHF. These high rewards encourage miners to dedicate much computing power to the mining of Bitcoin. A single specialized hardware mining unit calculates more than 100 Giga hashes per second [34]. Bitcoin mining in 2022 consumes about 200 TWh per year [35], which is almost four times the electrical energy consumed in Switzerland in 2020 [36]. The high energy consumption of Bitcoin is causing major criticism. Most other blockchains therefore use different consensus mechanisms that consume many magnitudes less power than the PoW consensus mechanism in Bitcoin (Figure 2).



Source: Adapted from *Sedlmeir et al.*

Figure 2: Comparison of energy consumption [37]

It is possible to add some arbitrary data to Bitcoin transactions [38]. For example, there is a field *OP_RETURN* in Bitcoin transactions where up to 80 bytes can be stored. This data is almost immutably stored on the Bitcoin blockchain together with the transaction it is stored with. Since every block includes the time it was created, this could prove that the data was known at the time the block was created. Since only small amounts of data can be added to transactions, this would be impractical for larger objects. A hash function calculates a value for every digital object. The length of the value is constant for all objects regardless of their size. Cryptographic hash functions are a one-way function that are collision-resistant [39, pp. 30–32]. Collision-resistance means that different digital objects practically never result in the same hash value

although theoretically this could be possible. Since cryptographic hash functions are one-way functions, it is also impossible to calculate an object from a given hash value – other than by guessing it using brute force. Therefore, if a digital object results in a specific hash value, the hash value proves that the corresponding digital object existed when the cryptographic hash value existed. This allows the cryptographic hash value to be publicly registered as a proof of existence of a digital object without disclosing the digital object itself. Adding a cryptographic hash value calculated from a digital object to a blockchain transaction can therefore serve as a timestamp for that digital object [40, pp. 73–74]. This, however, is not an eIDAS-compliant qualified electronic timestamp, but *Sorge/Leicht* point out, a single qualified electronic timestamp of the hash value of a block of a blockchain can be regarded as a eIDAS-compliant qualified electronic timestamp of this and all preceding blocks and all objects that are referenced by their hash values in these blocks [40, pp. 75–84]. If the address that signed the transaction can be identified with a person or institution, this could also be interpreted as proof that the institution or person endorses that digital object. However, the signature only proves that somebody with access to the keys of the institution wrote the cryptographic hash value of the digital object to the blockchain and the institution needs to express what is meant by it. Some jurisdictions already recognize the legal value of blockchain-based proofs [41] [42].

Besides permissionless public blockchains [43, pp. 4–5], there are also two other types of blockchains. There are permissioned but public decentralized ledger systems that restrict who can run a node that creates new blocks but read access to the content of the blockchain is not restricted and there are private permissioned blockchains where reading is also restricted to a controlled list of participants. While permissionless blockchains are open to everybody and the control is given away to an undefined community of people that want to participate in the system, a permissioned blockchain retains this control. Bad actors can be excluded, or a group of actors could be invited to influence the voting or operation in a specific way. Since all validators are known, the consensus mechanism can be governed much more easily. Often, *Proof of Authority* (PoA) or *Practical Byzantine Fault Tolerance* (PBFT) are used [44].

3.3 Smart contracts

The term Smart Contract was initially coined by Nick Szabo [45] and Vitalik Buterin [46] and is used with different meanings. It often describes one or more of the following aspects:

a) The **conclusion** of a legal contract by executing computer program code – especially code being executed by a blockchain.

b) The **execution** of a legal contract by executing computer program code – especially code being executed by a blockchain.

c) The **technology of programs/scripts** that are executed by a programmable blockchain and which executes transactions [43, p. 5].

Although the meaning of (a) and (b) provide some interesting legal discussions, in the context of this work, a smart contract means (c): small programs or scripts that are securely executed on a blockchain. Smart contracts render a blockchain programmable, so new types of transactions, *tokens* or other use-cases can be created on the same blockchain. *Tokens* are defined as *a digital representation of value on a shared distributed ledger that is owned and secured using cryptography to ensure its authenticity and prevent modification or tampering without the owner's consent* [43, p. 6]. Tokens can serve many purposes and represent many different tangible or non-tangible goods – or just themselves [47]. Tokens can be fungible when they are used as a currency or represent assets that are measured or counted. Tokens are *nonfungible* when they represent an entirely unique digital representation of assets [43, p. 4] like pieces of art. *Ethereum* [46] was the first and still is the most popular blockchain that supports smart contracts. While Bitcoin only has the Bitcoin token, Ethereum hosts about half a million different types of tokens [48] that allow standard token operations described in the token standard ERC20 [49].

The code for the transactions is executed and verified on every node of the Ethereum blockchain. This turns the Ethereum blockchain into an almost unstoppable *world computer* that will not deviate from the program code deployed and will execute it in an almost unstoppable manner and exactly as specified [50]. *Vitalik Buterin*, a co-founder called these scripts *smart contracts* [46, p. 13]. Calling a computer program a "smart contract" has led to confusion and *Buterin* has since apologized for it [51].

Smart contracts can be programmed in a similar way compared to normal programs. The programming languages *Solidity* allows to define a smart contract in an object-oriented way as an object with methods and properties [52]. There are three different storage possibilities: *Storage* which is permanent and expensive, *memory* which is cleared at every external function call and a *stack* [53]. The status of storage of a contract is incrementally stored on the blockchain in a data structure called *Merkle Patricia Tries* [54]. When a variable in the *storage* is changed, the new value is written in a new block. The old value will remain in the old block but will no longer be used. Merkle Patricia Tries allow to efficiently access the value of the variable in the block where a transaction was executed that modified the variable the last time.

Smart contracts can authenticate actors through their private keys. They can store hash values as a fingerprint of digital objects to timestamp and to sign those objects. Smart contracts can help increase supply chain transparency [55, p. 10]. They can be used to save a trail to show the source of the input materials for manufacturing. Last but not least, smart contracts are used to create and define the parameters of tokens. Using the Solidity smart contract language for Ethereum, for example, it only takes very few pages of code to define a new token together with proprietary rules for the transactions. These rules might set conditions that transactions need to meet in order to be executed. For example, transactions could be limited to a specific time interval, to specific parties, or could require validation by third parties, etc. These rules are programmed into the smart

contract which will automatically enforce them. Ethereum smart contracts allow this data to be managed, amended, or revised according to the rules defined and documented in the smart contract. Public blockchains offer a variety of advantages over a PKI-based qualified electronic signature: They do not require trust in single entities, do not require registration, have solved the issue of regular timestamping of signatures and are available on a global scale. However, DLT does not regularly provide a reliable authentication of actors. Another issue is the governance of blockchains. While blockchain technology offers a high degree of immutability, this is not always desired. Software almost always contains bugs. Rules might need to change, and attacks require the adaptation of protocols. Anybody that is changing the software will be able to manipulate the blockchain. Therefore, the decisions about the evolvement of software and protocol used for a blockchain, which is called *blockchain governance*, should not be done by a single party but in a decentralized manner. With Ethereum, this need for blockchain and smart contract governance became apparent when a bug in a smart contract called *Decentralized Anonymous Organization (DAO)* would have almost caused the loss of substantial funds [56]. The Focus Group on Distributed Ledger Technology at the International Telecommunication Union has collected applications, technical, regulatory and standardization issues regarding DLT in a series of reports that offer an introduction to these topics [57]. Standards organizations like the ITU or ISO are developing standards for distributed ledger technology like ISO TC/307 [58] or ITU study group16 question 22 [59].

For digital credentials, smart contracts can be used to check permissions, store hashes, add revocations and verify diplomas. Most times, a smart contract is not used directly but interacts with a user interface application. This user interface application can be deployed anywhere, multiple times and relies on the data stored in the decentralized smart contract. These apps are also called *decentralized apps*, or *DApps*. Those DApps are often used to verify digital credentials that can be verified against a blockchain – e.g., by means of comparing a hash value of the original credential file.

3.4 Data protection

Hessen in Germany introduced the first data protection law in 1970. The Council of Europe opened Convention 108 for signatures on January 28th, 1981. Currently 55 countries have ratified Convention 108 – including 8 countries outside Europe that are not members of the Council of Europe [60]. 16 countries have currently ratified the updated Convention 108+ [61] that was adopted in 2018. Data protection was introduced as a fundamental right by the German constitutional court in 1983. When Germany wanted to enforce a comprehensive census on its population, the constitutional court established the *right to informational self-determination* and positioned it as a fundamental right that protects citizens against the government [62].

Data protection protects natural persons in relation to the processing of personal data. Privacy (Respect for private and family life, Article 7) and data protection (Article 8 nr. 1) are considered fundamental rights in the EU [63] since

the charter was proclaimed in the year 2000. For the *European Economic Area* (EEA), data protection has been governed since May 25th 2018 by the *General Data Protection Regulation* (GDPR) [64] which repealed the prior Data Protection Directive [65]. In Switzerland, the *Federal Act on Data Protection* (FADP/DSG/LPD) [66] is currently being revised [67]. The revised law should enter into force in September 2023 [68]. For cantonal institutions in the Canton of Geneva, data protection is governed by *Loi sur l'information du public, l'accès aux documents et la protection des données personnelles* (LIPAD) [69]. The purpose of data protection is the protection of fundamental rights and freedoms of natural persons. It includes a broad range of obligations, which also include information security regarding processing personal data. The term and definition used in data protection regulation vary between jurisdictions. This work adapts the terms and definitions of the GDPR. The GDPR has been in force since 2016 with a start of application on May 25th, 2018. It has served as a model for data protection in the world and has been called a *gold standard* [70].

Data protection is guided by the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and last but not least accountability (Article 5 GDPR). The GDPR demands *data protection by design and by default* (Article 25 GDPR). Technical and organizational means like, for example, encryption, access control or data minimization, can reduce the risks to data subject. Data protection by default sets the most data protection-friendly setting as the default value so that users have to opt-in to processing personal data rather than force them to opt-out when they do not want their data to be processed. In the context of blockchain applications, data protection by design becomes particularly important for two reasons: First, while data in conventional applications can be deleted easily, the immutability of blockchains forces controllers to do it right from the start. Second, when a system is public and governed in a decentralized fashion, it is more difficult to enforce limitations on the processing. Technical restrictions can be a good – sometimes even a better – replacement for organizational measures, because they are more difficult to circumvent.

The GDPR has a broad area of application. Although not a Swiss law, it also applies to many companies in Switzerland if goods or services are offered to people in the EU or if a controller or processor is established in the EU (see Article 3 GDPR, also section 8.4.8). Excluded is manual data processing unless the data is part of a filing system or intended to form part of a filing system (Article 2.1 GDPR). The GDPR is not applicable to the data processing in the context of a purely personal or household activity (Article 2.2.c GDPR). This *household exemption* is important when blockchains are used directly by data subjects. The CNIL applies the household exemption to blockchain transactions that are entered into for a purely personal or household activity.

The GDPR knows the following roles in data processing: The *controller* determines purposes and means of data processing. The *processor* does the data processing, and the *data subject* is the natural person that the data can be identified with. It is important to note that roles can be taken by several persons

at the same time: Data can often be identified with more than one person. Processing can be done by multiple data processors and there can even be data sub-processors. There can be several controllers too. In this case, the controllers can either be *joint controllers* (Article 26 GDPR), that is, they jointly determine purposes and means of the data processing – or they can also be considered independent data controllers. The model of data controller and processor is a pattern that was true in the 1980s with computing centers that did the data processing for a customer. Today, this pattern is often too simplistic. For example, applications are distributed and updated through an application store. The processing is partly done on the device of the data subject under some control of the data subject and other parts of processing is done on one or more servers. Sometimes an open protocol is used, and the application is provided independently from the operation of the server. In case of, for example, COVID certificates, the data processing might then be requested when entering a restaurant. The identification of one or more controllers for the COVID certificate application seems to be very difficult. Similarly, with blockchains, there is some case-by-case elaboration by the CNIL who should be considered the controller, but there does not exist legal certainty (see also section 8.4.16).

Every processing of personal data requires a justification. Processing is almost any operation (Article 4 nr. 2 GDPR). Even continuous storage of data, allowing others to access the data or erasure of data is considered *processing*. However, the German Oberverwaltungsgericht Hamburg restricted processing to conscious activities and excluded mere unconscious storage of physical files [71]. Storage of data on a decentralized ledger, therefore, can hardly be excluded from the meaning of processing.

The main justifications are consent, contract, legal obligation or legitime interest:

- ***Consent*** (Article 6.1.a and Article 7 GDPR) must be informed and freely given. Consent can always be withdrawn, and processing needs to stop when consent is withdrawn. This renders consent a difficult basis for processing data on immutable blockchains.
- The processing of personal data can be necessary for the performance of a ***contract*** the data subject is party in (Article 6.1.b GDPR). If a delivery of an item purchased requires the address to be processed, the contract obligating the vendor to deliver the item can serve as a legal basis for the processing of that personal data. An education contract might include the obligation to issue a diploma at the end. Similarly, a contract requiring payment in Bitcoins could cover the processing of personal data (e.g. the Bitcoin address) on the Bitcoin blockchain.
- ***Legal obligations*** can also serve as a justification (Article 6.1.c GDPR). Merchants, for example, are required to keep records of their transactions. This obligation justifies the storage of records that contain personal data as long as required by law.
- ***Legitimate interest*** is another possible justification (Article 6.1.f GDPR). When, for example, personal data is required to defend unjust legal claims

that arise out of prior interaction, this data can be kept. Applicants for employment that are rejected might sue employers because of unfair discrimination. Employers therefore have a legitimate interest to store the documents of the application as long as applicants could sue the employer. Legitimate interest always requires balancing the interest pursued by the employer with the interest or fundamental rights and freedoms of the data subject. The data subject might also object to the data processing unless the controller demonstrates compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the data subject (Article 21.1 GDPR).

Possible justifications depend on the use-case. According to the principle of purpose limitation, every justification only justifies processing for a purpose that is directly connected to the justification given.

Even with a proper justification, there are still many obligations that need to be adhered to. There is the obligation to inform the data subject (Articles 12-14 GDPR). The data subject has a right of access (Articles 15 GDPR) which means that she can request a confirmation whether personal data relating to the data subject is being processed. If this is the case, details about the data processing as well as a copy of the data can be requested.

Controllers also have to respect the *right to erasure* ("*right to be forgotten*") (Article 17 GDPR). If the data processing is no longer necessary in relation to the purposes for which they were collected, they need to be erased. Erasure is also required when the justification is no longer there, for example because consent has been withdrawn or processing on the basis of legitimate interest has been objected to. This is often discussed in the context of the immutability of blockchains. The Austrian Datenschutzbehörde considers dereferencing already to be erasure [72] while the European Data Protection Board (EDPB) demands that the controller shall make sure that it is not possible to recover deleted data [73, p. 23]. For further discussion regarding the right to erasure see section 8.4.11. The data subject can demand to rectify incorrect data based on the *right to rectification* (Article 16 GDPR). While some data is disputed between the controller and the data subject, the data subject can demand that the processing of that data is restricted (Article 18 GDPR), meaning that the data may only be processed for limited purposes or with the data subject's consent. The *right to data portability* (Article 20 GDPR) obliges the controller to transmit the data provided by the data subject on request to another controller.

Controllers need to have *processing agreements* with processors (Article 28.3 GDPR), keep *records of processing activities* (Article 30 GDPR), implement an *appropriate level of security* (Article 32 GDPR) and *notify* the data protection authority and the data subject in case of certain *data breaches* (Article 33 GDPR).

When the processing particularly uses new technology and is likely to result in a high risk to the rights and freedoms of natural persons, a *data protection impact assessment* (DPIA) is obligatory. The assessment covers the necessity and proportionality of the processing, an assessment of the risks to the rights and

freedoms of data subjects and the measures envisaged to address those risks including the safeguards and security measures and mechanisms to ensure the protection of personal data (Article 35 GDPR).

3.5 Self-sovereign identity

Self-Sovereign Identity (SSI) is an identity that is under the control of a user and can be used for multiple services. SSI strictly separates the identifier from the claim. While identifiers are generated by the user, claims are certified as credentials by the entities that are entitled to do so. Users can generate as many identifiers as they wish and thereby protect their privacy, so that credentials cannot be linked.

Christopher Allen lists ten principles for SSI [74]:

1. **Existence**: *Users must have an independent existence*. Independent from a service provider.
2. **Control**: *Users must control their identities*. Identity is clearly separated from a claim. While a user may select an ID, even her official name, or birthdate is a claim and not the identity.
3. **Access**: *Users must have access to their own data*. No data must be hidden or dependent on gatekeepers. Claims by other entities regarding that user may be stored, hidden or deleted by the user. However, the user must not alter them.
4. **Transparency**: Systems and algorithms must be transparent. The system and their management must be open so that anyone is able to examine how they work.
5. **Persistence**: *Identities must be long-lived*. Users may choose to stop using an ID, but they should not be forced to do so.
6. **Portability**: *Information and services about identity must be transportable*. Identities should not be restricted to providers or jurisdictions.
7. **Interoperability**: *Identities should be as widely usable as possible*. Identities should be able to be used globally, not restricted to a country or a niche while users remain in control.
8. **Consent**: *Users must agree to the use of their identity*. Claims might be expressed by other persons without consent, however, they should not become valid without the consent of the user.
9. **Minimalization**: *Disclosure of claims must be minimized*. Data disclosed should be limited to the minimum amount of data necessary to accomplish the task at hand. For example, when a minimum age needs to be proven, neither the exact age, nor the name should be disclosed.
10. **Protection**: *The rights of users must be protected*. When in doubt about choosing between the needs of the network and the freedoms and rights

of a user, the latter should prevail. This can be ensured by censorship-resistant algorithms that run in a decentralized manner.

Blockchain technology enables the implementation of a decentralized identity provider that is not owned by a single entity. Thus it enables digital identities that are under (almost) full control of the associated subject [75]. De facto standards for *Decentralized Identity* (DID) [76] and *Verifiable Credentials* (VC) [77] have been published by the *World Wide Web Consortium, W3C*. Frameworks like *Jolocom* [78], *Sovrin* [79], *uPort* [80] and *Blockstack* [81] have been created. In contrast to other solutions, neither credentials themselves nor hashes of credentials are stored on a blockchain. While uPort and Jolocom are based on Ethereum, Sovrin and Blockstack come with their own, proprietary blockchains. Jolocom and Sovrin implement the W3C recommendations for DID and VC, uPort and Blockstack use proprietary definitions. All frameworks do not store verified credentials but only the decentralized IDs on the blockchain. Verified credentials – and with Blockstack also lots of other information are stored in cloud systems at the user's discretion. While Jolocom, Sovrin and uPort are limited to identity and credentials, Blockstack serves as a complete environment with single sign on for many different applications that deal with user associated data. Sovrin also integrates selected disclosure through Zero Knowledge Proofs. Neither Sovrin, Jolocom, uPort nor Blockstack offer out-of-the-box systems for university diplomas, but they can be used as frameworks to do so.

Chapter 4 State of the art and related work

Before defining requirements and proposing a design, the state of the art of existing systems for the verification of digital long-term credentials is surveyed. Most systems are at development stage or in very limited use. This analysis of the state of the art is limited to the field of university diplomas. It starts with the review of existing comparative studies, then defines a review matrix and then reviews individual systems.

4.1 Existing evaluations

Comparative studies can serve as a good entry point to the evaluation of digital diploma certification systems. They provide not only an input on existing systems and approaches but also input that leads towards evaluation criteria. This section only refers to papers that include an extensive comparison. Papers that mainly propose a specific solution but start with a brief comparison of approaches will only be referred to later on when specific solutions are being discussed.

In 2014, a pre-study was done by *Ronchi et al*, for *Switch*, a foundation to provide digital services to Swiss universities, the *University of Geneva* and the *University of Lausanne* [82] and compared different existing solutions and approaches:

- Digitally signed PDF (see section 4.3.1)
- Open Badge Hosted or Signed (see section 4.3.4.3)
- Secure Certificate Repository + Unique ID
- Trusted Timestamp
- 3rd party service (CVTrust, Accredible)
- Classic paper-based certificate

It must be pointed out that blockchain was not being discussed in this study in 2014. However, in 2020 two papers were published by *Jat* [83] and *Saleh/Ghazali/Rana* [84] that compared the same six blockchain-based systems. While *Saleh/Ghazali/Rana* also propose a framework (see 4.3.6.6), *Jat* is limited to the evaluation. Both compare the following systems:

- *University of Nicosia* (UNIC) (see section 4.3.5.3)
- *MIT Blockcerts*, which is based on *Open Badge* hosting (see section 4.3.4.4)
- *MIT Media Labs*
- *SmartCert* (see also SmartCert2 in section 4.3.6.7)
- *KMI-OU UK*, a use-case from *Knowledge Media Institute* of the *Open University UK* (see section 4.3.9.1)
- *RecordsKeeper* (see section 4.3.6.3).

The comparative studies apply different criteria for evaluation. All cover the main aspects as security, authenticity/recognition in some way, and privacy. *Ronchi et al* did the most comprehensive evaluation including the following aspects that were applied in the context of creation, verification, storage and distribution of the credentials [85]:

- Usability for credential holders and credential verifiers as well as for credential issuing organizations and their staff
- Implementation complexity and technical limitation due to format/protocol used
- Costs for individuals and organizations
- Long-term issues / durability
- Legal compliance, particularly regarding data protection regulation
- Reliability/security
- Revocation
- Distribution to credential holders and further distribution to credential verifiers

Jat used a different set of evaluation criteria [83, p. 9581]. He grouped the criteria into three categories without entering into too much detail. Like *Ronchi et al.* he included usability aspects:

- System features (Accreditation, Verification, Revocation)
- Security features (Counterfeit Protection, Privacy, Selective Disclosure, Transparency)
- Usability (User Experience, No Key Management, Accessibility)

Saleh/Ghazali/Rana [84, p. 80] did not include revocability and arrived at five criteria that they defined as follows:

- Authentication: Are students and verifiers required to have an account on the blockchain used?
- Authorization: Do students need authorization to share a diploma with an employer? Do employers need authorization to verify a diploma?
- Confidentiality: Is the student's personal data secured against unwanted access?
- Ownership: Is the diploma tied to a blockchain account that controls it?
- Privacy: Privacy of private keys to ensure that no fake diploma is created.

Since *Ronchi et al.* compared different systems, their results cannot be compared. For digital signatures, they saw the main disadvantages in the complicated and costly setup process and the missing revocation possibility. For Open Badge they raised doubts as to whether the system would gain broad acceptance. Trusted timestamps had the same issue of missing revocability. Third party services were seen as costly. Finally, a secure centralized certificate repository organized by participating universities and managed by Switch was seen as the best solution, however legal recognition and data protection regulation were seen as open questions.

			UNIC	*Blockcerts*	*Smartcert*	*KMI-OU UK*	*MIT Media Lab*	*RecordsKeeper*
Jat	System Features	Accreditation	No	No	No	No	No	Yes
		Verification	Partially	Yes	Yes	Partially	Partially	Partially
		Revocation	No	Partially	Partially	No	No	No
	Security Features	Counterfeit Protection	Partially	Partially	Partially	Partially	Partially	Yes
		Privacy	Yes	Yes	Yes	No	Yes	Yes
		Selective Disclosure	No	No	No	No	No	No
		Transparency	Yes	Yes	Yes	Yes	Yes	Partially
	Usability	User Experience	Yes	Yes	Yes	Partially	Yes	Partially
		No Key Management	Yes	No	No	No	No	No
		Accessibility	Yes	Yes	Yes	Partially	Yes	Partially
Saleh/Ghazali/Rana	Essential security themes to fulfill in educational certificate verification in blockchains	Authentication	No	No	No	No	No	Yes
		Authorization	No	No	Yes	No	Yes	No
		Confidentiality	No	No	No	No	No	No
		Ownership	Yes	No	Shared	No	Yes	Shared
		Privacy	Yes	No	No	Yes	Yes	No
	Salient Features, Functionalities		Handles fake certificates Tools available for the authenticity of the certificate Good in integrity, privacy, and ownership	Based on open platform	Resolves problem of fake certificate Student shares hash with the employer	Badges, certificates and web reputation in the blockchain	Offers more control to students Uses digital keys	Proof of authenticity in the certificate The entire verification process is based on ownership
	Shortcomings in feature/functionality		Requirements for an employer to verify the certificate is inadequate A student cannot authorize the prospective employer to verify the certificate No clear method of authenticity of parties	No separate verification service Vulnerable to spoofing attacks	Vulnerable to attacks Need for basic information security measures No clear method of authenticity of parties	Does not support employers as an entity Date is stored on public blockchain The certificate is vulnerable to manipulation No clear method of authenticity of parties	Level of trust is low The certificate can be accessed by everyone No clear method of authenticity of parties	Certificate tampering vulnerability

Source: Adapted from *Jat* and *Saleh/Ghazali/Rana*

Figure 3: Merged evaluation from Jat [83] and Saleh/Ghazali/Rana [84]

Since *Jat* and *Saleh/Ghazali/Rana* evaluated the same systems, their result was merged in Figure 3. While both agreed on some aspects, for example, on *authenticity/accreditation* requirement complied by only one system, the result differs on the *privacy* requirement. It was evaluated negatively by *Jat* for one system, but *Saleh/Ghazali/Rana* evaluated privacy negatively for three other systems. While *Jat* placed Blockcerts at the top, *Saleh/Ghazali/Rana* saw it last. *Saleh/Ghazali/Rana* also propose their own approach at the end of the paper,

which is evaluated here in section 4.3.6.6. Two years before, *Ghazali/Saleh* had already proposed a different approach (see section 4.3.6.5).

These comparative papers only covered some systems and approaches and only *Ronchi et al.* discussed properties and approaches/systems in some detail. The comparative studies, however, were able to demonstrate which properties are seen as important when evaluating a system for the certification of diplomas or other long-term credentials.

4.2 Evaluation criteria

For a detailed verification, a proper list of evaluation criteria is required. A diploma verification system is confronted with many concerns: The system should provide secure, durable, undeniable proof for a diploma at all times. This translates into *security*, *proof of authority*, *durability*, *autonomy, transparency* and *legal recognition*. Diplomas should also be *revocable*. Digital credentials should as well respect the privacy of credential holders and comply with *data protection* regulation. Then there are also more practical aspects like *usability*, *integration* and *automation*. Finally, a system should be *environmentally* sustainable and *economically viable* and provide proper *governance* in case some major revision or migration is required for technical or other reasons.

The led to the following reference list for the evaluations (Table 1):

Criteria	Description
Security	The certified diplomas shall be hard to forge. This includes the manipulation of existing diplomas as well as the creation of fake diplomas. Security also includes the fact that the revocation of a diploma should not be able to be hidden.
Proof of authority	Proof of authority means that it can be verified that the diploma has been issued by the university that it claims to be from and that the verification system has been authorized by the issuing institution. Is the website or the smart contract on a blockchain controlled by the institution that it pretends to represent? If somebody else who does not have the authority to grant or certify a diploma is certifying a diploma, this has little meaning. As a side aspect of this, the proof of authority could not just prove that the diploma has been issued by an institution with a specific name, but it could even include a certificate from the proper authority, that this institution is in fact a publicly recognized university that has the authority to issue diplomas. Some legal entities carry “university” in its name but are not properly accredited to issue valid diplomas [86].
Durability	When somebody graduates at the age of 20, she should be able to prove the authenticity of her diploma for decades, for example until the age of 70. Durability also relates to other aspects like security, proof of authority, legal recognition and governance but particularly requires that verification is still possible when the institution no longer exists.
Legal Recognition	A digital diploma should have similar value to the paper version. It should be more than a mere technical procedure to increase the trust in an unverified copy. Legal recognition is not evaluated in depth since it depends on governing local laws and regulations. When diplomas are used

	internationally, a notarization – or in case of member states of the Convention of 5 October 1961 *Abolishing the Requirement of Legalisation for Foreign Public Documents* an *apostille* – might be required. The legal validity of an electronic diploma allows apostilles and e-apostilles to be applied onto electronic diplomas in a similar way to paper documents.
Autonomy	Closely related to durability is autonomy. A digital diploma should be verifiable independently from the university in case the university server is not available, or the university ceases to exist. The verification should also not depend on any other single institution.
Transparency	Transparency is closely related to autonomy, which means that the system should not be a black box but that the verification mechanism itself can also be verified.
Revocability	It should be possible to revoke a diploma – for example because of error, fraud, replacement by a superior title or when the name and/or sex of a student changes.
Data protection	Diplomas should also respect the privacy and other data protection rights of credential holders. *Data protection* demands that credentials are only visible to those the credential holder grants access to or those who have a legitimate interest to review the data. According to the principle of data minimization, the verification should also leave no or the least possible trace in centralized servers. The EU *General Data Protection Regulation* (GDPR) is used as a reference here.
Usability	The system must be easy to use. It should not require the installation of additional software. Whenever the verification of a diploma is costly or requires a huge effort, employers or other people who should check a diploma might skip the verification.
Automation	Verification should be possible by automated recruitment systems: Upon the candidates' resumes uploading to a recruitment system, authenticity of the presented diplomas should be automatically verified through some kind of *application programming interface* (API).
Integration	It should be possible to smoothly integrate the emission of diplomas with the student administration system.
Governance	During the lifespan of a diploma many issues might arise concerning individual diplomas, keys, administrative processes, the University as well as software and external infrastructure used. It is impossible to predict every possible threat. A robust governance mechanism should be able to react to this by being able to manage keys, smart contracts and migrate the diplomas to a different infrastructure when required.
Economic viability	The system must not be too costly. This concerns the costs for issuing diplomas as well as for providing a system that is able to verify diplomas.
Sustainability	The system should not consume a lot of energy. Blockchains like *Bitcoin* or *Ethereum* that use the *Proof of Work* (PoW) consensus algorithm consume a lot of energy. Currently, a single Ethereum transaction on the public Ethereum network consumes about 76 kWh [87].

Table 1: Evaluation criteria

For every evaluation criterion a grade is given in the range of --, -, 0, + and ++. The grades are meant as a qualitative indicator of how much a criterion is fulfilled. The amount of information available on each system differs. Often, only a short

paper is published. For some, the source code and a detailed description was available. Some systems could be tested in action including verifying the information on a public blockchain. Only systems were evaluated in detail where enough information was available. Systems are grouped by their approach. The principle of the approach is being described first and then individual systems – if they exist – are described and evaluated. Most striking advantages and disadvantages are emphasized. Some systems combine different approaches. They are then listed in the most relevant category. A short evaluation of the 14 criteria listed above will be done and summarized in a table.

4.3 System evaluation

The different approaches are grouped into 9 categories:

The first three categories concern different types of signed or certified copies – electronic and on paper. First, it starts with *qualified electronic signatures* that already have a legal basis for several decades in the law. Second, *certified copies* are copies created by public notaries or other public institutions. They can be created on paper or electronically with a qualified electronic signature by the notary. Third, *apostilles* are a special instrument to verify documents when exchanged internationally. Apostilles also exist on paper as well as e-Apostilles.

The next category is online verification where an online system of the university or another institution verifies the diploma directly. It is based on the assumption that the verification service is available and trusted.

The use of blockchain technology covers the next three categories. The almost immutable ledger of a blockchain can record digital fingerprints of a diploma. The first category is mere timestamping of this fingerprint. The second category consists of dedicated blockchains. The third category is the use of smart contracts to accommodate a more sophisticated diploma management on a standardized blockchain.

The next category is *self-sovereign identity* (SSI). SSI aims at maximizing user control over their electronic identity and the verification of credentials. SSI also uses blockchain technology, but usually only for anchoring the decentralized identities, but not the credentials.

Finally, a category *other* is added to describe other systems that were not discussed in detail.

4.3.1 Qualified electronic signatures and seals using PKI

Qualified electronic signatures and qualified electronic seals are available and enjoy legal recognition. However, they lack international reciprocal recognition. In the long-term variant CAdES-B-LTA [88] (PAdES-B-LTA [89] for PDFs) that packages the certificate chain with the signature, regular time stamping is required to ensure legal validity. There is also a variant with less legal recognition: An advanced electronic signature might be recognized as legal proof but is not automatically deemed equivalent to a handwritten signature. CAdES-B-LT/PAdES-B-LT standardizes such an advanced electronic signature that does

not require regular timestamping. However, during the survey no university that uses either qualified or advanced electronic signatures or seals was identified.

Criteria	Evaluation	Grading
Security	Based on PKI – good as long as the chain of timestamps is not broken	+
Proof of Authority	Based on PKI – good as long as the chain of timestamps is not broken	+
Durability	Loses value when not regularly timestamped	-
Legal Recognition	Same as paper if chain of timestamps is not broken; full equivalence limited to a jurisdiction, e.g. EU or Switzerland	+
Autonomy	Validation can be done online, only list of revoked certificates needs online connection	+
Transparency	Procedures and laws are transparent	++
Revocability	No revocation of diplomas possible	--
Data Protection	Almost no personal data communicated outside the document viewer	++
Usability	Most PDF readers support qualified electronic signatures	++
Automation	Could be automated, standard APIs available	++
Integration	Can be automated, requires specific process and hardware	+
Governance	PKI governance provided by the trust centers, no individual revocations	+
Economic Viability	There are models with yearly fees and with remote signatures with fees per diploma. Models with yearly fees scale well.	+
Sustainability	Power consumption very limited	++

Table 2: Evaluation of Qualified Electronic Signatures

4.3.2 Electronic Certified Copies

An original paper credential can be replaced by a certified copy. The university itself as well as the state or a public notary can certify that a copy is identical to the original. In some instances, the notary might also certify the authenticity of the signature on the original copy and for some acts even the act itself (e.g., heritage or real estates). A notary can create a verified electronic copy of a document that has the same legal value as the certified copy on paper. The electronic copy is authenticated by an SCSE/ZertES-compliant qualified electronic signature. The validity is limited to Switzerland. The notary, however, can choose to apply a qualified electronic signature conformant to different standards, for example compliant to the EU-eIDAS-regulation that is accepted in the European Union. Copies of diplomas of Geneva or federal education institutions can be certified by the State of Geneva relatively cheaply for 5 CHF. Certified copies by a notary

start at 35 CHF. Although electronically certified copies are implemented in the law, they are not commonly offered by local notaries.

Criteria	Evaluation	Grading
Security	Based on PKI – good as long as the chain of timestamps is not broken and the paper original was not forged	+
Proof of Authority	Regarding the notary, strong proof of authority, based on PKI – good as long as the chain of timestamps is not broken. Regarding the university this depends on the scrutiny of the notary	+
Durability	Loses value when not regularly timestamped	-
Legal Recognition	Same as paper if chain of timestamps is not broken; full equivalence limited to Switzerland	+
Autonomy	Validation can be done online, only comparison with list of revoked certificates needs online connection	+
Transparency	Procedures and laws are transparent	++
Revocability	No revocation of diplomas possible	--
Data Protection	During verification no personal data communicated outside the document viewer	++
Usability	Several PDF readers support qualified electronic signatures	++
Automation	Could be automated, standard APIs available	++
Integration	Manual process, not very practical	--
Governance	PKI governance provided by the trust centers, no individual revocations	+
Economic Viability	Costs of at least 5 CHF per diploma	-
Sustainability	Complicated process, but not computationally expensive	0

Table 3: Evaluation of Electronic Certified Copies

4.3.3 Apostille

When using a foreign official document, the document generally needs to be authenticated by a Swiss authority to be valid in Switzerland and vice versa in a foreign country. This process requires an authentication chain where a public document in the origin country is certified by a cascade of authorities leading up to the foreign ministry of the state of origin, then the consulate of the state of production and finally the foreign ministry of the state of destination (Figure 4).

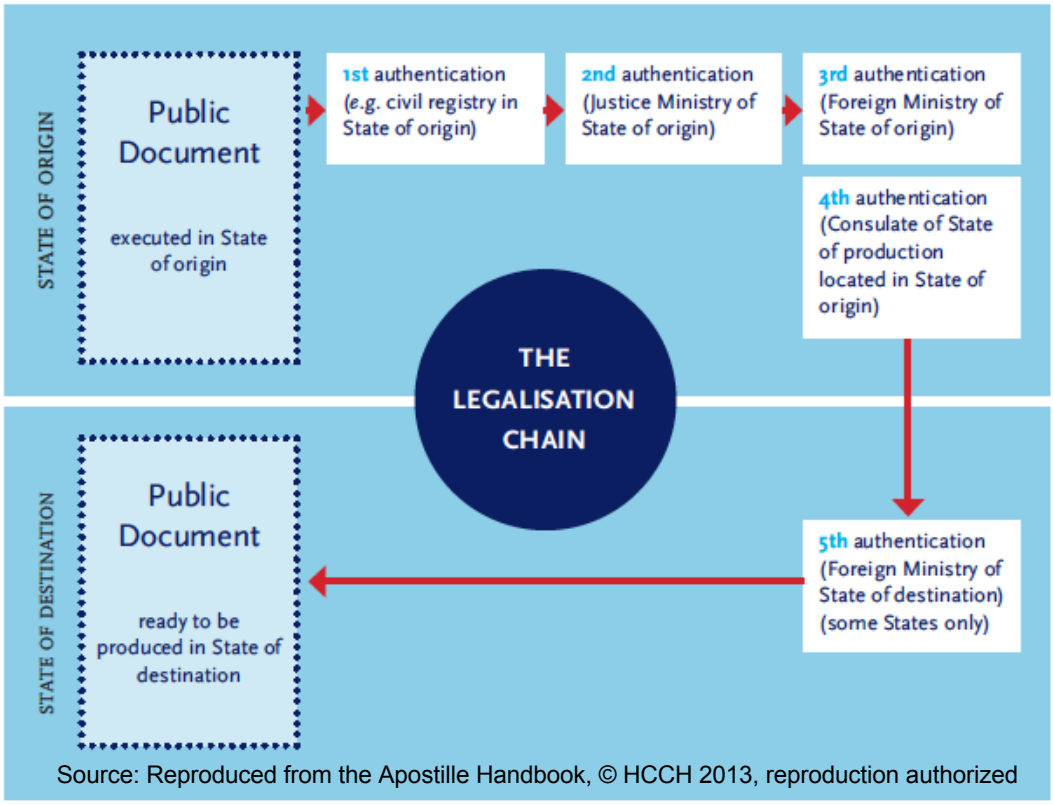


Figure 4: Legalisation Chain [90, p. 4]

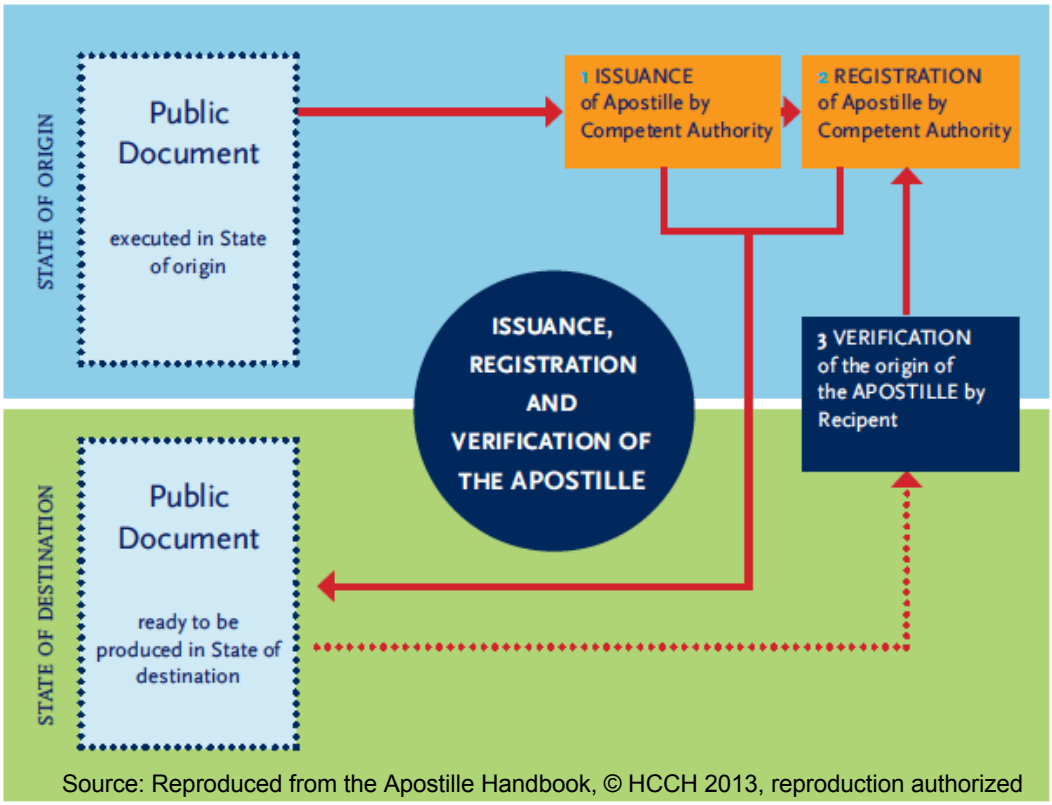


Figure 5: Apostille replacing the certification chain [90, p. 65]

To ease this process the Hague Convention of October 5th 1961 [91] replaced this requirement by introducing the legal instrument of an *Apostille*. The Apostille replaces the certification chain by a single, registered and verifiable certificate. An Apostille authenticates the origin of the underlying public document but does not certify the content nor that all requirements of domestic law for proper execution of the underlying public document are met (Figure 5).

Although the Apostille Convention was drafted only with a paper environment in mind, the Special Commission for the Apostille Convention launched the electronic Apostille Pilot Program in 2006. The electronic Apostille Program still authenticates paper documents but by means of an e-Public document by an e-Apostille recorded in an e-Register (Figure 6). An implementation chart shows which members have implemented e-Registers and e-Apostilles [92]. Up to now, Switzerland is not listed as having implemented either of them.

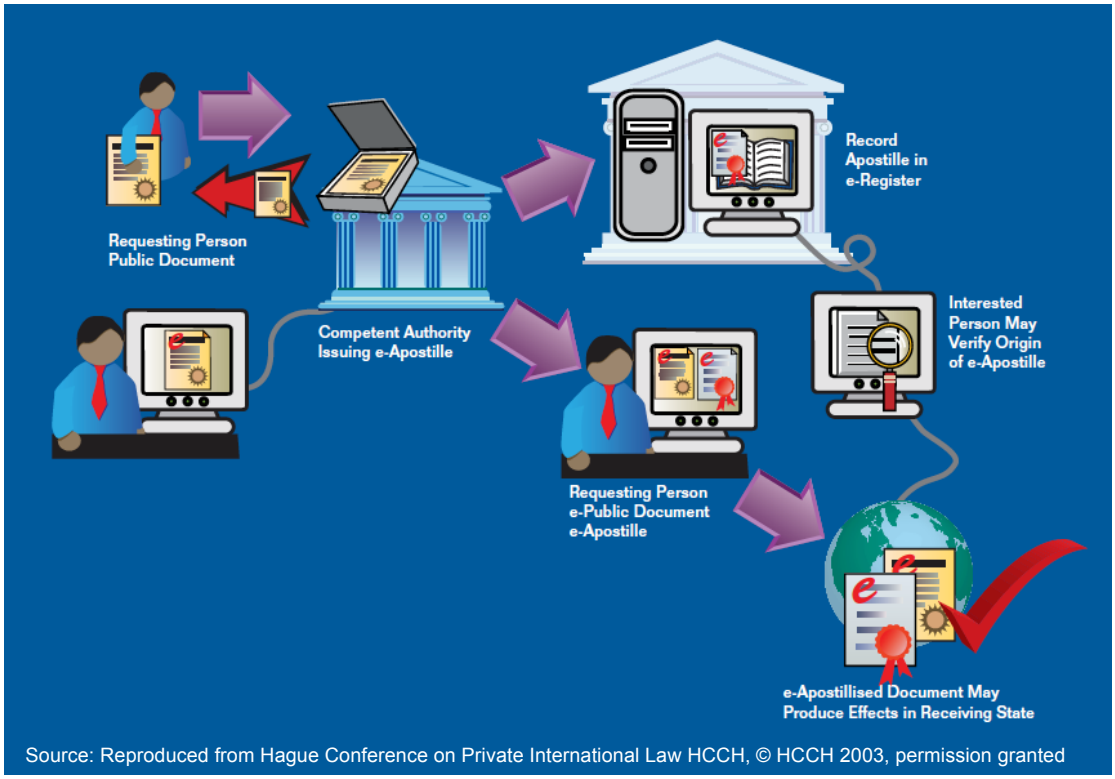


Figure 6: The workflow of the e-Apostille [93, p. 11]

Criteria	Evaluation	Grading
Security	Based on PKI – good as long as the chain of timestamps is not broken	+
Proof of Authority	Based on PKI – good as long as the chain of timestamps is not broken	+
Durability	Loses value when not regularly timestamped	-

Legal Recognition	Same as paper if chain of timestamps is not broken; equivalence in all states that have implemented the *e-Apostille Programme* (eApp); legal effects in issuing states may differ.	+
Autonomy	Validation can be done online, only list of revoked certificates needs online connection	+
Transparency	Procedures and laws are transparent	++
Revocability	No revocation of diplomas possible	--
Data Protection	During verification no personal data communicated outside the document viewer	++
Usability	e-Apostilles can be created as PDF-documents and most PDF readers support qualified electronic signatures	++
Automation	Could be automated, standard APIs available	++
Integration	Manual process, not very practical	--
Governance	PKI governance provided by the trust centers, no individual revocations	+
Economic Viability	Only website needed	++
Sustainability	Complicated process, but not computationally expensive	0

Table 4: Evaluation of Electronic Apostilles

4.3.4 Online Verification

A diploma could be verified by comparison through a website. Trust for this verification is created through authentication of the website through a TLS X.509 certificate [24]. The website can either offer a public listing or reply to a verification request where a confirmation requires the credential or some other form of authentication.

4.3.4.1 Public listing

Some universities publish their diplomas in an online journal. The University of Geneva lists their graduates online [94]. These archives go back until the year 1818 [95]. The names of students can be queried by search engines like Google. The indexing is not disallowed in the robots.txt of the University of Geneva website. However, a student can ask to be removed from that site.

This approach makes the verification of diplomas available to a wide public. At the same time, privacy aspects are only considered on demand (opt-out). A removal of some information already published, often will not be effective in protecting the student's privacy. A student that does not want to appear publicly in that list, is in danger of being suspected of having committed fraud when using her diploma. When the server of the university goes down, the information might get lost.

Criteria	Evaluation	Grading
Security	Relies on TLS certificates	+
Proof of Authority	Relies on TLS certificates	+
Durability	Relies on the availability of the server of the university	-
Legal Recognition	Can serve as proof, but difficult to capture the proof	-
Autonomy	Depends on the infrastructure of the university, but not on business hours	-
Transparency	Maximum transparency for those students who do not object	++
Revocability	Revocation possible, but revocation cannot be distinguished from fraud	0
Data Protection	No possibility of verification without public listing	-
Usability	Easy to search	++
Automation	Could be automated, but no standard API	-
Integration	Manual process	-
Governance	General website governance applies	+
Economic Viability	Operation of a website, not expensive	++
Sustainability	Operation of a website, not computationally expensive	++

Table 5: Evaluation of listing diplomas on the website of a university

4.3.4.2 My eQuals

My eQuals [96] is a common platform for providing online certificates for educational institutions in Australia and New Zealand. Documents can be shared through a link. The link can be protected by a pin and can have an expiry date. Documents can also be shared directly with institutions connected to My eQuals. It is also possible to obtain a cryptographically signed PDF, that is signed by My eQuals. However, My eQuals states that this should not be relied on, because it might not reflect the current status anymore. Institutions can revoke and update documents. Institutions that receive a higher volume of credentials (i.e., higher education institutions) may access credentials through a special portal as *Receiving Organizations (RO)*. Login to My eQuals can also be done through social media single sign-on with the university account. To have access independently from the university, students need to store their personal email in the system.

Criteria	Evaluation	Grading
Security	Relies on TLS certificates, also offers cryptographic signatures	++
Proof of Authority	Relies on TLS certificates and trust in My eQuals	+
Durability	Relies on the availability of My eQuals	0
Legal Recognition	Cryptographic signature could serve as proof but is not able to prove that the credential has not been revoked	+
Autonomy	Depends on the infrastructure My eQuals except for the cryptographically signed credentials that are autonomous but have limited validity.	0
Transparency	Some transparency due to the use of cryptographic signatures	+
Revocability	Revocation possible, limitation for the signed PDF indicated	+
Data Protection	Student controls access	++
Usability	Students need to create a login with their personal email addresses	+
Automation	API not yet provided. Receiving institution can access a special portal	+
Integration	Manual process	-
Governance	General website governance applies	+
Economic Viability	There is a cost per institution, numbers available on request	0
Sustainability	Not computationally expensive	++

Table 6: Evaluation of My eQuals

4.3.4.3 Open Badges

Open Badges [97] is a ten-year-old concept, standard and provides a set of open-source tools to create and manage credentials. The standard also addresses micro and soft credentials and the management of credentials. The aim of the system is to revolutionize the way we learn, not just the way we handle credentials. It advertises itself to be used for any achievement. The system is complex [98]. Students are required to store their credentials in software wallets that are called *backpack*. Originally it was a project at Mozilla. The standard was revised [99], [100] in 2018. The project has been transferred to IMS, a US non-profit member association. Open Badges can expire and can also be revoked. Open Badges can be verified against an online server or be based on JSON Web Signatures – a way to apply a digital signature on JSON data structures and base64 encoding.

Open Badges 2.0 consists of three types of modules [101]:

- An *Open Badge Issuer* is an application that allows for the creation of *Badge Classes* and the subsequent delivery of *Assertions* to recipients.
- An *Open Badges Displayer* is an application that displays successfully verified badges to viewers.
- An *Open Badges Host* is an application that can aggregate and publicly host Assertions for recipients. It also supports the export of badges at the user's request.

Badges contain visual representations. A badge is *baked* by including the assertion data into the metadata of the image, so that all data is included in the image file [102]. Baking allows all data to be included in one file.

Two kinds of badges are supported [103]:

- *Hosted Badges* that are successfully verified through https-requests.
- *Signed Badges* that are cryptographically signed using *JSON Web Signatures* (JSW).

Signed Badges are revoked using *Revocation Lists*. These revocation lists are publicly accessible and reference the revoked assertions through their IDs. These IDs are random numbers and can only be identified with assertions, if the assertions are known. Hosted Badges that are revoked should return a special return code that will identify them as revoked.

Mozilla introduced the Open Badge Backpack to store and share Open Badges credentials in a cloud. After Mozilla discontinued their Backpack service, alternative services were created – for example *BADGR* (section 4.3.4.4).

Between 2011 and 2015, Open Badge received considerable scientific attention. It has been mentioned in 53 peer-reviewed journal papers, 76 conference papers, 5 chapters in edited books and a research report [104, p. 7]. The literature is dominated by the discussion of innovative credential concepts like negative credentials, group credentials or student generated credentials [104, pp. 8–11].

Criteria	Evaluation	Grading
Security	Relies on TLS certificates in both variants (hosted and signed)	+
Proof of Authority	Relies on TLS certificates	+
Durability	Relies on the storage of the badge and the availability of the verification	-
Legal Recognition	Json Web Signature has some legal value as evidence, but does not have direct legal recognition	0
Autonomy	Open Badges is open-source but requires specialized software and services. In case of hosted badges, the verification depends on the host.	0

Transparency	Badges are cryptic and require special verification software and/or services. Code and specifications are public	-
Revocability	Revocation possible through revocation lists. Revocation lists depend on the availability of the institution.	+
Data Protection	Student shares credentials. Verification of credentials remains possible. Visibility of revocation requires access to the badge	+
Usability	Students need services and software store, display and verify badges	-
Automation	Open source. Integration possible	+
Integration	Possible	+
Governance	Open Standard. Many components need to be maintained	0
Economic Viability	Free system, but complicated to implement, hosted variant requires running a server. Paid system (BADGR) is easier to implement. Costs not publicly disclosed	0
Sustainability	Not computationally expensive	++

Table 7: Evaluation of Open Badges

4.3.4.4 BADGR

BADGR [105] replaces the Mozilla Open Badges backpack. It provides a full-service implementation to create and certify badges and micro credentials. BADGR offers access to online diplomas. There is a free and a paid version. The paid version allows the integration into the university computer system and university website. The strength of BADGR is the administration of micro credentials and *pathways* to acquire a pre-designed set of skills. Credentials from other universities can be imported if they comply with the Open Badges standard (see section 4.3.4.3). It is also possible to export badges using this format.

As an implementation of the Open Badges, the evaluation of BADGR follows that of the Open Badges standard.

4.3.4.5 Blockcerts

Blockcerts is an attempt by MIT's media lab (*Nazaré, Duffy, & Schmidt*) to connect Open Badges to the Bitcoin blockchain. Similarly to a Bitcoin wallet Blockcerts includes a wallet that provides the ability for the student to “prove” that the credentials belong to her [106]. For this purpose, a private/public key-pair needs to be generated by the student and the public key sent to MIT [107, p. 150]. The key-pair together with the credentials are then stored in an application that runs on the student's smartphone. The student receives a JSON file containing the Open Badge version of the diploma (see 4.3.4.3).

To reduce the costs of the transactions, multiple diplomas can be certified using a Merkle tree of hashes of the certificates. Revocation information is not available on-chain.

A security analysis can be found in [108]. *Baldi/Chiraluce/Kodra/Spalazzi* show that Blockcerts does not check the authenticity of the issuing institution [108, pp. 7–9]. To remedy this situation, they propose basing the signature on an established PKI infrastructure.

The Blockcerts solution was implemented at the University of Rome "Tor Vergata" and used to also record certificates that students received from other universities [109].

Using a private key to identify the student has several drawbacks. Firstly, credentials are non-transferable. However, a private key could be shared and therefore is of little use to prove that the student has herself acquired the credentials. Secondly, credentials usually carry identifying data like the name and the date of birth of the student, which can be verified against the name in the job application which usually is not anonymous, or to some official ID or passport.

Blockcerts is based on the Open Badge backpack concept and depends on a centralized infrastructure. Blockcerts was designed for the Bitcoin blockchain. Other blockchains could be used as well, but the extended functionality of, for example Ethereum smart contracts, is not used.

Criteria	Evaluation	Grading
Security	Forging of a Bitcoin entry is highly unlikely	++
Proof of Authority	Based on Open Badge verification through hosting the ID on the university website (TLS certificates). The Blockcerts protocol does not verify the issuer ID	-
Durability	Relies on the storage of the badge and the availability of the university's website	-
Legal Recognition	Hashes on blockchains are increasingly being recognized as legal evidence. However, here this can only refer to the fact that the certificate has not been tampered with after it has been created	0
Autonomy	Open Badges and Blockcerts are open-source but require specialized software and services. The Merkle tree is included in the certificate. However, neither the revocation list nor the verification of the institution is available via the blockchain	0
Transparency	Although the code and specifications are open-source, badges are cryptic and require special verification software and/or services	-
Revocability	Revocation possible through revocation lists. Revocation lists are not stored on-chain and depend on the availability of the institution	+
Data Protection	Student shares credentials. Verification of credentials remain possible. Visibility of revocation requires access to the badge and the institution‘s list	+

Usability	Students need services and software store, display and verify badges	-
Automation	Open source. Integration possible	+
Integration	Possible	+
Governance	Open Standard. Many components need to be maintained	0
Economic Viability	High transaction costs on public blockchains > 10 CHF	--
Sustainability	Public blockchains like Bitcoin or Ethereum involve very high CO_2 emissions	--

Table 8: Evaluation of Blockcerts

4.3.5 Simple Permissionless Distributed Ledger Timestamping

Although, the purpose of the creation of the Bitcoin blockchain was the creation of a digital currency [29], it can be used for other purposes too. Since Bitcoin transactions have a high level of immutability, any information contained in a transaction will be immutable as well. Since Bitcoin was the first blockchain, it was the first to be used this way.

4.3.5.1 Principles

In a Bitcoin transaction, additional data can be included through the OP_RETURN instruction. The amount of data per OP_RETURN instruction is very limited and has varied between 40-83 bytes depending on the Bitcoin version [110, p. 4]. Common cryptographic hashing functions like SHA2 or SHA3 produce hash values with a fixed size of between 224 and 512 bits – or 28 to 64 bytes. A hash value on the Bitcoin blockchain provides a secure time-stamp for the hashed document and is increasingly accepted as legal evidence in court [111][112][41]. This, however, does not mean that it is legally equivalent to a handwritten signature like qualified electronic signatures. In particular, a hash value on the Bitcoin blockchain can only be regarded as a secure timestamp. Additional evidence is needed to prove that the document has been created by an authorized person at the university.

4.3.5.2 Diploma.Report

Diploma.Report is a simple framework to use the OP_RETURN from Bitcoin to secure academic credentials [113]. To reduce the amount of Bitcoin transactions needed and the cost associated with these transactions, for every class or academic period, a class diploma report with a list of hashes of diplomas is created and the hash of that list is stored in a Bitcoin transaction [114]. The class diploma report is stored in cloud storage. To secure the authenticity of the diplomas, the Bitcoin address that paid for and authorized the transaction needs to be verified with a trusted source. Two schools used that system between 2015 and 2018 for a total of 679 diplomas in 7 batches [115]. The extra file on the cloud storage introduces a single point of failure. Revocation could be modeled by

removing that file from the cloud storage, however, this would not be very reliable, since the file could have been retained and copied to a different cloud storage.

Criteria	Evaluation	Grading
Security	Forging of a Bitcoin entry is highly unlikely	++
Proof of Authority	External to the system	--
Durability	Relies on the storage of the diploma register in a separate cloud	-
Legal Recognition	Hashes on blockchains are increasingly being recognized as legal evidence. However, here this can only refer to the fact that the certificate has not been tampered with after it has been created	0
Autonomy	The Bitcoin blockchain has a high level of autonomy. The cloud storage, however, requires continued maintenance	-
Transparency	Entry on the blockchain is transparent	+
Revocability	Revocation might be possible through removal of the diploma's report	0
Data Protection	Student shares credentials like a student shares copies of a paper diploma. The entry on the blockchain is useless without the diploma and the diploma's report	++
Usability	Verifiers were asked to calculate hash values themselves	-
Automation	Open source, integration possible	+
Integration	Possible	+
Governance	Few software components required. Storage of diplomas report in the cloud required; identification of the Bitcoin address with the university required	0
Economic Viability	Due to the verification of list of diplomas, transaction costs (> 20 CHF) can be divided by the number of diplomas per batch	0
Sustainability	More than 1000 kWh per batch of diplomas	--

Table 9: Diploma.Report

4.3.5.3 University of Nicosia / Block.io

In 2015, the University of Nicosia experimented with verifying academic credentials using the Bitcoin blockchain. This was also offered to other universities under the label block.co [116]. Contrary to Diploma.Report, the University of Nicosia includes a Merkle-tree of hash values instead of a list of hash values. This Merkle tree uses the Chainpoint format [117] and is stored as metadata in the PDF document of the certificate [118, p. 107]. The Bitcoin address which is then used for the issuing is also added to the metadata of the PDF document. This removes the requirement of storing the Merkle tree or a list

of hashes in a cloud like Diploma.Report does. To enable revocations, a *Blockchain Document Issuing Protocol* (BDIP) is used. This protocol uses the *OP_RETURN* field in Bitcoin transactions to issue or revoke credentials. For revocations, another transaction can be added by the same Bitcoin address [118, p. 109]. The protocol also allows the authority of the Bitcoin address to be revoked if the private key of the address has been compromised. Verification then requires finding the issuing transaction and checking whether the authority of the address or the credential has been revoked in another transaction.

Criteria	Evaluation	Grading
Security	Forging of a Bitcoin entry is highly unlikely	++
Proof of Authority	Through a trusted Bitcoin address, proof of authority of that address is external	0
Durability	Special open-source validation software is required	-
Legal Recognition	Hashes on blockchains are increasingly being recognized as legal evidence. However, here this can only refer to the fact that the certificate has not been tampered with after it has been created	0
Autonomy	The Bitcoin blockchain has a high level of autonomy	++
Transparency	Entry on the blockchain is transparent	+
Revocability	Revocation is possible. Either up to two credentials or a range of credentials can be revoked by a revocation entry	+
Data Protection	Student shares credentials like a student shares copies of a paper diploma. Entry on the blockchain useless without the diploma	++
Usability	A validation service has to be used	+
Automation	Open source. Integration possible	+
Integration	Possible	+
Governance	Some software components required. Root trusted Bitcoin address required	0
Economic Viability	Due to the use of Merkle trees, transaction costs (> 20 CHF) can be divided by the number of diplomas per batch	0
Sustainability	More than 1000 kWh per batch of diplomas	--

Table 10: University of Nicosia, Block.io

4.3.5.4 Gradbase

Gradbase is an early (2015) system where a hash out of relevant diploma data is calculated and written to the Bitcoin blockchain [119, pp. 21–23]. The verification is possible through a link, by scanning a QR-code that contains the link, through an online form or by using a browser plugin which can be used in connection with LinkedIn [119, p. 5]. The system does not seem to be very active anymore. The most recent messages on social media are from one year ago. Due to being

based on Bitcoin and the fact that the system requires one Bitcoin transaction per diploma, the cost per average Bitcoin transaction in the last 30 days was between 11 and 60 CHF, which is prohibitive for diploma verification.

Criteria	Evaluation	Grading
Security	Forging of a Bitcoin entry is highly unlikely, forging the QR-code however is easy	0
Proof of Authority	Through a trusted Bitcoin address	0
Durability	Special plugin is required	-
Legal Recognition	Hashes on blockchains are increasingly being recognized as legal evidence. However, here this can only refer to the fact that the certificate has not been tampered with after it has been created	0
Autonomy	The Bitcoin blockchain has a high level of autonomy. However, the coding of the entries in the QR-code is not available on the blockchain	+
Transparency	Entry on the blockchain is transparent	+
Revocability	Revocation is possible, but only one credential per revocation. This renders revocation expensive.	0
Data Protection	Student shares credentials like a student shares copies of a paper diploma. Entries on the blockchain are useless without the diploma. Data is hashed, additional entropy (*salt*) should be added	+
Usability	A validation service / plugin must be used, QR-code renders validation of paper possible. QR-code without plugin useless	0
Automation	Centralized API available, no mention of open-source API that directly connects to the Bitcoin blockchain	+
Integration	Possible	+
Governance	Some software components required. Root trusted Bitcoin address required	0
Economic Viability	Transaction costs of more than 20 CHF per diploma	--
Sustainability	More than 1000 kWh per diploma	--

Table 11: Gradbase

4.3.6 Dedicated Permissioned Distributed Ledger Systems

Instead of relying on an existing blockchains, these systems or approaches propose dedicated permissioned distributed ledgers for diploma blockchains that have been adapted to store the verification of diplomas.

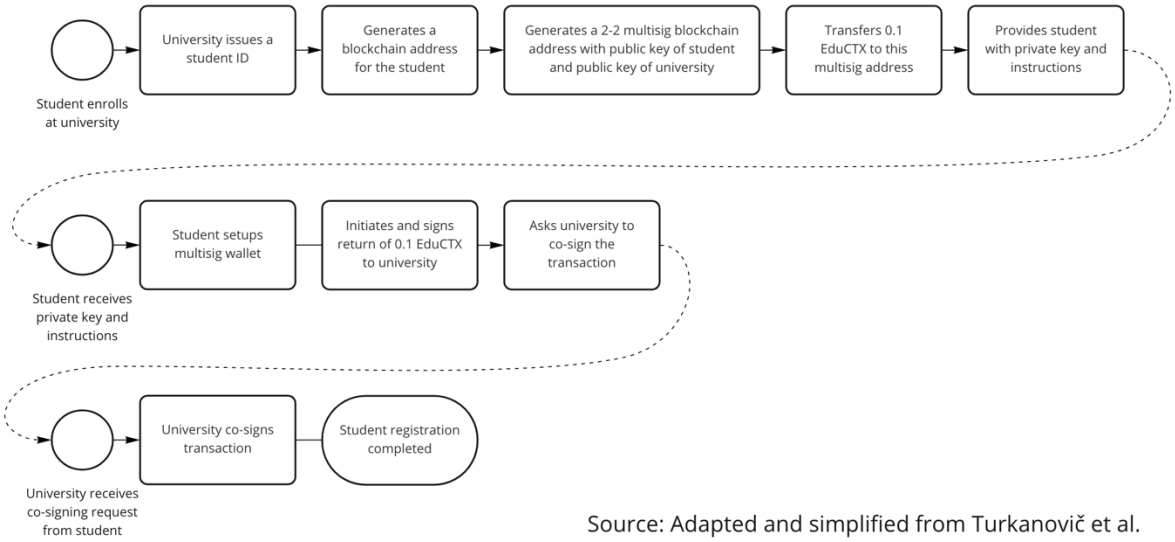
4.3.6.1 Principles

The purpose of the creation of the Bitcoin blockchain was the creation of a digital currency [29]. A side effect of this digital currency was a high level of immutability of the transactions. This feature of blockchain technology led to the creation of blockchains that are aimed at other use-cases. Since Bitcoin is not only creating a digital currency but is also based on the incentive that participants that create blocks will be attributed Bitcoins ("mining"), many blockchains created for other purposes, still include a digital currency to pay for the validation of transactions.

A permissioned distributed ledger system is a distributed ledger system where only a limited and pre-authorized group of actors can amend the ledger, i.e., create new blocks. The access to a permissioned distributed ledger system can be limited (private) or public [43, p. 4]. In permissioned ledger systems, the creation of blocks (*mining* or *block production*) is limited to people or institutions holding permissions to do so. Permissioned ledger systems can allow anybody or only a limited group of actors to create transactions. A permissioned distributed ledger system can use different consensus algorithms, like for example *Proof of Authority* (PoA). A disadvantage of permissioned DLT systems is possibly a lower number of validators, a dependency of validators with the entity that is attributing rights and limited possibilities to independent verification.

4.3.6.2 EduCTX (prototype 2017)

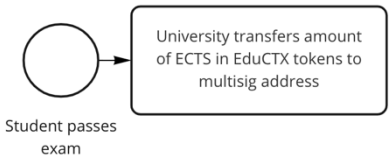
EduCTX was a prototype built using the *Ark* blockchain platform [120]. The system administers credit points of the *European Credit Transfer System* (ECTS) like a digital currency on a blockchain. The university creates a multisig-account for every student where two private keys are required for transactions. An initial 0.1 ECTS credit is transferred to that wallet and one of the private keys is transferred to the student. The setup is concluded by transferring the initial 0.1 ECTS back to the university (Figure 7). When a student passes an exam, the appropriate number of ECTS is transferred to her multisig account (Figure 8).



Source: Adapted and simplified from Turkanovič et al.

Figure 7: Process model of a student's registration in EduCTX, [120, p. 5120]

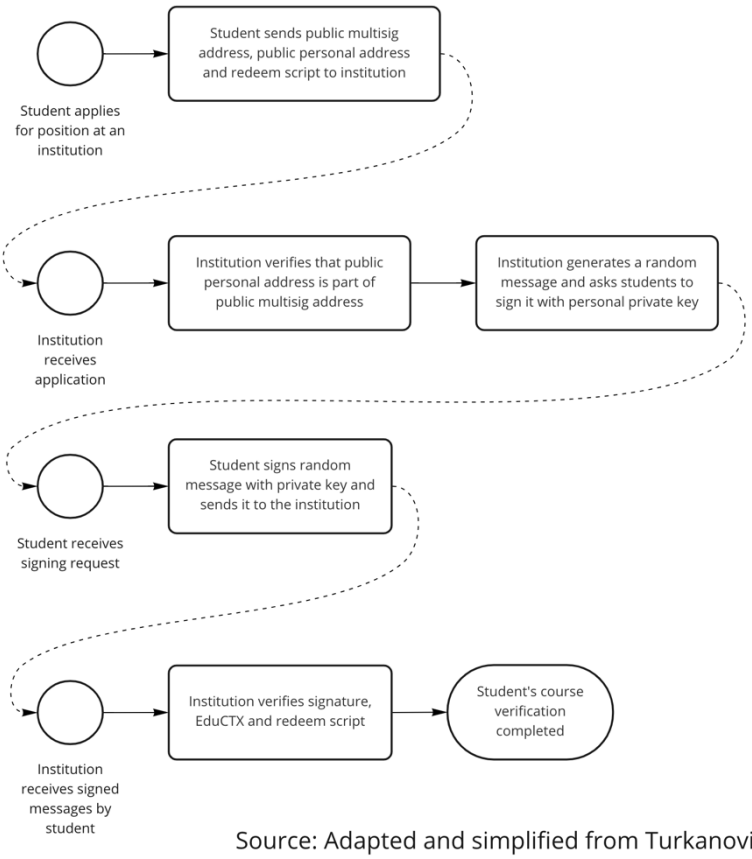
When applying for a position at an employer or a new university, the student sends her multisig address and proves that she is in control of the student key of the multisig-address. This can be verified by signing a message with the private key that can then be verified against the corresponding public key (Figure 9). A new university wanting to join the network, is verified by one of the current members and receives an appropriate number of ECTS-tokens from existing members (Figure 10).



Source: Adapted and simplified from Turkanovič et al.

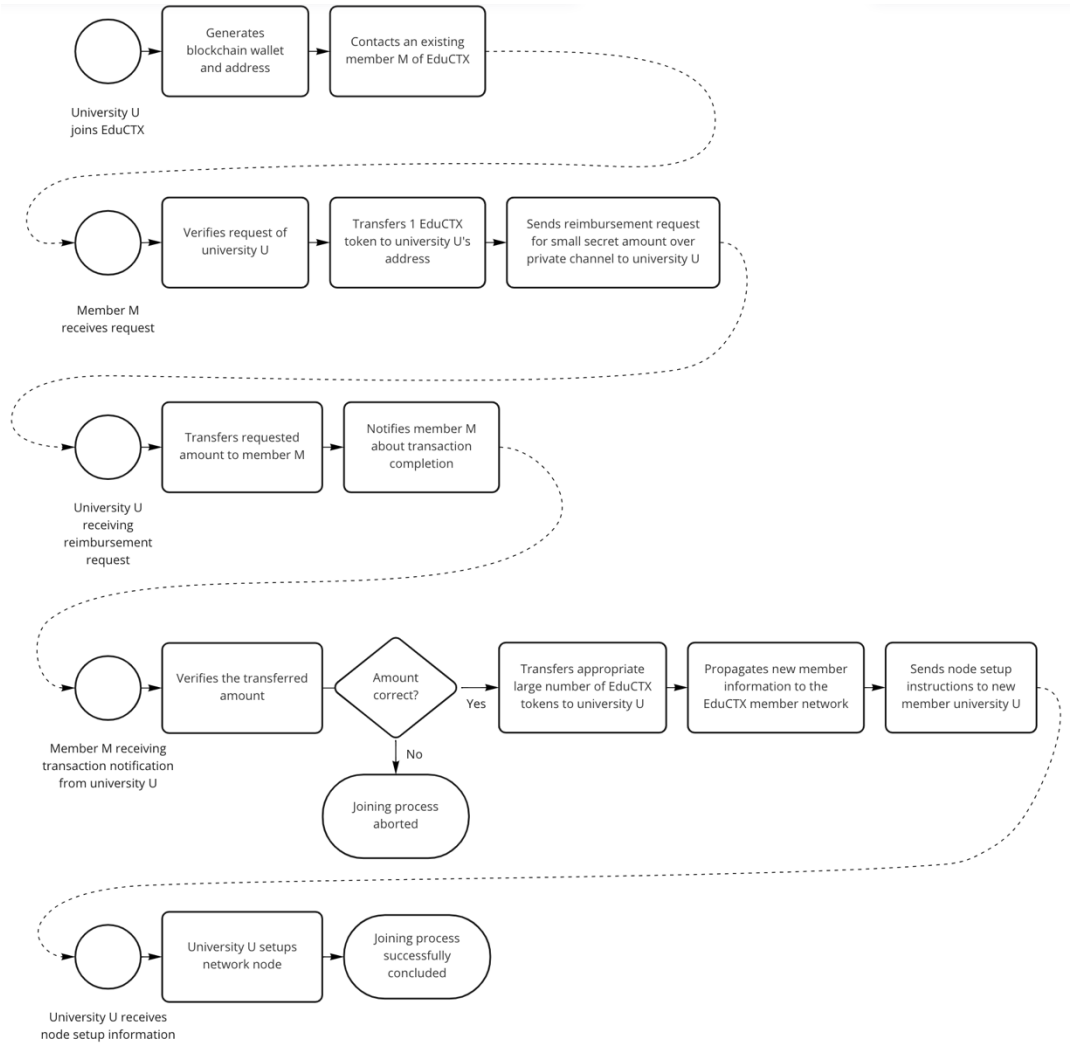
Figure 8: Process model for a student receiving a credential in EduCTX, [120, p. 5121]

The prototype system had several severe shortcomings: It neither included the identity of the course passed nor the identity of the student. If private keys were stolen, there was a risk of impersonation. Employers were not able to know the type of course for which the ECTS were granted. The system currently presented on the EduCTX-website is substantially different (4.3.9.6).



Source: Adapted and simplified from Turkanovič et al.

Figure 9: Organization verifying a student's record [120, p. 5122]



Source: Adapted and simplified from Turkanović et al.

Figure 10: Process model of a new university joining the EduCTX network [120, p. 5118]

Criteria	Evaluation	Grading
Security	Consortium blockchain of universities	+
Proof of Authority	Neither the university nor the student can be identified. It is only verified that the student holds a key of a multisig address	--
Durability	Relies on the network, the secure and private storage of the private key of the student.	-
Legal Recognition	No proper proof available	--
Autonomy	As long as the network is running and the student holding her key, the limited verification that the system is offering is available	+
Transparency	Complicated system with little transparency	-

Revocability	No revocation	--
Data Protection	Identifiability is very limited. However, once a student identifies her public address, the dates when several ECTS were received are visible and it is also possible to find out when and if new ECTS are received in the future	-
Usability	Complicated process	-
Automation	Possible, however some steps require interactions	+
Integration	Possible	+
Governance	Depends on the governance of the private blockchain and the IPFS nodes used	0
Economic Viability	A permissioned blockchain usually has no or much lower transaction fees than public blockchains. However, membership fees and the costs for running a node might need to be added	+
Sustainability	Much lower energy consumption	++

Table 12: Evaluation of EduCTX (2017 prototype)

4.3.6.3 RecordsKeeper

RecordsKeeper is a permissioned public blockchain that uses PoW with its own token XRK that can be mined [121, pp. 14–39]. Mining is bound to mining permissions. Requests can be sent via a Google Form request [122]. It is unclear what the criteria for mining permissions are. A token-sale was intended but cancelled in 2018 [123]. Data can be written and retrieved on that blockchain on a key-value base [121, pp. 44–47]. Anybody that holds its currency XRK can write files of up to 2 MB on the chain [121, p. 82]. Ten use-cases are provided – one of them is the verification of academic certifications [121, pp. 50–51]. There is only little information available on that specific use-case. The *Frequently Asked Questions* (FAQ) do not make a reference to the authentication of the source of a transaction [124]. The security of a permissioned PoW blockchain is limited. The amount of mining power at work is limited and could be outpaced by an attacker in a 51% attack. All information stored is public. Privacy needs to be achieved by encryption or hashing in the application. Since there was very little information available on the use-case for the verification of academic titles, no evaluation was included in this thesis.

4.3.6.4 CredenceLedger

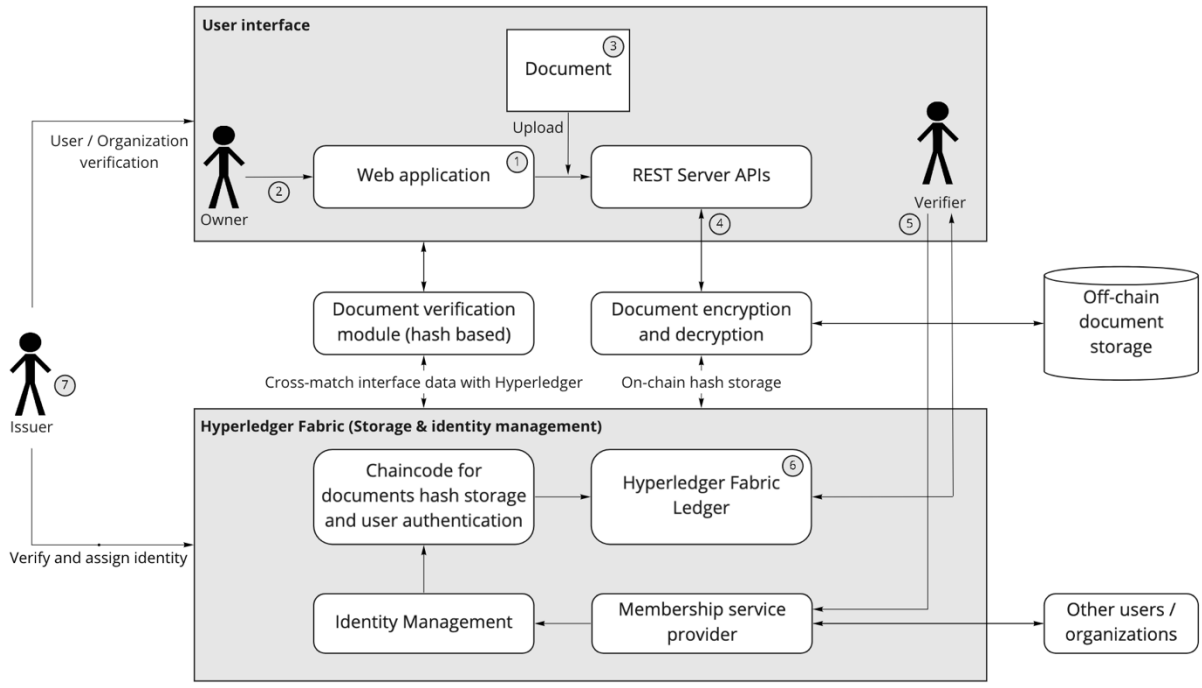
CredenceLedger is a proposed permissioned blockchain made for verifiable academic credentials [125, p. 4]. Similar to RecordsKeeper it is not based on an existing blockchain but a proper blockchain. The diplomas were meant to be stored on the chain and revocation information should be added in case of a revocation. Currently neither an implementation nor a detailed description has been found.

4.3.6.5 Ghazali/Saleh 2018

Ghazali/Saleh propose a solution in an academic paper in 2018 that consists of a signed hash that has been digitally signed by the university and the student. There is no discussion as to why the student should sign the diploma, how the certificates used for the digital signatures should be verified and what to do in case a certificate needs to be revoked [126, pp. 31–33].

4.3.6.6 Saleh/Ghazali/Rana 2020

In 2020 *Saleh/Ghazali/Rana* evaluated existing systems (see section 4.1) and proposed a Hyperledger Fabric-based system [84, pp. 82–84], (Figure 11). In this system documents are stored encrypted off-chain. Hash values are stored on chain. Identity Management ensures that only authorized people can verify a diploma. The issuer, the student and the verifier are required to have accounts with the system. Hyperledger is a private blockchain. Issues of durability, autonomy, legal recognition, integration and governance are not addressed.



Source: Adapted from Journal of critical reviews

Figure 11: System design proposed by Saleh/Ghazali/Rana [84]

Criteria	Evaluation	Grading
Security	TLS certificates and accounts based	+
Proof of Authority	Relies on TLS certificates	+
Durability	Relies on the availability of the private Hyperledger system and user interface	-
Legal Recognition	Can serve as proof, but difficult to capture the proof	-
Transparency	Private system, but hashes can be verified	0
Autonomy	Depends on the availability of the private Hyperledger chain and the user interface, but not on business hours	-
Usability	All participants are required to have accounts	--
Automation	Could be automated, but no standard API	-
Revocability	Revocation should be possible but not specified	+
Data Protection	Account management allows permissions to be fine tuned	++
Integration	Unknown	0
Governance	Private chain	-
Economic Viability	A private blockchain has costs comparable to a central database	++
Sustainability	Very limited power consumption	++

Table 13: Evaluation of Ghazali/Saleh

4.3.6.7 Smart Cert2

Smart Cert2 is the successor of SmartCert (see section 4.1) and co-funded by the Horizon 2020 program of the European Union. Depending on the functionality, the costs are between € 1-5 per student per year [127]. Smart Cert2 includes a PKI-based electronic signature [128] and stores a hash on woleet.io [129], a sidechain to Bitcoin. The advantage of this approach is the verified authenticity of the signing university and a prolonged validity of the electronic signature through the time stamp on a blockchain. The disadvantage is the proprietary sidechain.

Criteria	Evaluation	Grading
Security	PKI-based electronic signatures + Bitcoin secured sidechain	++
Proof of Authority	Relies on PKI	++
Durability	Relies on the availability of the sidechain. However, even when not regularly timestamped, the PKI signatures will provide some level of durability	+

Legal Recognition	Not clear, whether PKI-based signature is qualified or only advanced electronic signature. Either direct recognition or recognition as evidence	++
Transparency	Standards based PKI and use of a Bitcoin sidechain	+
Autonomy	Depends on the availability of the sidechain	+
Usability	Within the validity of the PKI-signature, usability of the PDF-reader. After that, proprietary access to the side-chain. Usability of that access unknown.	+
Automation	APIs available	++
Revocability	Unknown, PKI usually excludes revocation	-
Data Protection	PKI can mostly be verified locally and pure hashes on the blockchain do not comprise data	++
Integration	Unknown	0
Governance	Semi-private sidechain	-
Economic Viability	Medium-to-High fee range per student (€ 1-5)	-
Sustainability	Moderate power consumption since sidechain concept drastically reduces the number of Bitcoin transactions	0

Table 14: Evaluation of Smart Cert2

4.3.7 Smart Contract Based Verification

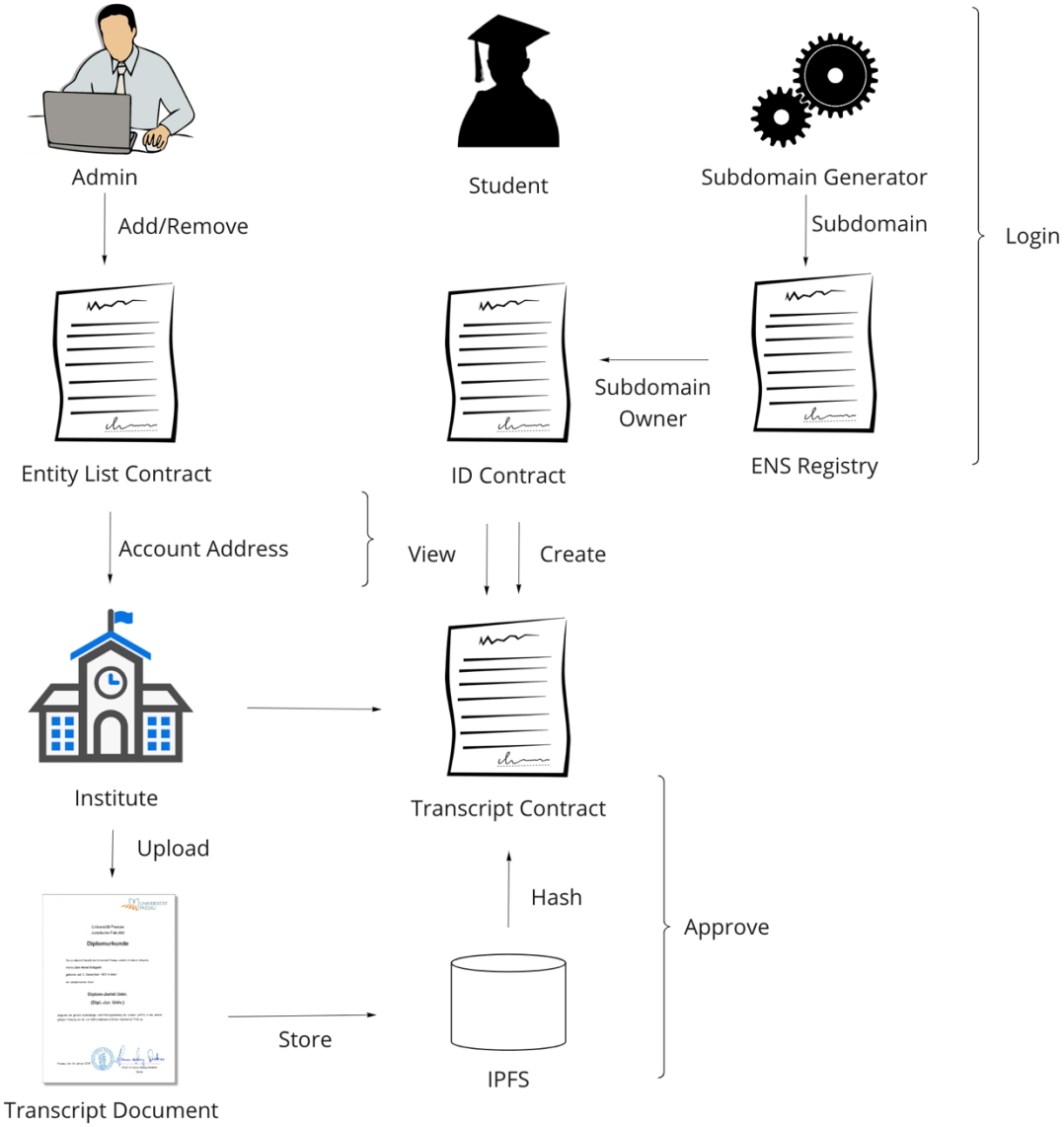
Smart Contracts are a means to program new types of transactions on standardized blockchains.

4.3.7.1 Principles

Smart contracts, as described in 3.3 offer the possibility to write programs on a blockchain to perform specific secure transactions on a general blockchain. While the security of a large blockchain can be relied on, a smart contract creates its own micro universe with a data store and hard coded rules. Most often Ethereum is used as blockchain with its smart contract language Solidity [52].

4.3.7.2 Transcripts DApp

Khedkar et al. propose a DApp-based approach [130, pp. 181–188]. The document is stored in the *Interplanetary Filesystem* IPFS [131, p. 185], a distributed file system where contents are identified and retrieved through their hash values. Several smart contracts are used to manage an institution that is entitled to create certificates. For every student and every credential, a new smart contract is created. The student initiates the process and requests a transcript of her diploma. The institution then uploads the documents to the IPFS and the hash value is stored in the application smart contract. The architecture is given in Figure 12 [130, p. 182].



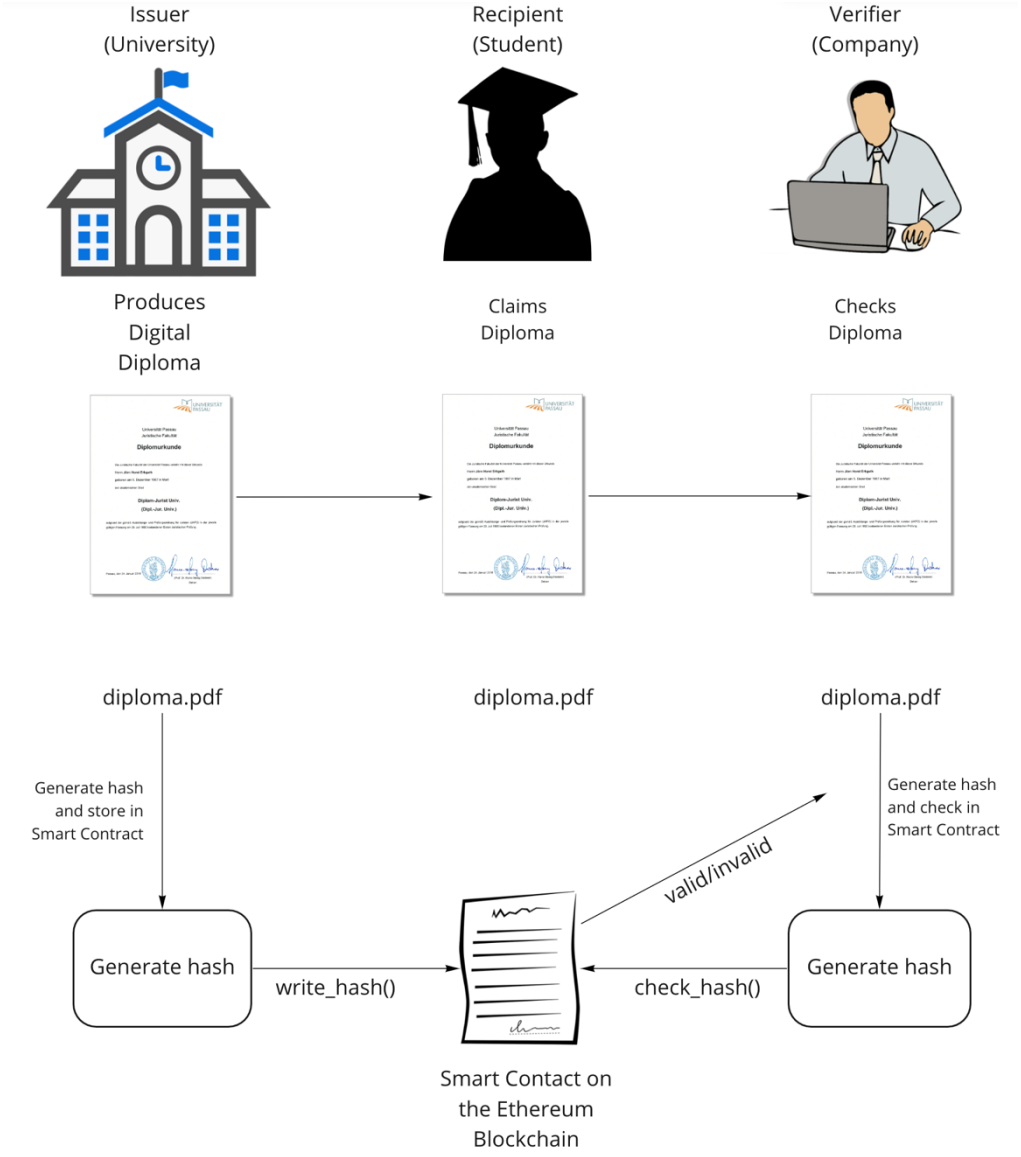
Source: Adapted from Proceedings of the International Conference on Blockchain Technology

Figure 12: Architecture of transcripts DApp [130]

The costs of the three transactions including the use of separate smart contracts for every transcript are listed with 0.0006 Ether and 0.07 USD [130, p. 188]. However, there is no reference to the underlying Ethereum gas price. So, this cannot be validated. Currently, the average Ethereum transaction fee is about 10 USD [132]. The creation of a smart contract is usually more expensive than simple transactions. Since a single diploma requires three transactions, the price could be higher than 30 USD for a single diploma. The price per transaction is highly volatile. However, even at the time the paper was written, the figures given in the paper seem to be unrealistically cheap. Another issue is the missing authentication of students requesting a transcript for their diploma. This has only been a prototype without sufficient information, so no evaluation table is given.

4.3.7.3 UZHBC

Gresch et al. describe a proposal for the University of Zurich [133]. The system calculates a hash value from the digital diploma and writes it by means of a smart contract to the Ethereum blockchain (Figure 13). The system offers two functions: A password-protected adding of a diploma hash value to the smart contract and an open verification of a diploma hash value.



Source: Adapted from Lecture Notes in Business Information Processing

Figure 13: UZHBC System Architecture [133, p. 190]

The system avoids complicated registration procedures for students. It also claims to address the fact that only the UZH can issue digital diplomas through that process. However, the paper does not address the identification of the smart contract. Without secure identification of the smart contract address with the university, anybody could copy the smart contract and control the copy. The copy would have the same functionality but a different address. This person then could

issue credentials and pretend that the University of Zurich has done so. Therefore, a form of authentication of the smart contract address with the university is needed, such as putting the smart contract address on the web server of the university or signing the smart contract address with a qualified electronic signature or seal. Revocation is not addressed by the system. Using public Ethereum currently translates into high issuing costs and a substantial carbon footprint.

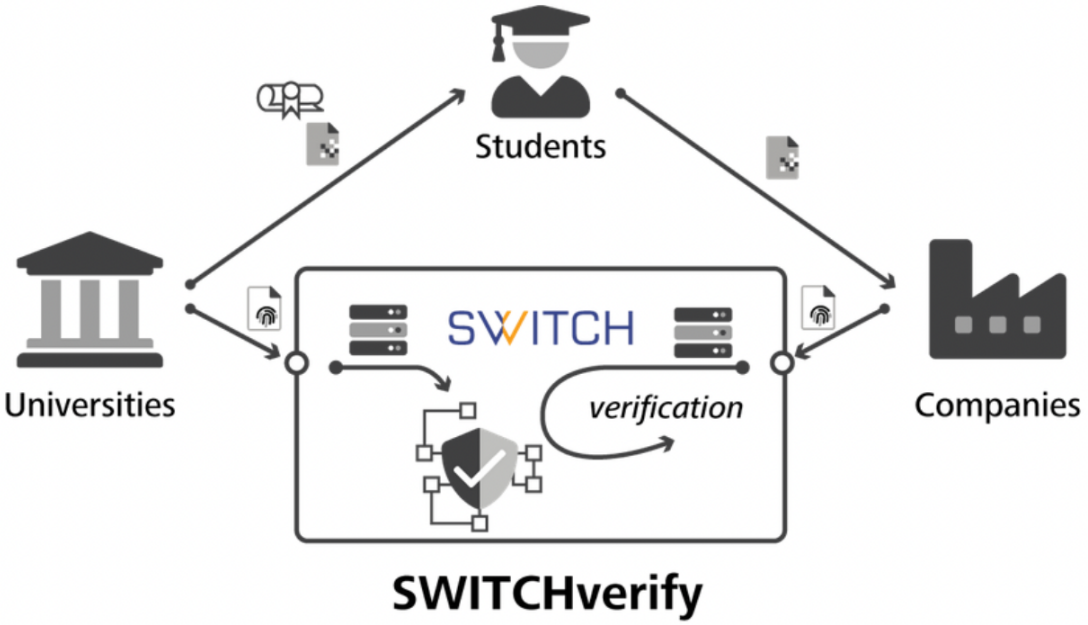
Criteria	Evaluation	Grading
Security	Public Ethereum blockchain	++
Proof of Authority	Not sufficiently addressed	--
Durability	Relies only on safeguarding of the original file by the student and the operation of the Ethereum blockchain	+
Legal Recognition	Possibly accepted as evidence	0
Autonomy	As long as the network is running and the student holds her file, and the authenticity of the smart contract can be verified. Otherwise, no dependance on systems of the University	+
Transparency	Simple Architecture, public blockchain, public smart contract	++
Revocability	No revocation	--
Data Protection	Hash values without the diplomas cannot be identified with the students. Together with the diplomas, no further information than what is already contained in the diplomas is available	++
Usability	Simple validation through a DApp, direct validation also possible	++
Automation	Possible	+
Integration	Seems theoretically possible but no API provided	0
Governance	No governance functionality included	--
Economic viability	Requires expensive public Ethereum transactions (> 10 CHF/diploma)	--
Sustainability	Certification of diplomas involve high carbon emissions. Verification does not do so	--

Table 15: Evaluation of UZHBC

4.3.7.4 SwitchVerify / Certifaction / University of Basel

Switch is a foundation founded in 1987 under private law by the Swiss Confederation and the eight university cantons of that time. Its objective is to create, promote and offer the necessary basis for the effective use of modern

methods of telecomputing in teaching and research in Switzerland [134]. Switch offers a product called *SWITCHverify* [135]. This diploma verification service is



Source: Reproduced from SWITCH, permission granted

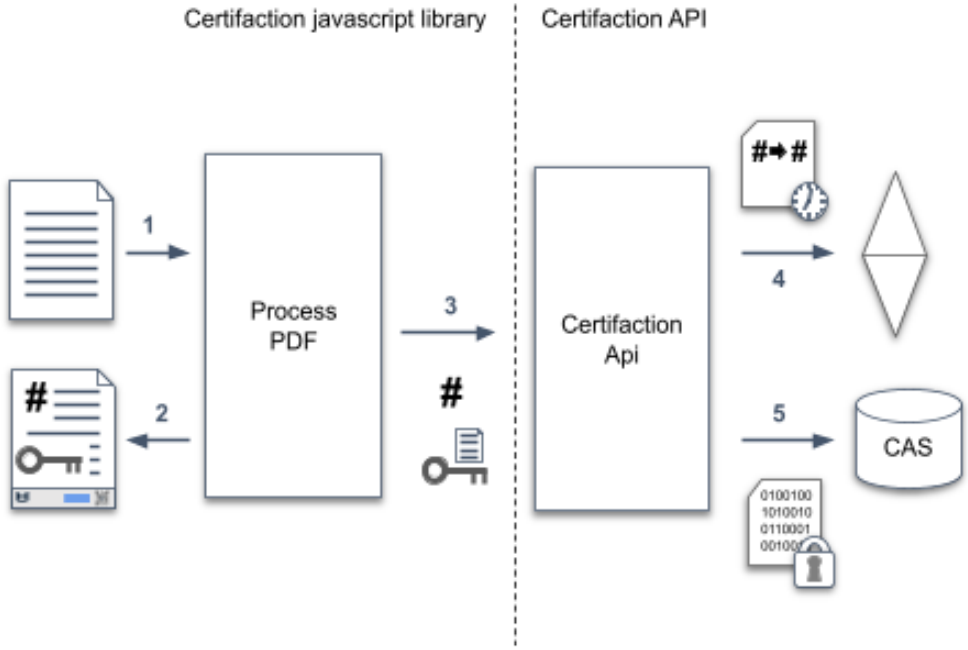
Figure 14: Overview of SWITCHverify [132]

provided through Certifaction AG. An overview is given in Figure 14. *Fabian Schär* from the University of Basel partnered with Proxeus and BlockFactory Ltd to certify diplomas [136, p. 49]. He co-initiated Certifaction [137].

Certifaction offers an API, a JavaScript Library [138] and a Command Line Interface CLI [139]. The JavaScript Library or CLI are used to process the PDF, so that the PDF never needs to be sent to the Certifaction server (Figure 15). Before a PDF is hashed, the archive ID, random data (*salt*) and a private-public key-pair is added as metadata. The salt makes sure that even with the knowledge of a very similar PDF the guessing of an otherwise private diploma is not possible. The key-pair is used to encrypt the claim. This claim includes the person or institution that registers the document and the claim that is associated with the document – e.g., whether the person/institution signs, certifies or simply registers the document. Revocations are also registered in the same way. By encrypting this information, the person or institution remains private to all but those that have the document. While a university might want to keep a public report of how many diplomas have been issued, others might want to stay private by not disclosing that they have registered something.

At least once a day, a transaction is sent to the Ethereum blockchain containing all new hash values. The smart contract does not, however, store the hash values in its persistent storage. Rather, the smart contract emits log-events. These log-events are stored on the blockchain but are not accessible by the smart contract. However, an external application, a DApp, can access them. This is a permanent storage method for Ethereum that reduces the storage costs by a factor of approximately 10 [140]. A direct validation through blockchain explorers

is possible but difficult since the check for revocations requires a search through all log-events that is currently not supported by blockchain explorers like etherscan.io. An open-source application to validate documents is provided on github [141]. Currently, some transactions hold up to 180 entries. The transaction price depends on the price of gas and Ether and is highly volatile. A transaction costs about 28000 gas + 2600 gas per document. Gas prices vary between 20 and 200 Gwei. One billion Gwei is one Ether. With an Ether price between 2000 and 3500 CHF this translates into a price per document of between 0.10 CHF and 2 CHF. Future volatility must be expected. But this price is not directly paid by the university, but Switch has planned the pricing for SWITCHverify to be around 5 CHF/student/year with an onboarding fee of 20.000 CHF per university and a free trial period until the end of 2021. The certificates per student is not limited. The Certifaction service is operational and is certifying about 5000 documents per month (as of mid 2021).



Source: Reproduced from Certifaction AG, permission granted

Figure 15: Certifcation software architecture [138]

Criteria	Evaluation	Grading
Security	Public Ethereum blockchain	++
Proof of Authority	Verified through SWITCH / Certifaction	+
Durability	Relies in theory on safeguarding of the original file by the student, the operation of the Ethereum blockchain. However, since the Smart Contract is undocumented, verification without certification could be difficult	0
Legal Recognition	Possibly accepted as evidence	0

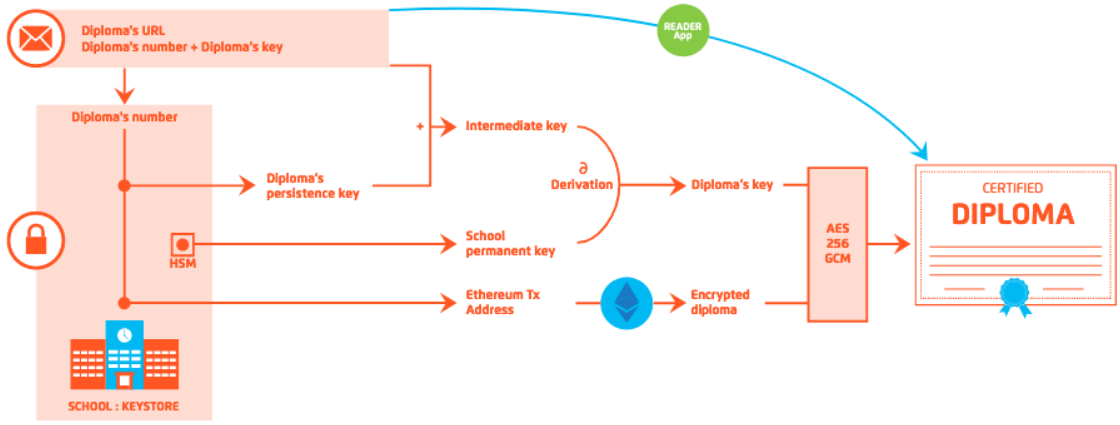
Autonomy	Currently requires the operation of a DApp with proprietary information	-
Transparency	Use of Public Ethereum, entries are log events of a smart contract	+
Revocability	Revocation possible but not easily visible directly on-chain	+
Data Protection	Hash values without the diplomas cannot be identified with the students. Together with the diplomas, no further information than what is already contained in the diplomas is available. Salt values that are added to PDF files increase this protection. Information about institutions and the type of transaction are also limited to those who have access to the diploma document	++
Usability	Simple validation through a DApp, direct validation due to missing transparency very difficult	+
Automation	Possible and supported	++
Integration	Possible, API and support provided	++
Governance	Governance through Certifaction. Not transparent	-
Economic viability	Based on a flat fee of 5 CHF/student	-
Sustainability	Bundling of transactions reduces the carbon emission compared to single transactions by a factor of approx. 10. Still considerably high carbon emissions	-

Table 16: Evaluation of SWITCHverify / Certifaction

4.3.7.5 BCDiploma / EvidenZ

BCDiploma is based on *EvidenZ* and offers micro credentials as well as Open Badges compatible credentials [142]. A white paper describes the concept and was used for a token sale (ICO) [143]. The tokens are required to certify documents. BCDiploma does not store hash values of diplomas but encrypted compact versions of diplomas on the Ethereum blockchain. Depending on the type of diploma, the payload data size for a diploma is between 200 and 520 bytes. At the current Ethereum gas and transaction prices, this translates into a transaction cost of up to 40 CHF per diploma. Every institution has its own Ethereum address which is vouched for by a third party called *validator*. First, BCDiploma is the only validator, but this is planned to be extended to other parties. Every diploma is encrypted using a combination of three keys: The diploma key, which can be part of a URL for the access to the diploma, a diploma's persistence key and a school permanent key. For the decryption, the Ethereum transaction address is also needed. The diploma's persistence key together with the Ethereum transaction address are stored in a keystore of the school and can be retrieved by the diploma's number, which can also be part of the diploma URL (Figure 16). The verification of a diploma therefore is based on an operational keystore of the school and a reader application that is able to

decrypt the information on the public Ethereum blockchain. The purpose of this encryption is to block the possibility to verify a diploma on request by a student. BCDiploma claims that this procedure is compliant with GDPR.



Source: Reproduced from BCDiploma white paper, BCD, permission granted

Figure 16: BCDiploma Crpyto Algorithm [143, p. 15]

The storage of the data of the diploma in encrypted form on a public blockchain is like the protection of a system with a password that can never be altered or deactivated. However, passwords need to be changeable to comply with information security standards [144, Ch. 5.1.1.2]. Although the key is never communicated to a third entity, this creates an unnecessary risk given the high immutability of a public blockchain. Putting the school's keystore in the loop creates the possibility that the link to the diploma will stop working when the diploma should not be accessible anymore (right to be forgotten). Only putting a hash value on a blockchain, however, would serve the same purpose, since the hash value is meaningless to everybody that is not already in possession of a copy of the diploma. The school's keystore, however, impacts the autonomy of the verification process and questions the added value of using an expensive public blockchain.

Criteria	Evaluation	Grading
Security	Public Ethereum blockchain	++
Proof of Authority	Verified through accredited validators	+
Durability	Relies on knowledge of the diploma number, the diploma key and the school's keystore being operational	0
Legal Recognition	Might be accepted as evidence although supplementary information is needed since process is not transparent	0
Transparency	Use of Public Ethereum but Smart Contract API is not published and independent verification impossible	-
Autonomy	Currently requires the operation of the verification DApp and the school's keystore	--

Usability	Through DApp – only URL required. No independent storage of the proof possible.	+
Automation	Possible	+
Revocability	Revocation possible, but revoked diploma cannot be distinguished from a fake diploma	+
Data Protection	Encrypted personal information is stored on a public blockchain. Risk is, however, limited due to protected storage of the encryption keys	0
Integration	Possible	+
Governance	Governance by BCDiploma, not transparent	-
Economic viability	Due to high Ethereum transaction fees very expensive	--
Sustainability	High carbon emission of public Ethereum	--

Table 17: Evaluation of BCDiploma

4.3.8 Self-Sovereign Identity Frameworks

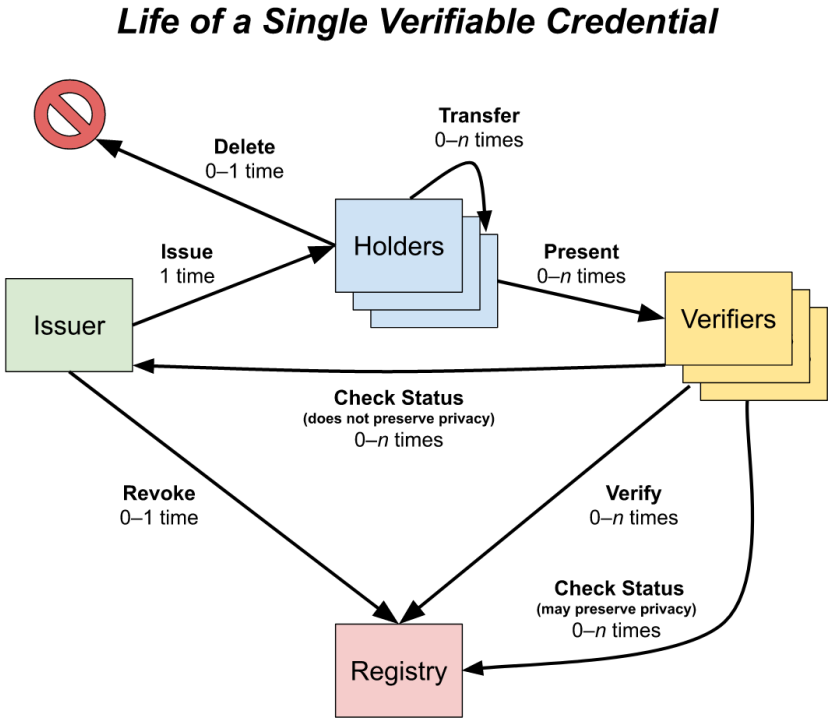
4.3.8.1 Principles

Self-Sovereign Identity (SSI) is motivated by a set of principles (see section 3.5). However, not every implementation adheres to all principles. When issuing a verifiable credential in SSI, Figure 17 shows that the holder of a verifiable credential has the control over its presentation, deletion and transfer while the issuer controls the issuance and revocation. Instead of presenting the credential directly, the holder can also use a verifiable presentation of the credential. This can be a subset of the claims contained in the credential or a zero-knowledge proof.

For cryptocurrencies, a wallet controls the usage of private and public keys to send and receive coins. This can be used for all token-based assets. Although credentials usually cannot be transferred, the wallet-based approach is also used for SSI and allows the credentials to be accessed or deleted as well as sign the credential with the private key of the wallet. This can authenticate the credential with the wallet and the user authenticating against the wallet instead of disclosing a name. The wallet can also be used to create a verifiable presentation. A verifiable presentation can offer the holder more control compared to sharing the verifiable credential directly:

a) Should the verifier be able to keep a proof of successful verification?
b) Should the verifier be able to detect a revocation that happens after the initial verification?
c) Should a revocation leave a trace so that a revoked diploma is distinguishable from a fake diploma?
d) Should the proof of a diploma include the mention of the name of the owner of the diploma (Principle 9, minimalization)?

Implementing all SSI principles would give negative answers to all four questions.



Source: Reproduced from W3C, license permits reuse, ©W3C

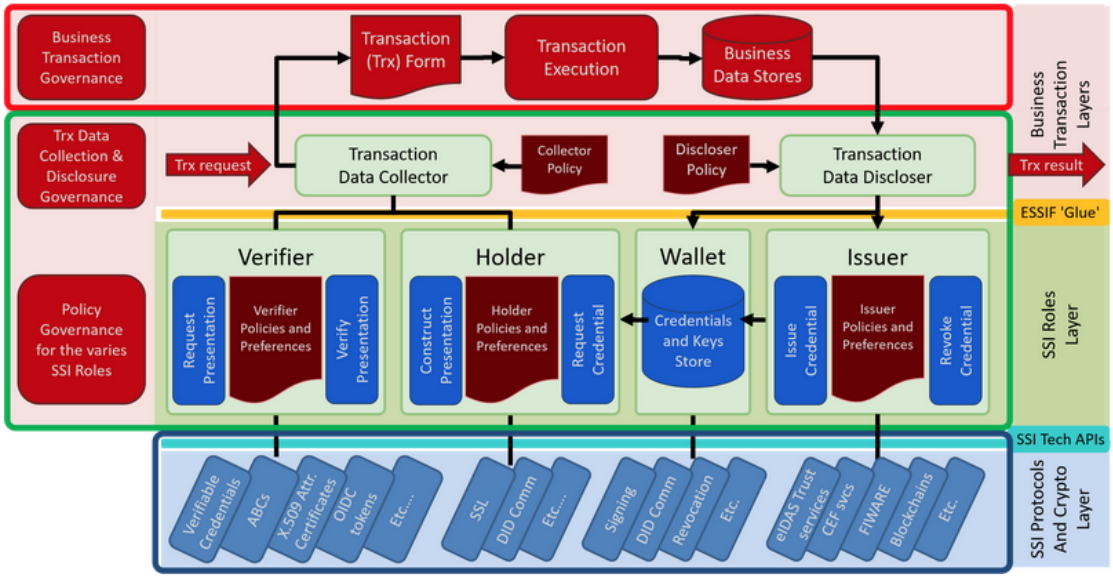
Figure 17: Verified Credentials Life Cycle [77]

The wallet approach requires special safeguards regarding the private key associated with the wallet. It must neither be compromised nor forgotten. In case a key has been disclosed, a key rotation mechanism is required that ensures that only the rightful wallet owner can create a new key. In case a key has been lost, some recovery mechanism should be included as well. As long as the university exists, it could always create a new diploma for a new wallet as well.

4.3.8.2 European Self Sovereign Identity Framework ESSIF

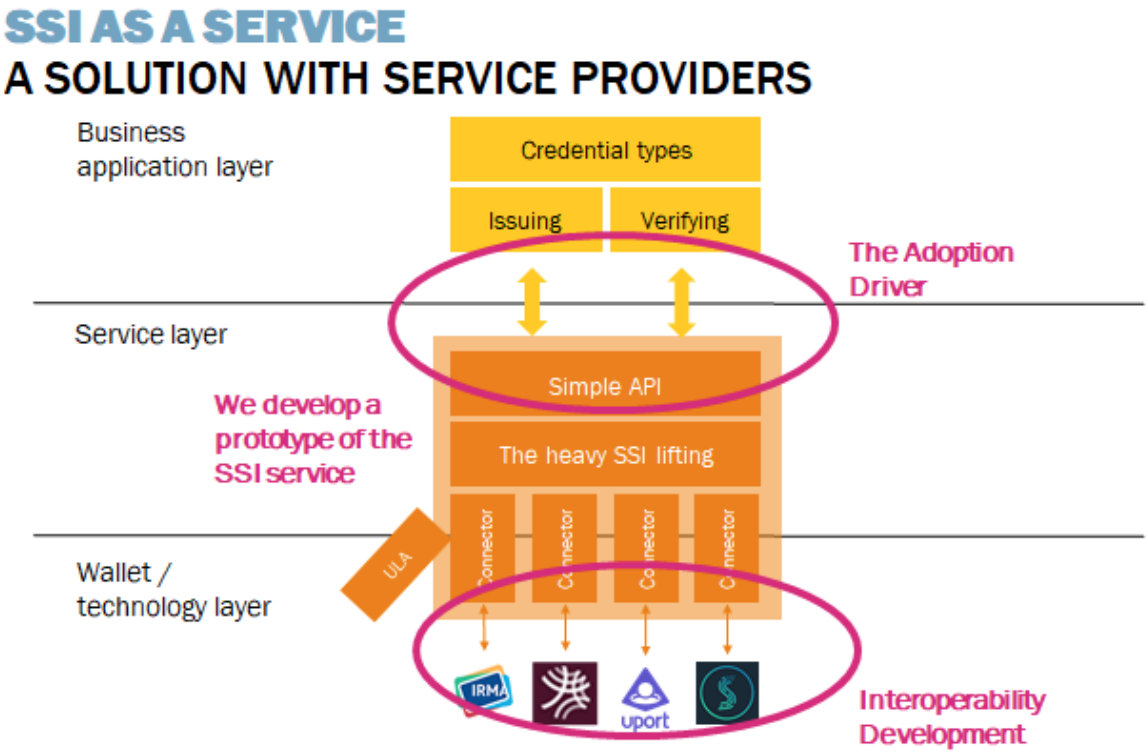
Different frameworks and different wallets would either force users to use different wallets simultaneously or would require implementing a solution using different frameworks in parallel. The European Self-Sovereign Identity Lab (eSSIF-Lab) aims at facilitating and verifying to and from any of popular SSI wallets. ESSIF views itself as an ecosystem of parties that work together to turn SSI technology into a scalable and interoperable infrastructure that businesses can use very easily [145]. It seeks to fund EU SME's that want to contribute the eSSIF-Lab vision.

An overview of the architecture for a single party is given in Figure 18. A set of documented APIs exists already. Like a web shop needs to provide different payment providers, eSSIF should be able to support different SSI frameworks (Figure 19).



Source: Reproduced from eSSIF-Lab, licensed under CC BY-SA 4.0

Figure 18: eSSIF-Lab Single Party Function Architecture [146]



Source: Reproduced from eSSIF-Lab, licensed under CC BY-SA 4.0

Figure 19: SSI as a service integrating service providers [147]

While the risk of losing access to a wallet that is only used to control the verification of diplomas, is relatively high, a wallet that has become integral part of everybody's digital life might be better suited. Those wallets will include ways to backup keys using one or multiple trusted parties that reduce the risk of

disclosure as well as loss of access to decentralized systems. Critical mass is a big issue for self-sovereign identity. Fragmentation of frameworks would enlarge this barrier and eSSIF could be a means of establishing bridges between frameworks to combine the users of all frameworks. This simplifies reaching a critical mass of user adoption.

One of the proposed use-cases for eSSIF are digital diplomas [148]. A suitable use-case could also have been vaccination passports. However, the European Commission decided not to use eSSIF for this purpose. The added privacy protection would probably not have compensated for the loss of usability. Having the data and the qualified electronic signature in a QR-code is much more convenient than expecting everybody to maintain a wallet to control the access to the vaccination passport.

The proposed revision of eIDAS [149] includes in Articles 3 nr. 42, 6a-6d, 10a, 11a, 12b, 12c and 45e European wallets. However, the relation to the eSSIF framework still seems unclear. As far as eSSIF is based on blockchain it uses the *European Blockchain Services Infrastructure* EBSI. A tender has resulted in seven distributed ledgers technologies to be offered under the EBSI umbrella [150].

4.3.8.3 Digital Credentials Consortium

After developing Blockcerts, MIT founded the Digital Credentials Consortium [151] together with 11 other educational institutions. Currently it is a white paper that proposes a solution. Like Blockcerts, it is based on a wallet that is installed on a device, such as a smartphone. The credentials can also be managed through a service of the university or a service provider similar to BADGR. Parties like employers or universities that rely on credentials can verify the credential using a verification tool of their choice that conforms to the new standard. To verify the authenticity of the issuer, the paper proposes a consortium-based approach, where the consortium registers participating institutions. Similar to Blockcerts, the solution includes a functionality for the student that the credential that carries her name is under her control. The paper lists the possibility to revoke credentials by the university, to erase credentials on the request of the student, and to reissue credentials in case of errors or name changes. The paper is based on the *verifiable credentials* data model of the W3C [77] that is designed for *decentralized identities* and self-sovereign identity. Due to the immense energy consumption of public permissionless PoW based blockchains, the consortium proposes to use a public permissioned blockchain. According to the paper the approach explicitly addresses privacy-by-design. The legal archiving requirements for certificates in countries vary between, for example the Netherlands (2 years) and France (50 years). The paper includes some discussions regarding GDPR compliance and the right to be forgotten but does not reach a conclusion. It includes the generally shared recommendation to minimize the data stored on a blockchain. Currently, the consortium has only published the white paper and there is a press release from a participating institution [152].

4.3.9 Other Approaches

For completeness some projects should be listed where either little information is available or that are not in production now, nor introduce important concepts that have not already been mentioned above.

4.3.9.1 KMI UK OU

The system form *Knowledge Media Institute UK Open University* (KMI UK OU) was based on Smart Contracts (Ethereum) and micro credentials. It was based on a partnership with the University of Ghent and the University of Texas. It was evaluated by *Jat* [84] and *Saleh/Ghazali/Rana* [118]. However, little information was available to evaluate the system.

4.3.9.2 Atala PRISM / Cardano

Cardano is a *Proof of Stake* (PoS)-based blockchain that was used in 2018 for a Horizon 2020 project to certify Greek diplomas [153]. In 2018, a pilot project was reported by the *national research and education network of Greece* (GRNET) [154]. In 2021 it was announced that it could be used on a large scale, including diploma verification in Ethopia [155]. On a Cardano forum, the question regarding what happened with the project was asked in May 2021 and closed without an answer for being “off-topic” [156]. When writing this thesis, neither a Cardano-based verification interface nor a paper with details could be found.

4.3.9.3 Bond/Amati/Blousson

As early as 2015, *Bond/Amati/Blousson* [157] propose employing a cryptographic signature and timestamps on a public blockchain. They address security and privacy concerns: The timestamp should also reduce internal fraud since this prevents diplomas from being backdated. They discuss different options like writing a hash of a diploma, creating a compact diploma record to be directly written and encrypted on a public blockchain. The password should be put on the credential. Against long-term vulnerability of encryption, a one-time-pad is proposed. This is an interesting early discussion. However, the use of a one-time pad encryption would make it possible to prove anything just by printing a corresponding password on a fake diploma.

4.3.9.4 Learning outcome, meta-diploma and micro-credentials

Duan/Zhong/Liu propose a system where students collect detailed achievements for a course which can come from automated evaluation software. Once sufficient achievements are collected, students can create a block record with their achievements for the course independently from the teacher. The block records will be stored in a “proof of accreditation” blockchain. [158]. The paper addresses the issue of proving detailed achievements, but does not discuss other aspects like security, privacy or long-term verification.

4.3.9.5 Central New Mexico Community College

The *Central New Mexico Community College* (CNM) also use an approach of micro-credentials. When students need to transfer to a different school, for example, when a college closes, they need to prove their detailed achievements to date [159]. Therefore, they receive micro-credentials for their transcripts as they pass exams and classes. This could in future also be extended to include micro-credentials for soft skills such as *empathy* or *critical thinking* [160]. The articles reviewed, however, do not offer technical details into the system used.

4.3.9.6 EduCTX (version 2020)

The system now described on the website is substantially different from the prototype evaluated in 4.3.6.2. Since no detailed information was available on the website, the author contacted EduCTX and received answers to his questions from the *Digital Innovation Hub* at the University of Maribor (Table 18). The blockchain has been changed, but it still uses IPFS and a wallet-based approach. The private key is crucial to access and protect the credentials. If the private key is lost, the credentials are lost and if the private key is compromised, the credentials are also compromised and an attacker could impersonate the credential holder.

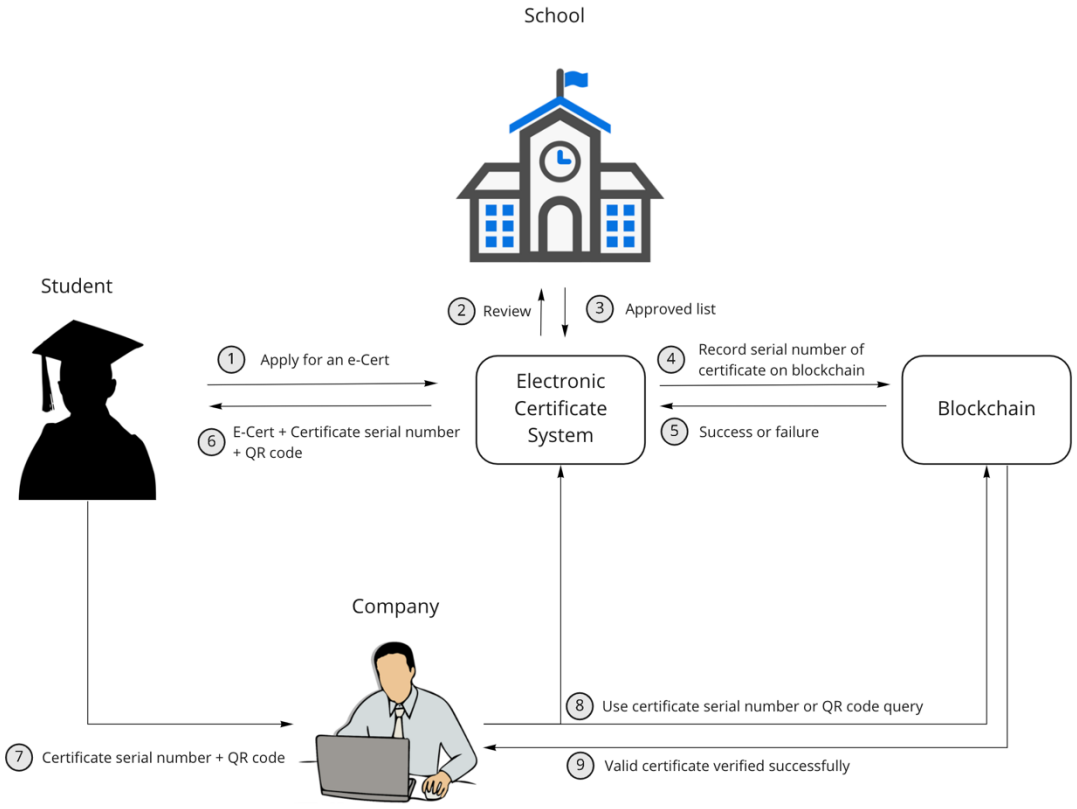
Question	Reply by the Digital Innovation Hub at the University of Maribor
An entry on the IPFS can be decrypted using the private key of the student. This will be done, for example, to present a diploma to a potential employer. How can the resulting PDF be verified by the employer?	Beside the PDF the students can download also a micro-credential (machine-readable format), which is digitally signed by the university. The PDF is just generated out of the data held in the micro-credential
Is there a possibility for a university to revoke a diploma in case of error or fraud?	Yes there is
What blockchain are you using? Are you using the public Ethereum blockchain?	Hyperledger Besu [which is an Ethereum client from hyperledger]
How much does it cost? Are there license costs to be paid to EduCTX? How much are the fees currently?	Currently no costs
Is there a possibility to prove a diploma when the private key of a student has been lost?	Once the student downloads his *micro-credentials* (MCs), this holds his personal information in it. He can then at any time send and re-send this MC to anyone, while the recipient can validate the MC using the EduCTX platform. However, if the student would lose his MC, he would need to login again to EducCTX to obtain it. To login, he needs his private key. If he

	loses the PK, he is unable to get the MC and needs to generate a new account (key pair) and to require new MCs to be issued to him
Is there a way to protect the privacy of the students if the private key of the student has been compromised?	If the PK is stolen from the user, the attacker could impersonate him and thus collect his MCs, which hold his private information
How many institutions do use your system? If it is based on public Ethereum, could you tell me the smart contract address?	Currently 3, but we plan to implement EduCTX within the European project ATHENA.

Table 18: Questions and answers regarding EduCTX

4.3.9.7 Southern Taiwan University of Science and Technology

Cheng et al. propose a smart contract-based diploma verification [161]. As described in Figure 20, a QR-code and a serial number are generated for each credential. Only the serial number is recorded on the blockchain. The credential is recorded together with the serial number and the QR-code in the electronic certificate system. The process is optional. Credentials are certified on demand of the students.



Source: Adapted from Proceedings of IEEE International Conference on Applied System Innovation

Figure 20: Process of the proposed process [161, p. 1048]

The serial number is not a hash value. In an example, *Cheng et al.* list it as TA00001 [161, p. 1050], however, the QR-code could be a hash value. The paper does not offer many details, but from the description given, it seems that the record on the blockchain does not allow the content of the credential to be verified but rather only verifies the existence of the serial number. The QR-code allows the detection of a tampered credential. However, it appears to not be stored on the blockchain. Verification is done by logging into the Electronic Certificate System. Revocation is possible. As can be seen in Figure 20, the verification is not done by directly communicating with the blockchain but is done through the Electronic Certificate System and hence depends on its availability. No details are given as to what kind of Ethereum blockchain is used relating to the amount of decentralization and the consensus mechanism used.

4.3.9.8 Blockchainized Certificate Verification Support System CVSS

Nguyen/Nguyen-Duc/Nguyen/Pham describe a *Blockchainized Certificate Verification Support System* (CVSS) and propose a system that uses the Ethereum blockchain [162]. They claim that the system provides decentralized verification, transparency, privacy and security, undeniability, economic savings and convenience. Institutions need to register and are verified through a KYC (Know Your Customer) process. A possibility to revoke credentials is included. There is a system smart contract for the administration of the system. Each school but also each student are required to have their own smart contract which they can control themselves through private keys. A wallet is used to store the certificates and the student smart contracts is meant to control the permissions to verify a credential. At the same time, credentials contain a QR-code representing a weblink which contains the necessary information for verification. There is no explanation how the student smart contract controls the verification of the credentials and whether verifiers need to be registered. The explanation in the paper given does not provide the level of detail required for a proper evaluation. The use of one smart contract per student leads to high financial and environmental costs per diploma and student. The paper proposes to port the solution to other blockchains.

4.4 Summary and Conclusion

A summary of all evaluations can be seen in Table 19. No system convinces in all points. Qualified electronic signatures have a good score but lack durability and revocability. My eQuals is a centralized system that has a relatively good score but is only possible where a centralized solution is desirable. Smart Cert 2, SWITCHVerify and Block.io partially show good scores but are weak regarding sustainability.

Criteria / System	Qualified Electronic Signatures	Electronic Certified Copies	Electronic Apostilles	Online Verification	My eQuals	Open Badges	Blockcerts	Diploma.Report	University of Nicosia, Block.io	Grad Base	EduCTX (2017)	Ghazali/Saleh	Smart Cert 2	UZHBC	SWITCHverify / Certifaction	BCDiploma
Security	+	+	+	+	++	+	++	++	++	0	+	+	++	++	++	++
Proof of Authority	+	+	+	+	+	+	-	--	0	0	--	+	++	--	+	+
Durability	-	-	-	-	0	-	-	-	-	-	-	-	+	+	0	0
Legal Recognition	+	+	+	-	+	0	0	0	0	0	--	-	++	0	0	0
Autonomy	+	+	+	-	0	0	0	-	++	+	+	0	+	+	-	-
Transparency	++	++	++	++	+	-	-	+	+	+	-	-	+	++	+	--
Revocability	--	--	--	0	+	+	+	0	+	0	--	--	+	--	+	+
Data Protection	++	++	++	-	++	+	+	++	++	+	-	-	++	++	++	+
Usability	++	++	++	++	+	-	-	-	+	0	-	+	-	++	+	+
Automation	++	++	++	-	+	+	+	+	+	+	+	++	++	+	++	0
Integration	+	--	--	-	-	+	+	+	+	+	+	0	0	0	++	+
Governance	+	+	+	+	+	0	0	0	0	0	0	-	-	--	-	-
Economic viability	+	-	-	++	0	0	--	0	0	--	+	++	-	--	-	--
Sustainability	++	0	0	++	++	++	--	--	--	--	++	++	0	--	-	--

Table 19: Summary of evaluations

To sum up:

- Qualified electronic signatures are legally well established. However, the need to regularly re-timestamp those signatures and the missing revocation functionality render them impractical as a sole means of verification.
- Online systems provide an easy way to verify diplomas – as long as the system is available online. They do not provide an independent way of verification.
- Certifaction / Switch and University of Nicosia / Block.co offer reliable verification systems. However, both of them are based on public blockchains with high carbon footprints and do not provide an easy and independent verification method.

While all systems provide some verification possibility for digital credentials, none properly addresses the long-term verification dilemma: How is it possible to verify a credential independently from the credential issuer or another central institution and at the same time be ensured that revocation by the issuing institution will be visible when verifying? Blockchains are frequently used, however, often in a hidden and not directly accessible way. The institution authorized to issue a credential is trusted. As long as the institution can verify a credential, there is little need to add decentralized trust. However, when the institution is not available anymore, independent trust is required. A blockchain that is not independently accessible by credential verifiers will not be able to provide this trust.

Based on this analysis, the next chapter will define the requirements for a system that is better suited for securing revocable long-term credentials.

Chapter 5 Requirements

Long-term revocable credentials are created by an authorized party and certify a qualification or other property of a natural or legal person. Long-term revocable credentials can be without an expiration date and should remain valid and verifiable even when the party that created them, the issuer, is no longer available. In case of error or for any other reasons, certificates should be revokable ex-tunc, that is to say that they should be treated as if they never had any value. The case discussed here is university diplomas, but other credentials may fall into this category as well. Credentials that are only revocable for the future (ex nunc) and remain valid for the past, and credentials that will cease to exist once the issuing institution ceases to exist, face less but different requirements.

Requirements are commonly divided into functional and non-functional requirements. Functional requirements define what a system should do while non-functional requirements define how this should be done. For the case of credentials, functional requirements would primarily include the creation, verification, and revocation of credentials but also functional governance requirements like key management and migration. The non-functional requirements would mainly focus on how this system should be created. Non-functional requirements focus on how to create trust for all stakeholders and include efficiency and usability. Trust can be created through secure technology, legal recognition, legal compliance and respect of legitimate user expectations of privacy and control.

While functional requirements are described in detail, often, non-functional requirements are either only expressed vaguely or in reference to standards or regulation. Thus, non-functional requirements often also result in specific functional requirements but are expressed in a more abstract way [163, pp. 840–841]. Non-functional requirements therefore often still require translation into a functional model. Particularly in the case of digital credentials, the functional part of issuing and reading a credential is rather simple, while the non-functional requirements pose the main challenge. For this work, non-functional requirements are first listed in a non-functional way. In a second step, non-functional requirements are translated into functional requirements.

5.1 Functional requirements

Digital credentials need to be issued and transferred to the credential holder. They need to be verifiable and revokable. An administration functionality can grant and revoke the permissions to create and revoke credentials. In case a system turns out not to be secure anymore the system must support the migration of all existing credential to a new, secure system.

The **issuance** of a credential shall be integrated into the system that creates or administrates the information contained in the credential. When administrating student records, a diploma should be issued from within the system in an integrated way. The certification of credentials should be integrated with the

student administration system to avoid synchronization problems. Every academic title should have the same status in the administrative system, in the credential database and on the blockchain.

In case of error, plagiarism or other legal obligations credentials shall be able to be **revoked**. The revocation differs regarding the **time** the revocation takes effect. A revocation can revoke the credential *ex tunc* at the time it had been created, some other time in the past, at the time it is being revoked (*ex nunc*) or at some time in the future. The difference is important. A doctor who received a diploma through plagiarism might lose her diploma ex tunc. This means that she practiced without the proper qualification although she was able to show a diploma that seemed to be valid. Still the physical diploma document was not a false credential, it just lost its validity retroactively. This should be modeled similarly in the digital world. Even a credential that is revoked ex tunc will not cease to exist but loses validity through adding the revocation notice.

Digital credentials that have been created should be **transferred** to students so that students can use them to prove to others, like employers, that they hold the university degree described in the diploma. Those who receive the digital credential shall be able to **verify** that they are authentic and that they have not been revoked in the meantime.

The technical permissions to issue or revoke credentials shall be granted to authorized persons and shall be terminated in case a person changes roles or in case the method to authenticate the person is no longer considered secure. An example for the latter would be a situation where a private key has been compromised.

A system or technology used for secure credentials could turn out to be not secure anymore. In this case, for example, a university should be able to reissue credentials on a new system. Therefore, complete information of the credentials needs to remain at the issuer of the credentials to **export** the information to create replacement credentials to a new system.

5.2 Non-functional requirements

Non-functional requirements are the main challenge in the context of long-term revokable credentials. Non-functional requirements focus on trust and include efficiency and usability. Trust is based on authenticity, security, transparency, durability, legal recognition, legal compliance, and respect of user expectancy of privacy and control. Non-functional requirements might partially seem contradictory. Particularly durability and data protection requirements like the right to be forgotten need to be well balanced to derive a functional design that properly translates these non-functional requirements into non-contradictory functional requirements.

A digital credential needs to gain acceptance. Acceptance is based on trust, economic efficiency, and usability. **Trust** in this context has many facets and starts with **authenticity**. A credential needs to be authentic and secure. Authentic means that it originates from the person or institution that is named as issuer on

the digital document and that the digital document has not been altered afterwards. The management of the rights to create or revoke credentials requires proper governance of **access rights**. The system also needs to be secured against manipulation. **Security** will not gain trust unless it is transparent. **Transparency** in the context of IT systems can be separated into two aspects. First, transparency means that the functioning is easy to comprehend for an average person. Making cryptography comprehensible to an average person is challenging and requires simplification. Simplification, however, hides important details. Therefore, transparency also means to provide all necessary details like open-source code and data to verify the correct functioning of a system. Since explanation of complex systems cannot be both, simple and comprehensive at the same time, transparency requires to address different levels of understanding separately:

- An easily comprehensible explication of how a system roughly works for the understanding of lay people.
- All necessary technical details that allow experts to verify the results of a system and the claims made.

Long-term digital credentials like diplomas need to be **durable**. This means that the verification needs to be possible for many decades after a credential has been created. Even when technology evolves and institutions might not be available anymore, the verification should still be possible. This results in two points: First, it should be **autonomous** meaning that the verification should be independent from the institution that issued the credential, but the institution that created the credential should be able to revoke it. Second, any change from the outside regarding organizational change, technological change or regulatory change should be handled by proper **governance**.

The credential should also enjoy **legal recognition**. Legal recognition of digital credentials has several layers. Direct recognition is based on laws like SCSE/ZertES [26] in Switzerland and eIDAS [23] in the EU. These laws determine the conditions under which digital documents are considered to have the same legal effect as paper documents. While individuals can apply advanced and qualified electronic signatures, institutions can apply advanced and qualified electronic seals. Legal recognition needs to be combined with the durability requirement which means that electronic seals should remain valid for a long time. Qualified electronic seals, however, are based on advanced and qualified certificates that expire. The expiration of a qualified electronic seal can be avoided when a timestamp proves that the qualified electronic seal was created at a time when the qualified electronic certificate was valid. The qualified electronic timestamp, however, is also based on a qualified electronic certificate that expires. Therefore, action is regularly required to preserve the legal validity of qualified electronic seals. One possible measure is to regularly apply new timestamps on a credential.

Besides legal recognition there is also **legal compliance**. While legal recognition ensures that a credential is legally valid, legal compliance ensures

that the system employed does not break the law. The most important law in this context is data protection law. For example in the case of an institution in Geneva, the Geneva LIPAD [69], the Swiss FADP (DSG/LPG/LPD) [66] (revised version [67]) and even the European GDPR [64] when there is a connection to the EU might apply. The requirements of data protection law are not only dependent on the applicable laws but also on the use case. Legal requirements might differ between different types of credentials and even between different types of diplomas. The same processing that might be legal in one use case could be illegal in another use case when there is a lack of appropriate justification for the processing. A thorough case by case analysis together with a *data protection impact analysis* (DPIA) might therefore be required when new technology is being used. Conflicts with other requirements like durability and autonomy need to be resolved. In this thesis this analysis focusses on university diplomas and might not equally apply to other long-term credentials. The legal analysis determines which regulation is applicable and how a system should be built to comply with the law. Data protection laws require **privacy and data protection by design**. That means that the functional design of a system already takes the data protection requirements into account. Rather than limiting the processing of personal data only by organizational means, it is also limited by technical means. Techniques applied are privacy enhancing technology and data minimization. Data that is not available cannot be illegally processed. Privacy enhancing technology like encryption, hash functions and zero knowledge proofs can limit processing of personal data to where it is justified. Privacy and data protection by design cannot be done isolated from other requirements. It means designing a system which not only can do what it should do, but also which is not capable of doing what it should not be doing.

Besides legal compliance with data protection regulation, **privacy** and **self-determination** of credential holders are also independent design goals by themselves. Although data protection laws already demand restricting processing of personal data to situations where it is justified, when there are several legally compliant options, the option that fosters privacy and self-determination better should be selected.

A system that does not provide sufficient **usability** will not be accepted. Usability means that a system can be used efficiently by its users. Usability can be extended to include an emotional component to also include **user experience**. Besides efficiency, it means that using a system is enjoyable and that the user trusts a system. Qualified electronic signatures and seals have been around for decades but have not gained widespread acceptance in many European countries due to lack of usability. A verification procedure that is not easy to use will not be used. Usability requirements might conflict with security or legal requirements. For example, unsecure scanned paper diplomas are easy to use, and published graduation lists that do not respect privacy requirements are easy to verify. Lack of usability can impede the acceptance of an otherwise superior solution. Removing unnecessary functionality and simplifying the workflow can be important to optimize usability.

The system also needs to be economically **efficient**. That means it should not require too many resources like funds for development or time to create and verify credentials, as such resources are scarce. It should also not use too much computing power and should not rely on a system that requires payment of substantial fees for the issuance or verification of credentials.

Last but not least the system needs to be **sustainable**. Sustainability includes the efficient use of resources of our planet. A technology that has a high carbon footprint like *Proof of Work* (PoW) blockchains needs to be avoided even in the case when neither the issuer, holder nor verifier of a credential themselves are required to provide these resources.

5.3 Translation of non-functional requirements

The non-functional requirements need to be evaluated and applied to the use-case of long-term revokable credentials. This can be focused on four non-functional requirements that lead to specific design requirements: Security by design, legal recognition by design, governance and privacy and data protection by design. These non-functional requirements will be analyzed in detail to be translated into functional requirements:

5.3.1 Security

Security is the central non-functional requirement for an electronic credential. The electronic certificate should not only provide some information but should prove that the information contained is authentic. This non-functional requirement of security needs to be translated into functional requirements. First, all valid credentials should be able to be verified over decades. At the same time, it should be impossible to alter an existing credential or to give the impression that there is a credential although no such credential has ever been issued.

It shall be hard to create the false impression of having a credential that somebody does not – or does no longer – hold. This means that falsified or non-existing credentials should not verify successfully. It also means that it should not be possible to mock-up a system that gives the impression that a non-valid credential is successfully verified. Finally, no credential that has been revoked should still verify successfully.

The system should also provide a proof of authority. It should not be possible to create a credential by a third party in the name of another institution. It should also be impossible for a diploma to be created in the name of a non-existing university that gives the impression of constituting an academic title. The latter is a requirement that goes beyond current paper credential. A paper credential requires a reference to an external trusted party to determine if that institution existed and was entitled to issue valid credentials of that kind, e.g., university diplomas. In the digital world, like the analogue world, this step also requires a trusted third party. However, the reference to that trusted third party could be integrated in the digital verification process.

Proof of authority should also address the dimension of time (durability). A diploma, for example, does not lose its validity if the institution renames itself, merges with another institution or ceases to exist. In the same way, an institution might have been authorized to issue diplomas, but no longer is. Therefore, this validation of authenticity needs to be linked to the issuing date of the credential.

Some credentials, like, for example, university diplomas, need to be verifiable for the rest of the life of credential holders which means for many decades. Security over such a long time cannot be provided by technical means only. A proper governance model should enable the migration of long-term credentials to a new system if necessary and should also be able to stop verification that is no longer secure. The governance model includes an organizational component that ensures that organizations can act, and it includes a technical component like a kill-switch to stop verifications of credentials that are no longer secure or no longer authentic.

To summarize, the non-functional requirement of security can be translated into the following functional requirements:

- Authentic credentials should always verify successfully.
- Revoked credentials should never verify successfully.
- Manipulated credentials should never verify successfully.
- Credentials from unauthorized sources should never verify successfully.
- The access to issuing or revoking a credential need to be secured to minimize the risk of abuse.
- The user verifying a credential needs to be sure that she is connected to an authentic verification system.
- The verification needs to be possible for decades after issuing a credential.
- When a verification system is no longer secure it should be deactivated, and credentials should be able to be migrated to a new secure verification system.
- The decision to stop an insecure system and to migrate to a new system should be possible and taken even if the entity that issued the credential is no longer available.

5.3.2 Governance

Authenticity and durability require proper governance of rules for the creation or revocation of credentials, implemented rights management regarding the access to the system to create or revoke credentials and procedures to act on changes in technology, organizations or regulation. Particularly challenging is the governance process in a decentralized, distributed and/or autonomous system comprised of many actors like a blockchain. Governance generally refers to *the way that organizations or countries are managed at the highest level, and the systems for doing this* [164], the meaning of governance of distributed ledger systems is more focused. Similar to other open-source software, governance for

blockchain refers to the *means of achieving the direction, control and coordination of stakeholders within the context of a given blockchain project to which they jointly contribute* [165, p. 21]. Governance in this meaning is not the automatic enforcement of rules through code but achieving a consensus about the modification of those encoded rules. Blockchain enforces many rules through code. When, however, the code has a bug or is regarded for other reasons as not leading to the result that it should lead to, a modification of the software should alter the coded rules. A revision of the software of a decentralized system, i.e., a *fork*, can result in the community unanimously accepting or rejecting the newly coded rules. However, this could also lead to a temporary or permanent split of the chain that creates uncertainty, lack of immutability of transactions and avoidable damage to the reputation of the system. A compromise should be reached beforehand and possibly off-chain. This reduces the risk of different variants of a blockchain – *forks* – operating in parallel until one variant is generally accepted, and the other variant is rejected or the blockchain is split permanently. The process of voting beforehand on modification proposals can be informal, it can also be coded into software or supported by a blockchain smart contract. Similar to the consensus through mining, a decision is reached electronically and is automatically enforced. Even in the case of a narrow dispute, no phase of uncertainty with low trust in the system is created. However, governance is always required to deal with unpredictable situations that have not been considered in the code. For example, the project *Decentralized Anonymous Organization DAO* included a broad set of smart contract-based governance rules. However, it also contained a bug that those rules were not able to deal with. In the end, only a fork on Ethereum was able to prevent the exploitation of that bug [56, pp. 6–7]. Similar to the governance of a blockchain or a decentralized anonymous organization, blockchain secured long-term credentials also require a means to deal with predictable and unpredictable problems. The resulting governance is a combination of rules and internal regulations as well as coded rules in the systems designed. The governance is dependent on the technology used and the internal regulation of the institution as well as the jurisdiction the institution is subject to.

For the governance regarding a long-term credential, in the design described above, the following governance aspects can be identified:

- The decision process at the issuing institution for issuing or revoking a long-term credential. This is an internal process specific to the issuing institution. For universities, for example, it might be determined by regulations of the university.
- The legal review, if the decision is challenged through the legal system – e.g., the potential holder sues the issuing institution because she does not agree with the result of the issuing process at the institution – e.g., for not having received the grade or title desired. This is an external process ruled by a combination of internal rules and the laws the issuing institution is subject to.

- The proper governance processes for the systems used are:
    - Governance of the certificates for qualified electronic signatures,
    - Governance of the TLS certificates for securing websites,
    - Governance of the blockchain used and the
    - Governance for the smart contract used.

  These governance processes need to be suitable for long-term credentials and need to be accounted for in the system design.
- The rules and access rights governing the creation and revocation of long-term credentials. This includes the administration of these access rights in the systems used.
- Adding or removing participating institutions.
- The governance on the meta-level regarding, for example the migration of the credentials to new systems or the change of the rules governing the participation in the system.

5.3.3 Legal Recognition

Sometimes digital credentials are just seen as an additional means to show an analogue document. Legal recognition is not considered important because the paper original can always be shown. The electronic credential is shown first and for convenience purposes only, while the paper original is relied on. However, electronic credentials are increasingly replacing paper documents and electronic credentials should enjoy similar legal recognition. For digital credentials there exist different levels of legal recognition. They might be considered equivalent to a manually signed document. Below that, the law recognizes a broad range of proofs in evidence procedures. These procedures can be lengthy and costly and should be – if possible – avoided.

In case the institution is still available and paper credentials, like diplomas, are still being recognized, an electronically verifiable credential only serves as a convenient method to prove a digital copy of a diploma. In doubt, diplomas can still be proven with the paper original or by verifying with the university. However, the electronic credential could become the only document that can be produced. Electronic diplomas should be able to fully replace paper diplomas. This requires the electronic credentials to have equal recognition compared to paper credentials. The legal validity of an electronic diploma depends on the regulations of the university that issues the diplomas, the jurisdiction the university is subject to and the jurisdiction where the diploma is being used. When diplomas are used internationally, a notarization – or in case of member states of the *Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents*, an apostille – might be required. Also, university regulation could define an electronic diploma as valid, that does not validate as a qualified electronic seal. Even then, a broad direct legal recognition of the qualified electronic seal applied will reduce the need for notarization or additional procedures.

Contrary to paper documents, legal recognition of qualified electronic seals is not permanent. Qualified electronic seals are based on qualified electronic certificates that are only granted for a maximum time of 3-5 years. The qualified electronic seal remains valid if it can be proven that the qualified electronic seal was created within the time of validity of the qualified electronic certificate it is based on. Long-term qualified electronic signatures therefore include the certificate and a timestamp of the signature (see for example the PaDES-B-LTA standard [89, Ch. 9]). This provides long-term validity as long as the certificate the timestamp is based on is still valid. Regular timestamping might be required to ensure a chain of valid timestamps. This is a process described for example in the German technical guidelines TR-ESOR [166, p. 14]. This procedure is not practical for students holding digital diplomas. Therefore, other means of extending the proof-value of a qualified electronic seal should be considered. The draft of the amended EU regulation eIDAS introduces electronic ledgers as a means of proof. As *Sorge/Leicht* point out in [40], a hash value on a blockchain where hash values of new blocks are timestamped before the certificate for the previous timestamp expires might already be sufficient under current law (see section 3.2). Further support to continued legal recognition might be available through the current eIDAS revision proposal and technical specification proposed by ETSI.

Qualified electronic signatures and qualified electronic seals once created based on a valid certificate cannot be revoked. This is similar to a handwritten signature. However, digital credentials might need to be revoked for various reasons. Revocation of a credential does not void the electronic signature or the electronic seal directly but adds important information to a certificate. Legal recognition, however, is still oriented at paper documents and therefore does not demand the revocation information to be attached to the verification. However, some university regulations demand that in certain cases of revocations the original diploma is returned to the university. The motivation behind the requirement to return a paper document is to prevent the further usage of the document. Since an electronic certificate can always be copied, returning an electronic document cannot answer this motivation. Therefore, the return of a paper document needs to be replaced in the university regulation by the revocation of an electronic certificate.

To summarize: While legal validity of electronic credentials varies between legal systems and will certainly evolve in time, current legally recognized mechanisms like digital qualified electronic seals should be included. Long-term verification needs to be ensured in a way that will be likely to earn legal recognition for a long time in the future. Blockchains might be used to avoid mechanisms that require constant action by students. Legal recognition in situations where analogue credentials were legally required to be returned to the issuer need to be mapped to the possibility to revoke digital credentials. Digital credentials where revocation information cannot be attached cannot comply with these legal requirements.

5.3.4 Privacy by Design and compliance with data protection regulation

The system should comply with data protection regulations – especially the Geneva LIPAD [69], the Swiss FADP (DSG/LPG/LPD) [66] [67] and the *European General Data Protection Regulation* (GDPR) [64]. In this study, the focus is on the GDPR.

The design should adhere to the principles of data protection by design and by default (Article 25 GDPR). *Data protection by design is based on the insight that building in privacy features from the beginning of the design process is preferable over the attempt to adapt a product or service at a later stage* [167, p. 11]. This is particularly true when almost immutable technology is used. *Data protection by default means that in the default setting the user is already protected against privacy risks* [167, p. 11]. A key element in data protection by design are *privacy enhancing technologies* (PETs). At the *Deutsche Institut for Normung* (DIN), the author participated in the development of a standard called *Privacy by Blockchain Design* DIN SPEC 4997 [168]. This standard lists PETs that can be used in the context of blockchains.

The two top criteria for privacy by design mentioned by *Danezifs et al*. are trust assumptions and involvement of the user [167, p. 14]. The trust assumptions for long-term revocable credentials can be described between credential issuer, credential holder and credential verifier. This is visualized in Figure 21. There is a triangle of trust between credential issuer, credential holder and credential verifier. The trust is about two main aspects: The trust that the credential holder holds the credential that he claims to hold and the trust that the credential verifier has a justification to receive information about the credential.

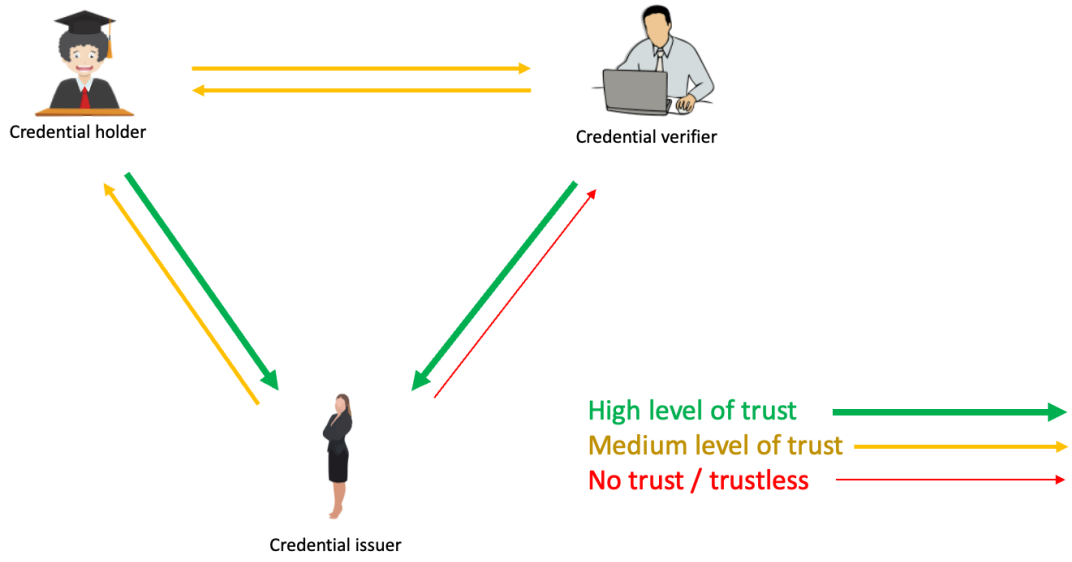


Figure 21: Trust levels between main stakeholders

The central trust issue of credential verification is between credential holder and credential verifier. The credential verifier cannot trust the credentials presented by the credential holder but requires verification. Both, the credential

verifier and the credential holder have identified themselves and know who the other is. The credential holder has established enough trust to the credential verifier, so that he is ready to present the information in the credential to the credential verifier and the credential verifier is bound to respect the confidentiality of the information received by the credential holder.

Between credential verifier and credential issuer there is an asymmetric trust relationship. The credential verifier trusts the confirmation of the credential issuer that the credential was issued on a justified basis. For example, an employer has trust in the confirmation of a university that an applicant has successfully passed the described educational program. The employer can check the status of the university and the contents of the educational program which are usually publicly available. On the other hand, for privacy reasons, the credential issuer should only give information to those who either have been authorized to do so by the credential holder or by those who have a legitimate reason to receive them. The credential issuer often does not identify the credential verifier. Therefore, there needs to be an element of trust that confirms the authorization of the credential verifier to verify the credential. This element of trust can be some specific authorization, a secret link or a token received from the credential holder. This token could by customized for the credential verifier or something that is independent from the credential verifier like a copy of the credential.

The credential holder has trust in the credential issuer. He relies on the judgement of the credential issuer to receive the credential and is dependent on the credential issuer when it comes to a possible revocation. On the other hand, the credential issuer knows the credential holder and has verified that the content of the credential is justified. The credential issuer respects the privacy and the self-determination of the credential holder regarding the usage of the credential.

Although the credential issuer is the one who is most trusted by all parties involved, the credential holder and the credential verifier also deserve to be protected from disclosure of the relation they have to the credential issuer. Usually, the credential issuer also does not have an interest to be actively involved in the verification process. Particularly in the situation where the credential issuer is not available, the credential holder and the credential verifier have a strong interest, that the verification process also works without involving the credential issuer. The trust in the credential issuer is therefore replaced by the trust in an electronic seal, the confirmation of a trusted third party and/or some trustless technology that confirms that a credential has been issued by the credential issuer. However, since there is a possibility that the credential issuer has revoked the credential, the credential issuer needs to have a possibility to add revocation information to the independent verification process.

Regarding the verification this leads to the following requirements:

- The credential holder should have control who can access the information in the credential.
- The verification should be limited to those who have access to the credential.

- The verification should be independent from the availability of the credential issuer.
- The credential issuer should be able to add revocation information to the verification.

While the repeated verification of a static credential does not provide new insights, the repeated verification of a credential that can show updated revocation notices, provides the information that the credential has not been revoked since the last verification. Therefore, it needs to be discussed, who should have access to the revocation information. There are the following alternatives:

a) When access to the credential has been granted by the credential holder, only the revocation information available at that time will be shown. Future updates will not be visible. This can be compared to a static confirmation by the credential issuer that at a specific time the credential was not revoked.

b) When the credential is presented to the credential verifier, the credential holder submits it with a verification time interval. All revocations issued within this time interval will be visible to the credential verifier. Revocations issued later will not be visible. This would be the scenario of a permit that is required for a specific time interval.

c) Whenever the credential is verified, the current revocation status is displayed. No revocation is hidden. This is appropriate for revocations that take effect retroactively (ex tunc). Ex tunc revocations concern all credential verifiers that have verified the credential in the past. Although a revocation information is added at a later stage, it is visible to credential verifiers that have verified the credential before when they verify the credential again. The possibility to verify a credential again is not technically limited to a specific time interval of, for example, employment. The hospital that has employed a doctor needs to know that the doctor was not properly qualified even when the doctor no longer works at the hospital. This option would also allow for credential verifiers to automate the check for revocation updates of credentials they have verified in the past.

d) The revocation information is published, so that even those, who have never seen the credential can take notice of the revocation.

The GDPR is based on the principles defined in Article 5 GDPR. Data processing needs to be lawful, fair, transparent, adequate, limited to the justified purpose and accurate. The GDPR therefore prohibits processing of personal data unless there is a proper justification to do so. When looking at these alternatives, it is necessary to analyze the justifications for making the revocation information available. There might be a legitimate interest or a legal obligation to inform about the revocation. In the analogue world, there often has only been options a) and d). The option a) did not protect the interests of credential verifiers well while

option d) also made the information available to people that had never put trust in the credential. Since revocations are often done retroactively (ex tunc) and not only for the future (ex nunc), the information needs to be available to past verifiers as well. This could be modeled in two ways: The credential could remain verifiable to take into account recent revocations, or the credential verifier could be required to ask the credential holder to grant another verification possibility. The latter option would give the credential holder more control. However, this would imply that, for example, an employer, who is in doubt whether an employee has received a diploma through plagiarism could not check for herself but would be required to ask the employee in question and even go to court before being able to learn that the university has revoked a diploma for that reason. In the use-case of long-term revocable credentials this seems disproportionate. However, the access to the verification and possible revocation notices are an important topic in the discussion of the self-determination of credential holders and the right balance between the different interests at stake depends on the use-case (see also section 8.4.19). For example, there are detailed regulations, how long employers are obliged and allowed to store credentials of job applications and employees [169]. Similarly, the *Berlin Commissioner for Data Protection* (BlnBDI) data protection authority fined a real estate company for storing data about current tenants that were not needed anymore but still being stored [170]. Although a court, the Landgericht Berlin later cancelled this fine for other reasons [171], it did not question the requirement of a fine-grained deletion policy. ISO has published ISO/IEC 27555 *guidelines on the personally identifiable information deletion* [172] (*personally identifiable information* is the US legal term for *personal data* with a slightly different meaning). Privacy by design could try to cast these rules into code and design. However, there are not only technical limitations to model all details using privacy by design. For long-term credentials, the system also needs to keep some flexibility if details of the law change. Otherwise, privacy by design could block legitimate processing of personal data in the future. Therefore, privacy by design can only offer a skeleton to exclude the types of processing of personal data that are clearly undesired.

To conclude for the use-case of long-term credentials, the current state of the revocation information should not be hidden from those who have verified the credential in the past and option c) should be chosen. The verification should remain possible and should also reflect recent revocations.

After a diploma has been revoked, what should be the result for the verification of a revoked diploma? Should it be the same as a forged document or should it reveal the fact that the document has been valid before but has been revoked? There is no analogy for this case in the analogue world. Obviously, a credential holder should no longer use a credential after its revocation. However, a credential might have been sent before the credential was revoked and the credential verifier might choose to verify it with some delay. It would impact the trust in the system, if a credential that successfully verified yesterday would be treated like a non-existent or forged document the next day. Credential verifiers deserve to know that the reason for a verification failure is not a damaged or

manipulated credential file but a revocation. Therefore, the credential should still verify, but with the revocation notice attached.

Should the revocation notice contain a revocation reason? Revocation reasons could contain information that might still be disputed or that are of confidential nature. The knowledge of some revocation reasons, however, could protect a credential holder. Credentials can be revoked because they are replaced with a corrected or even a superior credential, e.g., in the case of the CAS, DAS, MAS continued education certificates of Swiss universities where a prior CAS certificate needs to be returned when a DAS certificate is granted. So, adding a revocation reason should be optional and should not contain too many details.

To summarize, privacy by design and compliance with data protection laws can be translated in functional requirements that are largely dependent on the context of the credential issued. For diplomas this can be translated into the following:

- The credential should be controlled by the credential holder. Besides the credential issuer, no other entities should have access to the credential unless authorized or provided by the credential holder.
- The rightful possession of a copy of the credential justifies the verification of the credential including the question of whether it has been revoked.
- Retaining credentials longer than legally justified, for example by employers, might violate data protection regulation. However, determining whether a credential has been rightfully retained would be too complex to be modeled and enforced by the verification mechanism.
- The control of the credential holder over the credential is limited once presented to a credential verifier. The credential holder can neither block a verification nor remove a revocation notice.

Data protection concerns were a major topic in the evaluation and are further discussed in section 8.4.

To summarize, the main non-functional requirements have been analyzed and translated into a range of additional key functional requirements. During the specification and implementation phase these functional requirements derived from the non-functional requirements are refined and complemented with further details.

Chapter 6 Design

The following design describes a framework for the creation and verification of secure long-term credentials that can be revoked. It first discusses different verification methods and then proposes a combination of verification methods that complement each other. Based on that a framework for the secure long-term verification of credentials is designed. This framework consists of an architecture of modules for the creation and verification of credentials, the design of the credentials and a design for the long-term governance. After the overall architecture is described, a functional design is presented.

6.1 Choice of verification method

When selecting a verification method, privacy by design should be applied. *Danezifs* proposes eight privacy design strategies [167, pp. 19–22]:

- Minimize the amount of personal data that is processed (*select before you collect*)
- Hide information from plain view (render data unlinkable, encrypt)
- Separate data (process data by different systems and/or stakeholders)
- Aggregate data (aggregation can be an anonymization technique)
- Inform data subjects (data subjects should be informed about what the system does or could do, information is key prerequisite to control)
- Control (users should be able to use the information and to make informed choices)
- Enforce regulation (comply with regulation and provide users with tools to have regulation enforced if other stakeholders do not comply)
- Demonstrate compliance (accountability of the system)

In the context of long-term credentials, data minimization, data hiding, data separation and control by credential holders seem to be the most important approaches. Information of stake holders should be done when the system is deployed and the compliance with data protection regulation should be the result and demonstrated.

Four methods to verify electronic documents are reviewed:

6.1.1 Online Verification

A relatively simple verification method is to verify a credential against an online source. The local information, *controlled by the credential holder* is a reference and key to the trusted online source. Without that key, no information about the credential will be transferred. The key could be an identifier or the digital credential document itself. Using the credential itself as a key limits the access to people who are in possession of the credential and minimizes abuse. No list of credentials needs to be published.

The *authenticity* of the online connection might be verified by using cryptographic credentials and a secure online communication protocol like https that uses *transport layer security* (TLS). The trusted source could be the institution that authored the document or another trusted institution. This solution is rather simple and built on well-established chains of trust. This solution has several drawbacks that would need to be addressed:

The online verification *depends on the availability of a server of the credential issuing institution or of a service-provider*. If the server is not available anymore, the credential cannot be proven anymore. Alternatives could be a centralized but redundant server of a national or international entity or a decentralized approach, where credentials could be verified through a range of trusted verifiers.

A person or institution wishing to verify a credential might want to obtain a *permanent proof* for its validity at the time of verification. In case the online service to validate the credential is no longer available after the verification, the verifying entity will have no proof that it did successfully verify the credential. Accessing a website does not automatically offer this proof. However, the verifier could use a website evidence preserving server like Pagefreezer [173]. But this might incur additional costs and lowers usability. The website could also generate cryptographically signed proofs for a credential itself: It could, for example, generate a PDF containing a digital signature that can be downloaded when a credential is verified.

The online verification will be able to count how often every credential has been verified. Where the verification requests came from can also be traced. The data protection principle of data minimization requires this data to be limited – or at least requires other options to be offered as well, so that verification without leaving a trace is possible.

6.1.2 Qualified electronic seal

A cryptographic signature in the form of a qualified electronic seal is a legally recognized and established form to establish the authenticity of an electronic document created by an institution. An established public key infrastructure (PKI) provides a chain of trust to verify who has signed the document and that the document has not been altered since. Standard PDF-viewers like Adobe Acrobat and online services allow the verification of the document. However, this method also has its drawbacks that need to be addressed:

Qualified electronic seals cannot be revoked. Qualified electronic seals are based on certificates. In case the private key of a certificate has been compromised the certificate will be suspended for future use, but there is no provision in SCSE/ZertES or eiDAS to revoke existing electronic seals on the basis that they should not have been issued due to error or that plagiarism has been discovered. The possibility to revoke a qualified electronic signature is mainly a legal question. Qualified electronic signatures have the legal effect of a handwritten signature (Article 25.2. eIDAS). Since handwritten signatures cannot be revoked, a qualified electronic signature cannot be revoked either by law.

Qualified electronic seals correspond to the same technical requirements than qualified electronic signatures. However, a qualified electronic seal is a signature by a legal entity rather than by a natural person. Art 35.2 eIDAS states that the *qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked*.

Although analogue signatures and seals do not have a revocation possibility either, there is a unique analogue original that can be returned. To compensate for not having a unique digital original that can be returned, credentials based on qualified electronic seals require an additional revocation layer. A list of revoked credentials could be made publicly available. This list could include only credential numbers or hashes, so that it does not convey personal data to people that are not in the possession of the original document. Still a check against the revocation list might not always be done, lowers usability and re-introduces some kind of online verification service.

Qualified electronic seals are based on qualified certificates. These certificates have a limited term of validity. In case the private key of a certificate has been compromised, the certificate will be revoked. All credentials created after that revocation date will be invalid. Therefore, it is important to always verify that the qualified electronic seal was created before the certificate it is based on became invalid. Timestamping the signed document can prove that the qualified electronic seal was done before the certificate expired. The timestamping, however, is also based on a certificate that has a limited time of validity. Therefore, the timestamp needs to be re-timestamped before the certificate it is based on expires. A chain of timestamps can ensure that the qualified electronic seal remains legally valid and trustworthy. The requirements for a technical infrastructure to store cryptographically signed documents in a way that preserves their proof of authenticity is, for example, described in the German technical guideline TR-ESOR [166]. Unless those services become standard, they will be an almost unsurmountable barrier for students. Of course, the university could organize this kind of service. However, this would mean that the verification will again become dependent on an online service offered by the university.

In Switzerland the SCSE [26] and in the EU the eIDAS regulation [23] provide a basis for the legal recognition of cryptographic signatures using a certified public key infrastructure. Even though already in 2001 the UNCITRAL proposed a model law on electronic signatures [25], there is no global recognition of these qualified electronic signatures yet. Even the Swiss SCSE-compliant signatures are not fully recognized in the EU and vice versa. However, qualified electronic seals so far are the only digital verification methods with a direct legal basis. Therefore, this drawback still leaves an advantage compared to other methods.

6.1.3 Distributed ledger

A third method for certifying a credential is to store a digital fingerprint of the credential on a blockchain. It can at the same time record a permanent proof and additional information about revocations. In some countries such proofs on

distributed ledgers already have been recognized in courts [41]. The EU is proposing a revised eIDAS regulation that includes *qualified electronic ledgers* in Article 3 nr. 52, Articles 45i and 45h [149]. It thereby offers a chain of timestamps that could be a solution for the preservation of qualified electronic seals. Distributed ledgers also do not have a single collection point where verification requests can be monitored. Verification is possible against any node. Installing a node enables local verification that does not send any specific verification information to other systems. Therefore, the identity of who is verifying the credential can remain private. However, the distributed ledger also has some drawbacks:

The distributed ledger provides a high degree of protection against manipulation. However, the ledger itself does not prove the *identity of the author*. A chain of trust comparable to PKIs needs to be added. One possibility is putting the public key of the university on the web server of the university. Then this public key will use the chain of trust used for https/TLS. Other options are official registers or a chain of trust where other universities confirm the identity of the university. However, this approach involves the risk that somebody could establish a list of fake universities that confirm each other.

While PKI has detailed *governance* rules regarding compromised algorithm and data breaches, the governance of distributed ledgers is less standardized. Some countries like Malta or Liechtenstein have enacted laws that require appropriate governance for distributed ledgers that are used for crypto assets. The proposed eIDAS revision in Article 45i also authorizes the European Commission to enact implanting acts that define standards for distributed ledgers. As long as the adherence to appropriate standards is not warranted, there remains a risk of insufficient reaction and the university must be ready to migrate the proofs to a different distributed ledger. The governance including change management is further discussed in section 6.2.5.

As discussed above, the most secure blockchains, *Bitcoin* and *Ethereum* currently come with high financial and *environmental costs per transaction*. Ethereum is slowly migrating to prove of stake, which will reduce the environmental costs, but will not remove the financial costs. Permissioned public blockchains like the academic blockchain *Bloxberg* [174] or the *European Blockchain Services Infrastructure* (EBSI) [175] could offer an alternative.

6.1.4 Self-sovereign identity (SSI)

Self-sovereign identity also uses cryptographic signatures. Like PKI, the verification can be done in private. No central entity will know that a specific credential has been verified. Self-sovereign identity offers two advantages over qualified electronic seals: The separation of credential and identity information and the removal of hierarchical control:

Often credentials like diplomas contain identity information like the name, possibly also the date of birth. The credential will not directly identify its holder, but a photo ID or other additional means is required to identify the physical person. In situations where the name of the holder of a credential is not needed,

a credential could be accorded to a wallet rather than to a name. In case of transferable credentials, this wallet can be connected by some private key. In case of non-transferable credentials, this is not sufficient. The wallet might instead be identified with the person through a photo or via biometric data – like a fingerprint. When presenting a COVID19 vaccination passport or some age verification, the name of the person is not needed and should be hidden for privacy reasons if the link between the person and the credential is secure.

This privacy feature, however, comes at a cost: Students need to guard their wallets. They need to securely transfer wallets over decades between devices. When applying online, a second credential that link the ID to the name of the student is required and needs to be maintained. At the same time, university diplomas are mostly used in circumstances where the holders identify themselves with their names. Neither job applications nor the application to subsequent education is anonymous. While this feature can have very positive privacy implications, this refers to rather theoretical or at least rare situations in the context of diplomas where identification via name and date of birth is not possible or not desired.

Self-sovereign identity is based on decentralized IDs. There is no central entity that issues and controls the IDs of students and universities. With private identity systems like Google or Facebook, a private company could block an ID and thereby block the use of credentials connected to these ids. Government-held IDs could be blocked by governments, which can, for example, create problems for refugees. The public key of a decentralized ID is often stored on a decentralized ledger and therefore cannot be deleted, and the access cannot be blocked by a single actor. However, if the private key of a decentralized ID has been compromised or needs to be recovered, this requires a method to provide access or blacklist a decentralized ID as well. However, the holder of a decentralized ID is free to choose whom to attribute these powers. Compared to a diploma where the name of the person is simply included in the diploma, this solution seems to be overly complicated, burdensome and error prone.

While SSI undoubtedly offers very interesting privacy features, these features do not prove advantageous for many long-term credentials like digital university diplomas. At the same time, SSI must overcome usability issues on top of similar challenges compared to qualified electronic seals as discussed in section 6.1.2 and does not offer substantial advantages in this context. Unless SSI has been well established, a solution for secure digital diplomas should not be based on SSI.

6.1.5 Combination of verification methods

Online verification is user-friendly and supports revocation. The authenticity of the website can be warranted by TLS. There is the drawback that it depends on the credential issuing institution or a provider. Also, the verification server receives with the web requests data about the credential verifier and the credential holder. Of course, the server should not collect that information, but from a data

protection by design perspective, there should at least be an alternative that does not require trust in the server to not collecting this information.

Qualified electronic seals provide off-line verification which is optimal regarding privacy by design. However, they do not show revocations and require periodic new timestamps to remain legally valid.

Smart contracts on distributed ledger technology provide an independent online verification mechanism that separates the traces of verification since any node of the blockchain can be used for verification. Revocation is also visible. Draw backs are a low usability for direct verification and no established system to prove the authenticity of a record.

Similar to the qualified electronic seal, self-sovereign identity also uses cryptographic signatures to certify a credential. However, it offers the advantage to connect credentials to a decentralized id which allows to hide identity details, like the name of the credential holder. However, this general privacy advantage is not useful here, while it requires the use of wallets which would decrease the usability.

Rather than complementing these methods with proprietary features to address the missing functionality, methods could as well be combined. The main disadvantages of qualified electronic seals are the need for maintenance through continued timestamping and the missing revocation functionality. Distributed ledgers can offer both. Every new block represents a timestamp of all prior information on the chain. Putting a hash of a credential on a distributed ledger will constantly add timestamps to it. Smart Contracts on distributed ledgers can also add the revocation functionality that qualified electronic seals are missing. Vice versa, the disadvantages of a distributed ledger, the missing trust chain, can be overcome be the qualified electronic seals. Qualified electronic seals are based upon an official trust chain that securely identifies the institution that has issued the credential. Direct verification against a distributed ledger is possible but requires technical expertise. Online verification can overcome this barrier and provide an easy-to-use user interface. However, the dependence on a single server/service for online verification would limit the durability and autonomy of the verification process. A central online service would also enable tracking of the verification of a credential. Basing the design on a distributed ledger, however, allows the independent verification by different online services and the expert verification directly through a smart contract on a public distributed ledger. Therefore, the online verification is mainly seen as a user interface to the distributed ledger that can be replicated and shared between different institutions offering credentials.

From a data protection by design perspective, this combination allows to separate data flows which makes it more difficult to collect personal data – e.g., at the online server. Although it creates redundancy, which collides with the design goal of data minimization, the redundant personal data is very limited. The PDF-document is also used for all three methods and adding a qualified electronic seal does not run counter minimization of personal data. The hash values on the

blockchain add very limited amount of personal data and the credential issuing institution has to archive the credentials anyway.

6.2 Proposed framework

6.2.1 Architecture

As shown in the discussion above, neither online verification, nor electronic seals or blockchains verification alone can sufficiently fulfill all the requirements, but a combination of these methods could address all requirements. Figure 22 shows a schematic view how the different modules can be combined to create secure digital credentials.

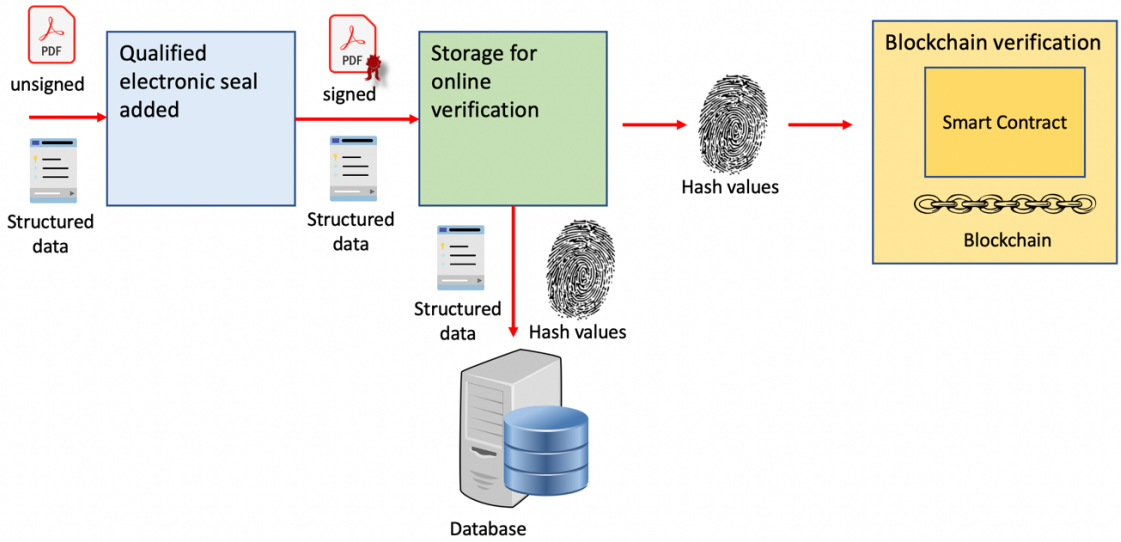


Figure 22: Proposed architecture for creating secure digital credentials

A PDF-file with the credential is created by the institution together with a dataset containing the data of the credential in structured form. A qualified electronic seal is added to the PDF. Hashes of the signed PDF and of the structured data are calculated. The structured data together with the hash values are stored in a database in the institution. The hash values are stored via a smart contract on the blockchain selected.

The verifiers can resort to all three methods. It is possible to verify the qualified electronic seal of the signed PDF. The digital credential can also be verified using the online verification system and a direct verification with the smart contract on the blockchain used is also possible. This leads to the six verification possibilities described in Figure 23:

① The signed PDF-file is verified using a PDF viewer that includes the verification of qualified electronic signatures and seals like Acrobat Reader or an official verification website like the validator of the Swiss Federal Administration [176]. This verification does not consider possible revocations and will also show an error once the certificate used for the original time stamping of the qualified electronic seal is expired. This

verification is also the only one that uses an officially recognized chain of trust to securely identify the issuing institution.

② The signed PDF-file is verified using the online verification. A simplified visual is displayed in the case of successful verification.

③ The credential data is entered manually or entered via a QR code from a visual copy of the credential, e.g. a printout. A simplified visual is displayed in the case of successful verification.

④ A link provided is verified using the online verification. This works if the link has not been deactivated by the credential holder. A simplified visual of the credential is displayed in the case of successful verification.

⑤ The hash value of the signed PDF can be calculated using any implementation of the hash-algorithm used. The hash value can then be verified by calling the smart contract using any node of the blockchain used.

⑥ The hash value of the diploma data can be calculated using any implementation of the hash-algorithm used. The hash value can then be verified by calling the smart contract using any node of the blockchain used.

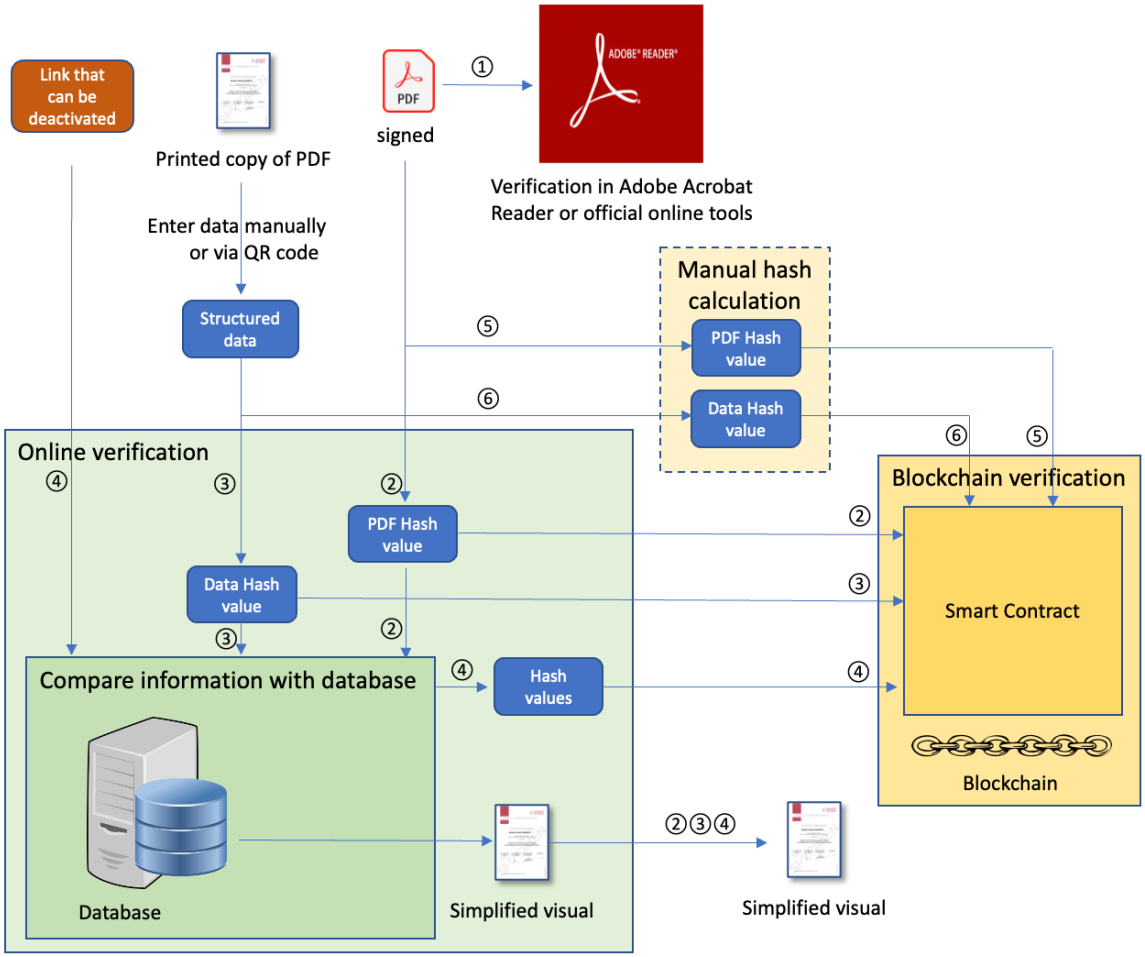


Figure 23: Verification options

Offering six possibilities for verification might look confusing compared to just one online verification possibility offered by other systems. However, the latter would not suffice the requirements of durability, autonomy and legal recognition. The direct verifications against the blockchain and the possibility to enter the credential data are fallback verification methods in case the other verification methods are not available.

The revocation is similar to the creation of a credential but does not concern the qualified electronic seal. The entry is modified in the storage for online verification and the smart contract on the blockchain. The blockchain will conserve a trace of the old entry.

6.2.2 Online verification

The online verification offers verification by accessing a trusted server of the issuing institution. The online verification can be split into two variants: A variant that has access to the records of the institution and another minimal variant that is limited to the blockchain and merely provides a user-interface to the blockchain verification, for example, when verifying credentials of other institutions.

The minimal variant can validate a long-term credential based on hash values of the file or its content. A web interface can access the credential file and can calculate a hash value already in the browser. The hash value will be used to consult the smart contract on the blockchain to find out whether the long-term credential has been granted and whether there has been a revocation in the meantime. If the verifier does not have the original file, but a paper copy or a non-identical digital copy, the verification via the hash value of the original file is not possible. However, the long-term credential data could be verified. This data includes, for example, the name of the credential holder, the name of the credential and the date of issuance. To avoid the possibility of guessing credential data, this data is required to have enough entropy, e.g., by adding a random parameter called *salt*. This data could be entered manually in a web-form or through a QR-code. The verification website will calculate a hash value already in the browser, access the distributed ledger and indicate whether the credential has been granted and whether there has been a revocation in the meantime.

Beyond this minimal requirement, a verification by a server of the issuing institution that has access to credential records can offer additional functionality. It could offer a short link to the credential. However, a link might be indexed by search engines or shared widely. Data protection regulation – namely the right to be forgotten – mandates that these links can be deactivated. A link does require the storage of credential data to show a representation of the credential when the link is entered. The link requires the credential data and not just the hash values of the credential. Data protection regulation requires that – unless the student wishes otherwise – no personal data will be transmitted to people without a good reason e.g., legitimate interest, legal obligation, contract, etc. Therefore, the access to the online verification shall be limited to people who can prove that they are already in possession of the information that is to be verified. The online verification could also make an image of the analogue secure credential available.

However, this puts analogue security features at risk. These security features include the use of special font variations. If the online verification server gets hacked, these features would be exposed. A simplified generated online representation without these security features can be sufficient to be displayed as confirmation of the successful online verification.

Entering data manually can be cumbersome. Uploading original files requires the original files. QR-codes could be used to facilitate this in three different ways:

a) The QR code could include a link to the credential on the online verification server.

b) The QR code could include the credential data.

c) The QR code could include the credential data together with some kind of cryptographical signature.

QR codes are frequently used for links. Smart phones automatically offer to follow a link that is contained in a QR-code visible through the camera of the smartphone. The link could also be combined with option b) or option c). However, QR-codes containing links are not very secure. They could include a slightly modified URL that is under the control of a forger and could host a similarly looking fake verification site. Allowing Unicode characters in URLs opens up the possibility to create URLs that look very similar [177]. Therefore, a QR code should not be used to enable a direct link to the verification server. Entering the URL manually is a small additional effort but reduces the risk to end up at a fake verification website. The URL for the online credential verification should use the domain or a subdomain of the issuing institution's website and should be simple because it needs to be typed in manually.

A QR-code could also be used to include the credential data (option b and c). This could be used to facilitate the handling for the verification of printouts or otherwise modified credential files. Option b) does not protect the credential data in the code. It would be possible to create a fake QR-code for a fake credential. If the QR-code is always verified by the online-verification, a fake QR-code would not go undetected. However, since reading QR-codes can also be done by standard photo apps, it could still give a false impression of security.

The QR-codes used for the verification of COVID19 vaccination passports uses the approach described in option c). The verification of that QR-code, however, requires a proprietary application. QR-codes compliant with ISO/IEC 18004:2015 can represent up to 2953 bytes. Qualified electronic seals compatible with eIDAS or SCSE/ZertES, however, are larger. Therefore, a QR code could represent credential data possibly together with a proprietary validation method, but not a qualified electronic seal.

6.2.3 Blockchain and smart contract-based verification

The blockchain can add two important aspects to the qualified electronic seal:

- **Revocation**: Although no old block of a blockchain will normally be modified after it has been written, new entries can state that prior

information is not valid anymore. Bitcoin is already based on that principle. Bitcoins received that have subsequently been spent in another transaction, are no longer under the control of the first recipient. This blocks double-spending of Bitcoins. Collecting all entries regarding a diploma would be tedious if the whole blockchain needs to be searched for updates that revoke an existing diploma. Smart contracts do that automatically. They offer a programming language – e.g., Solidity [52] – to render this almost as easily as modifying a normal program variable in any other programming language.

- **Continued time stamping**: A sequence of time stamping of a certified electronic seal means to hash the last time stamp, add the current time and sign it with a certificate of a trusted time stamping service. Blockchain is following a similar approach. It hashes the last block, adds the time, new content and adds the newly created block through the consensus algorithm to the blockchain. Although the block producer that has created that block might not be a trusted time stamping service, the consensus algorithm ensures that the new block does not introduce a timestamp that differs more than a couple of seconds. As *Sorge/Leicht* [40] point out (see section 3.2) a qualified electronic timestamp of a hash value of a single block of a blockchain can serve as a timestamp for all digital objects that are referenced by hash values on this and prior blocks. Regular (e.g., annual) qualified electronic timestamps of a blockchain could therefore preserve the validitiy of all qualified electronic signatures and seals for which hash values are stored on a blockchain.

Smart contracts also offer the possibility to manage access rights for creating and revoking diplomas beyond one private key that is a universal key.

It is important to choose the right blockchain. Although migration to a different blockchain needs to be possible, this should be avoided as much as possible. Migration voids the direct verification against the original blockchain and is difficult if the university does not exist anymore. The criteria for selecting a blockchain are:

a) **Enough active participants** to trust the system. This can be achieved by a large number of unknown participants (as in public permissionless blockchains) or by a smaller number of trusted known actors (as in public permissioned blockchains like EBSI, Alastria or Bloxberg).

b) **Trust in the technology** used. The technology used should be well tested so that the risk of critical bugs is low.

c) **Trust in the governance** of the blockchain. Within the lifespan of the long-term credential, like university diplomas, problems will almost certainly occur. A good governance will properly address these and update the blockchain code accordingly (also section 6.2.5).

d) **Trust in the long-term interest of participants**. A blockchain will lose its value as evidence when interest in it is lost. If the number of block

producers becomes small, it becomes easier to manipulate it. The participants do not have to stay the same, but there needs to constantly be a sufficiently high number of participants.

e) **Legality**. A permissioned blockchain has known participants in known locations. These are subject to the jurisdictions they operate in. If the activities of and on the blockchain are not compliant with the applicable laws, the long-term existence of the blockchain is endangered.

f) The **transaction costs** on that blockchain should be reasonable. The maximum number of blockchain transactions per second varies largely depending on the blockchain used but is usually limited. One way to reduce the risk of congestion is to have a dynamic fee structure. Less important transactions will wait for lower fees or will move to different systems. The disadvantage of dynamic fees is that they cannot be budgeted. Fees for an average transaction on public Ethereum, for example, varied between 0.50 CHF and 70 CHF during the last 24 months [132].

g) **Carbon footprint**. The *Proof of Work* (PoW) mining algorithm of public permissionless PoW blockchains like Bitcoin or Ethereum use a lot of energy (see 3.2 and 4.2). The selected blockchain should use a very limited amount of energy.

h) **Smart contracts**. It should be possible to program and use smart contracts scripts on the blockchain to model revocation and permission structures.

6.2.4 Credential data and the credential pdf

A credential as a PDF-file and the relevant credential data are the input of the certification system. The credential data depends on the type of the credential, e.g. university diploma. A university diploma includes the description of the diploma, the date of issuance, the full name of the holder and the issuing institution. It should also include a date of birth to avoid the abuse of the credential by people with identical names, since it otherwise only uses the name to identify the credential holder.

A cryptographic hash cannot be reversed. However, if the entropy of the data hashed is too low, a brute-force attack can be used to guess the information hashed. This is true for a hash of the PDF as well as a hash for the data. PDFs that are scanned contain noise which corresponds to a high level of entropy. PDFs that are generated automatically require some noise to be added. This noise, also called *salt* in the context of cryptographic hashing, can be hidden when generating a PDF. Regarding the direct verification of credential data, the salt needs to be explicitly added. The salt value could also be used as a unique ID. Adding a random *Universal Unique ID* (uuid), also called *Global Unique ID* (guid) [178] with 128 bits of data should be sufficient to stop a brute-force attack.

Digital credentials should look identical to analogue credentials on paper as long as they are used in parallel. Long-term credentials on paper – like university

diplomas – are either printed or calligraphed by hand. Secure paper and special fonts can enhance security. Since the new process adds superior security, these features could be abandoned in the long run. However, as long as paper credentials without digital security features are being used and recognized, these features should remain in place. To create a similar look for digital and analogue credential, there are three principal approaches:

- Paper first: Create a paper credential and then scan the paper credential to obtain the unsecured PDF. This is particularly important if manuscript signatures or preprinted templates are being used or the credential-creating process varies within the institution.
- Digital first: Create a complete (and secured) digital credential and then print it to obtain the paper version.
- Independent creation of similar looking analogue and digital credential.

While paper first is a good approach for the transition, it does not remove manual processes but adds another manual process for scanning the paper credential. Digital first is more efficient but might require redesigning and rebuilding the established credential generation process, for example at universities. The independent creation of analogue and digital credentials increases the risk of creating contradicting versions of a credential and should be avoided.

The PDF should contain information and instructions regarding the different verification possibilities and contain the credential data in a form that can be easily entered.

6.2.5 Governance

Governance aspects can be split into aspects that should be coded in the system and aspects that relate to laws, regulation of the issuing institution, contracts, workflows and procedures. Particularly regarding distributed ledger technology, a discussion between coded on-chain governance and more flexible off-chain governance emerged. On-chain governance refers to decisions that are taken by the means of the blockchain itself. Off-chain governance refers to decisions taken in other forms, e.g., taken by a foundation or voted on by means other than the blockchain itself. Every blockchain has an on-chain consensus mechanism for when it generates new blocks. If there is no agreement on what the next block should be, the consensus mechanism selects the choice of the “majority”. The “majority” could mean the majority of computing power in case of blockchains that operate with *Proof of Work* (poW) like Bitcoin or the majority of coins staked in case of *Proof of Stake* (poS). The minority might still continue as a different blockchain, which is called a *fork*. When there was a disagreement as to whether the Ethereum blockchain should be patched to remedy the DAO-bug, Ethereum split into two chains: Ethereum and Ethereum Classic [179, p. 76]. Some blockchains include additional voting mechanisms, for example the blockchain Dash includes voting on proposals that are funded directly through coins of that blockchain [180]. The counting of the vote and the payment is done automatically. The blockchain EOS introduced a “constitution” [181] and an extensive on-chain

governance model including an on-chain dispute resolution mechanism and still ran into problems. On the other hand, *Vitalik Buterin*, for example, a co-founder of the Ethereum blockchain favored a less formal off-chain mechanism arguing that governance is more than formal voting [182]. Particularly at an early stage, flexibility is more important than securing the governance rules through code. Changes are too frequent, and the risk of bugs outweighs the security benefit of coded rules. Therefore, a system should start with minimal coded governance and should extend this with time. Governance requirements have been identified in the following processes:

a) The decision process at the issuing institution for issuing or revoking a long-term credential.

b) Legal review, if the decision is challenged through the legal system.

c) The governance process for the systems used.

d) The rules and access rights governing the creation and revocation of long-term credentials.

e) Adding and removing of participating institutions.

f) The governance on the meta-level regarding the migration to a new system and regarding the modification of the governance process itself.

Coding governance can improve security because coded governance reduces the possibility to abuse the system. However, coded rules are also less flexible. Particularly in the beginning, only a minimal set of rules should be coded. When the frequency of modifications is going down and the system has reached stability, further rules might be transformed into code. However, many rules need to stay flexible and should not be coded at all.

The decision process (a) to issuing or revoking a credential is usually a manual process. Even if it becomes automated at one point, Art 22 GDPR and to a lesser extent Article 21 of the new Swiss data protection law at least demand manual oversight and the possibility to intervene manually.

The legal review, e.g., through courts (b) will not be governed by the system. If the legal review process is going to be automated, an interface to the certification process could be imagined mid- to long-term.

The governance process of the systems used (c) needs to be distinguished for the online server, the qualified electronic seal, the smart contract and the blockchain the smart contract is based on. The governance process for a qualified electronic seal is defined by law. A qualified electronic seal is created based on a qualified certificate by a verified qualified trust service provider. The procedure of issuing and – if needed – revoking a qualified electronic certificate is defined by laws like eIDAS or SCSE/ZertES and performed by qualified trust service providers. They make sure that the order for the qualified electronic seal is signed by proper representatives of the institution, that the certificate properly identifies the institution and that a proper representative of the institution receives the private keys to create qualified electronic seals in the name of the institution.

The online server uses TLS to encrypt the communication between a browser and the web server. TLS uses a certificate that identifies the web server. The identification can be done, for example in the case of the University of Geneva, with an extended validation certificate with the legal name of the institution and the id of the institution in the UID company register or the identification can be limited to the domain name. Although users usually pay little attention to the different types of TLS certificates [183], in case of doubt, the lock symbol in the URL-field of the browser can be clicked to see if further information about the institution controlling the website is available. For an online verification server, it is recommended to use an extended validation certificate so that users can verify the institution behind the website.

Blockchains come with a broad spectrum of governance. *Allen/Berg* define *blockchain governance* as the *process by which stakeholders exercise bargaining powers over the network* [184, p. 2]. A proper blockchain governance is one of the criteria to select a blockchain for the system. Unless the blockchain is dedicated to the system, the certification will not directly influence the blockchain governance. Since a sufficient number of nodes is a prerequisite for selecting a blockchain, a dedicated blockchain is rather not advisable. Therefore, the governance of the blockchain is not part of the designed system itself.

A smart contract runs on the blockchain chosen. The smart contract is dedicated to the issuing, revoking and verifying of credentials. Part of the smart contract governance is a possible migration to a new version of the smart contract. The smart contract address will be visible on the credential and should be verifiable, e.g., via the website of the institution. While the identity of the institution is also warranted by the qualified electronic seal, the revocation depends on the authenticity of the smart contract. Therefore, smart contract addresses should remain constant if possible. Although smart contracts on most blockchains cannot be altered, a smart contract might contain the possibility to set a redirection to a new version of the smart contract that can be activated through a special authentication key. There can be two different designs for the smart contract governance: A centralized or a decentralized model. In the centralized model, one institution holds the key to redirect and update. The institution decides on its own – possibly with an internal voting mechanism. In the decentralized model, a distributed voting model is integrated into the smart contract. Combinations and variants of these can be imagined: For example, the centralized model might be preceded by an informal decentralized process. To start with, a central update key should be sufficient but a possibility to decentralize should be planned for.

Unlike the certificates for TLS or the qualified electronic seal, a decentralized system does not have an authority that can delete or revoke things that went out of control. This would be the case if the master admin key has been disclosed to a person that cannot be trusted. One possibility to address that risk could be to modify the master admin key in that case. However, this would enable a fast attacker to modify the key herself and lock out the university from any access. This could be avoided by a superior admin master key that can only be

used to modify the admin master key. However, this creates the same issue for the superior master key. Therefore, there should be also a separate special master key that should only have one function: To destroy the smart contract. In case an attacker gains control of the system, the issuing institution can always destroy the system and setup a new one. This way, the much bigger damage of an attacker controlling the smart contract without the issuing institution being able to stop her can be largely reduced.

The systems involved in securing the credentials have their proper methods to authenticate users (d). A qualified electronic seal is generated by a signing device at the institution or by a trust service provider as a remote signature. The authentication can be done separately for the creation of the qualified electronic seal or it can be integrated into a trusted environment. The authentication can be done as batch processing of many credentials or individually. The appropriate procedures depend on the number and rhythm of the creation of certificates. A remote qualified electronic seal requires the least investment but has higher costs per seal. Signing locally with a signature card requires very limited investment in infrastructure and does not have external costs per credential, but is more difficult to integrate into an overall workflow. A hardware security module could be directly integrated into the process of generating qualified electronic seals. While this could be the most efficient way to generate credentials that have qualified electronic seals, this also requires a higher investment and is only economically viable with a high number of credentials issued.

To add or revoke credentials towards the smart contract, authentication with a private key is required. The authentication methods are not regulated but can be freely chosen. This might change with the upcoming revision of EU-eIDAS and the introduction of qualified electronic ledgers. Since a smart contract can manage different rights for different private keys, the rights management should be within the smart contract. An additional layer of rights management could be added when integrating the creation of the qualified electronic seal and the smart contract-registration of the hash values. A leveled approach is recommended from the admin keys of the smart contract as discussed above towards keys to add institutions (e), keys for admins at the institutions, keys for creating and keys for revoking credentials. The decision to add a new institution could be voted for through the smart contract or off-chain.

The governance process for the system itself including modifications to the governance process (f) should not be formalized in the smart contract in the beginning. On-chain governance is quite inflexible and might be added when the system has been introduced, development has almost stopped, and the system reached a high level of stability.

Chapter 7 Implementation

Based on the design (Chapter 6), a prototype was built for the University of Geneva. The University of Geneva regularly receives requests to verify paper diplomas. The University Geneva also has a program called *InZone* [185] for the education of refugees in refugee camps. For refugees the recognition of credentials is an issue that could benefit from legally recognized digital diplomas [186, p. 42]. The prototype was based on the University of Geneva's continuous education programs (formation continue) offering CAS, DAS and MAS degrees to graduates or people with similar work experience.

The prototype follows the design of the three verification components: Qualified electronic seal, online verification and registration and verification through a smart contract on a blockchain preceded by the creation of a diploma pdf and the extraction of diploma data (Figure 24).

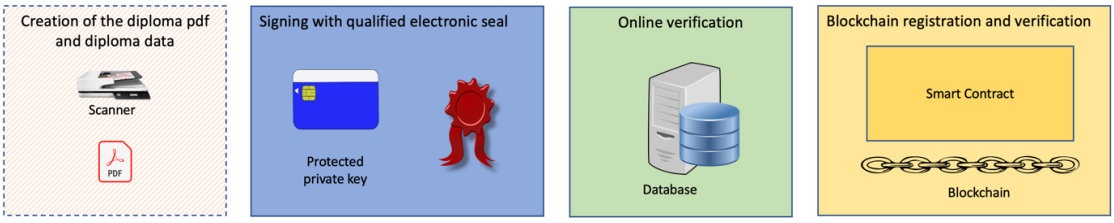


Figure 24: Modules for verification of university diplomas

7.1 Creation of the diploma PDF and diploma data

The creation of a digital diploma as digital credential requires the creation of a diploma PDF and the extraction of diploma data (see section 6.2.4). For the prototype the approach of paper first was chosen. To comply with data protection regulation, however, only specimens of diplomas were used for demonstrations and tests. Diplomas were scanned and diploma data was collected in an excel file. A random ID was added as a 128 bit guid. The module was not built as an automated module but the steps were performed manually.

The diplomas are bilingual with French on the front and English on the back. Both sides were scanned. An additional page was added explaining the available verification procedures. This includes the URL for the online verification, the diploma data in text and a detailed description of the direct verification using the smart contract in case the online verification is not available. Regarding the verification of the qualified electronic seal, it should be noted that this verification does not guarantee that diplomas have not been revoked in the meantime. It should also state that the verification will fail after a certain period of time due to expired certificates and that this can be seen in the detailed verification report. Further pages could be added, e.g., the so-called "supplement" describing the contents of the education program passed.

The university also makes an academic transcript (relevé de notes) available to the student. This contains detailed grades and is usually available

before the diploma is available. This academic transcript could also be verified through the proposed system. Due to data protection reasons, however, this should not be done in the same document, so that the student is able to freely decide whether she wants to make it available together with the diploma. In the prototype, the academic transcript was not included in the set of specimens.

7.2 The qualified electronic seal

A qualified electronic seal requires a qualified electronic certificate. In Switzerland these certificates are available from certified trust providers: Swisscom Schweiz AG, QuoVadis Trustlink AG, SwissSign AG and the Federal Office of Information Technology, System and Telecommunication. Offers were requested from the three private entities among them.

Swisscom offered a remote certificate through the company Skribble. A remote certificate is stored at a trust provider. The qualified electronic seals will be created at the trust providers. A two-factor authentication verifies that the request for the creation of a qualified electronic seal comes from an authorized person. Although initial costs for remote qualified electronic seals are lower, they come with certain disadvantages: The authentication is personal and not bound to the university, but to employees of the university. The costs do not scale well for a higher number of qualified electronic seals.

Obtaining a qualified certificate for generating qualified electronic seals proved more difficult for the university. These certificates are generated on the basis of the entry in the UID register. However, the entry of the university in this register was used for the VAT and labeled as such. A proper certificate requires a different entry. The administrative procedures to have a proper entry in the UID register and receive a certificate for that entry proved too complicated to be finalized during the prototype phase. The system was therefore used without adding qualified electronic seals. The creation of a qualified electronic signature, however, was tested with a personal qualified electronic signature.

There are different standards for a qualified electronic signature or a qualified electronic seal for PDF documents. For PDF documents the PAdES standard / ETSI EN 319 122 should be used [88]. For PAdES there are different levels: the basic level (B-Level), the basic level with added timestamp (T-Level), a timestamp with added verification related information like certificates (LT-Level) and one that includes verification related information for the signature and the timestamp added that will allow the signature to be validated beyond any event that may limit its validity (LTA-Level). The LTA-Level should be used for qualified electronic seals for long-term credentials.

7.3 Online verification

The online verification was chosen as the central component that should communicate with the database and the smart contract on the blockchain. The online verification should be accessible for the university administration as well

as the students via a web interface. To access the smart contract, a smart contract API was added. This led to the design shown in Figure 25.

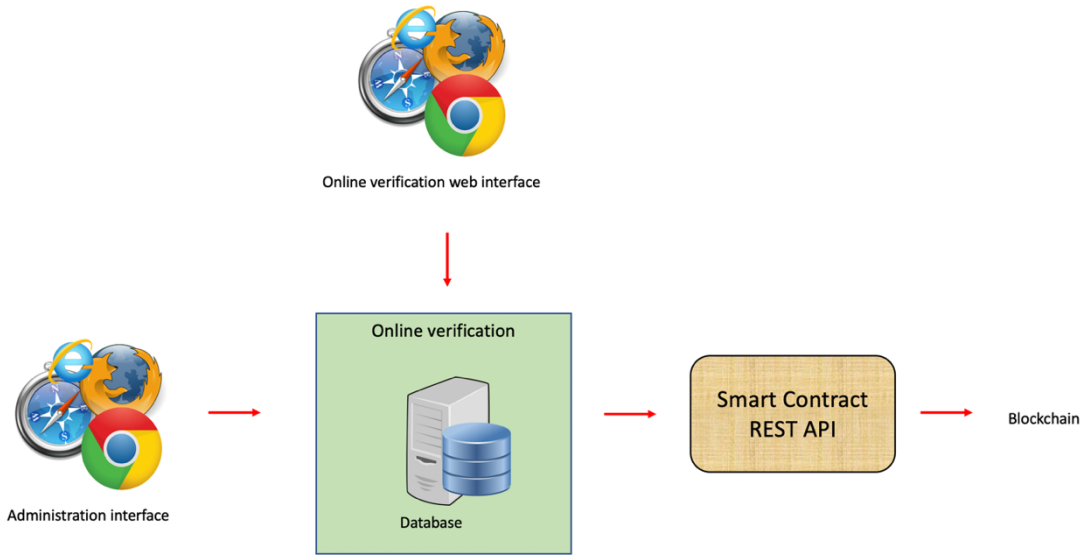


Figure 25: Interfaces to the online verification module

7.3.1 Administration interface

The administration and the verification interface were built with the framework *Concrete 5* [187]. They used the templates and layout of other websites of the University of Geneva.

The administration interface allows diplomas to be added and revoked. It is only accessible within the university intranet and requires an account with the appropriate access rights.

The admin interface allows all available diplomas to be listed, the database records to be verified with the smart contract entries, a diploma to be added and revoked. When revoking a diploma, a reason from a list of reasons can be added:

Revocation because of an error shall be added, when the diploma was issued because of an error in the records. ***Revocation because of fraud*** can signal when a diploma has been fraudulently created. Fraud should only be signaled if the decision on fraud is final. ***Revocation because of a replacement of the diploma*** can be used for multiple reasons. In the system of CAS, DAS, MAS diplomas, a DAS or MAS diploma can be based on the credit points earned in an inferior diploma. However, the inferior diploma has to be given back. The digital diploma therefore has to be revoked. To signal that there is no lack of qualification but that there exists a new, and even superior diploma, the revocation reason signals a replacement. This reason could also be used in case of a name or gender change. Finally, revocation signal ***no reason***. This might be a good choice, particularly if the revocation is disputed. The admin interface also allows a previously revoked diploma to be reinstated. However, a detailed

inspection of the blockchain will still show that the diploma had been revoked before.

7.3.2 Verification interface

The verification interface offers the verification by ID, by a hash of the PDF or by data (Figure 26). The verification by ID is based on the ID of the diploma. It allows a direct link to the diploma to be generated. Alternatively, the ID can be entered into a field in a form. The access via ID can be enabled or blocked on the request of the student for data protection reasons. For the verification by the hash of the PDF, the local PDF-file needs to be selected in the browser. The hash value is then calculated in the browser sent to the server. The diploma can also be verified by the relevant data printed on the diploma. The data is merged in a string which is then used to calculate a hash value. To reduce the risk of errors, the information to be typed in is included in a separate sheet of the diploma.

The verification server has two ways for verification. It has a local database, and it can verify the hash values with the blockchain smart contract. The diploma is only signaled as valid if both, the smart contract and the internal database confirm the validity.

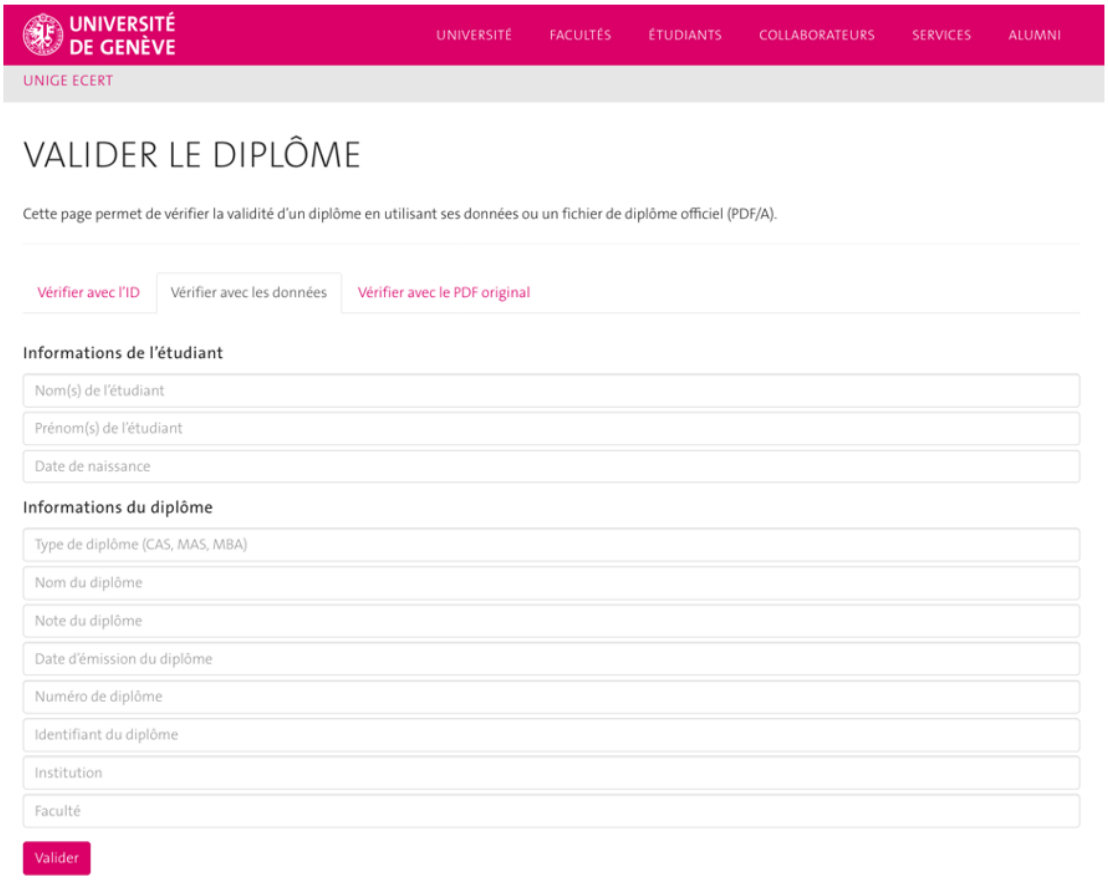


Figure 26: Verification screen

When the diploma is signaled as valid, a generated image is displayed (Figure 27). To protect the analogue anti-forging features, original diploma scans are neither stored nor displayed nor otherwise processed by the web server.

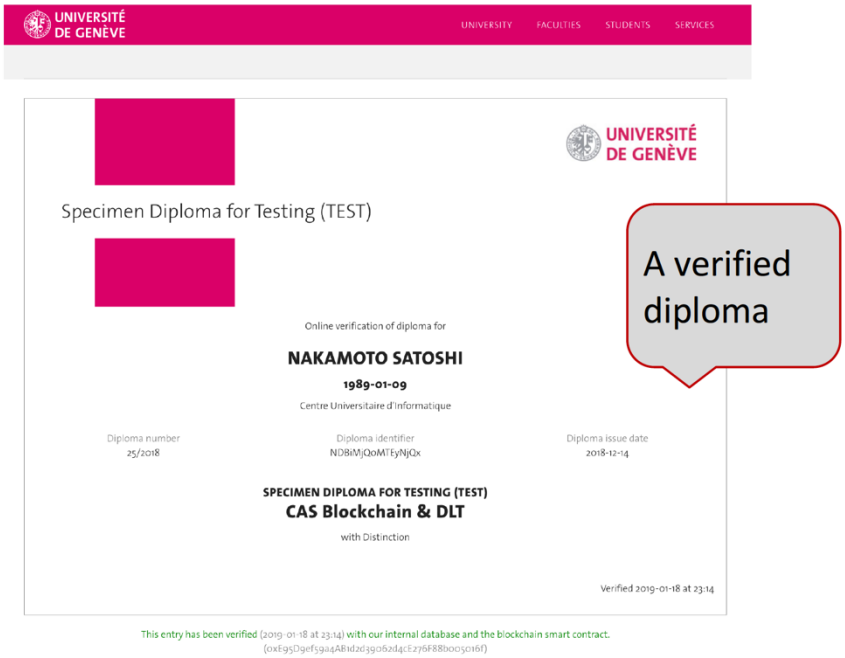


Figure 27: Display of a successfully verified diploma

The web interface also provides information about the system as well as the other three possibilities for verification using the qualified electronic seal or the blockchain directly.

7.4 Blockchain verification

For the blockchain verification a proper blockchain needs to be selected to deploy the smart contract. The smart contract needs to provide the required functionality and an API is required to access the smart contract.

7.4.1 Selection of the proper blockchain

The criteria for selecting a blockchain were discussed in section 6.2.3. The following blockchains have been evaluated: Bitcoin, Permissionless Ethereum, EOS – a *decentralized Proof of Stake* (dPOS) blockchain, the *European Blockchain Services Infrastructure* EBSI supported by the European Commission and the academic blockchain *Bloxberg*.

Bitcoin offers very limited smart contract functionality. At the same time, it has an extremely high carbon footprint and transactions are very expensive.

Permissionless Ethereum is the oldest blockchain that supports smart contracts in its own language Solidity that now has been adopted by other blockchains as well. It is currently in a transition phase from *Proof of Work* (PoW) to *Proof of Stake* (PoS). It is well maintained and has a strong governance to address technical issues but with little influence of any single user group. It is trusted for large scale monetary transactions. It still suffers from congestion and

high transaction fees. There are several testnets for Ethereum that can be used for tests, free of charge.

Forks of Ethereum like **Ethereum Classic** have reduced transaction costs and reduced carbon footprint, but also reduced security. Some bigger miners of the main Ethereum fork could just switch and take over Ethereum Classic. Blockchains like **Tezos** [188], **EOS** [189] or **Blockstack** [81] offer much lower fees and a much lower carbon footprint. Their *delegated Proof of Stake* (dPoS) consensus mechanism offers a relatively high level of security and includes governance elements. EOS, for example has a group of 21 block producers that are voted for by holders of EOS tokens. EOS supports smart contracts in the C++ programming language. There are no direct smart contract execution fees, but running smart contracts requires the purchase of sufficient virtual CPU and RAM on the network but is relatively cheap. There is an extensive governance model for EOS, which survived some initial difficulties.

It is planned for the ***European Blockchain Service Infrastructure EBSI*** [175] to offer different technical infrastructures. In a first prototype a testnet of public permissioned public variant of Ethereum was installed. For version 2, a tender resulted in seven contractors that will integrate their technology into the EBSI framework [150]. This was announced in October 2021. Details and actual systems will be available later. It is not ready yet. EBSI in particular announces the support of applications of self-sovereign identity and securing academic titles. While *BCDiploma* previously was announced to run on EBSI, the current concept for supporting diploma verification is quite different and is based on SSI-wallets [190, p. 23].

Bloxberg [174] is an academic blockchain based on the permissioned Ethereum variant with *Proof of Authority* (PoA). It supports Solidity, the best-established smart contract programming language. This system is supported by the Max Planck Digital Library and a large academic community that is trusted in the academic world. It does not demand transactions fees, has a very small carbon footprint and a defined governance. Bloxberg is still new and has limited resources and an appropriate legal entity is still missing. The interest of supporting an application that secures academic titles is high.

The prototype was first done on **Ropsten**, a public permissonless Ethereum testnet and then it was ported to **Bloxberg**. This is currently considered the best choice. Depending on the development of **EBSI**, EBSI could be an option in the future too.

7.4.2 The smart contract

For the prototype the smart contract was designed to support the registration of a credential using two hash values. One hash value is a hash value of the PDF-file and the second hash value is used to hash the diploma data (see 6.2.1 and 7.3.2). Hash values need to be practically unique, and no credential can be registered twice unless it is modified to result in different hash values. Diplomas can be revoked giving one of the revocation reasons described in section 7.3.1. A revocation also can be reversed to restore the diploma. All replies of the smart

contract are verbose, so in contrast to other solutions like Switch verify (see section 4.3.7.4), the smart contract can also be consulted directly and gives a well understandable answer.

The governance functionality was limited in the prototype. It includes different keys for granting and revoking of diplomas, a key for administration of these keys and a key that is capable of destroying the smart contract. For a future system that supports many institutions, the governance of keys for adding and revoking diplomas via the smart contract is critical. Therefore, a hierarchy of keys and permissions is proposed in Figure 28. The keys for adding a diploma should be integrated into the student administration system. If the revocation of a diploma is done through the student admin system, the key for revoking a diploma should also be integrated there – otherwise it is used manually. The institution admin key should be used to modify these keys, for example when employees leave, or software is replaced. The global admin key is used to set the institution admin keys, e.g., when institutions are added, or employees that had access to institution admin keys leave, or an institution no longer wishes to use the system. In the latter case the institution admin key can be set to a null value to which no private key is known.

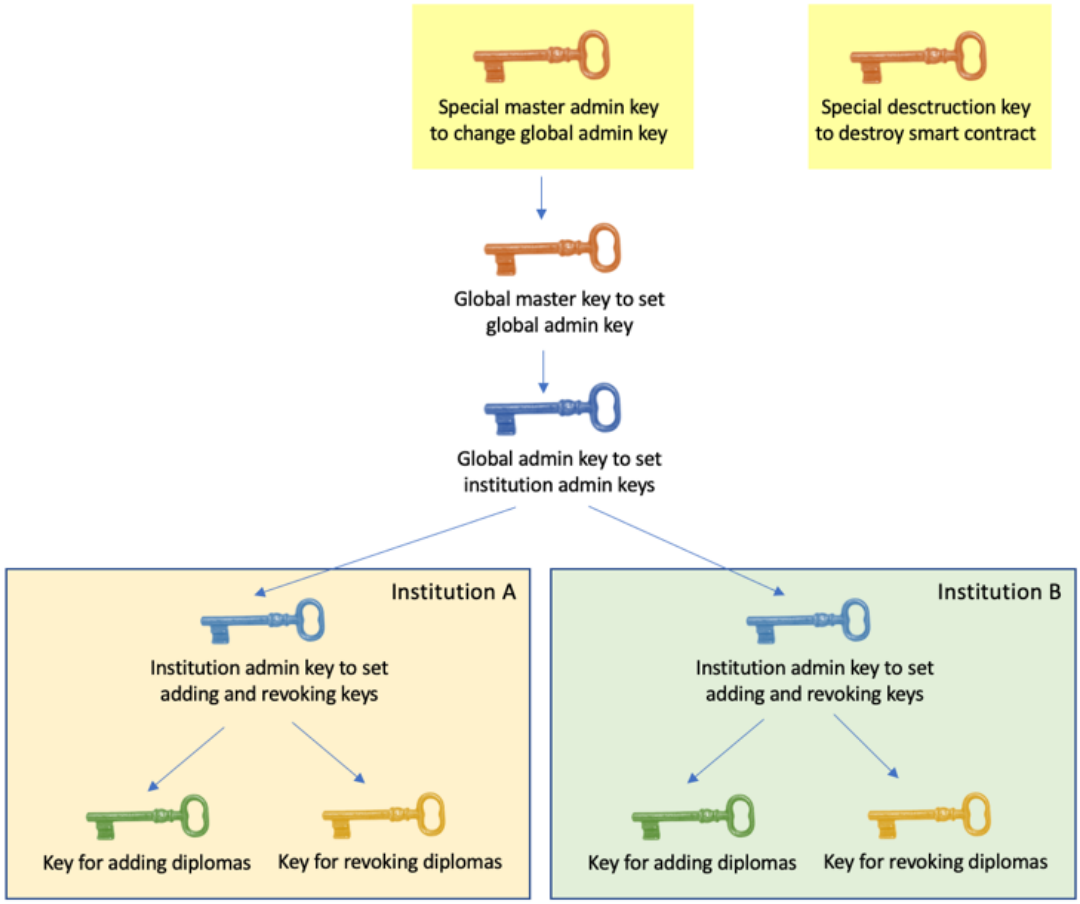


Figure 28: Hierarchy of keys

Smart contracts use asymmetric cryptography to check authorizations. A transaction is authorized by a private key by signing it with the private key. A

smart contract can then verify the authorization by verifying it against the authorized public keys stored on the blockchain. Figure 28 shows the proposed hierarchy of keys. The global admin key can be changed using the global master key in case employees that had access to this key leave. In exceptional circumstances, the global master key can be changed by the special master key and the smart contract can be destroyed by using the special destruction key. Both special keys are only to be used in exceptional circumstances and should be guarded by special trusted institutions – e.g. a notary.

The smart contract on the blockchain can be called using any node of the Bloxberg blockchain. The smart contract address is 0xcD77c7d1B2daAb94b5c7883B6e44385a30A16dD3. The source code has been uploaded to https://blockexplorer.bloxberg.org and can be verified against the complied code on the chain: https://blockexplorer.bloxberg.org/address/0xcD77c7d1B2daAb94b5c7883B6e44385a30A16dD3/contracts. The smart contract offers the possibility to add, revoke or verify diplomas. It offers the functionality described in Table 20. Write operations, particularly administration calls need to be signed by an appropriately authorized key.

Function	Type	Called by	Parameters	Return
Add diploma	Write operation	Student Administration System	Hash values of the signed PDF and the diploma data, *Institution Sequence Number*, 🔒	OK / Error
Revoke diploma	Write operation	Student Administration System or manually	One of the hash values of the diploma, revocation reason, it is also possible to set the revocation status to not-revoked, *Institution Sequence Number*, 🔒	OK /Error
Verify diploma	Read operation	Anybody	One of the hash values of the diploma or sequence number of the diploma on that smart contract	Both hash values of the diploma, diploma sequence number, revocation reason if revoked, number of entries for the diploma

Get detailed entry	Read operation	Anybody	Diploma sequence number, entry number	Entry of the diploma including status, revocation reason and date of the entry
Set key for adding diplomas	Write operation	Master admin of the Institution	Public key that should be authorized to add diplomas, *Institution Sequence Number* 🔒	OK /Error
Set key for revoking diplomas	Write operation	Master admin of the Institution	Public key that should be authorized to revoke diplomas, *Institution Sequence Number* 🔒	OK /Error
Set institution admin key*	Write operation	Admin with global admin key	Public key that should be authorized as Institution Master Key 🔒	OK /Error
Set global admin key*	Write operation	Admin with global master key	Public key that should be authorized as Global Admin Key 🔒	OK/Error
Set global master key*	Write operation	Admin with special master admin key	Public key that should be authorized as Global Master Key 🔒	OK/Error
List institutions*	Read operations	Anybody	Institution Sequence Number	Institution Name/Error
Destroy smart contract*	Write operation	Admin with special master admin key	🔒	OK/Error

* = functionality planned for future versions, not implemented in the prototype

Table 20: Smart contract functions

7.4.3 The RESTful-API for the smart contract

To access a smart contract of a blockchain requires access to a node of the blockchain. This node does not have to be under the control of the system and does not receive confidential information like private keys. The node receives transactions that are already signed. However, the node needs to be trustworthy enough to post the transactions received to the blockchain used and to reliably read from the blockchain. For this project a node was installed and continues to be maintained, but the use of blockchain nodes from third parties would be

possible as well. An Ethereum blockchain node offers a web3-API to read the blockchain, access smart contracts and send transactions [191, p. 3].

It is possible to directly access the web3-API of an Ethereum blockchain node via the browser and a Javascript library. However, this would have had two disadvantages. Creating a transaction requires the private key of the account that creates the transaction. Processing the private key in Javascript is possible but it is not secure. So, the Javascript library should not be used to add new transactions. This problem does not exist when reading transactions. However, when the verification combines the online database and the blockchain, this would complicate the verification web-app, that was programmed by an external service provider. However, a Javascript verification that only accesses a blockchain node is possible and could be added later.

To offer an easy RESTful-API to the online-verification, the online-verification was provided with an API built using the *Swagger* framework and Python [192]. This API could also be used by other universities in the future.

Although a smart contract can also be accessed through any node of the blockchain, the RESTful-API is more convenient to use for the web application and when writing to the blockchain.

The RESTful-API implemented the following functions:

- Diploma_add: adds a new diploma entry with two hashes
- Diploma_read: checks for a diploma with one of the hash values and extracts information about the diploma if one exists
- Diploma_update: revokes a diploma
- Diplomas: returns the list of diplomas
- Smartcontract: returns the address of the smart contract used for verification purposes

When a web interface or the student administration system perform blockchain writes, this must be signed by the respective private keys. This is checked by the smart contract. This creates two security risks:

a) The private keys might be abused to perform the operations for non-authorized certification or revocation of diplomas.

b) The private keys might be abused for other transactions that do not relate to the smart contract. This is particularly relevant if the blockchain used has relevant gas-fees for the transactions. In this case, the private key needs to hold enough cryptocurrency tokens to perform the transaction. These tokens could be transferred to a different account (“stolen”).

The API could just request the private key. However, this would also expose the private key to the layers above. The API should also not include the complete private key in its code. This would expose the private key to anybody who has access to the API source or object code. Let *privkey* be a private key. The API should include a function f_{key} that will generate *privkey* from a correct password

pass sent to the API. In case the correct password is not sent, it should return a value y that is different from the privkey:

$$f_{key}(x): \begin{Bmatrix} privkey\ for\ x = pass \\ y\ \neq\ \text{privkey for x}\ \neq \text{pass} \end{Bmatrix}$$

Since the API should support multiple private keys the function needs to be generalized for a number of n private keys.

$$f_{key}(x): \begin{Bmatrix} privkey_i\ for\ x = pass_i \\ y\ \notin\ \{privkey_i | i\ \in \{1 \dots n\}\}\ for\ x\ \notin \{pass_i | i\ \in \{1 \dots n\}\} \end{Bmatrix}$$

A simple method to generate such a function can be reached by splitting private keys into two parts and adding a passcode. Part$_1$ and the passcode from the pass. F stores the passcode and part$_2$. So, neither the API needs to store the complete private key nor does using the API require the knowledge of the complete private key.

Every key can also have a restricted IP range from which write requests are accepted. The API uses TLS. As further security against a replay attack, a challenge-response could be included and a timestamp to the passcode could be added. In such cases, the passcode would be hashed after the challenge or the passcode was added.

For the prototype phase this security feature was not implemented.

7.4.4 Integration in the future student administration system

The Geneva parliament enacted a law [193] that sponsors the University of Geneva to redesign digital services offered to its students. The verification of digital diplomas will be an integral part of this project. A proposal for an integration can be seen in Figure 29.

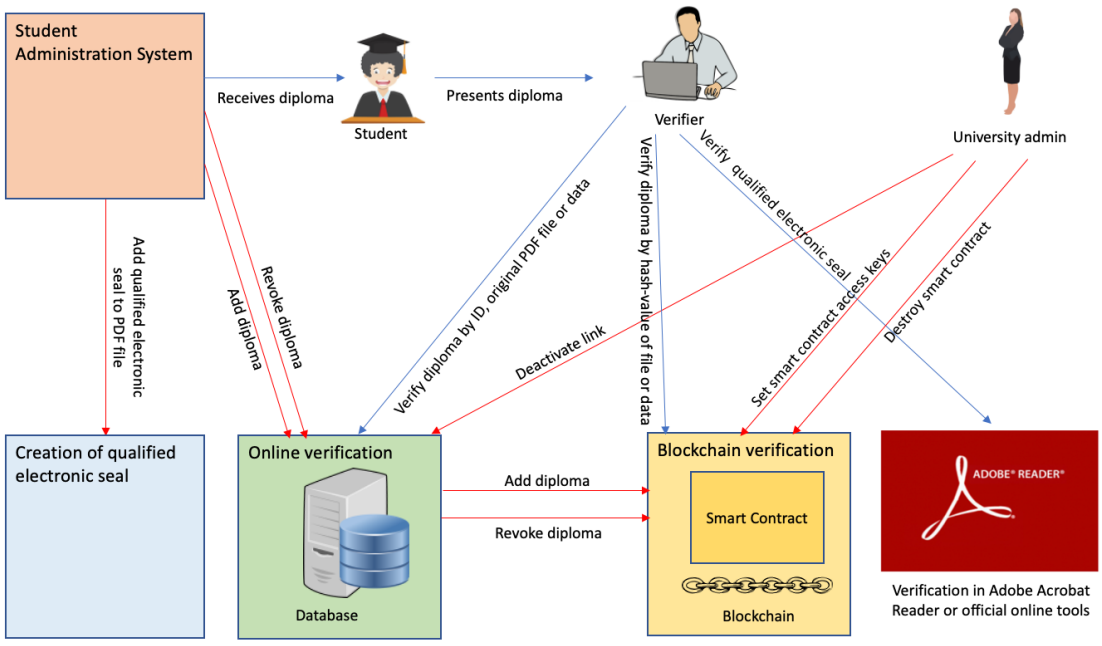


Figure 29: Proposal for the integration with the new student administration system

The online verification module could offer the functionality described in Table 21 for this integration. With the qualified electronic certificate for the creation of qualified electronic seals, a qualified electronic seal can be added to the PDF document. The private key of the qualified electronic certificate needs to be protected by special secure hardware like a smart card or a hardware security module. The seal creation process will be done inside that special hardware so that the private key will never leave that hardware. This can be either done locally or through a trusted service provide which acts a TTP and offers remote qualified electronic seals. For the creation of the qualified electronic seal, the user or service needs to authenticate. The proposed interface functionality is described in Table 22.

Function	Type	Called by	Parameters	Return
Add diploma	Internal API	Student Administration System	Diploma data, hash value of the diploma, 🔒	Diploma link / Error
Revoke diploma	Internal API	Student Administration System	Hash value of the diploma, revocation reason, 🔒	OK /Error
Deactivate link	Internal API	Administrator	ID of the diploma, 🔒	OK/Error
Verify diploma by hash	Public web interface and public API	Anybody	Hash value of the diploma.	Short version of the diploma, result of blockchain test / Error
Verify diploma by data, possibly through QR-code	Public web interface and public API	Anybody	Complete diploma data	Short version of the diploma, result of blockchain test / Error
Verify diploma by ID (only if activated by student)	Public web interface and public API	Anybody	ID of the diploma	Short version of diploma, result of blockchain test / Error

Table 21: Online verification module functions to add, revoke or verify a diploma

Function	Type	Called by	Parameters	Return
Add qualified electronic seal to PDF file	Local secure hardware module or remote service	Authorized persons or Student Administration System	PDF file, 🔒	PDF with qualified electronic seal / Error

Table 22: Interface to create a qualified electronic seal

Chapter 8 Evaluation and discussion

Evaluation is an integral and important part of design science research. *Vaishanvi* and *Kuechler* [17, pp. 159–171] describe seven patterns for evaluation:

The pattern **demonstration** applies a solution to a set of predefined situations. In the case of long-term revocable credentials, demonstrating that the prototype is capable of creating, validating and revoking credentials applies this pattern.

Evaluation can also be based on **experimentation**. Experimental data can be newly collected or collected from historic cases. The development of a prototype can also be regarded as the experiment – particularly when the development of the prototype produces insights that will already influence the further development of the prototype. For revocable long-term credentials neither historic data with the approach used nor data from the system is available. However, while building the system, important insights were gained. For example, the administrative burden to acquiring a certificate for the university to create qualified electronic seals was underestimated. On the other hand, the possibility to use a smart contract on blockchains proved difficult in the beginning when software libraries were still immature but reliable and straightforward at a later stage.

A **simulation** with test data is a standard technique in software development. All functions were tested with a set of test data. However, this only proves that the software works as planned. It does, however, provide little insight into the validity of the approach chosen.

An established evaluation **metric** or **benchmark** can be used to evaluate a design. Benchmarks focus on the performance of a system. Metrics can be quantitative and qualitative. Although some papers use evaluation metrics for the evaluation of system for the creation of long-term revocable digital credentials (section 4.1), none can be regarded as being established. A metric has been defined in section 4.2 to evaluate existing systems. The same metric should be applied to the framework designed.

Logical reasoning can be used to deduct the claims for assumptions using deduction rules. This is a comparable but weaker approach to a **mathematical proof**. Where claims regarding the framework are of a legal nature, this pattern could be applied as a form of legal reasoning. The application of the law to a specific case or type of problems is called *subsumption*. Legal reasoning follows rules that are called *logic* although they are different from the standard logic employed in mathematical contexts. Legal logic is non-monotonic. Adding new information to a theory can make a sentence underivable which used to be derivable on the basis of the theory without the added information [194, p. 43]. This would be considered a contradiction in standard logic. In law, a contradiction caused by new information does not void a legal argument or legal concept. Instead, it is the art of legal argumentation to deal with contradictions and to interpret a legal concept. This interpretation starts with the *wording*, the *context*

of legal rules and their *purpose* (teleological reduction). When a rule is absent that exists in somehow similar situations, the *analogy* argues that there is a gap that should be closed in a similar way. When the situation seems only similar but has important differences, the *argumentum e contrario* is used to argue in favor of a different treatment. When minor cases already justify a certain treatment, the *argumentum a maiore ad minus* is used to justify that a major case should at least be treated like the minor ones. These are only a selection of legal argumentation patterns [195, p. 651] that argue that a gap or a contradiction in the law should be solved by the extension or the restriction of existing rules – meaning by adding exceptions to the legal rule. Legal reasoning hence is not the mere application of existing legal rules to a specific case but includes shaping the rules of law in the context of the case. Reality can be much more complex than the law and it is a matter of justice to be able to adjust the law to new situations – of course in line with legal principles and fundamental rights. A *legal evaluation* of the framework therefore can only be considered similar to *logical reasoning*. However, important differences remain. In particular, the legal evaluation will help the interpretation of, in this case, data protection regulation of situations that might not have been taken into account when the data regulation was conceived.

The evaluation is structured as follows: It starts with a description of the tested use-cases with their results and learnings from the design and development phase. The evaluation compared to the requirements stated and the application of the metric defined in section 4.2 will provide an overview of the capabilities of the framework. Finally, the approach has been presented to different audiences such as university administrations, data protection experts, governments, academics, standards organizations and the blockchain community. Questions and arguments received by these groups are discussed in an approach similar to the logical reasoning approach described by *Vashnavi/Kuechler*.

8.1 Evaluation by testing

Testing is an integral part of software development. Tests, however, only verify that a software works according to its specification. Testing does not show that the specification provides a solution to the problem. The following tests have been performed:

- Loading of individual diplomas and a batch of diplomas
- Revocation of individual diplomas
- Verification of diplomas which have not been secured, which have been secured and diplomas which have been secured and revoked
- Verification of diplomas where hashes were only stored in the blockchain and of diplomas which were only registered in the database
- The following verification methods were tested: Verification of the original PDF using the online verification and direct verification using the smart contract on the blockchain. Verification of the data in the diploma using the

online verification and direct verification using the smart contract. Verification using the ID when the ID-verification was activated and when it was blocked.

- Since no qualified electronic seal was applied, the verification was not tested with a real qualified electronic seal. However, the verification of a qualified electronic signature was tested using Adobe Acrobat and using an official online validator [176].

All tests were successful, meaning that the verification succeeded in the cases it was meant to succeed and failed when it was supposed to fail.

8.2 Learnings from the design and development phase

Early tests in 2017 showed that accessing of Solidity smart contracts through available APIs at that time was not always stable. This largely improved later on. Also, security was a big issue. When keys for a testnet blockchain account were embedded in the Javascript/ECMAScript code of a publicly accessible website, the test-Ether was quickly stolen. Since it was only test-Ether this did not matter. However, it underscored the fact that weak security when using blockchains runs a high risk of being exploited.

The biggest learning was the experience in acquiring the certificate for issuing qualified electronic seals. A procedure designed for companies was particularly difficult for a university since there was no proper entry in the enterprise register. At the same time competences and procedures in the university were not clear and there was uncertainty regarding the risks associated with qualified electronic seals. Since a quick solution was not available, the qualified electronic seal was skipped when implementing the prototype. However, proper authentication is central to the trust in a digital certificate. The qualified electronic seal on every individual credential could – in theory – be replaced by a single qualified electronic seal for the smart contract address. This would reduce the number of qualified electronic seals to, for example, one per year. This, however, would remove the possibility to verify a credential directly in a PDF-viewer. The direct legal validity of a diploma that is confirmed by a smart contract with a qualified electronic seal also involves some uncertainty. Whether this approach would result in some cost-savings depends on the technology used to apply the qualified electronic seal. The costs and burden to receive the underlying certificate would not change. However, the costs for producing qualified electronic seals can be different for a solution that does not have to scale to a large number of seals per year. Fully automated systems require expensive *hardware security modules* (HSM) while a lower number could be generated using simple chip cards. Remote qualified electronic seals that are applied by a trusted service provider might also be a cheaper alternative for situations where only a low number of qualified electronic seals need to be applied.

8.3 Evaluation versus the requirements stated and metric defined

The proposed framework can be evaluated against the metric defined in section 4.2 to compare it against other systems. The result can be seen in Table 23. A more detailed picture can be obtained by an evaluation against the requirements defined in Chapter 5. The requirements have been separated into functional and non-functional requirements. Regarding the functional requirements, the creation, verification, and revocation of credentials were achieved. Some parts have not been incorporated in the prototype system but are included in the design. This relates to the integration of the credential integration into the student records administration system – in the case of university diplomas. The qualified electronic seal has not been added and governance functionality has only been partially implemented.

Regarding the non-functional requirements that have been translated into functional requirements, there have been functional requirements derived from the non-functional requirements security, governance, legal recognition and data protection:

The functional requirements derived from the non-functional requirement of security are fulfilled with the following exceptions:

- When the verification is limited to verifying the qualified electronic seal, a revocation of the credential cannot be detected. To check for revocations, a check against the online service or the blockchain directly is required.
- The verification of the qualified electronic seal will fail after the certificate that was used for the timestamp expires. Due to the fact that PAdES-LTA was used, the verification is still possible, but it will result in a warning message that can be ignored when the hash value of the document is confirmed by the smart contract. This could lead to some confusion when verifying old long-term credentials.
- The online verification is identified through the TLS and the URL. The smart contract address is not authenticated with the issuing institution. Since the credential PDF is signed with a qualified electronic seal, this could be negligible. However, it might not be obvious when using the blockchain smart contract that this is necessary. An option could be to link to a place where a document is stored that certifies the smart contract address and is signed with a qualified electronic seal of the institution. Since this is required only once, this document could even be stored on the blockchain in the smart contract itself.

While only basic governance functionality was implemented, the governance functionality should be implementable in a future production version. Concerning the official governance procedures regarding a certificate for creating qualified electronic seals, the prototype proved that this can be a lengthy process which should not be underestimated.

The direct legal recognition is dependent on the jurisdiction. A qualified electronic seal is recognized by the Swiss Law SCSE/ZertES [26] and the EU

eIDAS-regulation [23]. However, although both refer to the same technology, they refer to different chains of trust that are not reciprocally recognized. A SCSE/ZertES qualified electronic seal hence will only be recognized as an eIDAS advanced electronic seal and vice versa. The qualified electronic seal will be at most recognized only as an advanced electronic seal in case the certificate of the timestamp used is expired and the timestamp is not renewed before. As discussed in section 3.2, adding the timestamp of a credential to the smart contract should be able to preserve the direct legal validity. There might also be the possibility that the internal regulation of the issuing institution as well as the laws of the jurisdiction the institution is operating under, might prescribe the validity of a credential where the signature does not qualify as a qualified electronic seal.

The data protection requirements are met as stated in the requirements. The diploma is controlled by the student and revocations are only visible to those who have a copy of the diploma. The right to be forgotten is respected except for the revocation information. The revocation information stays available but only to those who are in the possession of the credential and therefore can be presumed to have a legitimate interest in knowing that the document that has been presented to them is no longer valid.

Criteria	Evaluation	Grading
Security	Bloxberg academic public permissioned blockchain	+
Proof of Authority	Regarding the qualified electronic seal (++), regarding the online verification (+), regarding the smart contract (0) since there is no established method to verify the authority of a smart contract. Publishing the public key of the smart contract on the website of the university or adding a qualified electronic seal to the smart contract address would help.	+
Durability	No other dependencies than safeguarding of the original file by the student and the operation of the Bloxberg blockchain (in case the university ceases to exist or loses the records)	+
Legal Recognition	Direct legal recognition only in the jurisdiction that provided the qualified electronic certificate for the creation of qualified electronic seals and a bit more limited legal recognition in many other jurisdictions.	+
Transparency	Transparent but complex architecture	+
Autonomy	Due to the combination of three techniques, the autonomy is well granted	++
Usability	Validation is simple, but multiple validation methods might lead to some confusion	+
Automation	Possible, API provided	++

Revocability	Revocation possible, not visible in the PDF document	+
Data Protection	Hash values without the credentials cannot be identified with the students. Together with unrevoked credentials, no further information than what is already contained in the credentials is available. Revocation information is available only to those with a legitimate reason to know	++
Integration	Possible, API provided, integration of qualified electronic seal depends on the solution chosen (card, HSM or remote signature/seal)	+
Governance	Extensive governance functionality potentially available	++
Economic viability	No costs per diploma if locally signed qualified electronic seals are used. If remote signature/seal is used, moderate costs per credential	+
Sustainability	Low carbon emissions per credential	++

Table 23: Evaluation of ECERT

8.4 Discussion with different audiences

The framework touches on many different aspects in a wide variety of subjects. Some are more practical, some are legal, some focus on technology, and some refer to ethics of privacy and informational self-determination. The author, therefore, went to relevant groups, spoke at conferences (three of them included a double-blind peer review process, five of them had published conference proceeding) even organized a proper conference on blockchain and GDPR, worked in standards organizations (with two pre-standards published) and published articles (three of them in high-ranking peer reviewed German legal journals). The author also contributed a chapter in a book. These activities enabled the author to receive the feedback to be discussed in this evaluation and are reported in this section. The following audiences were addressed with the following activities:

- To receive feedback from **university administrations**, the prototype was presented at the project group, in the context of the Séminaires d'innovation numérique *Digital Innovators* and also shown at the *Swiss University Continued Education* (Swissuni). The main questions here were the practical feasibility, the economic costs associated but also general questions regarding the sustainability of the blockchain based approach.
- The system was presented to **governments**. It was demonstrated at the Office cantonal des systèmes d'information et du numérique (OCSIN) and the approach was discussed at a meeting at the German Federal Ministry of Economic as well as at a meeting of the European Blockchain Observatory and Forum of the European Commission [196]. The main questions at the latter two addressed the compliance with data protection regulation and the right to be forgotten.

- The approach was discussed at **standards organizations** as the *International Telecommunications Union* (ITU) and the *Deutsches Institut für Normierung* (DIN). It is listed as a use-case GOV-006 [197] in the ITU *Focus Group on Distributed Ledger Technology* (FG-DLT). The approach was also discussed while drafting the standard DIN SPEC 4997, *Privacy by Blockchain Design* [168]. At the ITU the focus was existing hurdles to the adoption of blockchain based systems. At DIN the focus was again on GDPR compliance in combination with privacy enhancing technology.
- The approach was presented at **legal forums** like the IRIS-Conference in Salzburg 2018 [198] and 2019 [199], the EDV-Gerichtstag in Saarbrücken 2019, the Swiss Legal Tech Conference 2018 in Zurich, the conference *Datenschutz und Datensicherheit* DuD 2019 in Berlin, the 41st International Conference of Data Protection and Privacy Commissioners in Tirana, Albania 2019. To address the issue of *Blockchain and GDPR* the author organized a conference dedicated solely to this topic in Berlin in 2019 [200]. The legal community was also addressed by articles in major German legal journals like *Zeitschrift für Datenschutz* (ZD) [201], *Multimedia und Recht* (MMR) [202] and *European Data Protection Law Review* (EDPL) [203]. A chapter in a book called *data law in digitalization* was also contributed [204]. The article on Bitcoin and GDPR from 2017 [201] has been cited in the German legal literature that is available through the database Beck online in 25 commentaries and books as well as in 19 papers.
- The **computer science community** was addressed in peer-reviewed conferences at the GI-Jahrestagung Informatik 2019 in Kassel [205], the 35th Annual ACM Symposium on Applied Computing [206] and the 9th International Conference on Software Engineering and Service Science (ICSESS) [207]. The article on *Self-Sovereign Identity on Public Blockchains and the GDPR* [206] from January 2020 was referenced 19 times according to SSRN.
- The approach was also discussed at **internet governance** fora. The discussion took place at workshops organized by the author at the *Internet Governance Forum* (IGF) 2019 in Berlin, the *World Summit of Information Systems* (WSIS) 2019 and 2020 in Geneva and the EuroDIG conferences in the years 2018 to 2021. The approach was further discussed at the Swiss chapter of the Internet Society in 2019. The focus of these discussions was on empowering individuals and avoiding control by big private companies or governments.
- The **blockchain community** was addressed at the Geneva Blockchain Congress in 2019. The approach was also discussed at numerous blockchain conferences like the *Blockchain and Bitcoin Conference*, Geneva 2018, Blockstack *Decentralizing the World Tour*, Prague 2018, Blockchain Center Researcher PhD Meetup, Zurich 2019, the *Blockchain Hands On meetup*, Geneva 2019, at the *Conference on regulation and*

standardization in digital economy DLTReg 2019 in Moscow, the *Ural Forum* 2020 in Magnitogorsk, and the conference *Convergence* in Malaga in 2019. The approach was also presented to the Bloxberg consortium at the *Bloxberg Summit* in 2020 and 2021, the conference of the Bloxberg blockchain consortium. While the main topic there was the fear of creating an immutable blockchain system that would infringe data protection regulation there was also some discussion on the topic of self-sovereignty and the amount of user control.

The main questions and discussion are summarized and addressed below:

8.4.1 Is the system too complicated?

A system that uses three techniques is more complicated than other simple systems available employing only a single piece of technology. Particularly from university administrations this was asked together with the question, should the system replace paper diplomas or should it just supplement the current system? A simple system could be sufficient when durability does not matter since a paper backup is always available. Then a digital credential with limited use can be created by using only one of the three verification techniques employed. However, given the increased importance of digital credentials this corresponds only to a short-term vision.

8.4.2 Do we really need to use a blockchain?

Particularly from people in the German *Bundesamt für Sicherheit in der Informationstechnik* (BSI), the question was asked if there is a need for blockchain-based verification since a *Public Key Infrastructure* (PKI) has already been established. However, PKI has its weaknesses regarding revocation and long-term verification. As discussed in section 3.2, Sorge/Leicht [40] pointed out that creating a qualified electronic timestamp for one block of a blockchain automatically creates a qualified electronic timestamp for all documents referenced by hash values in this or previous blocks of that blockchain. Blockchain therefore can support long-term verification of qualified electronic signatures and seals.

Another issue of qualified electronic signatures/seals is the lack of global recognition. Even between the EU and Switzerland, qualified electronic signatures are not always recognized [208]. Decentralized ledgers add a layer of verification that is increasingly recognized by the law and will be part of the planned EU-eIDAS revision [149]. However, when systems use a blockchain as a black box without any possibility to directly verify the credentials towards the blockchain, this usage of blockchain technology does little to add security since the trust is limited to the online verification interface. In case of a stopped or manipulated verification service, the blockchain can only be used when the direct verification of credential against the blockchain is possible. In the design presented, the blockchain is the most important element to provide a durable means of verification that is independent from the issuing institution. The role of the blockchain, however, could be replaced by a central entity that warrants long-term credentials. In some countries – such as China (China Academic Degrees

and Graduate Education Development Center – CDGDC [209]) – institutions for the central verification of academic titles exist. However, neither the reliance on the issuing institution nor a central institution achieve the same durability as a distributed system. For this benefit to be accessible, the blockchain needs to be easily directly accessible.

8.4.3 Do we really need a qualified electronic seal?

Some blockchain enthusiasts would like to do everything without involving government-controlled institutions. However, credentials are only trusted because the issuers of the credentials are identified and sometimes even accredited or certified. Unless the system introduces a superior model of trust chains, it is advisable to base a system on the already established public key infrastructure. It has the advantage of being recognized by law, even when this includes only a limited number of jurisdictions.

8.4.4 Could the qualified electronic seal be attacked?

A qualified electronic seal uses the same technology as a qualified electronic signature that has the same legal value as a handwritten signature. While a number of attacks on X.509 certificates for TLS are known [210], successful attacks on qualified electronic certificates are less common. In 2018, some attacks that did not break the encryption but circumvented the encryption were discovered [211]: The *Universal Signature Forgery* (USF) attack disables signature verification while still displaying some signature information. The *Incremental Saving Attack* (ISA) is based on the possibility to incrementally save a document in such a way that some content is not covered by the qualified electronic signature. Finally, the *Signature Wrapping Attack* (SWA) relies on the fact that the part of the document that stores the signature must not be included in the signature verification. 20 of 22 PDF readers were vulnerable using at least one attack method. One showed limited attack success and one reader did not show any vulnerability. More recently, a new set of attacks were shown that were related to certified but not signed documents [212]. Certified documents can still allow some modifications like filling in forms. Most future vulnerabilities should be able to be fixed through updated PDF viewers or signature verification.

In addition to these technological risks, qualified electronic seals could be abused by people that have access to it. For example, a university administration could sell fake diplomas or the qualified certificate to generate qualified electronic seals on doctored credentials. Compared to a manual seal, the qualified certificate has additional protection through a password. However, an insider attack at the trust service provider or at the university remains possible. An attack on a qualified electronic seal might be discovered when comparing it to the blockchain or the online verification: Documents with qualified electronic seals that do not verify against the smart contract or the online verification have a high risk of detection. Insider attacks, however, might not be limited to one technology but include all three verification technologies. The blockchain entry, however, would indicate an unusually high number of credentials that have been issued by an institution. Large scale abuses could be detected this way.

8.4.5 Could the blockchain entry be manipulated or attacked?

University administrations asked about the possibility of manipulating or attacking the blockchain verification. A blockchain entry is exposed to three main risks:

- The private key of the university could be stolen or abused to create faulty entries. This risk can be minimized when private keys are known to as few people as possible.
- A copy of the smart contract could be written to the blockchain by an attacker. The copy is then controlled by the attacker. Since smart contracts are public, this cannot be prevented. An attacker could also print the manipulated smart contract address on a fake diploma. However, this fake diploma would not have a valid qualified electronic seal of the university.
- The blockchain used could be hacked. If the hacking refers only to the consensus mechanism, some blockchain entry might be removed or the date of the entries might be substantially wrong. Entries could still not be forged, but revocation information could be removed.

To summarize, a successful attack on the blockchain used could delete credential verification or revocation but could not create fake ones. An attack on the private key of the issuing institution could verify fake credentials. Proper surveillance of the system can reduce that risk and revoke fake credentials. The combination of three techniques makes it highly unlikely that all three methods are hacked from the outside.

8.4.6 Could the online verification be attacked or forged?

The web application could be hacked and then indicate success while verifying invalid diplomas. An exploit could be used to attack the web application and fake a credential including the answer from the smart contract. Another attack could be imagined by creating a fake copy of the web application placed on a server under a similar domain. Instead of typing the URL a link could be provided, for example, in an email. Like other phishing attacks this cannot be completely avoided. However, the successfully verified diplomas will neither have a valid qualified electronic seal nor can they be verified directly using the smart contract on the blockchain.

8.4.7 What happens if the cryptographic hash functions become insecure?

In the context of the immutability of distributed ledgers, the question of long-term security of cryptography – particularly of cryptographic hash functions is questioned. Cryptographic hash functions result in a practically unique value for every different document hashed. It is neither possible to reconstruct the document from the hash value nor to generate a second document with the same hash value (collision attack). A successful collision attack would enable attackers to create a fake diploma for an existing qualified electronic seal or an existing blockchain entry. Given the widespread use of hash functions, a successful collision attack on common hash functions would create a large impact. In the past, some hash functions were thought to be secure and later turned out not to

be secure [213]. Even worse, current hash functions are known to be breakable by very large quantum computers [214]. However, even then the complexity of the hash function employed is only reduced to 50% of its current length. Therefore, the cryptographic hash functions used should even hold against quantum computers for some time. Asymmetric encryption used for qualified electronic seals, however, is more vulnerable. Current algorithms might need to be replaced by post-quantum algorithms. However, standardization of post-quantum cryptography is not done yet [215]. Employing non-standard cryptography would run the risk of lack of verification tools in the future which could be worse than using current algorithms with known weaknesses towards very large quantum computers.

All three verification elements use state-of-the-art security tools and therefore provide a high level of security. However, given the long duration of preserving the diploma, serious security issues with the technology used cannot be excluded and the governance needs to consider such issues.

8.4.8 Does the GDPR apply to credentials issued in Switzerland?

When the University of Geneva issues credentials, four different legal data protection regimes could govern this process: the Geneva LIPAD [69], the Swiss FADP (DSG/LPG/LPD) [66] which is currently being revised, the European GDPR [64] and the Convention 108+ [216] that Switzerland has signed but not yet ratified. Since the University of Geneva is a public entity of the canton of Geneva, the federal data protection law FADP does not apply (Article 2.1 FADP), but the LIPAD is applicable. The convention 108+ only obliges member states to implement the rules in their own law (Article 4). GDPR as an EU regulation was also adopted in the *European Economic Area* (EEA) [217] to which Switzerland is not a member either. GDPR even applies when data processing is happening outside of the EEA, where GDPR is not directly applicable. Article 3 GDPR defines the territorial scope where the GDPR is to be applied. GDPR applies, particularly, when a controller or a processor is located in the EEA or when services are offered to data subjects in the EEA. When, for example, blockchain nodes are located in the EEA or educational services are offered online to people in France, GDPR might therefore be applicable. Since miners, block producers (the equivalent to miners in non-PoW blockchains) or node operators might be regarded as processors [218, p. 3] and classes might be offered online, both, LIPAD and GDPR might apply.

8.4.9 Is the hash value written on the blockchain personal data?

The immutability and distributed nature of blockchains is a frequent topic in the data protection community when blockchains are discussed. Data protection requirements have been discussed generally in the requirements in section 5.3.4. Still, the idea of some data being permanently stored without having somebody clearly accountable for it that can delete this data is hard to accept for the data protection community. However, to what data does GDPR apply? Is a cryptographic hash value of some personal data on a blockchain considered personal data? This is relevant, because GDPR is only applicable to personal

and not to anonymized data. At least this is stated in Article 2.1 and Recital 26 of the GDPR and generally agreed on [219, p. 188]. Only the German data protection authority decided otherwise in a case where a federal ministry was fighting in courts not to publish an anonymized expert report [220, p. 18]. The reason given for this decision is not convincing: Data protection rights of data subjects do not exist related to anonymous data even when this has been generated from personal data. There is no *fruit of the poisonous tree doctrine* which extends data protection rights to anonymous data [221].

When some data is considered personal data, GDPR might be applicable, and the processing is forbidden unless a specific justification exists. Even when there is a justification for processing personal data, GDPR comes with many obligations [222, Paras. 56–58] that might be difficult to meet when using a blockchain [223, pp. 1434–1435]. Therefore, it is recommended that personal data should not be written on an immutable blockchain [196, p. 5]. A credential containing the name of the credential holder and the type of credential is clearly personal data.

However, is the hash value of a diploma personal data itself? A report of the *Article 29 Data Protection Working Party* (WP29) – the predecessor of the *European Data Protection Board* (EDPB) considered hash values of personal data only to be pseudonymized data [224, pp. 20–21] which is not anonymized and hence still personal data. However, this report only mentioned a case where hashing was used for pseudonymizing data by replacing names with hash values. Using the analysis of this document, three risks to anonymization need to be considered, *singling out*, *linkability* and *inference* [224, p. 21]. *Singling out* means to “identify an individual in a dataset”. *Linkability* means to “link two records concerning the same data subject”, so when the person behind one record is known, the other record can be identified with the same person. *Inference* means the “possibility to deduce [information] with significant probability”. Under certain conditions like enough entropy and secure deletion of the original personal data, all of these risks can be excluded. Therefore it needs to be asked whether the analysis of WP29 must be generalized to a broader range of use-cases of cryptographic hashes of personal data [202, pp. 657–658]. The European Court of Justice decided in *Breyer* [225] that IP addresses can be personal data. The court decided this way, since the IP address identifies the provider, and the provider is under some circumstances allowed and obliged to identify who used that IP address at a specific time. A log entry of a web server that contains the IP address of a request is therefore considered personal data. It is not completely clear if the European Court of Justice can be read that way that in case this identification is not legally possible, the IP address would not be considered personal data [225, Para. 49]. There are also many IP-addresses that are clearly not considered personal data, like 127.0.0.1 the IP address that means *localhost* and always means the computer it is being used on. Even when an IP address or some other ID can be identified with a person, Article 4 nr. 1 GDPR requires not only the existence of some data but also of *information* to consider some data to be personal data. Pure random noise is data but does not contain information.

Does this mean data without information is not considered personal data even when it can be identified with a natural person? When an IP address is listed in a web server log, this information is clearly connected to the log entry so that the log entry can be identified with the person that used that IP address. In fact, this is frequently being used in Germany to prove copyright infringement [226]. A book with all possible IPv4 addresses, however, wouldn't be a very sensitive collection of personal data, but rather a boring possibly sequential list of numbers from 0.0.0.0 to 255.255.255.255. Only the connection of information about what has been done on the website, the IP address and the legal and not only theoretical possibility to identify the user behind the IP address renders the IP address sensitive personal data. As defined in Article 4 nr. 1 GDPR, *personal data* means any *information* relating to an identified or identifiable natural person. Therefore it can be concluded that without information there is no personal data [202, p. 658]. The information, however, does not have to be explicit; it can also be inferable by the context of the data. Having a book with *all* IP addresses does not provide a specific context. Having a book with all IP addresses that visited a specific website, however, would provide that context.

When a hash value of a credential is registered with the smart contract, the hash value is written to the blockchain. Can that hash value be identified with a natural person, e.g., the credential holder? Actually, it can. Everyone that has a copy of the credential can calculate the hash value and see that the credential is valid. This is exactly what the hash value is written for on the blockchain. Hash values have, for example, been discussed in the context of Facebook *custom audiences* (Figure 30) where an advertising company sends a list of hash values calculated from email addresses to Facebook so that Facebook can select the customers that are also Facebook users [227, pp. 681–682]. These hash values are personal data because of two reasons: First, they are used to identify Facebook users that are customers of the advertising company. So, their very purpose is to identify persons in a specific context. Second, the entropy of a hash value of a short email-address is rather small, so that hash values of email addresses can often be reversed by *brute force* which means by intensive guessing. As discussed above, the identification with a natural person alone, does not suffice. It also has to be connected to some information. This information does not have to be explicit but can be a context which will enable some information relating to a natural person to be derived [202, p. 656]. In the case of Facebook's custom audience if a customer of the advertising company is a client, the hash value conveys this information and Facebook is also able to identify the customer in its user-base. If a customer of the advertising company is not a Facebook user, the hash value would not directly convey any information to Facebook. The hash values would only convey information to the advertising company that could use the information that was hashed to re-identify it with the same information necessary to calculate the hash values. This would be a case where no information would be conveyed by the hash values. However, since the entropy of email addresses is quite low, brute force allows the cryptographic hash function to be reversed and the hashed email addresses to be determined.

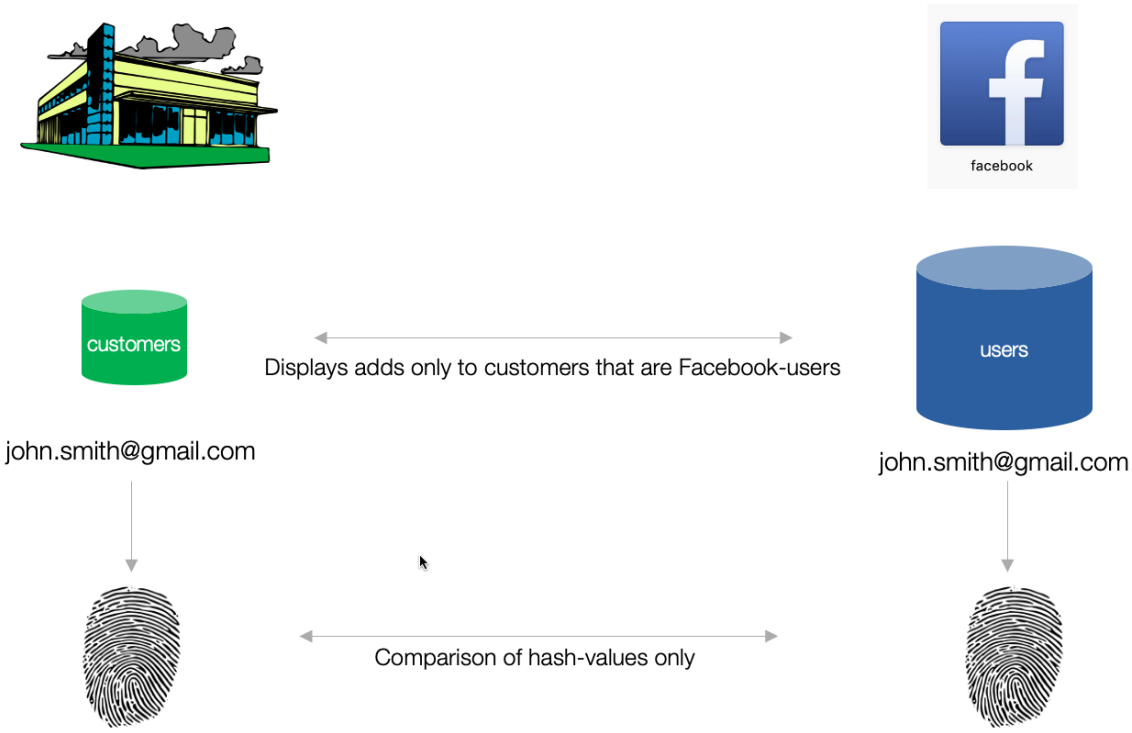


Figure 30: Schematic functioning of Facebook custom audience

When looking at hash values calculated from credentials, these will not directly convey any other information than the information that is in the credential. When written on the blockchain by the issuing institution, the hash value confirms that the credential is authentic, and the absence of the hash value would state that it is not authentic. However, the qualified electronic seal applied to the credential already conveys the same information. As a result, the hash value on the blockchain does only convey some information relating to a natural person to those who already have this information. This can be compared to an echo, which processes personal data when used with personal data, but does not store any personal information. As a result, the pure hash values stored in the smart contract should not be considered personal data.

This could raise the question as to whether the situation should be regarded differently should the credential not carry a qualified electronic seal. In this case, a tiny, but important bit of information is conveyed: The data about the authenticity. When compared to the analogue world, verifying a paper credential by analyzing the paper or ink could always be done. Verifying a digital credential using some external checksum (the hash value) might be seen as an integrative part of the credential itself even when that checksum is stored externally. Therefore, it could possibly be argued that external information that only allows the detection of manipulations to an electronic document should not be regarded as conveying additional information.

The Spanish data protection authority agencia española protección datos (aepd) and the data protection authority for the EU administration *European Data Protection Supervisor* (EDPS) jointly authored a paper on the *hash function as a personal data pseudonymization technique* [228]. This paper points to the risk of the use of cryptographic hash values as *pseudoidentifiers* [228, p. 14]. This can be avoided, when the specific credential and not some general identifier is used to calculate the hash values. To differentiate between anonymization and pseudonymization, the data protection authorities also mention the importance of what information is linked to the hash value [228, p. 21]. In the case of a certified credential, no other information is linked to the hash value. This renders the hash value on the blockchain anonymous.

However, when a credential is being revoked, this information, together with a category of the reason for the revocation is added. This, clearly, is no information that has been present or has somehow already been connected to the credential. So, the added revocation information renders the hash values personal data. The key to identify this data with the holder of the credential is the credential itself which serves as a means to calculate the hash values. This means that with access to the credential, there is additional information – the revocation information – that can be identified with the credential holder. Information that can be identified with a natural person is the broad definition of personal data in Article 4 nr. 1 GDPR even when this requires additional information – in this case the credential.

To sum up, the hash value of a non-revoked credential can only be identified if somebody already has the credential. Since there is no additional information or context stored on the blockchain, the hash value should arguably not be considered personal data. In case of revocation, however, the entry needs to be considered personal data.

8.4.10 Can credential holders be identified with blockchain accounts?

Most blockchains do not actively manage accounts, but participants can pick any random private key. The private key allows the public key [229] to be calculated. The public key, also called *address* has the function of an account number. Some permissioned blockchains require identification and authorization before new accounts can perform transactions. Bloxberg, being based on Ethereum, does not require this, and requires only having some native currency called *Bergs* to execute transactions. Bergs can be transferred from existing accounts or a *faucet* that distributes a small amount of Bergs to any address for free [230]. For Bloxberg, Bergs “pay” the “gas” for transactions but are not supposed to have value. The Bergs would have to be “paid” by the credential issuing institutions when sending new hashes to the smart contract. Since the number of Bergs required is small and Bergs are available for free, this should not be an issue. Holding or verifying credentials does not require Bergs. For cryptocurrencies that are traded at exchanges, people behind blockchain accounts can often be identified [201, p. 562]. The private key is not shared with anybody, and therefore is not processed by anybody else. However, since the private key allows the public key to be calculated, from a data protection point of view, both might be

able to identify natural persons using an account and therefore might be considered personal data [231, p. 5]. Since Bloxberg Bergs are not traded at any exchange, the risk of being identifiable are lower. In case of the framework proposed, accounts are only used by the credential issuing institutions, not the credential holders. The identification of these accounts with the institutions is desired. Credential holders do not need accounts for their credentials. Therefore, in the framework proposed, credential holders cannot be identified with blockchain accounts.

8.4.11 Is the right to be forgotten respected?

The right to erasure and the right to be forgotten (Article 17 GDPR) oblige the controller to delete personal data on request of the data subject. Even without a request by the data subject, data without a proper justification to be stored needs to be deleted. For example, consent can be withdrawn, or processing based on legitimate interest can be countered by an objection by the data subject. However, if there is a remaining compelling interest, the data subject cannot demand the erasure of the data.

The first question is, is there personal data relating to the data subject requesting deletion? If there is no personal data, there is no right to erasure/right to be forgotten. If there is personal data, it has to be verified, if there is a remaining justification to continue to store the data. Only if there is no remaining justification, must the data in question be deleted. In the latter case this requires answering what constitutes *deletion* in the context of credentials and cryptographic hash values.

A credential issuer might store different records relating to the credential holders. Records stored off-chain in conventional systems can be deleted easily. The following discussion, however, will focus only on data stored on the blockchain, because only this data is very difficult to delete. In case of a credential without revocation, the cryptographic hash value on the blockchain arguably does not constitute personal data (see 8.4.9). However, in case of a revocation the entries on the blockchain must be considered personal data.

In case the data stored on the blockchain needs to be considered personal data, it has to be asked whether there is a right to erasure concerning this data. The evaluation of this question depends on the specific use-case of the credential. What has been the basis for the processing of personal data in the first place? Does this original justification still exist? For example, if the original justification was consent, the consent could have been withdrawn. However, it must also be evaluated whether there are compelling legitimate grounds or legal obligations to keep the data. In case of revocations there might be a duty to protect others from deceit with a revoked credential.

There is an open discussion as to what should be considered *deletion* or *equivalent to deletion*. The French data protection authority CNIL considers only *perfectly hiding* information to be equivalent to deletion [232, p. 5], the Austrian data protection authority Datenschutzbehörde recognizes information that cannot be accessed without disproportionate effort as deleted [72, Pt. D.2]. *Finck*

mentions that several national data protection authorities recognize deletion that is not destruction but has doubts regarding the *European Court of Justice* (ECJ) [233, p. 76]. In its *Nowak*-decision, the court refers to destruction when talking about deletion [234, Para. 55]. However, that case refers to physical copies of a hand-written exam. While there is agreement that paper files can only be deleted through destruction the ECJ neither offered any insights or argumentation on this nor did it offer any indication that the equation of deletion and destruction regarding paper copies should be extended to electronic data. Even the term *destruction* does not make much sense for the digital world when single records are to be deleted. *Taeger/Gabel* consider that strictly non-reversible anonymization is not required, since factual deletion already suffices for anonymity [235, Paras. 100–101].

The French data protection authority CNIL advocates for storing only a cryptographic commitment of the data on a blockchain. A perfectly hiding commitment scheme would ensure that, upon erasure of the witness and the data committed, it would no longer be possible to prove or verify which information has been committed [232, p. 5]. A hash value with a key (otherwise called *pepper*) could also be used. At first sight, the protection using a separate key sounds like a good idea. However, the key would be always required when verifying the credential. Therefore, it would have to be included in the credential. Having to type an additional key that is included in the credential would only establish a usability barrier. The proposed framework therefore does not use an additional key but uses the credential as the key. However, it is important that the credential has enough entropy which eliminates the risk to guess it through brute force. In the case of a scan, the entropy is very high. In case of a generated PDF, it is important to include a *salt* value to ensure sufficient entropy. As another alternative CNIL also proposes to store data as cyphertext. Storing encrypted data on a blockchain, however, is problematic as discussed in the *BCdiploma* approach (section 4.3.7.5). It can be compared to a password protected system where the password cannot be changed.

If the credential has been deleted, it is not possible to link the hash value to a credential or a person. If the credential has already been disclosed to somebody, this person can identify the hash value with the credential when she verifies the credential. As long as there if no information on the blockchain that is not already contained in the credential, the hash value still is arguably not personal data (see section 8.4.9). However, in case the credential has been revoked but has been communicated before, the information about the revocation is still accessible to those the credential has been communicated to. Does the right to be forgotten include the right to remove the revocation notice? Here we have to distinguish three scenarios:

a) The credential holder has not given a copy of the credential to anyone and has destroyed her own copy. In this case, there is no legitimate reason to keep the revocation information. However, in this case, the revocation information on the blockchain cannot be identified with the credential

holder. The revocation information has been anonymized by deleting all copies of the credential.

b) The credential holder still owns a copy of the credential. In this case, there might be a compelling legitimate reason or even a legal obligation to protect others from abuse of the now revoked credential by retaining the revocation notice.

c) The credential holder has deleted all her copies, but copies of the credential have been sent to others. For example, former employers might discover that the credential has been revoked after the credential holder has left the company. If employers legally preserve a copy of the digital credential, there might also be a right to verify them including the information about ex tunc revocations.

As discussed in section 5.3.4, there is a justification to convey the revocation information to those who have access to the revoked credential which otherwise would give a wrong impression. The holder of the credential has no right to ask for the deletion of the revocation notice without deleting the credential. If somebody still has a copy of the credential, the right to be forgotten might apply to the credential and, for example, an applicant for a job could ask an employer to delete the copy of the credential the employer has received. This deletion would then remove any access to an existing or future revocation notice. Therefore, the right to be forgotten is respected when looking at the complete credential.

8.4.12 Can blockchains comply with data protection by design and data minimization?

The GDPR requires data protection by design (Art. 25 GDPR). Data protection by design includes data minimization. Art 5.1.e GDPR also requires *storage limitation*. Although, at first sight, the publicly accessible smart contract storing the immutable revocation notice on the blockchain seems to violate these GDPR principles [236, p. 424], it is a highly optimized implementation of privacy by design. Although autonomous, it can be revoked, and the revocation cannot be separated from the credential. Although immutable, the deletion of the credential will render the entry on the blockchain anonymous noise. Further elaboration on this topic can be found in *DIN SPEC 4997 Data Protection by Blockchain Design* [168].

8.4.13 Shouldn’t the revocation information be stored off-chain?

The revocation information could be stored off-chain. While this sounds well suited to comply with the right to be forgotten, it has some problematic consequences: The availability of off-chain data is not warranted. In case the revocation data is missing or has been manipulated, a revoked credential might still look valid and as not being revoked. The right to be forgotten, however, cannot be interpreted in a way that the credential can still be presented and only the revocation should be forgotten. This situation would rather impact the GDPR obligation of data accuracy. It would also impact credentials which have not been

revoked but which would lose trust, since it is not clear if a revocation notice has been lost. Therefore, the revocation notice should be stored in a similar way to the hash value used for verification – as this is done in the proposed framework.

8.4.14 Is the right to rectification respected?

GDPR also offers a right to rectification (Article 16 GDPR). Suppose a credential has been revoked in error, the proposed framework allows that error to be corrected and the credential to be reinstated. The verification will not directly show a trace of this correction. However, when closely inspecting the blockchain, it is possible to see that there has been a correction. This information is technically not erasable. Does the right to rectification include the right to have all traces of the wrong data erased? Article 16 GDPR mentions a supplementary statement. This is an indication that a complete eradication of all traces of the error is not a requirement for the rectification. *Finck* and *Herbst* confirm this interpretation that a mere supplementation should be considered sufficient [233, p. 73][237, Para. 29]. When verifying a credential, only the rectified information will be visible. The traces of the incorrect information are only visible by close inspection. This should be considered adequate to comply with Article 16 GDPR.

8.4.15 Should a redactable blockchain be used?

There are concepts of redactable blockchain that could be corrected by removing some information:

A blockchain could be built with chameleon hashes [238] that comprise a trap-door that allows to replace the content that a hash value refers to. With a special key, a second content could be created that will result in the same hash value. This approach, however, means giving up on decentralization. It would create a superuser that can replace content at will.

Another option would be to remove content that is no longer accurate from a blockchain. This procedure called *pruning* has already been included in the original Bitcoin paper [29, p. 4]. It can save storage space and could remove old data that is not used anymore. However, pruning replaces transparency of the past with trust in the parties involved. That is the reason why Bitcoin can be used with lightweight nodes that have old transactions removed, but as Nakamoto already wrote in 2008, this could render the system more vulnerable [29, p. 5].

Near-immutability of blockchains is not an accident. It is a feature that has been paid for with a high price. When immutability is not needed, blockchains should not be used. When limited immutability is required, a blockchain could be built to offer exactly that. For example, a book-keeping blockchain could be built to store all records for 10 years and then delete them. In the context of long-term revokable credentials, the possibility to revoke or reinstate a credential exposes credential holders to the risk of manipulation. Refugees could risk having their credentials revoked by their country of origin. Doctored credentials that were revoked could be reinstated by a regime. Having a trace on the system will offer transparency as to when a transaction was performed and protects credential-holders and credential-verifiers against manipulation attempts. Therefore, in this

use-case, rectification without a trace is not desirable and would not best protect fundamental rights and interests of data subjects. Directly showing only the current version but leaving a detectible trace seems to be the better way to balance interests involved.

8.4.16 How to deal with lack of clear accountability in distributed ledgers

Some scholars claim that distributed ledger technology is *profoundly incompatible at a conceptual level with GDPR* [239, pp. 17, 28]. One of the principles in Article 5 GDPR is accountability. The accountability of a permissionless blockchain is difficult to determine. Under GDPR, *controllers* are accountable (see the discussion in section 5.3.4). Several people or entities can be controllers at the same time. If two or more controllers jointly determine purpose and means of the data processing, they can be *joint controllers* and face additional obligations. It is difficult to determine the controllers of a blockchain. All node operators receive, store and possibly send the information stored on a blockchain. Some authors, therefore, suggest that all node operators of a permissionless blockchain should be considered controllers [240, p. 732] [223, p. 1433]. However, node operators and even miners – when they do not collide – cannot influence transactions. That is one of the main design achievements of blockchain technology [201, p. 563]. As discussed in 3.4 controllers determine the purpose and means of a blockchain or a transaction [218, p. 2]. Therefore it would not be fair to levy GDPR's obligation on them that they could not fulfill since they do not have sufficient control [241, p. 6]. In peer-to-peer systems like blockchains, participating data subjects risk being faced with obligations as controllers [242, p. 59]. *Janicki/Saive* consider that purely automatic processing that is done by a computer that cannot be attributed to a natural person, is not subject to GDPR [243]. *Teperdjian* suggests to *exclude more decentralized blockchain systems from the GDPR in whole or in part* [242, p. 35].

The French data protection authority CNIL takes a more nuanced approach. Only if a group of actors jointly decide to process data with a blockchain, could they be considered joint controllers [218, p. 2]. A consortium blockchain might meet that description. Other actors could be considered controllers as well: The French data protection authority CNIL suggests that an entity that carries out transactions on a blockchain could be a controller [218, p. 1] (similar [201, p. 564]). *Tatar et al.* suggest designating an entity as controller [241, p. 7]. However, GDPR only offers the possibility to designate a controller by Union or member state law (Article 4 nr. 9 GDPR). Some authors suggest that GDPR does not fit well for distributed systems, e.g. [242, p. 59] [244, p. 170] [245, p. 1227]. Regarding the aspect of determining the controller, *Finck* only sees a lack of legal certainty [233, p. 96], but claims that GDPR is sufficiently technology-neutral [233, p. 98]. Others see GDPR fit only for centralized data processing and question technologic neutrality [246, p. 35]. *De Rosnay* suggests that *this distribution of actors and actions requires a rethinking of legal categories* [247, p. 4]. Considering participating individuals as controllers might impede on their right to association or privacy. *Pesch/Sillaber* are concerned that a de facto ban would not only impact fundamental rights of trade or profession, the freedom of

association, or the freedom of expression and information, but also would not be practically enforceable [244, p. 171].

A blockchain often serves many applications. The rules on a blockchain for these applications are programmed in smart contracts. The people signing and sending transactions have control over their own transactions but not over the smart contract they use or the blockchain as a whole. This suggests differentiating these three levels of control: Control over the blockchain, over a smart contract (if used) and over a single transaction [203, p. 431]. While permissionless blockchains might not have a controller on the blockchain level, it is hard to imagine a transaction that will not have a controller on at least one of the three levels. Also, the rules for the processing by the nodes are fixed in advance and everybody sending a transaction is in almost full control of the outcome. A transaction sent to a blockchain cannot be tampered with by a node. The only uncertainty for the transacting party is, whether and when it will be put in a block, particularly when the number of transactions is high. Therefore, there is no real lack of accountability.

So, the three levels should be discussed separately:

- Regarding the blockchain level, permissionless Ethereum might not have a controller. Bloxberg, however, is a permissioned consortium blockchain. Members can be identified and regularly meet to agree on the purpose and to govern the blockchain. Some voting mechanisms are on-chain and some off-chain. The consortium also has the power to patch or fork the Bloxberg blockchain. Who should then be considered the controller? Should all consortium members be considered joint controllers, or only those actively mining? Or should only the *Iron Throne*, the institution that is administrating the consortium be considered a controller? *Spindler* suggests that the power to attribute rights does not directly influence the processing [240, p. 732]. However, the power to select actors that verify blocks, or vote is the ultimate control in a consortium blockchain. It can even be used to alter existing data on the chain. At *Bloxberg*, however, the Iron Throne does not decide on who is a voting member, but the members directly vote on that on-chain. Should this voting constitute a reason to consider them joint controllers? To reduce uncertainties and minimize liability, it is suggested to create a legal entity for the consortium which should be a natural candidate for a data protection authority when determining a controller. A legal entity could bear some of the responsibility that would otherwise be distributed to all Bloxberg members.
- The smart contract on the blockchain controls what transactions are possible. Smart contracts can be anonymous and immutable or might include administrative functionality that allows administrators, among others, to replace the code or block transactions. The long-term credential smart contract includes the possibility to attribute or remove rights to certify or revoke long-term credentials. It also includes the possibility to destroy the smart contract. As long as the University of Geneva maintains the

smart contract, it could be regarded as a controller on the smart contract level.

- Institutions certifying or revoking credentials are doing this by sending transactions. Only they control which academic titles or other certificates can be verified as long-term digital credentials. Credential holders and credential verifiers do not send transactions to the smart contract. They can send queries, but they will not alter data on the blockchain.

This suggests that the Bloxberg consortium is controller for the Bloxberg blockchain. The University of Geneva controls the smart contract and individual universities control the certification and revocation of credentials. However, are these three controllers *joint controllers*? Do they jointly determine the purpose and means of the processing (Article 26.1 GDPR)? Or do some of them process the data on behalf of the other one or the other two (Article 28.1 GDPR) and should they be considered processors?

The *European Court of Justice* (ECJ) had to decide on the complex scenario of a company homepage integrated in social media. So-called *fan pages* are edited by companies that are customers of *Facebook*. Facebook uses the information gained when people visit the fan page of the company to build profiles, place ads and improve their system. Facebook has much more control than the company. However the court found that because the administrator of the company can define the criteria and dimensions of the statistics like age, sex, relationship status or occupation, there is a sufficient contribution to the definition of purposes and means to consider the company a joint controller [248, Sec. 37]. Later on, the ECJ clarified in the *Fashion ID* case, that embedding a button that sends data to Facebook even if not pressed, does present a joint control on the processing of this data. However, the liability is *limited to the processing of the personal data in respect of which the joint-controller determines the purposes and means* [249, Para. 85]. The ECJ therefore has recognized that joint control is not a monolithic concept, but liability is limited to areas where a controller can directly or indirectly influence purposes and means of the data processing.

In case of consortiums working together, joint-control or in some cases also a controller-processor relationship seems to be adequate. In case of different universities using only the common protocol of a permissionless system, actors should be regarded as independent controllers. Regarding long-term credentials, the main control seems to be at the issuing institutions. Depending on the contractual arrangements, other Bloxberg members or a future Bloxberg association might be deemed processors regarding credentials issued by other institutions.

When accountability is not centralized, exercising rights might be more difficult for data subjects. However, when comparing the situation for the data subject as a holder of an academic title, neither the Chinese solution of a central repository [209] nor losing titles in case of a disappearing institution is preferable. When a blockchain can better protect the rights and privacy of the data subjects, GDPR

and its principles should be interpreted in a way that does not block the use of distributed solutions.

8.4.17 Other GDPR obligations of controllers

Besides the right to be forgotten (right to erasure) and the right to rectification GDPR offers a range of rights to the data subject and obligations to the controller (see 3.4).

- Obligation to inform data subjects about the processing (Article 12-14 GDPR). In this respect, blockchain verification is little different to conventional processing. Credential holders need to be informed about the processing to take place.
- Right of access (Art 15 GDPR). On a public blockchain, all data stored on the blockchain is public and accessible. Data stored at the issuing institution off-chain should be treated similarly to data in conventional processing.
- Right to restriction of processing (Article 18 GDPR). Local data at an issuing institution can be restricted. Data on the chain cannot be restricted but accessing the information in that data is restricted by the design of the framework. The credential holder can limit the processing by not sharing the credential which acts as a key to the information. A disputed revocation notice can be reversed, if necessary, by the issuing institution. Revocations or reversals of revocations are not possible if the institution does not exist anymore. The continuity in the verification however, justifies, that the restriction of processing might be not perfectly possible in a public verification method.
- Right to data portability (Article 20 GDPR). The credential is sent to the credential holder and the blockchain is publicly accessible.
- Controllers are required to have processing agreements (Article 26 GDPR) which define the duties of processors. Some duties are defined by the law and the protocol, and the enforcement is mainly through the code. Since the identification of node operators is much easier in a permissioned blockchain setting, a processing agreement should be possible and might still be required.
- Records of processing activities (Art. 30 GDPR) can be documented on a use-case basis.
- Distributed ledger technology is no replacement for IT security (Article 32 GDPR). While some attack scenarios are reduced through decentralization, other attack scenarios might even increase by using a decentralized ledger.
- Finally, since blockchain is still considered a relatively new technology, a *data protection impact assessment* (DPIA) might be required. The data protection authority of Bavaria, for example, publishes a list of 9 criteria and if at least two are met, there might be a high risk [250]. The use of

new technology and large-scale data processing might be those points that constitute a high risk. The French CNIL published a substantially different list [251]. Even if a DPIA might not be mandatory, it is at least recommended.

While a permissionless blockchain might shift some liability to the people sending transactions to the blockchain, obligations seem easier to manage in a permissioned blockchain of a consortium.

8.4.18 Can nodes of the blockchain be operated in third countries?

GDPR particularly limits the transfer of personal data to third countries (Articles 44-50 GDPR). Once data is transferred to a third country, where the GDPR does not directly apply, might not be enforceable and no adequate protection exists, GDPR could be circumvented. Adequate protection is evaluated by the EU Commission according to the standards set forth in Article 44 GDPR. With *Schrems I* [252] and *Schrems II* [253], the European Court of Justice decided, that there was no basis for the adequacy of decisions called *Safe Harbour* and *Privacy Shield*. Switzerland, on the other side, is covered by a valid adequacy decision of the European Commission. When personal data is put on a blockchain, and nodes operate outside the EEA, the data will be effectively transferred to a third country. This could mean that Articles 44-50 GDPR apply, which establish high barriers for transfer of personal data to third countries not covered by an adequacy decision [239, p. 27]. However, permissionless blockchains are public and even many consortium blockchains like Bloxberg are public. Controlling the transfer of data that is publicly available over the Internet is very difficult. It can always be transferred to third countries. In *Lindqvist*, the European Court of Justice therefore held that applying the regime of transfer to third countries would impede the use of the Internet and therefore publishing data on the Internet should not be considered a transfer to a third country regardless of the location of the server [254, Para. 70]. This decision was made under the former data protection directive [65] which did not contain any provision regarding the internet. Although some recitals of the GDPR mention the Internet now, the GDPR still has a similar provision regarding the transfer to third countries, which does not mention Internet or publication. This could be a strong indication that there was no desire to deviate from the Lindqvist decisions and that publications on the Internet should not be placed under the restrictive third country rule of Articles 44-50 GDPR. Therefore, the Lindqvist ruling might still apply and third country transfer rules of the GDPR should not impede the use of public blockchains which might have nodes in third countries.

8.4.19 Should the credential holder have control over verification and revocation information?

People from the *Self-Sovereign Identity* (SSI) community have questioned whether the system provides enough control to the credential holder. Once credential holders present the credential to somebody, they provide this person with a permanent key to verification and to checking for revocations. While those who have been presented credentials have a right to know whether this credential

has been revoked, it can still be asked who should be in control of this information. Should the credential holder be able at any time to decide whether a credential can be checked for revocations? In case of a diploma, this could mean that an employer is required to ask permission for subsequent verification and be forced to go to court in case this permission is not granted. This seems to put a high burden on employers. However, if a credential can be verified again on legitimate grounds, others that have the obligation to delete their copy of the credential but did not do so, would remain technically able to verify the credential for possible revocations as well. Either the credential holder or the person that has a copy will be able to determine whether a check for revocations is possible. Technically, the latter solution would be more difficult. A zero-knowledge proof could provide a means to provide a snapshot of the revocation status without the possibility to access further state changes [255]. Credential holders could create separate tokens that act as passwords for separate credential verifiers and time intervals, etc. and remove the possibility to learn about revocations that happened outside the time interval. This could limit verification to a one-time verification comparable to a passport that is presented without leaving a copy with the person the passport is presented to. Only revocation notices existing at the time of presenting the credential will be visible; future revocation notice will not be accessible. Once a credential has been verified, the process cannot be repeated to check for possible errors in the verification process.

Limiting verification is adding complexity to the handling. The credential document can no longer serve as a key, but special verification keys would need to be generated. The credential holder would need to have a means for authentication, like a wallet, to provide the verification possibility. As a result, the transparency of the system would suffer. In case the key or wallet of the credential holder was lost, a backup would be needed. This backup might even be necessary if a court should be able to replace the consent of the credential holder. While this solution might have a certain advantage for special use-cases, it negatively impacts usability and transparency which does not justify its use for long-term credentials that can be retroactively revoked (ex tunc).

8.4.20 Who should be informed when an academic title is revoked?

When a credential is revoked, of course, the credential holders should be actively informed – if possible. Beyond that, the system implements a very specific policy as to who should be able to see the revocation notice. During the discussions it became clear that there is no general standard. Informing too few might result in civil liability when damage is caused by the impression that the credential holder holds a valid academic title. If too many people are informed, this might be a data protection violation and might result in fines and damages as well. A hospital might be required to check the validity of the qualifications of a doctor. Other credential verifiers might have a more limited legitimate reason to do so. In case of plagiarism there might be a duty of the university to warn the public that a former student has been able to present herself as having a qualification that she never earned. This information should be spread to all people that might have been deceived by the academic title. The rules for informing the public about the

revocation of an academic title differ between countries. While Germany publicly announces the revocation of doctoral degrees, Austrian universities are neither allowed to inform the public nor even the person who has informed the university about the suspicious facts that led to the revocation. According to *Stefan Weber*, there is not even legal certainty in Austria how a thesis should be treated when it is considered to be plagiarized [256]. However, this refers to notifying the general public. In case of the revocation of an academic credential, the credential holder is required to return the physical document. The reason for this obligation is to avoid any usage of the revoked credential. The same should apply for digital credentials. Since digital credentials do not have a unique original, but every copy has the same quality and can be considered original when they carry a valid cryptographic signature, there needs to be a different way to ascertain that the revoked credential is not being used any longer. A publication of the revocation of a credential would inform potentially everybody even when the credential is no longer being used. At the same time, people to whom the revoked credential has been presented before might not have received this information. Therefore, the revocation information should be included directly in the verification process. This warrants that the revocation information is available where needed and not available otherwise.

8.4.21 Should the system migrate to Europass, EBSI, ESSIF or Switch?

Switch (section 4.3.7.4) is currently introducing a system to be available for all Swiss universities. EBSI announced a diploma use-case [190]. The *Europass Digital Credentials Infrastructure* (EDCI) announced the certification of credentials using qualified electronic seals [257]. The proposed amendment of eIDAS introduces *European Digital Identity Wallets* to which qualified electronic attestations of attributes can be issued (Article 45e [258]). The coming Swiss eID law should also introduce such attributes.

As this research was done, Europass, EBSI and ESSIF did not provide enough information to determine if they could serve as an alternative in the future. EBSI could be used as affordable and secure distributed ledger or the diploma use-case could be adopted directly. ESSIF should support the future eIDAS EU-wallets. The reliance on wallets offers little advantage for long-term revocable credentials but reduces the usability of a solution unless wallets are used anyway for other purposes. Switch is based on public Ethereum which still has a large carbon footprint. However, Ethereum is currently switching to *Proof of Stake* (PoS) which reduces this issue [259].

Following the choice of the majority of other credential issuers offers advantages: Trust can be higher and barriers to adoption might be lower if the past experience with the system was positive. The cost of maintenance can be spread over more participants and the effort to educate users is reduced. Therefore, a “second-best” system with a high adoption rate should have preference over a better system that would isolate a credential issuing institution.

8.4.22 How does one deal with bugs in the smart contract used?

Smart contracts on a blockchain are designed to be immutable. This can be a problem when a smart contract contains a bug. Two very prominent examples are the DAO-bug [260] and the parity-bug [261]. However, it is possible to create a proxy contract which switches to the current version of a smart contract [262]. This allows to leave the calling address of the verifying contract constant but to replace the code that is being executed. This system of a proxy smart contract subjects itself to new vulnerabilities: the private key to direct the proxy smart contract to the right version of the smart contract could be compromised or abused and the proxy smart contract could have bugs itself. The smart contract proposed for the verification is very simple. Adding versioning capabilities would add more complexity than the diploma verification itself. In a risk analysis the following two risks must be compared. The comparison of these risks needs to consider the probability of the risk and the damage incurred:

- The probability of a bug or modification required for other reasons in the smart contract without versioning and the damage incurred by destroying the existing smart contract and creating a new one.
- The probability of a bug or compromised security in the proxy smart contract and the damage incurred by destroying the existing proxy smart contract and creating a new one.

Since proxy smart contracts for versioning are quite common and well tested now. and that governance for managing multiple credential-issuing institutions is expected to evolve, the use of a proxy smart contract might be considered in the future.

8.4.23 How does one deal with outdated technology?

Technology evolves over time, particularly over decades. Change management requires versioning of components and migration of legacy credentials. A special challenge is that blockchain does and should not provide easy versioning (see section 8.4.22). The blockchain used might even be discontinued. Hashing algorithms might become insecure (see section 8.4.7). Another challenge is connected to the fact that credential files are controlled by the credential holders and cannot be easily updated by the credential issuer to a new format replacing the current PDF format carrying an electronic seal. Much easier should be the maintenance of the online verification. It is a custom web application that is open to revisions and versioning. Since the URL of the web application is communicated, this is the only element that needs to be kept constant. As a last resort, copies of the credentials should be kept at the issuing institution so that the issuing institution – as long as it exists – can carry out a migration to new technology i.e. new hashing algorithms.

8.4.24 How should the governance structure evolve over time?

As discussed in 5.3.2, the system requires proper governance on many levels. These structures depend on many factors like the number of actors involved, the systems used, the jurisdictions involved, etc. Most governance will be non-

technical off-chain governance. Some governance, like the governance of the blockchain used, could at least partly be on-chain. A scaling process with simple governance at the start should be used. Adoption of the university regulation, a data protection impact assessment, the governance of the blockchain used and an internal regulation about who should be able to certify which diplomas in which workflow seem to be a minimal governance for the start of the productive phase. Once more institutions join, governance should become more sophisticated. This prevents starting with an overly complex governance structure that risks creating a large overhead.

8.4.25 Could the smart contract be replaced by a Nonfungible Token NFT?

Nonfungible Tokens (NFTs) are becoming increasingly popular. People who had heard of NFTs asked whether NFTs could be used instead. In contrast to cryptocurrencies like Bitcoin or Ether, Nonfungible Tokens are unique. They are often used to claim “ownership” of a piece of digital art by incorporating a hash value of the digital art in the token. An NFT applies a timestamp to a piece of art or other digital artefact to prove that the person who created the token had access to the work at that time. NFTs are mostly issued on Ethereum and use a standard like ERC-721 [263]. This allows the easy sale and transfer of NFT tokens. NFTs could be programmed in a way that a commission on every blockchain-based sale of the NFT is paid to the artists – either based on the total value or the increase in value.

Credentials are not transferrable. The credential holder should not be allowed to transfer the credential to another person. Therefore, the model of using NFTs does not seem suitable. However, an issuing institution could keep the NFT relating to the credential under its control. In case of a revocation of the credential, the NFT could be destroyed or *burned* as the destruction of tokens is called [264]. Another issue is the authenticity. The NFT only proves that the credential exits. While the credential issuer still holds the key, the credential issuer could prove that it controls the NFT.

To summarize, credentials could be modelled using NFTs. However, the token must never be transferred. The overhead of creating a transferable token that must never be transferred seems to render NFTs an unnecessarily complex solution.

Chapter 9 Contribution and future work

This thesis successfully designed a framework for secure revocable long-term credentials. Beginning by providing the technical and legal background, a list of 27 systems were selected – 16 of them were evaluated. Requirements for a system that is suitable for revocable long-term credentials were discussed and a design proposed. A prototype was built, presented and discussed at the *University of Geneva* as well as in the canton, at conferences, at the university association, at the *International Telecommunications Union* (ITU) and the *Bloxberg* consortium. Important aspects were discussed in a meeting of the *Blockchain Observatory and Forum of the European Commission* and the *German Federal Ministry of the Economic* (*Bundesministerium für Wirtschaft und Energie*). The feedback was used to evaluate and adapt design choices and create a future vision.

The contribution of this thesis is in the following areas:

- It has been demonstrated that a framework for secure digital revocable long-term credentials can be created to respond to the almost contradicting requirements of long-term credentials being independently verifiable on the one hand and that are at the same time revocable on the other hand while sufficiently accounting for the right to be forgotten. This can be achieved by combining qualified electronic seals with a smart contract-based verification and an online system. While costs per credential remain low, the overall system has a certain complexity because of combining these techniques.
- While blockchain and GDPR are seen by some as *being profoundly incompatible at a conceptual level* [239, pp. 17, 28], it has been shown that a blockchain-based solution can serve as a continued decentralized trust provider in a situation where a credential issuing institution is no longer available. This serves the interests of the data subject well and also minimizes the exposure of revocation information which might be sensitive personal data. There are situations where blockchain can be a more privacy-friendly solution compared to centralized solutions that cannot always adequately protect the interests of data subjects.
- Different use-cases of cryptographic hash values of personal data have been analyzed to develop criteria to decide when cryptographic hash values should be considered personal data: Only when additional information or context is added (like revocation information) does a hash value become personal data itself.
- A model for determining controllers in a blockchain context has been proposed. Controllers should be determined for the blockchain level, the smart contract level and the transaction level separately.
- Although decentralized ledgers can secure transactions and credentials, they cannot yet authenticate institutions. It has been demonstrated that the established PKI infrastructure can be used and combined with blockchain

technology to offer a secure authentication. The eIDAS revision plans to introduce *qualified electronic ledgers* created by one or more *qualified trust service providers or providers* in Article 3 nr. 52 and Articles 45h and 45i [258]. Although this does not directly merge the concepts of distributed ledgers and PKI, it is a supports the legal recognition of a combination of both concepts.

- Based on the work of *Sorge/Leicht* [40, pp. 73–74], a single qualified electronic timestamp of a block of a blockchain could serve as a qualified electronic timestamp of the entire preceding blockchain as well as all documents whose hash values are contained in those blocks. This could remove the need to separately timestamp qualified electronic signatures/seals to maintain their legal validity.
- The concept of *Self-Sovereign Identity* (SSI) offers the possibility to disconnect credentials from other parts of one's identity. A diploma, for example, could be proven without disclosing the name on the diploma. It is still unclear if the future Swiss and EU proposals for an eID based on SSI will include this feature. For academic titles this feature should not be relevant in most cases. However, the use of wallets creates additional complexity. At the same time, SSI-based long-term credentials face similar challenges as qualified electronic signatures and qualified electronic seals.
- Credentials that need to be available for a long time need to be prepared for migration and decentralized systems require the appropriate decentralized governance.

Future work will address the following points:

- The long-term verification of credentials is part of the projet de loi of the Canton of Geneva for the University of Geneva [193, Ch. 3C]. The implementation for the University of Geneva will be based on this work.
- Once the Swiss proposal for the new SSI-based eID [14] is available, it should be checked how far it can be used and integrated in the system for the University of Geneva. The announced European Digital Identity Wallet by the eIDAS revision [258] shall also be considered for integration.
- The smart contract on the Bloxberg blockchain shall be made available to be used also by other institutions and an appropriate governance model shall be established in that context.

Furthermore, research is needed regarding the following topics:

- Currently, there is a global move towards the regulation of distributed ledgers. Technical norms are drafted, for example at the ITU, to adapt blockchain technology to regulatory requirements. These need to balance key properties of distributed ledgers like immutability and decentralization with regulatory requirements.
- A digital society is based on digital evidence. Analogue evidence is not only cumbersome to handle, but it is increasingly vulnerable through

artificial intelligence (AI)-based technologies like deep fakes. Preserving digital evidence will be an increasingly important task in the future. Immutability is not a technical problem of blockchain technology but a design decision. There is a need to develop a case-by-case guidance, how much and what type of immutability best serves the fundamental rights and interests of data subjects.

- If cash is abandoned in the future, privacy of monetary transactions risks being lost. The amount of privacy that transactions with *central bank digital currencies* (CDBCs) will enjoy is still under debate. So-called *privacy coins* employ privacy enhancing technology like zero knowledge proofs, ring signatures or state channels to ensure a high level of privacy for blockchain-based transactions. However, financial regulation regarding *know your customer* (KYC), *anti-money laundering* (AML) and *combating the financing of terrorism* (CFT) run counter to the interests of privacy. An intelligent balancing of interests could warrant privacy where possible and transparency where needed. Privacy by design could implement such policies in technical systems that protect small transactions from disclosure but open bigger transactions to appropriate oversight.

Chapter 10 Conclusion

Revocable long-term credentials like university diplomas face a specific challenge: Credentials remain valid even when the institution ceases to exist. Therefore, credentials need to be revocable by the issuing institution, but they also need to be verifiable even when the institution no longer exists. At the same time, data protection laws provide the credential holders with the right to be forgotten. Decentralized ledger technology can be a useful tool to verify long-term credentials that remain valid even when the issuing institution ceases to exist. Determining who should have access to revocation depends on the specific use-case and the retroactive effect of revocations. The legitimate interest of those who should be informed about a revocation need to be balanced with the right to be forgotten by the credential holder of the revoked credential that is no longer being used. Smart contracts on a blockchain can model a good balance here, provide the revocation information where justified and hide it in other cases.

The proposed framework does not use any of the *self-sovereign identity* (SSI) frameworks that are currently often proposed as the optimal approach. It still achieves most goals of the self-sovereign identity approach without burdening the credential holder to always preserve a wallet under two assumptions:

- There is no need to separate the credential from the name of the credential holder. SSI allows a person to be identified through a device that checks some biometric data rather than a name and a birthdate.
- There is no need to limit further verification of a credential once the credential holder has presented the credential to somebody. SSI could allow the creation of verification tokens that allow a credential to be verified only once or only during a limited time interval.

This is motivated and justified by the particularities of long-term revokable credentials like university diplomas. For other use-cases, this choice might be wrong. For example, a driver's license should only be verifiable during a limited time interval: A car-rental company should be able to verify the status of the driver's license only while there is an active rental contract. This is due to the fact that driver's licenses are usually revoked *ex-nunc* (from the time of revocation) and not *ex-tunc* (from the time of its issuing).

Sharing the smart contract with multiple institutions can create a good scaling effect and opens up the possibility of secure cross-verification of credentials. An academic blockchain like Bloxberg could serve as an ideal hub to establish this in the academic world. Bloxberg itself is at a promising but still early stage.

The proposed solution can be directly used or adapted to much more than diploma verification. It is suitable for other kinds of long-term revokable credentials, that are, for example, issued by an officially authenticated institution which should then stay under some but not full control of the institution. While the institution retains the possibility to revoke a credential, the credential holder will always be able to prove what has been issued in the first place and what

happened afterwards. This puts the citizen on a more equal footing with the administration. The citizen is not reduced to a pure object where acts or credentials could be manipulated without a trace. But the citizen has an undeniable proof of every action being taken and can seek legal recourse. While this documented trace often serves to ensure that a citizen is able to exercise her rights, there is a remaining tension with her rights as a data subject. An undeniable proof could also be used against the interests of the data subject. Therefore, the application of this framework and schema is limited to a situation where the issuing institution should stay in limited control and where credential holder and credential verifier have legitimate interests that not all traces are lost regardless of what the credential issuer is willing or able to do. Particularly regarding the revocation of credentials there is no catch-all solution because the legitimate interests of the parties depend on the type of credential and the use-case. Further development of identity solutions like SSI need to address this issue as well.

The design of this framework for revokable long-term credentials has its limitations. It has been designed under some assumptions that are connected to long-term revokable credentials. It has been assumed that the life span of credentials is rather long, and that the revocation is retroactive (ex tunc). For credentials that do not fall into this category, other, possibly more simple solutions might be adequate and data protection requirements might be different. This work is also based on the current state of development of the legal and technical framework of qualified electronic signatures and SSI. In case an SSI-framework will be widely established, the integration with such a framework should be considered. The main argument against SSI is the overhead that is connected to SSI and that is not required for long-term credentials. However, this argument becomes obsolete once SSI is well established.

Several questions raised in this work are still open or cannot be answered with certainty. The *European Data Protection Board* (EDPB), for example, had announced blockchain as a possible topic in the work program 2019/2020 [265] and listed a planned guideline in the work program for 2021/2022 [266]. By the end of 2021, there is still neither a statement from the EDPB nor jurisprudence about how to deal with accountability and immutability in these systems. After the French CNIL published a statement in 2018, no further legal certainty was reached. Legal scholars differ widely in their views and induce an uncertainty in the industry and potential users.

The regulation of distributed ledgers first focused on financial use-cases. With the eIDAS-revision, qualified electronic ledgers will now increasingly be recognized for other purposes, like credentials, by EU law. Other countries will probably follow suit. The EU Commission is advancing the project of a *European Blockchain Services Infrastructure* (EBSI). This certainly moves the focus from crypto anarchists to administrative use-cases. The impact on decentralization has yet to be seen. Will the administration accept a model where the responsibility for the underlying infrastructure is distributed? How will administrative blockchain governance deal with issues arising out of disputed transactions or content? Will

the administration tame the blockchain or will blockchain revolutionize the mindset of the administration?

The COVID-pandemic has emphasized where Western Europe is lagging behind in terms of technology. Electronic identity and cryptographic signatures are not widely used yet. This process is set to be accelerated now and the privacy-friendly approach of SSI is selected for the EU as well as Switzerland. However, the new technical specifications are not available yet and it is to be seen whether the control by citizens is maximized and the control of governments or service providers is limited to the required minimum. How will critical scenarios be implemented like a lost private key, a compromised private key, the information about the revocation of a credential, long-term verification and the prevention of unauthorized copying and borrowing of a personal wallet? Decisions by European governments might create a blueprint for other countries. Paper credentials of refugees cannot be remotely destroyed by the governments of their home countries. Electronic credentials should also be secured against attempts of destroying a credential or even the complete identity.

Solutions for electronic credentials do not require wallets and private keys. Demanding such unnecessary overhead in an isolated setting could reduce acceptance by citizens. However, online authentication and identification as well as qualified electronic signatures already require private keys. SSI could replace many passwords and password managers with a secure and privacy friendly way of authentication and identification. Once wallets are accepted for other purposes, they will not be a usability barrier for electronic credentials anymore. However, it has yet to be seen if these solutions will gain broad acceptance or whether they will suffer the fate of other digital projects initiated by governments, that were based on the best intentions on well-advanced open concepts but that took some wrong turns at later stages.

The answers to these questions will shape the balance of power between stakeholders like governments, industry, and citizens in our future digital society. Decentralization is an important but difficult piece in this puzzle.

Bibliography

[1] J. Lardner and P. Steiner, “The Whistle-Blower-Part I,” *New Yorker*, pp. 52–70, Jul. 1993.

[2] European Court of Justice, *Google Spain v. AEPD*, C-131/12, 13 May 2014.

[3] A. Smith, “Searching for Work in the Digital Era,” *Pew Reserach Center*, p. 30, Nov. 2015.

[4] “Mehrheit der Unternehmen setzt auf Online-Bewerbung, Bitkom e.V.” https://www.bitkom.org/Presse/Presseinformation/Mehrheit-der-Unternehmen-setzt-auf-Online-Bewerbung.html (accessed 27 Nov. 2020).

[5] A. Thiele, “Die Zukunft der Bewerbung: Papier mag (fast) keiner mehr,” *Bewerbung*, 18 Jan. 2018. https://bewerbung.com/zukunft-der-bewerbung/ (accessed 27 Nov. 2020).

[6] M. Bayern, “86% of companies are conducting job interviews via video conference,” *TechRepublic*, 30 Apr. 2020. https://www.techrepublic.com/article/86-of-companies-are-conducting-job-interviews-via-video-conference/ (accessed 27 Nov. 2020).

[7] “Buy Fake Diplomas, High School, College, Degrees, Fake Transcripts & Certificates,” *buydocument.net*. https://www.buydocument.net/ (accessed 21 May 2021).

[8] S. Roselli, “Un cadre est condamné pour un faux diplôme,” *TDG*, 18 Mar. 2017. Accessed: 06 Jan. 2019. [Online]. Available: https://www.tdg.ch/geneve/actu-genevoise/cadre-condamne-faux-diplome/story/27063090

[9] K. Kinser, “Degree Mills: The Billion-Dollar Industry That Has Sold Over a Million Fake Diplomas (review),” *The Review of Higher Education*, vol. 30, no. 1, pp. 77–78, 2006, doi: 10.1353/rhe.2006.0052.

[10] C. Mitchell, “PKI standards,” *Information Security Technical Report*, vol. 5, no. 4, pp. 17–32, 2000, doi: 10.1016/S1363-4127(00)04003-6.

[11] “Revision of Recommendation 14: Authentication of Trade Documents,” United Nations, Economic Commission for Europe, International Trade Procedures Domain (ITPD), Trade and Transport Programme Development Area for approval. [Online]. Available: https://unece.org/fileadmin/DAM/cefact/recommendations/rec14/ECE_TRADE_C_CEFACT_2014_6E_Rec14.pdf

[12] S. Ibrahim, “The Swiss eID law has flaws, but is another version worth the wait?,” *SWI swissinfo.ch*, 19 Feb. 2021. https://www.swissinfo.ch/eng/identit%C3%A0-digitale_eid--una-legge-imperfetta--ma-vale-la-pena-di-aspettare-/46380712 (accessed 12 Apr. 2021).

[13] The Federal Council, “Federal Act on Electronic Identification Services (e-ID Act), Popular vote on 7 March 2021,” 01 Mar. 2021. https://www.admin.ch/gov/en/start/dokumentation/abstimmungen/20210307/legge-sull-ie.html (accessed 12 Apr. 2021).

[14] Conseil fédéral, “Décision de principe du Conseil fédéral sur l’e-ID,” 17 Dec. 2021. https://www.ejpd.admin.ch/ejpd/fr/home/actualite/mm.msg-id-86465.html (accessed 27 Dec. 2021).

[15] “Electronic Signatures and Infrastructures (ESI); Scoping study and framework for standardization of long-term data preservation services, including preservation of/with digital signatures,” ETSI, ETSI SR 019 510 V1.1.1 (2017-05). Accessed: 06 Jan. 2022. [Online]. Available: https://www.etsi.org/deliver/etsi_sr/019500_019599/019510/01.01.01_60/sr_019510v010101p.pdf

[16] A. Abdul-Rahman, “The pgp trust model,” in *EDI-Forum: the Journal of Electronic Commerce*, 1997, vol. 10, no. 3, pp. 27–31. Accessed: 22 Nov. 2021. [Online]. Available: https://technodocbox.com/Email/72425360-The-pgp-trust-model-alfarez-abdul-rahman.html

[17] V. K. Vaishnavi and W. Kuechler, *Design science research methods and patterns: innovating information and communication technology*, Boca Raton, FL, USA: Auerbach Publications, 2008.

[18] C. Loebbecke, P. Bartscher, T. Weiss, and S. Weniger, “Consumers’ Attitudes to Digital Rights Management (DRM) in the German Trade eBook Market,” in *2010 Ninth International Conference on Mobile Business and 2010 Ninth Global Mobility Roundtable (ICMB-GMR)*, Athens, Greece, 2010, pp. 337–344. doi: 10.1109/ICMB-GMR.2010.16.

[19] Q. Liu, R. Safavi-Naini, and N. P. Sheppard, “Digital Rights Management for Content Distribution,” in *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003*, 2003, vol. 21, pp. 49–58.

[20] B. Stone, “Amazon Erases Orwell Books From Kindle Devices,” *New York Times*, 17.6.2009. Accessed: 11 Feb. 2022. [Online]. Available: https://www.nytimes.com/2009/07/18/technology/companies/18amazon.html

[21] D. Pogue, “The Perils of Copy Protection,” *Scientific American*, Aug. 2011, doi: 10.1038/scientificamerican0811-36.

[22] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” vol. 21, no. 2, p. 7, 1978.

[23] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, eIDAS, 2014.

[24] “Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks,” ISO / ITU, ISO/IEC 9594-8 / ITU-T X.509, Oct. 2019.

[25] United Nations, *UNCITRAL model law on electronic signatures: with guide to enactment 2001*, New York: United Nations Publication, 2002.

[26] *Swiss Bundesgesetz vom 18. März 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate*, SR 943.03, ZertES/SCSE, Accessed: 28 May 2018. Available: https://www.admin.ch/opc/de/classified-compilation/20131913/index.html

[27] “Skribble – Legally binding electronic signatures,” *Skribble*. https://www.skribble.com/en/ (accessed 04 Feb. 2021).

[28] *Federal Act on the Amendment of the Swiss Civil Code - Part Five: Swiss Code of Obligations*, SR 220, 30 Mar. 1911. Accessed: 07 Mar. 2022. Available: https://www.fedlex.admin.ch/eli/cc/27/317_321_377/en

[29] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system.” 2008. Accessed: 06 Jan. 2022. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[30] D. Chaum, “Blind Signatures for Untraceable Payments,” in *Advances in Cryptology*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Boston, MA: Springer US, 1983, pp. 199–203. doi: 10.1007/978-1-4757-0602-4_18.

[31] A. Back, “Hashcash - A Denial of Service Counter-Measure,” 01 Aug. 2002. Accessed: 27 Apr. 2017. [Online]. Available: http://www.hashcash.org/papers/hashcash.pdf

[32] T. C. May, “The Cyphernomicon,” 10 Sep. 1994. https://nakamotoinstitute.org/static/docs/cyphernomicon.txt (accessed 29 Dec. 2021).

[33] M. Graczyk, “Hashgraph: A Whitepaper Review,” *OpenToken*, 01 Feb. 2018. https://medium.com/opentoken/hashgraph-a-whitepaper-review-f7dfe2b24647 (accessed 18 Feb. 2018).

[34] J. Tuwiner, “5 Best Bitcoin Mining Hardware ASIC Machines (2021 Rigs),” 02 Mar. 2021. https://www.buybitcoinworldwide.com/mining/hardware/ (accessed 12 Apr. 2021).

[35] “Bitcoin Energy Consumption Index,” *Digiconomist*. https://digiconomist.net/bitcoin-energy-consumption (accessed 07 Mar. 2022).

[36] Verband Schweizerischer Elektrizitätsunternehmen VSE, “Stromverbrauch.” https://www.strom.ch/de/energiewissen/stromverbrauch (accessed 07 Mar. 2022).

[37] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, “The Energy Consumption of Blockchain Technology: Beyond Myth,” *Bus Inf Syst Eng*, vol. 62, no. 6, pp. 599–608, Dec. 2020, doi: 10.1007/s12599-020-00656-x.

[38] A. Sward, I. Vecna, and F. Stonedahl, “Data Insertion in Bitcoin’s Blockchain,” *ledger*, vol. 3, pp. 1–23, Apr. 2018, doi: 10.5195/ledger.2018.101.

[39] H. Delfs and H. Knebl, *Introduction to Cryptography*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2015. doi: 10.1007/978-3-662-47974-2.

[40] C. Sorge and M. Leicht, “Blockchain-based electronic time stamps and the eIDAS regulation: The best of both worlds,” *SCRIPTed*, vol. 19, no. 1, pp. 61–87, Feb. 2022.

[41] W. Zhao, “China’s Supreme Court Recognizes Blockchain Evidence as Legally Binding,” *CoinDesk*, 07 Sep. 2018. https://www.coindesk.com/chinas-supreme-court-recognizes-blockchain-evidence-as-legally-binding (accessed 23 Apr. 2021).

[42] C.-É. Armingaud and A. Feller, “Italy’s Legal Recognition of Blockchain - Based Timestamping,” *The National Law Review*, vol. XII, no. 43, Apr. 2019, Accessed: 12 Feb. 2022. [Online]. Available: https://www.natlawreview.com/article/italy-s-legal-recognition-blockchain-based-timestamping

[43] “Distributed ledger technology terms and definitions,” ITU-T, Focus Group on Application of Distributed Ledger Technology (FG DLT), Aug. 2019.

[44] S. D. Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, “PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain,” presented at the Italian Conference on Cyber Security, Milan, Italy, Jan. 2018.

[45] “Nick Szabo -- The Idea of Smart Contracts,” 1997. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html (accessed 17 May 2021).

[46] V. Buterin, “A next-generation smart contract and decentralized application platform, 2014,” *URL: http://www.ethereum.org/pdfs/EthereumWhitePaper.pdf*, 2014.

[47] L. Oliveira, L. Zavolokina, I. Bauer, and G. Schwabe, “To Token or not to Token: Tools for Understanding Blockchain Tokens,” presented at the International Conference of Information Systems (ICIS 2018), San Francisco, USA, 2018. doi: 10.5167/UZH-157908.

[48] etherscan.io, “Token Tracker | Etherscan,” *Ethereum (ETH) Blockchain Explorer*. http://etherscan.io/tokens (accessed 11 Feb. 2022).

[49] “ERC-20 Token Standard,” https://ethereum.org/en/developers/docs/standards/tokens/erc-20/ (accessed 11 Feb. 2022).

[50] H. Hughes, “The Mind Behind the ‘World Computer’: Ethereum’s Vitalik Buterin,” *Cointelegraph*, 16 Feb. 2020. https://cointelegraph.com/news/the-mind-behind-the-world-computer-ethereums-vitalik-buterin (accessed 11 Feb. 2022).

[51] V. Buterin, “Twitter,” *@VitalikButerin*, 01 Jan. 2018. https://twitter.com/VitalikButerin/status/1051160932699770882 (accessed 17 May 2021).

[52] “Solidity — Solidity 0.8.11 documentation.” https://docs.soliditylang.org/en/v0.8.11/ (accessed 05 Jan. 2022).

[53] M. Aliev, “Under the hood of Ethereum Virtual Machine: Solidity basics,” *Softblocks*, 06 Mar. 2018. https://medium.com/softblocks/under-the-hood-of-ethereum-virtual-machine-solidity-basics-f1930c19f972 (accessed 12 Feb. 2022).

[54] V. Saini, “Getting Deep Into Ethereum: How Data Is Stored In Ethereum?,” *Hacker Noon*, 29 Jul. 2018. https://hackernoon.com/getting-deep-into-ethereum-how-data-is-stored-in-ethereum-e3f669d96033 (accessed 12 Feb. 2022).

[55] M. Montecchi, K. Plangger, and D. C. West, “Supply chain transparency: A bibliometric review and research agenda,” *International Journal of Production Economics*, vol. 238, p. 108152, Aug. 2021, doi: 10.1016/j.ijpe.2021.108152.

[56] R. Morrison, N. C. H. L. Mazey, and S. C. Wingreen, “The DAO Controversy: The Case for a New Species of Corporate Governance?,” *Front. Blockchain*, vol. 3, May 2020, doi: 10/ggx45k.

[57] “Use-cases,” Focus Group on Application of Distributed Ledger Technology. Accessed: 12 Apr. 2021. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.pdf

[58] “ISO/TC 307 - Blockchain and distributed ledger technologies,” *ISO*. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/committee/62/66/6266604.html (accessed 12 Feb. 2022).

[59] “Question 22,” *ITU*. https://www.itu.int:443/en/ITU-T/studygroups/2017-2020/16/Pages/q22.aspx (accessed 12 Feb. 2022).

[60] Council of Europe, “Chart of signatures and ratifications of Treaty 108,” *Treaty Office*. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108 (accessed 11 Dec. 2020).

[61] Council of Europe, “Chart of signatures and ratifications of Treaty 223,” *Treaty Office*. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223 (accessed 11 Dec. 2020).

[62] BVerfG, *Volkszählungsurteil, Judgement of the First Senate from December 15th, 1983 – 1 BvR 209/83*, 1 BvR 209/83, 15 Dec. 1983. Available: https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/1983/12/rs19831215_1bvr020983.pdf

[63] *European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02*, Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

[64] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the processing of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, General Data Protection Regulation (GDPR), Accessed: 31 Dec. 2021. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[65] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Accessed: 06 Jan. 2022. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN

[66] *Swiss Federal Act on Data Protection (FADP) of 16.6.1992*, SR 235.1, Accessed: 06 Jan. 2022. Available: https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en

[67] *Swiss draft law: Loi fédérale sur la protection des données (LPD)*, 25 Sep. 2020. Accessed: 31 Dec. 2021. [Online]. Available: https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2020/1998/fr/pdf-a/fedlex-data-admin-ch-eli-fga-2020-1998-fr-pdf-a.pdf

[68] “Stärkung des Datenschutzes,” *Bundesamt für Justiz*. https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html (accessed 19 Apr. 2022).

[69] *Geneva: Loi sur l’information du public, l’accès aux documents et la protection des données personnelles (LIPAD) du octobre 2001*, A 2 08, Accessed: 19 Feb. 2022. Available: https://silgeneve.ch/legis/program/books/RSG/pdf/rsg_a2_08.pdf

[70] G. Buttarelli, “The EU GDPR as a clarion call for a new global digital gold standard,” *European Data Protection Supervisor*, 01 Apr. 2016. https://edps.europa.eu/press-publications/press-news/blog/eu-gdpr-clarion-call-new-global-digital-gold-standard_de (accessed 15 Sep. 2020).

[71] Hamburgisches Oberverwaltungsgericht, 5 Bs 152/20, 15 Oct. 2020. Available: https://justiz.hamburg.de/contentblob/14563474/4412454194f6066413132c9c7eb82f43/data/5bs152-20.pdf

[72] Datenschutzbehörde, DSB-D123.270/0009-DSB/2018, 05 Dec. 2018. Accessed: 06 Jan. 2022. Available: https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.pdf

[73] “Guidelines 4/2019 on Article 25 Data Protection by Design and by Default,” European Data Protection Board, Nov. 2019. [Online]. Available: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

[74] C. Allen, “The Path to Self-Sovereign Identity,” *Life With Alacrity*, 25 Apr. 2016. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (accessed 03 May 2021).

[75] A. Gruner, A. Muhle, and C. Meinel, “An Integration Architecture to Enable Service Providers for Self-sovereign Identity,” in *2019 IEEE 18th International Symposium on Network Computing and Applications (NCA)*, Cambridge, MA, USA, Sep. 2019, pp. 1–5. doi: 10.1109/NCA.2019.8935015.

[76] “Decentralized Identifiers (DIDs) v1.0,” W3C, Mar. 2021. Accessed: 14 Apr. 2021. [Online]. Available: https://www.w3.org/TR/did-core/

[77] “Verifiable Credentials Data Model 1.0,” W3C, Nov. 2019. Accessed: 14 Apr. 2021. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[78] “Jolocom - Decentralized identity & access management,” *Jolocom*. https://jolocom.io/ (accessed 17 Nov. 2020).

[79] Sovrin Foundation, “Sovrin: A Protocol and Token for Self- Sovereign Identity and Decentralized Trust.” Jan. 2018. [Online]. Available: https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf

[80] “uPort - Tools for Decentralized Identity and Trusted Data.” https://www.uport.me/ (accessed 17 Nov. 2020).

[81] M. Ali, J. Nelson, A. Blankstein, R. Shea, and M. Freedman, “Blockstack Whitepaper 2.0.” 30 May 2019. [Online]. Available: https://blockstack.org

[82] A. Ronchi *et al.*, “La dématérialisation des titres académiques, Etat des lieux, scénario et perspectives.” Apr. 2014. [Online]. Available: https://projects.switch.ch/export/sites/projects/eduid/.galleries/documents/D1.4.1_ecert_rapportfinal.pdf

[83] A. S. Jat, “Comparative Analysis of Existing Blockchain Based Certification DApps,” *International Journal of Advanced Science and Technology*, vol. 29, no. 4, p. 4, 2020.

[84] O. S. Saleh, O. Ghazali, and M. E. Rana, “Blockchain based framework for educational certificates verification,” *Journal of critical reviews*, vol. 7, no. 3, pp. 79–84, 2020.

[85] A. Ronchi *et al.*, “La dématérialisation des titres académiques, Etat des lieux, scénario et perspectives - technical evaluation.” Apr. 2014. [Online]. Available: https://projects.switch.ch/export/sites/projects/eduid/.galleries/documents/D1.4.1_technical_evaluation_grid.pdf

[86] “Unaccredited Universities.” https://www.scholaro.com/unaccredited-universities/ (accessed 17 Feb. 2022).

[87] “Ethereum Energy Consumption Index (beta),” *Digiconomist*. https://digiconomist.net/ethereum-energy-consumption/ (accessed 02 May 2021).

[88] “Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures,” ETSI, ETSI EN 319 122-1 V1.2.1, Oct. 2021.

[89] “Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile,” ETSI, Technical Specification ETSI TS 103 172 V2.2.2, Apr. 2013.

[90] Conférence de La Haye de droit international privé, *Apostille Handbook: a handbook on the practical operation of the Apostille Convention*, 2013.

[91] *Convention of 5 October 1961 Abolishing the Requirement of Legalisation for Foreign Public Documents*, HCCH, 24 Jan. 1965. Accessed: 04 Feb. 2021. Available: https://www.hcch.net/en/instruments/conventions/publications1/?cid=41&dtid=53

[92] "Implementation chart of the e-APP," HCCH. Accessed: 03 Dec. 2021. [Online]. Available: https://assets.hcch.net/docs/b697a1f1-13be-47a0-ab7e-96fcb750ed29.pdf

[93] HCCH, "Closer and Closer to Reality - The e-Apostille Pilot Program of the HCCH and the NNA." 2003. Accessed: 03 Dec. 2021. [Online]. Available: https://assets.hcch.net/upload/wop/genaff_pd10e2006.pdf

[94] "Université de Genève, Palmarès de l'université," 14 Dec. 2020. https://www.unige.ch/palmares/annee-2020/10/ (accessed 04 Feb. 2021).

[95] "Université de Genève, Diplômes universitaires - Archives," 04 Oct. 2018. https://www.unige.ch/archives/adm/documents-en-ligne/diplomes-universitaires/ (accessed 18 Feb. 2021).

[96] "My eQuals," *My eQuals Digital Credentials*. https://www.myequals.edu.au/ (accessed 21 Jan. 2021).

[97] "IMS Global, Open Badges." https://openbadges.org/ (accessed 21 Jan. 2021).

[98] K. Clements, R. E. West, and E. Hunsaker, "Getting Started With Open Badges and Open Microcredentials," *IRRODL*, vol. 21, no. 1, pp. 153–171, Jan. 2020, doi: 10.19173/irrodl.v21i1.4529.

[99] I. Hobson, "Raising the standard: Open Badges 2.0," *digitalme*, 27 Feb. 2018. https://medium.com/digitalme-an-open-badge-adventure/raising-the-standard-open-badges-2-0-192a2a9b6862 (accessed 28 May 2018).

[100] "Open Badges Specification Version 2.0 Changes." https://www.imsglobal.org/sites/default/files/Badges/OBv2p0/history/2.0.html (accessed 05 Feb. 2018).

[101] "IMS Open Badges 2.0 Certification Suite." https://openbadgesvalidator.imsglobal.org/openbadges20/instructions.html (accessed 13 Apr. 2021).

[102] "Open Badges Baking Specification." https://www.imsglobal.org/sites/default/files/Badges/OBv2p0Final/baking/index.html (accessed 13 Apr. 2021).

[103] "Open Badges v2.0." https://www.imsglobal.org/sites/default/files/Badges/OBv2p0/index.html (accessed 09 May 2018).

[104] T. R. Liyanagunawardena, S. Scalzavara, and S. A. Williams, "Open Badges: A Systematic Review of Peer-Reviewed Published Literature (2011-2015)," *European Journal of Open, Distance and E-Learning*, vol. 20, no. 2, pp. 1–16, Dec. 2017, doi: 10.1515/eurodl-2017-0013.

[105] "BADGR, Achieve Anything, Recognize Everything, The Easiest Way to Issue Digital Badges and Micro-Credentials." https://info.badgr.com/ (accessed 18 Feb. 2021).

[106] D. Belshaw, "Peering Deep into Future of Educational Credentialing," *Connected Learning Alliance*, 30 Mar. 2015. https://clalliance.org/blog/peering-deep-into-future-of-educational-credentialing/ (accessed 13 Apr. 2021).

[107] M. Jirgensons and J. Kapenieks, "Blockchain and the Future of Digital Learning Credential Assessment and Management," *Journal of Teacher Education for Sustainability*, vol. 20, no. 1, pp. 145–156, Jun. 2018, doi: 10.2478/jtes-2018-0009.

[108] M. Baldi, F. Chiaraluce, M. Kodra, and L. Spalazzi, "Security analysis of a blockchain-based protocol for the certification of academic credentials," *arXiv:1910.04622 [cs]*, Oct. 2019, Accessed: 14 Apr. 2021. [Online]. Available: http://arxiv.org/abs/1910.04622

[109] G. Capece, N. Levialdi Ghiron, and F. Pasquale, "Blockchain Technology: Redefining Trust for Digital Certificates," *Sustainability*, vol. 12, no. 21, p. 8952, Oct. 2020, doi: 10.3390/su12218952.

[110] M. Bartoletti and L. Pompianu, “An analysis of Bitcoin OP_RETURN metadata,” in *Financial Cryptography and Data Security*, Mar. 2017, pp. 218–230. doi: 10.1007/978-3-319-70278-0_14.

[111] *Arizona State Law § 44-7061: Signatures and records secured through blockchain technology; smart contracts; ownership of information; definitions*, AZ Rev Stat § 44-7061 (2020), Accessed: 23 Apr. 2021. Available: https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/44/07061.htm

[112] *Vermont Statute*, vol. 12 V.S.A. § 1913. Blockchain enabling, Accessed: 23 Apr. 2021. Available: https://legislature.vermont.gov/statutes/section/12/081/01913

[113] “Welcome to Diploma.report.” https://diploma.report/ (accessed 23 Apr. 2021).

[114] “Diploma.report Authenticating a diploma.” https://diploma.report/pages/blog-post (accessed 23 Apr. 2021).

[115] “Diploma.report school list.” https://diploma.report/issuers/school_list (accessed 23 Apr. 2021).

[116] “Block.co Validator,” *Block.co*. https://web.archive.org/web/20210604071705/https://block.co/validator-and-certificate-examples/ (archived version 04 Jun. 2021).

[117] “Chainpoint - Blockchain Proof & Anchoring Standard.” https://chainpoint.org/ (accessed 23 Apr. 2021).

[118] K. Karasavvas, “Revoking Records in an Immutable Ledger: A Platform for Issuing and Revoking Official Documents on Public Blockchains,” in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, Zug, Jun. 2018, pp. 105–111. doi: 10.1109/CVCBT.2018.00019.

[119] C. Colle, A. De Capitani, K. Lindroos, A. Maris, T. Virgl, and K. Zylka, “Gradbase Decentralised academic record verification using the Bitcoin block chain,” Imperial College, London, Jan. 2015. [Online]. Available: https://www.doc.ic.ac.uk/teaching/distinguished-projects/2015/l.colle.pdf

[120] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, “EduCTX: A blockchain-based higher education credit platform,” *IEEE Access*, vol. 6, pp. 5112–5127, 2018, doi: 10.1109/ACCESS.2018.2789929.

[121] “RecordsKeeper — RecordsKeeper documentation.” https://recordskeeper.readthedocs.io/en/latest/ (accessed 22 Apr. 2021).

[122] “RecordsKeeper Blockchain Mining Permission,” *Google Docs*. https://docs.google.com/forms/d/e/1FAIpQLSd1Dd2GAggCyom23HgiBhnQIjlLjMgRwf_UOQrHp9BUTRPEYA/viewform?fbzx=4878347243312853645&usp=embed_facebook (accessed 08 Mar. 2022).

[123] T. Sharma, “RecordsKeeper Token Sale Cancellation Announcement,” *Medium*, 16 Nov. 2018. https://medium.com/recordskeeper/recordskeeper-token-sale-cancellation-announcement-3e8effc40d21 (accessed 22 Apr. 2021).

[124] “Frequently Asked Questions — RecordsKeeper documentation.” https://docs.recordskeeper.com/en/latest/faq.html (accessed 08 Mar. 2022).

[125] R. Arenas and P. Fernandez, “CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials,” in *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, Stuttgart, Jun. 2018, pp. 1–6. doi: 10.1109/ICE.2018.8436324.

[126] O. Ghazal and O. S. Saleh, “A Graduation Certificate Verification Model via Utilization of the Blockchain Technology,” *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 10, no. 3–2, pp. 29–34, Sep. 2018, Accessed: 02 Oct. 2018. [Online]. Available: https://jtec.utem.edu.my/jtec/article/view/4707/3640

[127] “Smart Certificate Pricing.” https://cvtrust.com/pricing.aspx (accessed 02 May 2021).

[128] D. Goldenberg, “Smart Certificate 2.0 - Issue and share certified and trusted digital documents, case study,” iTextpdf Software, Dec. 2019. Accessed: 17 May 2021. [Online]. Available: https://itextpdf.com/de/node/14026

[129] “Timestamping – Block height is the new Time,” *Woleet*. https://www.woleet.io/timestamping/ (accessed 17 May 2021).

[130] S. Khedkar, A. Powar, N. Powar, C. Kille, and H. Kansara, “Transcripts DApp—A Blockchain-Based Solution for Transcript Application,” in *IC-BCT 2019*, Singapore, 2020, pp. 177–189.

[131] “IPFS Powers the Distributed Web,” *IPFS*. https://ipfs.io/ (accessed 02 May 2021).

[132] YCHARTS, “Ethereum Average Transaction Fee.” https://ycharts.com/indicators/ethereum_average_transaction_fee (accessed 02 May 2021).

[133] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, “The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling,” in *Business Information Systems Workshops*, Cham, 2019, vol. 339, pp. 185–196. doi: 10.1007/978-3-030-04849-5_16.

[134] SWITCH, “Foundation - About us.” https://www.switch.ch/about/foundation/ (accessed 03 May 2021).

[135] SWITCH, “SWITCHverify - Zertifizierung & Verifizierung von Hochschuldiplomen auf ihre Echtheit.” https://www.switch.ch/de/verify/ (accessed 17 Nov. 2020).

[136] F. Schär and F. Mösli, “Blockchain diplomas: Using smart contracts to secure academic credentials,” *Beiträge zur Hochschulforschung 3/2019*, pp. 48–58.

[137] F. Schär, “University of Basel fights diploma fraud with blockchain | Certifaction.io,” 30 Apr. 2019. https://certifaction.io/university-of-basel-fights-diploma-fraud-with-blockchain/ (accessed 03 May 2021).

[138] E. Mosanya, “JavaScript SDK Documentation - v1.0,” *Certifaction AG*, Jan. 2021. https://docs.google.com/document/d/1t3E3is6Jev5GZr8wW25jtDxcBb0p4ei1GfIBJiqkuS4/edit?usp=embed_facebook (accessed 03 May 2021).

[139] *Certifaction Command Line Interface CLI*, Github, 2021. Accessed: 03 May 2021. [Online]. Available: https://github.com/certifaction/cli

[140] J. Chow, “A Guide to Events and Logs in Ethereum Smart Contracts,” *ConsenSys*, 06 Jun. 2016. https://consensys.net/blog/developers/guide-to-events-and-logs-in-ethereum-smart-contracts/ (accessed 16 May 2021).

[141] *Certifaction*, Github. Accessed: 17 May 2021. [Online]. Available: https://github.com/certifaction

[142] BCdiploma, “Digital Credentials on the Blockchain.” https://www.bcdiploma.com/index.html (accessed 17 Nov. 2020).

[143] “BCDiploma Whitepaper.” 20 Apr. 2018. [Online]. Available: https://www.evidenz.io/img/pdf/BCD-WhitePaper_last.pdf

[144] “Digital Identity Guidelines,” NIST Special Publication, 800–63B. Accessed: 03 May 2021. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html

[145] “NGI eSSIF-LAB European Self-Sovereign Identity Framework Lab.” https://essif-lab.eu/ (accessed 14 Dec. 2021).

[146] “NGI, eSSIF-Lab Functional Architecture.” https://essif-lab.github.io/framework/docs/essifLab-fw-func-arch (accessed 15 Dec. 2021).

[147] “ESSIF-Lab / TNO SSI Service / developer-docs,” *GitLab*. https://gitlab.grnet.gr/essif-lab/tno-ssi-service/developer-docs (accessed 03 May 2021).

[148] “Diploma Functional Scope - EBSI Documentation.” https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/Diploma+Functional+Scope (accessed 23 Nov. 2021).

[149] *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2104 as regards establishing a framework for a European Digital Identity*, 2021/0136 (COD), 03 Jun. 2021. Accessed: 13 Jun. 2021. [Online]. Available: https://ec.europa.eu/newsroom/dae/redirection/document/76608

[150] European Commission, “European Blockchain Pre-Commercial Procurement,” 02 Oct. 2021. https://digital-strategy.ec.europa.eu/en/news/european-blockchain-pre-commercial-procurement (accessed 21 Nov. 2021).

[151] K. Hamilton Duffy, H. Pongratz, and J. P. Schmidt, “Building the digital credential infrastructure for the future.” Digital Credentials Consortium, 2020. Accessed: 17 Nov. 2020. [Online]. Available: https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf

[152] Hasso Plattner Institut, “Gegen Urkundenfälschung: Universitätskonsortium entwickelt technischen Standard für akademische Leistungsnachweise,” 05 Feb. 2020. https://hpi.de/pressemitteilungen/2020/gegen-urkundenfaelschung-universitaetskonsortium-entwickelt-technischen-standard-fuer-akademische-leistungsnachweise.html (accessed 14 Apr. 2021).

[153] A. Castor, “Cardano Blockchain’s First Use Case: Proof of University Diplomas in Greece,” *Bitcoin Magazine: Bitcoin News, Articles, Charts, and Guides*. https://bitcoinmagazine.com/business/cardano-blockchains-first-use-case-proof-university-diplomas-greece (accessed 03 May 2021).

[154] “Greek Project Uses Cardano Blockchain for Diploma Verification,” *CoinWire*. https://www.coinwire.com/greek-project-uses-cardano-blockchain-for-diploma-verification (accessed 17 May 2021).

[155] A. Dovbnya, “Cardano Developer IOHK Announces ‘World’s Biggest Blockchain Deployment’ in Ethiopia,” 27 Apr. 2021. https://u.today/cardano-developer-iohk-announces-worlds-biggest-blockchain-deployment-in-ethiopia (accessed 03 May 2021).

[156] D. Wleh, “What’s happened with Cardano Proof of University Diplomas in Greece?,” *Cardano Stack Exchange*, 26 May 2021. https://cardano.stackexchange.com/questions/745/whats-happened-with-cardano-proof-of-university-diplomas-in-greece (accessed 28 Dec. 2021).

[157] F. Bond, F. Amati, and G. Blousson, “Blockchain, academic verification use case,” *Buenos Aires*, Aug. 2015, [Online]. Available: https://s3.amazonaws.com/signatura-usercontent/blockchain_academic_verification_use_case.pdf

[158] B. Duan, Y. Zhong, and D. Liu, “Education Application of Blockchain Technology: Learning Outcome and Meta-Diploma,” in *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*, Shenzhen, Dec. 2017, pp. 814–817. doi: 10.1109/ICPADS.2017.00114.

[159] LedgerbackØDCRC, “The Age of Digital Diplomas: What can we learn from Central New Mexico Community College?,” *Greyscail Blockchain Review*, 14 Jan. 2019. https://medium.com/greyscail/the-age-of-digital-diplomas-what-can-we-learn-from-central-new-mexico-community-college-2bdd81840337 (accessed 28 Dec. 2021).

[160] J. Hope, “Give students ownership of credentials with blockchain technology,” *Enrollment Management Report*, vol. 23, no. 2, pp. 6–7, 2019, doi: https://doi.org/10.1002/emt.30533.

[161] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, “Blockchain and smart contract for digital certificate,” in *2018 IEEE International Conference on Applied System Invention (ICASI)*, Chiba, Apr. 2018, pp. 1046–1051. doi: 10.1109/ICASI.2018.8394455.

[162] D.-H. Nguyen, D.-N. Nguyen-Duc, N. Huynh-Tuong, and H.-A. Pham, “CVSS: A Blockchainized Certificate Verifying Support System,” in *Proceedings of the Ninth International Symposium on Information and Communication Technology - SoICT 2018*, Danang City, Viet Nam, 2018, pp. 436–442. doi: 10.1145/3287921.3287968.

[163] J. Eckhardt, A. Vogelsang, and D. M. Fernández, “Are ‘non-functional’ requirements really non-functional?: an investigation of non-functional requirements in practice,” in *Proceedings of the 38th International Conference on Software Engineering*, Austin Texas, May 2016, pp. 832–842. doi: 10.1145/2884781.2884788.

[164] “governance,” *Cambridge Dictionary*. Accessed: 28 May 2021. [Online]. Available: https://dictionary.cambridge.org/de/worterbuch/englisch/governance

[165] R. van Pelt, S. Jansen, D. Baars, and S. Overbeek, “Defining Blockchain Governance: A Framework for Analysis and Comparison,” *Information Systems Management*, vol. 38, no. 1, pp. 21–41, Jan. 2021, doi: 10.1080/10580530.2020.1720046.

[166] BSI, “Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR),” BSI Technische Richtlinie 03125, Mar. 2018. Accessed: 15 Dec. 2021. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03125/TR-03125_node.html

[167] G. Danezifs *et al.*, *Privacy and data protection by design - from policy to engineering.*, LU: Publications Office, 2014. Accessed: 18 Feb. 2022. [Online]. Available: https://data.europa.eu/doi/10.2824/38623

[168] DIN, “DIN SPEC 4997: Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology,” DIN SPEC 4997. Accessed: 19 Dec. 2021. [Online]. Available: https://www.beuth.de/de/technische-regel/din-spec-4997/321277504

[169] R. Müller, T. Geiser, K. Pärli, and M. Toneatti, Eds., “Anhang 1 Checkliste für Unternehmen im Umgang mit personenbezogenen Daten des Arbeitnehmers,” in *Löschungsanspruch von personenbezogenen Daten des Arbeitnehmers gegenüber der Arbeitgeberin*, Zürich: Dike Verlag AG, 2019.

[170] “Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft,” Berliner Beauftragte für Datenschutz und Informationsfreiheit, Nov. 2019. Accessed: 19 Mar. 2022. [Online]. Available: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf

[171] Landgericht Berlin, *Deutsche Wohnen*, (526 OWi LG) 212 Js-OWi 1/20 (1/20), 18 Feb. 2021. Available: https://openjur.de/u/2331402.ppdf

[172] “ISO/IEC 27555 PII deletion.” https://www.iso27001security.com/html/27555.html (accessed 19 Feb. 2022).

[173] “WebPreserver - Forensic Investigation & Preservation Tool,” *Pagefreezer - Monitoring and Archiving of Online Data*. https://www.pagefreezer.com/webpreserver/ (accessed 09 Jul. 2021).

[174] “Blockchain Infrastructure for Scientific Research,” *Bloxberg*. https://bloxberg.org/ (accessed 17 Jul. 2021).

[175] “EBSI Experience the future with the European Blockchain Services Infrastructure (EBSI),” *CEF Digital programme*. https://ec.europa.eu/cefdigital/wiki/cefdigital/wiki/display/CEFDIGITAL/EBSI (accessed 17 Jul. 2021).

[176] “Validate document,” *Validator is a service of the Federal Administration*. https://www.e-service.admin.ch/validator/upload/all/de?19-1.ILinkListener-languages-3-languageLink (accessed 17 Jul. 2021).

[177] R. Vidwans, “The Dangers of Unicode in Domain Spoofing Phishing Attacks,” *Clearedin*. https://www.clearedin.com/blog/the-dangers-of-unicode-in-domain-spoofing-phishing-attacks (accessed 13 Jul. 2021).

[178] “ITU-T Recommendation X.667,” International Telecommunication Union ITU, Sep. 2004. [Online]. Available: https://www.itu.int/ITU-T/studygroups/com17/oid/X.667-E.pdf

[179] V. Dhillon, D. Metcalf, and M. Hooper, “The DAO Hacked,” in *Blockchain Enabled Applications*, Berkeley, CA: Apress, 2017, pp. 67–78. doi: 10.1007/978-1-4842-3081-7_6.

[180] “Using Dash Governance — Dash latest documentation.” https://docs.dash.org/en/stable/governance/using.html (accessed 13 Feb. 2022).

[181] “EOS Governance, EOS User Agreement,” EOS Mainnet, Aug. 2021. Accessed: 23 Nov. 2021. [Online]. Available: https://github.com/EOS-Mainnet/governance/blob/eb817f225d26ec57db8b71668dc50638c5fa1957/eosio.system/eosio.system-clause-constitution-rc.md

[182] Vitalik Buterin, “Notes on Blockchain Governance,” 17 Dec. 2017. https://vitalik.ca/general/2017/12/17/voting.html (accessed 09 Sep. 2018).

[183] C. Thompson, M. Shelton, E. Stark, M. Walker, E. Schechter, and A. P. Felt, “The Web’s Identity Crisis: Understanding the Effectiveness of Website Identity Indicators,” in *28th USENIC Security Symposium (USENIX Security 19)*, pp. 1715–1732. Accessed: 15 Dec. 2021. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/thompson

[184] D. Allen, “Blockchain Governance: What We Can Learn from the Economics of Corporate Governance,” *The JBBA*, vol. 3, no. 1, pp. 1–10, May 2020, doi: 10.31585/jbba-3-1-(8)2020.

[185] “Université de Genève, InZone,” 21 Jul. 2021. https://www.unige.ch/inzone/who-we-are/who-we-are/ (accessed 19 Nov. 2021).

[186] B. Moser-Mercer, E. Hayba, and J. Goldsmith, “Higher education spaces and protracted displacement: How learner-centered pedagogies and human-centered design can unleash refugee innovation,” in *UNESCO Chair Conference on Technologies for Development*, 2016, pp. 41–52.

[187] “Concrete5.” https://www.concrete5.de/ (accessed 05 Jan. 2022).

[188] L. M. Goodman, “Tezos: A Self-Amending Crypto-Ledger Position Paper,” Aug. 2014, Accessed: 15 Dec. 2021. [Online]. Available: https://cryptorating.eu/whitepapers/Tezos/position_paper.pdf

[189] *EOS.IO Technical White Paper v2*, GitHub: EOSIO, 2018. Accessed: 09 Sep. 2018. [Online]. Available: https://github.com/EOSIO/Documentation

[190] T. Mouha and B. Champagne, “Diploma use case and ESSIF,” Feb. 2021. Accessed: 15 Dec. 2021. [Online]. Available: https://media.belnet.be/presentations/events/ebsi/20210224/diploma-use-case-and-european-self-sovereign-identity-framework.pdf

[191] *web3.js - Ethereum JavaScript API — web3.js 1.0.0 documentation*, Accessed: 21 Nov. 2021. [Online]. Available: https://web3js.readthedocs.io/en/v1.5.2/

[192] “API Documentation & Design Tools for Teams,” *Swagger*. https://swagger.io/ (accessed 21 Nov. 2021).

[193] *Projet de loi ouvrant un crédit au titre de subvention cantonale d’invertissement de 12 000 000 francs pour financer la refonte des prestations numériques aux étudiants de l’Université de Genève*, PL 12767, 26 Aug. 2020. Accessed: 27 Dec. 2021. Available: https://ge.ch/grandconseil/data/texte/PL12767.pdf

[194] J. Hage, “A theory of legal reasoning and a logic to match,” *Artificial Intelligence and Law*, vol. 4, pp. 199–273, 1996.

[195] T. I. Schmidt, “Grundlagen rechtswissenschaftlichen Arbeitens,” *JuS*, no. 7, pp. 649–654, 2003, Accessed: 14 Feb. 2022. [Online]. Available: https://beck-online.beck.de/Bcid/Y-300-Z-JUS-B-2003-S-649-N-1

[196] “Blockchain and the GDPR, a thematic report prepared by the European Union Blockchain Observatory and Forum.” 16 Oct. 2018. Accessed: 19 Dec. 2021. [Online]. Available: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

[197] “ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT),” *ITU*. https://www.itu.int:443/en/ITU-T/focusgroups/dlt/Pages/default.aspx (accessed 21 Nov. 2021).

[198] J. Erbguth, “Datenschutz auf öffentlichen Blockchains,” *Jusletter IT*, no. 22.2.2018, Feb. 2018, Accessed: 19 Dec. 2021. [Online]. Available: https://jusletter-it.weblaw.ch/issues/2019/IRIS/blockchain-und-dsgvo_ea104cc327.html__ONCE

[199] J. Erbguth, “Blockchain und DSGVO,” *Jusletter IT*, Feb. 2019, Accessed: 21 Dec. 2019. [Online]. Available: https://jusletter-it.weblaw.ch/issues/2019/IRIS/blockchain-und-dsgvo_ea104cc327.html__ONCE

[200] J. Erbguth, “Blockchain & GDPR, Conference by EDV-Gerichtstag.” https://blockchain-gdpr.info/conference-edv-gerichtstag/ (accessed 19 Dec. 2021).

[201] J. Erbguth and J. G. Fasching, “Wer ist Verantwortlicher einer Bitcoin-Transaktion?,” *Zeitschrift für Datenschutz ZD*, no. 12, pp. 560–565, 2017.

[202] J. Erbguth, “Wann sind kryptografische Hashwerte von personenbezogenen Daten selbst wieder personenbezogene Daten?,” *Multimedia und Recht MMR*, pp. 654–660, 2019.

[203] J. Erbguth, “Practitioner’s Corner, Five Ways to GDPR-Compliant Use of Blockchains,” *European Data Protection Law Review*, vol. 5, no. 3, pp. 427–433, 2019, doi: 10.21552/edpl/2019/3/19.

[204] J. Erbguth, “Bitcoin/E-Geld/Virtuelle Währungen,” in *Datenrecht in der Digitalisierung*, L. Specht-Riemenschneider, N. Werry, and S. Werry, Eds. Berlin: Erich Schmidt Verlag, 2020.

[205] J. Erbguth, “Smart Contracts und die DSGVO,” in *INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft*, Bonn, 2019, pp. 421–434. doi: 10.18420/INF2019_59.

[206] G. Kondova and J. Erbguth, “Self-sovereign identity on public blockchains and the GDPR,” in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, Brno Czech Republic, Mar. 2020, pp. 342–345. doi: 10.1145/3341105.3374066.

[207] J. Erbguth and J.-H. Morin, “Towards Governance and Dispute Resolution for DLT and Smart Contracts,” in *2018 IEEE 9th International Conference on Software Engineering and Service Science (ICSESS)*, Beijing, China, Nov. 2018, pp. 46–55. doi: 10.1109/ICSESS.2018.8663721.

[208] L. Ungerboeck, “Kauf von Doppelstockzügen wird Debakel für die ÖBB,” *Der Standard*, Wien, 20 Sep. 2021. Accessed: 20 Dec. 2021. [Online]. Available: https://www.derstandard.at/story/2000129788448/kauf-von-doppelstockzuegen-wird-debakel-fuer-die-oebb

[209] “China Qualifications Verification.” http://www.chinadegrees.cn/en/ (accessed 21 Nov. 2021).

[210] Y. Sheffer, Porticor, R. Holz, and P. Saint-Andre, “Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS),” Internet Engineering Task Force IETF, RFC 7457, Feb. 2015. Accessed: 05 Jan. 2022. [Online]. Available: https://www.hjp.at/doc/rfc/rfc7457.txt

[211] V. Mladenov, C. Mainka, K. Meyer zu Selhausen, M. Grothe, and J. Schwenk, “1 Trillion Dollar Refund: How To Spoof PDF Signatures,” in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, London United Kingdom, Nov. 2019, pp. 1–14. doi: 10.1145/3319535.3339812.

[212] S. Rohlmann, V. Mladenov, C. Mainka, and J. Schwenk, “Breaking the Specification: PDF Certification,” in *2021 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, May 2021, pp. 1485–1501. doi: 10.1109/SP40001.2021.00110.

[213] X. Wang and H. Yu, “How to Break MD5 and Other Hash Functions,” in *Advances in Cryptology – EUROCRYPT 2005*, Berlin, Heidelberg, 2005, pp. 19–35.

[214] L. Chen *et al.*, “Report on Post-Quantum Cryptography,” National Institute of Standards and Technology, NIST IR 8105, Apr. 2016. doi: 10.6028/NIST.IR.8105.

[215] I. T. L. NIST, Computer Security Division, “Workshops and Timeline - Post-Quantum Cryptography | CSRC | CSRC,” *CSRC | NIST*, 10 Mar. 2022. https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline (accessed 05 Apr. 2022).

[216] *Council of Europe: Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), “Convention 108+”, 18 May 2018*,

[217] O. H. Sletnes, *Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]*, p. 4. Accessed: 18 Feb. 2022. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22018D1022&from=EN

[218] “Blockchain – Solutions for a responsible use of the blockchain in the context of personal data,” Commission Nationale de l’Informatique et des Libertés CNIL, Sep. 2018. Accessed: 14 Sep. 2019. [Online]. Available: https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf

[219] A. Roßnagel, “Datenlöschung und Anonymisierung,” *Zeitschrift für Datenschutz ZD*, pp. 188–192, 2021.

[220] U. Kelber, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, *Studie “Kindeswohl und Umgangsrecht,”* 13-317/018#0127, 17 Feb. 2021. Accessed: 22 Dec. 2021. Available: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/AccessForAll/2021/2021-Studie-Kindeswohl-Umgangsrecht.pdf

[221] J. Erbguth and O. Stepanova, “‘Fruit of the poisonous tree’-Doktrin im Datenschutz?,” *Zeitschrift für Datenschutz ZD*, no. 5/2022, May 2022.

[222] N. Forgó, M. Helfrich, and J. Schneider, “Teil 1. Allgemeine datenschutzrechtliche Grundlagen und Strukturen, Kapitel 5. Grundsätze der datenschutzrechtlichen Prüfung, IX. Pflichten des Verantwortlichen,” in *Betrieblicher Datenschutz*, 3rd ed., München: C.H.Beck oHG, 2019.

[223] J. Schrey and T. Thalhofer, “Rechtliche Aspekte der Blockchain,” *NJW*, vol. 2017, pp. 1431–1436, May 2017.

[224] “Opinion 05/2014 on Anonymisation Techniques,” Article 29 Data Protection Working Party, 0829/14/EN WP216, Apr. 2014.

[225] European Court of Justice, *Breyer v. Bundesrepublik Deutschland*, C-582/14, 19 Oct. 2016.

[226] Bundesgerichtshof, I ZB 80/11, 19 Apr. 2012.

[227] R. Hoffmann and D. Schmidt, “Facebook-Profiling zu Marketingzwecken – datenschutzkonform?,” *GRUR*, vol. 2021, pp. 679–685.

[228] “Introduction to the hash function as a personal data pseudonymisation technique,” aepd EDPS, Oct. 2019. Accessed: 18 Feb. 2022. [Online]. Available: https://edps.europa.eu/sites/default/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf

[229] “ethereum-private-key-to-public-key,” *npm*. https://www.npmjs.com/package/ethereum-private-key-to-public-key (accessed 18 Feb. 2022).

[230] “Bloxberg Faucet.” https://faucet.bloxberg.org/ (accessed 05 Jan. 2022).

[231] R. H. Weber, “The Interplay of Blockchain Technologies and Data Protection,” *Jusletter-IT*, no. 30-September-2020, 2020, doi: 10.38023/e85a8001-b86f-4e40-93ef-d82253ed10eb.

[232] A. Jambert, “Blockchain and the GDPR: A Data Protection Authority Point of View,” in *Information Security Theory and Practice: 12th IFIP WG 11.2 International Conference,*

WISTP 2018, Brussels, Belgium, December 10–11, 2018, Revised Selected Papers, Cham, 2019, vol. 11469, pp. 3–6. doi: 10.1007/978-3-030-20074-9.

[233] European Parliament. Directorate General for Parliamentary Research Services., *Blockchain and the general data protection regulation: Can distributed ledgers be squared with European data protection law?*, LU: Publications Office, 2019. Accessed: 30 Dec. 2021. [Online]. Available: https://data.europa.eu/doi/10.2861/535

[234] European Court of Justice, *Nowak*, C-434/16, 20 Dec. 2017. Accessed: 18 Feb. 2022. Available: https://curia.europa.eu/juris/document/document.jsf?docid=198059

[235] M. Arning and T. Rothkegel, "DS-GVO Art. 4 Begriffsbestimmungen," in *DSGVO - BDSG - TTDSG*, 4th ed., J. Taeger and D. Gabel, Eds. 2022.

[236] M. Berberich and M. Steiner, "Practitioner's Corner - Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?," *European Data Protection Law Review*, vol. 2, no. 3, pp. 422–426, 2016, doi: 10.21552/EDPL/2016/3/21.

[237] T. Herbst, "DS-GVO Art. 16 Recht auf Berichtigung," in *DS-GVO BDSG*, 3rd ed., J. Kühling and B. Buchner, Eds. 2020, p. 11.

[238] G. Ateniese, B. Magri, D. Venturi, and E. Andrade, "Redactable Blockchain – or – Rewriting History in Bitcoin and Friends," in *2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, Paris, Apr. 2017, pp. 111–126. doi: 10.1109/EuroSP.2017.37.

[239] M. Finck, "Blockchains and Data Protection in the European Union," *European Data Protection Law Review*, vol. 4, no. 1, pp. 17–35, 2018, doi: 10.21552/edpl/2018/1/6.

[240] G. Spindler, "Datenschutzrechtliche Anforderungen an den Einsatz der Blockchain-Technologie im Aktienrecht," *Zeitschrift für Unternehmens- und Gesellschaftsrecht*, vol. 49, no. 5, pp. 707–748, Oct. 2020, doi: 10.1515/zgr-2020-0039.

[241] U. Tatar, Y. Gokce, and B. Nussbaum, "Law versus technology: Blockchain, GDPR, and tough tradeoffs," *Computer Law & Security Review*, vol. 38, p. 105454, Sep. 2020, doi: 10.1016/j.clsr.2020.105454.

[242] R. Teperdjian, "The puzzle of squaring blockchain with the General Data Protection Regulation," vol. 60, p. 61, 2020.

[243] T. Janicki and D. Saive, "Janicki/Saive: Privacy by Design in Blockchain-Netzwerken," *Zeitschrift für Datenschutz ZD*, no. 6, pp. 251–256, 2019.

[244] P. J. Pesch and C. Sillaber, "Distributed Ledger, Joint Control? – Blockchains and the GDPR's Transparency Requirements," *Computer Law Review International*, vol. 18, no. 6, Dec. 2017, doi: 10.9785/cri-2017-0602.

[245] A. Mirchandani, "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR," *Fordham Intellextual Property, Media and Entertainment Law Jorunal*, vol. 29, no. 4, pp. 1201–1241, 2019.

[246] "Computer Law Review International. A Journal of Information Law and Technology: Editorial Board and Correspondents," *Computer Law Review International*, vol. 19, no. 20, pp. 3–3, Dec. 2019, doi: 10.9785/cri-2019-192002.

[247] M. D. de Rosnay, "Peer-to-peer as a design principle for law: distribute the law," *Journal of Peer Production, 2015, Disruption and the Law*, pp. 1–9, Accessed: 06 Jan. 2022. [Online]. Available: https://halshs.archives-ouvertes.fr/halshs-01103885

[248] European Court of Justice, *Facebook Fanpage*, C-210/16, 05 Jun. 2018. Accessed: 03 Jan. 2022. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62016CJ0210&from=EN

[249] European Court of Justice, *Fashion ID*, C-40/17, 29 Jul. 2019. Accessed: 18 Feb. 2022. Available: https://curia.europa.eu/juris/document/document.jsf?docid=216555

[250] "Datenschutz Folgenabschätzung Bayerische Blacklist," Bayerische Landesbeauftragte für den Datenschutz, Mar. 2019.

[251] “CNIL publishes list of data processing operations requiring a DPIA,” *Bird & Bird*. http://www.twobirds.com/en/news/articles/2018/france/la-cnil-vient-de-publier-au-jorf-la-liste-des-traitements (accessed 18 Feb. 2022).

[252] European Court of Justice, *Schrems I*, C-362/14, 06 Oct. 2015. Accessed: 05 Jan. 2022. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62014CJ0362

[253] European Court of Justice, *Schrems II*, C-311/18, 16 Jul. 2020. Accessed: 05 Jan. 2022. Available: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:62018CJ0311

[254] European Court of Justice, *Lindqvist, C-101/01,* 06 Nov. 2003. Accessed: 24 Apr. 2022. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101

[255] M. Chase, C. Ganesh, and P. Mohassel, “Efficient Zero-Knowledge Proof of Algebraic and Non-Algebraic Statements with Applications to Privacy Preserving Credentials,” in *Advances in Cryptology – CRYPTO 2016*, vol. 9816, M. Robshaw and J. Katz, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 499–530. doi: 10.1007/978-3-662-53015-3_18.

[256] “Veröffentlichung oder Geheimhaltung von Plagiaten und Titelaberkennungen? Zur überholten ‘Amtsverschwiegenheit’ in Österreich,” *DOZ. DR. STEFAN WEBER*, 17 Apr. 2017. https://plagiatsgutachten.com/blog/veroeffentlichung-oder-geheimhaltung-von-plagiat-und-titelaberkennung-zur-ueberholten-amtsverschwiegenheit-in-oesterreich/ (accessed 17 Mar. 2021).

[257] “European Digital Credentials for Learning,” *Europass*. https://europa.eu/europass/en/european-digital-credentials-learning (accessed 13 Apr. 2022).

[258] *eIDAS revision*, 2021/0136 (COD), 03 Jun. 2021. Accessed: 13 Jun. 2021. [Online]. Available: https://ec.europa.eu/newsroom/dae/redirection/document/76608

[259] “The Merge,” *https://ethereum.org/en/upgrades/merge/*. https://ethereum.org (accessed 14 Apr. 2022).

[260] A. Madeira, “The DAO, The Hack, The Soft Fork and The Hard Fork,” *CryptoCompare*, 12 Mar. 2019. https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/ (accessed 05 Jan. 2022).

[261] G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali, and R. Hierons, “Smart contracts vulnerabilities: a call for blockchain software engineering?,” in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, Mar. 2018, pp. 19–25. doi: 10.1109/IWBOSE.2018.8327567.

[262] S. Azzopardi, *smart-contract-versioning*, 2018. Accessed: 05 Jan. 2022. [Online]. Available: https://github.com/shaunazzopardi/smart-contract-versioning

[263] “ERC721 - The NFT Standard - EthHub.” https://docs.ethhub.io/built-on-ethereum/erc-token-standards/erc721/ (accessed 22 Nov. 2021).

[264] AlexWGomezz, “Burning Your NFT: How to, Cost and Purpose.,” *Cyber Scrilla*. https://cyberscrilla.com/burning-your-nft-how-to-cost-and-purpose/ (accessed 22 Nov. 2021).

[265] “EDPB Work Program 2019/2020,” Feb. 2019. Accessed: 29 Dec. 2021. [Online]. Available: https://edpb.europa.eu/sites/default/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf

[266] “EDPB Work Programme 2021/2022.” 2021. Accessed: 29 Dec. 2021. [Online]. Available: https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf