Blockchain for Education: Lifelong Learning Passport

Wolfgang Gräther
Fraunhofer FIT
Sankt Augustin, Germany
graether@fit.fraunhofer.de

Sabine Kolvenbach
Fraunhofer FIT
Sankt Augustin, Germany
kolvenbach@fit.fraunhofer.de

Rudolf Ruland
Fraunhofer FIT
Sankt Augustin, Germany
rudolf.ruland@fit.fraunhofer.de

Julian Schütte
Fraunhofer AISEC
Garching, Germany
schuette@aisec.fraunhofer.de

Christof Ferreira Torres
University of Luxembourg
Luxembourg
christof.torres@uni.lu

Florian Wendland
Fraunhofer AISEC
Garching, Germany
wendland@aisec.fraunhofer.de

ABSTRACT

Certificates play an important role in education and in professional development in companies. Individual learning records become essential for people's professional careers. It is therefore important that these records are stored in long-term available and tamper-proof ledgers. A blockchain records transactions in a verifiable and permanent way, therefore it is very suitable to store fingerprints of certificates or other educational items. Blockchain reveals forgery of certificates and it supports learning histories. In this paper, we present the Blockchain for Education platform as a practical solution for issuing, validating and sharing of certificates. At first, we describe the conceptual system overview and then we present in detail the platform implementation including management of certification authorities and certificates, smart contracts as well as services for certifiers, learners and third parties such as employers. Finally, we describe use cases and first evaluation results that we gathered from end user tests with certifiers and conclude with a discussion.

Author Keywords

Certification, Certificate, Blockchain, Smart Contract, IPFS, BSCW.

ACM Classification Keywords

H.5 Information Systems

INTRODUCTION

In education, certificates confirm the achievement of certain learning outcomes and are until today mostly issued on paper or other physical formats. For example, a learner has participated in an enterprise-training course on usability engineering. After the successful completion of the course, the learner receives the certificate as a paper document that entitles him to use the protected title "Usability engineer with level A". Universities and educational institutions that award degrees to their students also issue many certificates.

Certificates include several statements. The most important are: the kind of qualification or academic title that is attested, the name and address of the issuer organization, the name and signature of the certifier who has validated the facts and is certifying that the qualification is true, the name of the learner and a date of the examination. Depending on the type of certificate, there can be additional statements about the examination regulations, the period of validity or further information necessary to make use of the certificate.

Learners usually receive a paper document that presents the certificate. Using paper certificates has the advantage of being difficult to forge due to built-in security features. In addition, recipients can easily store paper certificates or can show them to any person and for any purpose. However, there are some disadvantages such as the mainly manual activity for third parties to verify the certificate or the need for certification authorities to maintain a registry or database for certificates for a long period of time [1].

An alternative to paper certificates are digital certificates that are cryptographically signed (in the following, we will use the simpler term certificate). Compared to paper certificates, management and use of digital certificates is simplified. However, more effort is needed to secure the registry for certificates and an open standard for digital signatures has to be used, otherwise the global verification of digital certificates is not possible.

In particular, in the area of educational certificates, there exists the severe problem of fake degrees. Ezell and Bear report about fraudulent practices and the billion-dollar industry behind it [2]. Hence, blockchain technology seems ideal to solve many of the above-mentioned problems of current paper or digital certificates and fake degrees.

In the context of education and certification, the blockchain technology supports counterfeit protection of certificates, easy verification of certificates even if the certification authority no longer exists and automation of monitoring processes for certificates with a time-limited validity. When we look at certification processes from a blockchain perspective, we identify three main tasks. Firstly, identities of certification authorities have to be created and maintained.

Gräther, Wolfgang; Kolvenbach, Sabine; Ruland, Rudolf; Schütte, Julian; Torres, Christof; Wendland, Florian (2018): Blockchain for Education: Lifelong Learning Passport. In: W. Prinz & P. Hoschka (Eds.), Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies (ISSN 2510-2591), DOI: 10.18420/blockchain2018_07

Secondly, these certification authorities have to issue certificates to learners and the third main task is the verification of certificates by employers, for example. These three tasks have to be supported adequately by a blockchain-based infrastructure including the sharing of certificates by learners.

The *Blockchain for Education* platform aims to support counterfeit protection as well as secure access and secure management of certificates according to the needs of learners, companies, education institutions and certification authorities. In the next section, we present related work. We then provide an overview of the system including a description of the minimal viable product and the conceptual system architecture. The section prototype implementation explains in detail the management of identities for certification authorities and certifiers as well as the management of certificates represented as extended Open Badges[1]. The description of application portfolios and the verification service complete this section. Use cases and first evaluation results are presented in the next section. Discussion and conclusion sections close this paper.

RELATED WORK

The University of Nicosia was the first higher education institution that stored academic certificates on the Bitcoin blockchain [3,4].

The MIT Media Lab Learning Initiative together with Learning Machine, an enterprise software vendor, has developed Blockcerts, an open-source ecosystem for creating, sharing, and verifying blockchain-based educational certificates. The educational certificates contain basic information such as the name of the recipient, the name of the issuer, an issue date, etc. Note that interoperability with Open Badges assertions is given. Educational certificates are registered on the Bitcoin blockchain, cryptographically signed, and tamper-proof. Blockcerts makes it possible to verify who a certificate was issued to, by whom, and to validate the content of the certificate itself [5,6].

Based on Blockcerts, a pilot for academic and professional certifications will be developed in Malta [7] and the Federation of State Medical Boards in the US is currently launching a pilot for the issuing of official documents with Blockcerts to the blockchain [8].

In July 2017 the company SAP introduced TrueRec a secure and trusted digital wallet for storing professional and academic credentials based on Ethereum. TrueRec was made available to people enrolled in the online course *Touch IoT course for SAP Leonardo*. Over 4500 students will receive and can manage their certificate through TrueRec [9].

TNO, Netherlands Organisation for Applied Scientific Research, started recently the blockchain project *self sovereign identity framework*. This framework is designed to help supply official information in digital form and only share a minimum amount of personal data that is managed and stored in encrypted form in a wallet on one's own cellphone. This information provides official confirmation about the identity of the person [10,11]. Sovrin is another infrastructure that aims to support digital identities on a global scale [12].

Similar to certification is notarization where ownership, existence and integrity of documents is important. The Apostille notarization service and use cases such as car ownership or digital media licenses are described by McDonald and Oliverio [13].

Work related to the design and development of smart contracts in the Blockchain for Education platform is concerned with the correctness of security-relevant Ethereum contracts. Blockchain for Education uses approved smart contract templates of the OpenZeppelin[2] project and extensions of existing code analysis tools like Oyente [14] and Mythril [15].

SYSTEM OVERVIEW

Our system mainly supports certification authorities, learners and employers. It ensures higher efficiency and improved security for certification authorities through digitization of current processes, issuing and registering of certificates in a blockchain as well as automatic monitoring of certificates. To follow the Industry 4.0 approach [16] the platform supports machine-readable certificates. Learners are enabled to manage their certificates and to give access to selected certificates to third parties, i.e. the protection of privacy for leaners is ensured. Trustworthy verification of certificates is offered for employers.

Minimal Viable Product

Several workshops and meetings with our application partners, educational institutions and two personnel certification authorities have been performed to elicit the requirements for our system and to derive the minimal viable product. Starting from the requirements, we conceptualized for each user group features for the minimal viable product.

Features for Certification Authorities

Currently, certification authorities manage data of learners, learning courses and other relevant regulations as well as examination results in their own databases or even MS Excel sheets. This data is used to issue paper certificates for learners. Therefore, the import of data and examination results from legacy systems is a first important feature for certification authorities. After importing the data, certification authorities can browse the generated certificates. In addition, certification authorities need means to search for learners or to gain an overview of learners and their examination results according to learning courses. The overview enables certification authorities to print all

[1] https://openbadges.org/

[2] https://github.com/OpenZeppelin/zeppelin-solidity

certificates of a learning course at once. The second main feature for certification authorities is signing of certificates and storing them into the blockchain. Both actions are easily carried out simultaneously for all the learners in the previously mentioned overview.

Acknowledgement of validity and authenticity of a certain certificate is a further feature for all user groups of the minimal viable product. Furthermore, certification authorities need a means to revoke certificates. This could be necessary when plagiarism has been detected or misconduct of the certified learner was proven. Usually revocation occurs mainly for certificates with time-limited validity when the necessary actions have not been taken.

Features for Learners

At present, learners mostly receive paper certificates with built-in security features. Learners send or email copies or certified copies, sometimes digitized (scanned), to prospective employers. Hence, the importing of certificates and creation of an application portfolio is a major feature for the minimal viable product. Furthermore, learners need means to manage application portfolios as well as means for sharing them.

After sharing application portfolios learners are supported with information about employer's activities on their certificates such as reading or verifying, i.e. notifications for learners are a further feature of the minimal viable product. Similarly, monitoring of certificates with a time-limited validity support learners and is an additional feature of the minimal viable product. Note, that monitoring is also relevant for certification authorities but implies different actions. Certification authorities could remind learners and revoke certificates, if the conditions for renewal are not met.

Features for Employers

Currently, employers only receive copies, sometimes notarized copies, of the learner's paper certificates. In the first case, employers can proof the validity of the copies only by asking the issuing organization for the authenticity and validity of the certificate. This is a time-consuming and expensive process. Therefore, reading and verifying certificates is an important feature of the minimal viable product.

The derived features for certification authorities, learners and employers have been exploited to develop the conceptual system architecture. This process was supported by the use case canvas for blockchain described in [17] and the engineering framework presented in [18].

Conceptual System Architecture

An overview of the prototype architecture is shown in Figure 1. It comprises the blockchain including smart contracts, a public storage holding profile information of certification authorities, a document management system managing the actual payload of certificates tracked by the blockchain and the parties involved in the system, namely accreditation and certification authorities, certifiers, learners and employers. In the prototype implementation, only the document management system is a centralized system component.

Bootstrapping the Platform

Initially, two smart contracts are submitted to the blockchain by the accreditation authority (1). The first smart contract (IdentityMgmt) supports management of identities in the Blockchain for Education platform and the second one (CertMgmt) manages the lifecycle of certificates issued over the blockchain. Once the contracts are deployed (2a), it is the accreditation authority's task to register the public keys of certification authorities as legitimate issuer of certifiers in the IdentityMgmt contract (3a) and to submit public and non-personal profile information to the public storage (2b). It is important to note that the profile information is read-only and publicly readable, i.e. it is not subject to the access control mechanisms of the IdentityMgmt contract. It merely holds long-time profiles of certification authorities, such as their name and country, but does not include any personal information of certifiers or even learners.

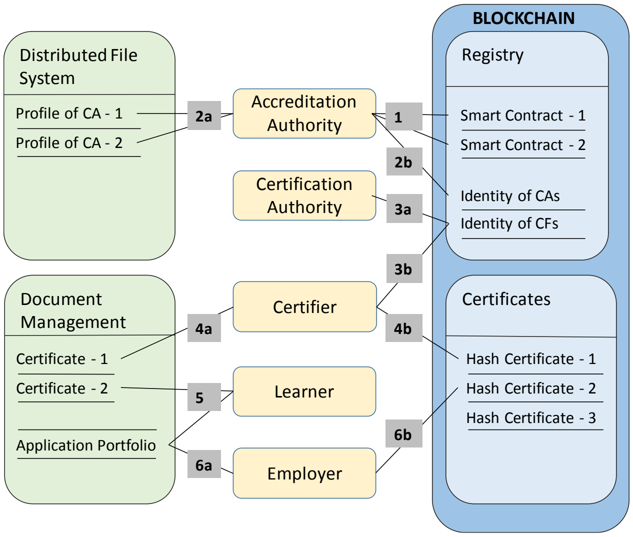


Figure 1: Conceptual Architecture

Registered certification authorities then add the public keys of certifiers to the registry of the IdentityMgmt contract (3b) and thereby delegate the right to issue certificates. That is, a holder of a private certifier key will typically be an employee of a certification authority who is entitled to issue certificates and signs them in the name of the certification authority.

Issuing Certificates

The certifier collects all information a certificate consists of. The dataset comprises qualification or title, name and address of the certification authority, name of the certifier, name of the learner, and the date. Then the certificate is signed by the certifier and stored on the document management system (4a) and its fingerprint is written to the blockchain (4b).

Creation and management of application portfolios

Learners are supported in the creation and management of application portfolios by a service of the document management system. Firstly, the learner has to register with the document management system. Then, a service for the flexible creation of application portfolios supports the learner (5). Completed application portfolios can be shared with potential employers who can verify the validity of these certificates.

Verifying Certificates

A service of the minimal viable product supports employers, for example, in verifying single certificates or all certificates of an application portfolio (6a, 6b).

PROTOTYPE IMPLEMENTATION

We implemented a prototype of the Blockchain for Education platform based on the Ethereum blockchain[3]. Two smart contracts written in Solidity[4] codify access control mechanisms (IdentityMgmt) and manage certificate records (CertMgmt) stored in the blockchain. The Interplanetary Filesystem[5] (IPFS) is used as a public distributed read-only storage for profile information of certification authorities. Finally, the BSCW document management system stores and validate certificates.

Identity Hierarchy and Rights Delegation

Identities in Blockchain for Education are managed in a hierarchy. On top is a set of accreditation authorities who are entitled to approve certification authorities. For instance, members of the European Co-operation for Accreditation could build the set of accreditation authorities in the Blockchain for Education platform. In Figure 2, we summarize the whole set of accreditation authorities to a single authority for the sake of simplicity and to reflect the current prototype setup. An accreditation authority is the owner of the smart contracts of an instance of the Blockchain for Education platform. It creates the initial smart contracts on the Ethereum blockchain. The IdentityMgmt contract allows accreditation authorities to create, update and remove certification authorities.

Certification authorities reside one level below accreditation authorities in the identity hierarchy. They are identified by their Ethereum address, which is derived from a cryptographic hash of their public keys. The address of a certification authority is mapped to its profile information stored on IPFS. Certification authorities cannot issue certificates themselves. They can only entitle employees by delegating the respective right to them. To do so, a certification authority calls the respective function of the IdentityMgmt contract and passes in the Ethereum address of its certifier. The smart contract ensures that only accredited certification authorities may delegate the right and automatically assigns the certifier to the delegating certification authority. Just as the right to issue certificates can be issued at any time to any certifier, it can also be revoked by the certification authority. This deauthorization could for example occur if a certifier leaves a certification authority or should otherwise loose the right to issue further certificates.

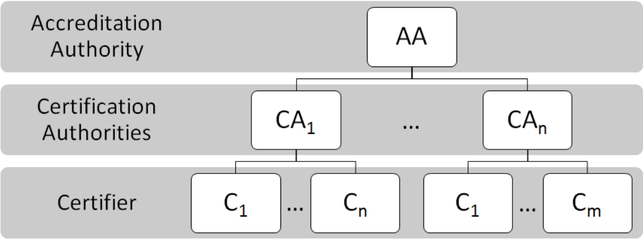


Figure 2: Identity hierarchy

Certifiers cannot delegate their rights further and cannot manipulate the access permissions. The role of certifiers is limited to the management of certificate records on the blockchain.

Certificate Management

Certifiers can create, revoke and delete references to certificates stored in the Blockchain for Education platform. This is implemented in the smart contract CertMgmt.

The accreditation authority instantiates the CertMgmt contract together with the IdentityMgmt contract. The CertMgmt contract requires the address of the IdentityMgmt contract to enforce access control. Any manipulative operation on the CertMgmt contract, such as adding a certificate, requires that the caller is a registered certifier of an accredited certification authority. Everyone can retrieve certificate records given the address of the CertMgmt contract and a hash of the certificate.

The CertMgmt contract uses certificate records to store certificate information in the blockchain. Currently, this information consists of the SHA256 hash of the certificate, the starting and expiration date and a status field (onHold) to indicate if a certificate is on hold. Dates are represented as UNIX timestamps and for future proofing, are stored as 256-bit unsigned integers. Similarly, the onHold status field stores a UNIX timestamp if a certificate is on hold. Thus, one can check when the onHold status was set for a certificate.

[3] https://ethereum.org/

[4] https://solidity.readthedocs.io/en/latest/index.html

[5] https://ipfs.io/

IPFS as a Public Tamper-Proof Read-Only Profile Storage

On the Ethereum blockchain, entities such as accreditation authority, certification authorities and certifiers are identified by their Ethereum addresses, i.e. a hash of their public keys. This provides anonymity and protects personal information, especially of the certifiers, as it is not easily possible to correlate an Ethereum address to a real person.

Certification authorities, however, must provide identifiable profile information to allow anybody who is verifying a certificate to verify the certification authority as well. Without this profile information, certifications would remain completely anonymous and consequently not suited to build a well-reputed track record for a learner. Therefore, every certification authority must provide an IPFS address where interested parties can look up the profile.

This is not only a requirement resulting from the European General Data Protection Regulation which objects any undeletable storage of personal information in a blockchain, but also an important feature for certification authorities who do not want to reveal personal information of their employees to competing authorities. In addition, actual storage on the blockchain is comparatively expensive. Therefore, profiles of certificate authorities are stored on the IPFS.

IPFS provides temper-proof, secure and distributed storage. The massively distributed block storage addresses entries by their hashes stored as a Merkle tree. The specifics of IPFS are abstracted away by numerous clients for different programing languages that let client programs access IPFS as any other block storage. Whenever an accreditation authority registers a new certification authority, it will first write the certification authority's profile information into IPFS and then submit the certification authority's public key and the IPFS address to the IdentityMgmt's registry. Afterwards, both the Ethereum transaction and the IPFS block with the profile information synchronized across all nodes in the network. It is thus the accreditation authority's responsibility to ensure that it does not register fake profiles and must validate profile information of certificate authorities before they are added to the blockchain.

The use of IPFS in the Blockchain for Education platform provides two advantages. First, no personal data is stored on the blockchain while providing proof of authenticity resulting from the immutable IPFS addresses. This allows the use of Blockchain for Education in fulfillment of data protection laws. For example, the European General Data Protection Regulation (GDPR) would in general object to any undeletable storage of personal information in a blockchain. Second, storing the profile information of certification authorities externally in an immutable way saves storage on the blockchain.

Certificates as Extended Open Badges

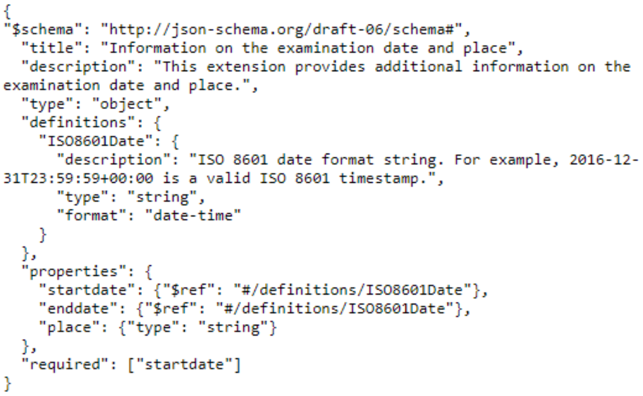
To digitize certificates we decided to represent certificates in JSON data format, compatible to Open Badges. According to the requirements of our application partners and our personnel certification authority, we extended the standard Open Badges schema by six additions. These are: unique id of the certificate, examination date and place, examination regulations in force, data about the certifier, data about the certificate recipient and the address of the trusted service that is offered to verify the certificate.

Unique Certification ID

This schema extension adds the property *assertionreference* of type *string* to our schema. Our personnel certification authority required this unique ID for legal reasons.

Examination Date and Place

Figure 3 shows the schema extension. The properties *startdate*, *enddate*, and *place* all of type *string* have been defined. The dates are formatted according to the ISO 8601 date definition. This schema extension is a prime example for all our other extensions.



```
{
"$schema": "http://json-schema.org/draft-06/schema#",
  "title": "Information on the examination date and place",
  "description": "This extension provides additional information on the
examination date and place.",
  "type": "object",
  "definitions": {
    "ISO8601Date": {
      "description": "ISO 8601 date format string. For example, 2016-12-
31T23:59:59+00:00 is a valid ISO 8601 timestamp.",
      "type": "string",
      "format": "date-time"
    }
  },
  "properties": {
    "startdate": {"$ref": "#/definitions/ISO8601Date"},
    "enddate": {"$ref": "#/definitions/ISO8601Date"},
    "place": {"type": "string"}
  },
  "required": ["startdate"]
}
```

Figure 3: Schema Extension for Examination

Examination Regulations in Force

This schema extension mainly adds the properties *title*, *url*, *regulationsid*, and *date* of the regulation to our schema.

Certifier

The properties *givenname*, *surname*, *certificationdate*, *certificationplace* and blockchain *address* are defined and added to our schema.

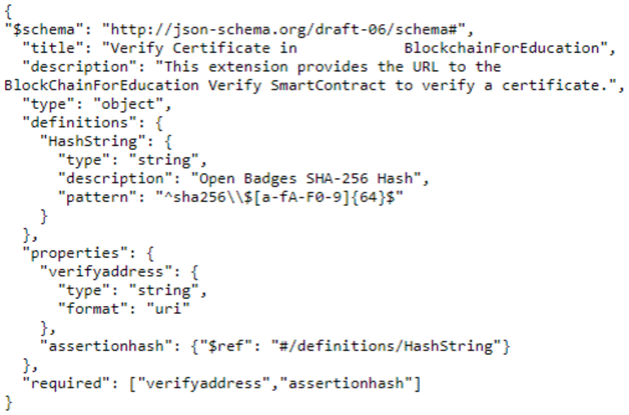
Certificate Holder

This schema extension adds the properties *givenname*, *surname*, *birthdate*, *birthplace*, and *email* to our schema.

Verify

Figure **4** shows the schema extension in detail. The properties *verifyaddress* and *assertionhash* have been defined. These properties allow third parties to implement their own verification service.

We used the validator service of the IMS Global Learning Consortium to verify our extended Open Badges certificates: Our certificates are valid in compliance with Open Badges 2.0.



```
{
"$schema": "http://json-schema.org/draft-06/schema#",
  "title": "Verify Certificate in           BlockchainForEducation",
  "description": "This extension provides the URL to the
BlockChainForEducation Verify SmartContract to verify a certificate.",
  "type": "object",
  "definitions": {
    "HashString": {
      "type": "string",
      "description": "Open Badges SHA-256 Hash",
      "pattern": "^sha256\\$[a-fA-F0-9]{64}$"
    }
  },
  "properties": {
    "verifyaddress": {
      "type": "string",
      "format": "uri"
    },
    "assertionhash": {"$ref": "#/definitions/HashString"}
  },
  "required": ["verifyaddress","assertionhash"]
}
```

Figure 4: Schema Extension for Verification

Managing Certificates in BSCW

BSCW is a Web-based groupware system [9] that is used in the context of the blockchain for Education project to store learning courses, data about participants and examination results. The import of data from legacy systems is supported by a service specially implemented for the blockchain for education project. Certification authorities import their data for a specific learning course, which results in a folder that contains generated certificates. A screenshot is shown in Figure 5.

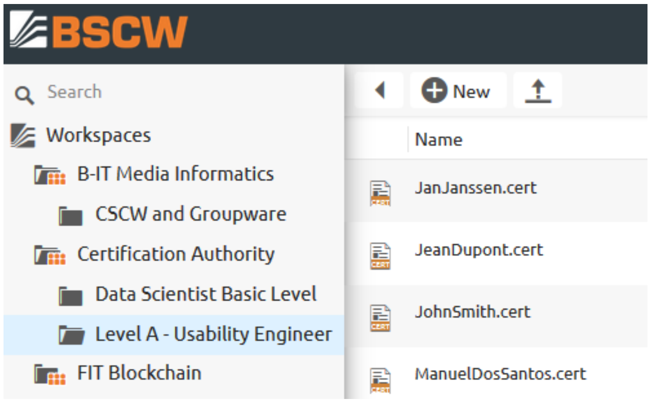


Figure 5: Personnel Certification Authority and List of Certificates

On the left hand side, Figure 5 shows a folder hierarchy. The folder named *Certification Authority* contains two folders for learning courses that contain for each learner, who has successfully finished the examination, the certificate in our extended Open Badge format. The folder *Level A - Usability Engineer* has been selected. Therefore, the respective certificates are presented on the right hand side of Figure 5. If certifiers click on a certificate, then a preview of the certificate is shown.

Send to Blockchain

After importing and previewing the certificates, the certifier can sign the certificates and write the certificates to the blockchain. This activity is carried out by the operation *send to blockchain*. Figure 6 shows this operation for the certificate *JanJanssen.cert*. If the operation could be executed, then the certifier is notified by a popup note that the certificate has been successfully written to the blockchain. Note, that only the fingerprint of the certificate and a few additional attributes are stored in the blockchain. The attribute *status* has by default the value valid, but it could be set to *on hold* or *invalid*. The attribute issuer contains the identity of the issuer of the certificate. A further attribute is the *issue date*. By default, the validity of certificates is not limited. In case of time-limited certificates, the attribute *expiration date* is set accordingly.

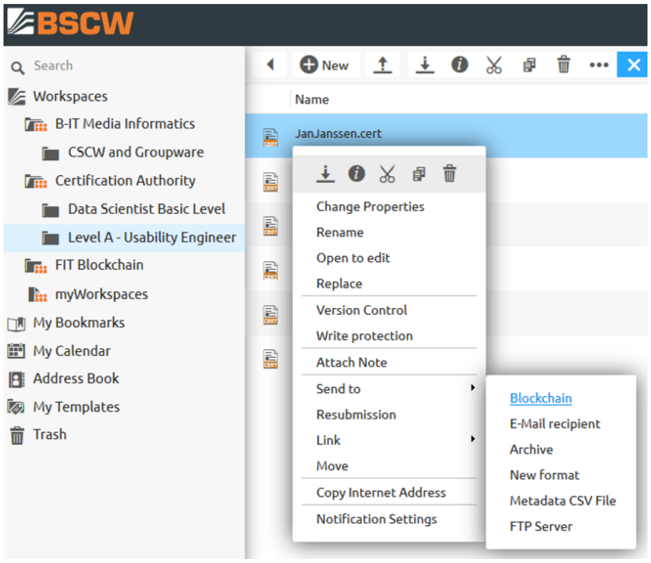


Figure 6: Write Fingerprint of Certificate to Blockchain

Sharing Certificates with Learners

After sending to the blockchain, the certifiers send learners their certificates in two formats: firstly, as encoded JSON file and secondly, as PDF document. Learners should then store the files safely in their personal archives. Note, that the PDF document contains as meta data the serialised JSON string of the certificate.

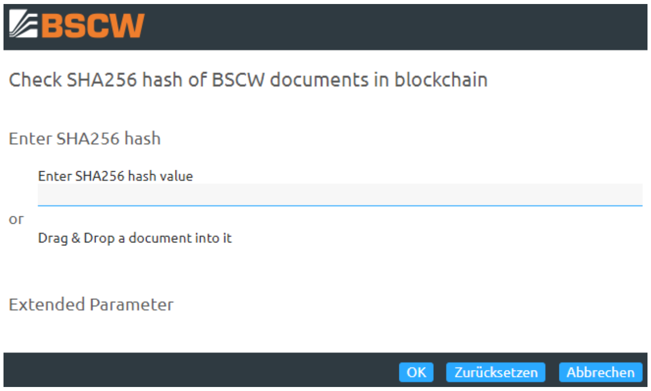
Application Portfolios in BSCW

Learners can self-register with BSCW, import their certificates into their personal folder and create different application portfolios adjusted to the respective employers. Application portfolios are mapped to folders in BSCW and structured in a two level hierarchy. The single folders contain the certificates in PDF format. The learner can share the application folder with a potential employer and the employer can verify the received certificates.

Verification of Certificates

For the trusted verification of certificates at hand, we have realized our own verification service. It is a free service offered on the landing page of the Blockchain for Education platform.

Users just drag and drop certificates, JSON or PDF documents are accepted, onto the service, which verifies the existence of the fingerprint of the certificate in the blockchain. As result not only true or false is presented, but also information about the registered issuer (if it is a registered certification authority) and for the certificate the values of the attributes status, issuer, issue date and if set validity. Figure 7 presents the user interface of the verification service.



Check SHA256 hash of BSCW documents in blockchain

Enter SHA256 hash

Enter SHA256 hash value

or

Drag & Drop a document into it

Extended Parameter

Figure 7: User Interface of Verification Service

USE CASES

The blockchain for Education platform enables tamper-proof archiving of certificates and their correct and permanent allocation to learners, as well as verification of certificates. In addition, three different scenarios are mainly supported. In the first scenario, a learner is interested in creating an application portfolio that contains selected certificates. The underlying groupware BSCW allows the creation of application portfolios. The learner adds the documents necessary for the application to the respective portfolio and share it with a potential employer. The employer can then verify the contained certificates by using the platform's verification service or other verification services that could cope with our extended Open Badges and that could call the specified smart contract.

In a second scenario, a learner has successfully passed an examination for a basic course on usability engineering. Later the learner took an additional qualification course on interaction and information design. After successfully passing this course, the learner automatically receives the qualification *senior usability engineer*. A smart contract is used to determine this new qualification. In a third scenario, a self-employed person presents *master craftsman in the area of high quality fitting* as professional qualification on the Web. Potential customers can verify the validity of the qualification as well as the issuing certification authority using a verification service.

Evaluation

The Blockchain for Education platform was developed in an iterative way with the participation of potential end users. A first version of the minimal viable product was intensively discussed with our personnel certification authority. This version contained already features for issuing and managing certificates. However, revocation of certificates was not foreseen and therefore introduced as an additional feature of the minimal viable product. In addition, our discussions with the personnel certification authority led to further smaller revisions and redesigns.

After internal testing, a workshop with a large German technical inspection association was organized to evaluate appropriateness of the Blockchain for Education platform for their certification authority. The workshop participants received a comprehensive presentation of the minimal viable product including the technical concepts and a demonstration of the prototypical platform was conducted. In the discussion, the participating certifiers confirmed our approach and were interested to use our platform for their certification processes. However, a few platform extensions will be necessary that primarily target import of examination results and specific extensions to our Open Badges schema. Issuing, validation and sharing of certificates remain almost unchanged.

DISCUSSION

Although certificates are currently issued as paper documents, we believe that there will be more digital certificates issued in the future. The usage of blockchain technology as presented in our paper has main advantages for digital certificates. Firstly, there is the decentralized immutable storage of digital certificates. Secondly, there is a verification service that allows third parties to verify easily the authenticity of certificates. Lastly, there are the identities of certification authorities and certifiers immutably stored in the blockchain. A non-blockchain platform that wanted to achieve counterfeit protection would have to implement appropriate services, especially services for digital signatures [20].

Certificates in the Blockchain for Education platform are represented according to the Mozilla Open Badges specification that became a quasi-standard. It is widely used and has the advantage, that its schema could be extended. There are a vast amount of APIs and tools available to create, manage or verify Open Badges.

A comparison of the Blockchain for Education platform with Blockcerts is especially interesting since it also supports certification processes based on blockchain technology. Blockcerts uses the Bitcoin platform and therefore cannot specify complex smart contracts. The Blockchain for Education platform employs smart contracts for the management of identities such as certification authorities or certifiers and for managing the lifecycle of certificates. In contrast to Blockcerts, our revocation model does not allow to show or validate revoked certificates. Other differences are mentioned in the next subsection on security and privacy.

Security and Privacy challenges

The Blockchain for Education platform tackles security and privacy challenges that have not been solved before. For instance, in contrast to the Blockcerts system, the hierarchical organization of identities, in the Blockchain for Education platform allows the actual certifiers to remain anonymous while still proving that they belong to an accredited certification authority. The security of the Blockchain for Education smart contracts is based on approved templates from the OpenZeppelin collection and undergoes verification with *Osiris*, an extension of the Oyente symbolic execution tool we developed to discover integer over- and underflows. We implement safeguards to suspend the smart contracts of an Education for Blockchain instance in case of discovered vulnerabilities. This prevents future manipulation of the stored records while maintaining read-only access. For future iterations, we consider implementing an update mechanism for our smart contracts. This would allow us to patch vulnerabilities. Moreover, we are developing a privacy-preserving storage of personal information in an append-only public ledger with the help of advanced cryptographic protocols.

Limitations and Future Work

The Blockchain for Education platform is currently in a prototype state and can be extended and optimized in different aspects. First, the identity scheme is strictly hierarchical with the accreditation authority as a single powerful root node. In case the accreditation authority's private key is compromised or lost, the whole system is affected. In our future work, we will introduce a multisignature scheme for the accreditation authority where the power of a single private key is distributed to *k* out of *n* members which can act together as the accreditation authority – for example a number of national members of European Co-operation for Accreditation.

Further, as the system runs on the Ethereum blockchain, it introduces monetary overhead. For instance, adding a certificate to the blockchain implies transaction costs, which must be paid by the certifier. In a future version, a certifier might issue a pre-signed raw transaction to a proxy of the certification authority, which will refund the certifier and submit the transaction to the blockchain.

ACKNOWLEDGEMENT

We would like to thank all members of the Blockchain for Education project team for their support. We also gratefully acknowledge the insights from external application partners, educational institutions and certification authorities.

REFERENCES

1. Alexander Grech and Anthony F. Camilleri. 2017. *Blockchain in Education*. No. JRC108255. Joint Research Centre (Seville site).
2. Allen Ezell and John Bear. 2005. *Degree mills: The billion-dollar industry that has sold over a million fake diplomas*. Pyr Books.
3. BlockCerts to be developed in Malta. Retrieved March 12, 2018 from http://www.educationmalta.org/blockcerts -to-be-developed-in-malta/
4. Mike Sharples et al. 2016. Innovating pedagogy 2016: Open University innovation report 5.
5. Digital Certificates Project. Retrieved October 10, 2017 from http://certificates.media.mit.edu/
6. Certificates, Reputation, and the Blockchain – MIT MEDIA LAB. Retrieved October 10, 2017 from http://certificates.media.mit.edu/
7. Case Study Malta|Learning Machine. Retrieved March 12, 2018 from https://www.learningmachine.com/case-studies-malta
8. Case Study FSMB|Learning Machine. Retrieved March 12, 2018 from https://www.learningmachine.com/case-studies-fsmb
9. Meet TrueRec by SAP: Trusted Digital Credentials Powered by Blockchain. Retrieved March 22, 2018 from https://news.sap.com/meet-truerec-by-sap-trusted-digital-credentials-powered-by-blockchain/
10. Self-sovereign identity framework. Retrieved March 22, 2018 from https://www.techruption.org/usecase/xxcvxcvxcv/
11. Saving millions and increase privacy with blockchain. Retrieved March 22, 2018 from https://www.techruption.org/savings-millions-privacy-blockchain/
12. Sovrin-Protocol-and-Token-White-Paper.pdf. Retrieved March 22, 2018 from https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf
13. Apostille White Paper. Retrieved March 22, 2018 from https://nem.io/wp-content/themes/nem/files/ApostilleWhitePaper.pdf
14. Luu, Loi, et al. 2016. "Making smart contracts smarter." *Proceedings of the 2016 ACM SIGSAC Conference*. ACM.
15. Security analysis tool for Ethereum smart contracts. https://github.com/ConsenSys/mythril
16. Industry 4.0. Retrieved March 31, 2018 from https://en.wikipedia.org/wiki/Industry_4.0
17. Sandra Klein, Wolfgang Prinz, and Wolfgang Gräther. 2018. A Use Case Identification Framework and Use Case Canvas for identifying and exploring relevant Blockchain opportunities. DOI: 10.18420/blockchain2018_02
18. Thomas Osterland and Thomas Rose. 2018. Engineering Sustainable Blockchain Applications. DOI: 10.18420/blockchain2018_05
19. Wolfgang Appelt. 2001. What groupware functionality do users really use? Analysis of the usage of the BSCW system. IEEE.
20. Clemens Brummer. 2017. Eduthereum – A system for storing educational certificates in a public blockchain. Unpublished master thesis, University of Innsbruck.