Case study

Cert4Trust

Cert4Trust offers a seamless end-to-end solution for digital certificates ensuring tamper-proof handling and trustworthy validation. The security of the system is guaranteed by using Blockchain technology and a micro-service architecture. The IHK for Munich and Upper Bavaria mainly developed this innovative product, from the early ideas and a proof of concept to a productive solution.

"Blockchain technology as a distributed and transparent database is a perfect frame-work for the Digital Transformation of Germany's federal system. Together with our partners we aim to make fully digital application processes, i.e. at universities or voca-tional schools, possible without the need for an attested paper copy." - **Armin Barbalata, Managing Director Digital transformation & IT services at IHK Munich and Upper Bavaria.**

- **Client: IHK for Munich and Upper Bavaria -** the IHK for Munich and Upper Bavaria is the biggest chamber of commerce and industry in Germany having about 390.000 member companies. The IHK is also one of the biggest corporate networks in Europe**.**
- **Contractor: j-labs software specialists** - Polish software company which provides complete development teams, individual engineers and outsourcing of whole projects in agile models in the field of software development. Currently the company has 350 engineers who support 40 various international companies mostly from Germany/Nordics and USA.
- **Product:** Cert4Trust / Certificate Blockchain
- **Industry:** Goverment
- **Goal:** Make possible to validate a digital document in terms of issuer, content and validity in an easy, fast and unequivocal way.

Challenges

1. Certificates are currently mainly issued on paper;
    - It takes time to produce and deliver a paper certificate
    - Paper can be lost / destroyed
    - Paper certificates can be easily forged
    - Application processes are mainly fully digital processes

2. When paper certificates are digitized, the integrity of the documents cannot be guaran-teed as no digital verification process exists.
3. IIt is not possible to "invalidate" existing paper or digital documents, once issued the is-suing authority cannot ensure the return of the certificate. The owner can therefore con-tinue to present the certificate even after invalidation.


Industrie- und Handelskammer Aachen

PRÜFUNGSZEUGNIS

nach § 37 Berufsbildungsgesetz

Michael Mustermann

geboren am 22.05.1988 in Berlin

hat die Abschlussprüfung in dem staatlich anerkannten Ausbildungsberuf

Steuerberater

mit der **Gesamtnote befriedigend (79 Punkte)** bestanden

Schriftliche Prüfung	**Note**	**Punkte**
Bürowirtschaft	ausreichend	(63)
Rechnungswesen	ausreichend	(63)
Wirtschafts- und Sozialkunde	sehr gut	(92)
Praktische Prüfung		
Auftragsbearbeitung und Büroorganisation	sehr gut	(93)
Informationsverarbeitung	gut	(82)

Von der Berufschule erteilte Note: **befriedigend (2,6)**

Aachen, 20 Februar 2016

Präsident
Dr. Herbert Reimann

Hauptgeschäftsführer
Andreas Richter

MUSTER

The challenge is about the digitalization of work traditionally done manually, and replacing the paperwork with an electronically signed documents.

The system created has to work on a massive scale, allowing multiple further institutions to join and provide secure way of proof-checking the certificates.

Project scope in a nutshell

The idea of the project is that the certificate issuer (i.e. IHK, HWK, schools) issues a digital version of the certificate as well as a paper version. The document should be ar-chived by the issuer and made available to the graduate through a download portal.

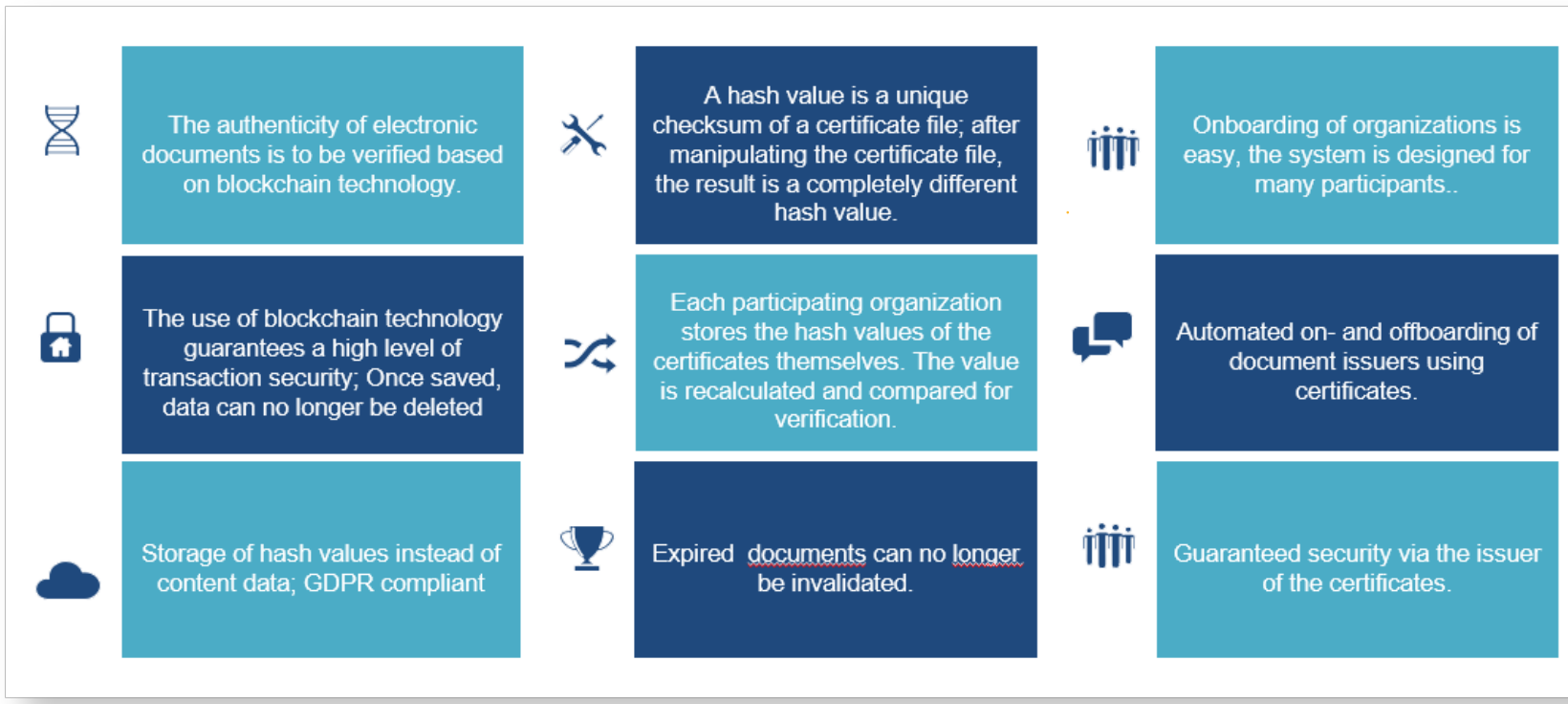
The hash value (sha3-256) calculated for each file, is stored in a Blockchain Smart Con-tract using an API. The use of Blockchain technology guarantees a high level of securi-ty. Once saved, data can no longer be modified or deleted.

Certificate validity can be checked by calculating the hash value again and comparing it with the values stored. An easy-to-use web application is available online to check certif-icates.

If a document becomes invalid, it can be marked as such. As no personal data is stored or revealed, the approach is GDPR compliant.

By design, multiple organizations can be on-boarded easily. On- and off-boarding is au-tomated using SSL certificates.

The Cert4Trust project uses its own Blockchain network built on Ethereum technology. Validator nodes are owned by German public institutions only, adding an extra level of trust to the system.



"The main challenge of the project was to design a complete and future-proof distributed system including our own Blockchain infrastructure. The code quality is exceptionally high. To achieve this goal we did a bunch of quality insurance measures. These activities ensures that the system fulfils high security and non-functional requirements. We are proud that central parts of the developed software are available as open source under MIT licence. This enhances the most important value of the system: trust." - **Markus Sprunck, Senior IT Architect at IHK Munchen.**

Smart Contracts

A smart contract is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or realization of a contract or any predefined process. Smart Contracts make credible transactions possible without third parties. These transactions are trackable and irreversible.

The Cert4Trust project uses Smart Contracts to store hash values in the Blockchain thereby establishing an unbreakable link between issuer and document. The contract receives a hash value and stores it in the Blockchain as an immutable value. Later on, users can get this hash value, and compare the value with their own generated value of a certificate copy they have received from another party. Moreover, Smart Contracts are designed in a way that allows changing the status of a certificate by

- Amending the certificate, e.g. changing its date of validity
- Invalidating or revoking the certificate

Each institution is the owner of its contract instances and has at least one in operation.
The contract owner is identified by signing the contract using a public SSL certificate from the matching organization-webpage.

Team and workflow

The Team consiststed of:

- **Project Manager** (IHK)
- **Lead IT Architect** (IHK)
- **2 backend and 2 frontend engineers** (j-labs software specialist)
- several other **specialists for Blockchain, security, UX design and testing**

The team worked together remotely – people involved worked in different locations. The work process was based on SCRUM using a Kanban board in Atlassian Jira. Standups were held twice a week; technical details and ideas were shared with engineers working in another IHK project in regular cross-team meetings. Releases were planned in 1-month intervals.

"It has been a great and positive challenge to support IHK in their new initiative. The Blockchain technology is just tailored to the project needs and perfectly resolves the problem of document validation. It also clears the path for many Blockchain solutions on the market. Thanks to the IHK Managers and the trust they put into our cooperation, our engineers were able to create real innovation. I am proud to say that as I say this, a new significant milestone is being achieved and the road further on is even more exciting" - **Marek Guzowski, Delivery Manager at j-labs software specialists.**

Technologies

- Java 11
- Ethereum (web3j)
- Truffle
- Ganache
- Spring Boot
- Keykloak
- Angular 10
- OpenShift\s2i
- Docker
- Ansible
- Vagrant &Terraform

Ethereum Blockchain Networks:

Ethereum is the second-largest public Blockchain network after Bitcoin. The concept of Smart Contracts was introduced by Ethereum in a public Blockchain. Ethereum is also very often used a consortium or private as well as public Blockchain with permissioned validator node access. Very good tools are available for development. Libraries and templates alreadyexist for many applications, which have been checked for security aspects by a large number of experts.

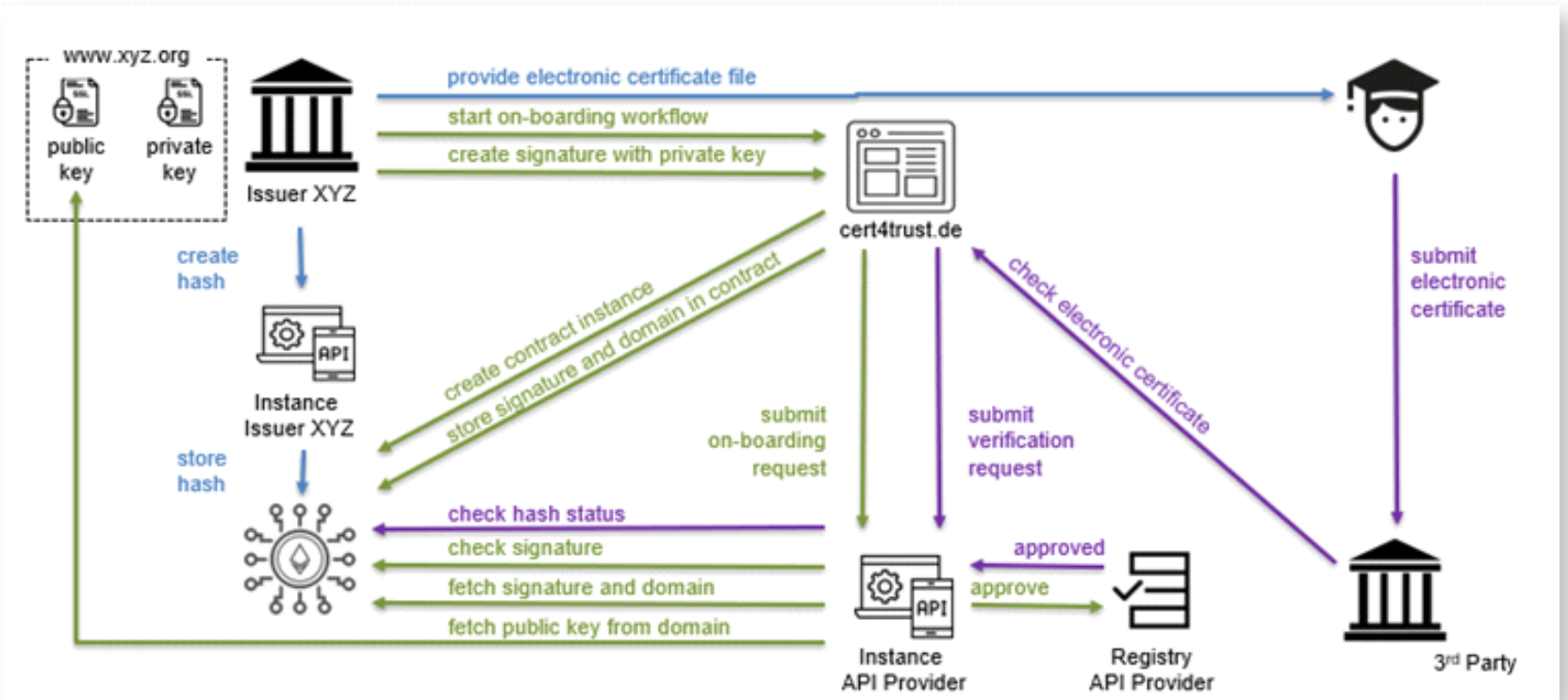
Hash values:

A hash value is a unique checksum of any file and can be recalculated anytime using a simple algorithm; after manipulating the file, the resulting hash value is completely different.

> *The use of Blockchain technology guarantees a high level of transaction security and perfectly resolves the problem of document validation.*

Functionalities

Interaction between parties are shown below:



1. **Application & validation process** (print in lilac)
2. **Storage process** (print in blue)
3. **Onboarding process** (print in green)

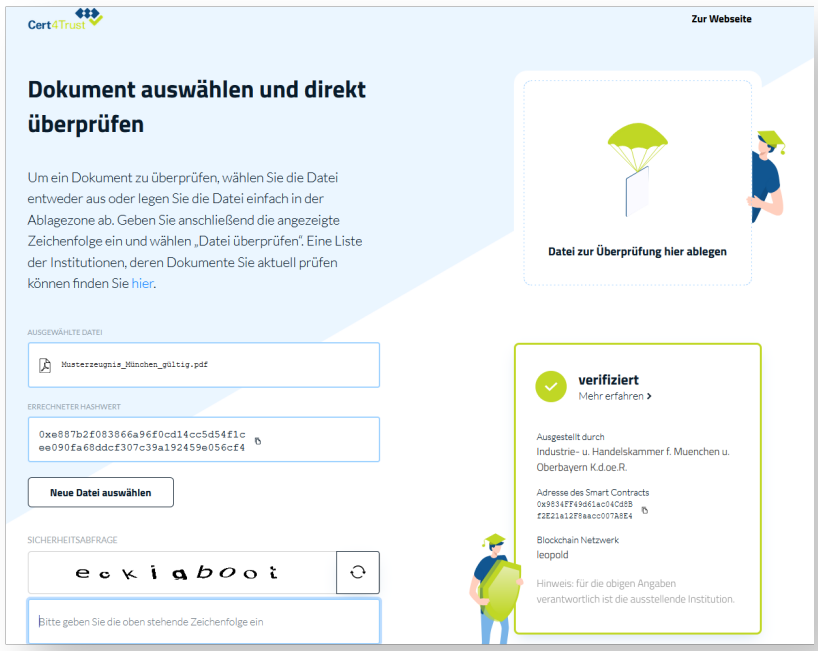
Current status and plans

Cert4Trust is a joint project of the Chamber of Industry and Commerce for Munich and Upper Bavaria (IHK), the Chamber of Crafts and Trades for Munich and Upper Bavaria (HWK), the City of Munich and the Bavarian Digital State Ministry. The partners work together to further improve the product and to move political and legal barriers.

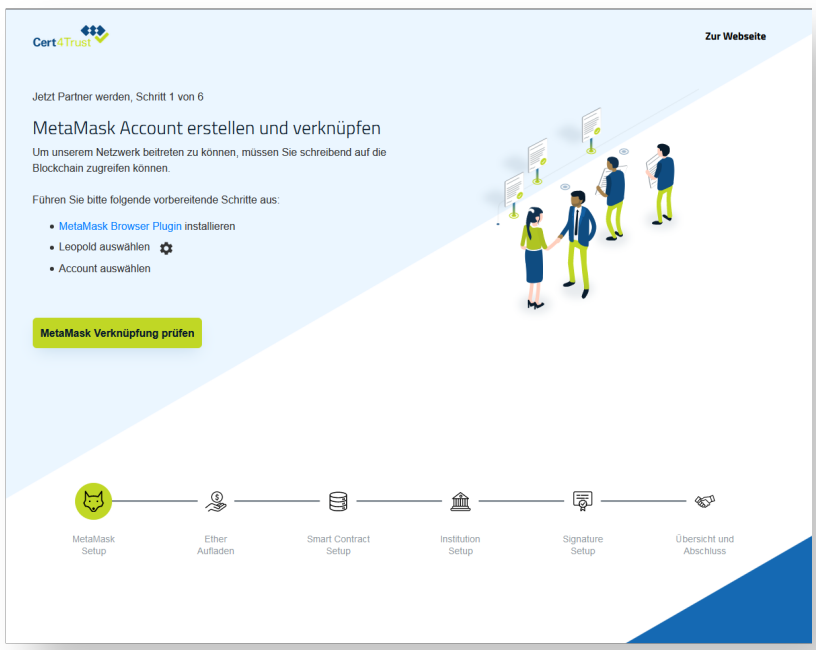
The designed application to validate certificates can be found online (https://check.cert4trust.de) and further information on the project and all parties involved is available online as well (www.cert4trust.de). As a proof-of concept, around 15.000 certificates were processed in spring 2020. Since summer 2020 the full IT solution is in productive use and fully integrated in the systems of IHK Munich.

1. Main page

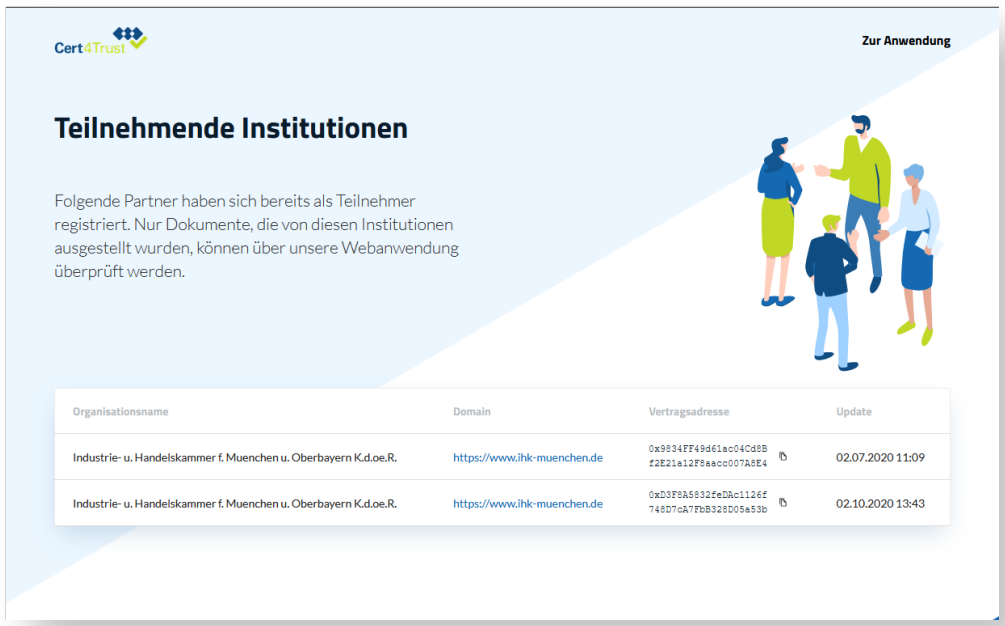
2. Document Verification



3. Registration of the institution in the blockchain



4. The list of registered and accepted institutions



IHK München und Oberbayern

IHK München und Oberbayern
www.ihk-muenchen.de

j·labs software specialists

j-labs GmbH
hello@jlabs.com
www.sdc.j-labs.com