NExT BiVD

ANNOUNCEMENT
WHITE PAPER

MARCH 2019

NExT

VITAKO

regio iT

BLOCKCHAIN BUNDESVERBAND

Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

LEGAL TECH CENTER

Bundesamt für Migration und Flüchtlinge

Fraunhofer FIT

Projektgruppe Wirtschaftsinformatik

GOAL

Announcement of BiVD's blockchain white paper

The forthcoming white paper of the initiative "Blockchain in der Verwaltung Deutschland (BiVD)" and Next Network present the most important organizational, technical and legal questions that have to be answered in order to develop future blockchain solutions for public administration. This position paper follows a "Green Field" approach and is the first in a series of blockchain white papers by the BiVD.

WHITE PAPER TABLE OF CONTENTS

03
White paper table of contents

04
Values and principles framework

05
Special features of blockchain technology Properties and added values

06
Fields of application in the public administration

08
Questions: Organisational Technical Legal

11
Who are we & time schedule

At the beginning, the white paper outlines the general framework of values and principles in which IT infrastructures for the German administration must be embedded.

Subsequently, the technical peculiarities and value-adding properties of blockchain technology for public administration are outlined and discussed against the background of the framework introduced at the beginning.

In the third section, important potential application areas of blockchain technology in public administration are presented. These application areas are based on the experience of the BiVD partners and on the results of European working groups.

In the fourth section, the white paper raises organizational, technical and legal questions, which have to be addressed before a blockchain infrastructure can be created in the German administration. In addition, specific requirements are derived from these questions.

Finally, the paper outlines a roadmap for the in-depth investigation of the issues within the framework of a white paper series by the BiVD.

FRAMEWORK OF VALUES AND PRINCIPLES

The security, integrity and authenticity of data forms the cornerstone of a successful digital transformation in Germany and Europe. At the same time, the lessons learned from digitisation to date show us that the question of how IT infrastructures are set up and operated is always crucial. The framework of values and principles that the Basic Law provides us with must also be reflected at the technical level.

At present, many IT systems used by different authorities require the centralisation of geographically fragmented databases. However, this centralisation entails the risk that the state might be able to monitor citizens and that hackers might be attacked by a large number of people. Blockchain technology breaks with this pattern: the technology enables the establishment and operation of a decentralized, federal IT infrastructure in which data remains under the control of citizens and authorities can nevertheless cooperate with each other across processes. The emergence of a parallel digital central state can thus be prevented.

If the once-only principle is correctly implemented using blockchain technology, certain master data of citizens and companies can only be collected once and remain available across all authorities. For this purpose, self-sufficient identities are particularly suitable, which enable the respective identity holder to exercise complete control over his personal data at any time, in particular the free discretion as to which data is transmitted to the service providers of digital services. The European legal area is characterised by citizen protection legislation such as data protection. The protection of personal data can be promoted, among other things, by the approach of data minimisation, so that only the absolutely necessary amount of data required for the use of the respective service has to be disclosed at all times.

A properly understood digital infrastructure gives the opportunity to help administration and norm addressees. It will often be possible to embed the right once it has been translated into digital structures. This means that rules and institutions of the state can be established as a "protocol" in a state blockchain infrastructure. Thus, the state legal framework can partly run as a technical protocol on the blockchain. Likewise, innovation-friendliness in jurisdiction and modern, agile legislative procedures are the necessary core of the legal handling of new technologies.

SPECIAL FEATURES OF BLOCKCHAIN TECHNOLOGY

Properties and added values

Blockchain solutions can strengthen trust between different actors (e.g. between authorities, companies, citizens). They enable their users to obtain a common view of the "truth" that cannot be manipulated or subsequently changed by individual users or third parties according to their own interests.

The core of every blockchain application is the so-called consensus algorithm. This algorithm implements a transparent and reliable mechanism for users to agree on the validity and order of the transactions to be performed on the blockchain. This enables a decentralized storage of an identical information status on the systems of the respective users at any time and provides them with a secure basis for the (subsequent) verification of the correctness and integrity of the stored information.

Decentralized storage also allows the actors complete control over their own personal data in the sense of self-sufficient identities (SSI) and thus allows the goals defined by General Data Protection Regulation (GDPR) to be realized more easily and better in the digital processes of the future.

Modern blockchain technologies can also store process logic in so-called Smart Contracts. These predefined process logics, which can be viewed by anyone, are automatically executed when certain conditions occur and can thus increase the efficiency, transparency and manipulation resistance of processes.

AREAS OF APPLICATION IN PUBLIC ADMINISTRATION

Blockchain technology can support public administration in a variety of areas. Put simply, blockchain provides an IT solution for federal business processes where digital sovereignty and the once-only principle play an important role. Below are the four most promising.

Blockchain-based identity solutions allow citizens to regain control of their digital identities and create identity credentials without revealing identity-related information. In addition, such identity solutions can enable citizens to participate in the sharing of identity-related information. Blockchain can therefore offer significant added value for the development of functioning federal e-government services.

In addition, blockchain technology can support the coordination of administrative processes across different authorities. The timely distribution of new information to all participants in the Blockchain network enables processes to be orchestrated across organisations. In this way, situations distributed across the network can be used, for example, as triggers for the start of subsequent processes at other authorities, thereby significantly reducing intermediate process times. If precise database references are also stored in the blockchain network, further information can be specifically requested if required. Blockchain can thus significantly improve the availability of information while at the same time maintaining the once-only principle.

Blockchain technology also enables digital tracking of certificates or ID documents. Blockchain solutions make it possible to identify the issuer and verify authenticity. At the same time, the blockchain solution guarantees the persistence of the document. Any ineffectiveness can also be noted on the blockchain at a later point in time. In concrete terms, a blockchain solution can be used to digitally track certificates or driver's licenses, for example.

Blockchain technology can also contribute to the modernisation of the register landscape. In concrete terms, blockchain technology makes it possible to create innovative new meta-registers in which data (changes) can be indexed in fragmented registers. In certain cases, however, existing registers could also benefit from mapping on a blockchain if they are registers that do not justify public belief.

In addition, many other applications are conceivable, such as automation of tax collection or earmarking of subsidies.

QUESTIONS

Organisational Questions

The issue of responsibility & governance plays an important role in public administration. For this purpose, the responsibilities regarding the implementation, operation and maintenance of a blockchain infrastructure must be clarified. Clear decision-making structures, powers of action and control mechanisms must be established that reflect the needs of the public administration and at the same time enable targeted implementation, stable operation and effective maintenance. In addition, it must be clarified how a blockchain infrastructure of the administration can be financed.

The topic of sustainable further development is also not yet guaranteed for many blockchain technologies. Blockchain technologies must continue to be adaptable to new findings and requirements in the future. This requires an active further development by appropriate developer groups and/or organizations if necessary with state participation. Without these further developments, any legal innovations cannot be implemented. From the point of view of the public administration, the development of an appropriate model for the sustainable further development of a blockchain infrastructure is therefore essential.

Technical Questions

In line with the organisational design, alternative network topologies must be illuminated by different combinations of public and private blockchains to form an overall system. In particular, requirements must be defined with regard to the interoperability of the blockchain solutions and components involved.

Based on the network topology and the usage characteristics of the application cases to be realized by the respective blockchain solutions, the exact requirements regarding the scalability of the blockchain infrastructure and the necessary security level of the consensus algorithm and the overall software must be critically evaluated.

The maximum number of transactions per second represents a challenge for many classic blockchain technologies in terms of their widespread application by citizens. Modern approaches address these limitations through alternative consensus mechanisms (such as proof of stake instead of proof of work) or through completely new, promising approaches (such as directed acyclic graphs), which still have to be tested in practice.

Although blockchain technology generally offers a high degree of resistance to manipulation, different consensus algorithms can differ greatly in their level of protection against attack scenarios of different kinds. The security guarantees of different technologies must therefore be critically evaluated and compared with each other, taking into account the desired network topology.

Legal Questions

The establishment of a blockchain infrastructure for the German administration also poses a number of legal challenges. If a blockchain network is actually operated decentrally, there is by definition no central intermediary that could be classically regulated or addressed by the user. The security previously offered by trusted third parties is being replaced by a software or execution environment in a decentralized network (protocols).

It is therefore of crucial importance to develop new regulatory options in the area of decentralised networks through soft governance, certified standards and intelligent regulation that are embedded in the digital fabric of a collectively operated administrative infrastructure (embedded law).

Although blockchain technology brings great advantages in terms of self-sufficient identity management, there are also major challenges that must be addressed with regard to the correction and deletion of data (such as the right to forgetfulness, which the GDPR has turned into). Best practices in the field of data minimization, among other things, must be established and promoted, and the promise of new technical solutions analyzed and tested.

With regard to the long-term preservation of evidentiary value and integrity protection, various approaches to ensuring eIDAS conformity must also be reviewed and evaluated. Important topics are the handling of cryptographic algorithms, on whose security blockchain technology rests, but which can lose their security suitability over time, the generation of trustworthy time stamps by qualified time stamp services or blockchain mechanisms, as well as the level of protection against quantum computers.

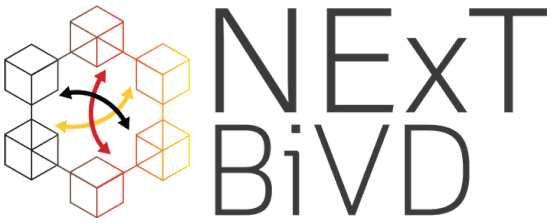
WHO ARE WE?

In 2018, the CIO of North Rhine-Westphalia launched the initiative "Blockchain in der Verwaltung Deutschland (BiVD)". In addition to the CIO department of the North Rhine-Westphalian Ministry of Economics and Digitisation, VITAKO together with RegioIT Aachen, the Federal Office for Migration and Refugees (BAMF) and the German Federal Blockchain Association (Bundesblock - Association advocating for blockchain technology in Germany) as well as the Fraunhofer FIT project group Business Informatics are initiative partners. In 2018, BiVD joined forces with the NExT Network to form "NExT-BiVD".

TIME SCHEDULE

The working group plans to publish the following documents:

- A first white paper with description of the use cases, detailed discussion of the organizational, technical and legal questions and a derivation of appropriate requirements.
- A second white paper with evaluation of different technologies and approaches, an analysis of relevant proof-of-concept projects and a sketch of the further steps of the BiVD.



MARCH 2019