EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Blockchain Technology in the Public Sector

The Swiss Federal Audit Office's View on Possible Applications

November 2019

Blockchain Technology in the Public Sector

The Swiss Federal Audit Office's View on Possible Applications

Blockchain – a leading technology for distributed ledger systems – is the subject of much debate. Many specialists believe that the new distributed ledger technologies (DLT) will revolutionise the way we carry out electronic transactions in the future. Opinion differs only as regards the speed with which these technologies will become established.[1] DLT use by public authorities is also under discussion. Initial pilot projects are already using blockchain technologies: since November 2017, the city of Zug has offered its residents a digital identity based on blockchain technology. Holders of a Zug digital ID were allowed to use it in a consultative vote in June 2018, and 72 people used the opportunity.[2] The canton of Geneva is testing the issuance of electronic commercial register extracts based on Ethereum; recipients are able to verify that they were genuinely issued by the canton.[3] In a public-private partnership (PPP), the canton of Aargau has established a blockchain-based car dossier[4]. This is designed to contain all relevant data on the entire life cycle of a car, from production to scrappage (manufacturer, importer, dealer, insurer, permits, garages, instances of damage, owners, leasing conditions, etc.) and should contribute to the digitalisation of the automobile ecosystem. Alongside the canton, around a dozen other partners have signed up to the PPP.

Like public authorities in general, the Swiss Federal Audit Office (SFAO) is having to examine the possible ramifications of DLT at audited administrative units. When is the use of this technology appropriate? What specific risks does it carry? And consequently: what questions does an administrative unit need to ask itself if it wants to adopt this new technology?

Based on an analysis of the state of technological progress, the SFAO has identified the following specific questions that need to be answered when deciding whether to use DLT:

1. *Can DLT support business needs better than other technologies?*

   DLT was originally developed to settle financial transactions reliably without an intermediary. In the meantime, a number of other interesting fields of application have been identified, for example the seamless documentation of the origin of goods (e.g. diamonds) or the automation of contracts (smart contracts) to name but two. However, there is currently a risk that people are turning to the new technology because of the hype surrounding it, without properly investigating whether its use is economical and brings real value-added, or whether it might in fact make workable overall solutions more difficult (e.g. interaction with other, non-DLT-based e-government solutions).

2. *Do business needs require that the data stored in the distributed ledger must never be changed or even deleted?*

   It is a feature of today's DLT systems that stored data cannot be changed once a transaction has been settled. This is an advantage in cases where traceability is important, but it also makes this technology unsuitable if data needs to be altered at a later date, even in isolated

[1] See, for example, https://hbr.org/2017/01/the-truth-about-blockchain
[2] https://www.luzernerzeitung.ch/zentralschweiz/zug/erfolgreiche-digitale-abstimmung-ld.1074829?reduced=true
[3] https://www.ge.ch/dossier/geneve-numerique/blockchain
[4] https://cardossier.ch/

cases. Its use is also problematic in business contexts where the parties have the "right to be forgotten" (e.g. criminal records).

3. *Are all participants allowed to see all the information stored in the DLT system? If not, are appropriate measures in place to ensure confidentiality?*

   Blockchain, for example, is designed as a peer-to-peer network. Each participant possesses a complete copy of the data. The advantage of this is that they are not reliant on trusted third parties.[5] As a result, each participant has access to all the data in principle. This is not acceptable in all cases. Encryption can prevent critical data from being viewed, but more complex access controls are difficult to implement. Anonymisation and pseudonymisation mechanisms have proved unreliable in practice. Therefore, sensitive data should not be stored in a blockchain.

4. *Has a suitable DLT been selected?*

   There is not just ONE blockchain. Behind the name used by the general public is a collection of different technologies[6] and blocks (e.g. cryptography, logic controllers, peer-to-peer networks, consensus mechanisms, smart contracts), which can be combined with each other in various ways. For each block, there are various implementation forms, each of which has its own strengths and weaknesses. In addition, DLT systems can be public or private, permission-based[7] or permission-less. Not every model is suited to every application and every environment. When selecting the technology, the overall context should be taken into account.

5. *Can the requisite level of information security be ensured?*

   DLT systems explicitly support the immutability of data and the traceability of transactions. To do this, they use high-quality cryptographic procedures. This, together with the distribution of responsibilities, can have a positive effect on security but is not enough on its own. Sufficient attention must be paid to the security of the distributed system as a whole. Areas warranting particular focus include: security of access controls, protection of hardware and software used by *all* participating nodes, security of the cryptographic methods and protocols employed, and defence against denial-of-service attacks. In addition, public blockchains must ensure that participants with a lot of processing power cannot manipulate data. According to an analysis by Germany's Federal Office for Information Security (BSI)[8], it cannot therefore be assumed that the use of a blockchain will, by definition, ensure the necessary security for a given application.

   A particular challenge arises when storing long-lived data in the blockchain: blockchain solutions are based on open source software. When, as is inevitable, the code is developed further, forking can occur as different developer communities change the code in different ways. Functions that people may have been relying on might no longer be available in future releases. Archiving data is also a challenge. And in the longer term, cryptographic methods that are regarded as secure today might no longer be adequate in the future.

[5] In real-world applications, such as bitcoin, the peer-to-peer principle has already been breached in some cases. Not everyone can, or is willing to, set up the necessary technical infrastructure. Many bitcoin users are therefore turning to third-party service providers.

[6] Blockchain, Ethereum, Hashgraph, etc.

[7] In a permission-based blockchain, transactions can be validated, or new blocks added to the chain, only by participants who have been authorised according to a defined process.

[8] See the BSI analysis at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf

All in all, we do not yet know enough about the limits of technology. Nor is it clear how transaction costs will develop over the long run.

6. *Is regularity ensured over time?*

   Like all other systems, DLT systems must be correctly implemented. It must also be ensured that the business logic is correctly configured (e.g. through smart contracts) in the system. The complexity of the technology makes it difficult to have the correct implementation verified by a neutral party. It must also be ensured on a lasting basis that changes to the system can be carried out in a controlled way. This, too, involves considerable effort in the case of distributed systems such as those in a public blockchain. In this regard, a private blockchain is easier to set up and maintain.

7. *Is there enough DLT expertise available?*

   The technologies involved are extremely complex and in-depth knowledge is still a rare commodity. The organisations concerned will probably purchase a solution. This carries the risk that neither the organisation concerned nor the supplier has staff with sufficient knowledge of using the technologies employed. This applies especially to further developments and any adjustments that might be needed to address faulty performance or security problems.