

# Distributed Ledger Technology

Cybersecurity – challenges for political Switzerland



## State of the art

Blockchain is a special form of Distributed Ledger Technology (DLT). DLT can be seen as a distributed database (ledger) held and updated independently by each participating node in a network. There is no central authority that maintains the database and communicates the records to the nodes. Instead, the records are constructed independently and held by every node. This means that every node processes every transaction and comes to its own conclusion. A consensus protocol ensures that each node maintains an identical copy of the database.

There are various ways of how to implement DLT, Blockchain being the most widely known one. Very often Blockchain is associated with cryptocurrencies like Bitcoin. It has to be noted that the terms should not be used interchangeably. Blockchain is the technology that most cryptocurrencies are built on.

## Challenges

Blockchain removes the need to trust a central authority such as banks, insurers, or notaries. Not having a central authority involved has advantages and disadvantages from a security point of view. There is no single point of failure but there is also no control point that may be able to identify and act on unforeseen problems. Instead, one has to trust the Blockchain technology itself and the built-in fault tolerance.

## Recommendations

Blockchain and DLT in general unveil new possibilities for a wide range of business applications. Blockchain-based solutions that are currently developed and promoted by start-ups will further mature. It is recommended that organizations planning to deploy blockchain-based solutions do a proper risk assessment with emphasis on the application that runs on top of the underlying blockchain platform.

Particularly in Switzerland there are many Blockchain start-ups. A recent report counts more than 800 companies with over 4'000 professionals active in Blockchain and cryptocurrency technology, located mainly in the «Swiss Crypto Valley» around Zug.

Blockchain security issues reported so far typically do not relate to the Blockchain platform itself but to the applications running on it. In this sense, Blockchain applications are not different from traditional applications, they both are exposed to similar security issues.

From an end user perspective, poor key management practices are a major concern. Lost or stolen keys are a widely reported problem that has immediate financial impact in the case of cryptocurrencies.

## Need for action

The Blockchain technology and its applications will further mature, in particular performance improvements to increase the transaction processing speed are to be expected as well as new security and privacy features.

On the legal side, the application of Blockchain to the finance industry has raised various questions. Therefore, in November 2019, the Swiss Federal

Council adopted the dispatch on the further improvement of the framework conditions for Blockchain and DLT based applications. Amendments to nine federal acts are proposed covering both civil law and financial market law. They are aimed at increasing legal certainty, removing barriers for DLT applications, and reducing the risk of abuse.

## References

CV VC: The Crypto Valley's Top 50 H1 2019, July 2019.  
<https://cvvc.com/application/files/2115/6453/7847/CVVC-Top50-H1-2019.pdf>

Swiss Federal Council: Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register, Nov. 2019.

<https://www.news.admin.ch/newsd/message/attachments/59301.pdf>

## Contact

Nicole Wettstein

Head of priority programme Cybersecurity

+41 44 226 50 13



<https://www.satw.ch/cybersecurity-challenges>

## Impressum

Swiss Academy of Engineering Sciences SATW

### Expert contributions

Karl Aberer, EPFL | Umberto Annino, InfoGuard | Alain Beuchat, Banque Lombard Odier & Cie SA | Matthias Bossardt, KPMG | Adolf Doerig, Doerig & Partner | Stefan Frei, ETH Zürich | Roger Halbheer, Microsoft | Pascal Lamia, MELANI | Martin Leuthold, Switch | Hannes Lubich, Board of Directors and Advisor | Adrian Perrig, ETH Zürich | Raphael Reischuk, Zühlke Engineering AG | Riccardo Sibilia, VBS | Bernhard Tellenbach, ZHAW | Daniel Walther, Swatch Group Services | Andreas Wespi, IBM Research Lab

### Editing and graphics

Beatrice Huber, Claude Naville, Adrian Sulzer, Nicole Wettstein

The views expressed here are those of the members of the SATW Cyber Security Advisory Board and do not necessarily reflect the official position of SATW and its members.

[www.satw.ch](http://www.satw.ch)

September 2020