Digital trust

How the company CryptoTec is contributing to the creation of a new world

Cologne, 02 March 2016
Digitalisation is spreading to more and more areas of our lives. Take photography as an example: within a decade, it underwent a complete digital transformation. And, as Telekom has announced, landlines will be phased out by 2018 as well and will be fully replaced by IP telephone services. Digitalisation and the Internet are changing the world at an ever faster pace. If one asks the founder of CryptoTec, Michael Mertens, what has happened so far is only the beginning. *"From my point of view, both digitalisation and the Internet are still in their infancy, but the whole thing is picking up momentum"*. He even takes one step further by talking of the start of a new epoch.

Trust as a business model
"*The digital world and the Internet as an instrument of communication are already providing us with a wealth of possibilities. We exchange news, we have access to information, we publish in real time across the globe and we do a lot more still on the Internet. However, today's Internet and digitalisation both have a major weakness: trust. For the most part, trust still requires human contact and hierarchical, institutional structures. Take a bank, for example. Whoever wants to take out a loan is usually presenting in person. Be it for identification or for confirmation of the loan contract in the form of a signature",* Michael Mertens says about the limitations of today's Internet.

All of this will – if Michael Mertens has his way – become obsolete very soon. Advances around the mathematical foundation, in the form of programming, have been so extensive that mathematics will act as the basis of trust. One example is Bitcoin: suddenly, money came into existence without banks or, indeed, without a government to issue it. Mere complex mathematical formulas, i.e. algorithms, are able to make people trust a means of payment which is recognised across the world and which can be rapidly transferred to anywhere – entirely without the involvement of banks. Everything is organised in a decentralised manner. Key

word: web of trust.

Block chain and PKI

The underlying technology for trust in the Internet is block chain, which in turn requires the so-called public key infrastructure (PKI). Public key infrastructure (PKI) automates complex key management and end-to-end encryption for users. With PKI, all participants can be authenticated as communication partners.

About Michael Mertens

Michael Mertens is one of the most important pioneers in the development of central (trust centre) and decentral (web of trust) authentication systems. Already while at university, he studied PKI-based encryption solutions. He became an independent businessman in 1992 and has been securing the digital communication of companies using the PGP software since then. Since 1995, he has been securing the electronic transfer of sensitive flight data for airports, also based on PKI. Mertens has been doing extensive work in the Internet-based securities trade since 2000. His task in the establishment of one of the very first online portals for securities trade ever was ensuring the encrypted and legally binding transfer of data. Since 2002, Michael Mertens has been looking extensively into the opportunities of block chain technology, and already then maintained intensive contact with the inventors of Bitcoin. Two years later, in 2004, Mertens developed software for securing financial transactions in the productive finance sector with turnovers of several billions in his then newly founded company iDev. This software utilised processes of today's block chain technology. These techniques were automated in the block chain for the very first time.

Digital currencies are only the beginning

Was has been graphically illustrated for money with Bitcoin will be used in a vast number of other sectors - birth certificates at the registrar's office, for example. The web of trust will make it possible to provide identification information online, and to thus prove a justified interest and receive a document in a fully automated process, which one can forward – also reliably. Even the fees for the provision of documents will be invoiced automatically. All without credit card institutes or employees at the registrar's office.

The Internet of things

If Michael Mertens has his way, not only information, such as documents, will be part of easy-to-authenticate digitalisation, but also "things". The Internet of things (IOT) will be fully imbued with possibilities in the near future, "*...one example. You are granted a commercial credit for the purchase of a car. If an instalment is not paid, the vehicle will no longer start. The vehicle can only be used again once the instalment has been paid"*, Michael Mertens illustrates the possibilities that are offered by including things in the Internet.

CryptoTec AG

Michael Mertens holds participations in various technology companies. His latest hobbyhorse is majority participation in the company CryptoTec which he founded together with Dr. Michael Raumann. The new company's goal was to develop absolutely secure communication. The company has already published several modules on the market and, besides its headquarters in Cologne, already has branch offices in Hong Kong and India. The entire technology behind the cryptographic portfolio (CryptoTec Zone) is based on sustainable, proprietary PKI. What caused a stir in the industry – among investors and not least among customers – is the tremendous complexity this system allows for, combined with the simultaneous highest possible ease of use. This is why the two founders of CryptoTec are now taking the next step, and intend to expand the widely tested communication solution. *"By using the PKI and block chain technology that CryptoTec Zone is based on, we want to create a universal platform that includes any currencies and standards in effect so far and which thus ensures safe, decentral and forgery-proof exchange online. In this respect, it is irrelevant which type of exchange we are talking about. Whether it be payment transactions, the Internet of things or self-executing smart contracts. We want to include all sectors of digital values in the new platform, to guarantee their integrity through sealing and to offer people the opportunity to move these values digitally at will"*, Dr. Michael Raumann explains the vision of CryptoTec.

Goal is not the "fully accessible human", but the opposite

When there is talk of authentication, some Internet users may think of complete transparency. At CryptoTec, efforts are made to achieve the exact opposite, namely the protection of privacy. Mertens explains in this regard, *"Actually, the*

current situation is outrageous. Let's assume you want to do something trivial, like purchase a product online. Today, you will still need either a credit card or one of the many payment systems such as PayPal. There are hardly any other ways to pay for something online. This is also where the problem starts. It is surprising how much information you have to submit to your bank before you get a credit card. Afterwards, the bank is privy to every payment transaction and can establish an exceptionally detailed personality profile for you. The same applies to any other institutional payment system. Sometimes, this information about you is also traded. With a payment system like, for example, Bitcoin, you can, first and foremost, regain your privacy because it really is of nobody's concern what you are doing with your money. Accordingly, it is at least as anonymous as cash and even safer than a conventional bank transfer – these are the advantages of block chain-based or PKI-based systems. Additionally, you are not only protected because you do not have to disclose information, but also because all transactions are virtually hacker-proof due to the utilisation or hard, asymmetrical encryption."

Block chain technology in international movement of goods

If CryptoTec has its way, the practise in international trade is one of the biggest problems in today's world. "In the sphere where the judicial system has no power across borders, banks ensure so-called trust. For example, payment transactions are ensured based on letters of credit (L/C) and in return for high fees. This is one of the key problems block chain technology can solve in the future. It will be possible to prepare self-executing smart contracts, which are confirmed online in a legally binding manner by the contractual partners and which create trust because they are self-executing and stored in the block chain. It becomes even more graphic when intelligent self-executing contracts are combined with, for example, monetary payments. Here, the term smart money is used. Dr. Michael Raumann has an example for this as well: *"Let's look at the example of the so-called rounds of financing in private equity financing. So: an investor wants to acquire shares in a company, in return for a payment of money. Usually, such an exchange is not made in a single transaction, but is subject to a range of conditions. For example, achievement of a certain turnover, or completion of a solution. This entire process of cash flow and transfer of shares, dependent on process developments, can be described using smart money and therefore can be executed in a manner verifiable by all parties and thus reliably."*

Summary

All in all, cryptography and associated central and decentral trust systems will fundamentally change the world as we know it today. Time will show how deep these changes will go for all parties involved, and which industries will suffer disruptive effects caused by this technology. The start, however, is well and truly under way.