INSTITUTE OF TECHNOLOGY ASSESSMENT

ITA-DOSSIER

Decentralising transactions with the Blockchain

In brief

- Blockchain is a decentrally organised database that archives and manages an ever-growing list of transactions.
- All information on transactions is permanently stored in a database that parallely exists at all nodes of a peer-to-peer network.
- Blockchain provides autonomy for individuals away from 'middlemen' such as public authorities and banks.
- However, this decentralisation rapidly reduces current forms of regulatory control.
- Possible negative social and economic consequences become less predictable and manageable.

What is it about?

Blockchain technology is a decentrally organised database of transactions. It relies on the two computer science fields distributed systems and cryptography, which have been continuously developed by scientists and activists since the 1970s. Blockchain technology was first put to widespread use in its application to the Bitcoin cryptocurrency in 2008. Information on each transaction (such as an exchange of cryptocurrency or the creation of a contract) is recorded by 'miners' (computers – nodes of the network) in a 'block' (data bundle) which is linked to a chain of existing and new blocks. Blockchain is typically managed as a peer-to-peer (P2P) network. The network follows a protocol for creating new blocks. The data in each block cannot be changed without changing all the data in all the blocks it is linked to.

The management of transaction data in blockchain through a network means that it can be fully decentralised, avoiding intermediaries or organisations such as central authorities. Institutions such as banks or public sector agencies are often viewed as being inefficient and bureaucratic, slowing processes down. Intermediaries can become very large and powerful monopolies with opaque processes which can foster distrust. By being managed and verified by a network, with all information always fully available to all participants, the blockchain automatically creates trust.

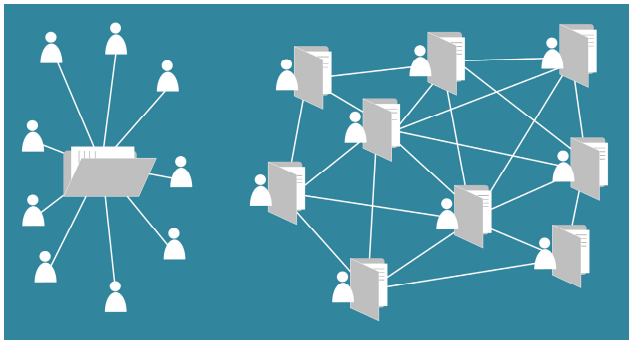


Illustration: ITA-NG

Centralised vs. distributed: The blockchain is based on a peer-to-peer network and cuts out the middleman

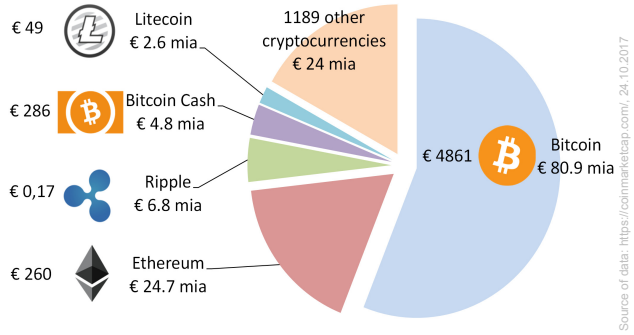
Applications of blockchain platforms are virtually limitless because the need to securely record transactions exists in every sector. The most famous application of blockchain technology is the cryptocurrency Bitcoin, but it has also been used in public systems such as registering votes. Other innovations which are being explored are the use of blockchain technology in the creation of 'smart contracts' for the protection of digital content and other intellectual property, registrations, paying taxes, legal contracts, as well as in smart grids and energy markets, and global supply chains.

Advantages: Continuous matching through the network ensures transparency, security and verifiability of transactions. Transaction costs can be made more efficient and potentially free of charge. Data is protected – for example user names are encrypted – yet amounts and pathways of transactions are permanently kept track of.

Disadvantages: The blockchain can potentially have negative consequences that can escalate if not regulated. Decentralisation does not mean that intermediaries and hierarchies cannot occur. Blockchain technology still suffers from shortcomings such as requiring immense amounts of computing power with a high demand for energy. Furthermore, intermediaries can be very helpful when customers have questions or problems about transactions. Who would you call in a fully decentralised network?

Bitcoins and 'smart contracts'

Bitcoin – the most popular of several digital cryptocurrencies – is a peer-to-peer payment system based on blockchain. Bitcoins are in use since 2008. Code and math is used to identify who owns Bitcoins and how they are used to pay for things. Bitcoin owners use their encrypted digital signatures in transactions. These signatures are easy to generate and verify, virtually unforgeable, and fully protect a person's identity. Bitcoin transactions are recorded in a distributed register which logs what is bought and sold and broadcasts it throughout the system. If a user feeds a transaction of bitcoins into the network, miners use computer processing power to verify the legitimacy of this pending transaction and add it to a block. In order for the network to accept the new block and add it to the distributed database, the miner needs to solve a mathematical proof to find a key that was generated by a one-way function infeasible of inverting and which is included in the last block of the chain. This takes up processing time and slows down the entire system to a few transactions per second. Even though Bitcoin value has fluctuated widely and has been criticised for its use in the black market, it has proven that the blockchain technology works.



The top five cryptocurrencies: Prices and market capitalizations

Blockchain technology spreads rapidly, and one recent promising avenue is their use in the creation of smart (or digital) contracts. Smart contracts, similarly to computer programs, have the possibility to involve clear definitions of roles and a specification of what will happen in different conditions. The contract can be signed with a digital signature, is made permanent, visible, verifiable and immutable. Each contract can include contingencies in case anything goes wrong in a transaction. It removes the need for both a third party and for trust between the two parties in the transaction. Ethereum is currently the most prominent open-source blockchain-based distributed platform for smart contracts and functioning applications are still in development in this highly dynamic emerging field.

What to do?

Austria needs to take bold and measured steps in the development of blockchain technology. Policy-makers need to take into account:

- **Societal needs:** Consumer risks have to be understood and protection be maintained. Knowledge needs to be gained about how to ensure that illegal activities are avoided, compliance with existing Austrian and EU laws need to be ensured. Technology development needs to be inter- and transdisciplinary, for example a close collaboration between people skilled in the content and context in which the blockchain will be used, together with programmers and users.
- **Economic requirements:** Start-ups and innovation potential need to be taken advantage of. Pilot and demonstration projects need to be invested in to explore the potential of blockchain technology in different sectors. Skills and training need to be upgraded to deal with the growing requirements of software developer skills.
- **Regulation:** Blockchain technologies carry with them their own questions about accountability and responsibility if something goes wrong. There will be different but important roles for institutions to ensure some rigidities, reliability and long-term predictability.

Further reading

Boucher P. et al. (2017) How blockchain technology could change our lives. STOA – Science and Technology Options Assessment, EPRS – European Parliamentary Research Service

europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

Contact

Tanja Sinozic

E-mail: tamail@oeaw.ac.at

Phone: +43(1)51581-6582

IMPRINT: Owner: Austrian Academy of Sciences; Legal person under public law (BGBl. 569/1921 i.d.F. BGBl. I 130/2003); Dr. Ignaz Seipel-Platz 2, A-1010 Vienna; Editor: Institute of Technology Assessment (ITA); Strohgasse 45/5, A-1030 Vienna; www.oeaw.ac.at/ita/en. | Frequency: The ITA-Dossiers are published irregularly and publish the research results of the ITA. The ITA-Dossiers are published in print in small numbers only and are made available open access to the public via the Internet portal "epub.oeaw": epub.oeaw.ac.at/ita/ita-dossiers | ISSN: 2306-1960 | This work is licensed under a Creative Commons Attribution 4.0 International License: creativecommons.org/licenses/by/4.0/ | ITA-Dossier no. 30, November 2017 | epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier030en.pdf |
Co-author: Niklas Gudowsky