CLIMATE | LEDGER INITIATIVE

Factsheet

April 2018| CLI_Factsheet_Introduction to Blockchain.docx

Tony Reyhanloo, Jürg Füssler and Sven Braden, CLI and INFRAS

An introduction to the blockchain and distributed ledger technology

The **blockchain technology**, or more generally **Distributed Ledger Technology (DLT)** promises worldwide, revolutionary restructuring of existing transaction systems. As a simplification, however, we are using the very common term «blockchain» in this text as a placeholder for the much broader concept that includes all distributed ledger technologies, even though blockchain is only one implementation of DLT.

The blockchain technology provides new ways for secure exchange and storage of data and digital assets, primarily designed for peer-to-peer transaction platforms. The technology does not necessarily require high level IT infrastructure from the start since it allows for onboarding of functionalities over time. Therefore, blockchains may have a truly global impact on the transfer of digital values.

Image source: www.unsplash.com

Blockchain Technology in a nutshell:

Every network based on blockchain technology is run by a protocol which sets the system's rules. These rules are fixed and binding to all parties. The infrastructure of a blockchain network consists of computer servers (nodes, validators, miners etc). These servers operate under the assumption that interactions are only made by servers permanently sticking to the protocols' rules. Intermediaries (e.g. banks, clearing houses, trading platforms, centralized service suppliers etc.) are hence not needed anymore. By means of blockchain technology, transactions can be verified, validated and linked to each other, for example by using transaction blocks, which is where the term blockchain come from. This leads to a history of transactions which is shared by the whole network.

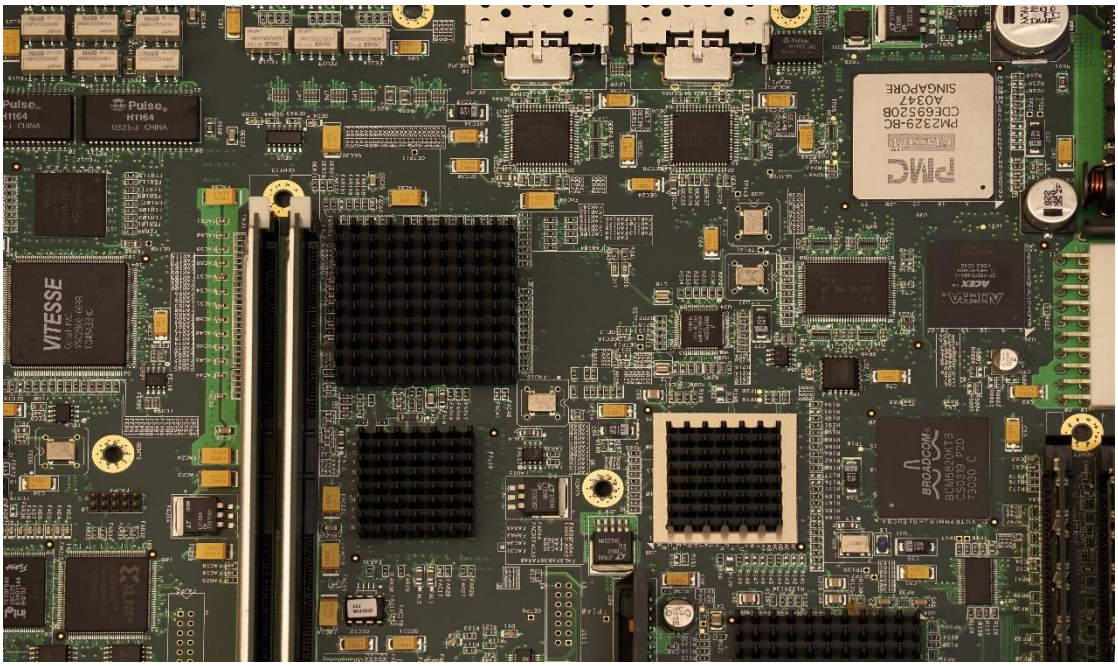

Image source: www.unsplash.com

Important features and advantages of blockchain technology: Blockchain databases are considered to be tamper-proof, not only because the individual information blocks are encrypted and decentralized, but also because transactions can be viewed by all parties involved. Since blockchain technology enables networks to work on an agreed set of transaction histories it is also possible to associate these transactions to conditions (which are also shared by the network): If transaction A has occurred, transaction B is automatically executed (principle of 'smart contracts'). Smart contracts are complementary mechanisms within blockchain networks, which allow for example for the automatic coordination of decentralized suppliers and buyers or the automatic allocation of pricing tags of environmental attributes. Therefore, blockchain technology provides new possibilities, e.g. for the energy market, by facilitating the direct exchange between decentralized energy producers and consumers. Complete transparency across all

transactions gives stakeholders within such networks the confidence to securely conduct transactions with anonymous partners. Advantages of the blockchain technology can therefore be summarized with the term 'multilateral interoperability', which encompasses multicast communication, immutability (no forgeries possible by fraudsters), real-time tracking of transactions and faster processing of payment transactions.

Is a blockchain network private or public? Blockchain networks can be public or private. Some require the identification of participants, others don't. This choice is based on whether identities and contents should be disclosed or not. Bitcoin for example is known to identify subscriber pseudonyms. In many regards, this is not a useful option for industrial blockchain networks, since participants in industrial networks are often asked to obtain information about their trading partners for compliance reasons (for example due to compliance requirements such as "KYC - Know Your Customer" provisions). There are currently certain open questions to be clarified regarding this "identity management", before blockchain based applications can be mainstreamed. This appears especially for the so called crypto currencies. In case of Bitcoin, the associated blockchain network is public and everyone can see every Bitcoin transaction that has taken place since its start in 2009 (see for example https://blockchain.info/de/blocks). The decision whether a transaction shall be accessible to the public or just to its network participants depends on the underlying protocol.

How do blockchain based networks operate? Blockchain networks can be seen as cross-checking instruments. A transaction is determined by two or more parties as correct and ticked off. Hence, a transaction is only qualified as correct if the evaluating party concludes that the transaction was created in line with the applicable protocol rules. If most of the parties consider the transaction to be correct (by applying a consensus mechanism) the transaction together with a series of other transactions is merged into a cryptographic code and built into a block. This block is appended to the previous block. In order to work tamper-proof and flawlessly, encryption techniques are used at the individual sections of the blockchain process. In addition, encrypted transactions or blocks of transactions are not stored in one central location but decentralised among all parties involved.

Energy consumption of the blockchain technology? Blockchain technology is associated with high power consumption and the necessity of high computer capacities. These associations are merely linked to patterns of a specific early network, the Bitcoin blockchain. The Bitcoin protocol provides for an open network that uses mechanisms with high energy consumption. In order to process transactions, the Bitcoin protocol requires fees of at least ten micro-bitcoins for each transaction. The higher the amount of the fee, the faster the transaction is confirmed. This makes

the network unattractive for any kind of microtransactions. In addition, the Bitcoin protocol applies the so-called proof of work as a consensus mechanism in order to determine the next computer who may add its transaction block to the network (provided the block has been recorded in line with the protocol rules). The proof of work mechanism requires the resolution of complex cryptographic tasks, which consume a high amount of energy. Although this mechanism contributes to the security and functionality of the Bitcoin network, it is highly inefficient form an energy and thus a climate perspective.

Image source: www.unsplash.com

Even though alternative options are already discussed (offset solutions for proof of work related emissions, deployment of renewable energies at mining sites), they are not solving the need for high energy consumption of the core protocol. Moreover, the capacities required to implement such alternative options should be used to address the challenges of the upcoming energy transition, rather than helping to justify a system which will, by design, grow only with an associated increase of energy demand (see for example the so-called difficulty adjustments within the proof of work mechanism). However, high power consumption is not necessarily a pre-condition for blockchain technology in general. The questions of power consumption related to blockchain networks directly relate to the way the respective blockchain protocol is designed (what consensus mechanism is applied, is the blockchain network open or closed, are tokens/coins being minted or are they pre-mined, how many transactions / unit time may be processed, second layer solutions for off-chain transactions etc). Hence, solutions for lower power consumption are available.

Other unresolved issues regarding blockchain technology mainly concern governance and socio-technical challenges (e.g. how to deal with the regulation of DLT-managed business models), legal and regulative aspects (e.g. who is legally responsible for the coding of the DLT protocol system; what is the role of governments in this regard), as well as scalability issues (e.g. how to deal with large data sets in a limited storage space, off chain/network solutions).

Conclusions: Blockchain technology offers participants greater autonomy and self-determination. However, technical challenges like the energy efficiency or the scalability of blockchain networks remain and may only be properly addressed by comprehensive research and respective field testing. These outcomes combined with carefully designed governance frameworks and legislation around liabilities, transparency and identity aspects may indeed lay the ground for a new digital era of our economy.

System comparison – classic platform vs. distributed ledger technology

	Classic platform	DLT
Organisational structure	Central, hierarchical	Decentralised
	The bigger the better	Small is beautiful again
	Dominance of the «sirenserver» with enormous computing powers that exceeds all other computers' performance within in the network	Computing performance
Economic system	Netarchical capitalism	Distributed capitalism
	Neofeudal monopolies	Peer-to-peer business, consensus economy
Who owns the platform?	Companies	No one (network belongs to users, cooperatives)
Control	One central station	Network protocol
	Top-down regulation	Algorithms
		Smart contracts
Transparency	Big brother	Little brother
	One sees everything	All (in the network) see everything, but no one can change how the system works
Security	Hacking, phishing, trolling, etc.	No vulnerabilities found yet
Location	National sites	Stateless
Trust	Management, brand	Algorithms und mass collaboration
Metaphor	Giant, octopus, spider	Swarm, ants, bees

Table: INFRAS. Source: GDI, Das Blockchain-Manifest, Wissensmagazin für Wirtschaft, Gesellschaft und Handel Nr. 2, Goldach, 2016

The Climate Ledger Initiative (CLI, www.climateledger.org) aims at providing objective and technology neutral information with regard to current and future climate-relevant applications which are based on distributed ledger technology. The work of the CLI is financially supported by the Governments of Liechtenstein and Switzerland as well as by the EU's Innovation Program Climate-KIC.

GOVERNMENT
PRINCIPALITY OF LIECHTENSTEIN

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Agency for Development
and Cooperation SDC

eit Climate-KIC