Collaboration in Higher Education for Digital Transformation in European Business

Managing Distributed Ledgers: Blockchain and beyond

http://www.chedteb.eu/

Rainer Lenz, rainer.lenz@fh-bielefeld.de in cooperation with

Jan Budík, Lukáš Novák – both Brno University of Technology/Czech Republic
Viire Täks – Tartu University/Estonia
Daniel Antonious Hötte, Bernd Kleinheyer, Ulrich Tamm, Margareta Teodorescu, Andreas Uphaus, - all University of Applied Sciences Bielefeld/Germany

Co-funded by the Erasmus+ Programme of the European Union

Abstract

The Internet of Value based on Distributed Ledger Technology strives for a strictly decentralised organisation of interactivities between peers without any centralised platform or intermediary. The technology is disruptive because core elements of the current organisation of value exchange will change radically. This applies in particular to four areas: (1) Proof of identity of customers, of clients, of users, of patients and the associated handling of private data; (2) Recording, documenting and certifying transactions, the change of value and entrepreneurial success; (3) Organisation of the value exchange and the transfer of values and utilities; (4) Integration of objects, of machines and of robots in communication and transaction processes.

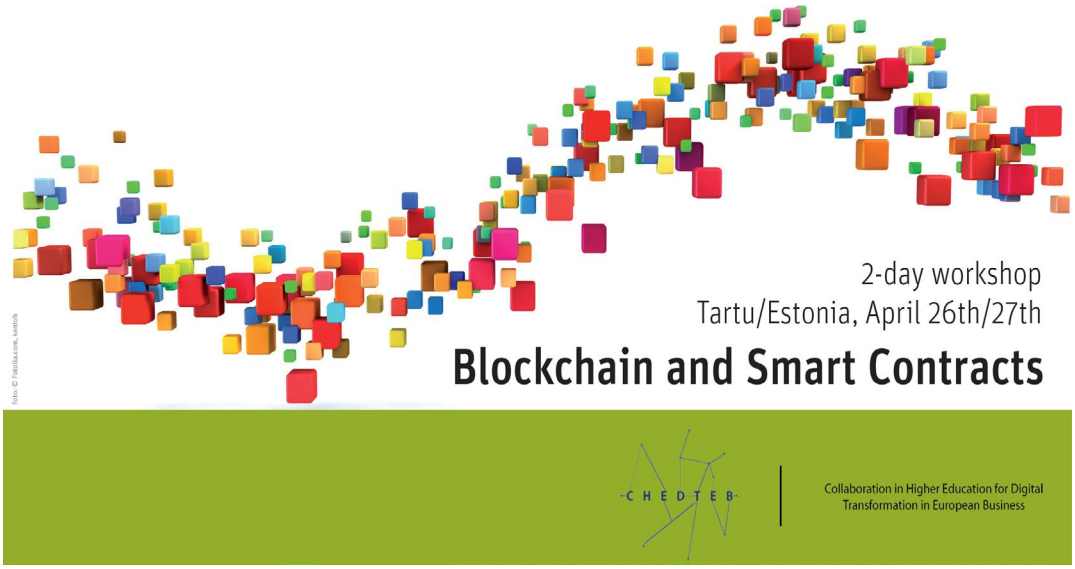
Distributed Ledger Technology is therefore not an innovation which comes overnight. The diffusion period takes longer – probably years or a decade – as radical changes within society are needed before distributed and shared ledgers become standard. Many technological aspects are not yet fully developed, so that the DLT is currently still in experimental mode. But the cases of use so far already show that the technology has the potential to revolutionize the nominal world of registration, certification, accounting and exchange of digital value and thereby enable completely new forms of collaboration and organization.

Table of Content

Why read this guide?

This guide explains the business logic behind Distributed Ledger Technology and follows the design thinking approach: which business problems can Blockchain solve and for which problems is the decentralized Blockchain technology less suitable? The way of thinking always starts from the business problem to be solved and looks subsequently for the adequate technology, not the other way around.

In this respect, this guide is primarily aimed at non-technical practitioners who are in one way or another involved in the process of digital transformation in their organizations. Most of these management positions are filled by information technology (IT) executives, who may understand the technology better than the consequences of restructuring business processes and managing people involved in the processes. This guide provides an assessment model for the best use of Blockchain and smart contract technologies within the corporate sector and delivers a coherent blueprint for implementation and application of these innovative technologies in business organizations.



The paper is the result of an intensive exchange of experiences, interviews, workshops and discussions that the involved universities conducted with companies from various sectors and regions as part of our EU project "CHEDTEB" over the last year. The Blockchain and smart contract topics aroused an astonishing level of interest within the manufacturing industry, especially among mid-sized companies seeing either the opportunities to streamline complex supply chain processes or feeling the upcoming pressure of new and more agile competitors.

In regular monthly meetings with an ever-growing working group, we promoted a collaborative learning process between the companies, which ultimately led to the development of first-use cases of Blockchain technology. Similar to the Blockchain technology itself, these workshop meetings were also based on the open source idea of sharing knowledge between companies and learning together. The ability and willingness to collaborate within a heterogenous group of IT experts, mathematicians (cryptography) and business people is very much needed for a successful learning process about Blockchain.

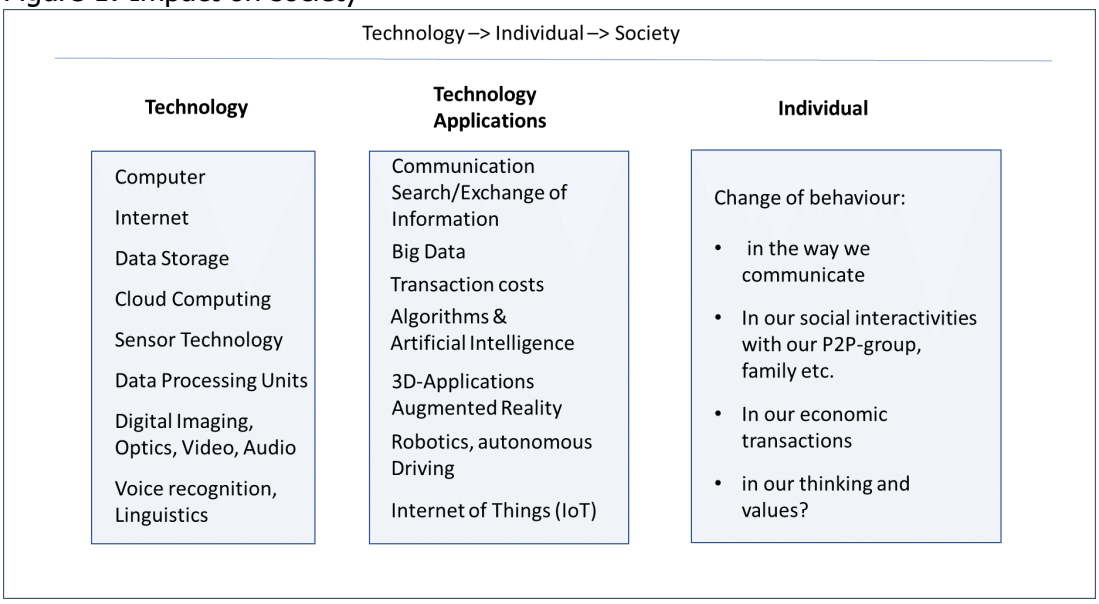
Finally, a word about international collaboration. It seems that the smaller countries in Eastern Europe are more advanced in Blockchain applications and development of first-use cases than the larger western ones. Perhaps it might be a cultural difference: an openness to experiment or the fact that entrepreneurship is already a subject in Estonian schools. However, as it is worth looking beyond national borders we organised a two-day workshop in Tartu/Estonia with the motto "Learning from others and starting now". Here different companies from transport and logistics, energy and IT sectors showed how to convert business processes to Blockchain technology and reported on their experience, advantages and risks. Videos, interviews and presentations from the workshop are partly embedded in this guide and are accessible via our project web-page http://www.chedteb.eu/.

1. Digital transformation and Distributed Ledger Technology

1.1. Digital Transformation of Society

Some of us still remember floppy disks and CD-ROMs. It hasn't been that long. In past years, data processing and storage technology have made significant progress and these advances, in turn, have enabled innovations in other fields such as optics, sensor technology, linguistics and voice recognition.

Figure 1: Impact on society



Source: the authors

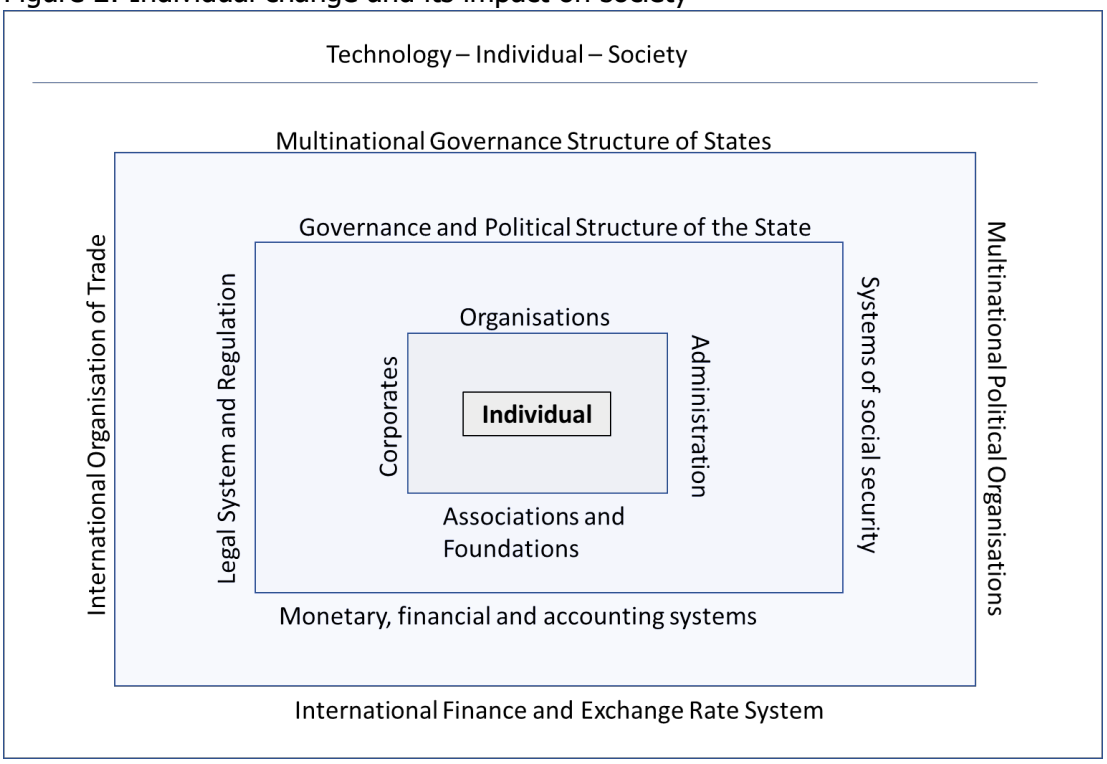
But pure technical progress itself is not what has changed our lives; it is the "apps", meaning the various applications of technology that make it easy, for example, to control a mobile phone by voice command or to orientate oneself in a foreign environment via GPS and route planner. For each technical advance, there are now software applications available that simplify our everyday lives and are usually easy and free to access for every user via mobile phone. Apps are successful because the time the user needs to familiarize themself with the new software program is significantly less than the advantage of using the application (speed, transaction costs, simplicity of communication, etc.). There has been technical progress since the beginning of mankind, but what is really new in the last 10 years, are the multitude of software applications offered via mobile phones or laptops, which are available to everyone for free or almost free. This has significantly shortened the period of diffusion from technical change to social impact and increased thereby the dynamics of social change.

One does not need to look at the large scoreboard of dating apps in the street to know that these software applications have changed lives and the behaviour of individuals in almost every part of life. It is the way people communicate with each other, the interactivities within peer groups and family, the thinking and values what have

changed in past years. These changes impact business life as consumers are increasingly bypassing retailers, banks and other intermediaries by using online platforms for transactions.

If the behaviour of the individual as the smallest unit in society dramatically changes, then the downstream organisations have to change as well because their products, services and processes are no longer fit for purpose. New business models emerge that are superior to traditional models of organization and therefore either replace traditional ones or force them towards digital transformation. Economically this implies that markets as places of exchange and trading and corporates as organisation of business are also subject to change. Most often, legislation and regulation is aligned to a certain type of organisation. For instance, banking law is applied to banks as a certain type of financial organisation. If individuals are using more and more peer-to-peer lending to access loans, then new legislation for crowdfunding needs to be developed. If the way business is organized is changing, then consequently the corresponding legislation has to be adjusted. Figure 2 documents the different levels of change within society.

Figure 2: Individual change and its impact on society



Source: the authors

1.2. Digital transformation of corporate business: from central to decentral

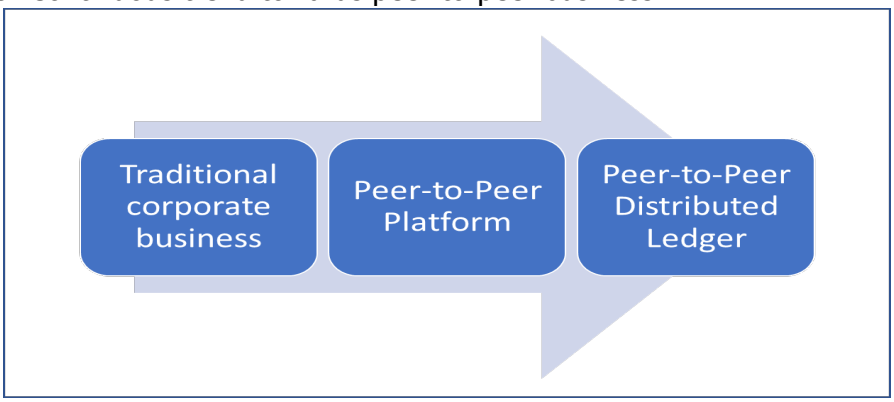
To get an idea of how future business organisations could look, Ronald Coase's "theory of the firm" could provide some useful insight. Based on Coase, the reason why firms exist is that centralised production within a single organisation is much easier to administrate, monitor and manage. Alternatively, the whole production process could be decentralised and every single part outsourced to external subcontractors

in the market. Coase argued that carrying out the work in a decentralized and fragmented manner by a network of market contracts would lead to much higher transaction costs than to organize the production within a single corporate structure (Coase, 1937).

Well, in 1937, Coase could not anticipate that progress in IT would reduce the search costs of finding appropriate external partners and would lower communication and contracting costs so much that if his theory were applied to the current situation it could lead to a reverse statement: As search, information, and transaction costs dramatically decrease, it becomes more efficient for firms to procure goods and services via a network of external market contracts rather than producing them within the firm. Digitalization breaks down the centralised production processes, thus opening up the company's boundaries. Supply chains become more and more complex by involving an increasing number of subcontractors.

This explains the trend in recent years towards a more decentralised organisation of corporate value chains combined with a higher degree of peer-to-peer business transactions without intermediaries. Platforms and the shared economy have created new business models that simply create value by organizing the exchange of information, products or values between users. With Distributed Ledger Technology, society and the economic system are now facing the next quantum leap towards a complete peer-to-peer economy that functions entirely without intermediaries.

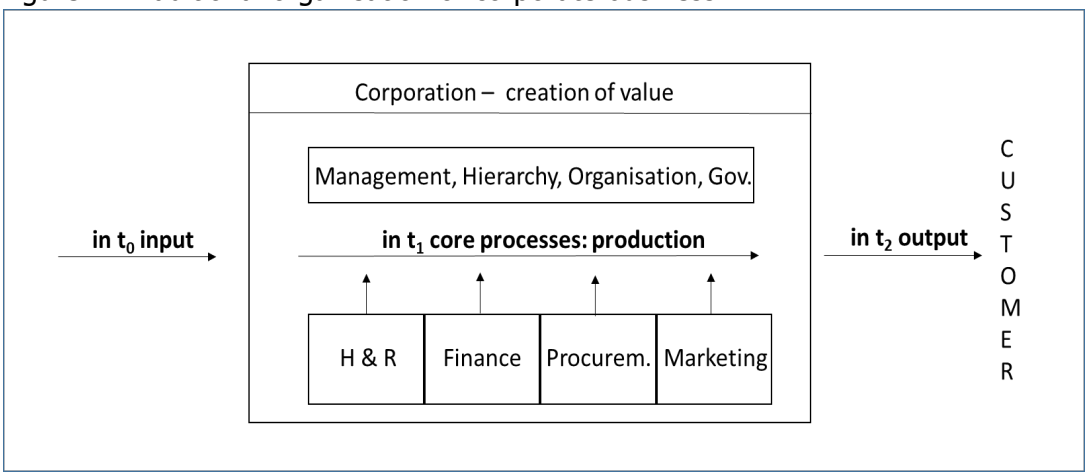
Figure 3: Continuous trend towards peer-to-peer business



Source: the authors

Traditional corporates are organised in a linear way as pipeline businesses, characterized by a clear hierarchy with different management levels focused on the value creating process of production. Human Resources, Procurement, Finance and Marketing are supporting functions for the value creation process, which start with the procurement of input material in t_0, continues in t_1 with an added value process of internal production and ends in t_2 with selling the final product in the market.
Unlike peer-to-peer (P2P) platforms, traditional corporates are brick- and mortar solutions with a limited scalability as they take the risk of having employees on long-term contracts and their own production lines with machines as fixed assets on their balance sheet.

Figure 4: Traditional organisation of corporate business



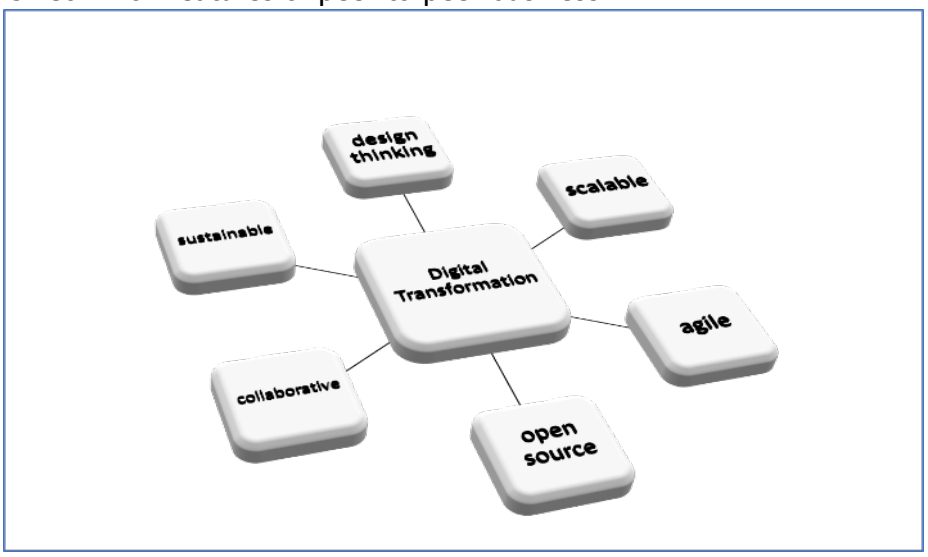
Source: the authors

In the last ten years in almost all sectors of the economy, new organizational models are emerging that operate as platform businesses. The best-known examples are Uber, a taxi company without taxis, Airbnb, a hotel chain without hotels, or Flixbus, a bus company without its own buses. What are the key success factors of these business models? They create value by facilitating the exchange of information or values between their users. In order to make these exchanges happen, platforms harness and create large, scalable networks of users and resources that can be accessed on demand. They are subcontracting every client order by setting up a platform, where all the interfaces with external stakeholders (users, subcontractors, payment systems etc.) are fully standardized and automated. The target is to develop such a platform architecture that allows scalability of the number of users, sessions and transactions processed by the system. While the initial investments for reaching a certain degree of scalability are very high, the marginal costs of setting up an extra user account are close to zero, which implies much greater benefits from economies of scale for platform businesses than for traditional businesses.

1.3. Common features of peer-to-peer businesses

The digital transformation of a traditional corporate business towards a more peer-to-peer business model implies a fundamental change in thinking, in corporate culture and organisation. The success factors of the peer-to-peer business lie in the following characteristics:

Figure 5: Common features of peer-to-peer business



Source: the authors

1. Design Thinking

Following the original definition of Brown (2008, p. 86), who was first in coining this expression, *"Design Thinking … is a discipline that uses the designer's sensibility and methods to match people's needs with what is technologically feasible and what a viable business strategy can convert into customer value and market opportunity."* It involves getting the best possible understanding of a users' needs and the problem to be solved by the product, including defining the problem strictly from the client's perspective, then generating new product ideas, prototyping and testing them. However, this process is iterative and not linear and takes place in close collaboration with clients. The approach seeks not to limit the creativity of developing new solutions by thinking about what resources are needed: first consider the ideal solution then the operational planning and not the other way around. In the past, product innovations were mostly driven by corporate technicians and engineers and sold by marketing people whose job was to convince customers of the benefits. In the design thinking mode, every innovation process starts from the customer's side and is operationalised by engineers.

2. Collaboration and Open Source Approach

In this approach, when developing production processes for a new product, companies should decide what they do best, identify where is their expertise and what could others do better. They should share information and collaborate with external partners in the supply chain. An open-source approach allows development and production of new products within a network of external partners. It requires a certain degree of openness and an outward-looking perspective in the corporate organisation.

Collaboration might be an expression everyone has an idea about. However, it is worth emphasizing the difference between cooperation and collaboration. Collaboration implies that a certain aim or goal can be reached only by joint efforts of participating partners. In other words, everyone depends for their success on the activity of the cooperating partner organisation. Successful collaborations require

a win-win-situation, where every partner benefit. In a cooperation it would be advantageous for the partners to work together, but they do not have to do so in order to achieve their goal.

3. Agile organisation

For a supply chain to be agile, its processes and organisation need a high degree of flexibility, which means they can react quickly to changes and be opportunistic. Decision-making must be rapid, with a flat decision-making hierarchy and employees empowered to decide autonomously. The corporate culture must allow for mistakes and risk taking. Now MVPs (Minimum Viable Products) are coming on the market, which on one hand shortens product development cycles, but on the other hand shifts the risk of product failures towards consumers.

4. Scalability

Within the collaborative organized supply chain all the interfaces of the corporate towards its stakeholders should be scalable in ways that are standardized and automated. Due to own capacity constraints, it is probably difficult to reach the point of full scalability. However, by close collaboration with network partners, which in effect become participants in the company's own production processes, a certain degree of scalability can be reached.

5. Sustainability

The new business process design has to be sustainable in the sense that it contributes to reaching the UN Sustainable Development Goals (SDGs) and aligns with the Global Reporting Initiative's (GRI) Sustainability Reporting Guidelines. Digitalization has led to a much higher degree of transparency and sensibility of clients and employees to the environmental aspects of business. People would like to know how much CO2 is emitted in production and if products are recyclable. In times of shortage of skilled labour, corporate social responsibility becomes a major argument for hiring people. The EU Commission made a first step with requiring reporting on environmental, social and employee-related, human rights, anti-corruption and bribery matters from EU companies with more than 500 employees. Further steps are expected to follow.

6. Coherency of digital transformation process

One difficulty in implementing such a process of digital transformation is that CEOs and top managers must lead a coherent process involving all employees and all departments. It cannot be done by an external consultant nor by the corporate's own Chief Information officer or Chief Digital Officer. Digital transformation is not just about installing new software applications, it is about implementing a new business organisation, model and corporate culture. Obviously, that might be difficult to do while order books are nicely filled and profitability is high, as the intrinsic motivation of top management to push for change might be not high enough to convert the current businesses model into a new one with an uncertain outcome.

1.4.Distributed Ledger Technology as facilitator of P2P-collaboration

Collaboration needs a lot of trust between partners as the desired result could only be reached together. Everyone depends on each other, like participants of a rope party when climbing mountains. Trust could be created when every participant has access to the same reliable information, at the same time, about activities and transactions. If only one shared database exists in the distributed network, recording all past transactions as a single source of truth for all participants, this is likely to be the case.

That is exactly what the Blockchain technology allows. It is a database technology for recording transactions within a network of peer-to-peer businesses. Blockchain has the advantage that data can be stored in the individual "blocks" in a tamper-proof way, which means that participants in the Blockchain are able to check the authenticity, origin and integrity of the stored data. As a peer-to-peer network, combined with a distributed time-stamping server, Blockchain databases can be managed autonomously. There is no need for a single administrator as administrator rights are distributed to all network participants.

Blockchain is a very simple database technology that enables collaboration, but it is not a magic bullet for success. It is just a technology to solve certain information problems, but if the problem itself is not well defined (no. 1), the participants are reluctant to share information (no. 2), decision-making processes are static and imbedded in a strong hierarchy (no. 3), data interfaces are not automated and standardized (no. 4), and the business process itself is not sustainable (no. 5), then a Blockchain application might be a waste of time and resources.

PwC (2016) put it well in its Q&A Blockchain FinTech

"Collaborative technology, such as Blockchain, promises the ability to improve the business processes that occur between companies, radically lowering the "cost of trust." For this reason, it may offer significantly higher returns for each investment dollar spent than traditional internal investments.

So what's the catch? You cannot get the return by yourself; you must be willing and able to collaborate with customers, suppliers, and competitors in ways that you have never done before."

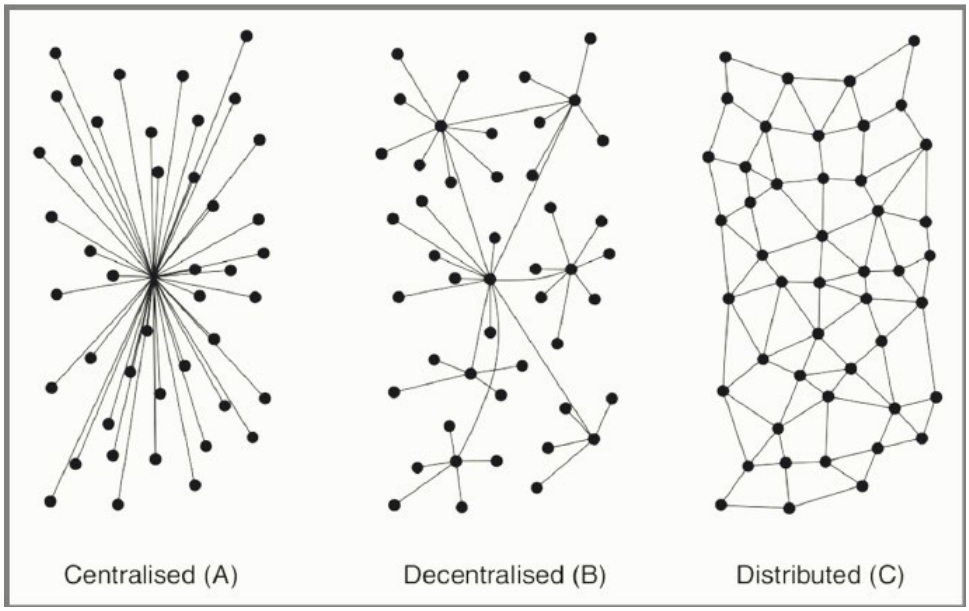
2. Distributed Ledger Technology: Internet of Value

2.1. Distributed Ledger Technology

Blockchain, probably thanks to Bitcoin, is the best-known type of Distributed Ledger Technology. If Distributed Ledger Technology (DLT) is the generic term, Blockchain is one type of DLT and Bitcoin is a specific application of the Blockchain technology for the use of payment tokens. The following section seeks to explain the overall idea of Distributed Ledger Technology compared to the traditional methods of using single ledgers for recording transactions.

A ledger could be defined as a database that records transactions in a chronological order with use of a time stamp. For example, if a bank customer opens his or her online bank account, transactions are sequentially listed. This is a ledger. For bookkeeping and accounting purposes, organisations typically run several ledgers for recording transactions within different parts and functions of the organisation. These single ledgers must be permanently reconciled and consolidated in one general ledger for monitoring and reporting organisational performance to management and for external documentation in business reports, balance sheets and income statements. Every corporate and every organisation is running its own ledger as a sealed and secured database. According to Fig. 6 it is a centralised ledger as the authorisation to change the ledger (right to write in) is exclusively with the corporate accountant.

Figure 6: Centralized, decentralized and distributed network models by Baran



Source: Baran (1964, p. 2)

A distributed ledger is a public ledger accessible by every participants of a network, that records transactions between peers in a chronological order by using time stamps. But unlike traditional ledgers, there is no single custodian such as the accountant in a corporate or in a bank, who has the exclusive right to change the state of the ledger by recording new transactions. In a distributed ledger every network participant can download the full list of transactions (complete history) and has the

rights to read, to write within (to change the state of the ledger) and to store the ledger. In a decentralised network, the authorization to change the ledger is restricted to a limited number of trusted nodes, while in a distributed ledger the authorization is with all network participants.

This automatically raises the question of who checks the accuracy of the new entries in a distributed database if there is no central institution or central custodian responsible for the integrity of the ledger? The validation of data in a distributed ledger is based on the following essentials:

1. The use of asymmetric private and public digital keys ensures that every new piece of information to be written in the database can be uniquely linked to the sending participant (proof of origin) and cannot be changed or manipulated because it is encrypted.
2. An automatically-running software algorithm called "consensus mechanism" guarantees that the same information is only recorded once in the database and the information is not duplicated. This is quite important as one would like to avoid, for example, that the same token is sold twice to different network peers. Therefore, the consensus mechanism solves the double spending problem as it always leads to a clear and unique distribution of ownership rights.
3. The recorded information is irreversible and immutable recorded within the database by using hash functions and time stamps for new data entries. Any attempt to change the data afterwards would destroy the chronological order and logical consistency of the chain of information and would immediately be detected.
4. The common database has high redundancy because it is kept by multiple network participants. Therefore, multiple copies exist within the network which are permanently synchronized, so that every network participant has at every time the same information. There is only one single source of truth within the network. The permanent synchronization of data and the existence of multiple copies makes the database resilient against hacker attacks.

In an ideal distributed ledger world, participants share a common ledger within a network and stop recording transactions in their own isolated ledgers. The peer-to-peer network is set up to be open-source and publicly-accessible, so all participants have equal rights and no hierarchy exists. Everyone is able to join the network and build any conjunction to peers within the network they desire. Every transaction - be it a bank transfer, a sale of real estate or a process for an insurance company - is carried out nearly just in time in one common ledger as database. The data is not centrally stored in the cloud. It is managed redundantly (multiple times) in the distributed network.

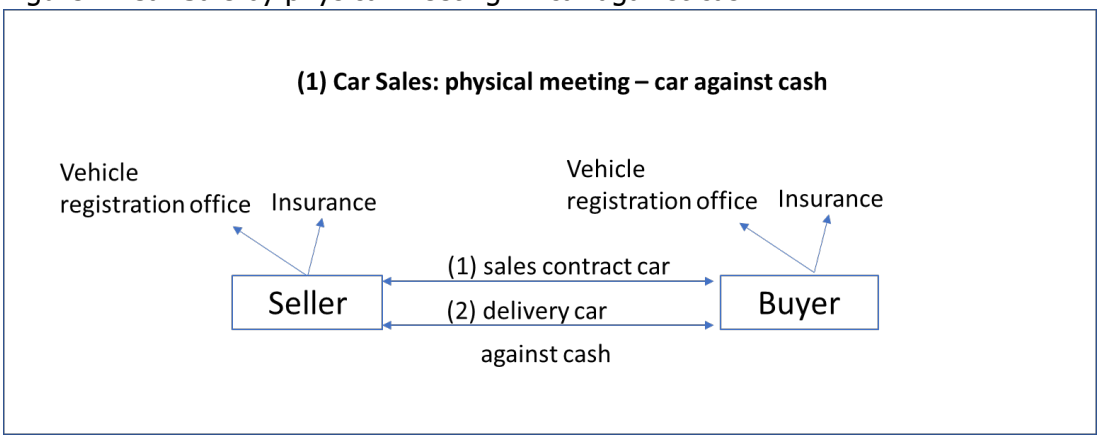
2.2. Example: Car Sale

The following example of a car sale illustrates the change of processes by recording a sequence of transactions within a common shared distributed ledger, instead of using various isolated organisational ledgers.

Car Sale: physical meeting - car against cash

The easiest way to sell a car is probably via a physical meeting between seller and buyer, signing a sales contract and handing over the car against cash. The sales contract contains the personal data of seller and buyer (identification via passport) and the technical details about the car (brand, type, age, technical defects, accidents etc.). The exact date and time when ownership changed are written in the sales contract document. Despite the fact that both parties receive a paper copy of the sales contract, the integrity of this document is not guaranteed. For instance, the time or other details within the contract could be fraudulently changed by one side after the event.

Figure 7: Car Sale by physical meeting – "car against cash":



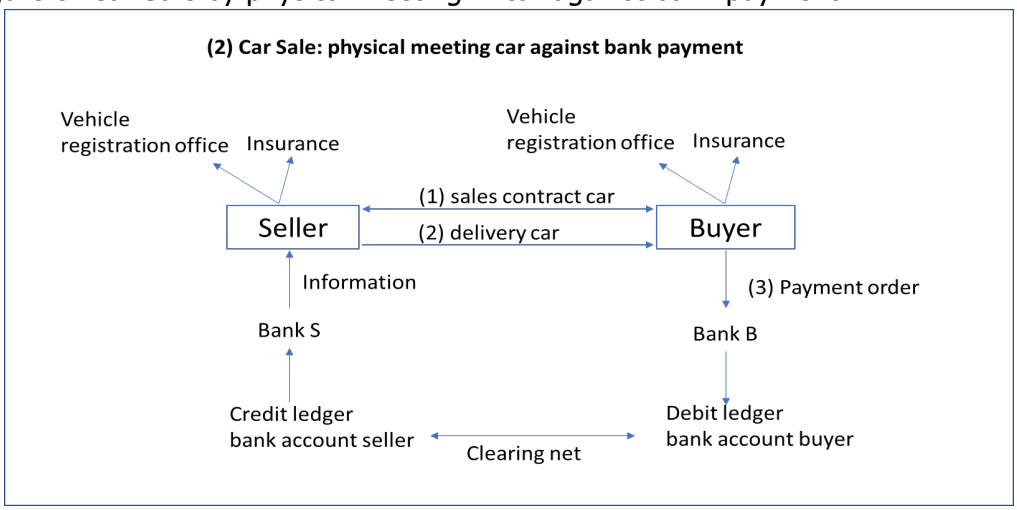
Source: the authors

After the deal is done, seller and buyer immediately inform their local vehicle registration offices and their insurers about the change in ownership. However, it would be optimal if vehicle registration offices and insurers were informed at the same time as the change of ownership happens. The time gap between change of ownership of the car and submitting the information to insurers and vehicle registration offices exposes seller and buyer to certain risks. Each organisation is running its own single ledger without any synchronisation or reconciliation of data changes between their organisations. Furthermore, in order to identify the individual and verify the change in ownership, all organisations register and store (probably the same set of) personal data about their clients.

Car Sale: physical meeting - car against bank payment

However, some cars might be too expensive to pay cash, so the buyer prefers to do the payment via their bank account. The buyer issues a payment order to their bank. The buyer's ledger is debited. Within two bank working days the amount is credited to the car seller's account via a clearing bank network.

Figure 8: Car Sale by physical meeting - "car against bank payment":



Source: the authors

Payment via a bank account makes this process of a car sale even more costly and cumbersome:

- As banks must comply with Know-Your-Customer regulations, the buyer's identification is done using previously-registered personal information and by their account number and Personal Identification Number (PIN). Furthermore, the transaction (online payment order) is verified by a transaction number (TAN).
- A bank remittance for changing the state of two different organisational ledgers takes one or two bank working days.
- This time difference between exchange of ownership of the car and the payment creates some credit risk for the seller not knowing if he or she will get paid. An ideal transfer would be "against-trade", meaning the car is transferred against payment, as with cash.
- A single transaction is recorded and reconciled in two different organisational ledgers, which are managed by different banks on behalf of their customers. To fully understand the effort and costs involved in maintaining an account on behalf of the client, one should bear in mind that this is only one ledger of thousands of customer accounts of a bank branch. The changes in each client ledger are in turn consolidated into various general ledgers of the single bank branch and of the banking group in order to manage the Bank's overall liquidity, investments and risks and for reporting to bank regulators.
- The bank client may pay monthly fees for having an account with a bank and takes the operational risk of the bank as a custodian of his ledger and the credit risk of the bank for keeping his deposits.

Car Sale entirely online

Is it currently possible to do the car sale in a secure way entirely online, meaning that the change of ownership - car against payment – is done on a digital basis? Probably not! Seller and buyer are confronted with the following difficulties:

- In most European countries, citizens do not have their own digital identity which makes it difficult to prove the identity of the counterpart.
- As the car itself cannot be transferred in a digital way, a digital identifier (asset token) is needed as a proxy. It fulfils two tasks:

- Being a legal title of ownership. Problem: most EU countries do not have secure digital vehicle titles and vehicle registration documents are of paper.
- Identifying the car (Type, Model, Colour, Serial No.), as such in its current condition. For used cars this might be more difficult than for brand new ones. In general, the digital identifier is the interface between the physical and the digital world.

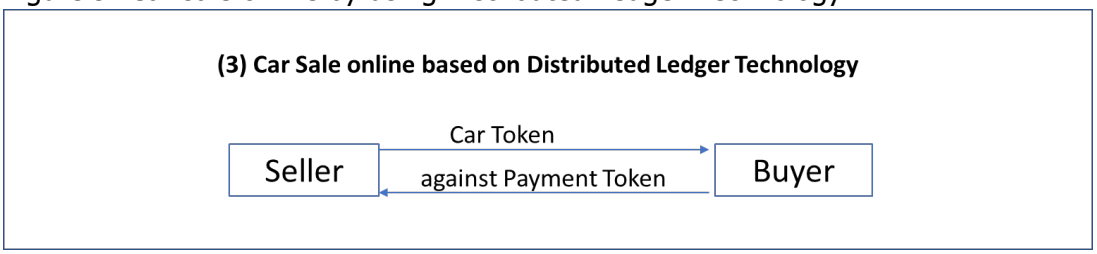
Currently the ownership of a car is documented by paper registration document, which cannot serve as a digital legal title of ownership.

- The payment could be done online via bank transfer but it takes time and creates by this a credit risk for the seller.

Car sale entirely online by using Distributed Ledger Technology

The optimal sale in this case would be "against-trade", as in example (1) in the sense of a direct exchange of values, without any intermediary between seller and buyer, "car against cash" but in a digital way. Therefore, the car needs to be substituted by a digital identifier and the physical cash by digital cash such as a payment token.

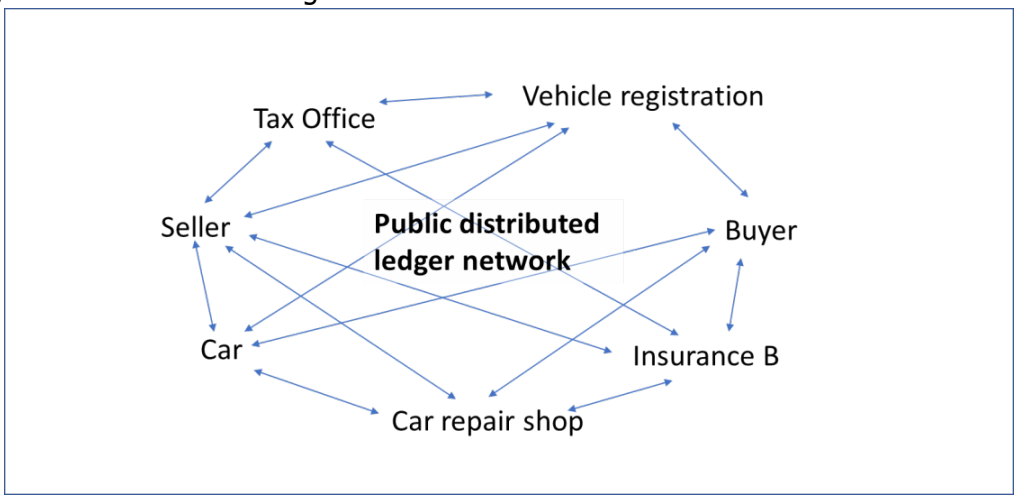
Figure 9: Car sale online by using Distributed Ledger Technology:



Source: the authors

Every participant involved in the car deal would be connected to the network and have access to the publicly distributed ledger. Access implies that everyone keeps their own copy of the database and has the right to see and to change the status of the database by writing and reading. The ledger is permanently synchronized making sure that every participant sees the same data at the same time.

Figure 10: Distributed Ledger of Car Sale Network



Source: the authors

The DLT solution for the online trade of the car is based on the following assumptions:

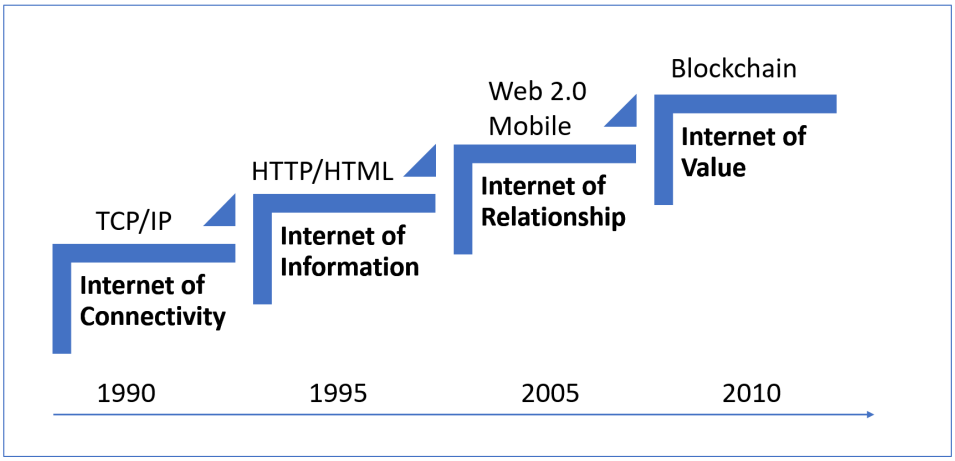
- **Buyer & Seller - Proof of Identity:** Buyer and seller are the sovereign of their own digital ID and verify each other's identity by using cryptographic tools such as private and public keys. This concept of identification differs significantly from the current way of identifying individuals: Every network participant is the sovereign of his or her own private data and especially their digital identification. For example, the car insurer receives a public key from the client, which provides them with temporary access to the relevant private data. Every access to the individual's private data is timestamped and registered. So the insurer could verify the identity of the client but has no reason to build up or to keep their own central repository of clients' identity data. The individual is their own custodian of their private database and decides who sees what. The window opened by the client for the insurer might be a different one than that opened for the vehicle registration office, as different private information is relevant.
- The **car token** represents a legal title of ownership and transfer of title is recorded on a Blockchain making it secure and accessible by all relevant parties. The car has its own ID as the token serves as digital identifier. All transactions related to the car could be recorded in the distributed ledger: Date of first registration of the vehicle, damages and repairs, mileage, technical details, GPS data, etc. The digital identifier is the public key giving the buyer access to relevant data. With this token and the underlying information, the car could be traded online. Furthermore, in days of automatic driving it might be the case that the car automatically drives to the charging station or to the car repair shop and does an automatically payment with its own wallet for the service received.
- **Seller as car owner identified?** Proof of Ownership: By having the complete history of recorded transactions, the seller of the car has to be at some point in the past listed as a receiver of the car, so the validity of a transaction could be proven. If the seller never received the digital assets, he or she could not be the owner.
- **Car sold twice?** - Prevention of double spending: The problem with digital assets is that they could easily be double spent, meaning the seller could have transferred the ownership of the car twice or even several times to different network participants. The data recorded in the ledger has to be accurate and consistent, which will not be the case when two conflicting transactions are recorded. A purely bilateral consensus with digital signatures about the deal between buyer and seller is not sufficient to prevent double spending as there might be several bilateral consensuses in the system. This problem is solved by the network protocol and some algorithm software, which determine the way to select only one of the conflicting transactions. Finally, the network as a whole validates the consistency of the recorded data with the given data history. It is worth emphasizing that the whole process of verification and validation is done by an automatically-running algorithm software within minutes and not by a central authority or an intermediate or central custodian.

- **Payment tokens** are used as a means of payment for acquiring goods or services to enable a direct exchange of value between network peers without the use of banks and banking ledgers. The most prominent example is Bitcoin.
- **Smart contracts,** could provide an automated way to trigger payments to a supplier once performance has been proven by tokens.
- **The deal is fixed!** Immutability and irreversibility of recorded data: Buyer and seller need to be 100% sure that once the data is recorded neither the data nor the time stamp can be altered. Here again the DLT relies on cryptography and uses hash functions to seal every record like a digital finger print.
- **Payment order, car insurance and vehicle registration** could be done by smart contracts. Distributed ledgers are databases which could store the transactions of digital assets as well as some software code that leads to the automatic execution of a transaction contingent on a certain event. At the same time as the ownership of the car is transferred, then the payment order should be sent out, the vehicle registration automatically changed, and the insurance contracted. Besides the convenience, the simultaneity of executed transactions reduces several risks for the parties involved and is an important feature of DLT.

2.3. The Internet of Value

The Distributed Ledger Technology facilitates the adaption of our economic life and its organizational framework towards the decentralized network structure of the Internet. Until now, the Internet was primarily used for decentralized communication, the public use of information via web pages and for social media. But the direct digital exchange of values between peers has been hardly possible as it still requires the involvement of several intermediaries which know and check the identities of those involved and document the change of ownership in siloed organisational ledgers. The Distributed Ledger Technology empowers peers to exchange digital assets without intermediates and without the use of platforms in a secured and trustful way. Within the new Internet of Value, the ability to initiate the exchange of values, the legitimacy of authorisation of ownership, the proof of identity and the transaction consent of a change in ownership rely totally on the responsibility of the peers and are done in a decentralised way within the network without using a central authority.

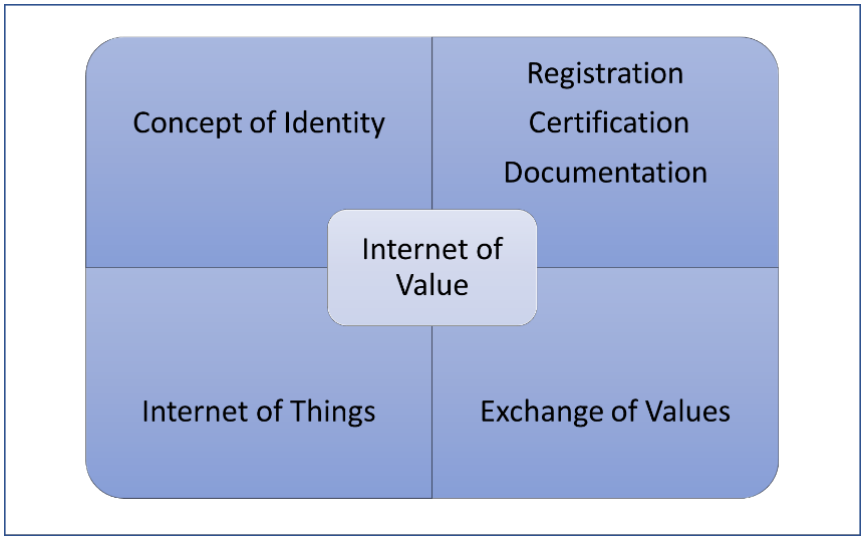
Figure 11: Evolution of Internet Applications



Source: In accordance with VDI (2018, p. 31)

The Internet of Value based on the Distributed Ledger Technology strives for a strictly decentralised organisation of interactivities between peers without any centralised platform acting as intermediary. The technology is disruptive as core elements of the current organisation of value exchange will change radically. This applies in particular to four areas: (1) Proof of identity of customers, of clients, of user, of patients and the associated handling of private data; (2) Recording, documenting and certificating of transactions, of the change of value and of entrepreneurial success; (3) Organisation of the value exchange and the transfer of values and utilities; and (4) Integration of objects, of machines and of robots in communication and transaction processes.

Figure 12: Core Elements of the Internet of Value



Source: the authors

2.3.1. Concept of Identity: Self-Sovereignty on private data

The proof of identity, the knowledge about who you are, is essential for any contractual relation in our society. The proof of identity relies on personal information such as name, date of birth, fingerprints, passport number, bank account etc.. The contracting parties must be 100% sure of the identity of the counterpart and its accountability in case of a breach of contract. Identity theft and misuse of personal information by hackers are high risks.

In the current system, the identity of individuals is provided by organisations, public administration and corporates. Nowadays, each individual has a hardly manageable number of passwords for the use of online services, processing of online transactions, payment services, credit card transactions, etc. because every online merchant, every bank, and every platform registers and collects personal user data and assigns passwords to determine the user's identity when logging in. This means that the same private data of a single user is stored redundantly in a large number of corporate data silos. The private corporate provides the user of a service with his or her identity and not the other way around. Each administrative identity system is proprietary and owned by the organisation that provides it. The balance of power between customer and company is characterized by a strong asymmetry, as the customer cannot understand what is happening with his or her data, how they are processed via algorithms, how much money the company earns with the users' data. The customer has to trust the company or the platform almost blindly.

Platforms such as Google, Facebook, Amazon and banks even offer this service as identity provider to other web-based organisations and services for the benefit of collecting more and more user data to feed data analytics and algorithms. At first glance, this might have a benefit for users that their Google or Amazon passwords are used more universally over the web, but it increases their dependency on a single company, which becomes gradually a monopolist of personal data.

As Finck (2018, p. 7) writes: *"Large intermediaries such as Google, Amazon, Apple and Facebook control how we search, shop and connect. They autonomously collect, store, process and monetize our data trails. This, in turn, enables them to expand their position of power in building on the data mountains they sit on, for instance to train new algorithms. Such market power has caused concern from a competition policy perspective as it burdens market entry."*

With this concept of identity management done by business organisations the individual has no control over their own personal data and has no chance to monitor the external use of their personal data for business purposes. And it is not very efficient either. If, for example, the personal address or credit card number changes, hundreds of data records from different organizations have to be updated because there is no automatic data reconciliation between private organizations. When moving from one place to another, the individual will probably change medical doctors but their health data does not move to the new doctor or hospital and remains in the disconnected data silo of the former practitioner. And even from a company perspective the handling of private data becomes costly and burdensome as the new European General Data Protection Regulation strengthens user rights by imposing clear legal duties on the corporate's handling of the user data.

The Distributed Ledger Technology is based on a decentralised concept of identification: Every network participant is the sovereign of their own private data and especially their digital identification. The private data and its attributes are owned and controlled by the individual, are stored by their in a digital safe and could be shared partly or fully, temporally or permanently and restricted or unrestricted concerning the use with other network peers via a public key. Every access of a third party to the private data base is registered, recorded and time-stamped. The self-sovereignty concept includes the right of data portability taking personal data away from one organisation and shifting it to another or to a private storage place.

Currently there are several attempts in the Blockchain developer community to reach the self-sovereign identity system of individuals such as Sovrin, uPort and Veres One. All these concepts have in common that the individual owns a decentral digital identifier, which empowers the individual as the sovereign of their private date to decide for themselves about publication of data to the outside world. External organisations do verify the identity of individuals but are no longer the provider and the issuer of the individual's identity. This concept of self-sovereign identity implies a radical shift for organisations, which would no longer have to register, process and store private user data and issue passwords. On the other hand, it might change the power relationship between individuals and platform businesses in regard to the use of private data for data analytics and algorithms.

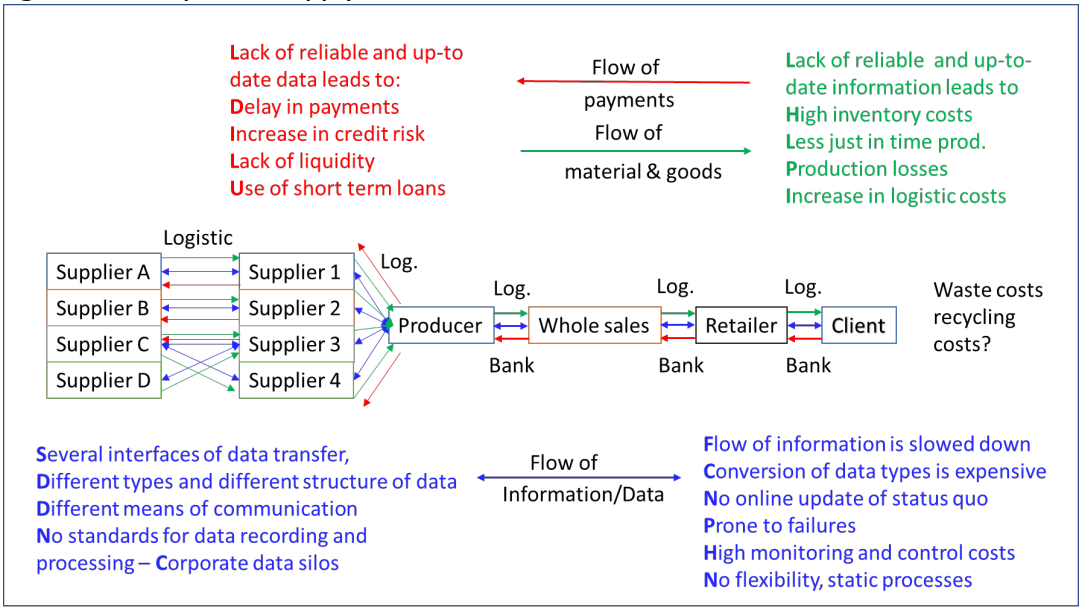
2.3.2. A game changer for registration, certification of value

Many companies already operate globally in the real economy and are integrated their decentralized international supply chains. But even though they act decentrally, the monitoring and reporting of transactions is still done centrally, on a corporate by corporate basis. The recording of transactions within different ledgers and the reconciliation with a general ledger has become extremely complex, time-consuming and prone to failures.

The use of cryptography enables DLT to record and to store the data in a tamper-proof way, which means that network participants can check the authenticity, origin and integrity of the stored data. In this way, the distributed ledger becomes an ideal solution for the storage of all kinds of certificates, registrations, reports and grades which are currently kept securely at high cost in the siloed databases of issuing organisations such as universities, corporates, health organisations, public administrations or land registry offices etc.. The physical flow of goods between parties, the transfer of ownership of the components and the stream of forecast data can all be tracked in a synchronized manner.

Iansiti and Lakhani (2017) compare the impact of Blockchain on the world of record keeping and accounting with the development of TCP/IP (transmission control protocol/internet protocol), which laid the groundwork for the development of the internet: "*TCP/IP unlocked new economic value by dramatically lowering the cost of connections. Similarly, Blockchain could dramatically reduce the cost of transactions. It has the potential to become the system of record for all transactions. If that happens, the economy will once again undergo a radical shift, as new, Blockchain-based sources of influence and control emerge.*"

Figure 13: Corporate supply chain



Source: the authors

Optimal supply chain management needs a frictionless flow of information about the physical flows of materials and goods and the flow of payments within the process.

Despite the fact that different actors are involved in the flows of material and payment, the flow of information has to unite all information within one shared ledger accessible to every supply chain participant. For instance, if there is some delay in the delivery of input material from supplier A at the very beginning of the chain, all subsequent participants need to be informed at the same time, so they can all respond immediately to the delay. The logistics company could change their transport routes, the producer could take a different client order first and the client is also informed about the delay. With a shared, distributed ledger every participant has at the same time the same information and everyone has the right to change the status of the ledger. This will ultimately lead to more flexibility of processes, lower inventory costs and a reduction in credit risk. Furthermore, the use of smart contracts combined with cryptocurrencies as payment tokens allows for some transactions to be automated.

DLT enhances transparency in the supply chain of products as every single part of a final product could be tracked in chronological order from the origin to the final point of sale. Even data such as the duration of use by the customer and the costs of waste could be recorded. The complete information of the product life cycle could be enriched with complementary data about the environmental costs of production by using sensors and cameras with their own network IDs. In this way, monetary values such as the price of a product or the profit of a company could be clearly linked to values of natural capital and environmental costs. Distributed Ledger Technology could be an enabler for a sustainability-based accounting of value.

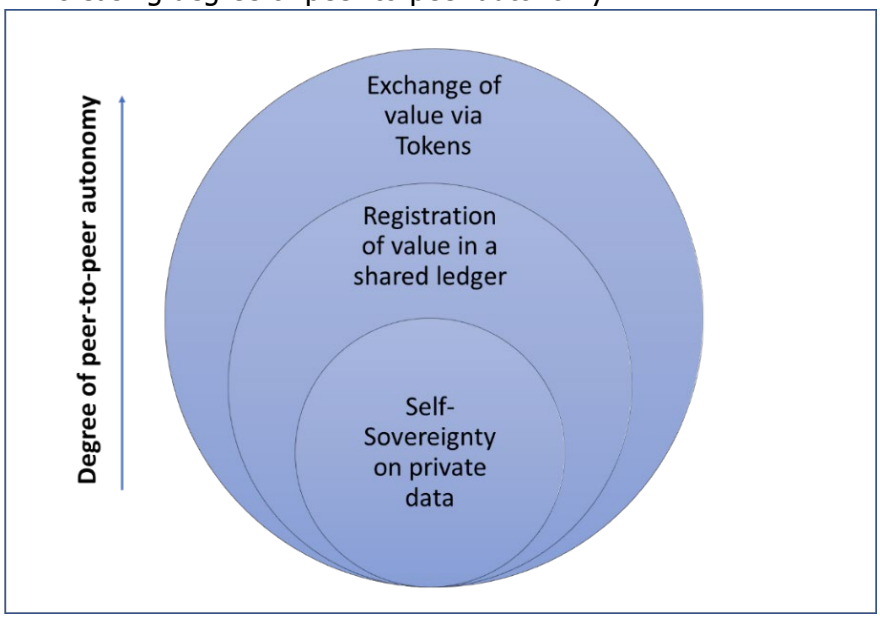
In some way DLT enables the nominal sphere of accounting and value to reunite with the physical world of trading goods in the supply chain. The decentralisation of both systems will radically lower the complexity of accounting and thereby reduce the costs of monitoring and controlling.

As IBM (2017, p. 5) writes about a "Message-based versus state-based communications":
"Today, organizations send messages back and forth to accomplish various tasks, with each organization maintaining its state of the task locally. On Blockchains, messages represent the shared state of the task, with each message moving the task to the next state in its lifecycle. Blockchains shift the paradigm from information held by a single owner to a shared lifetime history of an asset or transaction. Instead of message-based communications, the new paradigm is state-based."

2.3.3. Exchange of Value via Tokens

The Self-Sovereignty of Private Data and a decentralised registration of value in a shared common ledger are prerequisites for exchanging values as pure virtual assets directly between peers. The decentralised setting of DLT does not need a central authority to run a central account for value or execute the exchange of value. Peers are empowered to exchange value by their own initiative.

Figure 14: Increasing degree of peer-to-peer autonomy



Source: the authors

Focussing on underlying purpose and economic function, the Swiss financial market regulator FINMA (2018) categorises tokens into three types, but hybrid forms are possible:

- **Payment tokens** are synonymous with cryptocurrencies and have no further functions or links to other development projects. Tokens may in some cases only develop the necessary functionality and become accepted as a means of payment over a period of time. Payment-tokens are value-based means of payment as they are stored locally and not in an account of a central bank or a commercial bank.
- **Utility tokens** are tokens which are intended to provide digital access to an application or service.
- **Asset tokens** represent assets such as participations in real physical underlyings, companies, or earnings streams, or an entitlement to dividends or interest payments. In terms of their economic function, the tokens are analogous to equities, bonds or derivatives.

Payment tokens

Probably the most prominent example for a payment token is Bitcoin as it was the first issued token and Satoshi Nakamoto (2008) could be seen as the founder of the cryptocurrency idea. Since then (2010) more than 2,000 cryptocurrencies with a market volume of $210 bn (11/2018) have been created.

According to the Bank for International Settlements (2018, p. 97), "…*cryptocurrencies combine three key features. First, they are digital, aspiring to be a convenient means of payment and relying on cryptography to prevent counterfeiting and fraudulent transactions. Second, although created privately, they are no one's liability, ie they cannot be redeemed, and their value derives only from the expectation that they will continue to be accepted by others. This makes them akin to a commodity money (although without any intrinsic value in use). And, last, they allow for digital peer to-peer exchange".*

The most important point in the BIS-statement is the last one: "Payment tokens allow for digital peer-to-peer exchange". The current means of payment circulating in the financial system do not allow for digital peer-to-peer exchange as they are issued by central authorities within the two-tier system of commercial banks and central bank. Therefore, if the Distributed Ledger Technology is to gain acceptance in the real economy by trading directly peer-to-peer, payment token will need to become the natural complement for exchanging value on a digital basis.

As the BIS states, payment tokens are created privately and their value derives only from the expectation that they will be accepted by others. They do not serve as a legal tender recognized by a legal system such as coins and notes. However, following the current discussion, some central banks might issue digital forms of value-based cash in the future. The Swedish central bank announced a pilot project called "E-krona" in 2019 (Juks, 2018). The E-krona should be designed as a value-based payment token.

Utility tokens

In the past three years a lot of start-up companies with business models relying on DLT have issued utility tokens to raise money for business projects. Referring to the initial public offering of shares (IPOs) the issuance of tokens has been called *Initial Coin Offering (ICO)*. But unlike equities markets, the market for tokens is completely unregulated and no prospectus as a legal document to inform investors is required. However, ICO issuers are publishing a 'white paper', which provides investors some information about the company and the utility linked to the token. Most tokens are traded at market prices on digital token or crypto-exchanges, so investors can buy and sell. Investor protection is extremely low in this segment as neither the issuance of tokens nor trading of tokens on crypto exchanges are regulated by a financial authority and are not governed by financial law.

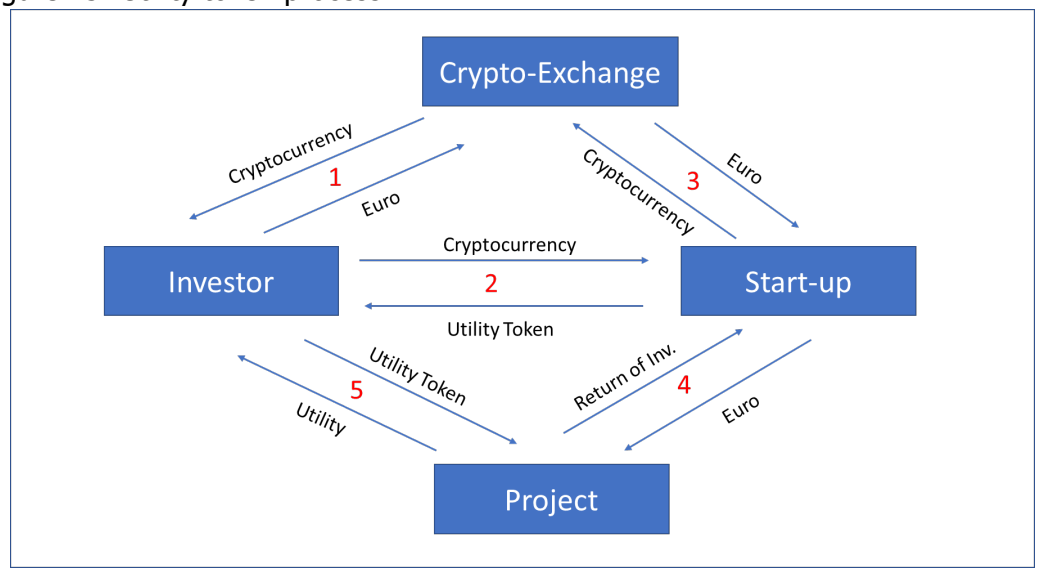
However, in general, utility tokens are comparable to reward-crowdfunding as the investor (pre-) finances a certain company project and gets in return a kind of voucher to receive a product or service at a later stage.

The SMSG (2018) points out the funding aspect of utility tokens for start-up companies by writing:
"37. Utility tokens representing services may facilitate trading in such services and present an alternate source of early stage funding for innovative projects. They are comparable to a voucher and to crowdfunding by coupon. They allow prefunding of a future business without diluting ownership. In this respect they represent an alternative model to traditional venture capital funding, insofar as the project-owner transfers a proportion of the project risk to future consumers without diluting ownership interests. 38. Apart from funding, those tokens also have a business dimension: by issuing those tokens the issuer creates a network of users, which further increases the value of the business."

A difference with crowdfunding is that the stream of cash flows and tokens relies entirely on DLT. Furthermore, smart contracts are used to automate the transactions. (1) The investors exchange fiat currency such as Euros against cryptocurrency. (2)

They buy the utility token in return for cryptocurrency (3) The company exchanges at least part of the cryptocurrency against fiat currency; and (4) invests the fiat money in the project. If the investment is successful the company receives a return of investment. The investors (5) are rewarded with a utility, which is linked to the project's product or service.

Figure 15: Utility token process



Source: the authors

Asset tokens

Asset tokens represent the ownership of the underlying asset and enable the exchange of value without physical transfer of the asset. In those cases where the asset token serves as a legal title securing ownership on the underlying asset it enables an "against-trade" exchange, in the sense that goods represented by the asset token are exchanged against payment (payment token). The function of the asset token is similar to the bill of lading used in international trade. The bill of lading serves as legal title to the shipped goods and, instead of an exchange of goods against payment, the bill of lading is used as a proxy for the shipped goods. This type of documentary payment is used in international trade to reduce the credit risk of exporters. It will be the same with asset tokens. Therefore, escrow accounts and trust brokers will no longer be needed.

Asset tokens function as well as digital identifiers for the underlying physical asset. If a physical object has its own ID, it can record its own history of origin. Big data plays a major role here. Information based on big data analysis can provide any buyer of an asset token with a very accurate representation of the current condition of the underlying object.

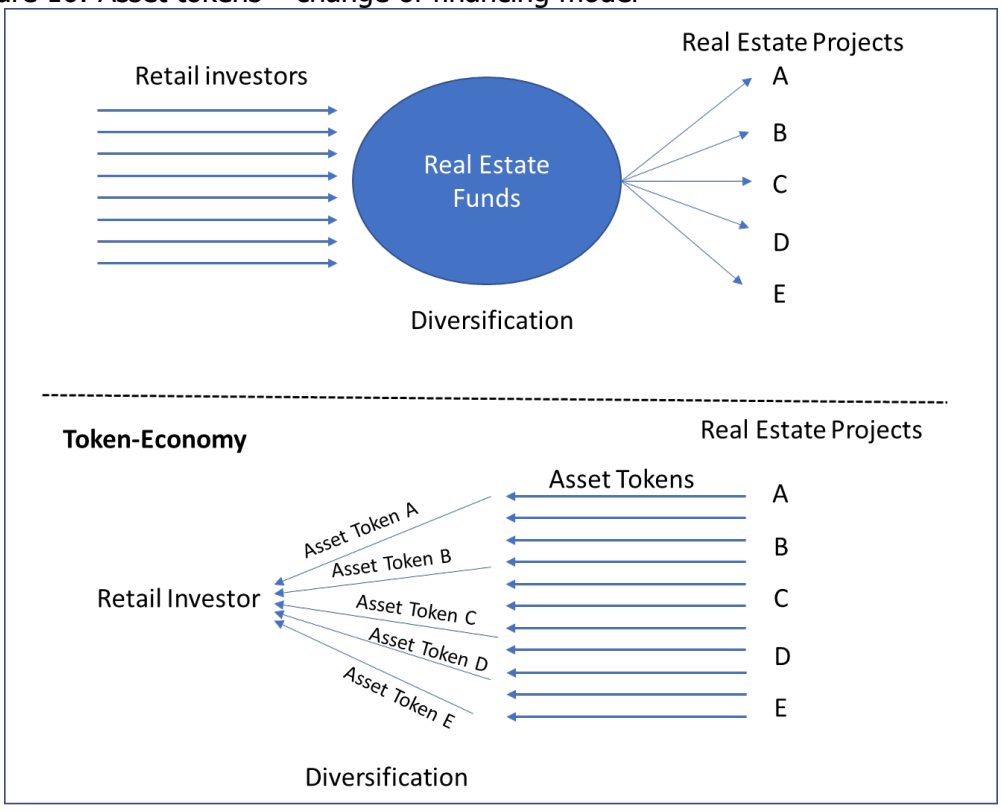
As Zwitter (2014, p. 2) states: "*Big Data represents reality digitally much more naturally than statistical data—in this sense it is much more organic.*" Furthermore, with the use of asset tokens the object becomes traceable within the supply chain which is beneficial for the corporates involved. The digital ID linked to products could solve problems of counterfeiting and product piracy as well.

The asset token might provide the bearer with real physical control over the asset. For instance, in the Sharing Economy such as car sharing this might be an advantage

as the asset token could at the same time serve as a key for opening and running the shared car.

Recently and for the first time, a building in Manhatten, New York, worth $30 million, has been sold in tiny pieces via asset tokens. The issuance of asset tokens by the real estate project empowers retail investors to set up their own diversified portfolio of real estate assets by buying directly with little volume – without middlemen - from the project owner. In the past they had to rely on real estate funds managed by a portfolio manager in order to participate in a pre-diversified portfolio, while paying fees to a portfolio manager. Here again, the features are similar to crowd funding: Assets are split up into small asset pieces (equity or debt) and sold to the crowd of retail investors. However, with crowd funding a platform does the matching between buyer and seller, which is not the case here. The token sale takes place without any intermediary, directly peer-to-peer. Figure 16 illustrates the difference between the business model of traditional real estate finance via funds and the token economy model.

Figure 16: Asset tokens – change of financing model



Source: the authors

Costs of token creation and issuance

The actual creation of a token is relatively simple and fast. Ethereum has certain standards for the creation of smart contracts and tokens (ERC-20), which define common rules for communication between network addresses and access to Smart Contract Code.

In contrast to IPOs, companies arranging an ICO are so far not required to publish a securities prospectus due to a lack of legislation and regulation. For the investor's information, there is only a so-called white paper describing the project and the use of the ICO proceeds. However, white papers are by intention not very concrete concerning the return on investment, as ICO issuers are reluctant to get involved with

financial laws and regulating authorities. The most expensive parts of an ICO are probably communication and marketing, which primarily take place via all possible social media channels. ICOs are listed for trading at Cryptocurrency exchanges, which are again compared to securities exchanges and act outside financial regulation.

Figure 17: Table of ICO costs

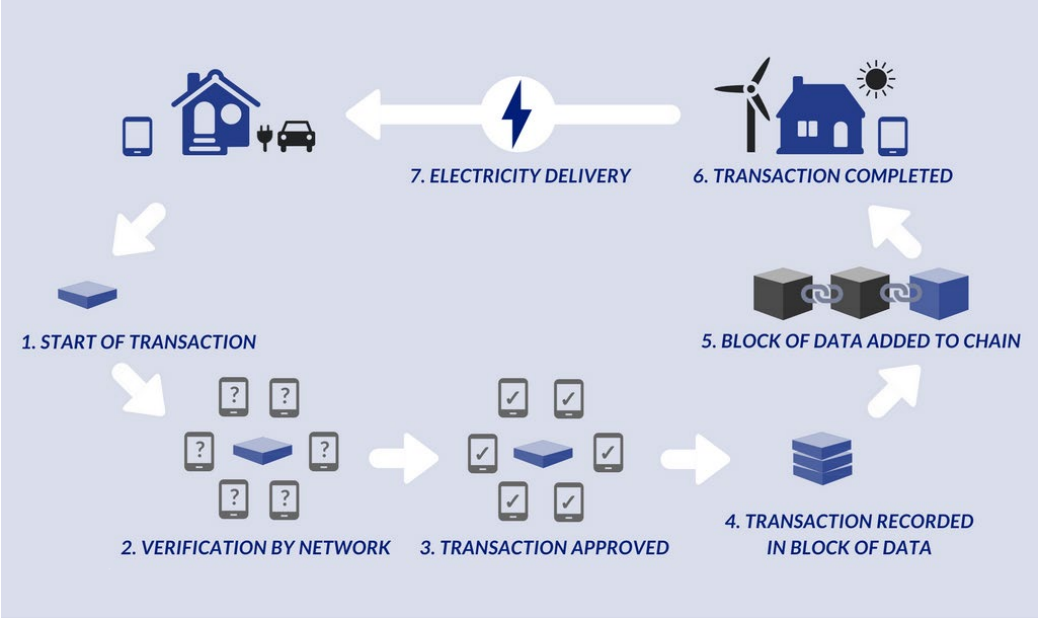
Expense	Cost ($)
Whitepaper	$5,000 - $15,000
Website	$10,000 - $20,000
Marketing	10% - 20% of Funding Target
Blockchain Dev	$5,000 - $15,000
Security Audit	$10,000 - $50,000
Legal Expenses	$50,000
Exchange Listing	$5,000 - $1,000,000

Source: Bitcoin market journal

2.3.4. Internet of Things

Progress in robotic and sensor technology, combined with big data analysis and self-learning algorithms, has led to a network of physical devices that can connect, collect and exchange data and take autonomous decisions. Decision-making by machines could include autonomous driving of cars, smart home decisions by heating systems, or business decisions. Objects are enabled to act and interact autonomously within a network by recording transactions and by just in-time validation and verification of transactions within the network, as shown in an example for the energy market in Fig. 18.

Figure 18: Application of Internet of Things in the Electricity Market



Source: website United Nation Climate Change

The energy market is organised decentrally like a grid with a lot of different producers and municipal energy suppliers connecting millions of households. What makes it complex is that many households already produce their own electricity using solar panels and are sometimes on the demand side and other times on the supply side. This is where DLT can fully demonstrate its strength. Energy supply might gain efficiency if consumers and producers were directly connected via the network, with smart contracts enabling autonomous transactions with just-in-time transaction recording.

For identification purposes, a digital identifier of objects becomes a prerequisite to know which machine has made which decision at what time. There is also the question of accountability in cases where machines make wrong decisions and cause damage.

3. Lack of governance structures

Distributed Ledger Technology is not an innovation that comes overnight. The application of DLT implies the entire reorganisation of business processes and a radical change in corporate culture towards collaboration and openness. It probably will take years to become a standard technology. The main challenge of DLT is the lack of governance structures, as well as pure technical issues such as the lack of scalability, and high energy consumption and latency time, which probably could be solved in the near future. There is also the question of whether this radically new form of a decentralised, peer-to-peer based exchange of values can be integrated into the existing legal system at all or whether completely new legal bases should be created. Although the economic benefits of using DLT are tangible, it will not work without legal certainty for users of the technology.

3.1. State Governance versus Libertarianism

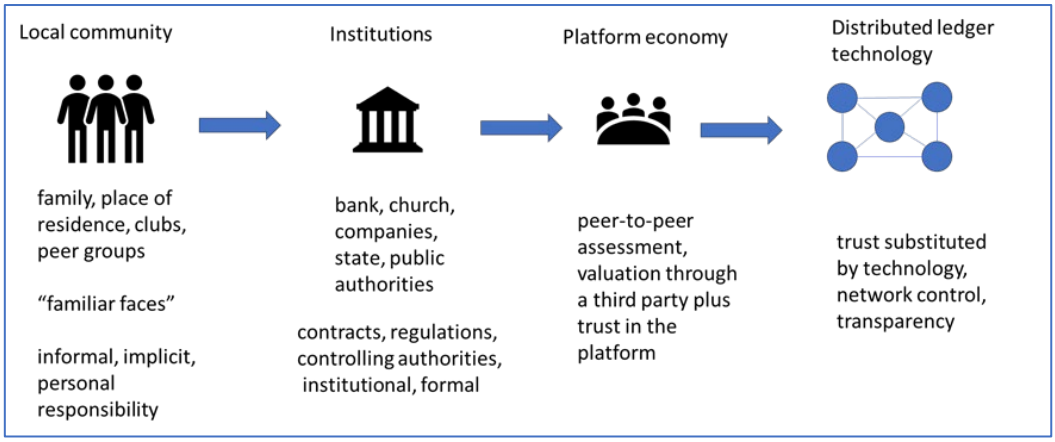
When reading the first lines of Satoshi Nakamoto (2008) famous white paper "Bitcoin: A Peer-to-Peer Electronic Cash System", the idea of creating a private cryptocurrency called Bitcoin could be easily linked to the Libertarian school of thought:

"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers."

In short Libertarians distrust central authorities and the power of the government and stand for a maximum of individual autonomy and freedom. Satoshi Nakamoto goes a step further by suggesting that cryptographic proof should substitute for interpersonal trust. In this sense the Blockchain is often called a trust machine.

According to this idea, technological progress brings a series of shifts of trust within society from interpersonal trust in the community, to institutional trust, to trust in peer-assessments on web based platforms, and finally to trust in the Distributed Ledger Technology.

Figure 19: The technological shift of trust in society



Source: Based on video of R. Botsman, We've stopped trusting institutions and trusting strangers (Botsman, 2016)

In local communities where everyone knows each other, less formal regulation is needed as interpersonal trust exists and regulation is more informal, based on social control. This might have worked as long as the community is small. But with increasing urbanisation society has shifted trust to institutions such as banks, central banks and public authorities, which are regulated by law. Users trust the institutions as they believe in the public regulation and enforcement of laws by public authorities. In the past years internet platforms such as Amazon, Airbnb or Uber arose, which create value by facilitating exchanges of information or values between their users. Despite the lack of public regulation of platform businesses, consumers trust platforms as they publish peer-to-peer assessments of their users. Finally, the Distributed Ledger Technology shifts trust towards a new level: trust in technology, network control and transparency.

It is probably an illusion to believe that DLT could work without trust as long as human peers interact in the network but the interface between the real and digital worlds is not perfectly covered. There are still some loopholes in the system. If the original document or certificate which is saved by using a hash function in the Blockchain is faked, it will be stored irreversibly as a fake in the distributed ledgers. Or if the cameras or sensors recording a physical transaction are manipulated, the digital record will be so as well.

With regard to the impact on society, another point seems to be important. The use of Distributed Ledger Technology strengthens the power of the individual vis-à-vis institutions, but at the same time shifts the risk to the individual. Intermediaries also absorb risks for their users. Should these cease to exist, individuals will have to bear the risks. One example is the concept of self-sovereignty of private data: For some individuals it will be a blessing but others will find it difficult to cope with this new responsibility. Therefore, the solidarity systems from the "old" world of central institutions (such as health, pension, unemployment insurance, etc.) must be integrated in a new form into the decentralized world of peer-to-peer networks. Perhaps completely new digital forms of social security for the individual will emerge in regional networks and communities. Whatever the peer-to-peer world will look like in the end,

it will need a layer of solidarity between the peers, so that the law of the strongest does not apply here alone.

3.2. Legal issues with DLT

The problem of regulation is that it is nearly always lagging three to five years behind reality. In the financial sector, for instance, the EU Commission just proposed a new law for regulating crowdfunding platforms. Politicians and regulatory authorities are still struggling with the regulation of the platform economy, so any regulation of Distributed Ledger Technology application cannot be foreseen in the next years. This is a misery as the adoption of such a radical new technology with huge potential impact on organisations will need public governance, a legal framework and regulatory authorities to act as trust brokers. Given the strategic relevance of DLT, European policy should therefore prioritise DLT within its legislative and regulatory processes.

However, it will not be easy to regulate this network technology without a local anchor, starting with the jurisdiction and court that will be responsible for regulating a web-based network distributed throughout the world. Could the European Commission do it or does it have to be done at G20 level with multinational intergovernmental organisations? Any regulation would need to develop a concept of democratic governance for the distributed ledger and the network behind it, without putting a central regulatory authority in place. A central regulator would probably contradict the idea of a distributed and decentralised network. It will be something totally new for any government and legislative authority to develop regulation for a network without direct intervention or enforcement power for public network authorities.

One idea based on Hileman and Rauchs (2017p. 61ff.) could be to integrate regulatory authorities as a node in the network receiving a full replica of ledger transactions or being copied into each transaction in which they show a specific interest. Moreover, regulators might be equipped with voting power in verifying and validating transactions, which empowers them to reject transactions immediately. In short, distributed ledger networks provide regulators with the opportunity to monitor, supervise and audit trades and agreements in real time, which could dramatically improve the capability of regulatory systems being in place today.

3.3. Legal issues with Smart Contracts

Distributed Ledger Technology and the associated automatic execution of transactions by software code ("Smart Contracts") entail considerable legal problems and contractual uncertainties for its users. This starts with the difficulty of identifying the location of the network and thus the relevant jurisdiction and competent court, if it comes to a dispute about a contract. Which contract law is applicable in which country and where is the place of jurisdiction?

Furthermore, a software code that represents an "if-then relationship" written in computer code instead of natural language that lawyers use is hard to characterise as a contract in the legal sense, even if the name "Smart Contract" suggests that is how it should be seen.

In most jurisdictions a legal contract is defined as follows:
A contract is an agreement giving rise to obligations which are enforced or recognised by law. The factor which distinguishes contractual from other legal obligations is that they are based on the agreement of the contracting parties. Treitel (2003(1-001))

Under common law the formation of contract generally requires an offer, acceptance, consideration of the offer (form of value that must be exchanged), and a mutual intent to be bound. Each party must have capacity to enter the contract. " Contract – Wikipedia"

Obviously, the software code does not formally represent a legal contract. The problem starts with the computer language which is not readable and understandable for the contractual parties. How could counterparties prove that the software code reflects their intentions if it is not readable? A conceivable solution might be a translator or something like a compiler of computer language in the natural language of legal drafting and vice versa. However, natural human language has its own interpretations and natural subjectivity which does not really fit with binary code. Frequently, lawyers use terms in legal contracts that are not clearly defined such as "may" or "in good faith" or "by mutual agreement" or "commercially reasonable manner" which are highly contextual and open to interpretation. These unspecified terms do not translate into a discrete yes-or-no interpretation of a binary code.

As Linklaters and ISDA (2017, p. 13) wrote: *"More fundamentally, it is very difficult (and perhaps not advisable) to strip a legal system of obligations of all ambiguity. The nuances of complex relationships can be difficult to define, let alone to reduce to paper, and words can mean different things to different people."*

As an English judge pragmatically noted:
"The words used may, and often do, represent a formula which means different things to each side, yet may be accepted because that is the only way to get 'agreement' and in the hope that disputes will not arise." Lord Wilberforce (1971)

It remains to be seen how this problem of the missing link between software code and the legal code of the lawyers will be solved.

3.4. Privacy, tracking and data protection

The concept of the self-sovereignty of the individual over his private data presents both advantages and risk for the privacy of end-users. Clearly, in a decentralized system like Distributed Ledger Technology, the user regains autonomy over his or her private data. But a common ledger, which is kept decentralized and without intermediaries, needs a much higher degree of openness and transparency compared to centralized solutions. Network peers need to verify the authenticity and integrity of the data by proving the history of transactions stored in the distributed ledger. Although Blockchain users may believe themselves to be anonymous by using pseudonyms, it might still be possible to find out the user's identity by tracking historical transactions and by recognizing certain patterns.

As De Filippi (2016, p. 0) wrote about the interplay between decentralization and privacy, in the case of Blockchain technologies *"….decentralized architectures cannot easily protect themselves against the analysis of metadata. Accordingly, if*

not properly designed, decentralized infrastructures intended to promote individual privacy and autonomy might turn out to be much more vulnerable to governmental or corporate surveillance than their centralized counterparts.
In order to allow for an effective coordination amongst a distributed network of peers, decentralized architectures generally rely on the disclosure of everyone's interactions. Hence, if the price of centralization is trust (as users need to trust centralized operators with their data), decentralization comes at the price of transparency (as everyone's interactions are made visible to all network's nodes)."

Is the EU's data protection legislation also relevant for distributed ledger applications? One could argue that this is cryptographic data and not personal data that is additionally encrypted with a hash function. As Finck (2018, p. 1) states, *"Even where data is encrypted or hashed it qualifies as personal data under EU law. The cryptographically modified data stored on a distributed ledger, in addition to public keys, are hence subject to the GDPR."*

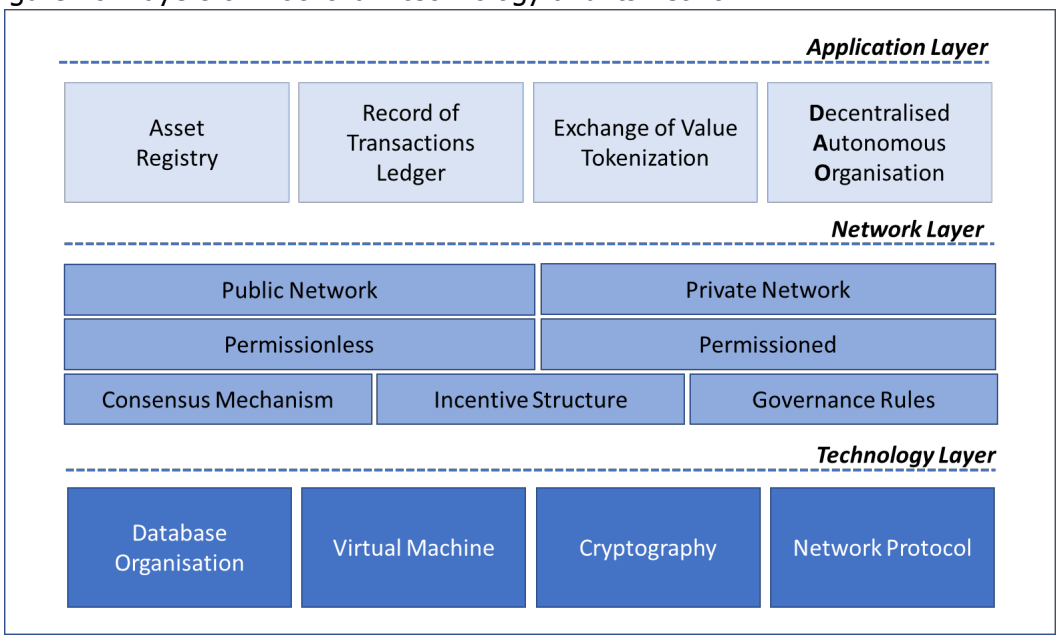
The application of the GDPR refers to the EU. If the data controller is resident in the EU or people whose data are processed on the EU, then the EU's General Data Protection Regulation (GDPR) applies. It is obvious that Distributed Ledger solutions are non-compliant with the GDPR. For this, many points can be cited where public Blockchain solutions are not compatible with the applicable data protection regulations. This begins with the fact that the role of "Data Controller" mandated by the GDPR does not exist in a decentralized, public network without intermediary. It continues with the question of the relevant jurisdiction and territorial scope. A central element of the GDPR is the user's right "to be forgotten". In Blockchain solutions, however, the data is stored irreversibly and unchangeably.

The overall idea of the GDPR approach is to return some data sovereignty back to users, which is clearly in line with the Distributed Ledger approach. However, the main issue is that GDPR regulation was designed for the current business world, which collects, stores and processes data in a centralised way and not for the decentralised distributed ledger world. Both worlds are so different that the GDPR seems hardly applicable to DLT in its current form and needs to be modified.

4. Blockchain Technology and Network

From a pure technology perspective Blockchain is only a special type of database. However, this would barely describe the overall idea of a Blockchain application. In order to gain a coherent picture of Blockchain technology and its network design it makes sense to distinguish between three different layers: (1) Application Layer, (2) Network Layer, and (3) Technology Layer. Following the design-thinking mode the intended application of Blockchain determines the design of the network (Layer 2) and at the same time the selection of the right technology (Layer 3).

Figure 20: Layers of Blockchain technology and its network



Source: the authors

4.1. Technology Layer

Blockchain technology was developed in the 1990s but only gained importance in 2008 with the invention of the Cryptocurrency Bitcoin by Satoshi Nakamoto. For a computer scientist, the Blockchain is a simple data structure, with data linked in a chain of "blocks" and managed redundantly (multiple times) in a distributed network. For the IT security experts, Blockchain has the advantage that data can be stored in the individual "blocks" in a tamper-proof way, which means that the participants in the Blockchain are able to check the authenticity, origin and integrity of the stored data. Thus, it is possible with Blockchains to provide the proofs of asset (i.e., token), transfer authentication and thus the proofs of asset ownership. For the process designer, using Blockchain technology means trusted collaboration between different participants within a network of peers and to exchange value by using tokens on a digital basis.

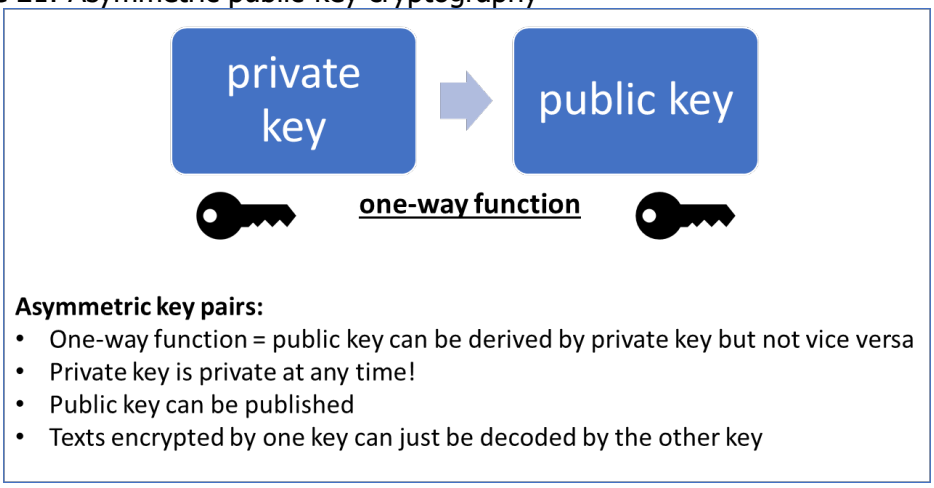
While Bitcoin can only record transactions in the database, the Ethereum database can also store software code in addition to transactions. This enables Ethereum to integrate Smart Contract applications, i.e. software that describes an if-then relationship. The software code is programmed in such a way that an autonomous reaction is triggered if a certain event occurs. In this case one speaks of a virtual computer or a virtual machine that is integrated in the database application.

Blockchain applications use two fundamental cryptographic concepts:

- **Asymmetric public-key cryptography** or digital signatures which ensures the transaction legitimacy of a sending network participant. Algorithm software generates a mathematically linked key pair from private and public key. The sender signs a message with his or her private key, which is only known to him or her, and sends the signed message to the recipient. The recipient can now verify the signed message with the sender's public key and thus

verify the authenticity of the message (if the two keys correspond). The message cannot be changed (content integrity) due to asymmetric encryption.

Figure 21: Asymmetric public-key cryptography



Source: Berentsen and Schär (2017)

- **Hash functions** are usually applied to secure a message against fraud. They compress an arbitrarily long message into a unique, fixed-length binary output (i.e., image) for instance, 256 bits in the standard SHA-256 - which is usually appended to the message. With a secure hash function (e.g., SHA-256), it is computationally impossible to recover the input from the output image. Also, the probability of generating the same output for any two different inputs is negligible.

4.2. Network Layer

Blockchain technology records all transactions within a network in a shared, albeit distributed ledger. The distributed ledger data is stored redundantly on all computers of the network. Since there is no central authority or central accountant for the ledger, but each user has the same read and write permission, there must be a common consensus mechanism for checking the logical consistency of the data in the database and preventing contradictory data from being stored. The consensus mechanism is the backbone of every distributed ledger and is of overall importance for the functioning of the Blockchain network.

If the Blockchain network is permissionless and accessible for everyone the mechanism to find a consensus within the network about data validation and storage needs to be fully automated and software based. In self-organised networks there might be some nodes with full rights to store, read and write data in the database which are not reliable. The consensus mechanism needs to be fully resistant against any attempts to tamper or to manipulate data. Finally, it is worth mentioning that in self-organized open-access ledgers without central authority every activity of network participants is driven by incentives and rewards. Therefore, the individual contribution to a common good such as a network consensus mechanism needs to be incentivised by a system of rewards.

In contrast, the requirements for the consensus mechanism in permissioned Blockchain are different. Access restriction has the advantage that one knows the identity of the network participants and their motivation. Depending on trust, the process of

data validation could be done by a group of delegates and needs to be less automated and software driven.

Currently three basic types of consensus mechanisms are used in Blockchain networks:

Proof-of-Work (PoW) is used for large public networks without permission and can also be described as a random mechanism. Network nodes compete to be the first to solve a complex mathematical puzzle and the winner gets a newly mined cryptocurrency in return for the invested computer power. This form of consensus mechanism ensures that only consistent transactions are stored in the blockchain. This solves the problem of double spending of digital values. This PoW concept is heavily criticized due to the high amount of energy wasted just for this purpose. Special computers are constructed which need a lot of energy for operating and cooling.

Proof-of-Stake (PoS): The basic idea behind the Proof of Stake concept is quite simple. The one who has the most to lose from false or inconsistent storage of data and the malfunctioning of the network application will make the most effort to check data consistency. Those network participants that hold high stakes within the network (owning a lot of coins) are more likely to be chosen for the validation of data. The PoS consensus is energy friendly as no puzzle has to be solved and no new cryptocurrency is generated.

Byzantine Agreement: The name comes from the situation in which generals of the Byzantine Empire had to coordinate their armies, which were separated in space such that communication was only possible via messengers. It turns out that a successful communication protocol can only be constructed if there are not too many "black sheep" or intrigants - the separating bound is less than one third. This protocol can be constructed and will not be discussed here.

Depending on whether the Blockchain is freely accessible to everyone or not, a distinction is made between public permissionless and public permissioned Blockchains. If you not only limit access to the network, but also restrict the circle of network participants who are allowed to validate new information in the data, this is referred to as a private permissioned Blockchain. In the following, the three types with their differences in the access authorization, the type of validation, the possibilities of network governance and the scalability of the database application are presented.

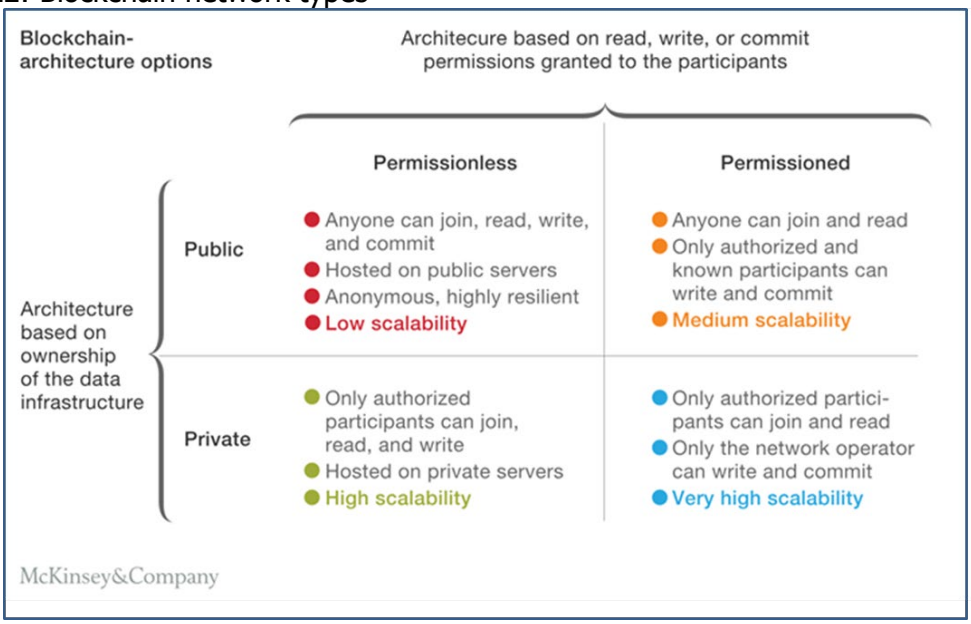
- **Public permissionless Blockchain**
  Public permissionless Blockchains such as Bitcoin or Ethereum are accessible for everyone as no permission is needed. Here, the network participants do not have to reveal their identity but can register by using a pseudonym. In this respect, there exists (pseudo-) anonymity for the users, which on the one hand is positive for the protection of personal data, but on the other hand can also lead to misuse and fraud.
  Furthermore, transactions recorded in the public Blockchain could be seen by every network participant and might allow a tracking of participant activities. The automatic and public validation of new information done by software algorithms makes it possible to include unknown or little-known participants in the process who are not trusted.
  The problem of double spending is solved in a public Blockchain by a random mechanism. Network nodes have considerable computer capacities and solve

an increasingly complex calculation puzzle in competition with each other (so-called "proof-of-work"). The new block with transactions whose arithmetic problem was solved first is appended to the existing block chain and stored irreversibly. The network node, which first solves the arithmetic problem, is rewarded with a certain number of mined crypto currencies for providing considerable computing power (energy consumption) in the interest of the public network.
This way of public verification of new data done by the whole network needs processing time, which reduces the scalability of public Blockchain solutions.
The governance of such public Blockchains is certainly a problem, since there is no central authority which decides about needed system changes. Theoretically, the Blockchain database belongs to the entire public network, so who ultimately decides on modifications or necessary adaptations in the database architecture? If no amicable solution can be found here, the existing Blockchain can be "forked", or divided, and a new public permissionless Blockchain database be created in parallel to the existing one.

- **Public permissioned Blockchains (often called consortium Blockchains)**
  Public permissioned Blockchains restrict access for trusted members of the respective consortium. The advantage of consortium solutions are a higher degree of corporate privacy and data protection.
  Here the identity of the participants is known, each member has the same user rights for reading and writing, and all consortium members have the possibility to validate the integrity of the data. Consortium Blockchains use semi-automated, multi-party consensus approaches for validation instead of a fully automated algorithm software for validation as used in public permissionless Blockchains. Such a semi-automated validation within a restricted circle of members enables a much higher data processing speed than in public Blockchain without permission. Therefore, consortium Blockchain solutions have a lower latency time and are more scalable for a higher volume of data. Governance issues could be solved within the consortium by stakeholder consensus agreements.

- **Private permissioned Blockchains**
  The private permissioned Blockchain has the same features as the public permissioned Blockchain. The only difference is that here not every participant has the right to validate new data. Validation rights are reserved to a small exclusive circle of participants, which are fully trusted by non-validating participants. This creates a kind of hierarchy between the validating and non-validating network members. Since the number of validators is strictly limited, less time is needed for validation, so this form of Blockchain is more scalable. In addition, the Blockchain is usually provided and operated by a private organization, which decides in cooperation with participating partners about changes in the network governance.

Figure 22: Blockchain network types



Source: McKinsey&Company (2018)

It is clear the majority of large enterprises will try to take advantage of the Blockchain application in a permissioned and private network. This way, many large companies can maintain their position of power as a central authority over smaller companies, and in addition, there is the advantage of the participants' trust in a protected space. It remains questionable, however, whether the advantages of Blockchain technology can be fully realized with such a centralized approach.

4.3. Application Layer

Compared to Blockchain-based databases, central database solutions have significant advantages: They are significantly more efficient in terms of the volume of information to be processed per time unit. The distribution of user rights to read and to write is much easier and thus allows more intelligent solutions in user administration and easier compliance with data protection regulation. The only disadvantage of central database applications is that they require trust in the central operator of the database applications.

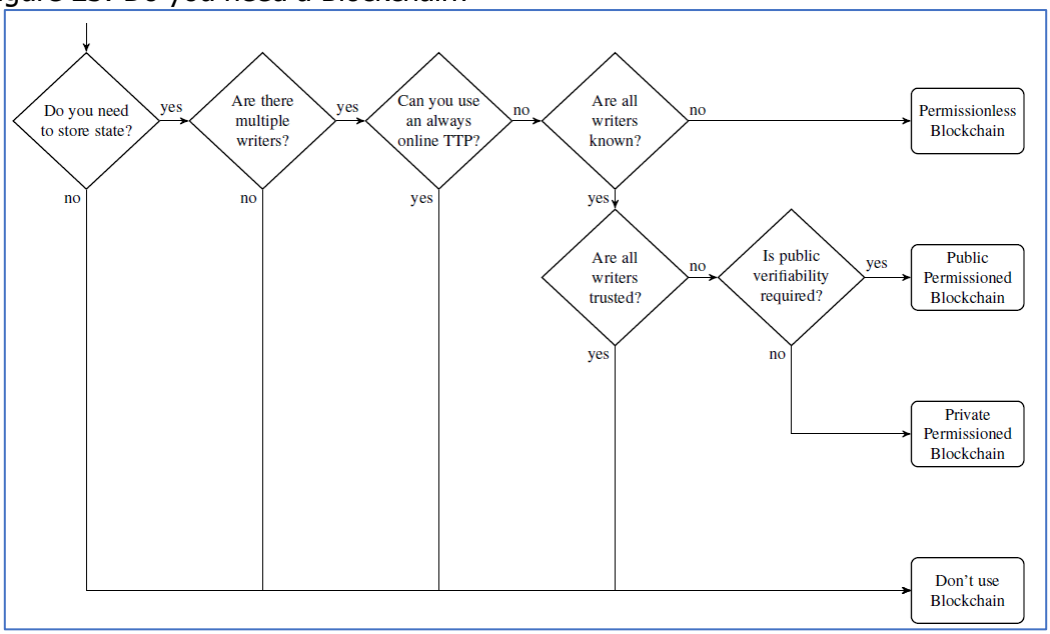
The substitution of trust in a central authority by transparency is exactly the advantage of a Blockchain. In a public Blockchain database accessible to everyone, each participant can verify at the same time who wrote what and how the state of a ledger has changed. Once stored, the information is irreversible and immutable, otherwise the logical consistency of the data stored in blocks would be destroyed. Thus, the two essential elements of the Blockchain complement each other: Public verifiability and integrity of data.

As Wüst and Gervais (2018, p. 2) point out: *The integrity of information is closely linked to public verifiability. If a system provides public verifiability, anyone can verify the integrity of the data."* Furthermore, the Blockchain data is kept redundantly as every writer within the network owns a replication of the data, which is permanently synchronized.

Blockchain solutions are therefore advantageous for processes in which a large number of participants are involved and in which it is of immanent importance for the participants to obtain complete and reliable information about the current status of the process at all times. The **reliable information about the current process status** enables the participants to react to changes at any time so that the process does not run statically but remains dynamic.

Wüst and Gervais (2018) sketched this in the following decision tree demonstrating for which case Blockchain solutions are most appropriate and for which case a central database might be the better solution.

Figure 23: Do you need a Blockchain?



Source: Wüst and Gervais (2018, p. 3)

Blockchain solutions are significantly less scalable than central databases. This is especially true for public Blockchain networks without access restrictions. The process of public validation within a permissionless network is time-consuming, so Blockchain applications are not suitable for storing and processing mass data at high speed.

Wüst/Gervais pointed out this aspect by the following table – figure 24:

	Permissionless Blockchain	Permissioned Blockchain	Central Database
Throughput	Low	High	Very High
Latency	Slow	Medium	Fast
Number of readers	High	High	High
Number of writers	High	Low	High
Number of untrusted writers	High	Low	0
Consensus mechanism	Mainly PoW, some PoS	BFT protocols (e.g. PBFT [6])	None
Centrally managed	No	Yes	Yes

Source: Wüst and Gervais (2018, p. 3)

From the above comparison of the advantages and disadvantages of Blockchain applications with those of a central database, it follows that Blockchain technology has

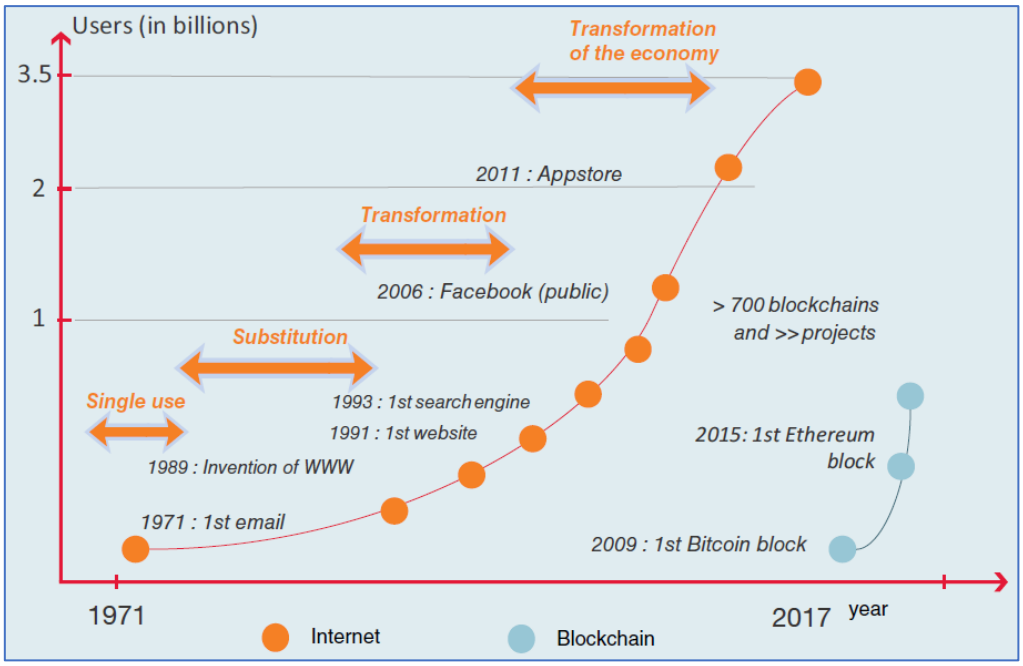
its greatest benefit in those applications where it is important for participants to document a certain state in a process or in a project in a reliable and tamper proofed way and where the decentralized and autonomous data collection by a large number of participants is advantageous. Blockchain applications reach their limits when processing mass data at high speed. Here they have clear disadvantages compared to central database applications.

Decentralised Autonomous Organisation (DAOs)
In public Blockchain networks with free access, every user has the same rights. There is no hierarchy. However, there can still be organizations or projects between the network participants that have hierarchy, are decentralized and self-organizing and function purely on the basis of well-distributed incentive systems. The basic prerequisite is that the Blockchain database application also offers the possibility to store software code, so that it is possible to execute processes autonomously based on rules encoded in Smart Contracts. The governance of such an organisation is fully decentralised by a consensus protocol between network participants.

4.4. Blockchain Use Cases

Previous research on technology adoption typically suggests that there are three classic stages of adopting a new, ground-breaking technology: exploiting a niche, substituting, and then changing the economy. These are, at least, the stages the Internet needed to reach its current development. This process has taken about three decades.

Figure 25: Development of the Internet compared to Blockchain



Source: CGI Business Consulting (2017, p. 9)

Given the current dynamics of the world economy in all respects, it might be possible for Blockchain – in contrast to the Internet – to take far less than three decades in order to become the technology in place. Though, despite the similarities between the Internet and Blockchain it is quite difficult to accurately predict how the adoption

curve of Blockchain will look. However, technology stakeholders commonly estimate that it will be much steeper.

There is currently an ever-growing interest in Blockchain, since this kind of technology has the potential to completely change the way businesses handle, manage, record, validate and verify their transactions. The basic business model is being shifted away from a centralized structure (exchanges, trading platforms) towards decentralized systems (no middlemen, no agencies, direct interaction between consumers). As such, expectations of disruption from Blockchain technology are high and the idea that Blockchain has the potential to redistribute markets and redefine the entire economic system is one that is widely agreed with today.

Over the past couple of years more than 2,500 patents have been filed that relate to Blockchain technology and several billion US dollars have been invested in Blockchain start-ups. A World Economic Forum survey of 800 executives and experts from the information and communications technology sector predicted that, by 2025, 10% of global GDP would be stored on Blockchains or Blockchain related technology (Espinel, O'Halloran, Brynjolfsson, & O'Sullivan, 2015). It is no surprise then that Blockchain has emerged as the hot new topic and as a key technology that will transform the way in which we share information. Just like the Internet, Blockchain makes use of existing technologies to create new and innovative usages and enable novel business models in a wide range of sectors.

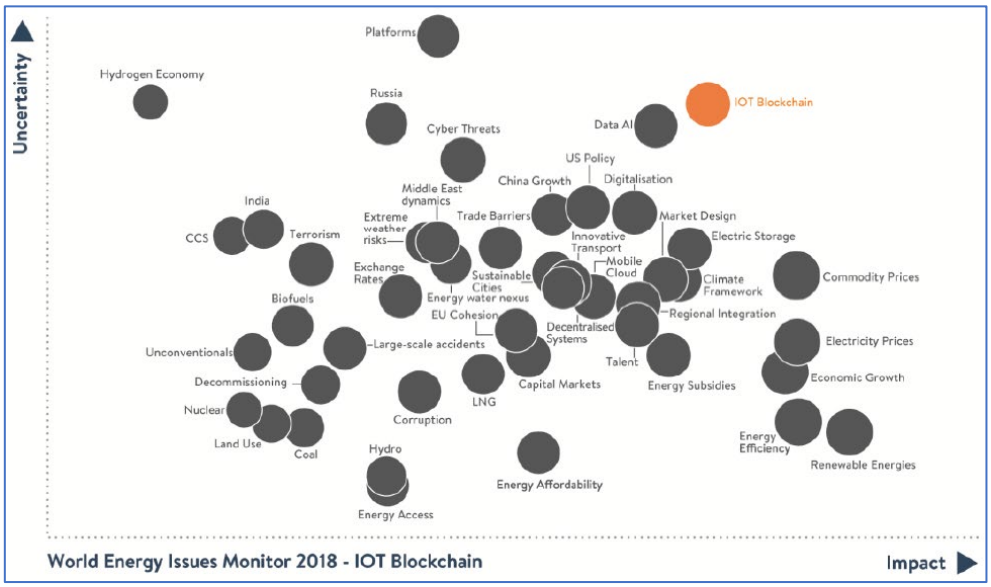
One of the sectors where Blockchain technology has been widely discussed, most probably because of the Bitcoin hype, is the financial services industry. The energy sector is also considered to be one of the industries where Blockchain could have the biggest transformative and disruptive impact. Compared to other industries, the energy industry still lags behind the financial services sector in Blockchain adoption, but is far more advanced than all other industries. Figure 26 shows the innovation curve and depicts the phases of development of Blockchain in the energy sector compared to the financial services and other industries as well. Whereas the financial sector makes the greatest progress and finds itself in transition between the "explore" and "growth" stages, the energy sector is following closely, being ahead of most other industries.

Figure 26: The innovation curve – phases of development

Source: World Energy Council (2017, p. 9)

Like other industries, the energy sector is also struggling with multiple uncertainties related to Blockchain technology, trying to successfully face its technological, regulatory and practical challenges. But according to a report by the World Energy Council the message for the energy community worldwide is that Blockchain technology is seen as one of the most important issues for the years to come, having both a high potential for impact and a great degree of uncertainty.

Figure 27: World Energy Issues Monitor map (2018)



Source: World Energy Council (2017, p. 3)

In order to explore the technological relevance of Blockchain within their organizations, energy and utilities companies need to evaluate in what way the technology could enhance the conventional energy business processes along the energy value chain. The decision on whether Blockchain could be a feasible technology to be adopted for a particular business challenge should be based on a comparison between business process characteristics, on the one side, and Blockchain technology capabilities, on the other side. Figure 28 presents the main characteristics a usage should have in order for an energy company to prepare a Blockchain adoption roadmap.

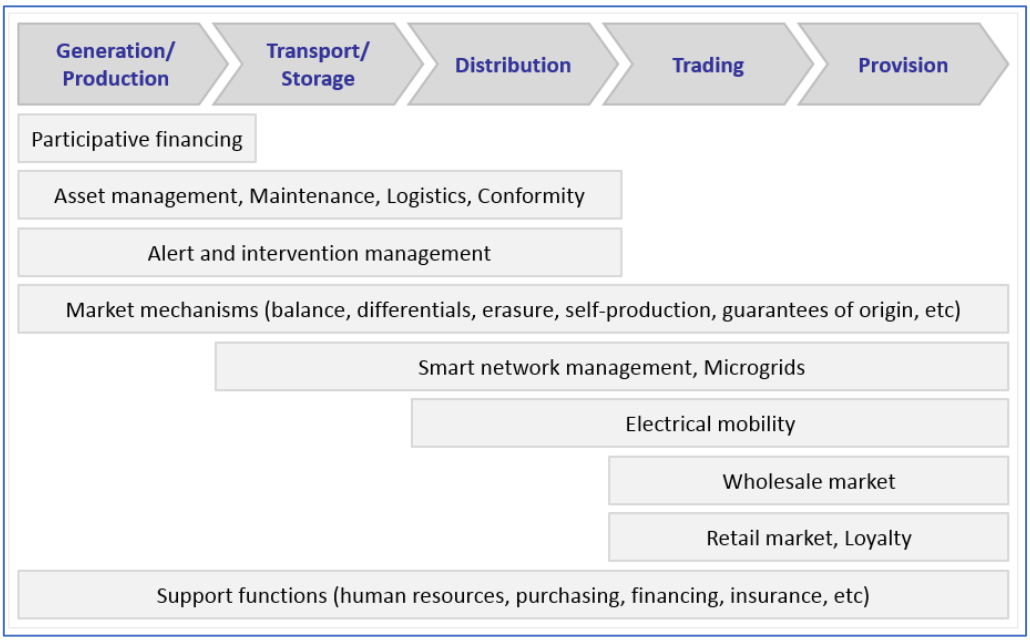
Figure 28: Characteristics of high-potential usages for Blockchain technology

	Shared repository	A shared repository of information is used by multiple parties
	Multiple writers	More than one entity generates transactions that require modifications to the shared repository
	Minimal trust	A level of mistrust exists between entities that generate transactions
	Intermediaries	One (or multiple) intermediary or a central gatekeeper is present to enforce trust
	Transaction dependencies	Interaction or dependency between transactions is created by different entities

Source: World Economic Forum (2018, p. 8)

Due to its ability to store and share data in a secure and transparent manner, Blockchain technology has been warmly embraced by the energy sector and the number of Blockchain projects in the energy field is constantly increasing. Figure 29 illustrates several Blockchain usages along the energy value chain, which are analysed in what follows:

Figure 29: Blockchain usages along the energy value chain



Sources: World Energy Council (2017, p. 7) & CGI Business Consulting (2017, p. 13)

Participative financing, solar renewable energy certificates

In the renewable energy industry Blockchain can be used in order to develop participative funding for renewable production projects between individuals, especially if the Blockchain is linked to remuneration in cryptocurrencies. For example, Blockchain can be used for authenticating and trading renewable energy credit certificates such as solar certificates. The start-up, Lumo, in France pays back its investors in SolarCoins. This is a cryptocurrency earned by generating solar electricity, which can be used as reduction vouchers for power producers.

Asset Management, Maintenance, Logistics, Inventory, Asset Retirement, Conformity, Quality, Health, Safety & Environment

Blockchain can be effectively used for certifying network inventory (equipment, devices, status, geopositioning, maintenance operations history, etc) by sharing a ledger between all participants along the value chain (energy operators, dealers, supervisory authorities). In this way, parts needing to be replaced can be easily identified and the authenticity of spare parts can be verified. Blocs & Compagnie is a French start-up offering auditing solutions for any internal and external enterprise business process by proposing a Blockchain enabled, cloud-based, Enterprise Content Management Solution as a service.

It is important to have a traceability system that can monitor and collect in a rigorous way all the information relating to the displacement of different items along the energy supply chain. The start-up CryptoSeal offers a Blockchain-based solution for the outdated wax seal by using a chip that exactly tracks the course of an energy product, from production to disposal. The chip contains identification data which is recorded and verified by Blockchain. By sharing data between stakeholders, customs clearance for imported products, such as petrol, can be simplified as well.

Alert and intervention management

Interconnected signals from the network together with Blockchain functions can be used to transmit certified alerts for optimizing interventions. Engie, formerly known

as GDF Suez – a French multinational electric utility company, which operates in the fields of electricity generation and distribution, natural gas, nuclear and renewable energy – is conducting in Yonne, France, an experiment where water meters send automatic alerts to technicians in the case of suspected leaks.

Market mechanisms

The market mechanism in the energy sector performs reconciliation techniques for measured quantities, such as for example reconstituting flows or, more recently, erasing or managing guarantees of origin. Not only can the guarantees of origin be traced by Blockchain, but the creation of guarantees of origin itself can be automated via smart contracts. The U.S. start-up Volt Market provides an energy origination, tracking, and trading platform which is driven by smart contracts on the Ethereum Blockchain. The Blockchain technology is used in this case for streamlining the distribution, tracking and trading of energy.

Smart network management, Microgrids

The Blockchain technology provides high potential also for network management, especially with respect to transportation and distribution processes. Thus, Blockchain can facilitate local grid balancing by evaluating options to reconcile fluctuations.

As the operational area is limited for distributed energy systems such as microgrids, the Blockchain technology is becoming more important for managing transactions within the microgrid. One example is LO3 Energy, a company that is developing Blockchain based innovations that provide solutions as to how energy can be generated, stored, bought, sold and used, all at the local level. Through Blockchain technology, LO3 Energy has established Brooklyn Microgrid and developed Exergy, a permissioned data platform that creates localized energy marketplaces for transacting energy across existing grid infrastructure.

Brooklyn Microgrid is a community-powered microgrid, where participants can locally engage in a sustainable energy network and choose their preferred energy sources. Brooklyn Microgrid's pilot project demonstrates the applicability of Blockchain in the peer-to-peer (P2P) energy market.

A further particularly interesting usage is the management of renewables self-consumption. This refers to several processes, including the assignment of flows to a user, billing and the generation of guarantees of origin. LO3 Energy in Brooklyn and SunChain in France provide successful experiments in this field. Furthermore, micro-transaction billing solutions such as France's TURPE system ("tarifs d'utilisation des réseaux publics d'électricité") can help in financing public infrastructure such as energy distribution networks that are open everywhere.

Electrical mobility, gas mobility

In the field of mobility there are several processes to which Blockchain provides very convenient and feasible solutions: automatic identification of vehicles connected to a charging station, assignment of flows to a self-producer, micro-transactions for billing power and using the charging station, smart charging, etc. In Germany, RWE is working on developing these usage together with the start-up Slock.it. BlockCharge, a concept from the RWE Innovation Hub, is also working on a Blockchain-based solution for charging, authentication and billing for electric vehicles. Innogy, a subsidiary

of the German energy company RWE, is making an active contribution towards modern methods of energy supply by enabling digital payments for charging electric vehicles over Ethereum Blockchains.

Wholesale and retail markets

While microgrids link a relatively small number of participants, grid settlements and wholesale market trading can involve many players and a large number of nodes. Energy stakeholders can use trading platforms with Blockchain to more easily open up to end customers – especially industrial ones – as well as simplifying international payments and ensuring the transparency of exchanges.

Blockchain can also be used for assessing customer satisfaction. A good example is Buuyers.com, which provides a Blockchain based solution for certifying the authenticity of customer comments. Another example is the UK-based Electron, which helps customer switching by building a Blockchain-based platform that facilitates better and faster supplier switching management.

Customer data management can make use of Blockchain by authenticating and managing data access privileges that correspondingly fulfil all requirements for transparency, traceability and equal treatment of those requesting access to the data. In this case, digital identity will be closely related to the question of security.

Support functions

There are several interesting Blockchain based solutions for support functions as well. These range from authentication of diplomas for HR to paying suppliers upon delivery, or from issuing off-market shares to auditing accounts. A good example is Postme, which offers a billing flow management service that is fully automated and traceable using Blockchain.

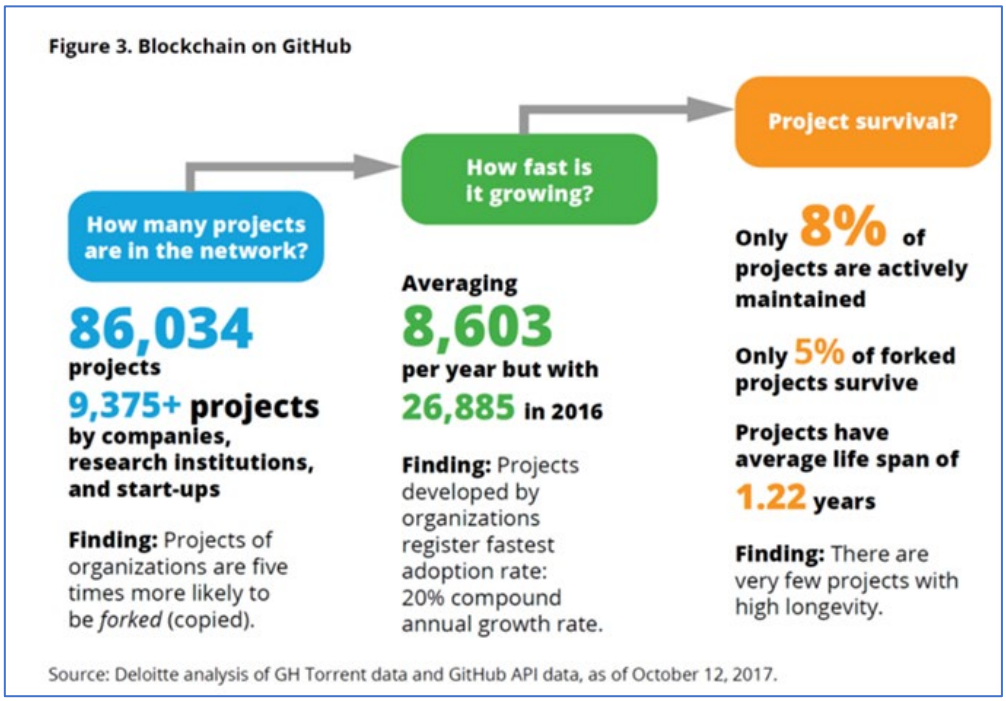
5. Guidance for starting a Blockchain project

In general, no Blockchain project should be started solely because of the Blockchain. The technology should be the solution to a specific problem and not vice versa. In some way this relates to the design thinking approach (p. 9): First get the best understanding of the needs and underlying problem before selecting the right technology to solve it. This basic principle is often forgotten in the hype surrounding Blockchain.

5.1. Learning from failed Blockchain projects

Maybe this is the reason why so many Blockchain projects on the open-source software developer platform GitHub failed early. According to Deloitte (2017), there were about 86,000 Blockchain projects on GitHub, of which only 8% were active and continuing. On average, Blockchain projects have a lifespan of 1.2 years.

Figure 30: Blockchain on GitHub



Source: Deloitte (2017, p. 5)

According to Deloitte (2017, p. 11), the following conclusions can be drawn from the GitHub data:

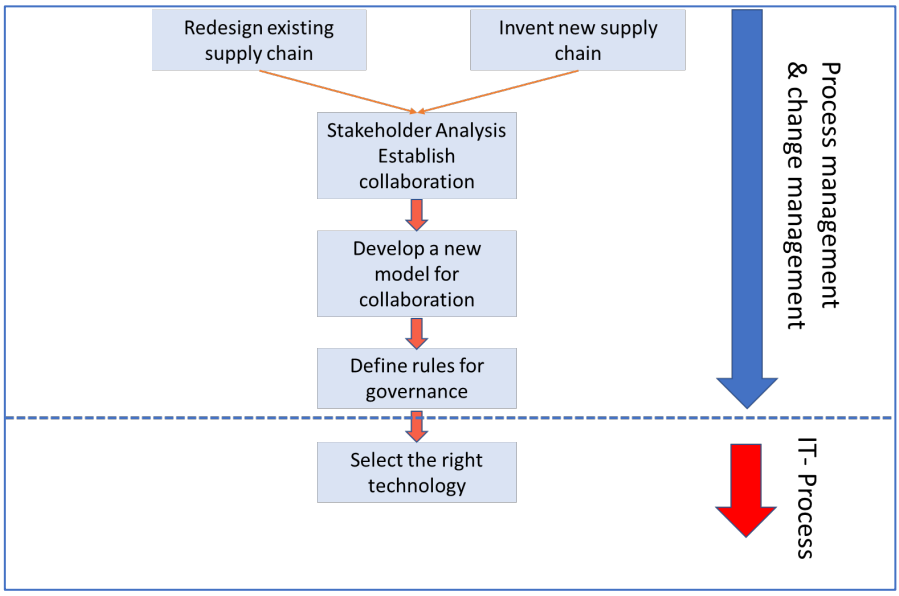
- *Projects done by organisations have a higher survival rate than those of individuals*
- *Projects that survive tend to have multiple committers with less concentration of activities attributed to one particular committer*
- *Projects that are often copied are more prone to survive*
- *Projects that are "forks" of other projects tend to have high mortality rates*

The message from the Deloitte analysis seems to be clear: Blockchain projects need a lot of resources (money and manpower), the project should be set up und operated in a collaborative manner, and it is not advisable to copy other projects instead of setting up an own project individually designed to solve a specific problem.

5.2. Starting Blockchain processes

The development and implementation of a Blockchain project consists largely of change management and process management work. Contrary to expectation, the selection of the technical Blockchain solution plays a subordinate role. Intensive communication, understanding each other's interests, taking people with you and convincing them, explaining the technical possibilities of the Blockchain in simple terms - these are the components for the success of a project and for the selection of project team members.

Figure 31: Sequence of starting a Blockchain project



Source: the authors

Identification of suitable process:
Blockchain projects are suitable for decentralized processes with a larger number of external participants, for whom it is absolutely essential to obtain reliable information about the status of a project or process at all times. Surely every manager in a company or its organization knows such processes of cooperation with a multitude of external partners. Usually these inter-organisational processes are characterized by a high number of failures, very long lead times, high costs of monitoring and a high dissatisfaction of those involved in this process. To identify a suitable process a shift of perspective is needed: From an intra-organizational view towards an inter-organisational perspective by understanding the interests of all involved stakeholders.

Recording of current workflow with key performance indicators
Once such a process has been identified, the next step is to record the workflow and the key performance indicators of the current process. One might assume that every company has already optimized its processes by using Business Process Management software. This is often the case, but the related information is based solely on internal company data and only within the boundaries of the individual company. Most processes have never been optimized as a whole for everyone, including external partners.
The recording of the entire process with its key performance indicators can hardly be carried out by a single organization and requires the cooperation of all participants. It is recommended to record the process with simple software without a high degree of detail and to limit the selection of indicators to the most important ones, so that the coordination process and the amount of work remain manageable.

Design of a Blockchain based process
This is the main challenge. Distributed Ledger Technology enables completely new problem solutions and therefore requires not only a deep understanding of the technological possibilities, but also the ability to think "out of the box". Consequently, the designers of the new process should not be guided by the given resources and the

current solution. This is not about optimizing the existing process, but about creating a new innovative solution for a certain problem.

Process designers should consider the following aspects:

- Design Thinking: The decisive factor for success is thinking from the point of view of the customer, the user or the user of the product. The new process must have a decisive advantage for the customer compared to the existing solution.
- Win-Win Situation: Blockchain applications require a collaborative interaction of a variety of stakeholders. This is only possible if each of the parties involved derives a substantial advantage from the redesign. Win-win solutions require a mutual understanding of the interests involved, intensive communication and persuasion in the community and the openness of all parties involved. Consequently, creating synergetic processes is very time-consuming.
- Selection of information: Starting from the ideal case, the question has to be answered for whom which information is optimal at which point in time. The information stored so far is often only of a monetary nature and relevant for cost accounting. However, sustainable management will in future also require the recording of information about the consumption of natural resources and information on downstream recycling costs, etc. The information will also be used to calculate the cost of the production process. The use of tokens and digital identifiers makes it possible to completely record the value chains of a product and also to precisely record environmental data.
- Use of intermediaries: With the increasing automation of process flows via Smart Contracts, the use of some of the existing intermediaries will probably no longer be necessary. The question is where Blockchains can be applied to optimize existing interactions and where new interaction patterns without a trusted central party can be established.
- Scalability/Agility: The newly designed process should not be static, but agile and scalable. This has the decisive advantage of rapid adaptability to changing environmental conditions.

Development of a governance model

This is certainly the most important part of the collaborative process. A governance structure must be created that is shared by all stakeholders. Ultimately, it is about hierarchies and the distribution of power. Are all participating companies working together with the same rights as owners of a process, or are the rights centralized to a small circle of companies or distributed only at one company?

Here the following questions are in the foreground:

- Who determines participation in the business process?
- Who distributes the read and write rights to the participants in the Blockchain database?
- How to validate the new entry in the Blockchain, automatically via an algorithm, such as Proof of Work, or more centrally via Proof of Stake or Proof of Authority. The decision on the consensus mechanism determines both the scalability and the latency of such a process. As Wüst and Gervais (2018, p. 2) write: "*In centralized systems, the performance in terms of latency and*

throughput is generally much better than in Blockchain systems, as Blockchains add additional complexity through their consensus mechanism."

- Changes in the process flow take place on the basis of a common, democratic agreement between the participants or via the hierarchy of the company with the most capital.
- How is the process monitored? Are there institutionalised solutions for a dispute between the participants?

It will be difficult for very hierarchical, centrally managed companies to engage in a governance model in which every participant has almost equal rights. But the economic advantages of the Blockchain solution can only be achieved if the high costs of centralized monitoring by one individual are replaced by a self-controlling, decentralized incentive system and transparency.

Convincing the top management

Ultimately, a decision to convert complex processes with a large number of external interfaces will always be made by the company's Executive Board. The decisive argument in favour of testing the technology will ultimately be the prospect of considerable cost savings and higher profits. So the key performance indicators of the current process have to be compared with those of the new Blockchain designed process.

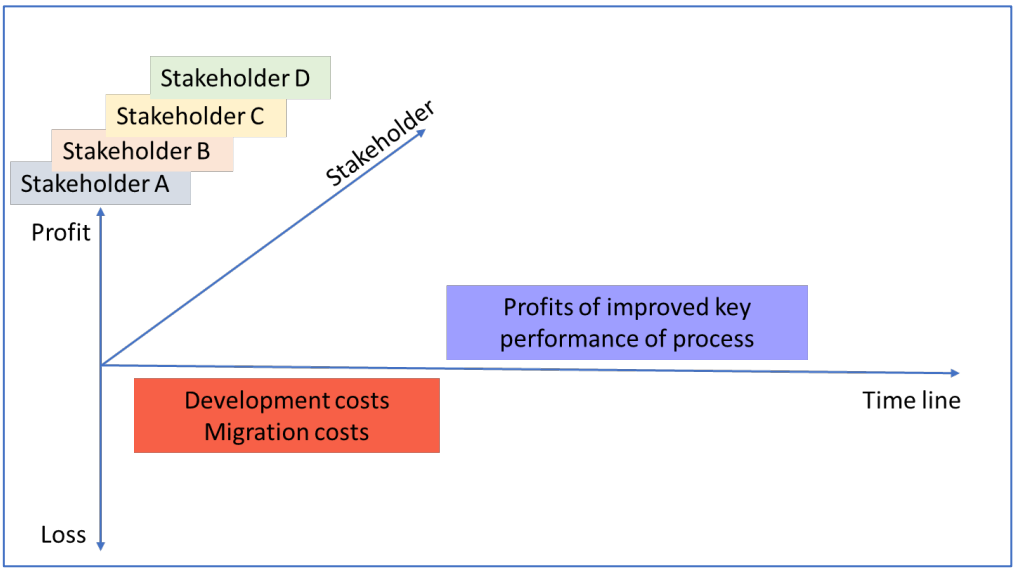
Figure 32: Convincing the management by KPIs

Key Performance Indicators	Current	Blockchain
no. of data interfaces, intermediaries, means of communication, persons involved		
Cycle time (planned, accuracy)		
Total inventory days of supply		
Cash-to-cash cycle time -> needed working capital		
Supplier fill rate -> actual delivery rate versus requested delivery rate		
On time departure from manufacturing subsidiaries to OEM		
Forecast accuracy, forecast volatility		
Monitoring and management costs		

Source: the authors

The Board would also like to have answered the question of migration costs, i.e. the costs incurred by the conversion of the existing process. The future savings by the newly designed Blockchain process must clearly exceed the costs of the process conversion, otherwise such an investment would not be worthwhile. However, in a win-win-situation the net present value of such an investment must be positive for each stakeholder involved in the process.

Figure 33: Positive Net Present Value for all stakeholders?



Source: the authors

If for each involved stakeholder the expected future profits exceed the initial costs of the process transformation, then the respective management can decide to carry out this investment or project. Of course, the Blockchain technology is totally new and everyone lacks experience. This naturally creates a considerable uncertainty and a not negligible risk of investment failure. Consequently, it is recommendable to start with a small simulation project that should be scalable. In the case of a successful test run, the project could be implemented on a wider scale.

6. Learning (higher education) and further research

Distributed Ledger Technology enables fundamentally new forms of collaboration between individuals or organizations within the network. It will accelerate and reinforce the already existing social trend towards disintermediation and decentralization towards peer-to-peer interactions and new network organizations. Distributed Ledger Technology is a disruptive innovation as it fundamentally changes core elements of existing forms of organization in all areas of society: in the way customers, users, clients, etc. are identified, in the documentation and registration of transactions, and in the exchange of digital values. Distributed Ledger Technology is therefore not an innovation which comes overnight. The diffusion period takes longer – probably years or decades as radical changes within society are needed before distributed and shared ledgers become standard.

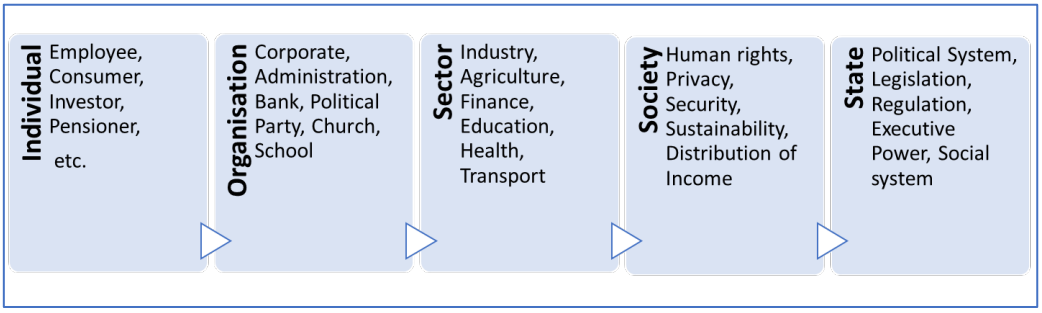
6.1. Research – general considerations

Distributed Ledger Technology will thus become a central research topic of the future for all areas and sectors of society. It should be pointed out that DLT is only a technology or a new concept for storing and processing data and as such neither good nor bad. Only the application to societal problems will raise the awareness of benefits and risks of this technology. So basic research of usages is needed at all levels of society to reach a coherent risk assessment and set up legislation and regulation that

facilitates the social benefits of this new technology and at same time protects individuals from its risks.

Referring to chapter one "Digital Transformation of Society" every change starts from the individual. In this respect, research questions need **to focus on the individual and their needs** following the design thinking mode. In order to arrive at truly innovative DTL applications and solutions, it is imperative not to limit the possibilities for existing organizations to existing resources. Starting from the individual and their need will probably result in completely new forms of collaboration, which have clear advantages over existing organizations in terms of agility, scalability and sustainability. Consequently, research starts with the individual and new models for P2P-collabortion, then analyses the implications for existing organizations and concludes with the assessment of benefits and risks for society.

Figure 34: The "block"-chain of research



Source: the authors

Recently, several European national financial authorities have opened "regulatory sandboxes" to work with FinTech companies and Blockchain start-ups in particular and to develop a mutual understanding of the technology, the new business models and societal implications. For start-up companies, this has the advantage of operating within a legally secure framework with a light regulation.

Jenik and Lauer (2017, p. 1) define regulatory sandboxes as follows:
"A regulatory sandbox is a framework set up by a financial sector regulator to allow small scale, live testing of innovations by private firms in a controlled environment (operating under a special exemption, allowance, or other limited, time-bound exception) under the regulator's supervision."

This is a new approach to financial supervision, no longer top-down due to the statutory power of the regulator, but rather that of a **joint, open and cooperative dialogue** that enables financial supervisors and lawmakers to react with more speed and agility. This change in mindset to a more collaborative regulatory approach suits much better the peer-to-peer business models of FinTechs.

Nevertheless, these sandbox trials with FinTech companies reveal a significant weakness in financial supervision, namely the lack of technical expertise among the regulatory agency's staff. These are usually experts in financial supervision and regulation, not algorithms, database applications and cryptography. This is probably also true for supervisory authorities in the health, transport and traffic or other sectors.

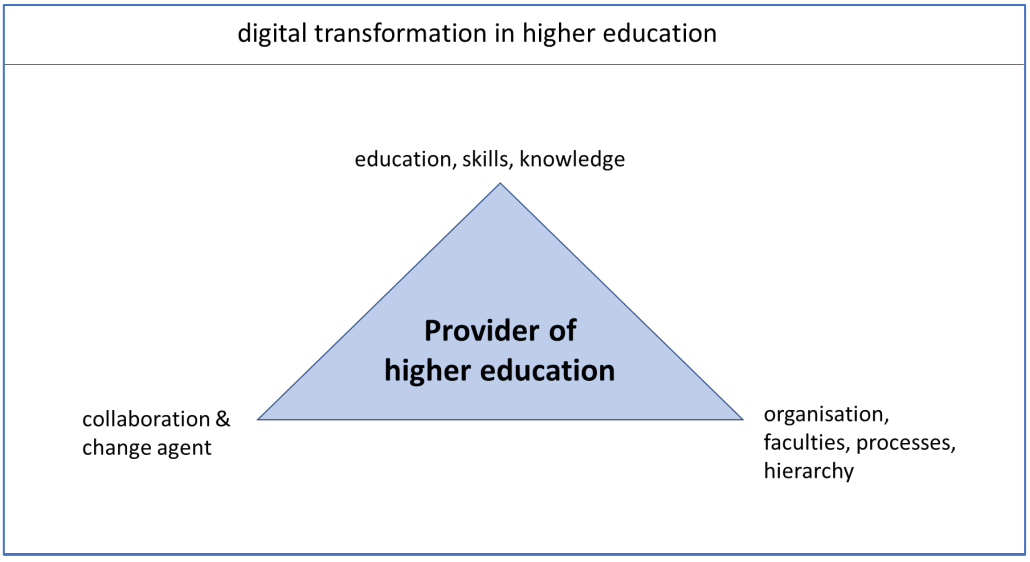
The assessment and understanding of digital technology-based business models requires a close collaboration of experts from different disciplines and a mutual understanding of the different perspectives of the underlying problem. In view of the **necessary interdisciplinarity of expert knowledge**, it is therefore questionable whether a sectoral approach for the supervisory authorities will continue to make sense or whether they will in future also cooperate in a network structure of experts depending on the problem at hand.

The same lesson from financial supervision and "sandboxes" can be applied to academic research on Distributed Ledger Technology: only an open and joint dialogue with research colleagues and, above all, practitioners from various disciplines can lead to success. The nice thing about the digital world of collaboration is that it is mostly about the subject, while external characteristics such as academic titles and hierarchy play a less important role.

6.2. DLT & Learning in higher education

Digital transformation and in particular Distributed Ledger Technology have fundamentally changed the landscape of higher education and will continue to do so. A provider of higher education is affected by digital transformation in three ways: First and foremost, of course, in the educational content, the structure of study programs and the didactic method of imparting knowledge. Secondly, the education provider is itself an organization with processes and is thus directly subject to digital change. Thirdly, the provider acts as a change agent for the regional community and collaborates with others in national and international research and education networks.

Figure 35: The triangle of higher education



Source: the authors

Education, skills and knowledge

Regardless of the field of study, each graduate is expected to have knowledge of the functioning of new digital technologies and a sound understanding of the advantages and risks of using new technologies. In addition to IT skills, students need to learn the psychology of behavioural change and communication. This is because

knowledge of change management will become indispensable for successfully shaping the transformation process of organizations. As a result, the future study programme will clearly increase in the interdisciplinarity of the taught content.

The didactics of teaching in particular will change fundamentally: the times in which the professor had a monopoly on a certain knowledge segment are finally over. The knowledge itself is available in all possible foreign languages and forms on the Internet. What is missing is the coach, who shows the student an individual educational path structured according to her or his needs and abilities. The interactive coaching of students using all available channels will replace the communicative one-way street of the traditional lecture in the lecture hall. This does not mean that the physical meeting of teacher and student will lose its importance. On the contrary, face-to-face meetings with professors are gaining intensity as they are quality time within a blended learning environment of video tutorials, virtual class rooms and webinars.

Decentralized, web-based organisation of higher education

As an organization, universities must question whether their processes are optimally structured in such a way that the overriding goal of providing the student with an optimal education as a user of the organization is achieved. Both the educational program as well as the organization of education must be geared to the changed requirements of digital transformation, otherwise the overall package of education will not be consistent and coherent.

But are today's universities sustainable organisations in terms of using scarce taxpayers' money efficiently to educate students? If one looks at the mostly oversized buildings of universities with the multitude of less-used offices of professors, one gets the impression that the age of purely physical and centralized knowledge transfer still prevails here. The lecturer's work is still counted in contact hours of teaching done per week per semester. Universities are still organisationally divided into faculties, which makes the interdisciplinary organisation of joint study programmes, workshops, research projects or conferences much more difficult. The same applies to the university administration, whose processes are mostly still paper-based and strictly hierarchically organized. Administration staff of universities often outnumber faculty members, which indicates a skewed allocation of resources.

Distributed Ledger Technology will decentralize the organization of education. The students become sovereign to their private data, including their education data. Equipped with their own identity, students will manage their grades as well as their ECTS points. In the future, the respective lecturer will send both the grade and the ECTS points to the student as part of the network and this information will be automatically validated and irreversibly stored in the Blockchain. The examination office is also a node of the network and thus simultaneously obtains the same information about the student's course studies. Certificates will be sent directly to the student via smart contract applications and stored in the Blockchain when the required number of credit points is reached (Grech & Camilleri, 2017, p. 33). A central repository of student grades at the university's examination office and a central registration of students' private data at the university's admission office will become obsolete.

The dematerialisation and decentralisation of the "university" organisation may even go further. In the future, students could enrol for individual modules or for a course of study via a web-based platform, whereby data management is based on blockchain peer-to-peer. Students could also take courses from partner universities, regardless of their location, as the exchange and recognition of credit points is just as decentralised via Blockchain as with their own modules. In the case of blended learning modules, a constant presence of the students on site is not necessary anyway, so that the students and the lecturer could meet only when required at logistically optimal locations.

In future, the tasks of an educational organisation will lie primarily in ensuring the quality of education, in advising and coaching learners and in its role as a service provider. Education for its own value and individual learning processes do not require such large "production sites" as universities.

Collaboration and change agent

Blockchain enables much closer cooperation between university teaching and research and between universities and the corporate world. The diffusion process of innovations such as Distributed Ledger Technology into academic teaching as well as into the working world must be significantly shortened, which means that the boundaries between studying and working must merge more strongly. The same applies to lecturers, who are constantly switching jobs between the real economy and academies. The university as a provider of education must develop a self-understanding that a central task of a public educational institution is to be the driver or motor for social innovation in the community.

Bibliography

Bank for International Settlements. (2018). *V. Cryptocurrencies: looking beyond the hype*. Retrieved from Basel:

Baran, P. (1964). On distributed communications networks. *IEEE transactions on Communications Systems, 12*(1), 1-9.

Berentsen, A., & Schär, F. (2017). Bitcoin, Blockchain und Kryptoassets: Eine umfassende Einführung. *Aufl. Norderstedt: BoD–Books on Demand*.

Botsman, R. (2016). We've stopped trusting institutions and trusting strangers. *TED Talks*. Retrieved from https://www.ted.com/talks/rachel_botsman_we_ve_stopped_trusting_institutions_and_started_trusting_strangers#t-682697.

Brown, T. (2008). Hardvard Business Review: Design Thinking. *Hardvard Business School Publishing Corporation*.

CGI Business Consulting. (2017). Opportunities for blockchain in the energy sector. *White Paper,*. Retrieved from https://www.cgi.com/sites/default/files/white-papers/cgi-blockchain-in-energy-sector-white-paper.pdf.

Coase, R. H. (1937). The nature of the firm. *economica, 4*(16), 386-405.

De Filippi, P. (2016). The interplay between decentralization and privacy: the case of blockchain technologies.

Deloitte. (2017). Evolution of blockchain technology: Insights from the GitHub platform. Retrieved from https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html.

Dierksmeier, C., & Seele, P. (2018). Cryptocurrencies and business ethics. *Journal of Business Ethics, 152*(1), 1-14.

Espinel, V., O'Halloran, D., Brynjolfsson, E., & O'Sullivan, D. (2015). *Deep shift, technology tipping points and societal impact.* Paper presented at the New York: World Economic Forum–Global Agenda Council on the Future of Software & Society (REF 310815).

Finck, M. (2018). Blockchains and data protection in the european union. *Eur. Data Prot. L. Rev., 4*, 17.

FINMA. (2018). FINMA publishes ICO guidelines. Retrieved from https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/.

Grech, A., & Camilleri, A. F. (2017). Blockchain in education. In: Luxembourg: Publications Office of the European Union.

Hileman, G., & Rauchs, M. (2017). 2017 Global Blockchain Benchmarking Study.

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard business review, 95*(1), 118-127.

IBM. (2017). Blockchain benefits for electronics: Taming complexity with better supply chain visibility. Retrieved from https://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03809usen/gbe03809usen-01_GBE03809USEN.pdf.

Jenik, I., & Lauer, K. (2017). Regulatory sandboxes and financial inclusion. *Washington, DC: CGAP*.

Juks, R. (2018). When a central bank digital currency meets private money: the effects of an e-krona on banks. *Sveriges Riksbank Economic Review*(3), 79-99.

Linklaters and ISDA. (2017). Smart Contracts and Distributed Ledger – A Legal Perspective. Retrieved from https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf.

Lord Wilberforce. (1971). Speech. In Prenn v Simmonds (Ed.).

McKinsey&Company. (2018). Blockchain beyond the hype: What is the strategic business value? Retrieved from https://www.mckinsey.com/business-functions/digital-

mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
PwC. (2016). Q&A: What is a blockchain? Retrieved from https://www.pwc.com/gr/en/publications/assets/qa-what-is-blockchain.pdf
Rauchs, M., Glidden, A., Gordon, B., Pieters, G. C., Recanatini, M., Rostand, F., . . . Zhang, B. Z. (2018). Distributed Ledger Technology Systems: A Conceptual Framework.
Sas, C., & Khairuddin, I. E. (2017). *Design for Trust: An exploration of the challenges and opportunities of bitcoin users.* Paper presented at the Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems.
Settlement", B. f. I. (2018). Cryptocurrencies: looking beyond the hype. In (pp. 91-114).
SMSG. (2018). *Own Initiative Report on Initial Coin Offerings and Crypto-Assets*. Retrieved from Paris:
Treitel, G. H. (2003). The Law of Contract, 11" ed. *Thomson Sweet & Maxwell, London*.
VDI. (2018). Blockchain - eine Technologie mit disruptivem Charakter.
Wang, W., Hoang, D. T., Xiong, Z., Niyato, D., Wang, P., Hu, P., & Wen, Y. (2018). A Survey on Consensus Mechanisms and Mining Management in Blockchain Networks. *arXiv preprint arXiv:1805.02707*.
World Economic Forum. (2018). Blockchain Beyond the Hype – A Practical Framework for Business Leaders. *White Paper,*. Retrieved from http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf.
World Energy Council. (2017). The Developing Role of Blockchain. Retrieved from https://www.worldenergy.org/wp-content/uploads/2017/11/WP_Blockchain_Exec-Summary_final.pdf.
Wüst, K., & Gervais, A. (2018). *Do you need a Blockchain?* Paper presented at the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT).
Zwitter, A. (2014). Big data ethics. *Big Data & Society, 1*(2), 2053951714559253.

Annex 1: Catalogue of research questions

INDIVIDUAL

Concept of Identity Individuals as sovereign of their personal data –

- risk/benefit analysis for individuals and corporate businesses
- behaviour change of individuals in dealing with their own data – consumer protection and education (literacy in data protection)
- change in business models of internet platforms
- technical solutions for societal problems – would it work?
- compliance with General Data Protection Regulation

Peer-to-Peer

- Peers are taking all the risks (credit risk, business risk, unemployment risk, etc.) – changes in society, layers of insurance, solidarity, community
- Consequences for social insurance: pension, health, unemployment etc.
- Distributed Ledger Technology and Consumer Protection

ORGANISATION

Transformation of organisations related to Distributed Ledgers

- Organisational changes needed to implement Distributed Ledger Solutions
- Incentivise collaboration: How to create synergies and win-win situations?
- Corporate Culture and Governance for Blockchain solutions
- Change Management, Hierarchy and Management

New business models of collaboration

- Supply chain management
- Identity Management
- Tracking of goods and services
- Certification and registration
- Blockchain based market and trading organisations

New types of Blockchain organisation

- Decentralised Autonomous Organisations (DAOs) – risk/benefit
- Decentralized Applications
- Internet of Things

SECTOR

- Logistics
- Agriculture
- Services
- Finance
- Energy
- Education
- Public Administration

STATE, POLITICS, GOVERNMENT

Legislation and Regulation

- Blockchain/Distributed Ledger Legislation (Lichtenstein)
- National or international regulation of Distributed Ledger networks
- Tokens – financial securities or a new legal type of value?
- Smart Contracts and the law of contracts
- DLT and GDPR compliance
- Opening regulatory sandboxes for Distributed Ledger start-ups
- Reinventing and or reforming the organisation of legislation and regulation in the age of network businesses
- RegTech – Legislation and regulation by software code
- Regulators as a node in a peer-to-peer network

State

- Centralised or decentralised governance models
- Rethinking federalism
- Representative democracy versus direct democracy by Blockchain
- State as provider of digital identity for citizens
- Creation of a public national Blockchain

Politics

- Voting via Blockchain – new types of direct democracy
- Reorganisation or reinventing political parties
- Transparency in political decision making
- Reorganisation of public administration with Blockchain
- Political movements instead of political parties

Government organisation

- Enhancing transparency and collaboration between governments, businesses and citizens
- Reducing bureaucracy – lean government
- Governance by artificial intelligence and transparent Blockchain solutions

International, multinational organisations, financial organisations

- Governance of international trade relations – bilateral or multilateral (GATT, WTO)
- Governance of international finance, payments, capital markets (IMF)
- Exchange rate systems and fiat money versus cryptocurrencies
- Central bank cryptocurrency as legal tender
- Creation of a public international Blockchain as infrastructure for international trade and finance

SOCIETY

- Blockchain and transformation towards sustainable economy
- Consumer protection rights
- Data protection
- Blockchain and regional community solutions
- Migration and Blockchain (identity, development aid, donation)
- Blockchain as an opportunity for developing countries
- Blockchain and economic and financial inclusion
- Climate change – tracking environmental costs