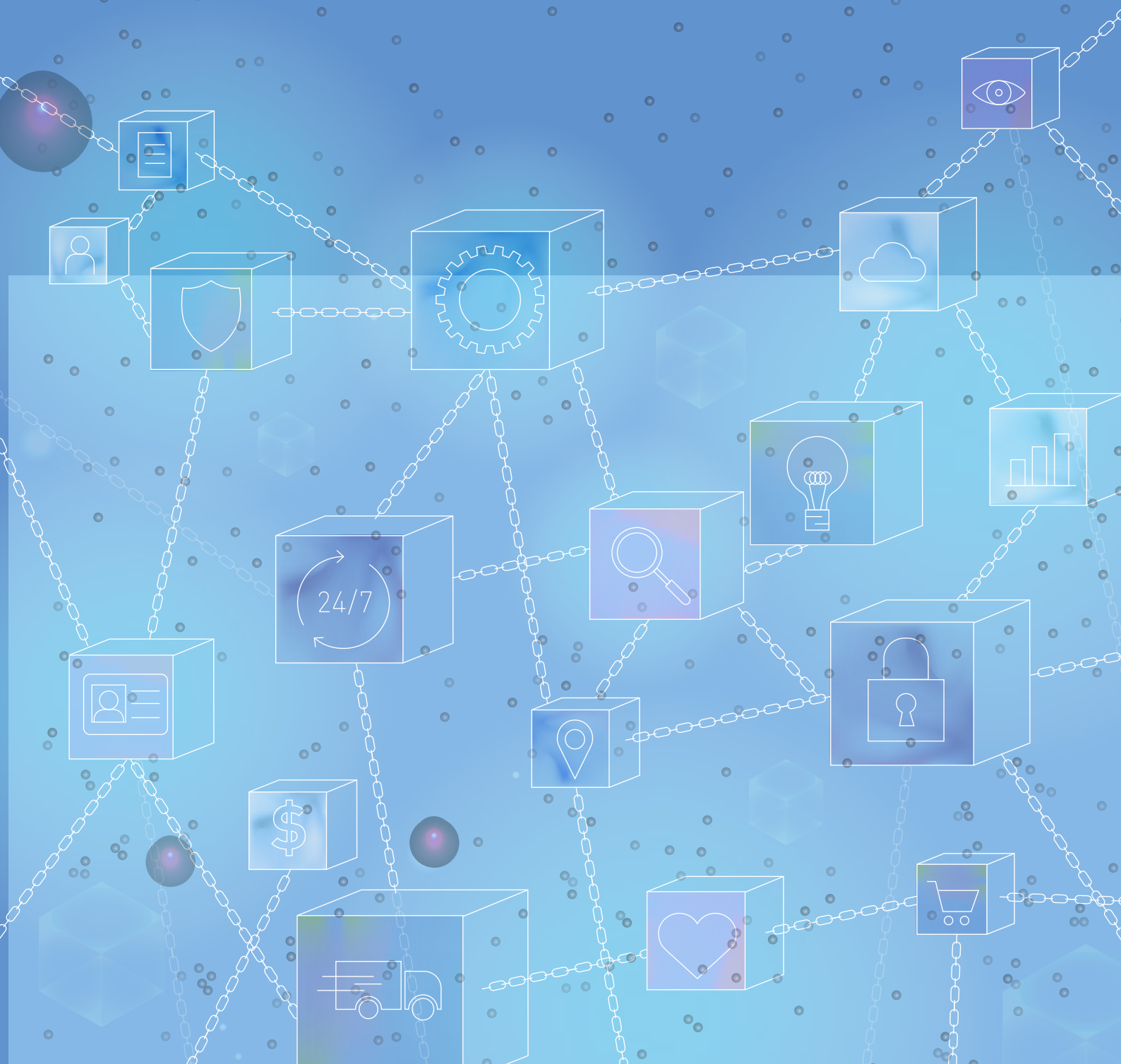
GDI GOTTLIEB DUTTWEILER INSTITUTE
CREATING FUTURES

HYPE OR HELP?

The real benefits of blockchain

By Jan Bieser and Daniel Fasnacht



Imprint

Authors
Dr. Jan Bieser, Dr. Daniel Fasnacht

Editing
Scribendi

Layout/Illustration
Joppe Berlin, www.joppeberlin.com

GDI Research Board
Alain Egli, Karin Frick, Dr. Jakub Samochowiec, Christine Schäfer

ISBN: 978-3-7184-7143-0

Publisher
GDI Gottlieb Duttweiler Institute
Langhaldenstrasse 21
CH-8803 Rüschlikon / Zurich
www.gdi.ch

Initiators
sminds/N9 House of Innovation, Inacta, EcosystemPartners

Industry and cooperation partners
This study was made possible by various partners who contributed their expertise and experience: aXedras, Blockchain Nation Switzerland, Swiss Federal Office of Energy, Generali (House of Insuretech Switzerland HITS), Green, Inacta, Kantonsspital Baden, Novartis, OVD Kinegram, Association of Swiss Electricity Companies VSE.

Table of contents

2 **Foreword**
4 **Summary**
6 **Initial situation**
10 **An introduction to blockchain**
> The blockchain technology
> Blockchain and distributed ledger technology
> Permissionless and permissioned blockchains
> How blockchain works
> Blockchain governance
22 **Benefits of blockchain technology**
> Goals of the use of blockchain
> Blockchain in corporate practice
31 **Blockchain in Switzerland and internationally**
34 **The shift to distributed value networks**
> Visions of distributed value networks
> Advantages and disadvantages of distributed value networks
> Blockchain and power concentration
42 **The potential of blockchain applications in detail**
> Self-sovereign identities
> Distributed management of sensitive data using health data as an example
> Tracking and tracing of goods using pharmaceuticals as an example
63 **Critical success factors of blockchain projects**
68 **Is the future distributed?**
69 **Acknowledgements**
70 **Appendix**
73 **Bibliography**

Foreword

Switzerland is often considered the most innovative country in the world. There is no secret formula behind this. It is a combination of well-known factors that make Switzerland innovative, including its best-in-class educational system with the famous Swiss apprenticeship system and some of the world's top universities. Switzerland has a stable, reliable, pragmatic democracy and a wealth of highly-performing SMEs. The Swiss government's bottom-up vision for science and technology prevents stifling innovation with unwieldy and poorly informed policies before the opportunities and risks are known. Finance Minister Ueli Maurer proved to be a visionary when he established Switzerland as Crypto Nation. The National Council followed him in 2020 by implementing policies that simplify the use of blockchain and distributed ledger technology (DLT). This legal framework enables innovation, promotes technology acceptance, removes barriers to blockchain adoption in all industries, and limits the risks of misuse. During these turbulent times, we now see how this approach is successful.

Innosuisse supports bottom-up approaches through its Innovation Booster initiative and promotes thematic communities that develop disruptive ideas and solutions. Blockchain is one of the most promising topics supported under this program.

For most people, blockchain is just about cryptocurrencies, investing, and speculating. This is about the same as using airplanes only for military purposes. Blockchain is a perfect example of a digitally native technology that enables solutions to old and new challenges and combines the real and virtual worlds.

As digitization advances every day, we cannot simply replicate the old paradigms of the physical world in this new space. For example, trust needs to be rethought in the digital world. Whenever traditional computer technologies, without blockchain, are used, one's trust in the technology will not exceed one's trust in the companies and people behind it. In practice, this often hinders technology acceptance.

Blockchain technology's beauty is that it allows the elimination of centralized trust authorities in the digital space. Instead, trust is created through distributed consensus-building among many network participants according to traceable and auditable rules while preserving privacy and giving control back to consumers. It is no surprise that such a technology flourishes in Switzerland, a country whose people and institutions value trust, fairness, reliability, privacy, and pragmatism.

Exploiting blockchain's potential will require visionary companies and people who see opportunities and benefits rather than risks and problems. Collaboration among large companies, SMEs, and start-ups is a critical success factor for such ventures. Universities and think tanks, such as the Gottlieb Duttweiler Institute (GDI), and innovative partners from the private sector create a strong foundation for interdisciplinary co-innovation.

This study shows the benefits of blockchain for the secure identification of citizens in the digital space and connects it to the consultation on electronic identity (E-ID) submitted to the Federal Council in June 2022. Ideas for product tracking with blockchain are well-known, and this study showcases the significant progress that has been made in this field. This

potential can be exploited in markets for tangible goods, such as pharmaceuticals or gold trading, and intangible goods, such as guarantees of origin for electricity. Data and data management play an increasingly important role in a digitized world. With blockchain, users can manage their sensitive health or financial data; data silos can be linked and protected against cyber attacks.

The potentials of blockchain suggested by the authors are vast and, if pursued further, will substantially contribute to the performance of Switzerland's economy. This will help Switzerland to remain one of the most innovative countries in the world.

André Kudelski
President Innosuisse and Entrepreneur

Summary

Many digital applications have become critical infrastructures for business and our everyday lives. Dependencies on digital infrastructures exist beyond the technology industry, as digital tools are also used to provide physical infrastructures and services in, for example, finance, healthcare, transportation, building management, energy, or manufacturing. Often, these applications are provided by central service providers, such as IT companies or network operators. Citizens must trust these service providers to ensure the systems' availability and integrity and not abuse their market power.

The introduction of Bitcoin and the blockchain technology behind it in 2009 raised the hope of reducing such dependencies—in the case of Bitcoin, the dependencies on (central) banks. Since then, the technology has been continuously developed to exploit the potential of blockchain in the corporate context. Today, it is no longer a technology specifically for cryptocurrencies, but a technology that offers advantages for digital applications in many industries. Yet, many leaders continue to find it difficult to assess the short- and long-term benefits of blockchain technology for their organizations. Therefore, the goal of this study is to provide a nuanced understanding of the potential applications, opportunities, and limitations of blockchain technology.

Blockchain can be used for two fundamentally different purposes:

More robust and efficient digital infrastructures: The distributed operation of a digital application on the systems of multiple business partners increases its tamper resistance and availability. Valuable assets can be digitally mapped and traded with tokens, and business processes can be automated with smart contracts. This simplifies cross-organizational collaboration and saves on costs and time. Once processes have been digitized in a secure manner using blockchains, new business areas can open up. For example, blockchain enables the creation of secure electronic identities that allow the secure digital identification of people, organizations, and objects. This can enable access management in buildings without physical keys, tamper-resistant authenticity certificates for goods, peer-to-peer marketplaces, or a robust data infrastructure for the Internet of Things.

Reduction of dependencies: Distributed operations additionally provide the possibility of eliminating dependence on central service providers. In self-regulating, distributed value networks, all members make decisions together and control each other without a central authority: Internet without Google, ride-sharing without Uber, and payments without banks. However, this is not only a technological but also a social process in which new forms of cooperation must be established and conflicts of interest overcome. If this succeeds, blockchain technology offers a suitable technological basis for implementation.

A literature search revealed more than 50 applications in 10 industries. In the enterprise context, centrally managed applications dominate the market with the goal of increasing system integrity, automation, and cost efficiency. Often, the attempt to deploy blockchain technology is also a driver for standardizing existing processes, as this is a prerequisite for digitizing them using blockchain.

Key challenges in implementing blockchain projects include establishing suitable governance structures for cross-organizational collaboration, eliminating regulatory ambiguities, ensuring data quality and security (on blockchains and in adjacent systems), and fostering trust and acceptance in the technology. If companies forge new partnerships with competitors and regulators, and collaboratively test applications, these challenges can be overcome. Switzerland is considered an international hub for blockchain with forward-looking blockchain regulations, leading research hubs, and over 1,100 companies developing blockchain solutions.

Due to the continued substantial progress in the digitization of processes, which has been further spurred, not least by the COVID-19 pandemic, it can be assumed that digital applications will continue to gain importance. The properties of blockchain—tamper resistance and availability, efficient data exchange, decision rules that can be fixed in smart contracts, and value trading with tokens—offer a suitable technical basis for creating robust and efficient digital infrastructures.

Initial situation

Tim Berners-Lee, the inventor of the World Wide Web, today laments what the Internet has become.[1] Instead of serving the common good and democratizing the dissemination of information, there is currently a great market concentration on the Internet. A few Big Tech companies (for example, Alphabet, Apple, Amazon, Meta, Microsoft, Alibaba, and Tencent) provide dominant digital platforms that grew exponentially and allow them to control the flow of information on the Internet. In addition, outside the technology industry, digital applications are used to optimize products and processes, or develop new business models. Intelligent algorithms in combination with data promise to process financial transactions more efficiently, predict machine failures, optimize supply chains, and diagnose diseases. Whether in transportation, energy supply, building management, finance, or healthcare, digital applications are used everywhere. A survey conducted in 2022 found that around two-thirds of Swiss companies said they were introducing or already implementing a data strategy.[2] Digitalization is an ongoing issue for Swiss SMEs and concerns them more than inflation, supply chain problems, or the skills shortage in the coming years.[3]

Many digital applications have become critical infrastructures for business and our everyday lives. For example, if the services of Google and Meta were to go down simultaneously, about 92% of all searches on the Internet would return no results, and the instant messages of about three billion users would not reach the recipient.[4] Economically significant failures of critical digital infrastructures have already occurred. In Switzerland, the systems of central payment service providers have already failed several times, resulting in significant losses of sales in supermarkets and restaurants.[5] In June 2022, the Swiss hospital association H+ fell victim to a cyber attack and subsequently shut down all servers for security reasons.[6]

So-called value networks usually form around digital applications in which multiple partners (often from different sectors) exchange goods, money, and information to jointly create value. The term "ecosystem" is also often used in this context. Because this term is used inflationarily and because we believe that a value network better describes the context of blockchain, we will use this term.

Value networks are often structured around a central service provider who takes on the intermediary role. The intermediary is the middleman who coordinates the exchange of data in the network and can determine the rules and conditions of interaction. For example, banks can set transaction fees, Uber can set fares and brokerage commissions, and Google can set the conditions for reusing collected user data. Those who want to use an intermediary's offers usually cannot influence the rules—they must be accepted.

When Bitcoin was introduced in 2009, there was a subsequent hype about cryptocurrencies and the blockchain technology behind them. With blockchain, digital applications are not run by an intermediary but distributed across the computer systems of multiple participants in the network. The hope is to reduce the dependence on and power of intermediaries and to trigger a shift from centralized to decentralized and distributed value networks (see Figure 1). For example, the idea

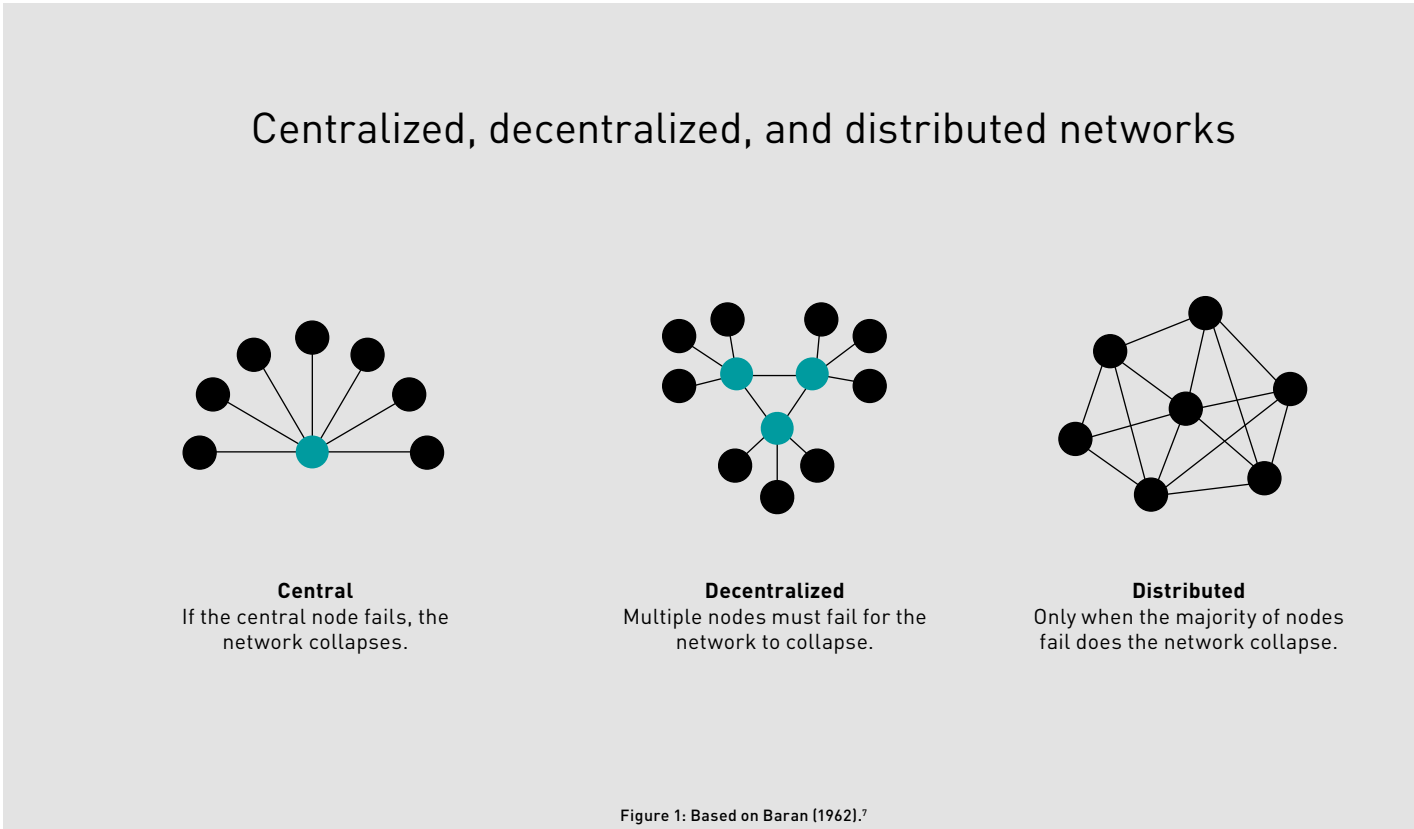


Figure 1: Based on Baran (1962).[7]

of Bitcoin was to create a currency that was not controlled by any central authority (such as central banks).

Since the publication of this idea, the technology has been continuously developed in order to exploit the potential of blockchain in a corporate context. Today, it is no longer a specific technology for cryptocurrencies, but a technology that offers advantages for applications in many industries. However, discussions about the potential applications of blockchain are still heavily influenced by cryptocurrencies and, since 2021, by so-called "non-fungible tokens" (NFTs). It is no wonder business leaders find it challenging to evaluate the short- and long-term benefits of the technology for their company. The questions we seek to answer are:

> What exactly are the advantages and disadvantages of blockchain?
> What is the concrete added value of blockchain in corporate practice?
> How can this value be exploited in a targeted manner?

In order to enable the beneficial use of blockchain, it is essential to move away from sweeping assessments and develop a differentiated understanding of the technology, its potential applications, and the opportunities and risks for industry and society. This study aims to contribute to this effort; thus, we address three aspects in this study:

> How blockchain works and possible applications
> How blockchain can contribute to a transformation from centralized to distributed value networks, as well as the opportunities and risks of this transformation
> Opportunities, challenges, and success factors in implementing blockchain applications

In this study, we occasionally mention cryptocurrencies to illustrate important blockchain concepts. However, the main focus is on applications beyond cryptocurrencies. We developed the content of this study based on literature research, in exchange with academics, and in close collaboration with experts from companies in different industries. This collaboration with the industry partners took place via bilateral discussions, project meetings, and three workshops, in which industry-specific applications were intensively discussed and evaluated. An overview of the partners is provided in the appendix. For ease of reading, references are not provided when describing basic or well-known (blockchain) concepts.


24/7

An introduction to blockchain

The blockchain technology

Blockchain technology was created in 2008 (and first implemented in 2009) by an unknown person or group with the pseudonym "Satoshi Nakamoto" with the application Bitcoin. To introduce a currency that is not controlled by any central authority, a system was created that regulates itself and prevents power concentration: the blockchain.

Traditionally, digital applications are run by a single organization that can set system rules and determine who can use the application and under what conditions. At least theoretically, this organization could also manipulate the data. If there is a program error or a cyber attack, the application may fail, or the data integrity may be compromised. In other words, any person or organization using a digital application and services based on it must trust that the operator can guarantee the protection goals of IT security: availability, confidentiality, and integrity (Figure 2). People usually do this subconsciously—for example, when they open a bank account or share their medical history when they visit a doctor. People trust that the systems that store account balances, transactions, blood values, or X-ray images are secure and function reliably.

Figure 2: Based on Laudon & Laudon (2019).[8]

Distributed applications, distributed ledger technology, and blockchain

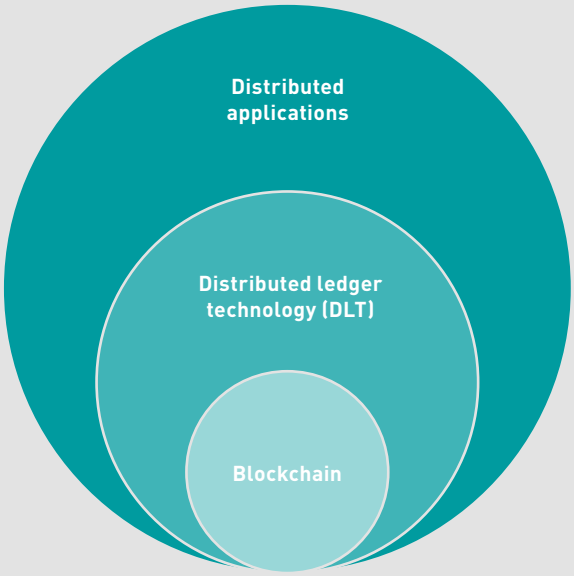


Figure 3: Based on Hileman & Rauchs (2017).[11]

Blockchain breaks the paradigm of centrally operated applications. Instead, applications are distributed across the computer systems of many parties who may also be end users. Not just one, but multiple parties have visibility into the system and can ensure that applications and the data they contain are not tampered with unnoticed. Even if the systems of individual parties fail, for example, due to system errors, the application continues to run stably on the systems of others. Because parties control each other, they no longer need to trust a single operator, and the need for a central authority can even be eliminated. But how exactly can this work? In the following, we explain essential blockchain terminology and how blockchain works.

Blockchain and distributed ledger technology

Blockchain and distributed ledger technology (DLT) are special forms of distributed applications (Figure 3). Distributed applications are run on multiple computer systems instead of centralized systems. Conventional distributed applications are usually managed by one party that all users must trust. Blockchain and DLT are unique in that they are designed to be used by multiple parties who do not necessarily trust each other.[9] They ensure the proper functioning of an application even if individual actors try to manipulate it or individual systems fail due to technical errors.

Blockchain is a particular manifestation of DLT in which transactions (changes to data) are bundled into "blocks" and stored on a blockchain. However, there are other types of DLT that are not blockchains. Today, however, the two terms are often used interchangea-

Differences between permissionless and permissioned blockchains

CATEGORY	PERMISSIONLESS	PERMISSIONED
Control of the network	Community	Central service provider or consortium of business partners
Access to the network	Not restricted	Only approved actors
Important application domains	Open platforms accessed by many parties, not all of whom know each other	Cross-organizational business processes
Main targets	Elimination of intermediaries Increasing the integrity, tamper resistance, and availability of digital infrastructures	Digitization and automation of business processes Increasing the integrity, tamper resistance, and availability of digital infrastructures Development of new business areas
Anonymity	Participants are mostly anonymous	Participants are usually not anonymous and also know each other outside the blockchain
Data sovereignty and access	Usually, everyone sees all data and transactions If necessary, data access can be restricted by off-chain data storage (see the "Data privacy" section in the following chapter)	Data sovereignty usually lies with the data owner to maintain confidentiality If necessary, the owner can share data, for example, for transactions with direct business partners

Table 1: Based on own research.

bly.[10] In this study, we use the term "blockchain," although many of our statements also apply to DLT as a whole.

Permissionless and permissioned blockchains[12]

Blockchain technology has been continuously developed since its introduction to meet the requirements of different applications. Today, two fundamentally different types of blockchains can be distinguished: permissionless and permissioned blockchains. However, there are also mixed forms of blockchain.

In the case of permissionless blockchains, any person or organization can participate in the network, carry out transactions, and provide computing power for the operation of the application. Usually, the participants do not know each other personally, and they act anonymously. Therefore, participation in the network is rewarded through incentive mechanisms. The best-known example is cryptocurrencies. On Bitcoin, miners who verify transactions receive Bitcoins for doing so. The common goals of permissionless blockchain applications are to avoid dependence on central authorities and to provide access to many people or organizations.

In permissioned blockchain applications, only selected actors are allowed to become part of the network. Anyone who wants to join must apply for membership and be approved. Permissioned blockchains are often used for enterprise applications (so-called enterprise blockchains). Here, organizations enter into contractual relationships outside of a blockchain, which is why additional incentive mechanisms on a blockchain are not necessarily required. One example is a system for product traceability that actors along the supply chain, such as manufacturers, suppliers, transporters, or retailers, can access. Ensuring system integrity and availability, increasing collaboration efficiency, automation, and cost reductions are the main goals.

Often, permissioned blockchain applications are not blockchains in the strict sense, as centralized decision-making entities continue to exist. These entities can be a single company, a consortium of companies, or an independent service provider that decides, for example, on the admission of new members to the network. These are nevertheless marketed as blockchain or DLT projects because they use several functionalities of blockchains (for example, distributed operations or digital signatures) and would probably not have evolved without the hype around blockchain. According to the 2019 2nd Global Enterprise Blockchain Benchmarking Study, more than 80% of permissioned enterprise blockchain applications are controlled by a centralized entity. However, many plan to distribute decision-making power among multiple network participants later.[12]

Table 1 summarizes the most important characteristics and application areas of permissionless and permissioned blockchains. Please note that there are additional variants and that the table only shows common areas of application and properties.

How blockchain works

In the following, we describe the basic functionality of blockchain. In practice, various combinations of the described techniques are used. We particularly address the differences between permissionless and permissioned blockchains.

Distributed operation

The most crucial difference from conventional applications is that blockchain applications are not run on a central computer system, but on the systems of multiple network participants. If one node illegally modifies the data, the other nodes would not accept the change. If one node fails, the system continues to run stably on the systems of other participants.

Distributed access

On permissionless blockchains, all nodes on a blockchain can access data from their systems. There is no central authority that controls who can view the data. However, on permissioned blockchains, data access can be restricted, and data sovereignty can remain with the owner of the data. For example, a node can see only its own transactions. This is important for maintaining confidentiality.

Consensus mechanism

In simple terms, consensus mechanisms are algorithms that ensure agreement on transactions between all nodes. They ensure that a transaction is legitimate and not illegally performed twice.

On permissionless blockchains, any node can usually view all data and verify the legitimacy of a transaction. Proof of Work and Proof of Stake (see box) are currently the best-known consensus mechanisms for permissionless blockchains. On permissioned blockchains, data access may be restricted to maintaining confidentiality, which is why other mechanisms are used. For example, the Corda enterprise blockchain platform uses automated notary services. In this case, only the business partners involved in the transaction must confirm it. A notary service automatically checks the transaction's legitimacy and ensures that there are no conflicts with other transactions.

Proof of Work and Proof of Stake

In Proof of Work, nodes verify transactions by solving cryptographic puzzles. Whoever is the fastest and thus validates a transaction receives a reward in the form of cryptocurrency. This process is called mining and constitutes a competition. Miners with great computing power have increased chances of solving tasks quickly and receiving rewards. Since many miners try to solve the puzzle and obtain the reward in parallel, the electricity consumption in Proof of Work networks is quite high. Bitcoin is one of Proof of Work's best-known applications. In theory, a malicious person or group of miners could attempt to provide at least 51% of the computing power on the network and thus gain control of the consensus mechanism (known as a 51% attack).

→

Proof of Stake requires nodes to offer a stake in the native cryptocurrency in order to be considered participants that validate transactions. Out of all stakers, an algorithm randomly determines who is allowed to validate a particular transaction and receive a reward for doing so. The higher the stake, the greater the probability of being selected.

Chaining

Once accepted, transactions cannot be changed to ensure that they cannot be denied afterward. To this end, transactions are stored in a chained manner. If Daniel transfers ownership of a valuable asset to Jan, and Jan passes it on to Karin, then the transfer of ownership is also recorded in this order. In practice, this ensures a single source of truth.

Encryption and anonymity

All data stored on a blockchain is accessible by all nodes in permissionless blockchains. However, even here, people often do not want the data to reveal too much. Therefore, participants do not use their real identity but an alphanumeric address, the so-called public key. The network only knows this public key and uses it to process transactions. All members also have a private key that only they know. Everything encrypted with the private key can only be decrypted with the corresponding public key, and vice versa. This ensures that only the actor possessing a private key can transact on behalf of the associated public key (this technique is called a digital signature).

Permissioned blockchains also use digital signatures. Here, however, actors must be approved before they become part of the network. The approval process can reveal the true identity of the actor. Thus, anonymity is not necessarily guaranteed. In enterprise applications, it is often desirable to know with whom one is doing business. To maintain the confidentiality of the data, data access rights can be restricted. For example, on the blockchain platform Corda, access can be restricted so that each node sees only its transactions.

Data privacy

Even while ensuring anonymity on permissionless blockchains, not all data, such as contract terms or prices, should be seen by others. So-called hash functions can assist in this regard. A hash function creates a hash value of data, which is a kind of data fingerprint. If the data is changed, the hash value also changes. It is impossible to draw conclusions about the data from the hash value.

Hash functions offer the possibility of storing actual data outside a blockchain (off-chain), for example, on the systems of the data-owning institution. The hash value is stored on a blockchain to prevent the data from being manipulated illegally. When the data is retrieved, the hash value allows checking whether the data has been manipulated. Off-chain data storage can be used on permissionless and permissioned blockchains.

Smart contracts

Smart contracts (self-executing contracts) are process steps written as program code on blockchains and are run automatically as soon as predefined conditions are met. For example, temperature sensors on product packaging for pharmaceuticals could continuously measure ambient temperature to ensure that cold chains are maintained. A smart contract could automatically mark the product as defective if the temperature is above a critical level for too long. Since this logic is written on blockchains and thus tamper-resistant, compliance with "contracts" is assured.

Tokens and tokenization

A token is a valuable asset that is digitally mapped onto a blockchain and is tradable. The most well-known token is Bitcoin, which can be traded like a currency and is therefore called a payment or currency token. Utility tokens map rights, such as voting or access rights. For example, platform providers can sell such tokens to users who want to gain access to the platform. The owner must show the token when entering the platform. A driver's license could also be mapped as a utility token. When renting a car, one must show this token using a smartphone. Security tokens are a form of financial securities, while equity tokens are a form of security tokens that are directly linked to company shares and voting rights.[13]

In the blockchain environment, "tokenization" refers to the mapping of tangible assets onto a blockchain as tokens. For example, a building worth CHF 10 million could be mapped into 100,000 digital tokens of CHF 100 each, which can then be traded.[14] Smart contracts could ensure that people who own such tokens also receive a share of the building's rental income. The division of ownership through tokens of value is called "fractionalization." Tokens can also represent less valuable assets, such as goods exchanged between companies along a supply chain to monitor their origin and identify counterfeits.[15]

One thing to keep in mind is that blockchains cannot ensure that transactions involving physical goods that take place on a blockchain will take place in the real world. This means that whenever a blockchain is used to manage objects that exist in the real world, mechanisms outside of a blockchain (off-chain) are necessary to ensure compliance with blockchain transactions. Such mechanisms may include audits, for example.[16]

Crypto currencies

A cryptocurrency is a virtual currency operated by a network through blockchain and is thus not controlled by a central authority. One goal of cryptocurrencies is to reduce dependence on (central) banks and thus avoid government intervention in the monetary system. The hope associated with cryptocurrencies is to create a distributed and robust financial system in which payments can be made faster and cheaper than in the traditional banking system. Bitcoin and Ether are the most well-known cryptocurrencies, with nearly 10,000 now listed on CoinMarketCap.[17] Cryptocurrencies are often criticized for their lack of controllability, immense val-

→

ue fluctuations, high electricity consumption, and use in illegal activities. Some economists also say that cryptocurrencies will never become real currencies, for example, because they are unlikely to be accepted by governments, and, therefore, cannot be used for important financial transactions such as taxes.[18]

Non-fungible tokens

NFTs are unique, non-substitutable valuable assets. While a Bitcoin can be exchanged for any other Bitcoin, an NFT digitally represents a valuable asset that exists only once or a few times and whose ownership rights need protection. NFTs are often used to protect the property rights of intangible assets (for example, digital art), as they are relatively easy to copy. For example, NFTs enable artists to sell their art directly without auction houses or galleries, which traditionally certify the authenticity of works and enjoy the trust of prospective buyers. In addition, smart contracts can fix terms, such as royalties, that must be paid automatically each time a work is resold. However, NFTs can also be used to map the ownership of tangible objects. In 2021, the market volume for NFTs was US$ 41 billion.[19]

One prominent example of NFTs is the collection of art forger Wolfgang Beltracchi. This artist came to dubious fame because he had forged pictures of great masters for years and sold them through well-known auction houses. He has created 4,608 digital artworks stored on a blockchain, each based in a different artistic style on the painting Salvator Mundi by Leonardo da Vinci. While the original painting was auctioned off in 2017 for US$ 450 million, Beltracchi offered his NFTs for sale for a total of CHF 55 million.[20]

→

The performance and electricity consumption of blockchains

Many experts have critically debated the performance of blockchains in terms of throughput (transactions per second) and speed or latency (time to complete a transaction). The so-called blockchain trilemma states that high scalability (i.e., increasing transaction volume without compromising speed), conflicts with the decentralization and security of blockchains. On permissioned blockchains, throughput and speed are usually sufficiently high, but decentralization and security are lower than on permissionless blockchains.

Electricity consumption is mainly high on permissionless blockchains that use the Proof of Work consensus mechanism. Estimates suggest that the Bitcoin system consumes more than twice as much electricity per year as the whole of Switzerland.[25] This is significantly lower for permissionless blockchains with Proof of Stake consensus mechanisms or for permissioned blockchains. The Ethereum Foundation, which switched from Proof of Work to Proof of Stake in September 2022 (the so-called "Merge"), expects this to reduce Ethereum's electricity consumption by 99.95%.[26] The downside is that members with greater financial resources have increased influence over the network. Ultimately, determining which construct is best suited for each application involves individual decisions.

Blockchain governance

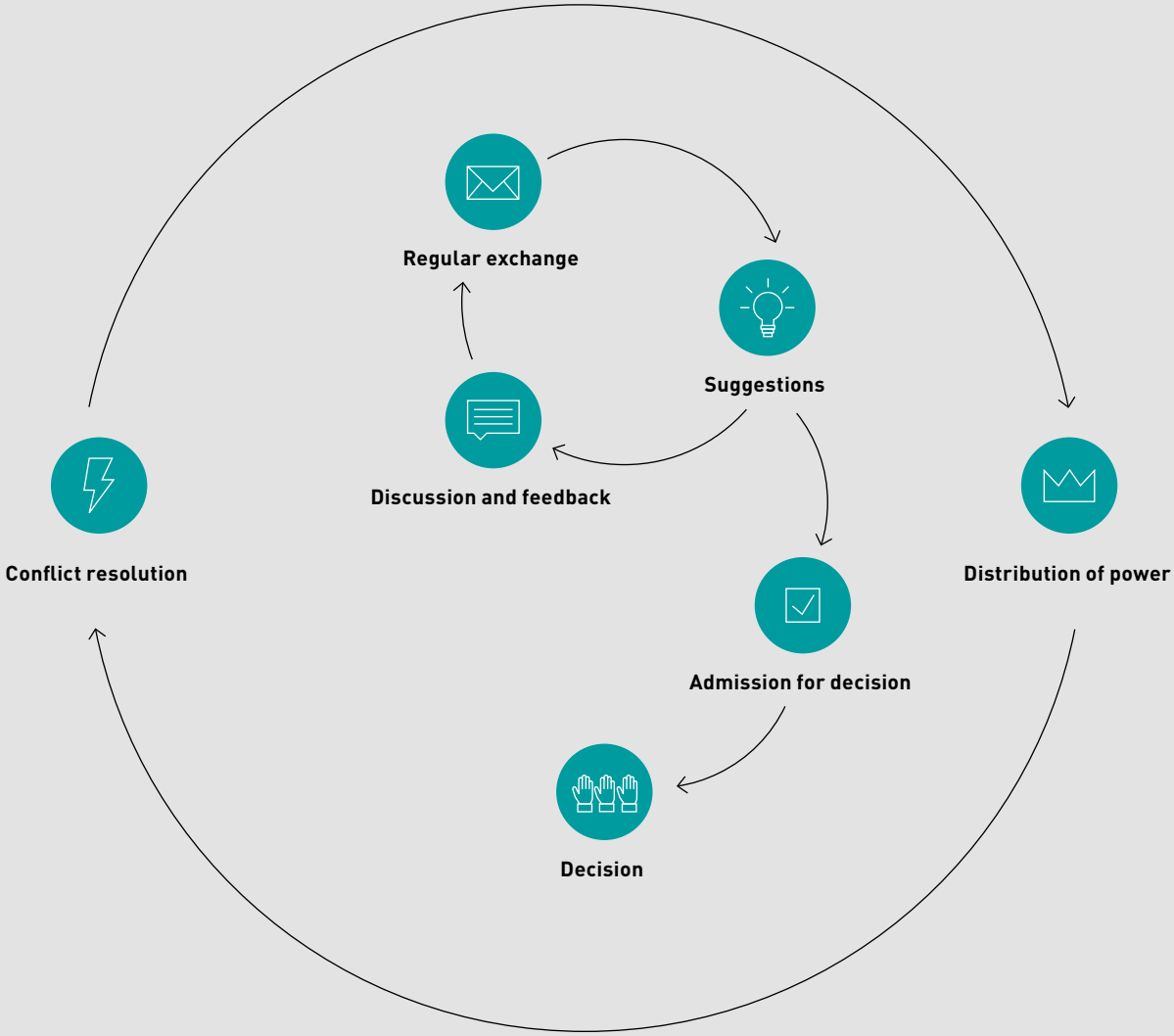
When many members make decisions in a network, the question arises as to how decision-making works. Governance deals precisely with this question. In the narrower sense, governance is less about procedural decisions, such as the validation of transactions. These are part of everyday operations, i.e., the rules and processes that ensure the basic functioning of an application. Instead, it is about decisions on changes to operations to react flexibly to changing market conditions. Examples of such decisions include changing the consensus mechanism from Proof of Work to Proof of Stake in permissionless networks or adding new members to permissioned networks.

Governance mechanisms determine who can influence the system and are thus crucial for an application's acceptance and long-term viability. When designing these mechanisms, the interests of the founding members play a role, as do those of all future potential network members. Bringing about decisions starts long before the actual decisions are made, as shown in Figure 4.

Blockchain differentiates between two types of decision mechanisms. On-chain mechanisms are written permanently into the program code of a blockchain. Off-chain mechanisms, on the other hand, involve decisions that are made outside a blockchain, for example, in meetings or at conferences.

On-chain decisions must be mapped in the form of clear rules. Often, this involves voting. On-chain voting is often used on permissionless blockchains, as the network members here

Governance mechanisms in blockchain projects



How are members informed about new developments, and how can they exchange information about them?

Who can submit change proposals through which channel?

Who can provide feedback on proposed changes and through which channel?

How are change proposals admitted for decision-making?

How are decisions made on admitted change proposals?

What happens in the event of conflicts that cannot be resolved by the members themselves, or in the event of malicious behavior by individual actors?

How can it be ensured that no actor influences other actors too much and thus accumulates an unreasonable amount of decision-making power?

Figure 4: Inspired by Barrera (2019).[21]

On-chain voting mechanisms of three blockchain solutions

NAME	DESCRIPTION OF THE VOTING MECHANISMS
DASH	Anyone can submit proposals for a price of a token. Master nodes can vote on proposals, with each master node having one vote. Anyone with at least 1,000 tokens can become a master node. Proposals are accepted if the difference between the number of approvals and rejections is at least 10% of all available votes.
TEZOS	Those who own tokens can assign them to a so-called baker who best represents their interests. Baker can become any node that has at least 6,000 tokens. Bakers can propose changes and decide on them. The proposal is considered accepted if a minimum number of tokens have voted and a qualified majority agrees.
EOS	All those who own tokens can assign them to so-called Block Producers. The 21 Block Producers with the most tokens can make decisions if at least 15 of them agree.

Table 2: Summary according to Watson Law (n. d.)[22] and own research.

do not know each other. In Table 2, we present exemplary on-chain voting mechanisms from three blockchain solutions.

For enterprise applications in permissioned blockchains, decisions are often made off-chain. Fixing the mechanisms on-chain is less critical, as the companies participating in the network usually know each other off-chain and enter into legally binding contractual relationships.[23]

On-chain and off-chain mechanisms can also be combined. For example, proposed changes can be submitted and discussed outside the blockchain (e.g., in forums) before being voted on the blockchain. In the Decred cryptocurrency project, minor decisions are voted on-chain, while strategic decisions are made off-chain according to defined rules.[24]

Benefits of blockchain technology

"Distributed ledger technology allowed us to increase transparency and B2B efficiency in the global gold value chain while maintaining data and transaction sovereignty of business partners. Trust in gold, thanks to the immutable integrity certificates, is reinstated."

Urs Rööslı, CEO aXedras

In the following section, we present the business goals of blockchain deployment and then summarize blockchain applications discussed in the literature and developed by companies.

Goals of the use of blockchain

Along the dimensions of degree of automation and power concentration, we distinguish four goals of blockchains: integrity, automation, cooperation, and the creation of distributed value networks (Figure 5).[27]

Integrity

The main goal of integrity is to create a tamper-resistant data registry ensured by the distributed operation architecture of a blockchain. Illegitimate changes would be noticed, and the high availability of the system is guaranteed, as it continues to run even if individual nodes fail. Examples of blockchain applications with an integrity goal include digital land registers, authenticity certificates for valuable assets to prevent counterfeiting, and proofs of origin for goods such as food.

The demand for information with integrity about products and organizations is increasing by tendency. For example, private and institutional investors are increasingly considering sustainability criteria in their investment decisions. This requires data capturing along the entire supply chain, including the origin of ingredients and the means of transport used.

Automation

Another goal of blockchain technology is to automate as many process steps as possible, for example, with smart contracts. Tokens can be used to map physical goods and virtual assets, such as ownership or access rights, and make them tradable. Increasing efficiency and avoiding human errors in manual processes are the main focus. For example, digital twins—digital representations of physical objects—can be created securely, thereby digitizing and automating production, warehousing, and auditing processes.

That processes are representable with conditional logic is a prerequisite for automation. The more structured a process is, the greater the potential for automation, for example: After receiving a payment specifying the order number, a payment receipt confirmation is issued automatically, and the corresponding receivable is booked out of the distributed accounting system.

Not all steps can be automated via blockchain when physical objects play a role. An interface to the real world is necessary, as blockchain exists only in the digital world. Off-chain mechanisms, such as audits for compliance and product identifiers, are necessary.

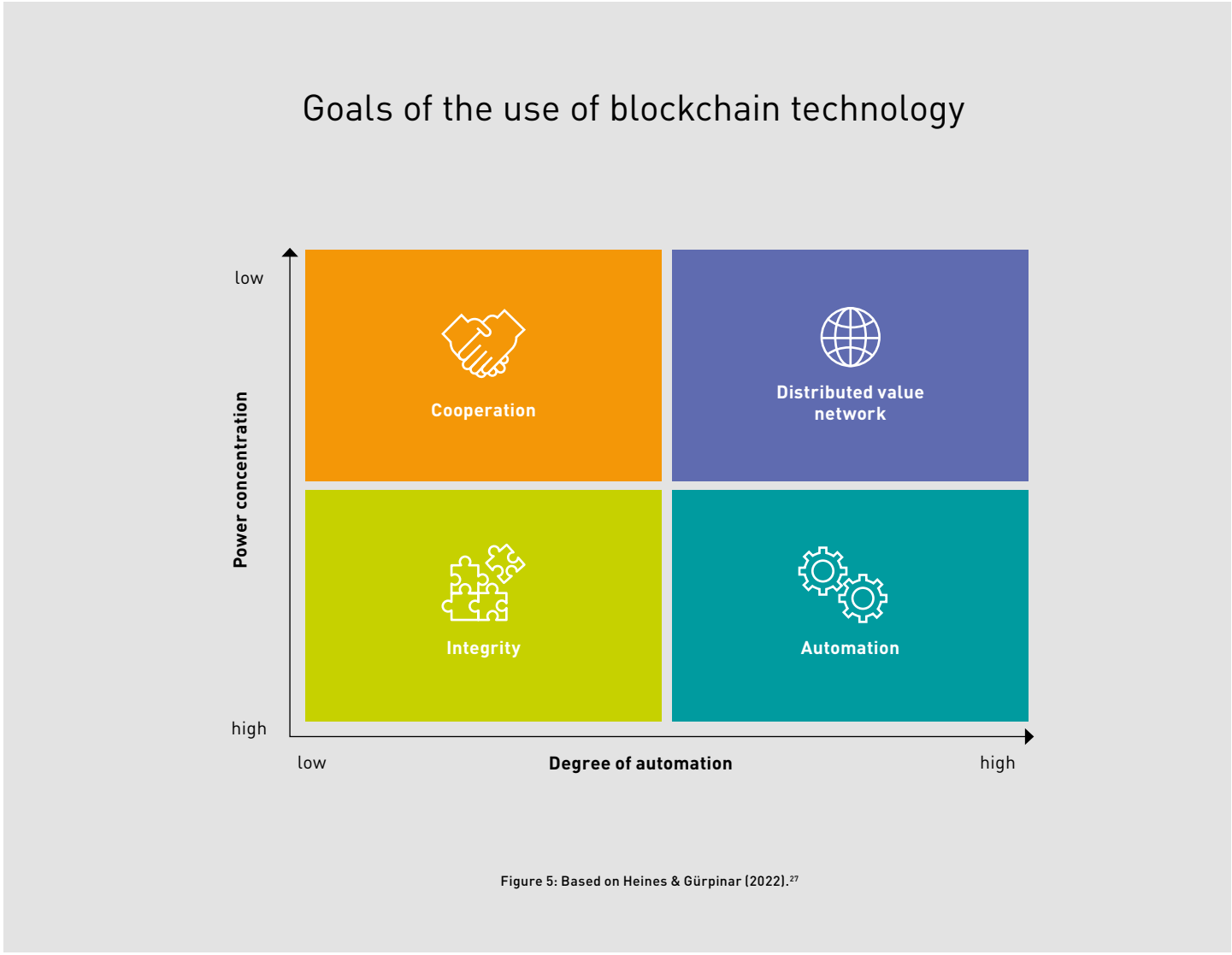


Figure 5: Based on Heines & Gürpinar (2022).[27]

Cooperation

Another goal of blockchain technology is to reduce coordination efforts and enable efficient collaboration among many parties. For this purpose, the cooperation processes are formalized as logic and directly written on-chain into the program code, making them tamper-resistant. Standardizing and digitizing cooperation processes often require initial effort and coordination among the involved stakeholders.

One example is product tracking systems: Manufacturers, suppliers, traders, transport service providers, and points of sale share information about products, their origin, and delivery routes via blockchain to increase transparency, product safety, and support planning.

Distributed value networks

In centrally organized value networks, an entity provides an infrastructure on which users interact and exchange data. In distributed value networks, the participants' systems jointly form a digital platform. Together, they can decide on the conditions for participation and the rules of interaction. Collaboration and business processes are written as completely as possible in the program code of a blockchain. This lowers transaction costs, making the solution easy to scale and giving more people or organizations access. Unlike conventional marketplace-oriented platforms such as Uber, Facebook, or Airbnb, the decision-making powers are not in the hands of a few influential organizations but are distributed across many shoulders. For example, in a peer-to-peer car sharing solution, all members could vote on decisions regarding system

changes. Driver's license verification takes place automatically in the background, and payment is triggered in cryptocurrency when the car is unlocked.

In Figure 6, we describe the guiding questions to help identify targets for the use of blockchain technology. The figure is based on an analysis of existing decision models for blockchain deployment.[28] We have simplified the complexity of these models and mapped the guiding questions to the four objectives outlined earlier. Any decision to use blockchain technology will, of course, require deeper analysis.

Decentralized autonomous organizations

New forms of organization may be needed to create distributed value networks. Decentralized autonomous organizations (DAOs) are a new organization form enabled by blockchain technology. In a DAO, no traditional management functions exist; instead, the members, often individuals who hold stake in the company, make decisions through voting. Operational processes are automated as much as possible using smart contracts, allowing the organization to fulfill its purpose autonomously.[30]

DAOs reduce dependency on central entities and are transparent and efficient because processes are written in code and automated. However, there are unresolved liability issues with DAOs, and they may still require human intervention in the event of unforeseen events. For example, in 2016, due to a DAO hack in the Ethereum blockchain in which more than 3.6 million Ether were stolen, a profound change was made to the program code (a so-called hard fork) to reverse the hack.[31] This protocol change led to the co-existence of Ethereum Classic and Ethereum. The latter has the largest market capitalization next to Bitcoin and is a core backbone of NFTs and decentralized finance (DeFi).

→

Blockchain in corporate practice

In practice, companies usually pursue combinations of these goals, and the goals build on each other. Integral data storage and processing is a minimum prerequisite for automation and cooperation with blockchains, which in turn are prerequisites for creating distributed value networks.

Discussions about the potential applications of blockchain technology often revolve around the complete elimination of intermediaries through distributed value networks. However, suppose the goal of blockchain use is to increase data integrity, automation, or cooperation efficiency. In that case, it is still possible for a central entity or consortium of business partners to control the network. In 2019, over 80% of permissioned blockchain applications deployed by enterprises worldwide were controlled by a centralized entity.[32] Accordingly, it is not necessarily required to abolish proven

Blockchain goal framework

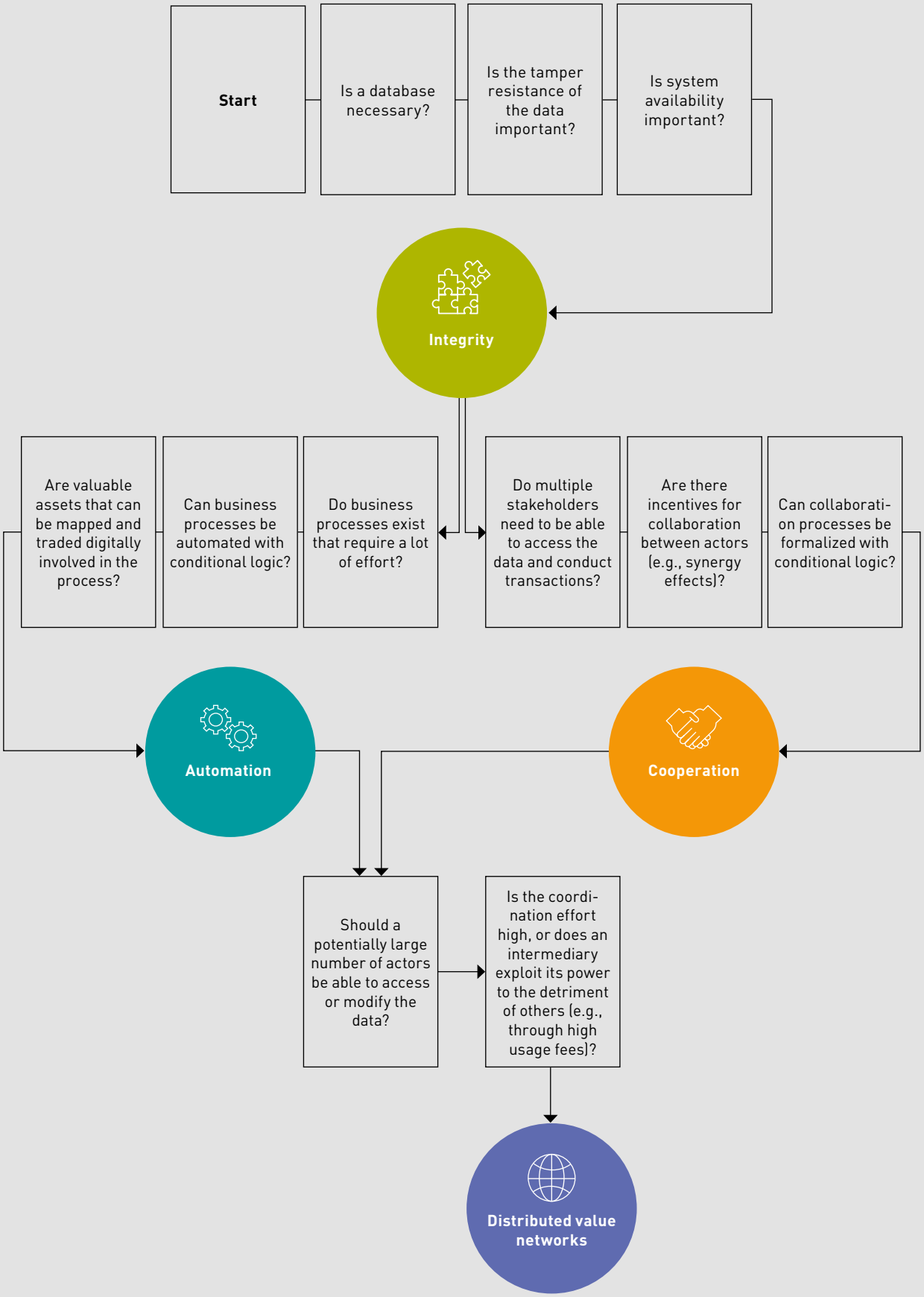


Figure 6: Inspired by Meunier (2016).[29]

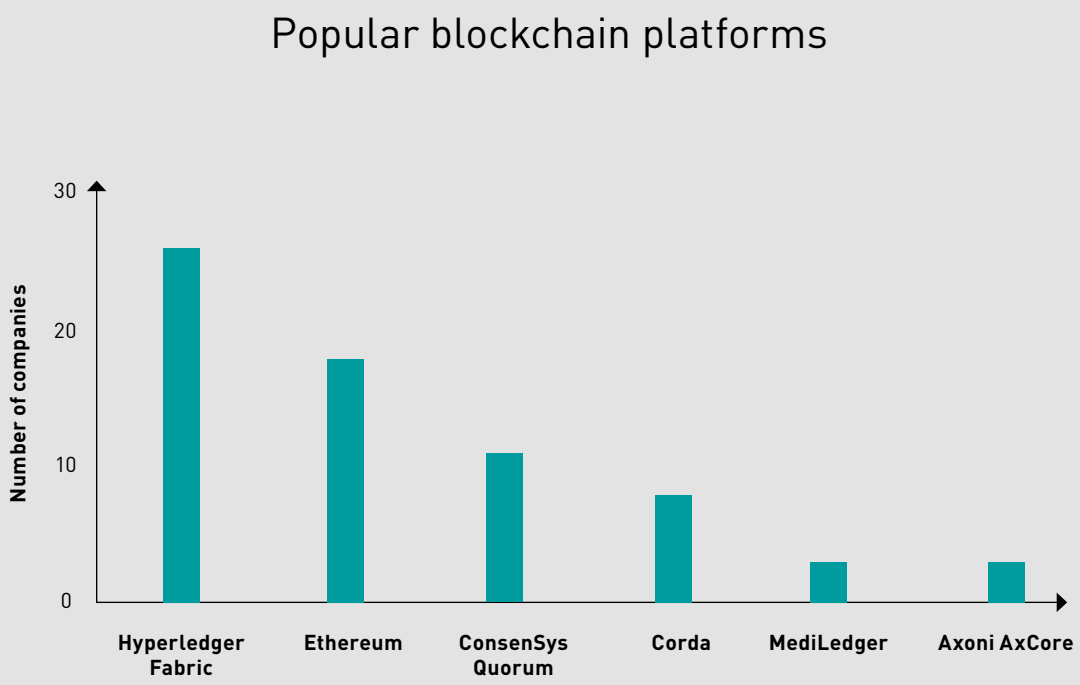


Figure 7: Blockdata (2021).[33] Number of the largest 100 listed companies using a blockchain platform.

structures, such as central service providers, to deploy blockchain beneficially.

For enterprise applications, permissioned blockchains play a significant role. A network of business partners wants to remain in control of the value network and be able to ensure that data confidentiality is maintained. The application is distributed on multiple approved organizations' systems to increase tamper resistance and availability. Lastly, clearly defined interfaces and smart contracts securely automate data exchange across organizations.

Many technology service providers offer blockchain infrastructure and development environments that allow organizations to develop permissioned and permissionless blockchain applications (Figure 7).

Often, the attempt to deploy blockchain technology is also a driver for standardizing existing manual processes, as this is a prerequisite for digitizing them using blockchain. If business processes are mapped in a tamper-resistant manner using blockchain, many new applications and business models can open up. Electronic identities (e-IDs) are one example: blockchain allows the secure identification, organizations, or objects in the digital space. This creates many new possibilities, such as access management to buildings without physical keys, tamper-resistant authenticity certificates for goods, peer-to-peer marketplaces, or a robust data infrastructure for the Internet of Things. According to the 2nd Global Enterprise Blockchain Benchmarking Study, most companies are pursuing the goal of cost reduction through the use of blockchain in the first step and subsequently also the goal of developing new business areas and increasing revenues.[34]

Tracing gold using digital twins

Switzerland plays a central role in the global gold market. Over a third of gold is refined in Switzerland and Zurich is one of the most important global trading centers for gold alongside London. Data exchange along the gold value chain is characterized by data silos and a lack of data standards; thus, transparency, efficiency, and protection against counterfeiting suffer. Creating transparency about gold's origin and provenance while maintaining confidentiality regarding ownership, prices, and sourcing volumes remains a challenge.

aXedras was founded by specialists from the precious metals and IT industries to develop a specific product platform that addresses these challenges. The solution was found in a permissioned DLT system, through which 30 members already exchange data globally on physical products while maintaining sovereignty over confidential transaction details. Each physical product receives a digital twin with an integrity certificate that provides tamper-resistant documentation of origin and chain of custody along the supply chain, ensuring the integrity of data and the products. This increases efficiency for members in collaborating along the supply chain and transparency to buyers (industrial, jewelry, and watchmaking companies) and financial investors.

The most significant difficulty in implementation was convincing the independent players in the global value chain to join the network. Good contacts and relationships in the gold industry and the neutral position of aXedras as a pure technology provider were helpful. This platform, proven for gold, has the potential to digitize further supply chains for high-value products, thus ensuring greater transparency, efficiency, and trust. An expansion of the platform is foreseen.

Blockchain applications in various industries

The benefits of blockchain described above offer advantages in many industries. Due to the continuing digitization of processes, which was further spurred by the COVID-19 pandemic, the number and types of blockchain applications will likely continue to grow. Figure 8 illustrates the possible applications of blockchain technology in 10 different industries.

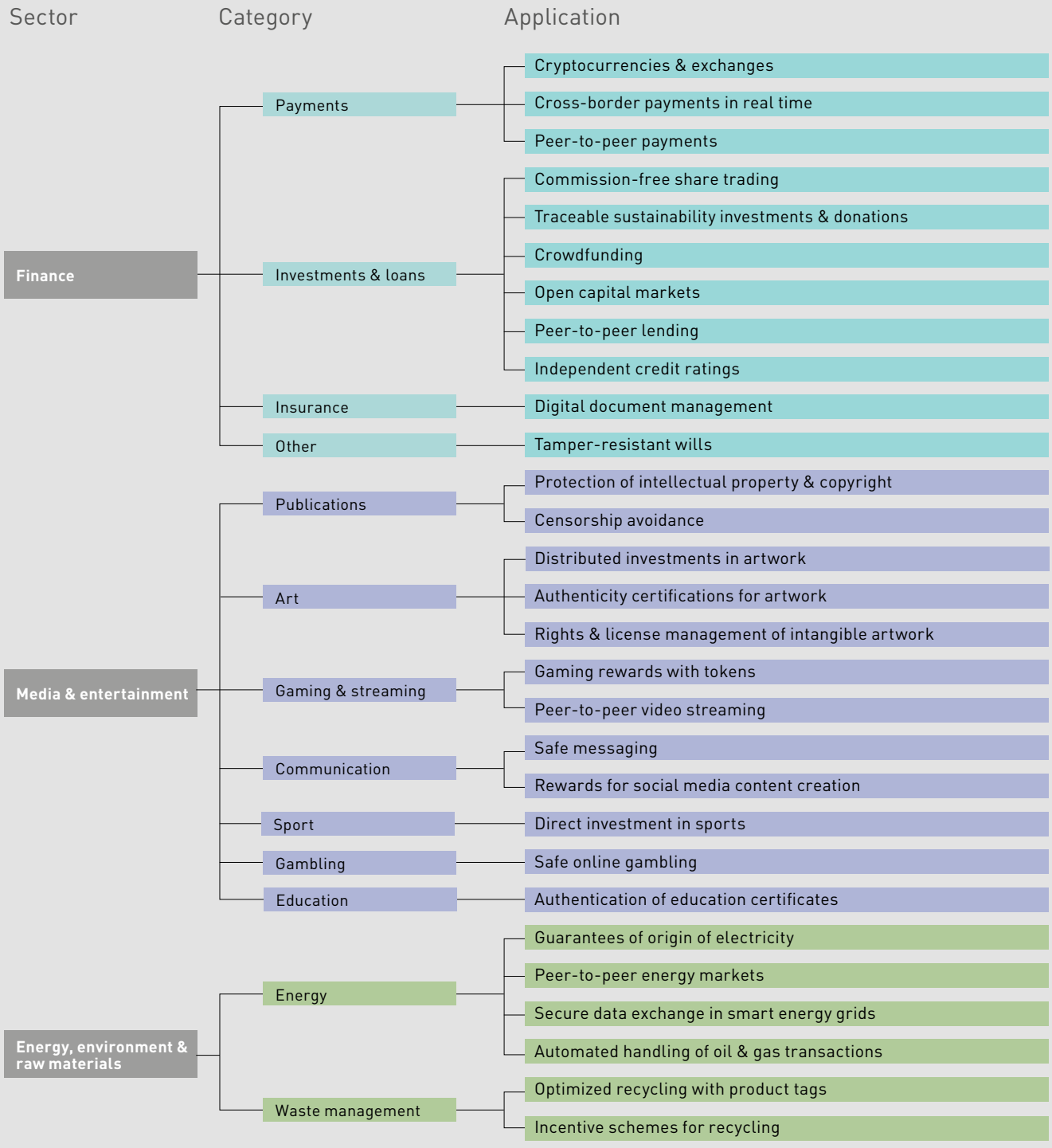
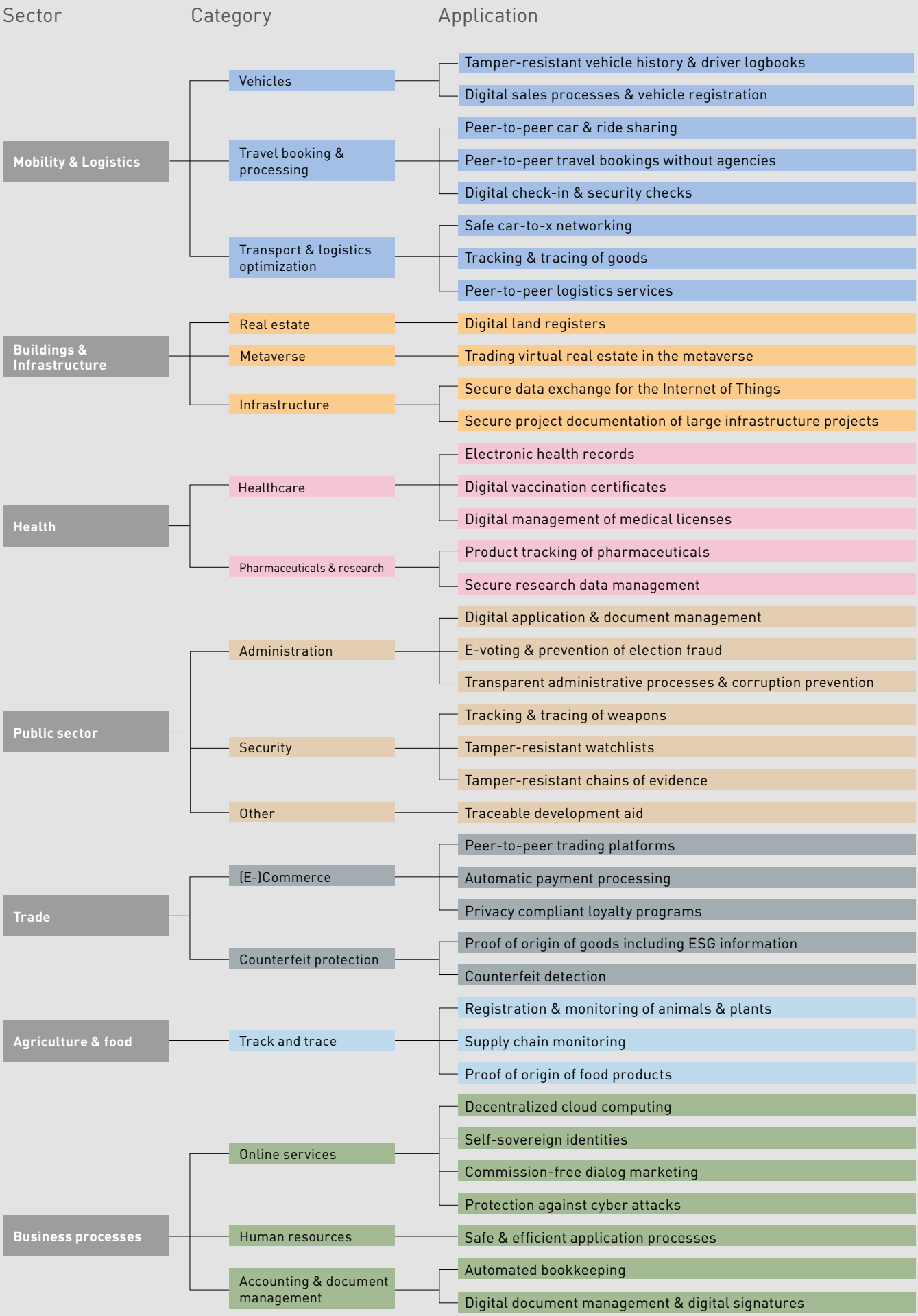


Figure 8: Based on CB Insights (2022)[35] and further research.


Sector
Category
Application
Mobility & Logistics
Vehicles
Tamper-resistant vehicle history & driver logbooks
Digital sales processes & vehicle registration
Travel booking & processing
Peer-to-peer car & ride sharing
Peer-to-peer travel bookings without agencies
Digital check-in & security checks
Transport & logistics optimization
Safe car-to-x networking
Tracking & tracing of goods
Peer-to-peer logistics services
Buildings & Infrastructure
Real estate
Digital land registers
Metaverse
Trading virtual real estate in the metaverse
Infrastructure
Secure data exchange for the Internet of Things
Secure project documentation of large infrastructure projects
Health
Healthcare
Electronic health records
Digital vaccination certificates
Digital management of medical licenses
Pharmaceuticals & research
Product tracking of pharmaceuticals
Secure research data management
Public sector
Administration
Digital application & document management
E-voting & prevention of election fraud
Transparent administrative processes & corruption prevention
Security
Tracking & tracing of weapons
Tamper-resistant watchlists
Tamper-resistant chains of evidence
Other
Traceable development aid
Trade
(E-)Commerce
Peer-to-peer trading platforms
Automatic payment processing
Privacy compliant loyalty programs
Counterfeit protection
Proof of origin of goods including ESG information
Counterfeit detection
Agriculture & food
Track and trace
Registration & monitoring of animals & plants
Supply chain monitoring
Proof of origin of food products
Business processes
Online services
Decentralized cloud computing
Self-sovereign identities
Commission-free dialog marketing
Protection against cyber attacks
Human resources
Safe & efficient application processes
Accounting & document management
Automated bookkeeping
Digital document management & digital signatures

Blockchain in Switzerland and internationally

Since the introduction of the blockchain idea in 2008, the number of blockchain companies has increased steadily. The volume of investment in such companies also increased significantly. According to information from the portal Blockdata, by far, the most investments in blockchains in 2021 were made in the United States, followed by the United Kingdom, Hong Kong, Canada, and France.[36] According to Blockdata, 81 of the world's 100 largest listed companies were already using or testing blockchain technology in September 2021.[37]

Switzerland is considered a global leader in blockchain technology development. Advantages associated with Switzerland include the availability of experts, a high level of political and economic stability, openness to new technologies, and clear and pragmatic regulations in the area of blockchain.[38] For example, in 2018, the Swiss Financial Market Supervisory Authority (FINMA) became the first regulator to publish guidance on the classification of tokens and Initial Coin Offerings (a method of acquiring capital via tokens).[39] Laws for distributed electronic registries and DLT trading systems in Switzerland were in force since August 2021.[40] Switzerland is also at the forefront of blockchain research. The University of Zurich's Blockchain Center ranked first in the Western world in 2022 in an international ranking conducted by CoinDesk and MIT.[41]

Zug is a hub for blockchain companies because it is home to Crypto Valley, a federally funded association for blockchain and cryptography. According to a study by CV VC, more than 1,100 blockchain companies were active in Switzerland in 2022. A separate query on the company database Crunchbase shows that most Swiss blockchain companies develop applications for the financial sector, followed by companies that generally advance blockchain technology, for example, in the form of blockchain enterprise platforms. This confirms Switzerland's expertise in developing blockchain applications in the financial industry and beyond.

Below, we present global and Swiss statistics on the use of blockchain. The industry classifications used in the statistics differ, as they come from different sources.

Global blockchain statistics

Blockchain investments by venture capital funds, banks, and large companies by industry and economic sector in 2021

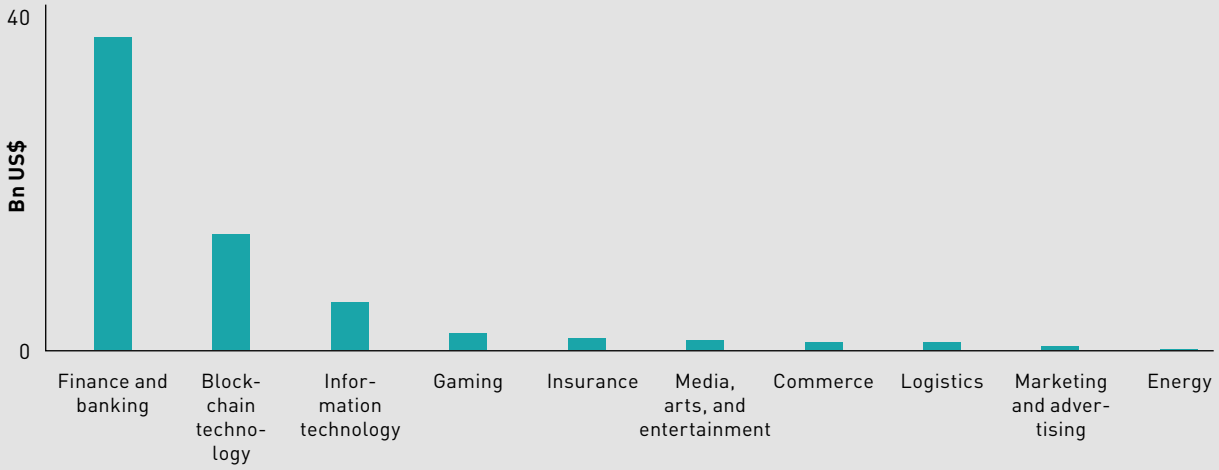


Figure 9: Blockdata (2021).[42]

Operational enterprise blockchains by industry in 2019

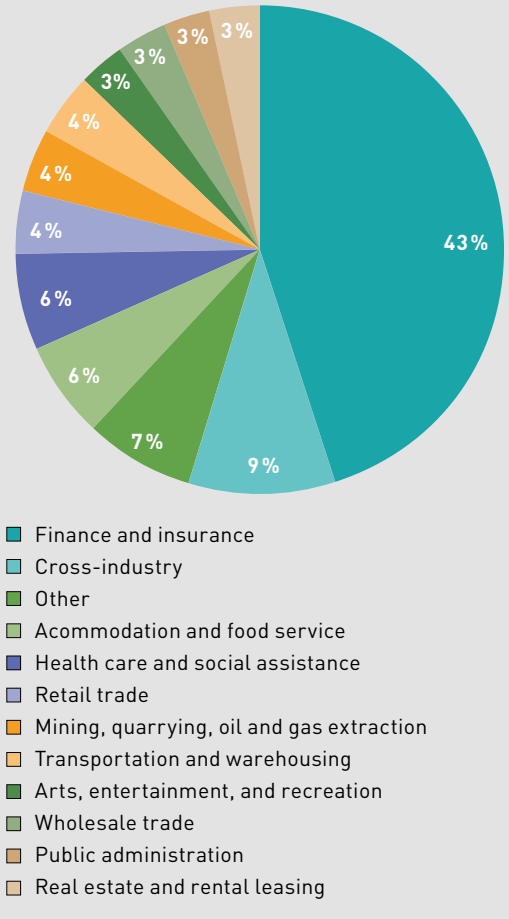


Figure 10: Rauchs et al. (2019).[43] Based on a study of 67 operational, permissioned blockchain applications in an enterprise context.

Operational enterprise blockchains by use case in 2019

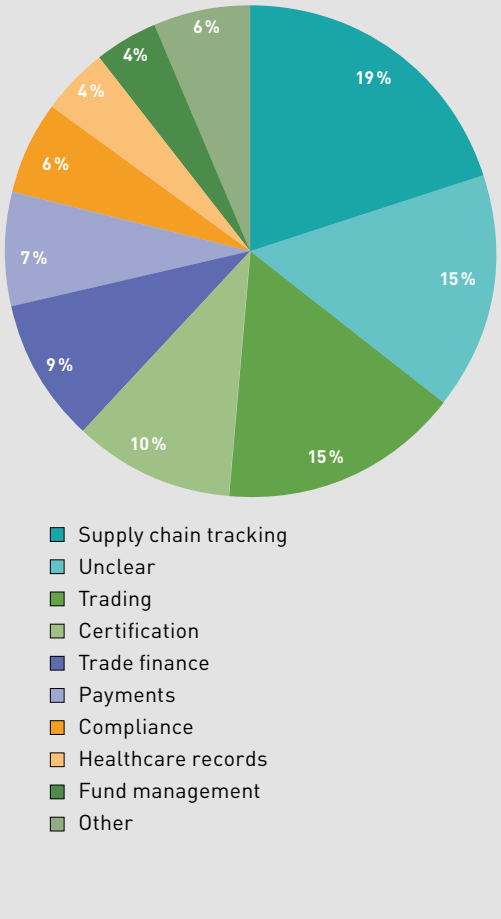


Figure 11: Rauchs et al. (2019).[44] Based on a study of 67 operational, permissioned blockchain applications in an enterprise context.

Swiss blockchain statistics

Companies and employees

1,135
Number of blockchain companies in Switzerland and Liechtenstein in 2021

5,766
Number of employees

Figure 12: CV VC (2023).[45]

Blockchain companies in Switzerland by industry and economic sector

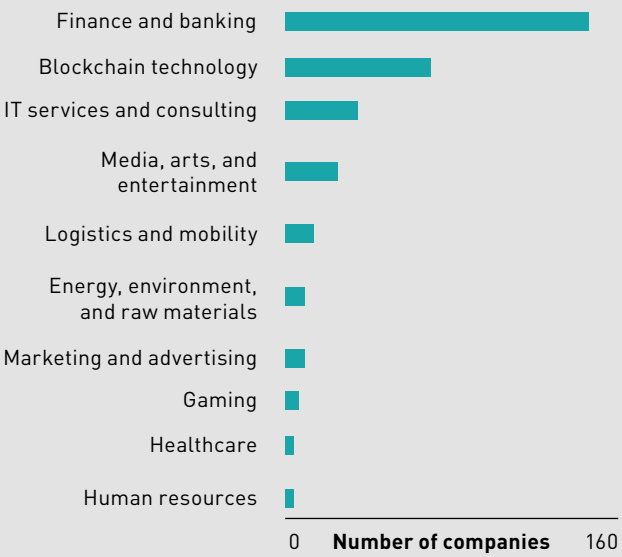


Figure 13: Own query on Crunchbase.com (date: 19.10.2022).

Blockchain companies in Switzerland and Liechtenstein by canton in 2022

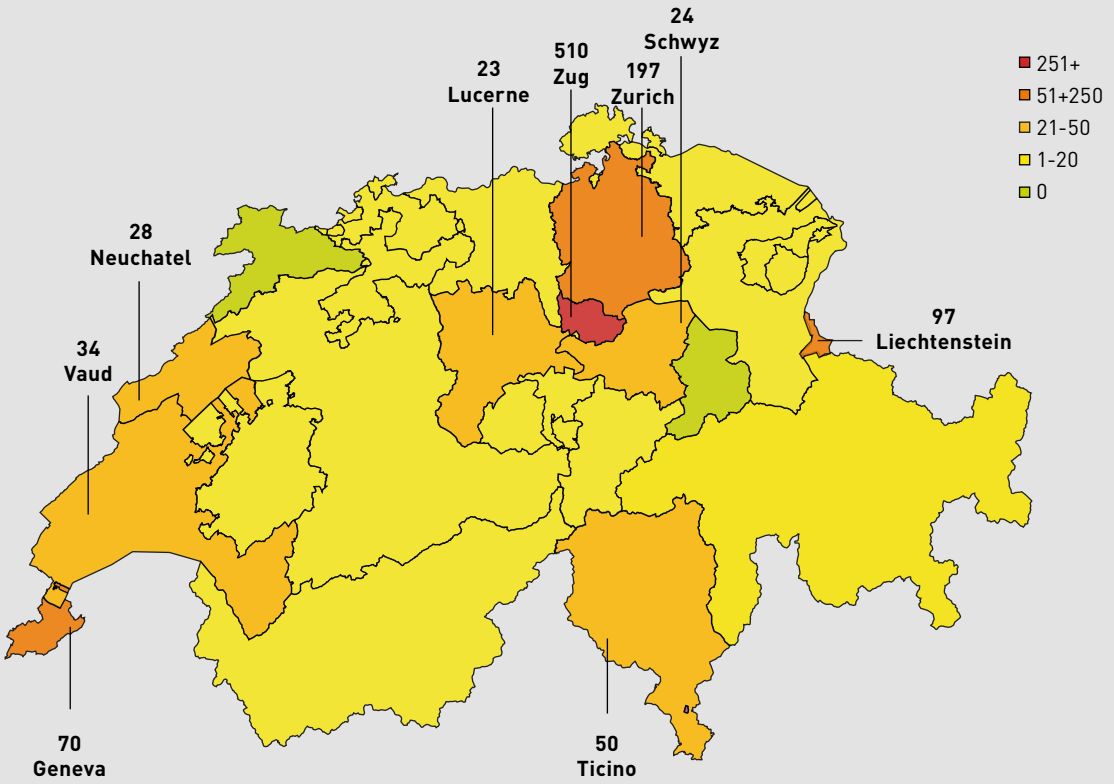


Figure 14: CV VC (2023).[46] Only cantons with more than 20 companies are mentioned.

The shift to distributed value networks

"Blockchain enables entirely new business models. Thanks to this infrastructure technology, data and value can be stored and traded efficiently, resiliently, transparently, and securely."

Roger Süess, CEO, Green

Today, most companies use blockchain to increase the integrity and availability of digital infrastructures, leverage efficiency and cost-cutting potential, and tap into new business areas. Many experts believe that, in the long term, blockchain could completely dissolve existing centrally organized structures in favor of distributed value networks. Questions of whether, how, when, and with what probability these scenarios will occur are usually left open. This change is not only a technological but also a social process that requires the solution of many conflicts of interest. Therefore, we should critically scrutinize such predictions. Nevertheless, perceiving such visions is essential to discussing the technology's opportunities and risks.

In the following section, we use examples from four industries to illustrate the hopes placed in distributed value networks and then discuss their advantages and disadvantages.

What is Web 3.0?

Web 1.0 refers to the Internet of the past, in which people mainly surfed static websites without creating or sharing content themselves. Web 2.0 describes today's Internet, wherein users communicate and share content. These interactions take place primarily on large platforms controlled by a few companies that generate profits from the collected user data. Web3 or Web 3.0 are collective terms for many visions of the future of the Internet, in which digital content and revenues generated with data are shared fairly among users, creators, and providers. Platforms are not owned by a few powerful companies but by the participants who take part in the development and thus receive shares. Blockchain is the foundation of this vision, as it allows the management of ownership and transactions between many participants in a tamper-resistant and automated manner.[48]

Visions of distributed value networks

Sharing economy

Today

The sharing economy intends to increase the utilization of goods through shared use, thereby reducing the number of goods produced. Although the sharing economy seems to be a collaborative project, the reality is different. Much of the shared consumption is coordinated by central intermediaries. For example, Uber organizes ride sharing, and AirBnB manages accommodation sharing. These providers have gained so much market power that they can dictate the terms of sharing. For example, Uber has repeatedly been criticized for precarious employment. Many sharing platforms charge high fees for their services. For Uber, it is 25% of the fare.[47]

Often, goods are not shared between users but are provided by companies for users. For example, for car sharing, companies places new cars on roads. Whether this reduces the number of vehicles on the streets and the number of kilometers driven is contested.

Future

Private individuals offer their property for use by others, especially products that are not worth buying because they are expensive and rarely needed. This is true not only for cars or accommodations, but also items such as drills, parking spaces, or tents. The initiation of sharing transactions takes place on a platform provided and controlled by a network of organizations and individuals using blockchain technology. The fee structure covers costs but is not for profit. Sharing contracts are concluded directly between sharers and users (peer-to-peer). The contractual terms for sharing are negotiated directly between them. Requirements for sharing, such as driver licenses for car sharing, are verified automatically via the electronic identities of the members, which are also realized via blockchain. Once all transactions are concluded the fees paid are documented transparently and tamper-resistant for tax offices. The taxes due are automatically calculated.

Online publications and advertising

Today

Free content is offered everywhere on the Internet: on streaming platforms, news websites, blogs, or social media platforms. Often, content is shared without asking the creators or financial compensation. Most content creators make little or nothing from creating original content and sharing their knowledge with others. Only a few very successful and popular content creators or influencers earn well from their online presence. At the same time, a small number of companies profit significantly from the voluntary sharing and consumption of online content. They collect as much information as possible about their platforms' users to show them targeted advertising that corresponds as closely as possible to their personal interests. For each advertising click, money flows from the advertisers to the Internet companies, and only little remains with the content creators. The users of these digital offerings do not know what data is collected about them and how it is monetized. The user-friendliness of the Internet suffers significantly from this model, since advertisements and prompts to open an account or subscribe to a newsletter are constantly displayed and cover the actual content.

Future

Every contribution published on the Internet is, by default, unambiguously assigned via self-sovereign identities that are realized with blockchain to its creator. Internet users have full transparency about the information collected about them. They can share their data voluntarily or for remuneration and set the conditions themselves. An open market for content and data thus evolves. For example, people receive financial compensation if they provide their data for advertising purposes and agree to see advertisements. The revenue generated by advertising is automatically divided among the data-sharing individuals, the operators of portals or blogs, and the content creators. Reusing intellectual property on the Internet is automatically recognized and compensated for with cryptocurrencies and smart contracts.

Electricity trading

Today

Electricity is mainly generated in central power plants, distributed by grid operators, and sold to households by energy suppliers. The origin of the electricity—which power plant it comes from, used energy carriers—is certified with so-called guarantees of origin, and consolidated in central registers. This allows the monitoring of the electricity mix and ensures that producers and suppliers only sell produced electricity. According to a decree by the Swiss Federal Department of the Environment, Transport, Energy and Communications, electricity suppliers have to inform their customers and the public once a year about the energy carriers used to generate the electricity and whether the electricity was generated in Switzerland or abroad.[49] However, consumers do not know which plants generated their electricity. Small electricity generation plants, such as photovoltaic systems on the roofs of houses, are not registered in the system at all. If the central systems for monitoring certificates fail, there is a risk that important information will be lost.

"In future energy systems, many entities, such as PV systems, storages, electric vehicles, heat pumps, and buildings, are connected via Internet of Things technology. Blockchain could enable secure and reliable data exchange between them."

Dr. Matthias Galus, Head Digital Innovation Office, Swiss Federal Office of Energy

Future

Central power plants hardly exist anymore, and many distributed plants and storages generate and store electricity. The origin of electricity is recorded automatically via measuring devices at generation plants and stored in a tamper-resistant, highly available blockchain register. This ensures that generated electricity is sold only once, with the correct characteristics. Private households that both consume and generate electricity can sell surplus electricity directly—without detours via electricity suppliers—to consumers (peer-to-peer).

Consumers have insight into the origin of the purchased electricity via blockchain, can flexibly change suppliers, and compile their electricity mix right down to the generation plant. The electricity price is calculated automatically and in real time from current supply and demand. If the electricity supply lowers, the price rises immediately, creating incentives for expanding renewable energy. System failures are unlikely because it is operated not by a central instance but on many distributed nodes of a blockchain network.

Payments

Today

The banking industry is teeming with intermediaries responsible for processing payments between different parties. Banks execute payments on behalf of individuals and organizations, and transactions between banks are processed via the Swiss Interbanking Clearing System, which is operated by SIX. Credit card companies ensure people can make cashless payments at many merchants in Switzerland and abroad. A single credit card payment involves three entities that settle the payment between the buyer and the merchant.[50] Each of these entities wants to make money, and merchants and cardholders bear the cost of doing so. From a technical point of view, real-time transfers with countries like the U.S. are already possible. However, many regulations make international payments cumbersome, slow, and expensive. Banks that grant loans or manage investments also charge substantial fees. If the systems of a central intermediary fail, many services are no longer available.

Future

People can send money directly (peer-to-peer) from smartphone to smartphone via a digital wallet without intermediaries. The transfer is free of charge and works in real time, even across national borders. People can lend each other money 24/7 from anywhere in the world and freely negotiate the conditions of the loan. Investments in companies are no longer processed via service providers, but directly and without fees between the money lenders and the companies. Since everything is fully automated, costs are low, making it possible to invest in smaller companies that are not traded on the stock exchange. This is realized with legally secure, self-sovereign identities and the automation of payment and investment processes using blockchains and smart contracts. The system hardly ever fails because it is not operated by a central entity but in a distributed manner, collectively by many participants.

What is decentralized finance?

Decentralized finance (DeFi) is a blockchain system for managing digital assets that is operated without intermediaries (peer-to-peer). Almost all traditional banking services, such as account management, remittance, credit transactions, or securities trading, can be processed via the system. By using blockchain and eliminating intermediaries, the speed of the system increases, and costs decrease.[51]

Advantages and disadvantages of distributed value networks

If a digital application is no longer operated on the computer systems of a central instance but on the systems of several participants, availability, tamper resistance, and protection against cyber attacks increase. In distributed value networks, also decision-making authority is spread across many shoulders to prevent power concentration. Future distributed value network scenarios usually focus on advantages and disregard disadvantages. However, the concentration of decision-making power can also benefit certain decisions. Two examples are provided as follows:[52]

> Decisions that require a significant amount of expert knowledge and experience: This may be the case with decisions to invest in radical innovations whose long-term benefits are difficult to assess today.
> Decisions aimed at keeping an organization healthy in the long term but may have a negative effect on many in the short term: An automaker's decision to move entirely to e-mobility and mobility-as-a-service may be profitable for the organization in the long run. However, employees in the production of combustion engines would not necessarily support this decision.

The concentration of decision-making power aims to ensure consistency and predictability in organizations and systems. The focus shall lie on the organization's long-term health rather than individuals' benefits.[53] However, this increases dependence on leaders, and the potential for power abuse increases. For example, on large platforms with few alternatives, platform operators can dictate the terms of service. Large intermediary platforms such as Booking.com or Uber are frequently accused of exploiting their dominant position at the expense of hotels or taxi drivers.[54] Distributing decision-making powers among many network participants (for example, hotels or taxi associations) could be a remedy.

There is no universal answer to determine the to which extent strategic decision-making power should be concentrated or distributed. Democratic systems attempt to combine the advantages of distributed and concentrated decision-making: citizens elect their political representatives at regular intervals, delegating decision-making powers to them for a specified period. Through the separation of powers, different state organs exercise some control over each other. Similar systems also exist at the corporate level: In Swiss and German stock companies, boards of directors and supervisory boards supervise management, with both bodies being controlled by shareholders' general meetings. These are attempts to exploit the advantages of concentrated decision-making while at the same time preventing abuse of power through control mechanisms.

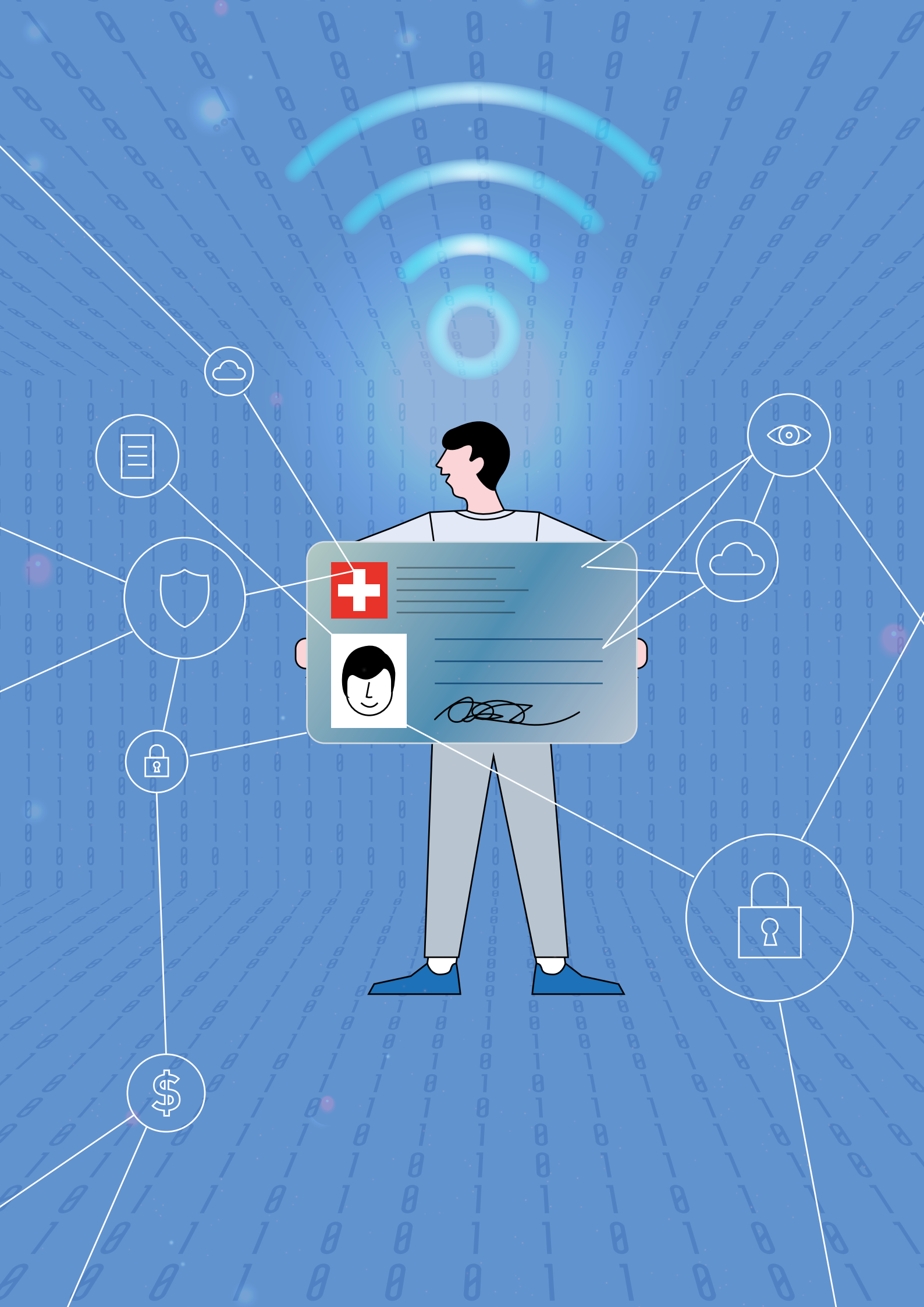
Blockchain and power concentration

Even if decision-making powers are distributed in the network, structures in or around the network that promote power concentration may evolve.

Bitcoin miners decide whether to accept a change by installing software updates. The changes it contains are accepted only if most miners install a particular software update. In principle, each miner can make their own decision. In practice, however, some have significantly more influence than others, because community acceptance of changes depends on the support of a Bitcoin elite. Most influence have core developers who review Bitcoin's code and large miners who provide much computing power to the blockchain network.[55] The 50 largest miners (0.1% of all miners) control about 50% of the computing power used for mining.[56] Several times in the past, Bitcoin's core developers have tried to convince large miners to support a particular update.[57]

Also, not all users of a digital service desire to participate in the provision of the service and be involved in all decisions. For many consumers, the availability of a trustworthy and user-friendly service is the most important factor. People are happy not to have to worry about technical issues. Private, for-profit companies have recognized this and provide services to simplify the use of blockchain applications, which can lead to power concentration. Coinbase, one of the largest cryptocurrency trading platforms, is a private for-profit company with a large impact on the cryptocurrency market. The so-called "Coinbase Effect" describes how the price of a cryptocurrency increases as soon as it is announced that it will become tradable on Coinbase. However, the effect seems to decrease as more cryptocurrencies are traded on Coinbase.[58] Still, a golden rule for many cryptocurrencies is, "Get listed on Coinbase, and your price will skyrocket."[59] Another example is the cryptocurrency trading platform FTX, which filed for bankruptcy in November 2022, triggering a drop in the value of many cryptocurrencies.[60]

To effectively prevent power concentration, it is necessary to distribute decision-making power across many organizations in overarching value networks that may consist of several blockchain applications. At the same time, incentive mechanisms must ensure that participants cooperate, even in conflicts of interest. Blockchain technology does not solve conflicts of interest per se. However, it is a vehicle that has triggered interest in distributed value networks in many sectors. Blockchain's technical characteristics—distributed operation, tamper-resistance, decision rules that can be fixed in smart contracts, and tokenization—are conducive to developing distributed governance structures. Many blockchain companies have already proven that the concentration of power can be prevented. In Tezos, any person or organization holding at least one token can participate in voting.[61] Sometimes, such systems use the number of tokens for weighting member votes, which can promote power concentration.



The potential of blockchain applications in detail

To identify the opportunities of using blockchain and the challenges of implementing blockchain projects, we examined three potential blockchain applications in more detail:

> Self-sovereign identities
> Distributed management of sensitive data using health data as an example
> Tracking and tracing of goods using pharmaceuticals as an example

For each of these applications, we describe the current status quo without using blockchain technology, develop a target picture of a potential blockchain solution, and identify opportunities, risks, and hurdles in implementation based on the literature and workshops with industry partners.

Self-sovereign identities

Status quo and challenges

Many interactions on the Internet require people to identify themselves using authentication techniques. Common techniques include usernames and passwords, biometric authentication (fingerprints, facial recognition), multi-factor authentication,[62] and online video identification.[63] In the wake of the COVID-19 pandemic, authentication via the Internet became even more important, for example, for opening an account via live video and photos of documents for identification.

Today, many people create several accounts for authentication on different websites. Storing personal data in all these systems is inefficient and creates security risks. In addition, many outsource identity management via the so-called social login to third parties, usually private companies. For example, Facebook, LinkedIn, and Google login are now often used for authentication on other websites. While this is a convenient alternative to creating many different logins, the practice raises privacy concerns because identity service providers can track where and when one logs into other services.[64] The case of Cambridge Analytica, which used personal data from Facebook to influence elections in the U.S. and the U.K., has vividly demonstrated the potential for the misuse of such data.[65]

In Switzerland, there have already been several attempts to create a more suitable system for identity management and authentication using electronic identities or e-IDs. SwissID, for example, is a Swiss Post system for electronic identification as well as the signing of documents. In March 2021, the Swiss electorate rejected a federal law on electronic identification services, mainly because they felt that private companies should not act as identity providers.[66] As a result, the Federal Council commissioned the development of a new law that would include the following principles:[67]

> Privacy by design: The system should ensure data protection.
> Data minimization: Data flows should be minimized.
> Distributed storage: Data should be stored in a decentralized manner.
> State identity provider: The identity issuing process and the operation of the infrastructure should be in state hands.

The subsequent consultation showed that a majority preferred the use of a self-sovereign identity (SSI) to implement the solution.[68] In addition, a majority demanded the so-called ambition level 3, in which both public and pri-

vate entities can issue e-IDs. This means that the state provides the infrastructure for e-IDs and uses it to issue state e-IDs (e.g., identity cards), but also allows others to use the infrastructure, for example, for training certificates, work certificates, employee, and member IDs.[69] A consultation on the e-ID Act has been underway since the end of June 2022.[70]

Target image

In contrast to the traditional identity paradigm with a central identity authority, SSI is a concept that allows individuals, organizations, or machines to digitally generate an e-ID and manage it themselves, usually in an SSI-enabled app, a "wallet," on the smartphone.

Issuers supply so-called verified credentials to credential holders (e.g., citizens), who store them in their wallets on their smartphone. In the case of identity cards or passports, the issuer would be the state; in the case of driver's licenses, the road traffic licensing authority; in the case of graduation certificates, the university; and in the case of personalized concert tickets, the point of sale or concert organizer. Holders transmit their credentials from their smartphone wallet to a verifying party (e.g., the police that checks a driver's license) via a secure channel. The verifier checks the authenticity of a credential with cryptographic proof stored in a register. The register is realized with blockchain to ensure data immutability and avoid a single point of failure.

"Using blockchain, we can create identification solutions for secure and trustworthy interaction in the digital world, even if we don't know our counterpart."

Orlando Hirt, Managing Director, OVD Kinegram

To ensure data minimization, citizens can always decide which data they share with verifiers. These "zero-knowledge proofs" also support data minimization. They guarantee that only the minimum information necessary for interaction is shared.[71] This is not possible with today's physical ID checks. For example, for age verification, one has to provide their entire ID, which includes additional information, such as one's name.

One advantage over conventional identity verification procedures is that verifiers do not have to ask the issuer of a credential directly whether it is genuine, but can verify authenticity independently via the register. As a result, neither an issuer nor a social network can find out via its social login service with whom credentials are shared. To ensure privacy by design, the register does not store the actual credential data, but only the cryptographic proofs ("hash values") to check the credential's authenticity. The credentials are stored exclusively on citizens' smartphones (off-chain) so that no one can access them without their knowledge. Specially protected areas on smartphones (secure elements) are used for this purpose; however, they are not yet available on all models.[72] When a credential loses its validity, it can also be stored in the register. Citizens can also generate credentials, for example, pseudonyms, for logging into streaming platforms.

SSI architecture

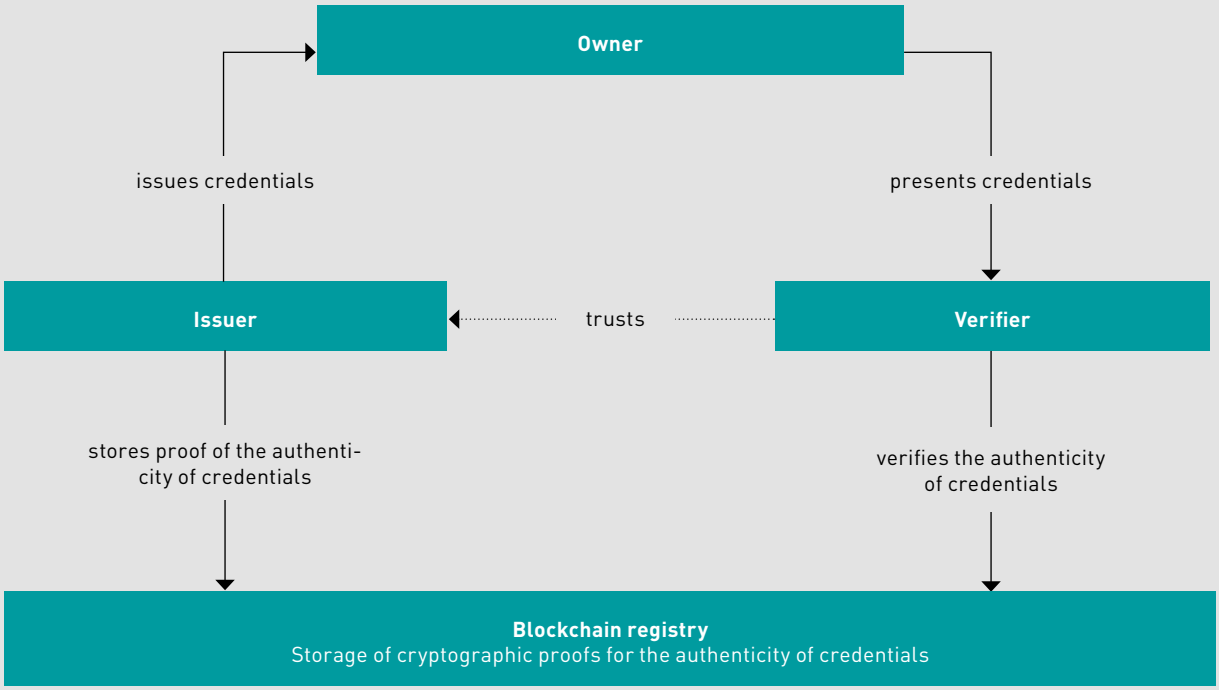


Figure 15: Based on Federal Office of Justice (2021).[73]

In principle, SSIs can be used to identify individuals, organizations, and machines, for example, for the Internet of Things (IoT). Figure 15 shows the basic architecture of the SSI. The solution could also be used in the physical world, for example, for access management of rooms without physical keys.

According to the Federal Office of Justice's Discussion paper on the target vision for an e-ID, the state would provide several functionalities:[74] an automated process for issuing e-IDs through the Swiss Identity Service, software for issuing and verifying state e-IDs and other credentials (Institutional agent), and a secure wallet for storing the credentials on citizens' smartphones. The state would also provide the distributed registry, an identity hub, to allow people to manage their identities (including backups), and an authentication service that state and private platforms can use as a login service.[75] The system should allow the minimal use case of issuing and verifying government e-IDs to be realized exclu-

SSI architecture based on the envisaged solution in Switzerland

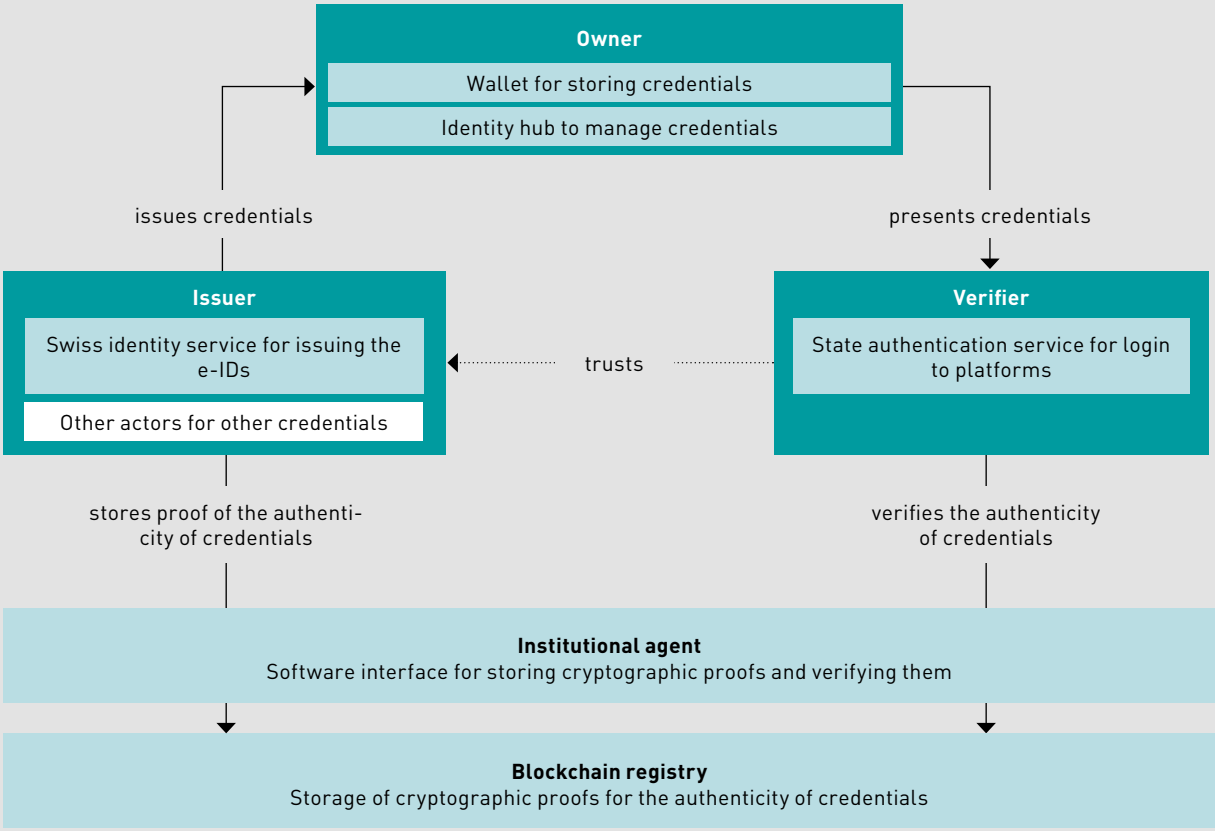


Figure 16: Based on Federal Office of Justice (2021).[76] The functionalities provided by the state are highlighted in light blue.

sively with government-provided components. Nevertheless, the goal is to open the system for use by other providers. Third-party applications also need to ensure accordance with principles such as data minimization or privacy by design. Figure 16 illustrates the functions that the state provides according to the target vision e-ID.

Opportunities

Our industry partners consider data protection and data security to be the main advantages of SSI. Citizens have full control over their credentials and can decide with whom they share them. As a result, less personal data resides in other companies' systems, reducing the risk of misuse. Hacker attacks on personal data become less attractive as the centralized storage of personal data diminishes. SSI can also be a means for raising awareness among the population on data protection. Today,

Processes and applications simplified or enabled by SSI

INDUSTRY	APPLICATION
Online services (for example, e-banking, e-commerce)	User-friendly and secure login to online services Faster onboarding of new customers including legitimation checks (know your customer) Secure online trading Secure peer-to-peer marketplaces without intermediaries
Health	Digital vaccination certificates Electronic health records E-prescriptions Online medical consultation
Transportation	Secure peer-to-peer marketplaces for car sharing and ride sharing Digital identification of vehicles for interaction with fuel or toll stations Digital driver's logbook
Buildings	Secure digital access control to buildings and rooms Secure property and room rentals
Travel and events	Contactless hotel check-in Faster check-in at airports Personalized event tickets
Public sector	E-voting Digital issuance of documents such as residence confirmation Faster admission of refugees

Table 3: Based on own research.

many citizens are still careless with their data, whether it is health data collected via health trackers by private companies or sensitive documents uploaded to a private provider's cloud. SSI could demonstrate that data-driven services can be delivered without giving private companies access to a lot of personal data. Finally, SSI could help close media disruptions. For example, certificates of residence or extracts from debt collection registers could be applied for and issued exclusively digitally.[77] Media disruptions may also be avoided when interacting with private companies, for example, during check-ins at airports.[78]

Table 3 shows an overview of existing processes and new applications simplified or made possible by a functioning SSI. Ultimately, the population's trust in digital services could grow if a distributed infrastructure is used to provide identity management without a private company controlling it. The disclosure of the open source code would further strengthen trust in the application.

Hurdles and risks

One key question concerns how decentralized an SSI can be if the state mainly provides the necessary infrastructure. On the one hand, this could pose the risk that citizens and companies do not fully trust the solution, leading to low adoption. On the other hand, the Swiss electorate rejected a solution coordinated by private identity providers. Thus, creating a distributed solution that is jointly controlled by the state and by private companies could be a suitable approach. DigitalSwitzerland, an association for digital innovation in Switzerland, also suggested this approach.[79]

To promote acceptance and trust in the technology, educational work on the functioning and security of SSI is also necessary. Suppose that the solution does not find broad acceptance. In that case, there is a risk that many incompatible identification solutions exist in parallel, impairing user friendliness. Developing an SSI solution also requires considerable cross-national coordination because regulations, e.g., data protection, are not yet compatible,[80] leading to questions about what data may be requested from users. Governance design also affects data security. The fewer actors involved in providing SSI, the likelier it is to create a single point of failure. For instance, a solution operated in Switzerland can fail due to Switzerland's telecommunications networks facing outages.

An SSI solution cannot fully guarantee data protection compliance. There is no way to control how organizations handle the information they receive through an SSI solution. One remedy to this problem is requiring credentials to be resubmitted for each transac-

tion. For example, driver's licenses could be resubmitted each time when booking a shared car instead of storing it in the driver's account. However, there is no technical way to guarantee that a provider does not save the license in secret.[81]

In addition, organizations may request significantly more personal information than they need. This is frequently the case today. For example, the Facebook Messenger app wants access to phone numbers, text messages, calls, and emails—all unnecessary information to provide the messenger service.[82] Finally, the possibilities for collecting data from citizens are increasing if more and more manual processes are digitized with the help of SSI. For example, if room access management by physical keys is replaced with SSI, the system could collect data about people entering the premises.

If the credentials are stored exclusively on citizens' smartphones, they would be lost if the smartphone is lost. Creating a backup in another location could negate the data protection benefits of SSI. Solutions to this problem are currently in development.[83]

Some industry partners expressed concerns regarding the performance of blockchains in terms of throughput, speed, and scalability. However, other study partners and the relevant technical literature consider this challenge to be solvable due to the continuous development of the technology. The decisive factor is the solution architecture.[84]

The Decentralized Identity Foundation and the World Wide Web Consortium are driving the development of global standards on the Internet for SSI.[85] The EU also develops an international SSI solution as part of the European Self-Sovereign Identity Framework.[86] IDUnion is an example of a distributed SSI solution involving more than 50 public and private players in German-speaking countries.[87] KILT is another private sector-driven project for SSI, in which the community—instead of intermediaries—decides how the solution works.[88]

Summary

SSI provides clear advantages over the authentication solutions commonly used today: citizens can manage their identities, control access to their personal data, and cannot have their behavior tracked by third parties. However, even with SSI, privacy principles could still be violated, as citizens cannot control what happens to their data once they share it. Companies may also continue to request and collect unnecessary amounts of data. Therefore, compliance with data protection principles must be ensured by technology and regulations (for example, through sanctions). Despite these challenges, a functioning SSI would significantly improve the current status quo and strengthen informational self-determination.

SSI is also an enabler of many new applications and business models, especially for peer-to-peer businesses. For example, secure and automated identification enables contracts for vehicle sharing to be concluded directly between renters and rentees, reducing dependence on platform operators who charge intermediary commissions. A working SSI could also be used in the physical world, for example, for access management to rooms without keys or security checks at airports without physical badges.

Central to successful SSI implementation is a solution architecture and governance structure that both companies and citizens trust and is internationally compatible. Since many are skeptical about SSI (or blockchain in general) and do not fully understand the technology, further education is needed. The consultation process initiated by the Swiss Federal Office of Justice assists in identifying a solution that is broadly accepted.

Use of blockchain in Estonia

Ten years ago, Estonia started using blockchain in e-government and e-health. Today, blockchain technology is used for managing ID documents, health data, electronic prescriptions, tax returns, or for electronic voting. Sensitive data is not stored directly on the blockchain but in government systems. However, blockchain helps ensure the data's integrity by making unauthorized changes very unlikely.

Public trust in digital technology is quite high in Estonia. The country was one of the first to introduce e-IDs around 20 years ago. Almost 50% of the population voted online in the 2021 local elections.[89] The canton of Jura in Switzerland has tested the Estonian blockchain solution to make digitally issued official documents tamper-resistant. Furthermore, it has been using blockchain for debt collection register extracts since February 2022.[90]

Distributed management of sensitive data using health data as an example

The amount of personal data collected and processed digitally is continuously increasing. Despite the revision of data protection laws in Switzerland and the EU, many citizens are concerned about the use of their data on the Internet. According to a survey conducted in Germany in 2021, concern about a lack of privacy was the second most important reason why people turned away from social networks.[91] This seems justified, as many online services had to pay hefty fines for violating privacy laws.[92] Blockchain can help strengthen the protection of sensitive data and informational self-determination. In the following section, we analyze this using the example of health data.

Status quo and challenges

Systems for the electronic and consolidated storage of health data—electronic health records (EHR)—are currently being developed in Switzerland and neighboring countries. According to the Swiss Data Protection Act, processing health data is subject to strict requirements because health data is personal data requiring special protection (sensitive data). For example, data collectors have to get explicit personal consent and inform data subjects about the collection, even if health data is gathered via third parties.[93]

Today, health data is usually stored in the systems of the institutions that collect it (for example, in doctors' offices or hospitals). As a result, different institutions record the same data multiple times. If data exchange takes

place, it is often not automated.[94] Due to the scattered, unlinked data silos, neither patients nor doctors have a complete view of patients' health histories, negatively impacting the quality of medical diagnosis and treatment.[95] Furthermore, there is a risk of data theft through cyber attacks if institutions do not adequately protect their systems. Stolen health data is big business on the darknet.[96]

The goal of the EHR is to solve these problems by centrally managing data. At its core is informational self-determination: an EHR can only be created with personal consent, patients have full control over their data and access to it, and every transaction must be recorded. Since healthcare is the responsibility of the cantons, with different requirements depending on the canton, Switzerland chose a decentralized EHR structure:[97] Technical-organizational associations of medical professionals can offer EHR systems that are audited by a certification body. As of November 2022, eight associations in Switzerland passed the audit, and about 13,000 EHRs were opened. The project is significantly behind schedule compared to the initial planning, mainly due to the complexity of the certification procedures.[98]

At the same time, several stakeholders in Switzerland are working on a value-based healthcare system. Today, billing for medical services is usually based on fixed-cost rates. The idea behind value-based healthcare systems is to link payments to actual improvements in health. Therefore, additional data on the health of individuals, even after treatment, is required. Further measures to increase efficiency in healthcare are preventive healthcare and encouraging patients to treat themselves if possible (self-care).[99] Finally, people increasingly use commercial mobile health services for healthcare monitoring and prevention. Many technology companies collect health data on a large scale with fitness and health apps. In a 2021 survey conducted in Switzerland, 36% of respondents said they used apps for fitness and exercise.[100]

By creating consolidated views on securely stored health data, an EHR not only improves medical treatment and diagnosis, but also supports the realization of a value-based and more preventive healthcare system. The health data stored in such a system would also be interesting for health research or other data-driven business models, such as insurance premium discounts for healthy lifestyles.

Target image

In the following, we illustrate one way to map the system described above using blockchain technology, taking into account current literature and our industry partners' opinions.[101]

All parties interact with the system through a front-end application that offers different functionalities, depending on their needs. When a healthcare provider generates new data about a person, they can add it to the patient's healthcare record, which is secured with blockchain with the patient's consent. However, the actual health data, such as lab results or X-rays, remain off-chain in the provider's database. In the blockchain itself, only metadata (references to the storage locations of the data), access permissions, and the hash value of the data are uploaded. This is necessary because personal data must be erasable according to data protection law (the "right to be forgotten"), which contradicts the immuta-

bility of data on blockchains. Instead of decentralized storage in healthcare providers' systems, data could also be stored in a central database operated by a trusted party. However, this has consequences for the data's availability, integrity, and confidentiality.[102]

"Many data silos exist in healthcare. Blockchain offers a way to manage them efficiently and securely, increasing the quality of diagnosis and treatment."

Dr. Daniel Heller, Chairman of the Board of Directors, Kantonsspital Baden AG

Patients can view their data and manage access permissions. Since they can also revoke access rights, this concept is called *dynamic consent*.[103] Patients receive notification for all new data processing or access requests and must give explicit consent. Smart contracts ensure compliance with access rights and automate data exchange. If, for example, an insurer wants to access the data, the smart contract automatically checks whether the insurer is authorized to do so. Only if this is the case is the data made available from off-chain storage. At the same time, data integrity is checked with the hash value. Incentive mechanisms, such as payments for the provision of data, for example, data donation for research purposes, could also be stored in smart contracts. Figure 17 shows the basic architecture of the system.

The unique identification of all parties involved in an EHR is also relevant for this use case but will not be discussed further here. In principle, blockchain offers possibilities for the unique identification of persons, organizations, and machines, as explained in more detail in the use case for self-sovereign identities.

Opportunities

According to the industry partners, combining off-chain storage of sensitive data with access management implemented via blockchain is a feasible and fundamentally suitable solution from a technical perspective. Since patients manage access to their sensitive data, the solution leads to more personal responsibility. The complete view of a person's health data, including all vaccinations and medications, has many advantages, for example:

> Improved diagnosis and therapy in practices and hospitals
> Higher-quality and tailored treatments for patients
> Development of new therapies and preventive measures in medical research
> Cost savings for insurers and insurees due to improved prevention and treatment

The regulation of access rights via smart contracts eliminates manual data exchange processes and avoids redundant data queries. Patients retain control over their data and manage access rights themselves. The manipulation of data is unlikely due to hash values. Cyber attacks on blockchains are unappealing because the data is distributed and not stored centrally. However, the data stored in the IT systems of the data creators (for example, in the practice or hospital) remain potentially vulnerable. Based on this system, a marketplace for health data could be created. Patients could offer their data anonymously to other organizations, such as research institutes, in return for a service.

Architecture of a system for the distributed management of health data

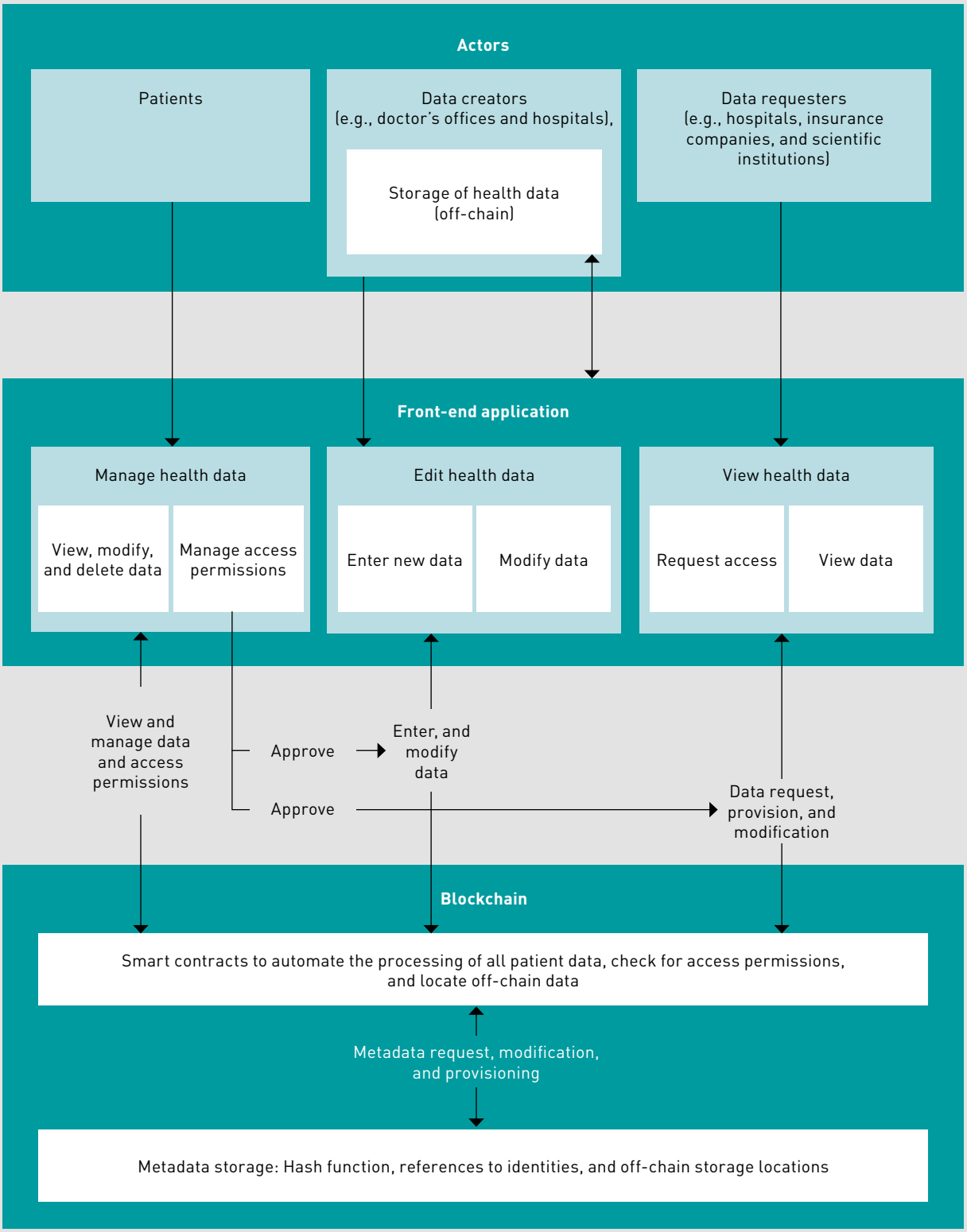


Figure 17: Own illustration.

Hurdles and risks

The hurdles identified here coincide considerably with the challenges of self-sovereign identities because both applications aim to store personal data in a confidential and tamper-resistant manner, and empower citizens to manage access to it. Thus, the creation of a system that patients and all other stakeholders in the healthcare system trust is challenging. Educational work is necessary to gain patients' trust, taking the privacy paradox into account. This states that most people are willing to share data despite major privacy concerns, for example, when using social media or health trackers. One explanation for the paradox is that people are more willing to put their worries aside and share information if they expect concrete added value for them. Therefore, when communicating an EHR solution, the focus should be on concrete benefits that can be realized quickly, such as the possibility of improved diagnosis or personalized recommendations. If communication emphasizes data protection issues instead, patients might become skeptical. Patients could also be incentivized through the financial benefits of sharing data. Health insurers already grant discounts when policyholders share specific health data with them.[104]

A similarly big challenge is to convince all stakeholders in the healthcare system of the EHR's value, i.e., providers (hospitals, doctors' offices, ancillary and nursing services, pharmacies, laboratories, and pharmaceutical companies), partners (technology companies, health insurers, and research institutions) and other stakeholders (Federal Office of Public Health, interest groups, etc.). Many stakeholders would need to invest in standardizing and adopting data exchange formats. Also, not all organizations might be willing to give up their sovereignty over collected patient data. If data control is entirely in patients' hands, they might also favor other institutions with data donations.

To address these issues, our industry partners believe that a governance structure that fosters collaborative control over the system is required. It must provide fairly-distributed incentives for all stakeholders. The governance structure also impacts the solution's acceptance. On one hand, distributed governance, where no party can individually control the system, can build trust because the parties can monitor each other, and manipulation becomes unlikely. On the other hand, patients may be more willing to trust a nameable organization. This is the case today, for example, with banks, which centrally manage and process their customers' financial data and transactions.

As with SSI, a challenge is that patients cannot control what happens to their data once they share it. For example, in the U.S., a menstrual cycle monitoring app sold personal data to Facebook.[105] In another case, GPS data of people who visited abortion clinics were sold online.[106] Even if this data is anonymized, individuals can often be identified by linking data from different data sets.[107] Cyber attacks are also possible, particularly if data requesters store received patient data on their systems. Data could be lost if off-chain systems that store patient data fail. Finally, smart contracts are binding in the legal sense according to the code-is-law principle, but liability and the possibility of legal action are unclear, which leads to uncertainty.

"Blockchain allows taking back control of sensitive health and financial data, strengthening citizens' informational self-determination."

Dr. Samyr Mezzour, Chief Innovation Officer, House of Insurtech Switzerland HITS

Summary

The question is not if but when and how a more suitable health data management system will be implemented. The status quo has many disadvantages:

> The fragmented storage of health data is inefficient.
> It does not enable patients to control their data.
> It prevents a complete view of a patient's health history, which affects the quality of diagnoses and therapies.

The main advantage of the blockchain solution described above is that it provides a consolidated view of health data and allows patients to control their data and access to it. Blockchain ensures that data cannot be manipulated by third parties unnoticed, and smart contracts allow for a high level of automation in data exchange. The solution would support the transition from institutional to patient-oriented data management in a continuum of care network—from prevention to early detection, therapy, and aftercare.[108]

However, we cannot blindly trust technology because what happens to data once it is shared cannot be controlled by technology. Other control mechanisms, such as audits, are required. In terms of implementation, the biggest challenge is to ensure that the multitude of different interests in the healthcare system can work together on a solution. Industry associations could provide support here. Only when all key stakeholders use the system can proper health data consolidation occur. Ultimately, trust in data security and user acceptance are also critical for patients to participate. Some partners suggested that an EHR solution should first be tested on a small scale to demonstrate the benefits to skeptical stakeholders.

Partial lack of trust in central instances, pressure to increase efficiency, changing customer needs, and data security are challenges in other industries. The financial industry is similarly regulated as the healthcare industry, with parallels in data protection concerns. Today, the custody and trading of assets is managed by intermediaries. With a distributed blockchain solution, traditional financial products, such as lending, can be managed autonomously via smart contracts. The hope of decentralized finance (DeFi) using blockchain technology is to make the financial system more trustworthy, efficient, cost-effective, and transparent.

Tracking and tracing of goods using pharmaceuticals as an example

Traceability in supply chains aims to create transparency about the origin, transfer, processing, and use of goods and information to monitor and optimize processes. Customers benefit from protection against counterfeiting, product safety, and transparency.[109] The need to clarify the origin of goods exists in many industries, such as food, luxury goods like watches, or raw materials like gold. Consumers today want to know where lithium in batteries comes from, and regulators want to know the carbon footprints of companies. Blockchain allows the mapping of physical products in the digital space and the creation of efficient systems for tracing and tracking goods without one player accumulating much market power. In the following, we explain this using the example of pharmaceuticals.

Status quo and challenges

GS1 is an international, private, non-profit standardization organization that provides systems for product traceability. According to its website, the GS1 system covers almost 100% of all pharmaceuticals approved in Switzerland.[110] The GS1 system defines number ranges that help to uniquely identify products, facilities, logistical units, and other objects. Manufacturers can create the numbers and attach them to the packaging of pharmaceuticals in the form of a two-dimensional barcode. Actors in the value chain scan the barcodes and add further information on process steps, such as transport or repackaging. When pharmacies or hospitals dispense drugs, they can trace their origins and ensure their genuineness. Once a drug is sold, this is noted in the GS1 system to ensure that the numbers cannot be copied and used for other product units. Seals on packages are used to prevent the illegal replacement of drugs. In principle, manufacturers could transmit incorrect data on the drugs produced to the GS1 system and instead package counterfeit products. However, this risk would be negligible for large manufacturers, as such an approach could cause considerable damage to their reputations if discovered. The Swiss Agency for Therapeutic Products (Swissmedic) and RefData, a database in which information on all approved pharmaceuticals is published, also use the national GS1 labeling system.

For data exchange between these actors, the Global Data Synchronization Network (GDSN) from GS1 can be used, which consists of 49 certified data pools (as of September 2022) and a global registry for connecting them.[111] When an actor performs a process step on items, the actor loads that information into one of the data pools. If an actor requests access to product data, it sends a request to a data pool. From there, a request is sent to the Global Registry to determine which data pool holds the data and to determine whether the requester is authorized to access the data. The GDSN uses a data model that divides products into categories and assigns attributes to each type. Figure 18 illustrates the current system.
According to GS1, one challenge of the current system is that smaller producers are not connected to the GS1 system because the effort to adopt the system is too high. In these cases, only the Swissmedic approval number is added to the products; this does not allow for monitoring of the origin. Also, not all hospitals are connected to the GS1 system, partly

System for tracking and the approval system for pharmaceuticals in Switzerland

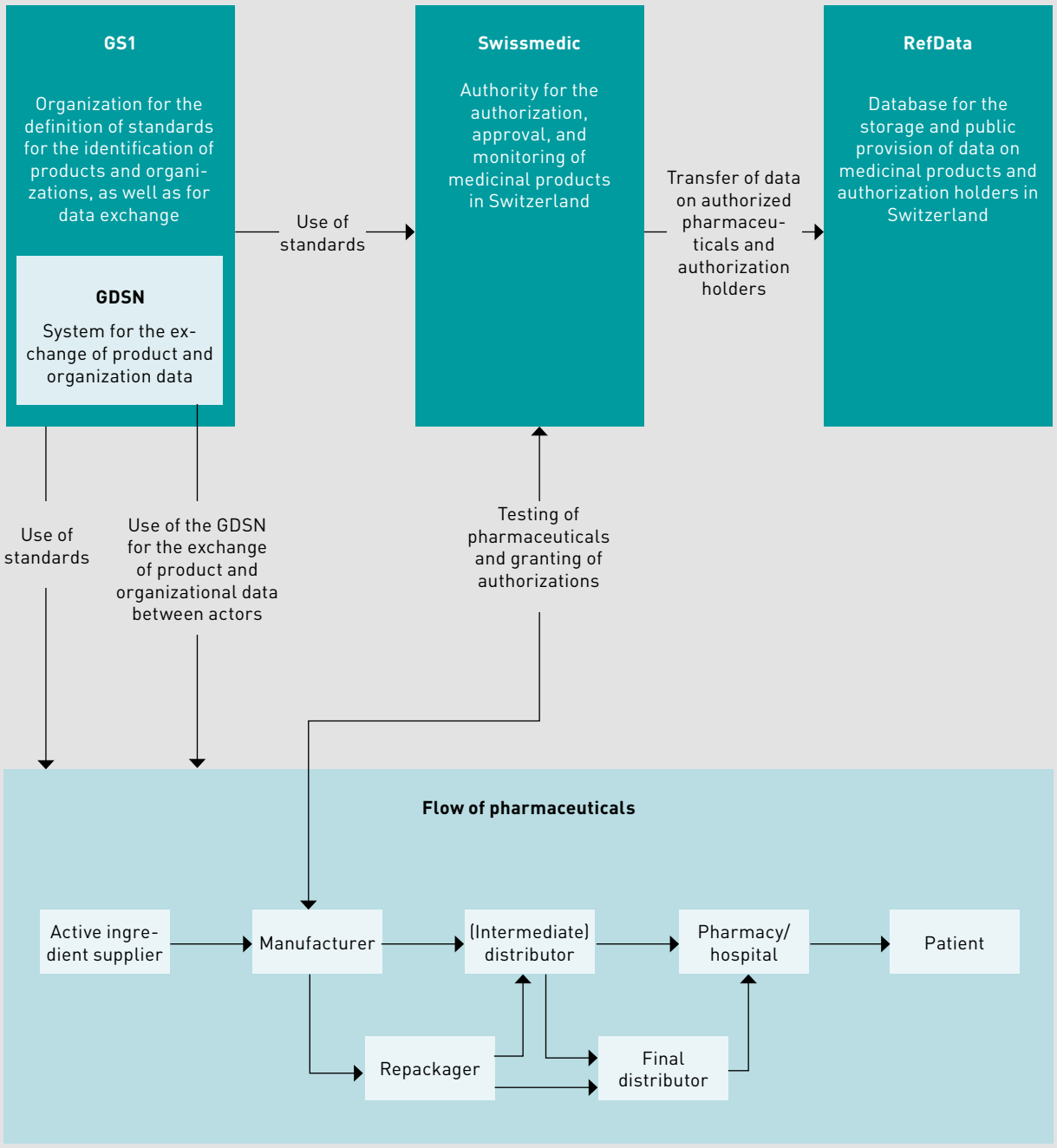


Figure 18: Own illustration based on the GS1 system.

because the GS1 system is not known everywhere, and the legislator has not defined a national standard for the traceability of pharmaceuticals. In addition, drugs are sold in Switzerland via the Internet by sales outlets that are not officially authorized. Counterfeits could also reach the market in this way.

According to some of our industry partners and a U.S. pilot project on drug traceability with blockchain, the system's response time is relatively long due to many (partly manual) interfaces.[112] This can be problematic in the case of product recalls. The current system also does not allow forward tracking, i.e., manufacturers cannot see their drugs' route to the dispensary and when they are dispensed.

Target image

Our target image illustrates one way to map the system described above using blockchain technology. We have taken inspiration from the U.S. pilot project FDA DSCSA Blockchain Interoperability Pilot by IBM, KPMG, Merck and Walmart.[113] Figure 19 illustrates the system.

Actors access the system via front-end applications. They can create product events, such as manufacturing, shipping, or dispensing a drug. They can also take measures to ensure product safety, such as checking the product's origin or initiating a recall. Via defined interfaces, the front-end application communicates with the back-end application, which writes the product and organizational data and retrieves them from a blockchain register. The back-end ensures that only authorized actors have access to the data and that only data in the correct format is written in the blockchain. The back-end can also connect to external systems for automated data exchange, such as the GS1 system or ERP systems.

There are two options for storing data: First, all data could be stored on a blockchain. The pilot project in the U.S. used this option. It has the advantage that all data is unchangeable. However, the disadvantages are that the data is stored redundantly on the systems of the data generators and the blockchain, the data cannot be deleted on the blockchain, and the data volumes stored in a blockchain can become very large. The data stored on a permissionless blockchain can also be viewed by all actors, which may lead to the disclosure of trade secrets, such as production volumes.[114]

Another option is to store only metadata about the products on the blockchain. These include references to the storage location of the data, the access conditions, and the hash value of the data. The actual data would remain off-chain in the data creator's database. When an actor requests data, the system checks access rights, retrieves the data from off-chain storage, and checks its integrity using the hash value. This solution has several advantages:

> Fewer data would need to be stored in the blockchain.
> The data stored off-chain would be erasable.
> The actual data would not be visible to all blockchain nodes.

Off-chain storage would be mandatory if personal data were ever to find its way into the system, because it must be erasable according to Swiss and European data protection laws.
Smart contracts can be used to automate further business processes. For example, if a product is damaged during transport, a reor-

der could be placed automatically, or a payment could be triggered automatically when a product is received. Access authorization to data could be controlled via smart contracts, as described in the previous use case. In addition, sensors can be connected to the system to upload product information to the blockchain automatically. For example, temperature sensors on product packaging could continuously measure ambient temperature to ensure that cold chains are maintained. If the temperature is above a critical value for too long, a smart contract could automatically mark the product as defective and remove it from the supply chain. The Swiss start-up Modum develops such solutions, and it was bought by the American company Roambee in 2021.[115] In general, the more data is written automatically to blockchains by machines instead of manually by humans, the lower the risk of data entry errors creeping in.

In the U.S. pilot project, a track and trace solution for pharmaceuticals was set up using a permissioned blockchain with three nodes—manufacturer, retailer, and dispensing point. According to the report, the project was successful. All product information could be stored in the system, actors' systems could be connected, and drugs could be traced by all actors and invalidated once dispensed.[116] In addition, the recalls were quickly communicated to the actors.

Opportunities

Workshop participants saw the most significant opportunities in the efficiency increase. These relate to the elimination or simplification of data interfaces, the immediate availability of information on pharmaceuticals, and the automation of process steps. According to the U.S. pilot project report, recall information can be sent to all relevant stakeholders in a maximum of 10 seconds. In contrast, today, this takes up to three days.[117] However, latency may increase as more actors use the system. In addition, tamper-resistance and, thus, data integrity increases, since it is unlikely that data change goes unnoticed. This improves counterfeit protection and increases product safety. Still, according to one partner, the solution is not a disruption (i.e., a fundamental change of processes, technologies, or business models), but an efficiency improvement of the existing (GS1/GDSN) system.

In the current system, all actors must at least trust GS1 and the data pools connected to the GDSN as they control the data exchange. If the blockchain solution were collaboratively operated and managed by a consortium of organizations along the supply chain, intermediaries' dependence on them could be reduced. This would also eliminate a single point of failure, as the system continues to run even if individual actors fail.

In principle, the solution offers the potential to automate even more process steps using smart contracts; for example, the automated processing of payments as soon as products have arrived or of reorders as soon as inventories run out. For this to work, however, other systems would have to be linked.

Hurdles and risks

In the workshop, partners raised concerns about the maturity and performance of blockchain technology. However, other partners involved in implementing blockchain projects have set them aside. Nevertheless, when developing solutions, developers must carefully

Architecture for a pharmaceutical tracking system using blockchain

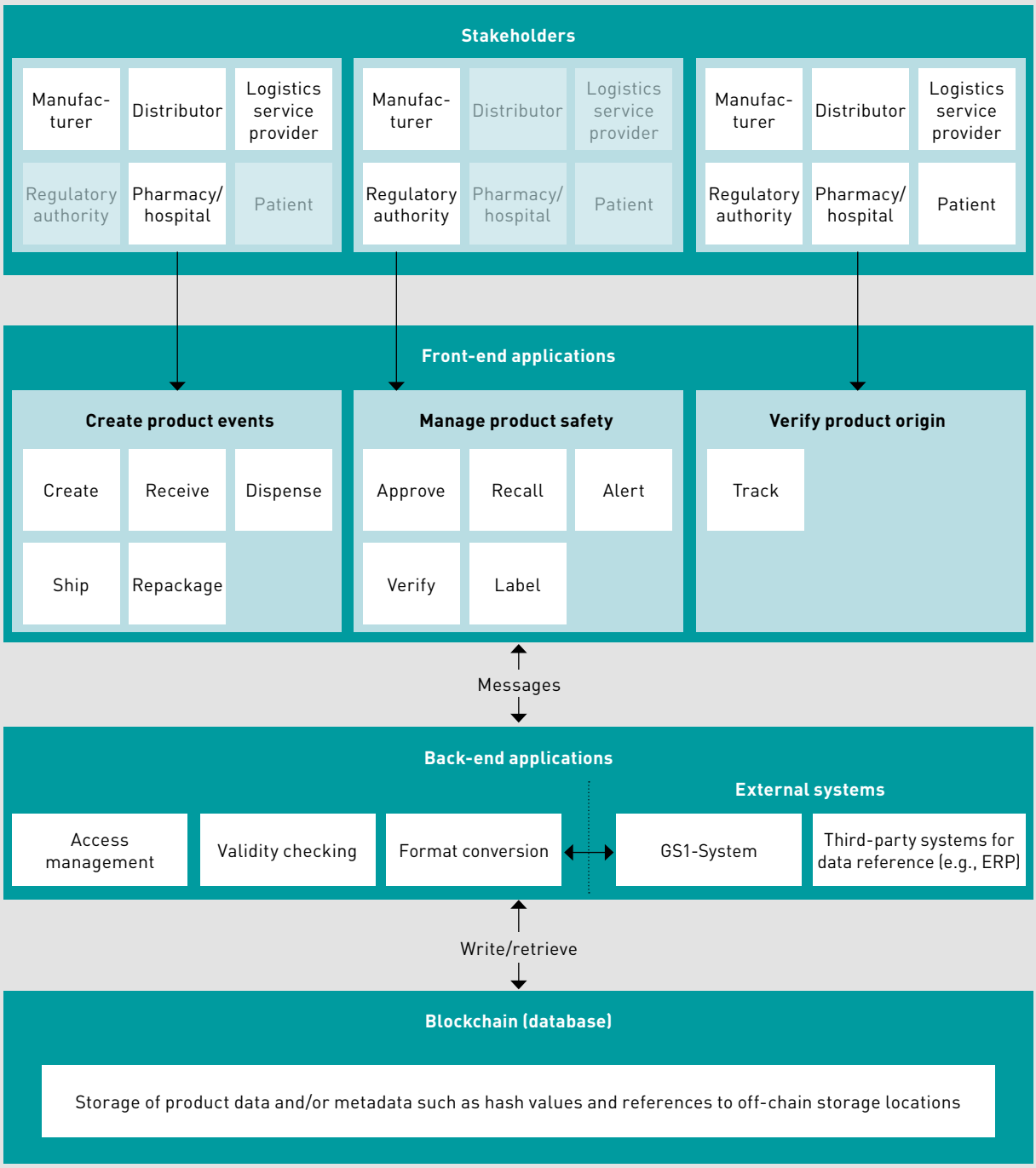


Figure 19: Own illustration.

select an architecture that enables sufficiently high performance in terms of speed, scalability, and throughput.[118]

The partners mentioned the diverging interests and motivations of the actors required for implementation as a core challenge. The current system works sufficiently well and requires high investments. Hence, there is no urge to change. Complicating matters further is the fact that drug supply chains are global: a large number of actors are involved, and many country-specific regulations must be considered. The system requires the development of precise data management and exchange standards, which is difficult given the complex requirements. Finally, the development of the solution and the necessary parallel operation of old and new systems generate high costs during the transition period. Efficiency gains can only be realized later, making it challenging to convince reluctant players. Industry partners proposed testing the solution on a small scale—in one country or for a specific drug. If the expected added values materialize, further players could be convinced, and the system could be scaled.

Widespread use of the system can only be achieved if a collaboration model ensures that the added value generated by the solution is distributed fairly among all partners. This includes off-chain collaboration, for example, for decision-making on system adjustments, and automated on-chain collaboration, for instance, regarding the definition of data interfaces or automated processes. GS1 has already established a collaboration model for many actors, which could be built upon.

If blockchains are designed to be permissionless, the anonymity of the actors could be preserved. However, less trusted actors could then gain access. Since all actors have insight into the transactions processed on permissionless blockchains, trade secrets such as production volumes or customer relationships could be disclosed.[119] There is also a risk that actors can be identified via transaction data, even if they are anonymized using public keys. Blockchain actors could use changing pseudonyms to make identification more difficult. With a permissioned blockchain, only approved actors can access the system. This would mean that their identities could be revealed in the approval process. However, this does not seem problematic since companies need to know their business partners.

Another challenge is that even blockchains cannot ensure that only correct data is stored. The so-called GIGO principle (garbage in, garbage out) also applies to blockchains. Therefore, many data collection and writing processes should be automated so that human errors can be avoided. Finally, the system would not prevent illegal sales of drugs over the Internet.

Summary

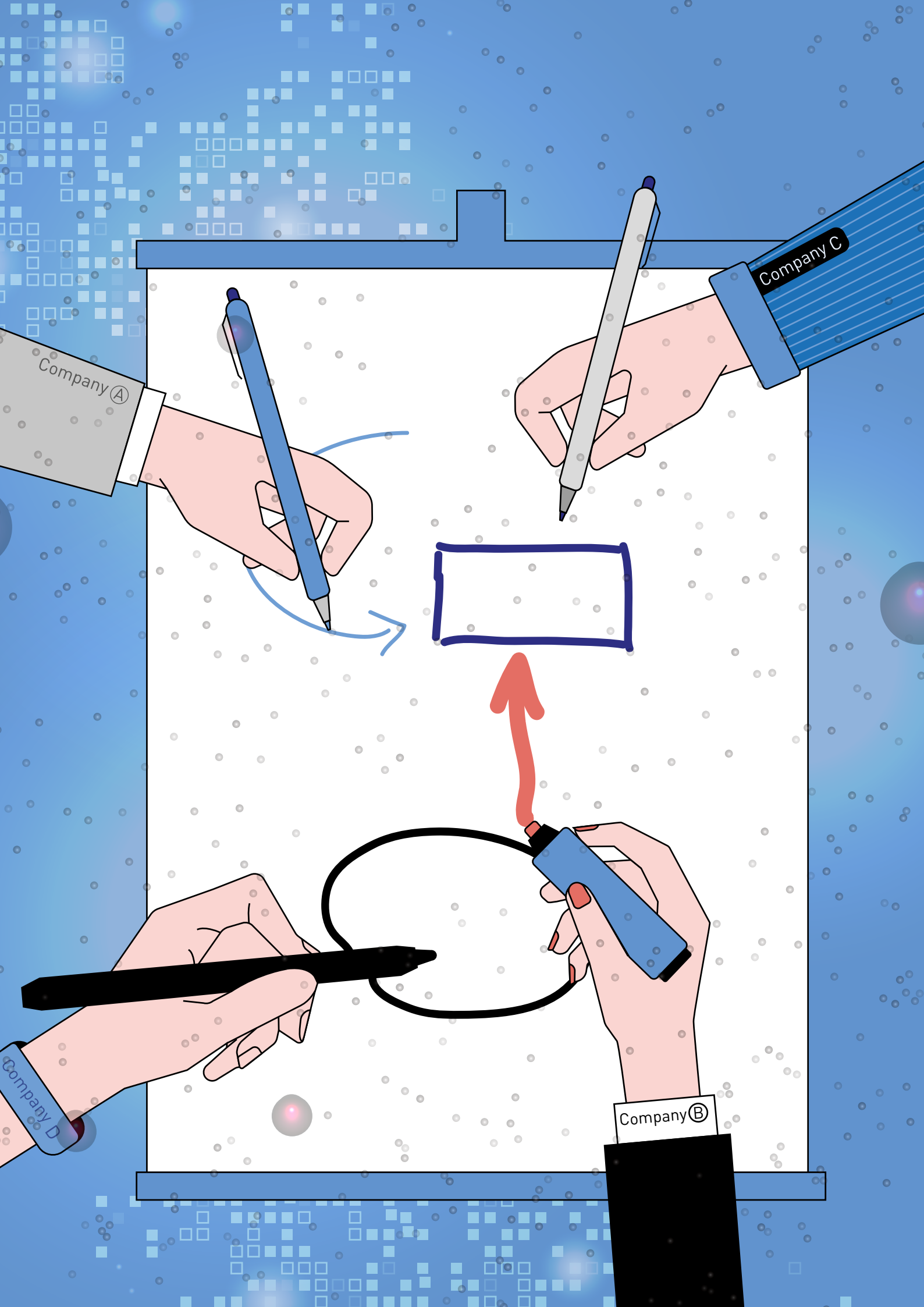
The blockchain solution described for tracking and tracing pharmaceuticals offers clear advantages over the current status quo: manual interfaces would be reduced, processes automated, data exchange accelerated, transparency, counterfeit protection, and product safety increased. The successful realization of such a system depends largely on the actors' will in the pharmaceutical supply chain. Negotiating a suitable collaboration model and agreeing on internationally compatible

standards will require an extensive amount of time and high costs. The systems in use today also took several decades to develop. GS1, for example, was founded as early as 1974. Because collaboration models in the pharmaceutical supply chain have already been developed for this system, it is advisable to build on it. At the same time, the need for change did not seem to be as high as for the other two applications discussed. The current GS1 system has the potential for improvement, but it works fundamentally.

"Blockchain technology, with its decentralized characteristics, is a good fit for a transparent and CO2-neutral energy system, where households and businesses increasingly produce, store and trade electricity themselves and want to know about its origin."

Markus Riner, Head Digitalization and IT,
Association of Swiss Electricity Companies VSE

Some of the weaknesses of today's system can also be solved without blockchain. These include the lack of forward tracking, the automation of reorders, and the elimination of manual interfaces. Nevertheless, blockchains offer a suitable basis for digitally mapping physical products and tracking their path along value chains efficiently and securely. This also provides benefits to other industries. For example, our industry experts find great potential in the energy industry. Blockchain can not only digitally map flows of physical products, but also of intangible goods such as electricity certificates.


Company Ⓐ
Company C
Company D
Company Ⓑ

Critical success factors of blockchain projects

We have identified critical success factors in the development and introduction of blockchain applications and clustered these in seven categories. We derived them from the analysis of the applications in the previous chapter and from the literature. Figure 20 illustrates all of the factors, which we explain in the following section. The appendix contains a detailed description of each factor.

Benefits and economic viability

Before starting a blockchain project, companies should conduct a business case analysis to determine whether the features of blockchain offer advantages over the status quo. The benefits realized through blockchain must significantly exceed the investment and operating costs, taking into account uncertainties and project risks. Stakeholders must fairly share the added value and costs generated by the solution. Successful implementation is only possible if all those who are essential for the solution's success are incentivized to support its development and use. Lastly, convincing stakeholders with high market power to participate in a solution can be difficult, because the introduction of a blockchain solution can reduce their influence.

Project design and implementation

Developing a blockchain solution and successfully establishing it in the market require many resources, coordination, and time. To ensure successful implementation, all significant stakeholders must have a shared project vision and realistic expectations regarding opportunities, risks, and project duration. An average of 25 months for enterprise blockchain projects elapses between the initial feasibility study and productive deployment.[120] The project must bear the necessary technical and professional knowledge and resources (time, money, employees) to realize the solution. Since blockchain remains a relatively young technology, is continuously being developed, and offers a good amount of design freedom, implementation should occur step by step. Interim results should be tested, and feedback should be collected and considered in the development. The solution should be scaled only after a successful pilot.

"Blockchain allows organizations to collaborate in new ways and develop new business models. However, the technology is only an enabler. The right incentive and governance mechanisms are important."

Daniel Rutishauser, Head of Blockchain, Inacta

Technical implementation

Blockchain offers many design options in technical implementation, such as access restrictions, consensus mechanisms, the number of nodes, the design of smart contracts, and combinations of on-chain and off-chain data storage. Therefore, it is important to precisely match the solution's architecture to the long-term requirements of the use case.

In addition, media disruptions and interfaces should be eliminated, processes automated, and manual steps avoided. Redundant data storage should also be eliminated if system availability is maintained. Since the electricity consumption of blockchains is very high in some cases, the added value generated by the solution must justify its electricity consumption. However, high electricity consumption is usually only a problem for permissionless blockchains that use the Proof of Work consensus mechanism.

Data quality and security

Blockchain technology makes it more challenging to alter data unnoticed. However, it cannot ensure that only the correct data is captured. Therefore, it is necessary to ensure technically and procedurally that the data written on blockchains is accurate and that human errors are avoided as far as possible, for example, by automating many data collection and writing processes.

Because data is stored in a distributed manner, blockchains tend to be less susceptible to cyber attacks than conventional solutions. Nevertheless, cyber attacks are possible if, for example, node systems are penetrated, or intruders gain access to private keys. It is possible to attack network members' systems after data have been imported from a blockchain or if data is stored off-chain. Therefore, it is necessary to protect blockchains, node systems, and their private keys.

Off-chain governance structures can impact data privacy. For example, new members of permissioned blockchains must be approved. Admission processes may expose their identities. Aggarwal and Kumar (2020) discuss other possible attacks on blockchains and protection mechanisms against them.[121]

Governance

Effective governance mechanisms ensure that all stakeholders learn about recent updates and decisions relevant to them through appropriate channels, have the opportunity to contribute and discuss proposals, and are appropriately involved in decision-making processes. In addition, data models and interfaces must be standardized for cross-organizational data exchange. Governance mechanisms also define procedures for dealing with conflicts between participants or unfair behavior by individuals. The development of suitable governance structures is even more challenging the more stakeholders are involved, the more diverse their interests are, and the less they trust each other.

Trust and acceptance

Blockchain is associated with the myth that it makes trust unnecessary, because it makes it difficult for members to change data without being noticed. This is particularly advantageous for peer-to-peer transactions, because no intermediary has to ensure the partners' trustworthiness and the transaction's legality and security. Today, for example, Airbnb provides this service for overnight stays in private homes, and users pay a premium for it. The premium could be reduced if parts of this service are automated by blockchain.

Nevertheless, a lot of trust is necessary for successfully establishing a blockchain solution. The partners involved in the project must be willing to work together and trust each other and the technology. For successful scaling, the target group of the solution must also trust the technologies and providers. For example, if patients distrust an electronic health record provider, they will not share their health data, no matter how good the technology is.

Only if a sufficient number of the target group uses the system can the parallel operation of several solutions be avoided and the expected efficiency potentials be leveraged. Marketing and communication play a decisive role in the acceptance of the solution. For example, the participating organizations can form a

Critical success factors of blockchain projects

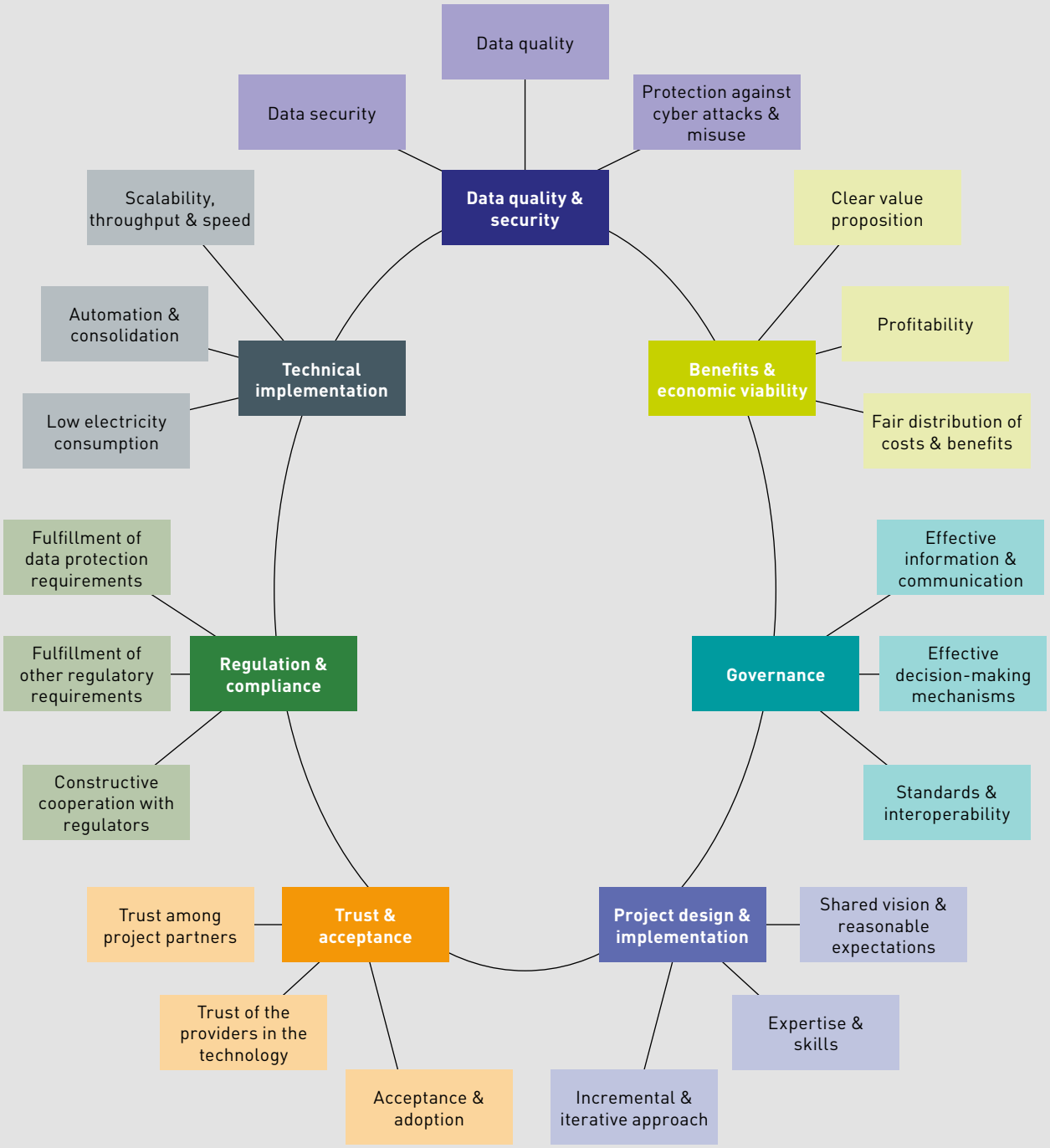


Figure 20: Based on own research.

consortium and appear on the market as a new entity with a new brand, disguising their identities.

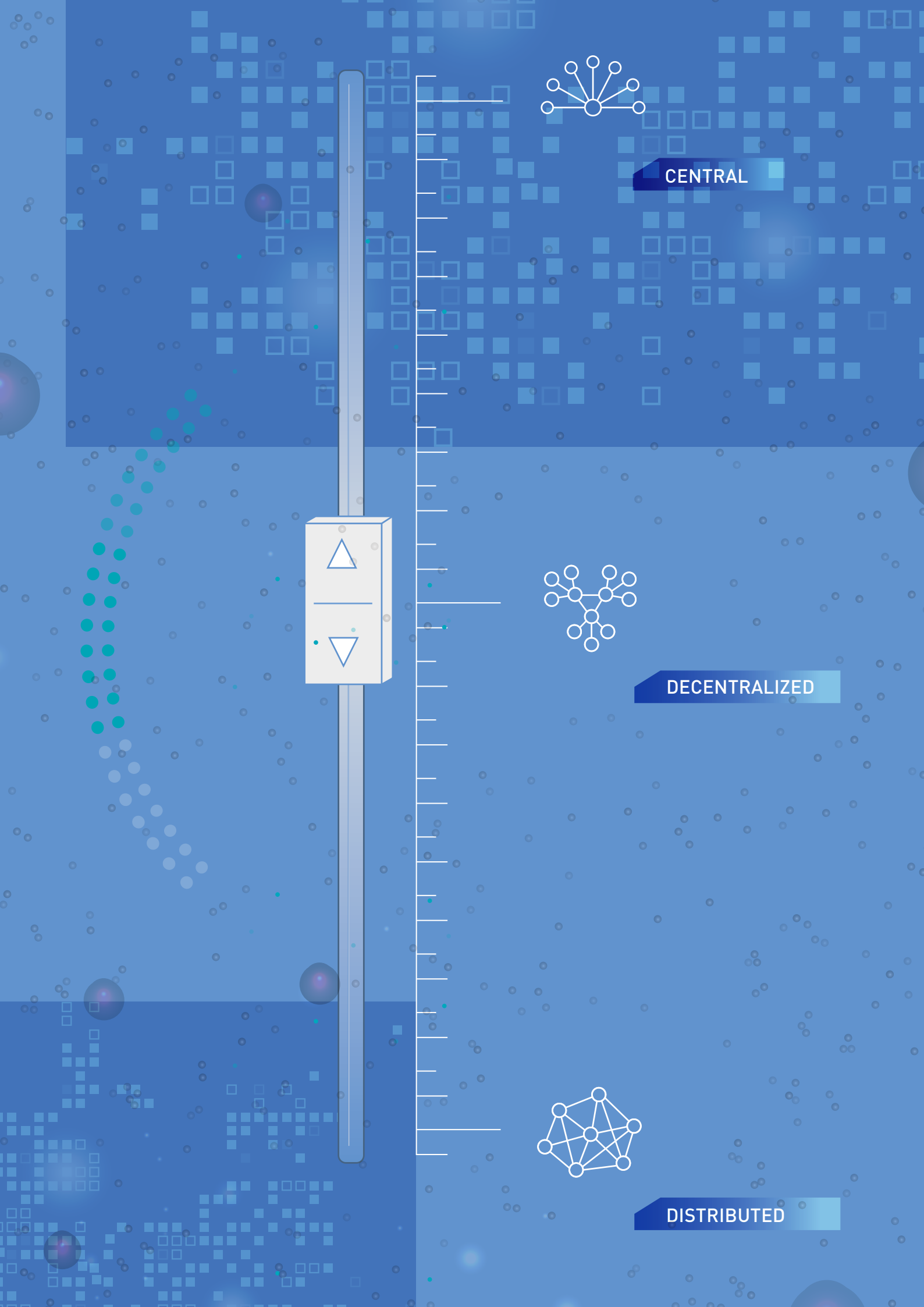
To gain broad acceptance, communication should focus on tangible user benefits. Putting too much emphasis on data protection or security in marketing might trigger skepticism and mistrust. According to Liudmila Zavolokina, a business informatics scientist at the University of Zurich, a "blockchain must do what is expected of it, and its mechanisms and objectives must be clear."[122]

Regulation and compliance

Since blockchains facilitate the cross-organizational exchange of—often personal and sensitive—data, it is imperative to ensure that data protection requirements are met. According to Swiss data protection laws, personal data must always be erasable. Thus, personal data must never be stored on the blockchain itself but only in off-chain storage.

Since data protection regulations differ across countries, data protection is a major challenge. Technical systems should ensure compliance as much as possible. However, technology alone can never do this entirely, which is why additional control mechanisms, such as audits, are necessary. For example, actors who received data via blockchain could store it in their own system and use it for other purposes unnoticed. Furthermore, there may be other regulatory requirements. For example, the Markets in Financial Instruments Directive and the Basel IV regulations govern special requirements for financial data.[123]

Because the many legal aspects of the use of blockchains are still unresolved, constructive cooperation with regulators is essential. Above all, accountability in liability cases must be regulated. These questions are not easy to answer in distributed organizations without a central authority. However, their clarification is essential for creating trust in blockchain solutions and their providers.[124]


CENTRAL
DECENTRALIZED
DISTRIBUTED

Is the future distributed?

As digitalization advances, the availability, integrity, and security of digital infrastructures are becoming increasingly crucial for the economy and our everyday lives. Blockchain allows the creation of more robust and efficient digital infrastructures. On a technical level, blockchain can ensure that systems are always available and protected against manipulation. Valuable assets, such as money, gold, patents, or works of art, can be digitally mapped and traded using tokens, and processes can be automated using smart contracts. This potential exists in the digital world and in value networks for physical products, which can be managed more efficiently and securely with blockchains. Once processes are digitized in a tamper-resistant way using blockchains, many new applications and business areas can open. For example, electronic identities based on blockchain technology allow us to securely identify people, organizations, and objects in the digital world. This strengthens privacy on the Internet and enables new applications, such as access management to buildings and rooms without physical keys, peer-to-peer marketplaces, or a robust Internet of Things (IoT) infrastructure.

Blockchain's properties also provide a suitable technological foundation for a shift to distributed value networks. In a collaborative, self-regulating value network, blockchain technology supports all participants in interacting and controlling each other efficiently and securely without the need for a central authority. However, this transformation is not only a technological but also a social process with many conflicts of interest to overcome. Especially in the case of established applications, it can be challenging to dissolve existing structures. However, new applications can be planned right from the start so that only a few dependencies arise.

The key challenges to implementing blockchain projects include establishing suitable governance structures, eliminating regulatory ambiguities, ensuring data quality and security (on blockchains and in adjacent systems), and creating trust and acceptance in a blockchain solution. Should we be able to conquer these challenges, we can create secure and efficient digital and physical value-creation processes and increase trust in digital infrastructures.

Because blockchain is continuously advancing, we can only speculate about its long-term impact. One thing is sure, however: the properties of blockchain—tamper resistance, availability, efficient data exchange, decision rules that can be fixed in smart contracts, or value trading with tokens—offer a suitable technical basis for creating efficient and robust digital infrastructures.

Acknowledgements

We thank all partners for their support and cooperation in the preparation of this study. We thank Dr. Ralf Grötker for methodological support, Karola Klatt for editing, Maja Kunze for proofreading the German version of this report, and the reviewer from Scribendi for editing the English version of the report. In addition, we thank Anne van Berkel Meier, Dr. Roger Heines, Prof. Dr. Burkhard Stiller, Dr. Liudmila Zavolokina, and Dr. Rafael Ziolkowski for reviewing parts of the paper and providing their expertise. Special thanks go out to Mathias Ruch and Dr. Pascal Ihle for integrating our study into the Open Ideation phase of the NTN Innovation Booster Blockchain Nation Switzerland (Innosuisse), to André Kudelski for the foreword, and to Dr. Daniel Heller for political support.

Appendix

Study partners

UNTERNEHMEN	KONTAKT
aXedras	Urs Röösli (CEO) Kathrin Wolff Schmandt (Senior Advisor)
Blockchain Nation Switzerland	Dr. Pascal Ihle (CEO)
Swiss Federal Office of Energy	Dr. Matthias Galus (Head Digital Innovation Office)
EcosystemPartners	Dr. Daniel Fasnacht (CEO)
Generali (House of Insurtech Switzerland HITS)	Pietro Carnevale (CEO) Dr. Samyr Mezzour (CIO)
Green	Miki Mitric (Head of Business Development) Roger Süess (CEO)
Inacta	Daniel Rutishauser (Head DLT & Financial Services)
Kantonsspital Baden	Maximilian Grimm (Innovation Manager) Dr. Daniel Heller (Präsident des Verwaltungsrates)
Novartis	Marco Cuomo (Manager Applied Technology), Daniel Fritz (Domain Architect Supply Chain)
OVD Kinegram	Patrick Brouwer (Program Manager Digital Solutions) Orlando Hirt (Managing Director)
sminds/N9 House of Innovation	Sandro Schmid (CEO) Jacqueline Schleier (Member of the Executive Board)
Association of Swiss Electricity Companies VSE	Markus Riner (Head Digitalization & IT)

Table 4.

Critical success factors of blockchain projects in detail

CATEGORY	SUCCESS FACTOR	DESCRIPTION
Benefits and economic viability	Clear value proposition	The features of blockchain must help overcome challenges and problems that exist in the status quo (e.g., high intermediary costs and cross-organizational data exchange). The benefits to be realized through blockchain must be clear and relevant for all stakeholders.
	Profitability	The benefits to be realized through the use of blockchain must significantly exceed the investment and operating costs, even taking into account uncertainties and project risks.
	Fair distribution of costs and benefits	Stakeholders must fairly share the added value and costs generated by the solution. All stakeholders essential to the solution's success must be incentivized to support its development and use.
Governance	Effective information and communication	All stakeholders must be informed about developments and decisions relevant to them through appropriate channels and have the opportunity to contribute and discuss proposals.
	Effective decision-making mechanisms	The collaboration model (on-chain and off-chain) must involve all partners appropriately in decision-making according to their roles.
	Standards and interoperability	Data models and interfaces must be standardized for cross-organizational data exchange.
Project design and implementation	Shared vision and reasonable expectations	Stakeholders must have a shared project vision and realistic expectations regarding opportunities, risks, and duration.
	Expertise and skills	The project must bear the technical and professional knowledge and resources (time, money, employees) required to realize the solution.
	Incremental and iterative approach	Since blockchain offers many design options, the implementation should occur step by step. Interim results should be tested and feedback should be received in the development stage. The solution should be scaled only after a successful pilot.
Trust and acceptance	Trust among project partners	The partners involved in the project must be willing to work together and fundamentally trust each other.
	Trust of the providers in the technology	The partners involved in the project must trust the technologies.
	Acceptance and adoption	The parallel operation of several solutions can only be avoided—and the expected efficiency potentials realized—if a sufficient number of the target group use the system. Therefore, the target audience must trust the technology and the providers. Marketing and communication are crucial for the acceptance of a solution.

CATEGORY	SUCCESS FACTOR	DESCRIPTION
Regulation and compliance	Fulfillment of data protection requirements	The data protection laws of all countries involved must be met. The technology and processes should ensure this. Additional control mechanisms, such as audits, may be required.
	Fulfillment of other regulatory requirements	The regulatory requirements of all countries involved, such as special requirements for handling financial data, must be met.
	Constructive cooperation with regulators	Since many legal aspects of blockchain use are still unresolved, constructive cooperation with regulators is necessary.
Data quality and security	Data security	Access management must ensure that only authorized persons have access to the data, that the data is always available when access is needed, and that data, once stored, is complete and unchanged.
	Data quality	At the technical and process level, it is important to ensure that only correct data is written to blockchains and that human error is avoided to the greatest extent possible.
	Protection against cyber attacks and misuse	The solution needs to be equally or less vulnerable to cyber attacks than conventional solutions. Data misuse must be ruled out as much as possible, both technically and through control mechanisms.
Technical implementation	Scalability, throughput and speed	The technical architecture of the solution enables access for a sufficient large number of users. A sufficient number of transactions can be carried out simultaneously (transactions per unit of time) at a sufficiently high speed (latency).
	Automation and consolidation	The technical architecture of the solution ensures that as many media breaks and interfaces as possible are eliminated, processes are automated, and manual steps are avoided. Redundant data storage is eliminated if system availability is not negatively impacted.
	Low electricity consumption	The added value generated by the solution must justify its electricity consumption.

Table 5: Based on own research.

Bibliography

[1] Brooker, K. (2018): "I was devastated": Tim Berners-Lee, the man who created the world wide web, has some regrets. Vanity Fair, 08/2018. https://www.vanityfair.com/news/2018/07/the-man-who-created-the-world-wide-web-has-some-regrets

[2] Kaat, C. (2022): Wo Schweizer Firmen auf dem Weg zum data-driven Business stehen [Where Swiss companies stand on the way to data-driven business]. IT Markt. https://www.it-markt.ch/storys/2022-05-11/wo-schweizer-firmen-auf-dem-weg-zum-data-driven-business-stehen (retrieved: 18.10.2022)

[3] Ryf, S.; Siegenthaler, P.; Fasnacht, D.; Fichter, C. (2022): NZZ-KMU-Barometer: Lieferkettenprobleme und Fachkräftemangel – die Zukunftsaussichten von Schweizer Unternehmen verdüstern sich [NZZ SME Barometer: Supply chain problems and skills shortages - the future prospects of Swiss companies are darkening]. https://www.kalaidos-fh.ch/-/media/KFH2019/Dokumente/News/2022/Wirtschaft/Ergebnisbericht-NZZ-KMU-Barometer-2022.pdf (retrieved 18.10.2022)

[4] Statcounter (n. d.): Search Engine Market Share Worldwide. https://gs.statcounter.com/search-engine-market-share (retrieved: 18.10.2022); Primary source not accessible. Cited from: Statista (2022): Most popular global mobile messenger apps as of January 2022, based on number of monthly active users. https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (retrieved: 18.10.2022)

[5] Watson (2019): Schweizweite Störung im elektronischen Zahlungsverkehr [Switzerland-wide disruption in electronic payment transactions]. https://www.watson.ch/schweiz/wirtschaft/425414560-bezahlung-mit-ec-karten-wegen-stoerung-schweizweit-ausgefallen (retrieved: 18.10.2022); Thomi, S. (2022): Mitten im Samstagseinkauf: Störungen bei Twint, Postfinance und weiteren Banken [In the middle of Saturday shopping: disruptions at Twint, Postfinance and other banks]. Luzerner Zeitung. https://www.luzernerzeitung.ch/news-service/wirtschaft/online-zahlungsmittel-mitten-im-samstagseinkauf-stoerung-bei-twint-app-postfinance-und-visa-ld.2300310 (retrieved: 18.10.2022)

[6] Wingeier, C. (2022): Hackerangriff auf Schweizer Spitalverband [Hacker attack on Swiss hospital association]. Inside IT. https://www.inside-it.ch/hackerangriff-auf-schweizer-spitalverband-20220621 (retrieved: 21.10.2022)

[7] Baran, P. (1962): On Distributed Communications Networks. RAND Corporation, California, USA.

[8] Laudon, K.; Laudon, J. (2019): Management Information Systems: Managing the Digital Firm. 16th edition. Pearson.

[9] Rauchs, M.; Blandine, A.; Bear, K.; McKeon, S. (2019): 2nd global enterprise blockchain benchmarking study. University of Cambridge, Invesco.

[10] Ibit 9

[11] Hileman, G; Rauchs, M. (2017): Global Blockchain Benchmarking Study. University of Cambridge, Visa, EY.

[12] Based on: Ibit 9

[13] Schmitz, P. (2019): Was ist ein Token [What is a token]? Blockchain Insider. https://www.blockchain-insider.de/was-ist-ein-token-a-854928/ (retrieved: 18.10.2022); Schiller, K. (2022): Was sind Security Token? – Die Vor- und Nachteile [What are security tokens? – The advantages and disadvantages]. https://blockchainwelt.de/security-token/ (retrieved: 24.10.2022); Schiller, K. (2022): Was ist ein Utility Token? Beispiele und Erklärung [What is a utility token? Examples and explanation]. https://blockchainwelt.de/utility-token/ (retrieved: 24.10.2022). Schiller, K. (2022): [Equity Token und ETO: Was können sie wirklich (Equity Token and ETO: What they really can do]?[https://blockchainwelt.de/equity-token-eto/ (retrieved: 24.10.2022).

[14] Lu, M. (2022): Blockchain Applications: Tokenization of Real Assets. Visual Capitalist. https://www.visualcapitalist.com/sp/blockchain-applications-tokenization-of-real-assets/ (retrieved: 18.10.2022)

[15] Ibit 11

[16] Ibit 11

[17] CoinMarketCap (n. d.): Today's Cryptocurrency Prices by Market Cap. https://coinmarketcap.com/?page=95 (retrieved: 18.10.2022)

[18] Martin, W. (2017): There's a 'fatal' flaw in cryptocurrencies which means they can never be real currencies. Insider. https://www.insider.com/bitcoin-cryptocurrency-ubs-wealth-management-economist-paul-donovan-2017-11 (retrieved: 26.10.2022)

[19] Primary source not accessible. Cited from: Dailey, N. (2022): NFTs ballooned to a $41 billion market in 2021 and are catching up to the total size of the global fine art market. https://markets.businessinsider.com/news/currencies/nft-market-41-billion-nearing-fine-art-market-size-2022-1 (retrieved: 10.1.2023)

[20] Gerbl, E. (2021): Fälscher-Ikone Wolfgang Beltracchi malt jetzt digital [Forger icon Wolfgang Beltracchi now paints digitally]. Bilanz. https://www.handelszeitung.ch/bilanz/falscher-ikone-wolfgang-beltracchi-malt-jetzt-digital (retrieved: 18.10.2022)

[21] Barrera, C. (2019): A Framework for Blockchain Governance Design: The Prysm Group Wheel. Prysm Group on Medium. https://medium.com/prysmeconomics/a-framework-for-blockchain-governance-design-the-prysm-group-wheel-703279c1b0dd (retrieved: 18.10.2022)

[22] Watson Law (n. d.): Blockchain governance: what is it, what types are there and how does it work in practice?. https://watsonlaw.nl/blockchain-governance-what-is-it-what-types-are-there-and-how-does-it-work-in-practice/#:~:text=In%20the%20context%20of%20blockchain,into%20question%20contemporary%20authority%20structures (retrieved: 18.10.2022)

[23] Ibit 11

[24] Decred Project (n. d.): Introduction to Decred Governance. https://docs.decred.org/governance/overview/ (retrieved: 18.10.2022)

[25] Bocksch, R. (2022): Bitcoins Stromverbrauch übertrifft den der Ukraine [Bitcoin's electricity consumption exceeds Ukraine's]. Statista. https://de.statista.com/infografik/18608/stromverbrauch-ausgewaehlter-laender-im-vergleich-mit-dem-des-bitcoins/ (retrieved: 18.10.2022)

[26] Finews (2022): The Merge: Ethereum 2.0 ist geboren [The Merge: Ethereum 2.0 is born]. https://www.finews.ch/news/finanzplatz/53360-the-merge-eth-ethereum-bitcoin-umstellung-proof-of-stake-vitalik-buterin (retrieved: 18.10.2022)

[27] Heines, R. Gürpinar, T. (2021): Towards a typology of blockchain-based applications: a conceptualization from a business perspective. Konferenzband zum Scientific Track der Blockchain Autumn School 2021, Hochschule Mittweida, 92-101. https://doi.org/10.48446/opus-13082

[28] Meunier, S. (2016): When do you need blockchain? Decision models. Medium. https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1 (retrieved: 18.10.2022)

[29] Ibit 28

[30] Schlatt, V.; Schweizer, A.; Urbach, N.; Fridgen, G. (2016): Blockchain: Grundlagen, Anwendungen und Potenziale. Fraunhofer-Instituts für Angewandte Informationstechnik FIT.

[31] Ibit 30

[32] Ibit 9

[33] Schweiger, L. (2021): 81 of the Top 100 Public Companies are using blockchain technology. Blockdata. https://www.blockdata.tech/blog/general/81-of-the-top-100-public-companies-are-using-blockchain-technology (retrieved: 18.10.2022)

[34] Ibit 9

[35] CBInsights (2022): Banking is only the beginning: 65 big industries blockchain could transform. (retrieved: 18.10.2022)

[36] Bijkerk, M. (2022): Blockchain Venture Funding per Country. Blockdata. https://www.blockdata.tech/blog/general/blockchain-venture-funding-per-country (retrieved: 18.10.2022)

[37] Ibit 33

[38] Koopman, M. (2018): Blockchain in Switzerland: Opportunities for future cooperation between Switzerland and the Netherlands. Kingdom of the Netherlands.

[39] Finma (2018): Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs). https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?sc_lang=en

[40] State Secretariat for International Finance SIF (2022): Blockchain / DLT. https://www.sif.admin.ch/sif/de/home/finanzmarktpolitik/digit_finanzsektor/blockchain.html#:~:text=Die%20Schweiz%20hat%20am%201,die%20Integrit%C3%A4t%20des%20Finanzplatzes%20zentral (retrieved: 18.10.2022)

[41] CoinDesk & MIT (2022): Best Universities for Blockchain 2022. https://www.coindesk.com/layer2/2022/09/26/best-universities-for-blockchain-2022 (aufgerufen 18.10.2022)

[42] Blockdata (2021): Blockchain & Crypto in 2021 - A review in data. https://www.blockdata.tech/blog/general/blockchain-crypto-in-2021-data-review (retrieved: 18.10.2022)

[43] Ibit 9

[44] Ibit 9

[45] CV VC (2023): Top 50 Report 2022. Prepared in collaboration with Bank Frick.

[46] Ibit 45

[47] Uber Technologies (n. d.): Tracking your earnings. https://www.uber.com/gh/en/drive/basics/tracking-your-earnings/#:~:text=Uber%20charges%20partners%2025%25%20fee%20on%20all%20fares (retrieved: 18.10.2022)

[48] Edelman, G. (2021): The father of Web3 wants you to trust les Wired. https://www.wired.com/story/web3-gavin-wood-interview/ (retrieved: 18.10.2022)

[49] Federal Department of the Environment, Transport, Energy and Communications DETEC (2017): Verordnung des UVEK über den Herkunftsnachweis und die Stromkennzeichnung [DETEC Ordinance on the Guarantee of Origin and Electricity Labelling]. 730.010.1.

[50] Schindele, M. (2019): Wie funktioniert eine Kreditkartenzahlung [How does a credit card payment work]? Payment Technology Law. https://paytechlaw.com/kreditkartenzahlung/ (retrieved: 18.10.2022)

[51] Finma (2021): Decentralized Finance (DeFi). Jahresbericht.

[52] Vantrappen, H.; Wirtz, F. (2017): When to decentralize decision making, and when not to. Harvard Business Review. https://hbr.org/2017/12/when-to-decentralize-decision-making-and-when-not-to (retrieved: 18.10.2022)

[53] Ibit 52

[54] SRF News (2017): Nationalrat knöpft sich booking.com vor [National Council takes booking.com to task]. https://www.srf.ch/news/schweiz/nationalrat-knoepft-sich-booking-com-vor (retrieved: 18.10.2022); Kolbe, C. (2019: Uber hat seine Schweizer Fahrer um halbe Milliarde geprellt [Uber has cheated its Swiss drivers out of half a billion]. Blick. https://www.blick.ch/wirtschaft/gewerkschaft-unia-klagt-an-uber-hat-seine-schweizer-fahrer-um-halbe-milliarde-geprellt-id15645475.html (retrieved: 18.10.2022)

[55] Hacker, P. (2019): Corporate governance for complex cryptocurrencies? A framework for stability and decision making in blockchain-based organizations. In: Hacker, P.; Lianos, I.; Dimitropoulos, G.; Eich, S.: Regulating Blockchain: Techno-social and legal challenges. Oxford Academic.

[56] Graffeo, E. (2021): Bitcoin is still concentrated in a few hands, study finds. Time. https://time.com/6110392/bitcoin-ownership/

[57] Ibit 55

[58] Bitpush News (2021): Does the 'Coinbase Effect' Still Exist, and What Does it Mean for the Market? Medium. https://bitpushnews.medium.com/does-the-coinbase-effect-still-exist-and-what-does-it-mean-for-the-market-cc1a19c6fa1c#:~:text=This%20trend%20has%20continued%20over,listings%20in%202020%20and%202018 (retrieved: 18.10.2022)

[59] Hyse, K. (2021): What is the coinbase effect? BSC news. https://www.bsc.news/post/cryptonomics-what-is-the-coinbase-effect (retriefed: 18.10.2022)

[60] Zhen, S.; Ranganathan, V. (2022): Further details emerge on FTX bankruptcy and missing funds. Reuters. https://www.reuters.com/technology/further-details-emerge-ftx-bankruptcy-missing-funds-2022-11-12/ (retrieved: 5.12.2022)

[61] Ibit 22

[62] Laudon, K. ; Laudon, J. ; Schoder, D. (2015): Wirtschaftsinformatik [Business informatics]. Pearson Studium.

[63] Doerk, A.; Hansen, P.; Jürgens, G.; Kaminski, M.; Kubach, M.; Terbu, O. (2020): Self Sovereign Identity Use Cases – von der Vision in die Praxis [Self Sovereign Identity Use Cases - From vision to practice]. Bitkom.

[64] Ibit 63

[65] Townsend, M. (2022): Facebook-Cambridge Analytica data breach lawsuit ends in 11th hour settlement. The Guardian. https://www.theguardian.com/technology/2022/aug/27/facebook-cambridge-analytica-data-breach-lawsuit-ends-in-11th-hour-settlement (retrieved: 18.10.2022)

[66] Raaflaub, C. (2021): e-ID ist vom Tisch – Neustart folgt sogleich [e-ID is off the table - a new start is imminent]. Swissinfo. https://www.swissinfo.ch/ger/abstimmung-7_-maerz-2021-e-id/46414110 (retrieved: 18.10.2022)

[67] Federal Office of Justice FOJ (2021): Discussion paper on the target vision for an e-ID.

[68] Federal Office of Justice FOJ (n. d.): Öffentliche Konsultation zum "Zielbild E-ID" [Public consultation on the "Target Image e-ID]. https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/staatliche-e-id/zielbild-e-id.html (retrieved: 18.10.2022)

[69] Ibit 67

[70] Federal Office of Justice FOJ (2022): e-ID: Bundesrat eröffnet Vernehmlassung [e-ID: Federal Council opens consultation]. https://www.bj.admin.ch/bj/de/home/aktuell/mm.msg-id-89515.html (retrieved: 18.10.2022)

[71] Schellinger, B; Sedlmeir, J.; Willburger, L.; Strüker, J.; Urbach, N. (2022): Mythbusting Self-Sovereign Identity (SSI). Fraunhofer Institute for Applied Information Technology FIT.

[72] Ibit 67

[73] Ibit 67

[74] Ibit 67

[75] Ibit 67

[76] Ibit 67

[77] Mingot, S. (2022): Mit repräsentativen Use Cases das Potenzial von Self-Sovereign Identity ausloten [Exploring the potential of self-sovereign identity with representative use cases]. Adnovum. https://www.adnovum.com/de/blog/mit-repr%C3%A4sentativen-use-cases-das-potenzial-von-self-sovereign-identity-ausloten (retrieved: 18.10.2022)

[78] Hotta, E. (n. d.): Self-sovereign identity use cases. Cheqd. https://cheqd.io/blog/self-sovereign-identity-use-cases (retrieved: 18.10.2022)

[79] Digital Siwtzerland (2022): Building a Swiss Digital Trust Ecosystem: Perspectives around an e-ID ecosystem in Switzerland.

[80] Ibit 79

[81] Loskamp, H. (2022): Mythen und Fakten. Ist Self-Sovereign Identity gefährlich [Myths and facts. Is self-sovereign identity dangerous]? Logbook. https://jolocom.io/blog/mythen-und-fakten-ist-self-sovereign-identity-gefahrlich/ (retrieved: 18.10.2022)

[82] Dewey, C. (2014): Yes, the Facebook Messenger app requests creepy, invasive permissions. But so does every other app. Washington Post. https://www.washingtonpost.com/news/the-intersect/wp/2014/08/04/yes-the-facebook-messenger-app-requests-creepy-invasive-permissions-but-so-does-every-other-app/ (retrieved: 18.10.2022); Lovejoy, B. (2021): App privacy labels show stark contrasts among messaging apps. 9to5Mac. https://9to5mac.com/2021/01/04/app-privacy-labels-messaging-apps/ (retrieved: 18.10.2022)

[83] Ibit 71

[84] Strüker, J.; Urbach, N.; Guggenberger, T. et al. (2021): Self-Sovereign Identity - foundations, applications, and potentials of portable digital identities. Fraunhofer Institute for Applied Information Technology FIT; Ibit 71

[85] W3C (n. d.): W3C. https://www.w3.org/ (retrieved: 18.10.2022)

[86] European Comission (n. d.): What is EBSI. https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/ESSIF+Functional+Scope (retrieved: 18.10.2022)

[87] IDunion (n. d.): IDunion. https://idunion.org/ (retrieved: 18.10.2022)

[88] BOTLabs (n. d.): KILT. https://www.kilt.io/ (retrieved: 18.10.2022)

[89] E-Estonia (n. d.): We have built a digital society and we can show you how. https://e-estonia.com/ (retrieved: 18.10.2022)

[90] Republic and Canton of Jura (n. d.) : Quel était le cas d'usage pour le pilote [What was the use case for the pilot]? https://faq.jura.ch/space/CN/635175035/Quel+%C3%A9tait+le+cas+d'usage+pour+le+pilote+%3F (retrieved: 18.10.2022)

[91] Primary source not accessible. Cited from: Rabe, L. (2022): Aus welchen Gründen nutzen Sie keine sozialen Netzwerke mehr [For what reasons do you no longer use social networks]? Statista. https://de.statista.com/statistik/daten/studie/1283718/umfrage/gruende-fuer-abkehr-von-social-media-plattformen-in-deutschland/ (retrieved: 23.10.2022)

[92] Brandt, M. (2022): Amazon und Meta führen die DSGVO-Top 10 an [Amazon and Meta lead the GDPR Top 10]. Statista. https://de.statista.com/infografik/25449/fuer-verstoesse-gegen-datenschutzgesetze-verhaengte-geldbussen/ (retrieved: 23.10.2022)

[93] Federal Assembly of Switzerland (1992): Federal act on data protection. 235.1.

[94] Boydak (2021): Automation in der Krankenversicherungsbranche [Automation in the health insurance industry]. https://boydak.ch/de/automation-in-der-krankenversicherungsbranche/ (retrieved: 18.10.2022)

[95] Federal Office of Public Health FOPH (n. d.): Verbreitung und Nutzung des EPD [Dissemination and use of the EPD]. https://www.bag.admin.ch/bag/de/home/strategie-und-politik/nationale-gesundheitsstrategien/strategie-ehealth-schweiz/umsetzung-vollzug/verbreitung-nutzung-epd.html#:~:text=Mit%20dem%20EPD%20sollen%20die,Patientinnen%20und%20Patienten%20gef%C3%B6rdert%20werden (retrieved: 18.10.2022)

[96] Davis, J. (2021): Dark web analysis: healthcare risks tied to database leaks, credentials. Health IT Security. https://healthitsecurity.com/news/dark-web-analysis-healthcare-risks-tied-to-database-leaks-credentials (retrieved: 18.10.2022)

[97] EPD (n. d.): Was ist eine Stammgemeinschaft [What is a stem community]? https://www.patientendossier.ch/eroeffnung/was-ist-eine-stammgemeinschaft (retrieved: 18.10.2022). Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren (2019): Wer kann auf das EPD zugreifen? Gesundheitsfachpersonen nach EPDG [Who can access the EHR? Health professionals according to EPDG]. Factsheet.

[98] Federal Office of Public Health FOPH (2022): Zertifizierte (Stamm-)Gemeinschaften [Certified stem communities]. https://www.bag.admin.ch/bag/de/home/strategie-und-politik/nationale-gesundheitsstrategien/strategie-ehealth-schweiz/umsetzung-vollzug/zertifizierte_stammgemeinschaften.html (retrieved: 4.1.2023); Konferenz der kantonalen Gesundheitsdirektorinnen und -direktoren (2022): Elektronisches Patientendossier: Die Einführungsphase läuft [Electronic patient dossier: the introductory phase is underway]. Factsheet.

[99] Federal Office of Public Health FOPH (n. d.): Prävention in der Gesundheitsversorgung [Prevention in health care]. https://www.bag.admin.ch/bag/de/home/strategie-und-politik/nationale-gesundheitsstrategien/strategie-nicht-uebertragbare-krankheiten/praevention-in-der-gesundheitsversorgung.html (retrieved: 18.10.2022); WBF/EDI (n. d.): Gesamtsicht Aus- und Weiterbildung Medizin im System der Gesundheitsversorgung [Overall view of education and training in medicine in the health care system].

[100] Gfs Bern (2021): Swiss eHealth Baromter 2021.

[101] Based on the workshops with the industry partners and various studies: Azari, A.; Ekblaw, A.; Vieira, T.; Lippman, A. (2016): MedRec: Using Blockchain for Medical Data Access and Permission Management. 2016 2nd International Conference on Open and Big Data (OBD), 25-30. https://doi.org/10.1109/OBD.2016.11; Shreshta, A.; Vassileva, J.; Deters, R. (2020): A Blockchain Platform for user data sharing ensuring user control and incentives. Frontiers in Blockchain, 3:497985, https://doi.org/10.3389/fbloc.2020.497985. Mamo, N. ; Martin, G. ; Desira, M; Ellul, B. ; Ebeje, J.-P. (2020): Dwarna: a blockchain solution for dynamic consent in biobanking. European Journal of Human Genetics, 28, 609-626. https://doi.org/10.1038/s41431-019-0560-9

[102] Mamo, N.; Martin, G.; Desira, M; Ellul, B.; Ebeje, J.-P. (2019): Dwarna: a blockchain solution for dynamic consent in biobanking. European Journal of Human Genetics, 28. https://doi.org/10.1038/s41431-019-0560-9

[103] Mamo, N.; Martin, G.; Desira, M; Ellul, B.; Ebeje, J.-P. (2019): European Journal of Human Genetics, 28. https://doi.org/10.1038/s41431-019-0560-9

[104] Helsana (n. d.): Helsana+ App. https://www.helsana.ch/de/private/services/apps/helsana-plus.html?utm_source=google&utm_medium=gsn&utm_campaign=2022_01_sea_plus_app_01&utm_term=de_all_rsa&utm_content=plus_app&gclid=Cj0KCQjwxIOXBhCrARIsAL1QFCZ4SPRPg-dwwuqphtnW9Yiw--azPdfV9EvKG8coWZ06fUriozBqzzEaAtqwEALw_wcB (retrieved: 18.10.2022)

[105] Schechner, S.; Secada, M. (2019): You give apps sensitive personal information. Then they tell Facebook. Wall Street Journal. https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636?mod=e2tw (retrieved: 18.10.2022)

[106] Cox, J. (2022): Data broker is selling location data of people who visit abortion clinics. Vice. https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood (retrieved: 18.10.2022)

[107] Rocher, L.; Hendrickx, J. ; de Montjoye, Y. (2019) : Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun 10, 3069. https://doi.org/10.1038/s41467-019-10933-3

[108] Evashwick, C. (1989): Creating the continuum of care. Health Matrix, 7(1):30-9. https://pubmed.ncbi.nlm.nih.gov/10293297/

[109] Batt, J.; Da Forno, M.; Pfarrer, R. (2017): Rückverfolgbarkeit in der Lieferkette: Grundlagen und Prozesse [Traceability in the supply chain: fundamentals and processes]. GS1 Switzerland.

[110] GS1 Switzerland (n. d.): Medicinal products. https://www.gs1.ch/en/industries/healthcare/pharmaceuticals (retrieved: 18.10.2022)

[111] Bayard Consulting (n. d.): Was ist das GDSN [What is the GDSN]?; ECR (n. d.): GS1 Global Data Synchronization Network (GDSN). https://www.ecr.digital/book/gs1-standards/gs1-global-data-synchronisation-network-gdsn/ (retrieved: 18.10.2022)

[112] IBM; KPMG; Merck; Walmart (2020): FDA DSCSA: Blockchain Interoperability Pilot Project Report.

[113] Ibit 112

[114] Bischoff, O.; Seuring, S. (2021): Opportunities and limitations of public blockchain-based supply chain traceability. Modern Supply Chain Research and Applications, 3(3), 226-243. https://doi.org/10.1108/MSCRA-07-2021-0014

[115] Modum (2021): Roambee Acquires Modum's Condition Monitoring Division. https://www.modum.io/news/roambee-acquires-modum?hsLang=en (retrieved: 23.10.2022)

[116] Ibit 112

[117] Ibit 112

[118] Ibit 114

[119] Ibit 114

[120] Ibit 9

[121] Aggarwal, S.; Kumar, N. (2021): Chapter twenty - Attacks on blockchain. Advances in Computers, 121, 399-410. https://doi.org/10.1016/bs.adcom.2020.08.020

[122] Saraga, D. (2022): Distributed Trust. Universität Zürich. https://www.news.uzh.ch/en/articles/2022/Blockchain-Zavolokina.html (retrieved: 18.10.2022)

[123] Krecké, E. (2019): 'Basel IV' and the stability of the financial industry. Geopolitical Intelligence Services. https://www.gisreportsonline.com/r/basel-iv/ (retrieved: 18.10.2022)

[124] Ibit 122

Publisher
GDI Gottlieb Duttweiler Institute
Langhaldenstrasse 21
CH-8803 Rüschlikon
www.gdi.ch