Digital Transformation: How the Blockchain Promotes Mutual Trust within an Ecosystem

Thomas Zweifel and Johannes Kirchhofer

1 Introduction

In recent decades, digitalization has fundamentally changed our private and business worlds. Initially, digitalization was concerned with internal company processes: Data was standardized, processes harmonized, and procedures optimized, in order that companies could meet the needs of their customers more quickly and cost-effectively.

The second phase saw the optimization of external company interfaces, in other words the bilateral interfaces with customers and suppliers. The main aim was to optimize a company's direct value-added chain, notably by reducing risks, e.g., through lower storage costs, faster turnaround times, or increased delivery capacity. These connections and solutions were often shaped by the bilateral relationships with suppliers and customers, and customized to the company's individual requirements, although industry standards did develop over time in certain areas.

The third phase, which emerged in recent years, has seen new ecosystems being formed, no longer centering around individual value-added chains for specific products but rather on complex value-added networks and platforms. The companies involved are much more digitally interconnected. This enables complete vertical integration, where production is controlled by a single company, from the raw materials all the way through to the end product or service, as well as complete horizontal integration, where a specific product or service is offered across various sectors. If necessary, the production of goods and services can be distributed much more granularly across a number of companies, meaning small companies have the opportunity to participate in highly specialized niche global markets. Businesses also benefit from further cost reductions and increased customer satisfaction. Moreover, they are able to switch from a model based on standardized products produced in large volumes to more customized, faster mass production or even automated single-unit production.

2 Growing Data Volumes: Versioning, Ownership, and Responsibility

Data volumes are increasing, not only within companies but also within ecosystems. In this type of network, it is difficult to ensure the traceability of datasets and any modifications to them over time, because digital data can easily be copied and customized in any version. Moreover, the data itself is increasingly becoming a product or an essential component of digital services. It is therefore vital that companies retain control of these data streams and processes while still being in a position to exchange data with other parties. In addition, there is the question of who is responsible for the collection, maintenance, and accuracy of this data, as well as who bears any associated liability for it. Likewise, who is permitted to use the data and to what extent, and to whom does the data belong?

In many countries there are legal challenges associated with data ownership, for example, in Switzerland where no right of ownership of data exists. Datasets stored digitally are not physical items and can be easily copied without affecting the original dataset. Consequently, even the concept of data theft is complicated, since the idea that a stolen object is no longer available to

the victim is not the reality – the stolen copy simply becomes a new, independent dataset. Of course, other legal protection options exist for certain data types, but this is far from true in all areas. For example, copyright laws can be invoked for plans, images, or pieces of work. Furthermore, data protection regulations impose legal restrictions, in particular with regard to personal data, biometric characteristics, or other datasets which may be used to identify individuals. In most other areas, however, it is necessary to look to contract law, including the granting of usage rights and contractual penalties. The problem with this is that all the partners involved have to conclude contracts with each other and use a shared platform that clearly sets out and has the authority to regulate the associated relationships, rights, and obligations.

3 A Shared, Centralized Platform without Trust?

Managing shared data and processes requires a shared technical platform. In the simplest case, the partners agree to use a centralized platform. But who exactly builds this platform? Who bears the construction and operating costs? Who decides on any future expansion, the roadmap, and the needs of the participants? How do you ensure that a centralized platform like this does not shut down unexpectedly, become bankrupt, or get taken over by another, undesirable provider who can then arbitrarily change the rules? This dependency relationship between companies and a platform operator requires clear contractual security and a high degree of trust on the part of companies. A centrally managed construct is therefore conceivable, but complex in terms of its implementation and not suitable for all parties.

4 Trust is Good, Control is Better: A Distributed Platform

Distributed ledger technology has seen algorithms come onto the market in recent years, some of which have been around for some time, but have only recently found their way into more widely available solutions. In particular, the combination of cryptographic signatures and timestamps with decentralized, distributed data storage can help resolve some of the issues cited previously. The signatures and tamper-resistant timestamps ensure that the author of a dataset and also the time of publication is clearly defined. If a signed dataset is written to a distributed database with *n* locations (referred to as nodes), all nodes and all users can verify who the author is and the time at which the dataset was published, based on the signature and timestamp. A distributed database also significantly reduces the risk of downtime since the data is no longer stored only in a single location or at one central company; instead all authorized companies have their own individual copy. It is important to note that, depending on the technology used, e.g. in the case of the Corda product, not every node needs to have access to all of the datasets; when datasets are distributed to the nodes, it is possible to ensure that they are only stored on those nodes for which the author has granted permission. This targeted distribution, fine-grained access control and, if necessary, encryption prevent any unauthorized access to the data, even if a node should fall into the wrong hands.

Solutions using distributed ledger technology eliminate the need for a centralized platform; a distributed platform enables the individual nodes to take back control of their data. Moreover, a modern, distributed database using distributed ledger technology solves the problem of multiple versions and obsolete copies of datasets, as the versioning system ensures the latest version of the dataset is always available on the distributed database, together with its entire history if needed. In addition, the decentralized platform has the option to use smart contract functionality to regulate usage rights for datasets or contractual penalties in the case of misuse.

In short, each company is able to determine when it publishes particular information on the distributed ledger, who has access to that information within the ecosystem, and how that information can be used. The rights and obligations fall to the individual author of the dataset or their respective company.

5 Permissioned vs. Public

This solution not only enables datasets to be exchanged faster and more reliably, it also provides a reliable history for traceability. This transparency also makes it easy to spot cases of misuse, as the authors of a dataset guarantee its integrity through the respective timestamp and their digital signature. The individual nodes only have to validate the timestamp and signature of the authors to confirm the respective data packet; they do not have to have any knowledge of or validate the content of the data packet itself.

Depending on the implementation (see also the article by Dr. Fazekas), majority decisions would have to be manipulated in order to tamper with these security mechanisms, i.e. more than half of the nodes would have to be compromised. Recently, this problem has been more prevalent with public blockchains as users of public blockchains are, by definition, anonymous. This makes it difficult to control how many nodes a user controls and whether a user can manipulate majority decisions to their advantage by gaining more than half of the nodes. Even though artificial obstacles such as proof of work have been introduced, this development represents a real threat to public blockchains. However, since the implementations described here relate to permissioned blockchains, i.e. consortium-based ecosystems comprising known companies and users, this risk is much less significant.

It is also possible to make clever use of the underlying technologies to ensure compliance with other requirements for data protection, such as the subsequent deletion of personal data, without compromising the consistency of the respective ledger.

6 Coopetition: Win-Win Situation for Everyone Involved

In a consortium-based ecosystem such as this, it is particularly important that all participating companies are able to reconcile conflicting interests within the common ecosystem, but also sufficiently delimit or differentiate their own business models. This balancing act between cooperation and competition is often referred to as coopetition. In this case, competitors come together, along with suppliers, partners and companies operating in similar fields, to form an ecosystem that brings efficiency gains for everyone. However, at the same time the companies are, to some extent at least, competing to win end customers for their products and services. Despite this competitive situation, a shared platform based on distributed ledger technology can still bring additional benefits for each individual participant, for example, by reducing the time and money spent on data acquisition and management or by optimizing their production process. These added benefits usually outweigh the competitive element, creating a win-win situation within the ecosystem over third parties that do not use such an ecosystem.

Alongside the efficiency gains and resulting competitive advantages, there is also the possibility to develop new business fields and business models. A platform of this kind, which is built and used collectively, has the potential to evolve into a data exchange platform that uses smart contracts to regulate fee-based access to the datasets. This also provides an added incentive to publish high quality data and keep data up-to-date. Moreover, it opens up another business channel which can provide an additional source of income for the publishing company, while allowing data purchasers to cut costs by purchasing existing data rather than collecting their own. Other potential uses include the evaluation of anonymized metadata, or up- and cross-selling.

7 Distributed Ledger Technology: A Unique Opportunity

All in all, distributed ledger technology opens up numerous new opportunities for companies to cooperate more efficiently and effectively and gain a strategic advantage. If you want to assess

the potential of distributed ledger technology for your own business, you should first look at the other companies in the ecosystem. We live in a highly networked world where business is conducted across borders every day, meaning that competition between ecosystems will have a much more significant impact on your own success in the future. Customers no longer want to piece together the different components needed to solve their own problems; they want to have their needs met from a single source. This creates a completely new brand of customer loyalty. Against this backdrop, innovative business models will help make better use of hidden reserves such as data in the future.

Technical contribution: Köhler-Schute, Christiana (ed.): Blockchains und Distributed-Ledger-Technologien in Unternehmen, Grundlagen, Konzepte und Praxisbeispiele, juristische Aspekte [Blockchains and Distributed Ledger Technologies in Companies: Foundations, Approaches and Practical Examples, Legal Aspects], Berlin: KS-Energy-Verlag, 2019 (ISBN: 978-3-945622-09-4)

Courtesy of: KS-Energy-Verlag, Berlin 2019