Blockchain

A step-by-step guide to implementation

fir an der RWTH Aachen

Roland Berger

Introduction

Distributed ledger technologies, of which the best known example is blockchain, were expected to make their big breakthrough in 2018. Instead, the opposite happened. Cryptocurrency price slumps and delays in promising projects became symptoms of a new sense of caution. Organizations tried to use blockchain in unsuitable applications, and underestimated implementation hurdles.

Despite this, the need for effective data exchange and data management in today's connected world remains high. Decentralized solutions, intelligent sensors, global supply chains and vast quantities of customer data will further stimulate demand for specialized and powerful data management systems. Blockchain therefore remains one option to enable a secure and interconnected world. The following five-step approach will help you harness blockchain's potential, avoiding common mistakes and overcoming implementation hurdles on your way.

Contents

Step 1

Decide if blockchain fits

The first step in your blockchain journey is the most important. You have to define what you and your partners actually require from your data management system. The "Technology seeks application" adage is especially pertinent in the case of blockchain technology. Distributed ledgers are often applied to problems that are a poor fit for the technology. While they can be used to build a distributed data management system between several entities, they are not the only solution. It is important to understand that the technology is not a "better" way to store, exchange and manage data but simply "another" way.

A: The five-step approach

1. **Decide if blockchain fits**
2. **Identify suitable blockchain settings and incentives**
3. **Identify and close organizational resource gaps**
4. **Evaluate costs and benefits before prototyping**
5. **Build your blockchain piece by piece**

Source: Roland Berger

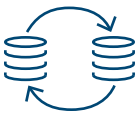
B: Data management technologies

BILATERAL DATA EXCHANGE

EXAMPLE	Typical examples are e-mail, telephone, electronic data interchange (EDI)
PRINCIPLE	Data is not systematically stored. Transactions are only traceable between direct participants
ADVANTAGES	Easy to use; low investment and maintenance costs; no central authority
DISADVANTAGES	No traceability; no ecosystem-wide data analysis possible; falsification of data possible; when standards are changed each partner must adapt IT; redundancy of data

Bilateral data interchange, paired with centralized databases, is still the prevalent system used by organizations to exchange data

Source: Roland Berger

CENTRALIZED DATABASE	DECENTRALIZED DATABASE	DISTRIBUTED LEDGER
		
Typical client/server architecture within organizations, for example Oracle, MS SQL, SAP HANA, PostgreSQL, MySQL	Common data management architecture used by multiregional organizations. Typical examples are: Cassandra, Hadoop, Hive, MongoDB, Elasticsearch, Industrial Data Space	Young data management architecture, mainly used for cryptocurrencies. The dominant version is blockchain, while other examples include hashgraph and IOTA
All data is stored and updated in one single database on one hardware solution. A trusted authority decides what data is stored and updated	Data is stored where needed on several connected databases. A trusted authority decides what data is stored and updated	All data is stored and updated in one single database, stored on all participants' hardware. An algorithm, called the consensus mechanism, decides what is stored and updated on the database. There is no central authority
Single trusted source; no duplication of data; high performance; easy to operate and maintain; high acceptance among users	High availability and fault tolerance; high performance; high scalability; highly customizable, depending on the application	Single trusted source; no duplication; no single point of failure; proprietary traceability of transactions
Trusted database provider needed, including costs for the provider; single point of failure; limited scalability due to bandwidth; no proprietary traceability of transactions[1]	Duplication of data points; no single trusted source; no proprietary traceability of transactions[1]	Limited scalability due to bandwidth and consensus mechanism; limited tolerance for corrections; frequency of data writing is limited; difficult to implement

[1] Transaction history can be traced by additional data log

CLOUD SOLUTIONS are not simply generic database architectures. Rather, the term describes the on-demand availability of data management services to users over the internet. The cloud provider takes on the role of a central, trusted intermediary, which observes and controls data access.

All of these solutions have their raison d'être. By answering the following questions you can determine if blockchain is the right solution in your use case:

1. **Shared database:** Do you need a structured database that is shared among entities?
2. **Multiple writers:** Is there more than one entity generating transactions that modify the database?
3. **Absence of trust:** Do the entities not trust each other to modify their database?
4. **Disintermediation:** Do you want to avoid having a central party acting as a transaction gatekeeper?
5. **Dependent transactions:** Do you have transactions that depend on each other?

If you answered "no" to any of the questions, then you should not apply blockchain. Instead you should have a closer look at one of other proposed data storage and management solutions. → B

But if you answered "yes" to all five questions, then read on as the remaining four steps will help you successfully manage your blockchain project.

Step 2

Identify suitable blockchain settings and incentives

IDENTIFY BLOCKCHAIN SETTINGS

Once you have identified blockchain technology as the most suitable database technology for your use case, you need to identify the correct blockchain settings. There are various technical solutions with which to set up and manage a blockchain. The decision dimensions for the right kind of blockchain can be broken down as follows:

- → **Who has read and write rights for the data stored in the blockchain?** (Private or public)
- → **What is the degree of centralization?** (Number of nodes)
- → **What kind of consensus mechanism is used?** (Proof of work vs. proof of stake, for example)
- → **What kind of data do I need to store on the blockchain?** (Oracle needed?)

→ READ AND WRITE ACCESS

Blockchains can be designed to restrict someone's ability to access, contribute or store information. There are generally three levels of access. The most obvious is reading, or who is permitted to access what data. For example, complete transparency poses obvious problems concerning proprietary and private data, but it can also increase trust and accountability. The next level is contributing transactions, which describes the permission needed to send transactions (data) within the network. This does not necessarily mean that the transaction will be stored on the blockchain; a supplier could be permitted only to read selected details of a product and contribute data. Whether this data is actually accepted and added to the blockchain is determined by the consensus mechanism (see below). This is the third level of access and allows someone to add new data to the blockchain, subject to validation by the respective consensus mechanism.

→ DEGREE OF CENTRALIZATION

A key characteristic of a blockchain is the redundant storage of the entire set of data across multiple

participating nodes in the network. A node can be any electronic device with access to the network and the capability to process data (e.g. a PC or smartphone). Any fully integrated node will store an entire local copy of the blockchain, receive every single transaction within the network and contribute to the validation process. However, there is no standard on how many nodes with the complete set of data need to exist, or how many different parties should control them. A high degree of decentralization implies a high number of independent nodes and therefore greater data safety, integrity and reliability. A high degree of centralization implies the opposite, but offers advantages around scalability and implementation. In many business applications local versions are stored by cloud providers, offering the necessary IT infrastructure.

→ CONSENSUS MECHANISM

The consensus mechanism describes the process by which the network "agrees" on the next block (of data) to add to the blockchain, or more specifically, which node gets to decide. Achieving consensus on the anonymous internet is a difficult task as in many cases a simple vote does not work. Bitcoin came up with a solution: the consensus algorithm. It is considered the heart of a blockchain application and picks the node that decides which block will be added to the blockchain. There are two different mechanisms. Proof of work: This mechanism relies on the assumption that someone who contributes a significant amount of effort to the blockchain is interested in its accuracy. The chances of a node becoming the decider increase with the amount of "work" it does, usually measured in processing capacity. However, this can lead to high costs and compromised scalability (a common example is the Bitcoin blockchain). The mechanism is like the consensus achievement process at Wikipedia. A user could create several accounts and thus promote their own opinion as a majority opinion (Sybil attack). This is prevented by giving low credibility to accounts that have delivered very few contributions. An opinion from an account with many contributions is given more credibility. Proof of stake: Here the underlying assumption is that someone who has a high stake in the trustworthiness of the blockchain is interested in its accuracy. The higher their stake is, the more likely they will get to decide on a new block. Almost anything can constitute a "high stake", which in turn allows distribution of influence similar to shareholder principles when it comes to steering a company.

→ ORIGIN OF DATA (USAGE OF ORACLE)

While data stored on the blockchain can't be manipulated or compromised, the technology is poor at validating the reliability of a node's data. Beyond plausibility checks there are no mechanisms to, for example, trace whether a parameter was "made up". You may have to establish a system that verifies the origin and trustworthiness of the original data. Several solution providers are attempting to address this issue by certifying specific data sources. However, this undermines the general principle of the blockchain, which tries to avoid dependency on third parties when it comes to establishing trust. This should be taken into account when trying to integrate data from specific origins. Unreliable data may have a negative impact on an otherwise reliable database and involving a third party may compromise independence.

DESIGN AN INCENTIVE SYSTEM FOR PARTICIPANTS

To ensure your partners' participation in the blockchain system you need an incentive scheme. This can be intrinsic (economic advantages for your own organization) or extrinsic. The market power of the blockchain initiator or payments to participants are common examples of extrinsic incentive systems. One argument that can be used to entice a partner to participate is the prospect of a closer bond between the companies. For example, if you get your subcontractor to write in a shared blockchain, they know that your organization will be reluctant to swap them out as it will require a another provider to qualify.

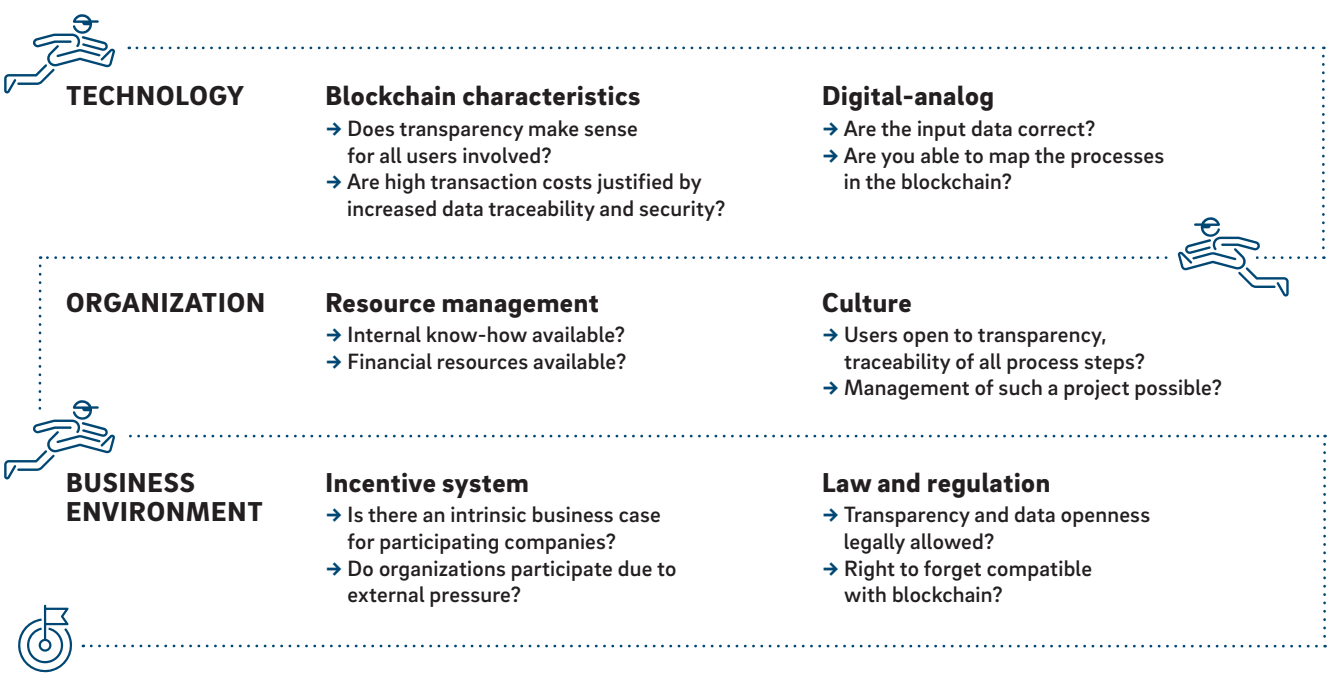
Step 3

Identify and close organizational resource gaps

To ensure the success of a blockchain project you need to check if your internal resources can cope with the challenge. The key factors to ensure a rigorous cost-benefit analysis of the use case, as well as successful implementation, include:

- **Business model understanding**
- **Process knowledge**
- **Technological know-how**

C: Blockchain implementation hurdles



Source: Roland Berger

Step 4

Evaluate costs and benefits before prototyping

Understanding what the organization's business model is and developing potential new business models is critical in determining if the use case will achieve long-term business goals. It is about the danger the intended use case poses to the current business model, as well as the opportunities it can open up. In addition, an understanding of the business models and trends in the economic environment is important. Questions such as "What is my partner trying to achieve through their role in the use case?" or "Is that contrary to our own interests?" must constantly be revisited.

As with every IT project, knowledge about business processes is crucial. In many organizations, very few employees have an actual, comprehensive overview of these processes. It is therefore worthwhile including a process review in the blockchain project.

The organization needs technological know-how about data management systems, and blockchain especially, to determine if the possibilities and limitations of the technology match its own interests. In particular, employees should thoroughly assess whether other database technologies are a better fit. In case of doubt, train employees to use them. However, it is not necessary to employ a large number of programmers to code and maintain the blockchain yourself – these resources can easily be outsourced to external service providers. But the organization still needs a limited number of experts to validate the work of the external service providers. After concluding step 3, you should be able to answer all questions regarding the common blockchain hurdles, whether they are of a technological, organizational or business environmental nature. → C

After working out which kind of blockchain you need, how to incentivize your partners and how to build up the necessary internal knowledge, you need to reevaluate the benefits and costs of the use case. Methods such as NPV/ROI calculations should form the basis of the analysis. However, be aware that the success of the project is highly dependent on your business partners, too. Combined with the immaturity of the technology, this means the upward and downward risks of the project are higher than in conventional business investments. These points are key to the evaluation of the project's financial viability.

Step 5

Build your blockchain piece by piece

IMPLEMENT A PROTOTYPE/ PROOF OF CONCEPT

After establishing the financial viability of the use case, you can start building a blockchain prototype, or proof of concept. However, first note the following points:

- It is a widespread misconception that blockchain can digitalize processes or replace digitalization. Blockchain is a digital data technology that needs digital infrastructure to work, including digitalized inputs, processes and outputs.
- If your organization is already sufficiently digitalized you need to integrate your blockchain system into this infrastructure. It won't be economically feasible to build a fully redundant IT infrastructure for your blockchain project.
- Remember: Blockchain projects are set up between organizations or departments that do not fully trust each other. Such cross-entity projects have no structure that converges on one decision-maker, but rather a structure that converges on the responsible managers of all entities involved. The fact that these managers tend to all have their own target horizon complicates goal-oriented cooperation, in particular. It is therefore advisable to rely on service providers who can cope with the task of cross-organization coordination and cooperate with companies that have previously proved to be good partners, e.g. through industrial associations.
- However, once the set-up is clearly defined and alignment between partners is ensured, the blockchain project becomes a comparably ordinary IT project. Responsibilities must be defined, maintenance plans developed, interfaces between the systems programmed and access rights distributed.

TEST AND LEARN FROM THE PROTOTYPE

It is essential to understand that a blockchain, by definition, is more difficult to update (including bug repairs) than classic databases with a central intermediary. Put simply, the more participants that take part in a blockchain, the more difficult it is to change protocol, as every participant must agree to the update. Therefore, it is essential to undertake comprehensive testing and clearly regulate cooperation between blockchain participants in advance. Furthermore, KPIs must be defined to compare the performance of legacy systems (central databases) and blockchain based systems. However, organizational learning will ensure that the one-off costs of extending the use case or future use cases will decrease.

GO FROM PROTOTYPE TO PRODUCT

A fundamental advantage of blockchain is that the technology replaces confidence in a central intermediary. This advantage is lost if the organization that launched the blockchain becomes a new form of intermediary by maintaining the power to alter the blockchain code without the approval of other participants. To avoid this happening, make the blockchain code available to all users, opening up access to the blockchain, or cede decisions to a consortium. Depending on the use case, it may be useful to attract other participants in order to benefit from network effects.

Conclusion

Blockchain is only one of many database technologies that can be used to store, exchange and manage data between entities. It is not necessarily the best technology to use in every data storage and management scenario. You therefore have to check very carefully that blockchain fits your use case before starting the implementation process.

However, even after concluding that blockchain is the best fit, you need to honestly evaluate the benefits and costs of such an IT project. If your existing system works properly with only minor hitches, experience shows that the benefits of blockchain often do not outweigh the risks and costs of implementation.

ROLAND BERGER, founded in 1967, is the only leading global consultancy of German heritage and European origin. With 2,400 employees working from 35 countries, we have successful operations in all major international markets. Our 52 offices are located in the key global business hubs. The consultancy is an independent partnership owned exclusively by 230 Partners.

The Institute for Industrial Management (FIR) is a non-profit, intersectoral research and educational institution at RWTH Aachen University concerned with business organization, information logistics and corporate IT with the aim of establishing the organizational basis for the digitally integrated company of the future.

PUBLISHERS

FIR (Institute for Industrial Management) at RWTH Aachen University
Campus-Boulevard 55
52074 Aachen
Germany
www.fir.rwth-aachen.de/en/

Roland Berger GmbH
Sederanger 1
80538 Munich
Germany
www.rolandberger.com

CONTACTS

FIR:

PROF. DR.-ING. VOLKER STICH
Managing Director
blockchain@fir.rwth-aachen.de

ROLAND BERGER:

DR. MARTIN STREICHFUSS
Partner
martin.streichfuss@
rolandberger.com

AUTHORS

FIR:

PROF. DR.-ING. VOLKER STICH
Managing Director

JAN RESCHKE
Head of Department
Production Management

DAVID HOLTKEMPER
Head of Research Unit
Supply Chain Management

ROLAND BERGER:

DR. MARTIN STREICHFUSS
Partner

DR. JOERG ESSER
Partner

DR. CURT CRAMER
Project Manager

RAFAEL GEISLER
Consultant