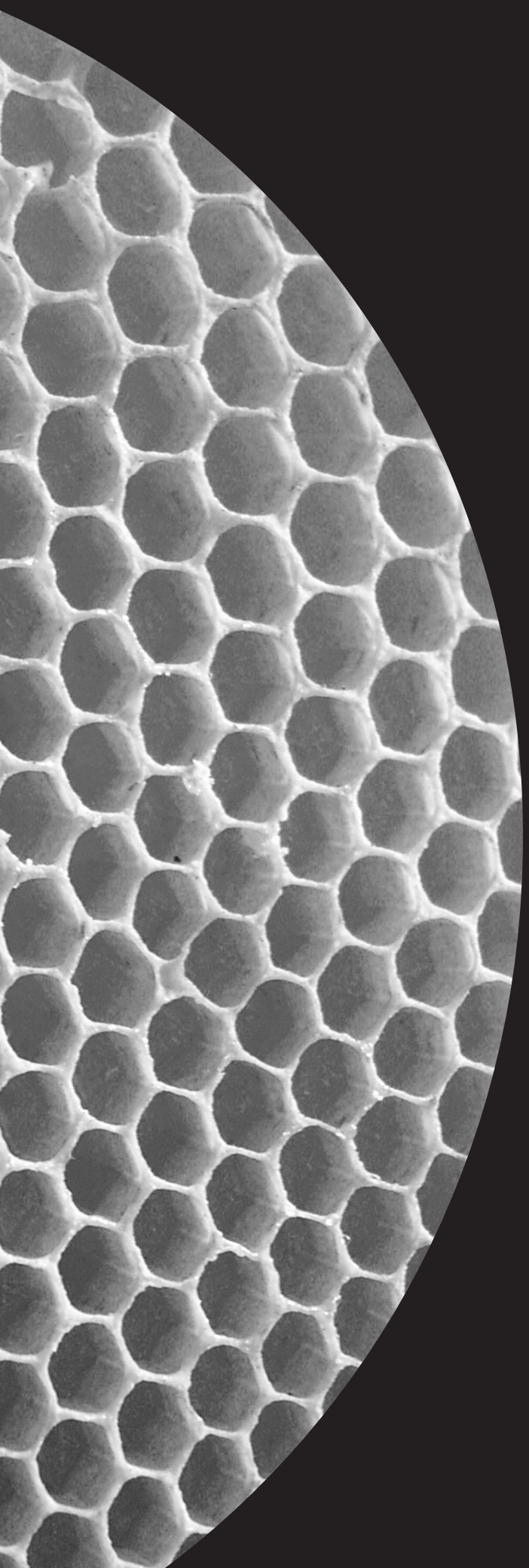
DXC.technology

# Beyond the buzz: blockchain, from myth to practise



# Blockchain, the web of value

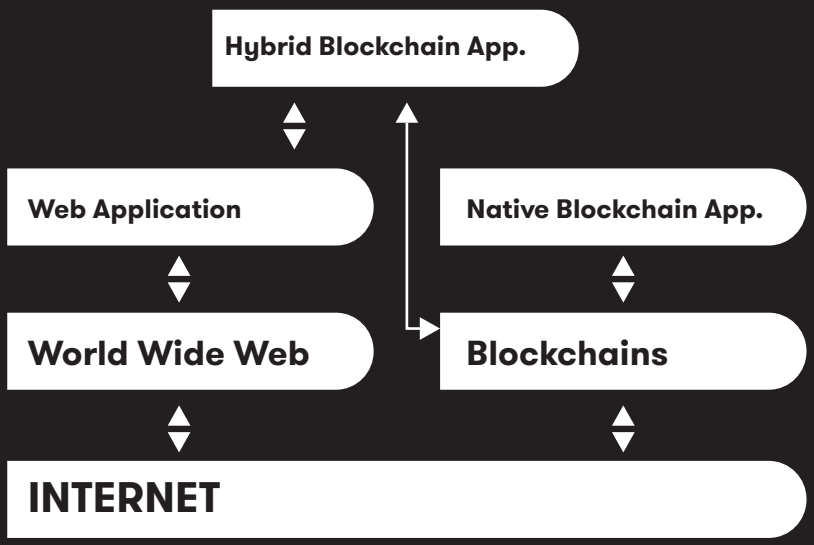
**By making it possible to exchange information almost instantaneously, the Internet has ushered in a revolution. However, carrying out a transaction on the network – such as a payment – requires implementing complex intermediation, verification, and compensation mechanisms. Blockchain promises to do away with this limitation by making it possible to transfer – and not just share – a piece of information.**

On the web, the sender keeps a copy of the data being sent. With blockchain, data is transferred once and for all to the recipient, and what's more, the data transfer is certified without having to use a trusted third party. It's exactly like a bank note passing from one hand to another.

From that point on, it becomes possible to confer intrinsic value on the information, whose authenticity, integrity, and legitimacy are guaranteed from owner to owner. Blockchain therefore makes it possible to create unassailable, tamper-proof digital assets and to achieve digitization and disintermediation for documentation (identity, authenticity, ownership, provenance, etc.), rights (usage, access, authorization, etc.), traceability (receipt, reading, editing, time-stamping, etc.), and even units of account (loyalty points, currency, etc.).

From mobile payments to protection against counterfeiting, logistics, and access control, blockchain opens up a field of applications we hardly considered before. Applications that streamline, secure, and drastically reduce the cost of transactions, free from the trust-related controls and procedures currently required today.

This is why we are currently witnessing an almost irrational enthusiasm for a technology that is still not yet mature. We do not necessarily need to grasp all of the technical subtleties in order to understand that a tool capable of rendering most of intermediaries obsolete is capable of radically redefining value chains and redesigning entire sections of economic activity. In all sectors, from banking to distribution, from energy to the public sector, this outlook is perceived both as a threat and as an opportunity. And to avoid being swept away by what will be the size of a tidal wave in two or three years, we need to prepare now.




## What answers does this revolution bring?

**Blockchain is a technology based directly on the Internet, but separate from the Web. It is therefore possible to create applications exclusively on the blockchain or hybrid applications that access it via the Web.**

# The ABCs of blockchain

Blockchain technology first appeared in 2009, with the launch of bitcoin, the cryptocurrency that introduced the principles, put them into practise, and is to this day their most successful and emblematic application. Eight years of operation and millions of users have abundantly validated the foundations of blockchain technology, clearing the way for its use in business.

## Trusted operation

The Blockchain is a trust factory between a group of people which allow them to exchange assets safely without the need for intermediaries. An “asset” is any “object” of value that will be recorded and controlled by the log throughout its lifecycle. Example: a medical product, a currency, etc.

The blockchain ingeniously implements a set of preexisting technological units: peer-to-peer, distributed database, asymmetric cryptography, self-execution, etc.

Without going into too much detail, it consists of a log that is replicated on every node of a large network, in which every transaction is, and remains immutable.

All new transactions must be validated by the network, which must correctly indicate that it is recorded subsequent to the preceding transactions. The minimum number of members required for this verification depends on the consensus used. In the case of bitcoin (mining*), it is 51% of the members.

Once it has been validated, the transaction is recorded in a “block”, which is stored next to the previous ones in order to form the new end of the chain.

The security of the system thus resides on a practically insurmountable double obstacle: having a majority of members accept the illicit operation and reconstituting the chain in its entirety to take it into account. Members have a much greater interest in ensuring that the chain runs smoothly, for which they are rewarded. From this principle, there are three key characteristics:

- Trust is inherent: it does not depend on an administrator or institution that would have, as a last resort, the upper hand over the chain, but rather it is produced ex nihilo, by simple construction. In this respect, it can be said that the blockchain is a trusted operation. A transaction can be carried out if and only if one has the legitimacy to do so, without a trusted third party being necessary to confirm it.
- Transactions are unalterable: once they have been registered in the chain, it is no longer possible to return to them. This is a powerful asset for authentication, audit, and traceability applications, but it may also be a disadvantage when considering certain rights, such as the right to retract or forget. A transaction can be corrected or cancelled (by a new transaction), but not deleted from the history.
- The log is transparent: all members of the chain have access to the entire chain and to the transactions within it. Yet again, this is a powerful advantage in terms of integrity and trust, but it will have to be reconciled with obvious confidentiality requirements.

## Smart contracts

A “smart contract” can be a contract in the legal sense of the term. Above all, it is a technical means of executing it (i.e. based on a set of management rules). With support for multiple signatures, it is event-driven and programmable. It can thus automate workflows.

These smart contracts give the blockchain the option of programming, meaning that a transaction can be conditioned to a triggering event, such as an alert threshold, a presence detection, a combination of factors, etc.

## Public/private blockchain

Similar to a secure extranet, a private blockchain covers the main principles of the blockchain, the difference being that the nodes between which information circulates are known, and their number is limited. Trust is no longer distributed over a large community, but rather it relies on a few identified members.

It is preferable to use a private blockchain when the data to be entered in the log must remain private and shared only among a preauthorized number of nodes or participants. The validation task is distributed among all of these nodes.

A public blockchain, on the other hand, can benefit from extended capabilities in terms of security and scalability. Because data recorded in the log is public, DXC strives to be able to share it securely, without having to decipher it or reveal it, using homomorphism on the blockchain.

bitcoin

The underlying chain for the cryptocurrency of the same name has proved its reliability. However, its difficulty to program and its relative slowness is the price of its robustness. It currently takes about ten minutes to validate a transaction, and it can support no more than 7 transactions per second.

ethereum

Ethereum is a distributed computer for programming and executing smart contracts. Launched in July 2015, Ethereum has yet to demonstrate total security and its scalability in order to support industrial-scale enterprise applications.

HYPERLEDGER

Launched in late 2015 by Linux Foundation, Hyperledger is a platform backed by the top names in the IT (IBM, Intel, etc.) and banking (J.P. Morgan, SWIFT, etc.) industries. This governance guides it toward a private blockchain with obvious confidentiality requirements, which are lacking in cryptocurrency.

## Key dates in the Bitcoin

**2007**

Economic crash 2007-09

Sub-prime crisis

Financial crisis

**2008**

bitcoin.org domain name

Nakamoto publishes his paper

Finney talks about blockchain

**2009**

Bitcoin 0.1.10 alpha version

First transaction between Nakamoto and Finney.

Exchange rate is established

**2010**

First blockchain flaw corrected

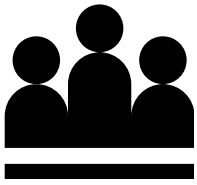
Replacement of Satoshi by Gavin Andresen

# Bitcoin

## The state of bitcoin today. July 2017

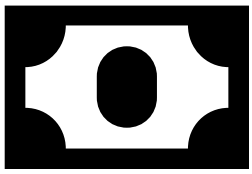
### 16M Bitcoins

- The size of the bitcoin blockchain = 145 GB
- $10,000/mining server, for a gain of 0.04 BTC/day (~€90.day)
- Power consumption per server ~ $2.50/da



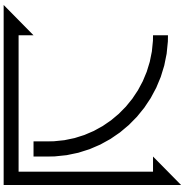
### 10M users

- With the goal of more than 100 million in 2017
- Growth thanks to Bitcoin 2.0



### 1 BTC = $2,500

- Nearly €2,250 (as of July 1, 2017)
- On October 5, 2009, the first exchange rate was established. At the time, 1 BTC = $0.0001.
- On February 9, 2011, parity with the dollar was achieved.



### 151% growth

- Within 3 years, investments grew by 151%.
- It took 4 years between 2010 and 2014 to achieve an investment of $1 billion.
- $1 billion invested in half a year

**2011**

Parity with the USD

Media attention and speculative bubble

**2013**

The value of the bitcoin increases greatly, temporarily surpassing $1,000

**2014**

MtGox officially declares bankruptcy.

eBay adopts bitcoin (Braintree)

**2015**

Nearly $4 billion USD in investments in bitcoin technologies

**2016**

Multiplication of blockchain experiments, exponential rise in the cryptocurrency exchange rate (+120% for bitcoin)

# Blockchain in business: use case and first attempts

Blockchain technology has countless applications, such as speeding up banking transactions, improving loyalty programs, recording wills and property deeds, and controlling the distribution of musical works. Here are some sample use cases.

## Insurance

With the growing popularity of usage-based insurance (UBI) thanks to the possibilities of the Internet of Things (IoT) and connected cars, blockchain technology appears to be a natural way to carry out the associated translations. We can imagine, for example, a model that uses a micropayment system, vehicle sensors that record and transmit the kilometres travelled, and blockchain technology to bill the user accordingly.

## Banking and payments

Thanks to the bitcoin example, this is the first field of use that comes to mind when talking about blockchain technology. Blockchains could revolutionize person-to-person transactions (payments, credits, etc.), international payments, and bank accounts, and also considerably lower compliance costs and operating expenses.

## Manufacturing

With the rise of the IoT, manufacturers must centralize and track data sent by various suppliers along the supply chain. The blockchain could collect this data, store it in the cloud, and offer all stakeholders a shared view of the parts, components, and assembly data over the course of the manufacturing and logistical processes.

## Security

After biometrics and other technologies that are pushing authentication methods, blockchain technology appears to be the next step. It could create a “digital identity” to which a perpetual history of an individual’s transactions would be associated. Once the initial block containing the individual’s personal identifiers has been constructed, it is unalterable and can be used as proof of identity.

## Healthcare

A blockchain could securely store and share information currently contained in electronic medical files. The system could go even further by executing insurance policies.

## Public sector

The government issues and stores a great deal of personal information that blockchain technology could more easily secure and handle, such as property records, land registry data, vital records, vehicle registrations, taxes, licenses and patents, etc.

## Traceability

Guaranteed traceability is a major issue that applies to many fields: data, products, care, devices, logistics, etc. Smart contracts can be used to control the entire value chain and ensure traceability according to pre-established clauses and the roles of the parties involved.

## Marketplace

Blockchain technology and smart contracts can automate relationships between multiple parties in a marketplace. Framework agreements, performance contracts, compensation, and accounting become automated.

## KYC and KYB smart contracts

A company often has suppliers, partners, and customers. The relationship with all of these parties can be covered in a solid framework that automates and simplifies the relationship and ensures the proper execution of each contract.

## Innovative loyalty program

Blockchain technology can automate the lifecycle of loyalty points and benefits programs, including issuance, accumulation, use, and the transfer of benefits between individuals, merchants, and programs. It allows for more flexible and targeted marketing campaigns.

## Regulatory compliance

Transparency and auditability are central to the concerns of regulatory authorities and thus companies. Blockchain technology addresses this need using guaranteed traceability, sequencing of evidence, and log auditability.

# A roadmap for getting started

Blockchain technology is not expected to fully mature until 2018-2020. However, preparations should be made now because there are numerous obstacles that will need to be overcome. This is why those who are thinking about it today will be primely positioned tomorrow and leaders thereafter. To help companies adopt blockchain technology, DSC offers a four-step roadmap. The first two steps are already available: Awareness and Test & Learn.

### Awareness

As breakthrough innovation, blockchain technology still lacks maturity. Skills are rare, and there have been only a few successful implementations. The subject is slow to be abstracted from the technology, and the concepts are still being developed, with a lack of standards and tools, as well as questions regarding scalability. In addition, there are psychological barriers, particularly due to the association between blockchain technology and bitcoin, which has somewhat of a notorious reputation, and due to the system's decentralized governance. These are similar to the struggles faced by the cloud in its early days. And we saw what happened to it.

Like the pioneers of cloud technology did a decade ago, the first step is to understand the technology and, especially, its potential implications for the company's business. Just as not all applications are meant to be used in the cloud, not all processed are likely to be "blockchained". Initially, use cases will need to be identified by asking whether generating, programming (possibly), and transmitting non-falsifiable digital assets could speed up, simplify, or reduce transaction costs. This may include, for example, monitoring a dynamic right, identifying customers (KYC), or packaging an event with sensitive information.

### Test & Learn

Once the use case has been identified and defined, the blockchain requires some smallscale experimentation. This study and demonstration phase will provide a wealth of lessons from a technical standpoint (implementation, performance, etc.) and from a business standpoint (acceptance, uses, etc.). Some companies have already made the leap, which, among other benefits, builds their reputation and their modern image, as such pioneering projects attract much media attention.

Consider Bouygues Immobilier, for example, which announced the implementation of a local smart grid demonstrator based on blockchain technology in October 2016. Based on Ethereum, the system will allow interactions between solar energy generators and consumers to be tracked and monitored within the Lyon Confluence district.

**Roadmap for adopting blockchain technology**

| Awareness | Test & Learn | Return on investment | Integration and deployment |
|---|---|---|---|
| • Understand | • Evaluate the technologies | • Initial Go Live | • Decommission existing systems |
| • Identify | • Demonstrate feasibility | • Deploy new services on blockchains | • Integrate other blockchains |
| • Specific use cases | • Initial learning | • Integrate with other external blockchains | • DAO (Decentralized Autonomous Organization) |
| | • Reinforce the brand image | | |

# Are you blockchain ready?

## 10 criteria for adopting a blockchain approach

### 1. Exchange of Assets

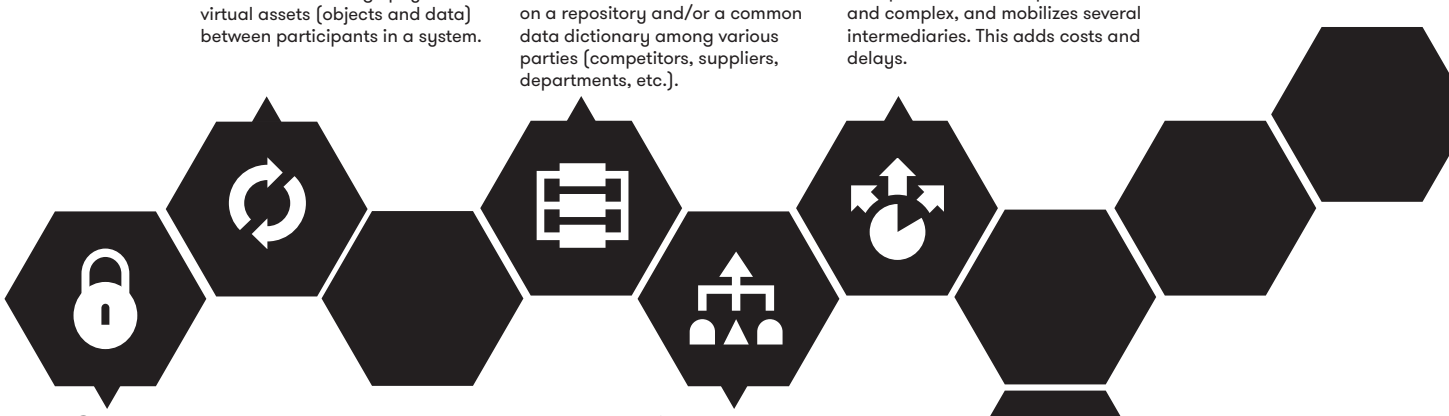
You need to exchange physical or virtual assets (objects and data) between participants in a system.

### 2. Common Repository

You want to have a shared view on a repository and/or a common data dictionary among various parties (competitors, suppliers, departments, etc.).

### 3. Complex Value Chain

Your process chain is specialized and complex, and mobilizes several intermediaries. This adds costs and delays.



### 4. Guaranteed Security

Your operations require strong authentication and permanent security checks, an electronic signature, and so on.

### 5. Guaranteed Traceability

Your operations present a complex chain of events for which proofs must be produced with a guarantee of immutability and non-repudiation.

### 6. Instant transactions

You want to automate your processes and transactions, so that they are closer to real time.

### 7. Shared Solution

Several participants within a value chain must use the same solution to ensure less fragmentation and more maintainability.

### 8. Auditability

For compliance purposes, you want to set up continuous monitoring of audit trails by introducing automation of checks and verifications by smart contracts.

### 9. Trust Foundation

You wish to build a foundation of solid trust and a "common source of truth" among the parties of a value chain (individuals, businesses, connected objects, etc.).

### 10. Business Process Automation

You want to benefit from the programmability of blockchains and the self-execution of smart contracts in order to automate your business processes.

## Count your points

### ✕ Between 0 and 4 points

Focus on approaches with traditional or centralized solutions. Your usage does not necessarily make it possible to derive great value from the capabilities of blockchains.

### ✓ Between 5 and 10 points

You are "blockchain ready"! Today you can benefit from the power of distributed registers and reduce the costs and the burden of your requirements. Let's talk about it.

# Questions & Answers

Blockchain technology raises many good questions that are all aspects that companies must clarify before committing to its adoption.

## What does blockchain technology look like for the end user?

From the user's perspective, the blockchain might resemble a database, for example. Of course, it is very different in how it works (the "base" is now active and programmed), and it can offer many new functionalities. The technology will remain invisible and hidden, behind an ordinary application interface.

## What are te risks associated with blockchain technology?

The blockchain is secure by design, and eight years of bitcoin operation have demonstrated the validity and soundness of the implementation methods. However, there are other types of risks, including:

- Private key security: As the only proof of the user's identity for accessing the chain, this can be stolen, hacked, or usurped if sufficient precautions are not taken.
- Smart contract robustness: Being programmed, these themselves are susceptible to flaws.
- Data storage and confidentiality in a public structure:
  The transactions themselves are secure, but the associated information must also be and should be visible only to their owner and to authorized individuals
- Volatility of blockchain cryptocurrency (public): Necessary for rewarding the work of validating members of the community, a surge in prices could jeopardize the system's economic attractiveness.

## What is the current legal and regulatory framework?

The subject of blockchain technology is thorny for lawmakers: On one hand, it is a popular innovation among companies that is evolving extremely quickly and too often we risk having inadequate or even mortifying provisions, and on the other hand, it is a technology that promises to shake up the balance of particularly sensitive industries – banking, health, legal professions, intellectual property, etc. – and therefore requires the highest level of vigilance.

Currently, the law reflects this in-between state, with blockchain technology already being recognized (European Parliament resolution, Sapin 2 Law), but with cautious vagueness. However, the April 28, 2016 ordinance, which amends the Monetary and Financial Code, states that "the issuance and sale of mini-notes may also be recorded in a shared electronic recording device," which is the first implicit recognition of the legal value of an entry in the blockchain.

# Glossary

Blockchain technology involves many concepts and therefore a specific vocabulary. Here are some of the terms that are commonly encountered in the literature.

### DAO (Decentralized Autonomous Organization)

An organization whose operating rules are recorded in the blockchain and are therefore transparent and inalterable.

### Dapps (decentralized distributed applications)

Blockchain technology makes it possible to develop applications that can be executed on multiple network nodes. A smart contract is one particular example.

### Hash

When a new block is created, a network-specific algorithm transforms the block into a code, called a “hash,” to represents it and ensure its integrity. This transformation is possible only in one direction. It is the verification of the validity of this “hash” by minors that results in the acceptance of the transaction and the addition of the block to the chain.

### Miners

In reference to mining, which they carry out in order to validate transactions, this term refers to members of the community that keep the blockchain up and running.

### Oracle

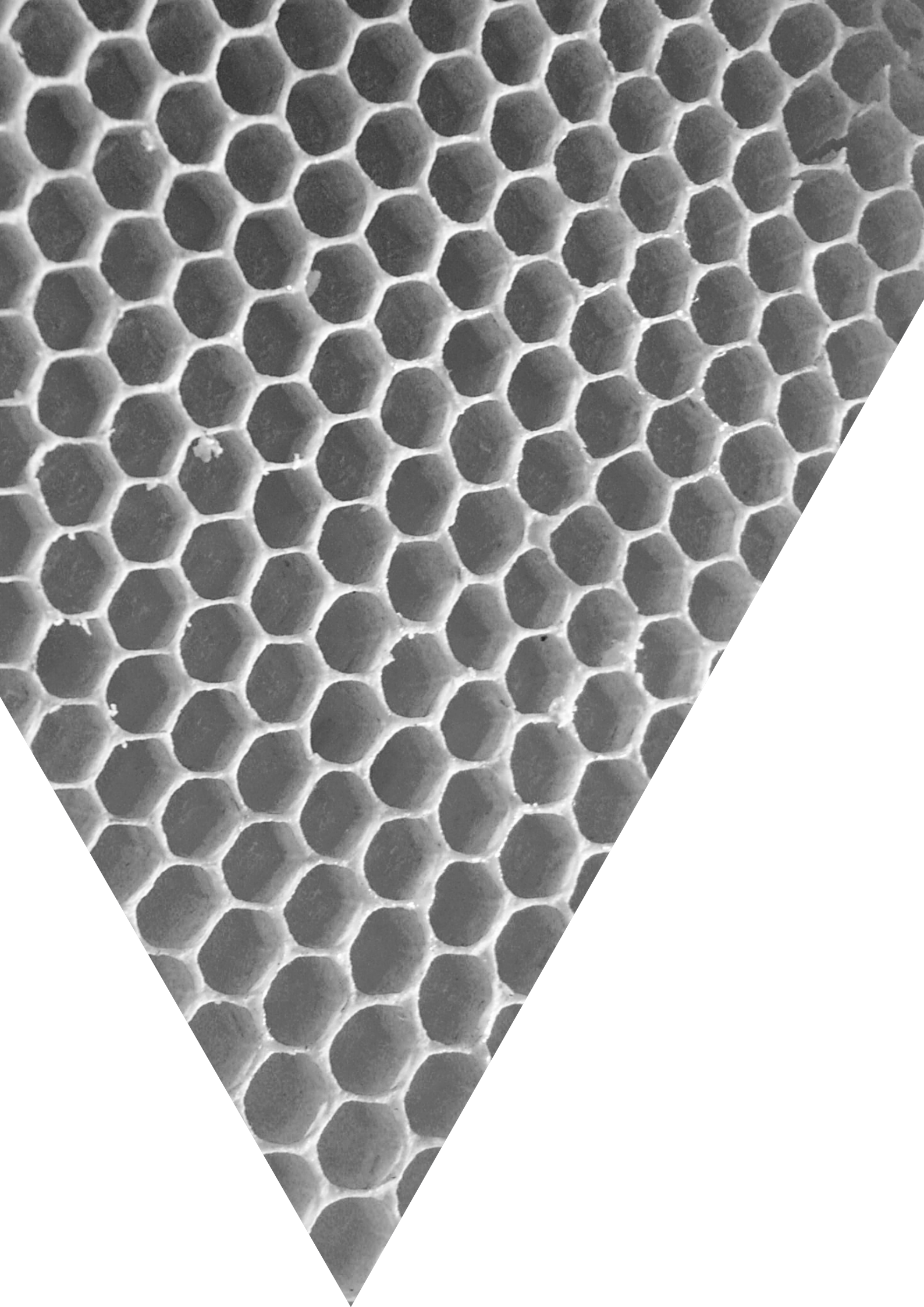
Third-party data source, deemed reliable and agreed upon between the parties, decided by the execution of a smart contract. For example, Météo France for weather conditions.

### Proof-of-work mining

This is the original method of validating blocks by consensus, implemented by bitcoin. It is based on the “Byzantine Generals” problem. That is, what strategy should be implemented to validate an order despite the presence of “traitors” within the organization (Byzantine Fault Tolerance)? The solution to proof-of-work is to reach a consensus with a minimum of 51% of the network members. Slow and energy-intensive, it can be substituted with other proof methods (proof of stake, Proof of usage, etc.), which are less robust. There are other proof mining methods that exist. Proof of stake is 1,000 times faster, as well as proof of authority, etc. Each meets the needs of specific use cases.

### Side chain

Mechanism for developing a chain alongside the main chain, and the possibly reintegrating it..



# Blockchain: what you need to remember

Here is a quick and easy reference guide for this technology, which you could soon find very close to you.

## What it is

A blockchain is an intelligent, chronological, distributed, and verifiable asset log that is protected against any falsification by a trusted system distributed on constituent nodes. The blockchain manages a secure, decentralized chronology of all transactions performed since the start of the distributed system.

Transactions submitted by a user network are documented in information "blocks," which are sequenced together by referencing the secure ID of the previous block. The perpetually growing chain is maintained by a peer-to-peer network of specialized calculation nodes, but each user can access the entire log at any time and view it. Blockchain technology can be defined in three different ways:

- Functionally: An active, chronological, distributed, and verifiable log that is protected against any falsification by a distributed trust system.
- Technically: A combination of paradigms: network application (P2P), distributed database, block processing, asymmetric cryptology, self-execution (Event-Driven), and Proof-of-Work.
- Socially and economically: A trusted operation that allows a group of people to exchange assets securely without using an intermediary.

## What it is not

It is not a database, at least not in the traditional sense. Data does not reside in a single location or on a central server. The blockchain is replicated over the entire network and therefore does not require a centralized "authority" to store and secure it. And it is no longer just bitcoin, which is only one application of bitcoin technology. However, alternative currency has played a key role in demonstrating the value of blockchain and its possible applications.

## Benefits

One of the primary benefits of blockchain is trust. While traditional databases require secure access to a central server, trust in blockchain technology is inherent in transactions, which are secured by cryptographic systems, using many transactions over the Internet. The non-use of a trusted third party makes it possible to automate processes and thus drastically reduce costs.

Other benefits include transparency (all transactions are visible to all participants) and inalterability. It is practically impossible to modify transactions without being detected, which virtually eliminates the possibility for fraud and censorship. We should also mention the availability, maintainability, and interoperability of the blockchain, which reduces interface costs with various fragmented protocols since it automates and replaces them.

DXC.technology

For more information about this paper, contact
Michel Khazzaka, Partner, Banking & Payments.
mkhazzaka@dxc.com

**About DXC Technology**

As the world's top independent IT services company, DXC Technology (DXC: NYSE) helps its clients harness the power of innovation to thrive on change. Created by the merger of CSC and the Enterprise Services division of Hewlett Packard Enterprise, DXC Technology serves nearly 6,000 private and public sector clients in 70 countries. Our technology independence, global talent, and extensive partner network allow us to offer advanced and powerful IT solutions and end-to-end services. DXC Technology is recognized among the world's best corporate citizens. For more information, visit www.dxc.technology