



OECD **BLOCKCHAIN** POLICY FORUM

Distributed Ledgers:
Opportunities and Challenges
4-5 September 2018 | Paris - France



OECD **BLOCKCHAIN** PRIMER

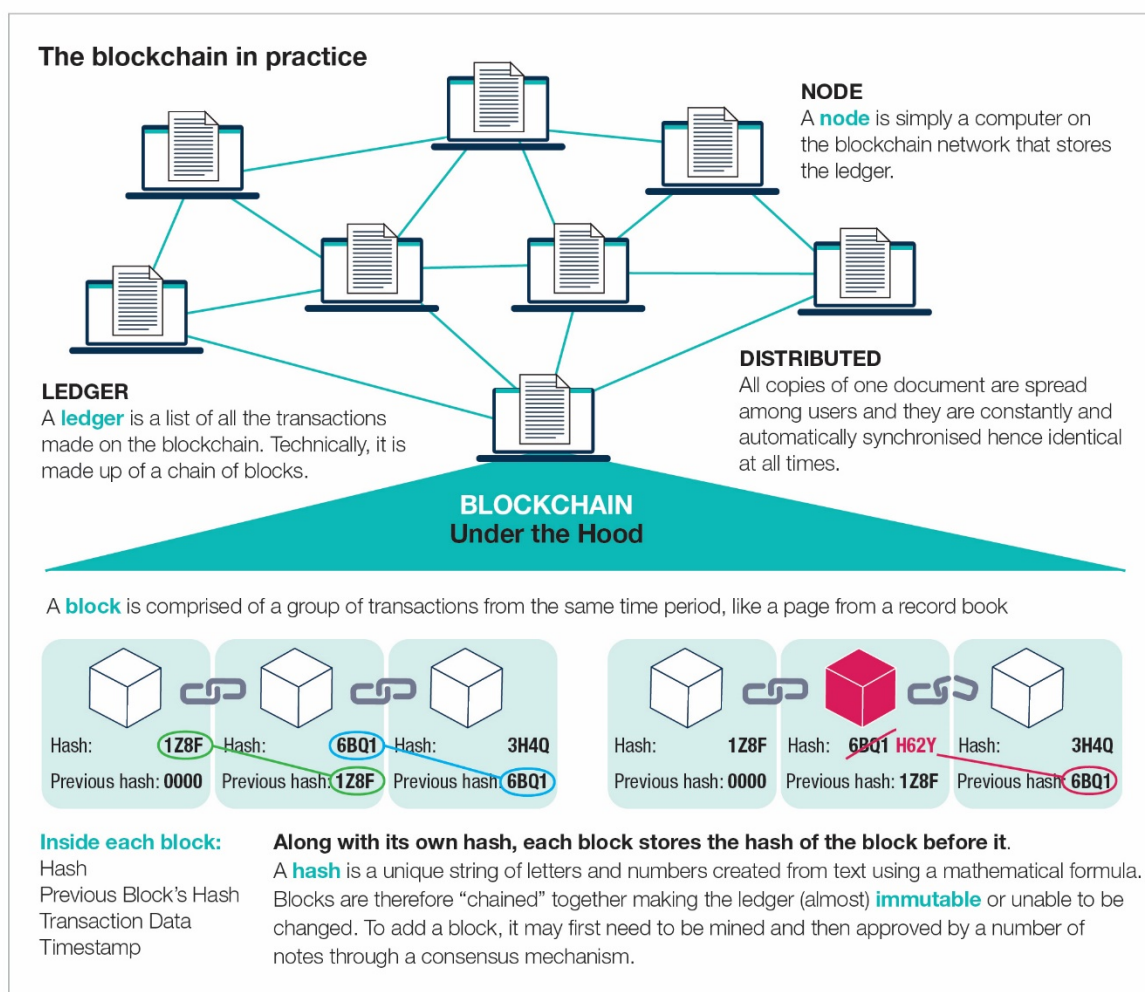


The OECD Blockchain Primer

This Primer provides an introduction to blockchain technology, outlines some of the potential benefits it can bring, and considers the risks and challenges it poses. While not comprehensive, it is an overview of the key concepts and terms intended to help people better understand this emerging technology and its growing impact.

A technology? A currency? The new internet?

Blockchain has the potential to transform the functioning of a wide range of industries. Its features can increase the transparency and traceability of goods, data and financial assets, facilitate market access and improve the efficiency of transactions. Fulfilling blockchain's potential, however, depends on a policy environment that allows innovation and experimentation, while balancing the risks of misuse. Governments will play a significant role in shaping policy and regulatory frameworks that help address challenges presented by the technology, and foster transparent, fair and stable markets as blockchain develops.



Fundamentally, blockchain is a combination of already existing technologies that together can create networks that secure trust between people or parties who otherwise have no reason to trust one another. Specifically, it utilises *distributed ledger technology* (DLT) to store information verified by *cryptography* among a group of users, which is agreed through a pre-defined *network protocol*, often without the control of a central authority. The marriage of these technologies gives blockchain networks key characteristics that can remove the need for trust, and therefore enable a **secure transfer of value and data directly between parties**.

Due to this unique ability, blockchain can diminish the role of intermediaries, who can command market power and collect significant fees, slow economic activity, and are not necessarily trustworthy or altruistic keepers of personal information. Although mostly known for its digital financial asset applications (like Bitcoin), blockchain technology is poised to have an impact on a wide range of sectors. The OECD is exploring its policy implications in a variety of areas including health, transportation, agriculture, environment, and supply chain management.

What is a blockchain?

A blockchain is a shared **ledger** of transactions between parties in a network, not controlled by a single central authority. You can think of a ledger like a record book: it records and stores all transactions between users in chronological order. Instead of one authority controlling this ledger (like a bank) an identical copy of the ledger is held by all users on the network, called **nodes**.

Different types of blockchain

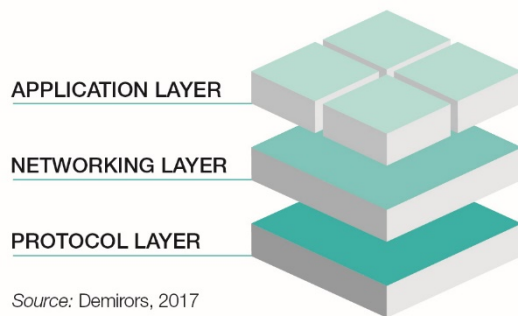
Before going further, it is important to note that not every blockchain is made the same. While there are a number of variable features, two of the most important are the “**openness**” of the platform (public or private) and the **level of permissions required to add information** to the blockchain (permissioned or permissionless). **Public** blockchains (like Bitcoin) are open for anyone to read and view, while **private** blockchains can only be viewed by a chosen group of people. Similarly, **permissioned** blockchains permit just a select group of users to write (i.e. generate transactions for the ledger to record) and commit (i.e. verify new blocks for addition to chain). In contrast, **permissionless** blockchains allow anyone to contribute and add data to the ledger.

Table 1. The main types of blockchain segmented by permission model

			READ	WRITE	COMMIT	EXAMPLE
Blockchain types	OPEN	Public permissionless	Open to anyone	Anyone	Anyone	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Supply Chain ledger for retail brand viewable by public
	CLOSED	Consortium	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger
		Private permissioned (“enterprise”)	Fully private or restricted to limited set of authorised nodes	Network operator only	Network operator only	External bank ledger shared between parent company and subsidiaries

Source: Hileman & Rauchs, 2017

The layers of blockchain



Blockchain comprises of three layers that each add different components to its development. As you can see, it is not necessary to get involved in the most technical layers in order to develop an application or use the blockchain.

The **protocol layer** lays the foundational structure of the blockchain. It determines the computing language the blockchain will be coded in and any computational rules that will be used on the blockchain.

The **networking layer** is where the rules set up on the protocol layer are actually implemented.

The **application layer** is where networks and protocol are used to build applications that users interact with.

Blockchain's key characteristics

Distributed

One of the core aspects of a blockchain is that it is a distributed ledger, meaning that the database is maintained and held by all nodes in the network. No central authority holds or updates the ledger, rather each node independently constructs its own record by processing every block (group of transactions), deciding if it is valid, then voting via the **consensus mechanism** on their conclusions. Once a change in the record is agreed, each node updates its own ledger. In contrast, traditional databases are stored and maintained centrally, which can make them high-value targets for hackers and criminals.

Immutable

In general, once a transaction is added to a blockchain ledger, it cannot be undone. This immutability is one of the principal aspects that contribute to the trustworthiness of blockchain transactions. A blockchain's immutability is secured through its use of cryptography (see below for an explanation of **hashing**). In a traditional, centralised database an authorised user can connect to the server to add or modify the data without other users' approval or detection. Because all of the data is held in one place, if the security of the server or the authority that runs the server is compromised, data can be modified or permanently deleted. This may sometimes be irreversible and occur without anyone realising it.

Agreed by consensus

No block can be added to the ledger without approval from specified **nodes** in the network. Rules regarding how this consent is collected are called **consensus mechanisms**. Consensus protocols are crucial in ensuring that every block is valid and that all participants agree and maintain the same version of the ledger. They heavily affect the incentives for nodes to be act honestly and are therefore the most important variables when designing a blockchain.

Misconceptions about blockchain

Pseudonymous

Contrary to popular belief, in general, blockchain technology does not allow its users to be totally anonymous. Rather, public blockchain platforms tend to be **pseudonymous**: user identities can be anonymous but their accounts are not, as all of their transactions are visible to all other users. On these platforms, user accounts can be created without any identification or authorisation process. This allows users to use a pseudonym. **Permissioned** blockchains can require a user's identity to be verified before they are able to access or use the blockchain.

...Well "almost" immutable...

While rare, it is possible for the blockchain to be compromised if nodes pool their resources and collude to approve incorrect ledger entries. However, the larger the network, the more difficult it becomes to carry out this attack. In most systems, it would cost the attacker many more resources to carry out the attack than they would gain from the attack itself. Additionally, some **private blockchains** allow for central authority nodes to change information on the ledger. Lastly, advances in quantum computing (supercomputing) threaten some current cryptographic security measures, but there is equally the likelihood that blockchain's security will evolve with quantum computing capabilities

Blockchain under the hood: How does blockchain actually work?

Hashing: a cryptographic fingerprint

A hash is like a digital fingerprint; it is unique to each piece of data on the blockchain. Users put information regarding their transaction (name of receiver and sender along with the amount transferred) into a cryptographic hashing algorithm – a complex mathematical formula – and receive a set of letters and numbers that is distinct to that transaction. The specific input, if unchanged, will always produce the same exact hash. If, however, any part of the data input is changed (for example a malicious actor changes the amount transferred), the hash would change to an entirely different set of characters and make it incompatible with the rest of the chain. Therefore, even without seeing the details of the transaction, nodes can quickly tell that the data within the block has been tampered with and reject that version of the ledger. It is this cryptographic security that makes blockchain ledgers more trustworthy and (almost) **immutable**.

Examples of Hashes

Input	Hash Output (using SHA 256 algorithm)
OECD	879D5ACDCDA51A6F1B00EBFE77513D9B19F574499C867997EE1FB6B1FA6DDBB0
OeCD	19C91C8433AC66422E8B13A468B3E96D5D7924BEB1164F8412484900C7C1EDC6

Note: Even subtle changes like upper or lower case significantly alter the hash.

Mining

For some blockchains, in order to add blocks to the ledger transfers must go through a mining process. Mining is method of adding transaction records, via blocks, onto a public ledger. Miners are nodes in the network that ensure the transactions in the block are valid. Specifically, they ensure the sender has not already used the funds it wants to send to the receiver. Once they finish the verification, they have to ask the network for **consent** to add it to the ledger. In order to do so, they have to follow the **consensus mechanisms** chosen for the platform.

Consensus

As mentioned before, one of blockchain's key characteristics is the consensus mechanisms it uses to gather consent. Agreement among nodes regarding the "state" of the ledger is essential for the function of the blockchain ledger. The bitcoin blockchain utilises a consensus model called Proof of Work, which requires the miner to compete against other miners to create and broadcast blocks for approval. If successful, they are rewarded in Bitcoin. There are other consensus mechanisms like Proof of Stake, Proof of Authority, Proof of Elapsed Time, and Proof of Burn – all of these are variations on the means for the network to agree on changes to the ledger.

What are Digital Financial Assets?

A digital asset that works as a medium of exchange.

The term *tokenisation* describes the process of transferring rights to a real world asset into a digital representation – or token – on the blockchain. Being in possession of that digital token then gives you the right to that asset and the ability to trade and track it digitally.

The three main types of token are:

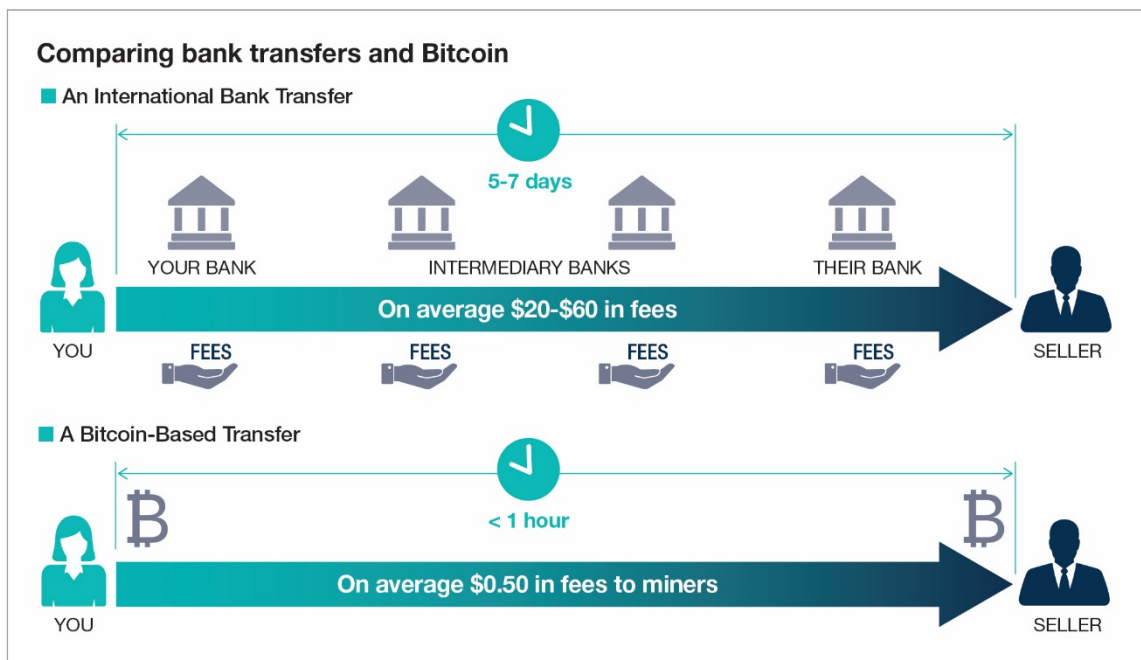
<p>Payment Tokens Commonly known as a cryptocurrency, a payment token can be a store of value and a unit of measurement. <i>e.g. Bitcoin</i></p>	<p>Utility Tokens A token that represents a right to a good or service, similar to a gift card. <i>e.g. StorjCoin</i></p>	<p>Security Tokens A token that provides equity or equity like investment in a company. The holder of the token has rights to the company's future profits <i>e.g. tZERO</i></p>
---	--	---

Why is this important? What can it be used for? One example: Bitcoin

In today's financial system, banks are an essential intermediary for financial transactions and transfers. They verify the identity of the sender, the ability of the sender to make a transfer (i.e. a sufficient account balance) and accuracy of the recipient's address. In this context, the bank acts as the only trusted third party.

However given the bank stores all data on a single centralised ledger, it therefore creates a **single point of failure**, whereby hackers or malicious actors can direct all their efforts for cyberattacks or manipulation to this specific entity. Additionally, these financial intermediaries charge **fees** to process transactions. In the case of international remittances, these fees are significant compared to the overall value of the transaction.

It was in this environment that the first blockchain application, a digital currency (cryptocurrency) called **Bitcoin**, was born. It created a peer-to-peer currency that enables users to transfer value to one another without having to go through a bank. Due to Bitcoin's use of cryptographic hashing, mining, and consensus mechanisms, users are able to verify transactions without needing a central authority controlling a single ledger.



Blockchain beyond finance

Blockchain technology goes far beyond cryptocurrencies and tokens, and its usefulness as a wider economic and administrative tool is well worth exploring. The table below describes just a small sample of blockchain’s potential to transform supply chains, healthcare and the energy sector.

Table 2. Examples of blockchain’s potential in supply chains, healthcare and the energy sector

Policy Area	Description	Potential Benefits	Potential Risks/Obstacles
Due Diligence in Supply Chains	Blockchains allow multiple parties to access the same database to track and record and audit products as they move along the supply chain	<p>Enhanced Transparency A more transparent supply chain will help companies and consumers identify risks of adverse impacts (i.e. human rights abuse and financial crime), and on that basis, prioritise further efforts to prevent or mitigate such risks.</p> <p>Sharing Value of Due Diligence Using blockchain technology to tokenise due diligence data (attaching a monetary value to access to the data), could potentially help fund due diligence efforts.</p> <p>Financial Inclusion Blockchain technology can lead to greater integration of informal actors and SMEs in the formal supply chain by helping overcome cash flow barriers through self-executing smart contracts.</p>	<p>Difficulty Controlling Data Quality Widely known as the “Garbage in Garbage Out” issue where the information entered on the blockchain is only as good as its source.</p> <p>Upfront Costs and Lack of Access In order to link the physical world to the digital, supply chain stakeholders have to invest in technology as well as facilitate access to and encourage uptake of the technology.</p> <p>Fragmentation Despite being created for very similar purposes, multiple blockchain initiatives have developed, operating on different platforms, identifying and collecting information differently, and with different governance structures.</p>
Healthcare	Blockchain could be used to provide more robust Patient Healthcare Information data management systems. Instead of medical information being siloed, patients and healthcare providers can choose what they share with whom.	<p>Continuity of Care Information can be shared between different healthcare stakeholders and end users could find it easier to share information to new providers.</p> <p>Cost Effectiveness Providing better data sharing between stakeholders can increase the ability of health care organisations to provide cost effective care and reduce clerical errors that are at best inefficient and at worst life threatening.</p>	<p>Privacy rules While some healthcare blockchain solutions will make only high level demographic information publicly viewable, it is conceivable that the combination of demographic data and geographic location could reveal sensitive information</p> <p>Data security Given the information stored (or linked onto the blockchain) is highly sensitive, data security is a potential risk.</p>
Energy	Blockchain can enable decentralised peer-to-peer electricity markets, allowing individuals and entities to balance supply and demand and trade electricity without going through a central entity.	<p>Lower Transaction Costs Without intermediaries, costs can be significantly reduced along the electricity value chain. This could potentially lead to more competition and a broader range of options for consumers.</p> <p>Facilitating distributed and low carbon electricity Blockchain could reduce the complexity of managing systems with large numbers of small-scale renewable and distributed energy resources, accelerating their deployment.</p>	<p>Scalability and technical performance As is, several types of blockchain have difficulties scaling (for example, due to data volumes and transaction speeds).</p> <p>Energy consumption To reach scale in energy applications, blockchain technologies will have to develop less energy-intensive frameworks for processing transactions.</p>

Blockchain beyond borders

The areas where major blockchain progress is taking place are as diverse as the applications they are creating. The global nature of blockchain's development can help distribute opportunities for wealth creation and economic development more widely than before. It is important for governments to develop the right policies to harness the potential benefits of this technology while mitigating its risks and potential for misuse. To do so, it is essential for countries to cooperate in order to share best practices and ensure interoperability. Regulatory fragmentation will hinder the progress towards useful applications of blockchain technology.

Figure 3. The global development of blockchain



Note: The economies engaged in different stages of using blockchain include: Argentina, Australia, Austria, Barbados, Belgium, Bermuda, Brazil, Cambodia, Canada, Chile, China, Denmark, Estonia, Finland, France, Georgia, Germany, Ghana, Hong Kong (China), India, Israel, Japan, Kazakhstan, Kenya, Luxembourg, Malta, Mauritius, Mexico, Netherlands, Norway, Palestinian Authority, Papua New Guinea, Russia, Senegal, Singapore, South Africa, South Korea, Sweden, Switzerland, Thailand, Tunisia, Ukraine, United Arab Emirates, United Kingdom, United States, Venezuela.

Source: OECD calculations based on data collected by the Illinois Blockchain Initiative.

<https://illinoisblockchain.tech> and <https://bit.ly/blockchain-govt-tracker>

The role of the OECD

The OECD provides a forum for discussion, sets international standards, and helps build capacity in governments – and is bringing these core competencies to the opportunities and challenges presented by blockchain. It is already helping governments find the right experts and practitioners to engage with, consider the need for cooperation in the international policy environment, and identify and share best practice for governments managing and using blockchain.

An integrated and holistic approach is key to maximising the benefits of this technology, both between sectors and between markets. The OECD's multidisciplinary expertise and deep links with industry, academia, governments and other international organisations mean it is able to join the dots for domestic priorities and global actions. If blockchain is going to be one of the transformative technologies of our time, the OECD is here to make sure governments are ready.

References

Berryhill, J., T. Bourgery and A. Hanson (2018), "Blockchains Unchained: Blockchain Technology and its Use in the Public Sector", *OECD Working Papers on Public Governance*, No. 28, OECD Publishing, Paris, <https://doi.org/10.1787/3c32c429-en>.

Demirors, Meltem (2017), *Oxford Blockchain Strategy Programme*, Saïd Business School, University of Oxford, UK, last accessed 7 August 2018 <https://www.getsmarter.com/presentations/uk/oxford-said/what-stakeholders-are-involved-in-the-blockchain-strategy-system>

Hileman, G., Rauchs M. (2017), *Global Blockchain Benchmarking Study*, last accessed on June 2018 https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf

Pike, Chris (2018), "Blockchain Technology and Competition Policy", *OECD Issues Papers on Competition* last accessed on 7 August 2018, [https://one.oecd.org/document/DAF/COMP/WD\(2018\)47/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2018)47/en/pdf)

Ray, Shaan, (2017) "Blockchain versus Traditional Databases", Online, last accessed 7 August 2018, <https://hackernoon.com/blockchains-versus-traditional-databases-cla728159f79>

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries. This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.