The potential of distributed ledger technologies in the fight against corruption.

Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

IMPRINT

As a federally owned enterprise, GIZ supports the German Government in achieving its objectives in the field of international cooperation for sustainable development.

Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn, Germany

Friedrich-Ebert-Allee 36 + 40
53113 Bonn, Germany
T +49 228 4460 - 0
F +49 228 4460 - 1766

E info@giz.de
I www.giz.de

Programme/project description:
Division Global Policy, Governance
Section Governance, Human Rights
Anti-Corruption and Integrity Programme
E: anticorruptionprogramme@giz.de

Responsible:
Nicole Botha, Anti-Corruption and Integrity Programme

Commissioned Author:
Niklas Kossow, Hertie School of Governance, Berlin - Germany

Design/layout:
Jeanette Geppert – pixelundpunkt kommunikation, Frankfurt

Photo credits/sources:
Cover © GIZ / Florian Kopp, p. 4 © GIZ / Thomas Imo/photothek.net, p. 9 © GIZ / Gerdhard Sippe, p. 10 © GIZ / Michael Duff, p. 15,16 © GIZ / Dirk Ostermeier

On behalf of
German Federal Ministry for Economic Cooperation and Development (BMZ)
Division 400: Sectoral and thematic policies, governance, democracy and rule of law
Bonn

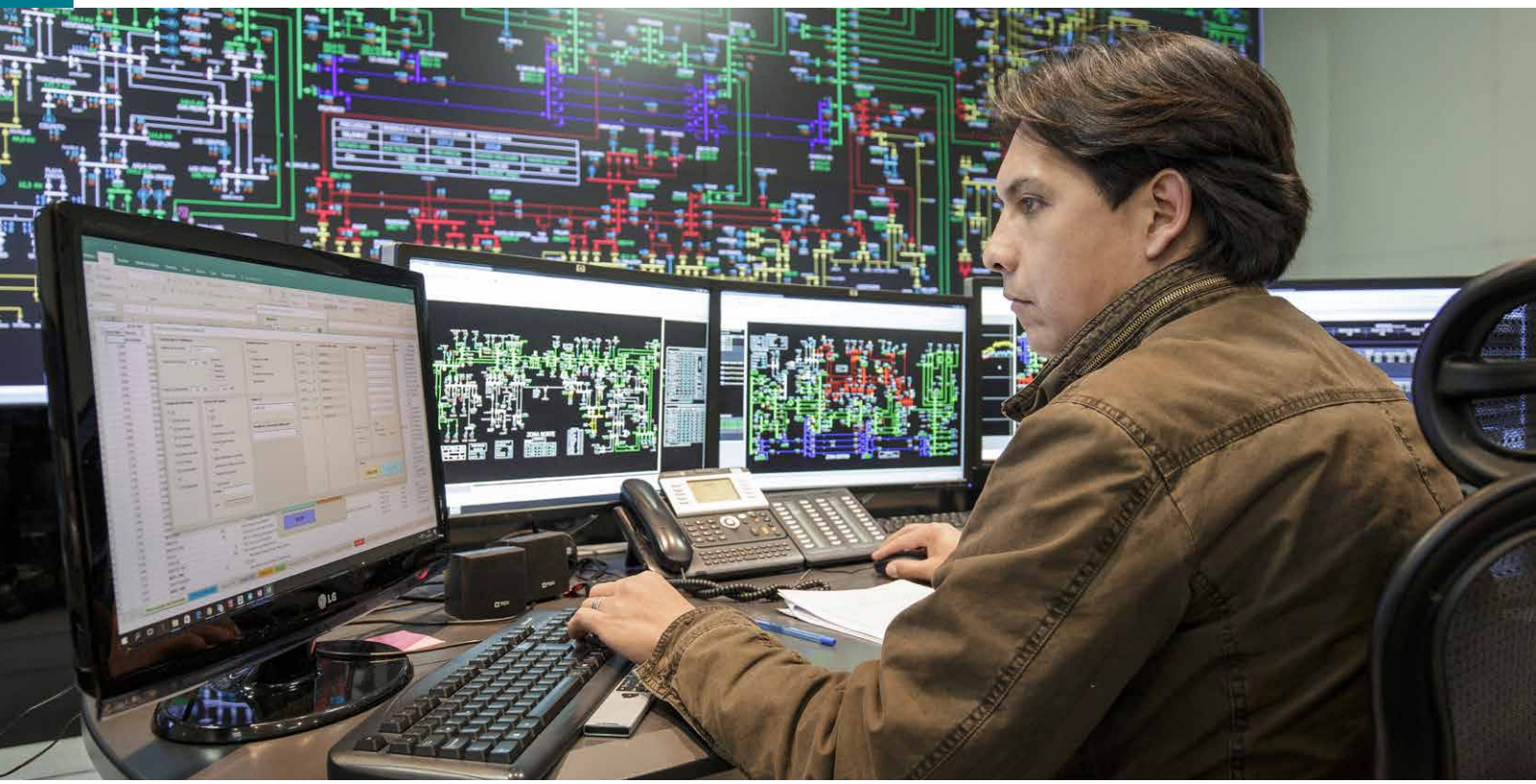
GIZ is responsible for the content of this publication.

Bonn and Eschborn, April 2020

Disclaimer

The publication "The potential of distributed ledger technologies in the fight against corruption" was commissioned by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, Anti-Corruption and Integrity Programme, on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ). The contents of this publication do not represent the official position of neither BMZ nor GIZ.

INTRODUCTION



Over the past two decades, academics and development practitioners have written extensively about the harmful impact of corruption on economic development and social outcomes. From an economic perspective, corruption diverts resources away from their most productive uses, acting as a regressive tax that supports the lifestyles of the elite at everyone else's expense. Corruption undermines the legitimacy of political systems by providing the elite with alternative ways of holding on to power, rather than through genuine democratic means.

This situation has brought the question of how best to combat corruption to the forefront of the international development agenda. In recent years, the debate has also turned to the use of digital technologies and new approaches that can be applied to anti-corruption. Since 2017, increased attention has been paid to distributed ledger technology (DLT), often referred to as blockchain, with discussions on whether or not it can play a role in combating corruption. This study seeks to answer this question by looking at three specific areas: supply chains, aid delivery and public administration. It will evaluate whether DLT can indeed help to address corruption in each respective context. These three areas are key in development cooperation and offer much scope for the implementation of DLT. For each area, the paper will analyse the corruption risks, highlight which of these could be lowered by employing DLT and illustrate each with real-life examples.

Before looking at these specific use cases, the paper will briefly outline the key tenets of anti-corruption theory and explain the methods to analyse corruption risks. It will also provide a very brief explanation of how DLT works and how using it can enhance key anti-corruption programming principles. The study is based on in-depth desk research and various DLT project databases. Furthermore, it relies on a series of qualitative interviews with project leads and experts, which were conducted in April and May 2018. The study was commissioned by the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, on behalf of the German Federal Ministry for Economic Cooperation and Development (BMZ). It was first drafted as an extended, internal study and then adapted to this current format for publication.

ANTI-CORRUPTION PROGRAMMING AND CORRUPTION RISK ANALYSIS

For the past 30 years, an increasing number of scholars have looked at the nature of corruption and how best to address it through anti-corruption programming. Our interpretation of corruption and the way it develops has a strong impact on our chances of fighting it. In this context, there are two perspectives on corruption that stand out:

- **Corruption as a principal–agent problem**: this model looks at public officials and their relation to superiors and the public. One person or entity (the 'agent') is able to make decisions on behalf of, or that have an impact on, another person or entity (the 'principal'). Problems (corruption) arise when agents, who have access to information that is not available to the principals, ignore their mandate and act in their own best interests (Klitgaard, 1988).
- **Corruption as a collective action problem**: this model assumes that everyone involved – i.e. rulers, public officials and citizens – are 'maximisers' of their own self-interest. However, this does not mean that they are all, by definition, corrupt. Rather, according to collective action theory, rationality is understood to be 'bounded' – interactive or reciprocal – in the sense that it is highly dependent on shared expectations about how other individuals will act. In a context where corruption is the norm, principals are thus likely to be patrons of corruption themselves (Mungiu-Pippidi, 2013).

As Peiffer and Marquette (2018) point out, both perspectives are complementary rather than contradictory. They also posit the notion that corruption oftentimes provides solutions to problems and thus serves a societal function. Anti-corruption programmes should reflect all of these perspectives on corruption. The German Federal Ministry for Economic Cooperation and Development (2012) has addressed this in its nine guiding principles on anti-corruption. Among others, they stipulate that anti-corruption measures should strengthen transparency, participation, accountability and integrity and should be based on a systemic, risk-based approach.

Assessing specific corruption risks in particular areas is therefore a vital step in appraising the potential value of action to tackle corruption. This can also be helpful when evaluating a specific technology, such as DLT, and requires categorising the corruption risk factors, i.e. the attributes, characteristics or factors of an individual, institution or process, which increase the likelihood of corrupt behaviour (Mills May, 2012). They can be monitored from different perspectives: one being the way in which they contribute to the wrongdoing, either by enabling corruption or by failing to contain it, thus perpetuating the phenomenon; the other is at the level at which the corruption can occur. The Table summarises the main types of corruption risks identified in the relevant literature according to the level at which they occur (*see page 6*). It must be emphasised, however, that there is no exhaustive and universal list of corruption risks and that concrete corruption risks and risk factors can only be determined by conducting assessments that consider the specific circumstances and characteristics of the organisation, sector, project or process in question.

Factors that encourage corruption at different levels of decision-making.

LEVEL	DEFINITION	SPECIFIC RISK FACTORS
CONTEXTUAL FACTORS	Factors outside the organisation or sector's control	• unclear or inconsistent legislation regulating a certain sector or field of work • absence of basic legal framework needed to fight corruption and strengthen integrity • authorities' powers are unclear • work of public sector institutions has not been aligned or reconciled • inefficient law enforcement and prosecution • inefficient or incompetent oversight institutions or supervisory authorities • non-transparent public finance processes • poor or wrong understanding of proper public sector functioning
ORGANISATIONAL FACTORS	Factors within the organisation or sector's control that are the result of their action or inaction, such as the rules and policies on good governance, management, decision-making, operational guidance and other internal regulations	• poor strategic and operational guidelines (policy) or inadequate policies, procedures or systems • chronic failure to follow existing policies, procedures or systems • institutions, projects, etc. have unclear mandates • poor or inconsistent internal rules and regulations • absence of warning and alert systems in the event of irregularities • weak managerial and administrative anti-corruption measures • inadequate/weak review, supervision, oversight and control procedures and audit mechanisms • absence of rules and procedures that promote ethical behaviour and transparency • inadequate or insufficient system for training and educating public officials, including superiors and supervisors • inadequate human, finance or time resources in the organisation or its teams • high levels of power or influence, not consistent with their actual position
INDIVIDUAL FACTORS	Factors that could motivate individuals to engage in corrupt or unethical behaviour	• lack of knowledge (ignorance) • lack of integrity • lack of practical skills • pressures in the work environment • inadequate supervision or performance review • inappropriate relationship with clients • omission of conflict of interest declarations • feelings of dissatisfaction or perceptions of unfairness at work
WORKING PROCESS FACTORS	Factors that arise from working procedures in an organisation	• high levels of personal discretion • non-transparent or unrecorded decision-making • poor organisation of work processes • unconnected work process and procedural gaps • lack of vertical and horizontal checks in the work process

Source: Adapted from Selinšek, 2015

These factors will form the basis for an evaluation when examining the use of DLT in the context of supply chains, aid distribution and public administration. For each of these areas, this paper will present a brief analysis of corruption risks and then show to what extent the use of DLT could address these.

BLOCKCHAIN AND DISTRIBUTED LEDGER TECHNOLOGY AS AN ANTI-CORRUPTION TOOL

DLT refers to a data storage system that uses a peer-to-peer network of independent computers owned by independent entities, referred to as nodes, rather than a centralised server infrastructure. It is used to record transactions and share them across a network of participants. The most well-known type of DLT is blockchain, which was developed as part of the Bitcoin digital currency system and published in a white paper by Satoshi Nakamoto[1] in 2008. The technology provided the answer to a hitherto unresolved challenge of digital currencies: how can trust in a currency be established without relying on a central authority? In other words, how do you prevent a unit of a digital currency from being spent twice, without a central authority validating the transactions?

In a DLT system, transaction data is stored simultaneously across a network of distributed nodes. It is often referred to as blockchain since in the most common types of DLT transactions, data is structured in blocks. This can technically be any kind of data small enough to fit in the block.[2] However, since there are also distributed ledger technologies that avoid data being stored in blocks, the term DLT is more inclusive.

Key to the operation of distributed ledger systems is a consensus mechanism that ensures that nodes verify the data and agree which data will be stored. The way this mechanism operates varies between different types of DLT or blockchain solutions and is typically based on cryptography. It prevents unauthorised copies of the ledger's digital entitlements from being created or transferred simultaneously to more than one party. The consensus mechanisms ensure these systems do not rely on a single trusted third party authorising the transactions. They are thus a necessary element of DLT. While this can seem like a complex way to store data, these systems enable the secure verification of transactions without relying on a trusted third party. They therefore help to build trust in the distributed data storage system without requiring a central authority to provide this trust.

Deciding which is the most appropriate consensus mechanism to use depends very much on how access to the respective DLT system is implemented, especially when deciding who has access to the respective system. It also helps to distinguish between different types of systems. In a public blockchain, a node can be any computing device able to connect to the network. In a private or permissioned ledger, they are computing devices which have been granted access by the system's owners. The latter is thus less inclusive but can oftentimes use more efficient algorithms. In most cases, participating nodes store full copies of the data on a blockchain, therefore these systems avoid the risk of one single point of failure and promise more efficient data handling. Hybrid blockchains combine elements of both public and private blockchains.

An important use of DLT are so-called smart contracts. These are contracts which are written in computer code and stored on a DLT system. They are designed to be self-executing, which means that their code stipulates that they are only initiated once certain specified conditions are met. Smart contracts can be highly complex as they are subject to a variety of conditions being met to unlock some sort of value.

While it is important to understand the differences between types of DLT systems, this paper cannot go into more detail on how they function or which cryptographic algorithms they use. It is sufficient to summarise DLT systems as distributed data storage systems that provide a means to avoid middlemen and enable an exchange of data between a variety of players.

1 Satoshi Nakamoto is a pseudonym. The true identity of the person who created bitcoin has not been established.

2 The block size varies between different blockchains. On the bitcoin blockchain, it has been increasing over the years but has remained fairly constant since mid-2016 at about 0.8–1.2MB. This means around 1,500–2,000 transactions per block, as noted by https//www.blockchain.com

Attributes of DLT and their link to anti-corruption

When applied in use cases and specific applications, a number of attributes can thus be assigned to DLT which distinguish it from other data storage solutions:

DISINTERMEDIATION: A core feature of all types of DLT is the removal of a single point of failure and a central authority that could be attacked. Private blockchains also avoid a centralised server architecture, even though a central authority decides who can access the system. Disintermediation has two key advantages:

- **Security:** distributed ledgers are less vulnerable to attacks, in particularly to DDoS[3] attacks (Rodrigues et al., 2017). A distinction can be made between increased *external* security, in which records are protected from outside attack and increased *internal* security, in which distributed ledgers make it harder for people within an organisation to tamper with the data. With permissioned ledgers, the number of nodes is limited, which makes them more vulnerable to outside attacks, but also limits potential legal challenges, such as privacy concerns or questions about data sovereignty and storing data in other jurisdictions. They also limit data access by third parties.
- **Efficiency:** by-passing an intermediary and connecting individuals directly can lead to considerable efficiency gains and fast transaction times. This, however, depends very much on the type of consensus-building mechanism, the transaction rate and the costs involved. Public blockchains tend to be considerably less efficient than permissioned blockchains. By-passing intermediaries can, nevertheless, help to design systems that have fewer bottlenecks.

IMMUTABILITY: once data is entered on the blockchain, it cannot be changed. The use of cryptography and the way the data is linked prevents it from subsequently being altered. The time and origin of the data can also be determined. Attributing the origin of the data can be easier in permissioned blockchains as public blockchains are technically also open to users who hide behind pseudonyms.[4] The immutability of the data can have two significant advantages:

- **Accountability:** transactions can be assigned to a device or person that entered the data at a specific point in the distributed ledger and at a specific time. These individuals can also be linked to the data and held to account. Fraudulent data can be detected more easily and more accurately and fraud can be attributed.
- **Trust:** there is more trust in the system as the data cannot be changed once it has been entered onto a blockchain. While this is a vital feature of cryptocurrencies, it can also be a positive attribute in other DLT use cases. They can provide a way to monitor the data that is being stored, trusting that specific data has not been manipulated. This, of course, requires the data being available to be read by anyone or on there being inbuilt audit mechanisms. It also does not guarantee that the data is accurate when it is entered. If corrupted data is entered on a DLT system, it will remain corrupted. It is more likely that this data entry will be able to be attributed, but it does not change the quality of the data itself.

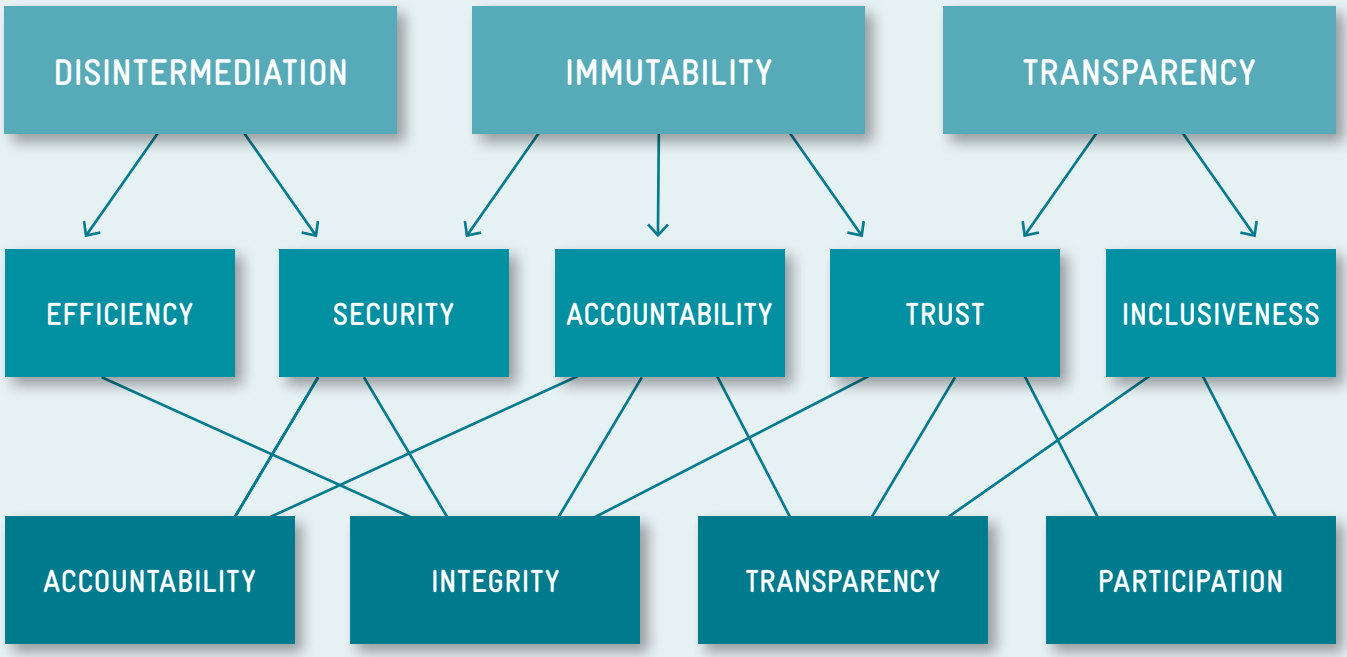
TRANSPARENCY: transparency plays an important role in public blockchains. All data is available to read (unless it is specifically encrypted) and transactions on the blockchain can be monitored by anyone in the system. This can build trust in the transactions that are recorded. Several researchers also argue that public blockchains lead to greater inclusiveness as technically anyone can validate the transactions. Transparency and inclusiveness are, of course, much more limited in permissioned blockchains. Yet, these attributes can be stipulated through specific design principles that factor these in mind. They can also increase transparency and trust between cooperating partners using a permissioned ledger.

As has been pointed out, the prevalence of the attributes outlined here differs between DLTs. The Figure *on page 9* shows how DLT's three core principles are linked to anti-corruption principles. These are four principles that form the cornerstone of the BMZ's Anti-Corruption Strategy: transparency, participation, accountability and integrity (Federal Ministry for Economic Cooperation and Development, 2012).

3 In Distributed Denial-of-Service (DDoS) attacks a large number of computing devices are coordinated to all try and access a service (often an internet server) at the same time, causing it to crash due to the overload, thus making its data unavailable.

4 Pseudonymity in DLT systems is often mistaken for anonymity. Apart from some digital currencies, which are built to secure anonymity, the origin of transactions generated by the nodes within the system can clearly be traced. Often, however, pseudonyms are used which make specific attribution difficult. Because of this, many people expect cryptocurrencies to be used to facilitate illicit financial flows or money laundering. However, law enforcement bodies in several countries have pointed out that attribution actually becomes much easier if, for instance, bitcoin is used for money laundering purposes: identities can easily be attributed by transaction patterns and data is then stored in an immutable ledger, making it possible to use it for prosecution purposes (Kossow & Dykes, 2018).

Links between key blockchain attributes and anti-corruption principles



POTENTIAL APPLICATIONS OF DLT IN ANTI-CORRUPTION

So far, this report has looked at the theoretical potential of DLT in tackling corruption, as well as the basic concept of anti-corruption theory and corruption risk analysis. It will now consider three fields that are vital to development cooperation: supply chain management, aid delivery and public administration. For each field, the report will briefly outline the corruption risks, present examples of DLT use cases and give a short evaluation of how far corruption risks could be addressed in the cases being examined. In analysing corruption risks, the report relies on the methodological scheme outlined above to support its analysis.

Supply chain management

Corruption risks

Supply chains form an important backbone of the world economy. Their sustainability and integrity have an impact on the livelihoods of most of the world's population. Yet corruption can arise in supply chains for a number of reasons.

First, supply chains typically involve a multitude of stakeholders, both public and private. In many cases, companies have an obligation and interest to exercise due diligence in order to prove to their customers, business partners and state authorities that they are using responsible supply chains. Section 1502 of the Dodd–Frank Act (2010), for instance, demands due diligence on the origin of tin, tantalum, tungsten and gold used by publicly listed US companies (Ayogu & Lewis, 2011). However, given the myriad of parties involved in any given supply chain, due diligence is increasingly difficult. Corruption risks are a significant factor: certificates of origin can be falsified, shipments changed, and fraudulent deliveries added to a supply chain in order to mask the true origin of the goods. This also applies to customs administration, which is an integral part of most supply chains and where discretion applied in processing the goods can result in a risk of corruption.

Second, a lack of transparency and complicated paper trails can make it very difficult to follow supply chains. A surprising number of supply chains still work with non-digital ledgers and, even if digitalised, the information is often stored in a variety of different formats: digital folders, email inboxes or even filing cabinets. This lack of transparency is also an issue for customs where corruption risks are especially high, as customs officials are in a position of power to extort bribes. Shipping companies are also known to use bribery to speed up processes (Albisu Ardigó, 2014).

Potential DLT applications and use cases

DLT-based supply chain management solutions could potentially lower these corruption risks as the distributed ledger is used to keep track of goods throughout the supply chain. The ledger in the context of these applications stores all the data on the provenance of the goods and thus makes it easier for businesses to track the goods as they are passed down the supply chain. In this context, we should draw a distinction between clearly identifiable goods and bulk goods. The first category includes industrial products, or parts with licence numbers or unique identifiers. Some raw materials can also be uniquely marked; diamonds, for example, often have unique identifiers which are engraved using a laser. Bulk goods that cannot be uniquely identified, on the other hand, include agricultural products such as coffee, sugar or fruit, but also minerals and metals, such as gold or tin. While these can often be traced back to their farm or mine of origin, it is also possible to mix them with other products or even mint them together. As a result, ascribing a specific origin in these cases is much harder than with uniquely identifiable goods. DLT solutions to manage supply chains for these goods thus take slightly different forms.

Uniquely identifiable products

DLT solutions are already being implemented for uniquely identifiable goods, in particular for diamonds. For several years, there have been attempts to keep so-called blood diamonds, gems from conflict-prone areas known to finance terrorist groups, off the world market (Orugun, 2004; Bieri, 2016). Furthermore, synthetic diamonds, which are sometimes hard to distinguish from authentic diamonds, have been brought onto the market. The certification and authentication of diamonds is thus vital to the trade and also prone to corruption risks. Everledger[5] is a UK-based start-up which uses a DLT application to keep track of diamonds, thus making it easier to verify their origin and authenticity. It aims to provide a global register to track diamonds and other valuable items. The company assigns each diamond an individual identifier based on the diamond's digital thumbprint. The diamond is registered on a blockchain with a certificate of origin for the rough diamond produced using the Kimberley Process[6] (Bieri, 2016). Data on the diamond and its ownership is transmitted to the Everledger network, which is hosted on the IBM Hyperledger Fabric,[7] a blockchain solution launched by IBM and that involves a myriad of companies. The blockchain here works as a hybrid blockchain solution. It offers a permissioned chain for certain participants. In addition, it offers a security layer that allows the authenticity of the transactions to be verified (Hyperledger, 2017). This system makes it possible to trace ownership and provenance and to verify authenticity when trading. The use of DLT ensures the data is made available to relevant stakeholders and is protected against any changes. This principle is also applied to other products which are uniquely identifiable, such as wines, art and other luxury items.

Bulk goods

As with diamonds, metals and minerals come from specific mines, yet their provenance is hard to trace. They are often brought from illicit origins into formal channels and turned into valuable assets by smelters and refineries (Bleischwitz et al., 2012; Koning & Enough Project, 2013). Since minerals and metals still need a certificate of origin, there is scope for corruption when obtaining one. To improve the tracking of their supply chains, Walmart,[8] along with several other companies, has proposed implementing blockchain-based solutions in their supply chains. The retailer has been working with IBM Hyperledger Fabric and has also been developing its own solutions to register food deliveries or packages on a blockchain and thus increase their traceability. Berlin-based start-up Minespider[9] suggests a similar approach for conflict minerals and is already running pilots with companies as large as Volkswagen (2019). To register minerals on the blockchain, they propose a mass balance approach: minerals produced at certified mines are weighed and registered on the DLT-based database using a smart contract containing encrypted information on the minerals, in particular on due diligence. This information is passed on as the minerals are traded. Which information is passed on can therefore be tailored to the needs in the supply chain: some can be made accessible to the public, some to all the stakeholders involved, some only to the next participant in the transaction. With bulk goods, it is almost impossible to ensure that only the certified goods are passed along the supply chain and that no other goods are sent in the delivery. The system suggested by Minespider, however, ensures that the original quantity of certified minerals matches the amount specified on the certificates from the original mines. The money for these minerals, matching the correct amount, can thus be passed on to the correct producer, thanks to the information stored on the blockchain. This according to *Minespider*, would fulfil the requirements in section 1502 of the Dodd–Frank Act (Williams, 2018).

5 http://everledger.io/

6 The Kimberley Process is a certification process for rough diamonds that was introduced in 2000 to reduce the circulation of conflict diamonds, see https://www.kimberleyprocess.com/

7 https://www.ibm.com/blockchain/hyperledger

8 https://www.hyperledger.org/resources/publications/walmart-case-study

9 http://minespider.com/

Corruption risks addressed

Considering the current use cases and potential blockchain applications, using a blockchain for supply management could address the following corruption risks:

Variety of parties involved: using DLT to track supply chains provides a solution to the challenge presented by the large number of parties involved in a supply chain. By providing one system, paper trails can be simplified and confusion reduced. Opportunities for corruption can arise from confusion: a lack of accountability and responsibility for the shipped goods or for the different stages in the supply chain. The use of DLT can help to lower these risks, provided that all stakeholders can be added to the system.

Reducing complexity: using one system that involves all the stakeholders to keep track of the supply chain reduces complexity as the systems are streamlined and easier to monitor.

Increasing transparency: since the accuracy of the supply chain records is improved and, thanks to DLT, they cannot be changed, it is much easier to understand where the products have originated, where any fraud might have taken place and where bottlenecks and hold ups might occur. Since a major problem is transparency at customs, keeping accurate records can also help to identify hold ups at customs and unusually long processing times.

DLT solutions are unlikely to address the corruption risks posed by individual and external factors in supply chain management. Individual motivation to engage in corrupt activities will also not be mitigated. However, DLT can make it harder to manipulate the supply chain data. With DLT, the legal, regulatory and institutional frameworks that shape the supply chains will largely remain unchanged. Since custom payments and systems are at present unlikely to be connected to a DLT system, many corruption risks in this area are not likely to be addressed through the use of DLT.

Aid delivery

Corruption risks

While there is no systematic evidence for it, several donor reports suggest that corrupt practices in aid delivery are not unusual. The most common corruption scheme in the context of aid delivery seems to take place in the form of bid rigging, which involves aid-funded projects being manipulated in order to be carried out by specific contractors. Bid rigging can involve bribery, nepotism and favouritism and often leads to overcharging or the questionable implementation of projects, often with money syphoned off for private gain. A lack of clear rules, policies and procurement procedures, as well as a comprehensive system of corruption risk management are a key driver of corruption in this area and aid is sometimes even seen to fuel corruption by providing additional resources (Heggstad and Frøystad, 2011; Hart, 2016).

Implementing projects on behalf of donor agencies often involves contact with the local government or authorities, a situation in which there is a high risk of corruption. Bribery also continues to be a problem as agency staff often have the discretion to award funding. While many of these problems come down to the individual agency, they are particularly pronounced in fragile states and contexts with weak administrative capacity (Chayes, 2016). Failing to keep records or falsifying documents can be a problem and incomplete paperwork can therefore increase the risk of corruption.

Potential DLT applications and use cases

Several organisational and working process factors can be addressed through DLT applications that have already successfully been tested. This includes the use of DLT in delivering aid to individuals and providing budget support or project financing. Using DLT can increase transparency and trust between partners and improve data handling. Smart contracts could also help to lower corruption in procurement, although there has not been much progress made on projects in this area.

Delivering aid to individuals

One of the most prominent DLT applications in the context of international development is the Building Blocks project implemented by the World Food Programme (WFP).[10] This project involves using a DLT-based application to facilitate the delivery of food vouchers to residents of refugee camps. Rather than receiving cash transfers, the refugees are given coupons that they can redeem in specific shops in the camp. Building Blocks gives an account to each refugee registered in the system, which currently covers more than 100,000 refugees in Jordan. When they spend money in the refugee camp's shops, the refugees identify themselves through an iris scan as they did before the Building Blocks project was introduced. Now, however, the transactions are recorded and deducted from the individual accounts which are

10 https://innovation.wfp.org/project/building-blocks

stored on a private blockchain. The actual payments from the World Food Programme to the shops are then executed as bulk rather than individual transactions. This leads to better documentation and considerably lower transaction fees, resulting in savings of around USD 40,000 per month. To record the transactions, the project uses a permissioned blockchain that strictly limits the number of nodes in the system and can only be accessed by the World Food Programme. The project was extended to include beneficiaries of UN Women in 2019, meaning that the agency is now also hosting some of the nodes in the Building Blocks system.

Providing budget support and project finance

A large amount of aid provided by donor agencies is not distributed directly to the beneficiaries on the ground, but rather in the form of project finance. As with all large payments, considerable corruption risks can arise in financing projects. DLT could be the solution to reduce these risks. The German development bank KfW has developed the TruBudget system to improve the management of project finance and workflows.[11] TruBudget is a blockchain-based workflow tool used to track the implementation of one or more development projects. A consortium blockchain serves as a ledger that allows partners to record transactions which show how projects are implemented and how money is spent. By using a custom-built application on a permissioned ledger, the system can give several participants access either to read or write on the ledger and can also customise who can change permissions. Nodes can be hosted both in the partner countries and with donors in order to build trust. TruBudget offers the possibility of following all workflows involved in a project: from budget allocation and project definition to tenders, contracts and reports/indicators and payment. By tracking all the transactions, the system creates greater transparency among project partners. Thanks to the use of DLT, projects can be followed up without the risk of paperwork being lost or falsified.

As an open source platform, TruBudget can technically be employed anywhere and easily adapted to specifications in different country contexts. KfW is currently undergoing different pilot phases in Brazil, Burkina Faso, Ethiopia and Georgia. These projects are bringing together state institutions and donors and TruBudget is being adapted to manage the workflow in several projects. Using the platform creates greater transparency and accountability between project partners. As a result, the donors are able to channel their funds directly through government accounts more easily. TruBudget thus enables donors to use the partner countries' systems thus providing more sustainable and efficient support. While not being the project's primary aim, it also contributes to better oversight and in turn helps to reduce corruption risks.

Corruption risks addressed

We can see how DLT applications address the risks of corruption when delivering aid.

Missing or fraudulent paperwork: Using DLT in the context of delivering aid can help to provide accurate documentation on the distribution of aid. Regardless of how aid is distributed – directly to individuals, through project finance or budget support – using DLT to document the process can help to show where the money has gone. DLT makes forging paperwork much harder and makes it possible to identify who entered what information into the system and when. If DLT documentation is made mandatory, the missing paperwork cannot be used as proof and forged documents can be traced back to the person who entered them into the system. While funds can still be diverted, DLT makes it easier to understand at what stage this happened.

Coordination: DLT applications can improve coordination between different project partners by providing a system that can integrate a variety of players. It is easier for them to coordinate as they are working on the same system and using the same data. Since a DLT-based system documents the work, the result is better and more complete project data. It can also lead to increased trust between the parties involved in the project as they are able to check each other's work. This would be a valuable asset in cooperation between donors and host governments and reduce corruption risks in this area.

However, it is important to remember that DLT can be used to lower corruption risks but it is unlikely to reduce corruption per se. Several risks remain – contextual factors and individual motivations leading to corruption will persist. Favouritism, for instance, is often hard to prove and corruption schemes are carefully designed. Dealing with unfamiliar partners can still be problematic and bid rigging in the context of public procurement, which is often subject to nepotism, remains an issue. While there are proposals to use smart contracts to reduce corruption risks in public procurement, at the time of writing there have not been any successful cases of using this technology for this purpose.

11 https://openkfw.github.io/trubudget-website/

Public administration

Public administration covers a broad range of public services and state agencies. This report focuses on upstream government bodies and refers to those dealing with central government functions (Manning & Holt, 2014), which includes public procurement and tax authorities, as well as the administration of government data. In these areas, public servants often have discretion when dealing with large amounts of public spending or income, or they handle data that is linked to financial incentives.

Corruption risks often arise where there is discretion over resources. This is often driven by overly complicated and lengthy processes. Excessive red tape creates corruption risks as more public servants are in positions to exploit processes for their own gain and people can be tempted to try and speed up processes through corrupt means. Another factor is a lack of documentation or fraudulent paperwork, as well as a lack of oversight. For civil servants, personal motivation to engage in corrupt behaviour can arise from low pay or personal relationships with service users or businesspeople. Added to which are the multiple layers of bureaucracy leading to further inefficiencies in the public service. DLT can help to address some of these risks, albeit to a limited degree. There is a large number of blockchain projects that deal with public administration functions. Here, we will present use cases that are concerned with the handling of data.

Securing government data

Some of the most advanced applications of early forms of DLT involved securing stored government data.[12] In several projects, this has been applied to land registries. This approach is taken by Bitland[13] in Ghana, Avalon-life[14] in Costa Rica and ChromaWay[15] in the Indian state of Andhra Padesh, among others. The best known of these projects is the Exonum[16] project in Georgia. It was implemented by the Georgian Government in cooperation with BitFury[17] and with technical legal assistance from GIZ.

Exonum takes a digitised version of the Georgian land registry and adds a security layer to it. Rather than storing actual data from the land registry on a blockchain itself, the system takes cryptographic images, so-called hashes, from land registry entries and stores them on a private blockchain. The hashes can be re-applied and used to identify potential data breaches and unwarranted changes in the land registry. Since the integrity of land certificates can be verified within seconds, this solution is much more efficient than other safety mechanisms. By allowing users to verify the authenticity of ownership certificates, it removes a roadblock in the context of land registries where verification could sometimes take days. Digitalising land registries with the help of DLT-based systems could be of particular interest in countries that do not yet have fully developed land registries and where corruption and land grabbing remain an issue.

Securing contracts

As previously mentioned, smart contracts are a key DLT application with potential in public procurement. This of course only applies to projects funded by international donor agencies or national governments. Whereas no specific use case could be identified, the potential is certainly there. In the context of land registries, however, there are precedents for the use of smart contracts. ChromaWay is also working on a project with the Swedish government to handle land sales using smart contracts based on a permissioned blockchain. The company argues that securing sales agreements between different parties is even more important than securing land titles, because the former are legally binding and often determine the outcome of a land dispute in court. The smart contract concept that ChromaWay put forward would enable different players to sign on using apps specialised for their role as buyers, sellers or money lenders. ChromaWay seeks to create a decentralised and efficient way to handle land sales. Using a digital identity, the seller and buyer can both log into the system, digitally sign the transactions and their banks can then confirm these transactions or confirm that they have granted the respective loan or mortgage. The Swedish land registry then receives a notification of the sale and transfers the deed to the house or land. This system would be built on a permissioned blockchain, which could potentially offer read access to everyone as house sales in Sweden are generally made public.

12 Estonia is often cited to have implemented a functioning blockchain as a security layer in its data exchange system. However, its system cannot be called a blockchain, although it is rather similar to one (Kivimäki, 2018). Whether to call the security layer in the Estonian system a blockchain is not only a question of semantics, but also highlights a key feature lacking in the system: the absence of decentralisation. Estonia relies on a centralised server architecture.

13 http://landing.bitland.world 14 https://avalon-life.io 15 https://chromaway.com 16 https://exonum.com/index 17 https://bitfury.com

Corruption risks addressed

The DLT applications highlighted above only focus on land registries as an example in the context of public administration. Yet, the principles of securing and improving data storage can also be applied to other fields and help to lower some corruption risks.

Control over data: public servants controlling specific data, such as entries to land registries, can prove to be a corruption risk in the absence of proper prevention and oversight mechanisms. Corrupt public officials could, for example, change data in exchange for a bribe or to extract undue benefits for themselves. DLT solutions have some potential to mitigate these risks. Depending on how they are implemented, they enable the public (if read access is public) or auditors (in the case of a permissioned system) to check on entries in the register and thus spot data that has been incorrectly entered. It also makes it possible to trace exactly who entered the specific data and allows the system to flag data fraud automatically, thus helping to prevent these practices.

Inefficiency and excessive bureaucracy: excessive red tape and bureaucratic processes are known to increase corruption. DLT has limited potential to address these by providing platforms that connect several officials within the same system. It can therefore help those working on the same projects to coordinate. The platforms can also help to build in accountability by enabling superiors to check on civil servants who are under their responsibility, while also allowing these lower-ranked civil servants the opportunity to flag up wrong-doings at a higher level. Incorporating different government departments can lead to increased accountability and enable extra checks to be carried out on public servants.

As can be seen from the cases presented above, the use of DLT will not help to reduce corruption risks arising from external factors or from the work process within the organisations themselves, nor will it address those that are individually motivated. DLT can help to detect corruption and also prevent it by acting as a deterrent. Naturally, this effect can be limited through the adoption of new technologies.

CONCLUSION

The aim of this report was to evaluate the potential of distributed ledger technology in combating corruption. It examined three areas of development policy – supply chains, aid delivery and public administration. As explained in the first part of the study, its potential impact in the context of anti-corruption was evaluated by analysing the corruption risks in the respective fields and then considering use cases and how they address these risk factors.

The factors leading to corruption risks were considered from four different levels: contextual factors, organisational factors, working process factors and individual factors. An analysis of the three areas showed that DLT has the potential to lower the risk of corruption. However, this potential relates to specific problems stemming from organisational or working process factors. Here, the use of DLT can improve efficiency, improve the quality of paperwork and increase transparency, trust and accountability between partners. This will help to address corruption risks, even though it will not necessarily help to fight corruption since corruption relies on many different factors.

In addressing organisational and working process factors, DLT can help **prevent** corruption as it makes it harder to hide corrupt practices and can include accountability mechanisms. According to the principal–agent theory on corruption, DLT can deter civil servants tempted to engage in corrupt activities since, if applied in a certain context, it can help to **detect** corruption. As data is stored in an immutable, distributed ledger and different parties (sometimes even the public) can connect to the system, it is harder to hide behind false or missing data. Outright data fraud can easily be detected in DLT systems and it would thus be harder to commit. It is, however, much less clear if DLT could support the **prosecution** of corruption. While DLT supports the attribution of data entries, it is also possible to circumvent clear attribution.

None of the use cases and concepts highlighted in this report used straightforward implementations of public blockchains. There are several reasons for this: public blockchain solutions are currently too inefficient and costly and they present unresolved legal issues and concerns about the privacy of users. Crucially, few organisations have the incentive to embrace the full disintermediation and decentralisation that public blockchains represent, as this would require surrendering some control over the data and applications. This is also highlighted by Walport (2016), who sees permissioned ledgers as more suitable for government applications. Consequently, the solutions presented here do not fully incorporate the principles of decentralisation and transparency.

Yet, even the hybrid and private ledger-based solutions described here have some potential to address specific corruption risks. DLT is advancing rapidly and the technology is improving. For anti-corruption specialists, these developments remain an exciting field to watch.

REFERENCES

Albisu Ardigó, I., *Corruption in Tax and Customs Authorities*, Transparency International Anti-Corruption Helpdesk, 2014, Available at: *https://www.transparency.org/files/content/corruptionqas/Literature_Review_of_Corruption_risks_in_Customs_and_Tax_2014.pdf*. Accessed 12 September 2019.

Ayogu, M. and Lewis, Z., *Conflict Minerals: An Assessment of the Dodd-Frank Act*, Brookings, Washington D.C., 2011, Available at: *https://www.brookings.edu/opinions/conflict-minerals-an-assessment-of-the-dodd-frank-act/*. Accessed 01 June 2018.

Bieri, F., *From blood diamonds to the Kimberley Process: How NGOs cleaned up the global diamond industry*, Routledge, London, 2016

Bleischwitz R., Dittrich M. and Pierdicca C., 'Coltan from Central Africa, international trade and implications for any certification', *Res Policy*, Vol. 37, No. 1, 2012, pp. 19–29

Chayes, S., *Corruption and State Fragility*. Fragility State Group Policy Brief. No 1, 2016, Available at: https://www.usip.org/sites/default/files/Fragility-Report-Policy-Brief-Corruption-and-State-Fragility.pdf. Accessed 25 October 2019.

Federal Ministry for Economic Cooperation and Development. (2012). *Anti-Corruption and Integrity in German Development Policy: A Strategy*. Bonn: BMZ. Available at: http://www.bmz.de/en/publications/archiv/type_of_publication/strategies/Strategiepapier323_04_2012.pdf. Accessed 25 September 2019.

Hart, E., *Why is corruption risk management so hard? Assessing current practices in development aid*. U4 Brief No. 11, May 2016, Available at: https://www.u4.no/publications/why-is-corruption-risk-management-so-hard-assessing-current-practices-in-development-aid.pdf. Accessed 30 September 2019.

Heggstad, K. and Frøystad, M., *The basics of integrity in procurement*. U4 Issue, No 10, October 2011, Available at: *https://www.u4.no/publications/the-basics-of-integrity-in-procurement.pdf*. Accessed 15 September 2019.

Hyperledger, *Hyperledger Fabric release 1-1*, 2017, Available at: *https://hyperledger-fabric.readthedocs.io/en/release-1.1/*. Accessed 28 June 2018.

Klitgaard, R. (1988). *Controlling Corruption*, University of California Press, Berkley, CA.

Koning, R. de, and Enough Project, *Striking gold: how M23 and its allies are Infiltrating Congo's Gold Trade*. Enough Project, Washington, DC, 2013, Available at: *https://enoughproject.org/files/StrikingGold-M23-and-Allies-Infiltrating-Congo-Gold-Trade.pdf*, Accessed 21 June 2018.

Kossow, N. and Dykes, V., *Bitcoin, Blockchain and Corruption: An Overview*, Transparency International Helpdesk Answers, Berlin, 2017, Available at: *https://knowledgehub.transparency.org/assets/uploads/helpdesk/Bitcoin-blockchain-and-corruption_2017-PR.pdf*. Accessed 13 July 2018.

Marquette, H., and Peiffer, C., 'Grappling with the "real politics" of systemic corruption: Theoretical debates versus "real-world" functions', *Governance*, Vol. 31, No. 3, 2018, pp. 499-514

Mills May, A., *Causes of corruption in public sector institutions and its impact on development: Turning what we know into what we do*, Expert Group Meeting UNPAN, 14th June 2012, Available at: *http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan049589.pdf*. Accessed: 15 July 2018.

Mungiu-Pippidi, A., 'Controlling Corruption Through Collective Action', *Journal of Democracy*, Vol. 24, No. 1, 2013, Available at: *https://www.journalofdemocracy.org/sites/default/files/Mungiu-Pippidi-24-1.pdf*. Accessed 10 September 2019.

Nakamoto, S., *Bitcoin: A peer-to-peer electronic cash system,* 2008, Available at: *https://bitcoin.org/bitcoin.pdf*. Accessed 30 September 2019.

Orogun, P., 'Blood Diamonds and Africa's Armed Conflicts in the Post—Cold War Era', *World Affairs*, Vol. 166, No. 3, 2004, pp. 151-161

Reform, Dodd-Frank Wall Street, and Consumer Protection Act. "Public Law 111-203." US Statutes at Large 124 (2010): 1376

Rodrigues, B., Bocek, T., Lareida, A., Hausheer, D., Rafati, S., and Stiller, B., *A Blockchain-Based Architecture for Collaborative DDoS Mitigation with Smart Contracts*, IFIP International Conference on Autonomous Infrastructure, Management and Security, Springer, 2017, pp. 16-29

Selinšek, L., *Corruption Risk Assessment in Public Institutions in South East Europe: Comparative Research and Methodology*, Regional Cooperation Council, Sarajevo, 2015, Available at: *http://rai-see.org/wp-content/uploads/2015/10/CRA_in_public_ins_in_SEE-WEB_final.pdf*. Accessed 26 September 2019.

Volkswagen, *From mine to factory: Volkswagen makes supply chain transparent with blockchain*. Press Release, 2019, Available at: *https://www.volkswagen-newsroom.com/en/press-releases/from-mine-to-factory-volkswagen-makes-supply-chain-transparent-with-blockchain-4883*. Accessed 07 October 2019.

Walport, M., *Distributed ledger technology: Beyond blockchain*, UK Government Office for Science, London, 2016, Available at: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf*. Accessed 31 August 2018.

Williams, N., *Minespider: Open Protocol for Supply Chain Due Diligence. v.0.29b*, MineSpider GmbH, Berlin, 2018, Available at: *http://minespider.com/wp-content/uploads/abridged-white-paper-v0.29b.pdf*. Accessed 28 June 2018.

GLOSSARY OF TERMS

Bitcoin

Bitcoin is a digital currency or cryptocurrency that was released as an open source protocol in 2009 and is based on a blockchain architecture. It was created by Satoshi Nakamoto, an unknown pseudonymous author. Despite a myriad of cryptocurrencies published since, bitcoin arguably remains the most well-known cryptocurrency.

Blockchain

A blockchain is a type of distributed ledger used to store transaction data of any kind. Developed as part of the bitcoin whitepaper by anonymous author Satoshi Nakamoto a blockchain was first used to store data on cryptocurrency transactions. It uses cryptography to immutably store data in blocks of data that get then linked to each other using a consensus-building algorithm.

- **Consortium Blockchain**
  A consortium blockchain is a type of private blockchain that is collectively run by a consortium of actors and in which the consensus process is controlled by a previously selected set of nodes. This type of DLT thus has some degree of decentralization, since no actor can govern the blockchain by themselves; however, the number of involved parties is typically fairly low.

- **Hybrid Blockchain**
  A hybrid blockchain brings together elements of private and public blockchains. They typically offer a dual structure in which some data is stored on a private, permissioned ledger that only involves key stakeholders, and other data is stored on a public ledger. For instance, transaction data itself gets stored on a private ledger, safeguarding privacy and access to information. Simultaneously, hashes of the data get stored on a public ledger so external actors can verify the integrity of the system.

- **Private Blockchain**
  A private or permissioned blockchain is a type of distributed ledger that is restricted to one or a select number of parties. In this system there is a central authority or a group of actors who decide who can take part in the system. In a private blockchain, permissions to write on to the blockchain and read data from the blockchain is restricted, oftentimes to only very few nodes. These type of blockchains are thus not transparent to those who are not part of the system and are also less secure to attack. Their level of decentralization heavily depends on how the governance of the blockchain is set up and on how many partners are involved.

- **Public Blockchain**
  A public or *permissionless* blockchain is a type of distributed ledger that is publicly available and that anyone can participate in. Any party that has the necessary computing device can technically download and install the respective core programme of a public blockchain and become part of distributed ledger system. In a public blockchain transactions can thus be audited by a large number of parties. Public blockchains are secure against outside attacks, but face challenges on legal issues such as privacy and questions of data sovereignty. They are, currently seen as inefficient since their consensus building algorithm uses a lot of processing power and data storage capabilities are limited.

Block on a Blockchain
On a blockchain, data is stored in shape of a block. Each block includes data on transactions, a hash of a previous block and, in a proof-of-work based blockchain, a nonce to enable a consensus building algorithm. New blocks contain previously unknown information and are added to the end of the blockchain.

Block explorer
An online tool allowing anyone to search the contents of a public blockchain. It makes it possible to follow and trace transactions, as well as analyse properties of a blockchain.

Consensus
A key problem in a distributed ledger system is to create a reliable process despite the presence of many participating parties. This requires a mechanism to agree on which transactions happened and in which order, thus building consensus on the data within the system between the participating parties. Blockchain systems all have a consensus-building algorithm that ensures that consensus on what data is part of the system can be achieved.

DDoS attacks
In Distributed Denial of Service (DDoS) attacks many computing devices are coordinated to all try and access a service (often an internet server) at the same time, causing it to crash due to the overload and thus making its data unavailable.

Digital currency
A currency that is only available in digital form. Typically, it has a money balance that is recorded digitally. Early forms of digital currencies were used in the context of online computer games. Since the advent of so-called cryptocurrencies, most notably bitcoin, digital currencies have grown significantly in their market cap and are often backed by distributed ledgers relying on cryptography. Digital currencies are often defined in opposition to traditional currencies or fiat money.

Directed acyclic graph (DAG)
Directed acyclic graphs (DAGs) are a type of data storing infrastructure used by several distributed ledger systems. In these kind of structures data is added continuously, and consensus is passed on from one node to the other, thus avoiding bottlenecks and the high energy costs associated with many blockchains. DLT systems based on DAGs do not broadcast transaction data in the form of blocks. Nodes communicate with the network when submitting transactions. Each transaction that is submitted confirms two previously submitted transactions that are chosen at random. Each transaction thus has two parent transactions, leading to the construction of a graph. This graph is directed, as confirmations always go in one direction and not backward. It is acyclic in the sense that information cannot form a cycle, but always refers to new nodes. This leads to a considerable increase in the number of transactions per second that can be recorded.

Distributed consensus algorithm
In order to decide who can add the next block to the blockchain and to verify the data that is added to it, the system needs a specific mechanism to build consensus amongst all participating nodes. This validation system is referred to as a distributed consensus algorithm.

Distributed ledger technology (DLT)
A distributed ledger is a database that is stored on many computing devices at the same time, without relying on a centralized server architecture. A blockchain is one type of DLT.

Distributed Network
A network that does not rely on one centralized authority but is based on a distributed system of several parties. In a computing network this means no central server stores all the data and no central authority decides on the rules within the system. Instead, a network of distributed nodes fulfils these functions.

Ethereum
Released in 2015, Ethereum is an open software platform based on blockchain technology. It enables users to write smart contracts and develop decentralized applications (Dapps). It uses a native crypto-currency token called Ether, used for transaction fees, mining rewards and other services on the network. Ethereum provides a developing framework that makes it easy for other developers to adapt it for many different applications on the same platform.

Encryption
Using mathematics and computer code to protect data from unauthorized access. Encryption algorithms typically transform data into a string of characters. Encrypted files can be decrypted with the right decryption key.

Hash
Within a blockchain, each block contains a cryptographic image of the previous block, a so-called hash. A hash value is a fixed-size set of data and the result of a hash-function. It functions as a one-way street, meaning it is easy to verify the result but hard or impossible to reconstruct the original data.

Intermediary
An intermediary in transactions is a middleman between two interacting parties. In a monetary transaction an intermediary could, for instance, be represented by a bank.

Know your customer
Laws and regulations that require financial institutions to identify their customers and keep personal information on them.

Mining
The process of adding new blocks to a blockchain in a proof-of-work system. The name stems from the fact that this process requires a considerable amount of computing power and is thus very laborious.

Node
A node is a computing device that connects to a DLT network and stores data from the respective system, such as all data stored in a blockchain.

Full node
A full node is a node that does not only stored all data within a blockchain, but also takes part in the consensus-building process, for instance, by mining blocks.

Nonce
A nonce is a random number provided by each block within a proof-of-work system. It provides an initialization for the hash-function and can be adjusted to keep the hash rate stable.

Oracles
In smart contract applications, oracles are applications that make external data usable for a smart contract. An oracle referring to weather data, for instance makes it possible to enforce a contract if certain weather conditions are met.

Practical Byzantine Fault Tolerance (PBFT)
In permissioned DLT systems, an algorithm that is frequently used is practical byzantine fault tolerance (PBFT). Here every node calculates independently if they accept the transactions that were broadcast as valid and if they should be added to the chain of information. They compare their decision to other decision they reach from nodes in the system and broadcast it to the network. The consensus is reached based on all decisions of the nodes within the system. This way, the anonymity of the consensus building mechanism is given up, but the algorithm is highly efficient.

Proof-of-work
The proof-of-work algorithm which remains the most common consensus building algorithm in the context of public blockchains. It is using computing power, and thus electricity, in order to establish consensus: each block provides a type of cryptographic puzzle, in form of a nonce, a random number that makes it much more difficult and computing power intensive to create the needed hash than it is to verify it. Full nodes within a blockchain system are thus competing to be allowed to add a new block. Once a node found the necessary solution, it broadcasts the new block to all other nodes in the system, so they can verify it. If 51% of all nodes accept the block as having been correctly calculated, it is added to the blockchain. The owner of the node that added the block is rewarded for its efforts through distribution of a digital currency. This process is referred to as mining. The amount of time that it takes to add a block depends on the number of participants in the system and on the difficulty of the proof-of-work that must be provided. The latter is adjusted to keep this time constant: in the context of the bitcoin blockchain, a new block is written every ten minutes.

Proof-of-stake
Proof-of-stake algorithms are an alternative consensus building protocol. Participants in this process are called validators. They need to show that they own an economic stake in the system, in shape of crypto-currency assets. These assets get locked. The mining power of the individual validators is attributed according to their stake in the system. A validator with a 1% stake can mine 1% of all blocks. Once a block is mined the funds of the validators are released together with an interest rate.

Smart contracts
Computer protocols that facilitate, verify or enforce the negotiation of a contract are referred to as smart contracts. They translate the logic of a contract into code and typically tie in conditionality involving a variety of parties, including oracles.

Validation system
A system built to establish the validity of data within the system and thus establish consensus between different parties.

Validator
A name for a participant in a blockchain-based system using a proof-of-stake algorithm. They validate the data that is entered onto the respective blockchain.

Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn

Friedrich-Ebert-Allee 36 + 40
53113 Bonn, Germany
T +49 228 44 60-0
F +49 228 44 60-17 66

Dag-Hammarskjöld-Weg 1 - 5
65760 Eschborn, Germany
T +49 61 96 79-0
F +49 61 96 79-11 15

E info@giz.de
I www.giz.de

On behalf of

Federal Ministry
for Economic Cooperation
and Development