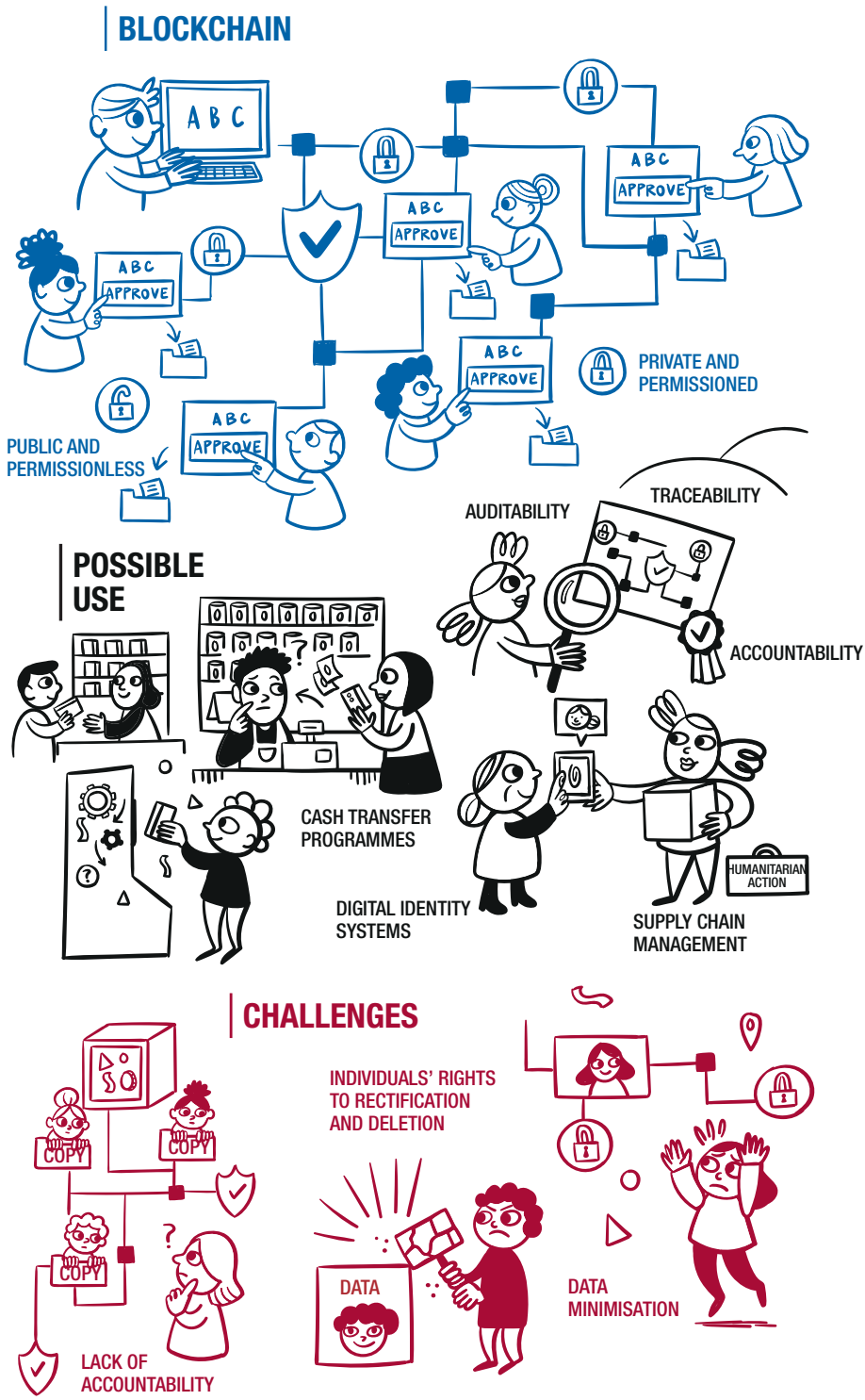

CHAPTER 15

BLOCKCHAIN

Vincent Graf Narbel*

* The author would like to thank Robert Riemann (European Data Protection Supervisor), Giulio Coppi (Norwegian Refugee Council) and Bryan Ford (Swiss Federal Institute of Technology in Lausanne) for their contributions to this chapter.

15.1 INTRODUCTION

In recent years, "Blockchain" has become a buzzword and various organizations, including in the humanitarian sector, are trying to find a use for this technology. It has been argued that Blockchain could improve efficiency in humanitarian programmes involving, for example, financial transactions and supply tracing.[1] It has also been suggested that Blockchain could enhance transparency and trust in information integrity.[2] However, achieving such improvements could be offset by a number of practical and data protection challenges. These are discussed below, along with any anticipated benefits and risks.

This chapter presents a simplified and easy-to-understand explanation of Blockchain technology, the main parties involved and its various architectures (Sections 15.1.1 to 15.1.3). Since Blockchain is a complex technology, this discussion is by no means exhaustive. It merely supports the data protection analysis that follows in Sections 15.2 to 15.7.[3]

15.1.1 WHAT IS BLOCKCHAIN?

A Blockchain is "in essence an append-only decentralized database that is maintained by a consensus algorithm and stored on multiple nodes (computers)".[4] This definition includes a number of complex technical elements that are addressed in more detail below. Essentially, Blockchain technology is a special way to store data in a database. As such, any type of data can be stored on a Blockchain, including Personal Data. On a Blockchain, each piece of data is stored one after the other in a chain (which is why it is called "append-only").[5] This is done by grouping data in blocks and by adding, to each new block, a cryptographic pointer (a reference or link) to the previous block.

The design of Blockchains is guided by a desire to increase security (in the broad sense of the term). In particular, and as mentioned above, Blockchain technology aims to enhance transparency and trust in the integrity of the database. Blockchains are "distributed" and often "decentralized". While these are two different concepts,

1 Vanessa Ko and Andrej Verity, *BlockChain for the Humanitarian Sector – Future Opportunities*, DH Network, UN OCHA, November 2016, 12–14: https://reliefweb.int/sites/reliefweb.int/files/resources/BlockChain%20for%20the%20Humanitarian%20Sector%20-%20Future%20Opportunities%20-%20November%202016.pdf.

2 Ibid., 8.

3 For more detailed definitions and explanations of Blockchain technology, please refer to: Jean Bacon et al., "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers", *Richmond Journal of Law and Technology* (blog), 6 November 2018: https://jolt.richmond.edu/blockchain-demystified-a-technical-and-legal-introduction-to-distributed-and-centralised-ledgers.

4 Finck, "Blockchains and data protection in the European Union".

5 Note that this property is the reason why they are also called ledgers: a ledger is a book that stores (traditionally monetary) transactions in append-only mode.

they bear a common feature – namely, they indicate that the data being processed are not managed and stored centrally. Here, "distributed" means that there are multiple copies of the database stored on different computers, while "decentralized" means that the power and authority to decide what data are added to the ledger is not held by a single entity or individual, but is instead shared between many entities or individuals that have to work together. In this chapter, these entities or individuals are referred to as "validators" (since they, together, validate the data to be stored on the Blockchain). Usually, the higher the number of validators, the more complex the rules they have to follow to reach an agreement. These rules are reflected in a "consensus protocol" (see Section 15.1.2 – Types of Blockchain, below for further details).

The computers that hold a copy of the Blockchain are called "nodes" (since they represent nodes in a vast network). Nodes can be passive (only storing an up-to-date copy of the Blockchain) or active. Active nodes are also validators, and are said to be "mining" the data (i.e. participating in the consensus protocol to validate new insertions). Sometimes validators are called "miners" by analogy.

"Users" are the parties who wish to add information to the Blockchain (hence creating data that need to be validated and recorded on the Blockchain).

A piece of information will only be inserted into the Blockchain once it has been validated. This makes it extremely difficult for a malicious party to add data to the Blockchain, since any addition has to be accepted by the validators first.

Moreover, the blocks of information on a Blockchain are time-stamped and, as mentioned above, contain a cryptographic link (pointer or reference) to the previous block. This means that, even if a malicious party succeeds in changing data contained in a particular block, it also has to modify the following block (as the cryptographic pointer it contains will have changed), as well as all subsequent blocks through to the end of the chain. These changes would unlikely go unnoticed because of a Blockchain's decentralized design, which means that every validator would have to agree to them. Since, in practice, it is very difficult (though not totally impossible) to change information on Blockchains, they are often referred to as immutable ledgers.[6]

When information is added on the Blockchain, a mechanism involving public and private keys is used to secure the transactions. Blockchain users own one or more such key pairs. The public key, or a value derived from it, serves as the user's address on the Blockchain. It is publicly known and used to verify the origin and destination of added information.[7] Even though Blockchain addresses do not by themselves reveal the

6 Finck, "Blockchains and data protection in the European Union", p. 19.

7 Ibid.

identity of the person they relate to, they are still considered to be pseudonymized Personal Data as they are linked to one specified individual (the user who adds or receives information). They could be traced back to the individual's IP address, for instance, which could lead to identification.[8] As Blockchains are near-immutable, public keys could potentially remain on the Blockchain for as long as the ledger exists.

Several companies provide Blockchain analytics services that specialize in providing platforms for investigative and compliance needs in Blockchain-based transactions. They offer Blockchain intelligence to gather, analyse and interpret data from various Blockchain networks. Their platforms enable the identification and monitoring of transactions, addresses and entities involved in Blockchain activities. These investigations help businesses and regulatory agencies to comply with Anti-Money Laundering (AML) requirements. Another use case is to support law enforcement agencies in combating illicit activities using cryptocurrencies. These investigations are possible because the Blockchain public addresses can be used to reidentify users. Several new designs have been proposed to guarantee a higher level of anonymity, for instance Monero or the ZCash protocol. They come with their own limitations and Humanitarian Organizations have to balance those limitations carefully. However, Humanitarian Organizations should also be mindful of the need for more privacy when deploying off-the-shelf Blockchain-based solutions.

Some of the above characteristics of Blockchain technology can be advantageous for Humanitarian Organizations. For example, the decentralized architecture can potentially increase security, since there is no single point of failure or compromise in such systems. This means that potential attackers need to compromise several links in order to compromise the Blockchain as a whole. This set-up increases system integrity because it is claimed to almost always guarantee data immutability.

In light of the fact that information is time-stamped and close to immutable, and the fact that responsibility is shared, it has been argued[9] that Blockchains can be most valuable when:

- they are used to track ownership of complex things over time;
- there are multiple groups or parties involved;
- there is no well-established or effective central authority (also known as a trusted Third Party) in place;
- groups or parties involved need to work collaboratively;
- a record or proof of transactions is required.

These examples show that the one of the main benefits of Blockchain technology is its resistance to a single point of failure or compromise. This is due to the ledger's distributed design, which ensures that multiple nodes have to work together to add

8 Ibid., pp. 24–25.

9 Ko and Verity, *BlockChain for the Humanitarian Sector*, 9.

new data to the Blockchain. Moreover, because the whole ledger is copied to multiple nodes, it becomes difficult to change information on the ledger and data remain available even if one node is compromised, thereby increasing their integrity.

It is important to note that Blockchain technology will most likely not be needed when there is no issue with the level of integrity (i.e. there is enough trust between the parties involved in a specific programme and there are sufficient levels of auditability), or simply if other current technology offers a sufficient degree of integrity and availability. In such cases, a more traditional solution with a central database, for instance, may prove more efficient, faster, and cheaper to implement, and, overall more proportionate from a data protection perspective.

Another element to take into account is the exit criteria. Humanitarian Actions are often designed to be temporary. If a Blockchain is used in a CVA program, for example, the process to shut down the program, discard Personal Data and close the beneficiary's account may be complicated by the distributed and immutable nature of the Blockchain.

15.1.2 TYPES OF BLOCKCHAIN

Blockchains can be built in different ways, according to system design choices. One key decision, for instance, is whether or not the Blockchain will be public. Although there is no universally agreed definition of each type of Blockchain, the following definitions are more commonly used:

Table 15.1

Blockchain	Permissionless: Anyone can become a validator (node or miner).	Permissioned: Validators (nodes or miners) are predefined and authorized by a governing body.
Public: Everyone can access ("see" or "read") the data stored on the Blockchain and add transactions.	Everyone can read the transactions on the Blockchain (which are public) and participate in the consensus protocol as a validator for new transactions. It is worth noting, however, that data added to the ledger may be encrypted and, therefore, those without the decryption key will not be able to decipher and read their contents. The public keys and time-stamps, however, remain visible to all. This type of Blockchain (public permissionless) is used by Bitcoin.	Everyone can read the transactions on the Blockchain (which are public) but only predefined parties can become validators and participate in the consensus protocol to validate new insertions. Such Blockchains could, for instance, help to improve supply-chain transparency, since only those parties involved in the handling of goods would be authorized to alter the ledger (as validators), whereas any member of the public could check the transactions.

Table 15.1 (*cont.*)

Blockchain	Permissionless: Anyone can become a validator (node or miner).	Permissioned: Validators (nodes or miners) are pre-defined and authorized by a governing body.
Private: Only authorized users can access the data on the Blockchain.	In theory, this type of Blockchain allows only predefined parties to access the data stored on the Blockchain, but anyone to participate in the validation of new insertions. In practice, however, this would be hard to implement because validators are able to store a full copy of the ledger. Consequently, it would be difficult to conceive a platform in which validators are not allowed to access the information on the ledger.	Only predefined users can access ("read") the data stored on the Blockchain and only predefined validators (not necessarily the same users) can participate in the validation of new insertions.

Besides choosing who can "read" or "write" on the Blockchain, system designers must also decide how validation will take place. Blockchain validation processes are regulated by consensus mechanisms (or consensus protocols), which consist of a set of predefined rules that divides trust among the parties. These rules allow them to store data immutably without a central authority (or trusted Third Party), thereby preserving the integrity of the ledger.[10] In other words, consensus mechanisms define how new information is validated by the parties in the Blockchain and, if deemed valid, added to the ledger.

There are different types of consensus protocol. For example, in Blockchains that use proof-of-work protocols, validators need to earn the right to validate a transaction by solving complex mathematical problems using brute computational force, which requires considerable processing power and electricity.[11] In proof-of-stake protocols, meanwhile, the parties have simple voting rights, and the weight of their vote may vary according to their stake in the Blockchain.

To illustrate some of the different choices that have to be made when developing a Blockchain, it is useful to think of the system like a corporation. Corporations

10 Walid Al-Saqaf and Nicolas Seidler, "Blockchain technology for social impact: Opportunities and challenges ahead", *Journal of Cyber Policy*, Vol. 2, No. 3, 2 September 2017, pp. 338–354: https://doi.org/10.1080/23738871.2017.1400084.

11 Pisa and Juden, *Blockchain and Economic Development: Hype vs. Reality*, 8.

typically hold board meetings. There need to be rules governing how board members are chosen and who has the right to vote and make decisions. One option is to have a closed group decide who joins and leaves the board (akin to a permissioned Blockchain). Another possibility is to allow anyone to sit on the board as long as they buy enough "stock" in the company to give them voting shares (a proof-of-stake Blockchain). A third option is to decide that anyone can sit on the board as long as they can prove they devoted enough energy to a task in the past 10 minutes – an artificial barrier to entry (a proof-of-work Blockchain).

15.1.3 BLOCKCHAIN IN PRACTICE

Scholars and practitioners propose the following advantages and challenges of using Blockchain technology:[12]

Advantages:

- There is no need for a trusted Third Party (a central authority) to maintain the integrity of a shared record: transactions inserted on a Blockchain are verified by participants through a consensus mechanism. The breadth of this benefit, however, varies depending on how the Blockchain is used.
- Eliminating a trusted Third Party reduces costs. For instance, Blockchain could support cross-border cash transfers directly between the parties to a transaction, removing the need for a bank or another financial institution, which often charges fees.
- A Blockchain acts as an audit trail, since the way data are stored and connected can make it easier to track the origin and movement of physical assets tied to a digital token.[13]
- Transparency is increased, especially in public Blockchains, because more parties can access the ledger. In private Blockchains, however, this benefit may be reduced or in some cases non-existent.
- Blockchains improve integrity and availability, since they provide operational resilience and entail no single point of failure or compromise.[14]

Challenges:

- An appropriate governance structure needs to be determined for each Blockchain solution.
- Although Blockchains are considered "trustless", there are parties involved in the system who nevertheless have to be trusted. These include the developers behind the code, as well as designers who create applications that interact with the Blockchain or Cloud Services where data may be stored.

12 For more details, see: Finck, "Blockchains and data protection in the European Union"; Bacon et al., "Blockchain Demystified".

13 Pisa and Juden, *Blockchain and Economic Development*, 9.

14 Other characteristics of the technology, however, may make it more vulnerable to attacks (see challenges below, as well as Section 15.5.4 – Data security).

- Blockchain increases the number of access points for possible attacks by malicious parties, thereby posing security risks. Moreover, some consensus mechanisms – albeit not frequently used – accept a transaction as valid when 51 per cent of the validators approve it. So, if a consortium of validators gains control of 51 per cent of the nodes, they could jointly take control over the ledger.
- The technology is dependent on Internet connectivity.
- Some Blockchains, such as those that use proof-of-work protocols, consume much more electricity than alternative technologies.[15]
- Individuals must be informed, through information notices, about the Processing of Personal Data, and must be able to exercise their rights (such as erasure, rectification, and withdrawal of Consent) in respect of their Personal Data.
- Private permissioned Blockchains may be more appropriate for certain types of humanitarian programme (such as Cash and Voucher Assistance), since these architectures involve a limited number of participants. In some cases, however, this may lead to the reintroduction of trusted parties and to a decrease in transparency.
- Compatibility with data protection requirements in different jurisdictions is a concern (see below).

While Blockchain technology can help improve transparency in many situations, it does not solve the underlying problems that create so-called bad data. In other words, if someone stores unreliable records on a Blockchain, they will remain unreliable and the system will not achieve its potential benefits.[16]

These advantages and challenges of Blockchain have significantly influenced their use. Blockchains are frequently used to manage transaction histories recording the ownership or custody of, or responsibility for, assets such as cryptocurrencies. They are also used to notarize or assign time-stamps to supply-chain, digital-credential and other documents, as well as to enforce the terms of a contract (through the use of smart contracts).[17]

15.1.4 HUMANITARIAN USE CASES

Humanitarian Organizations have begun exploring possible applications of Blockchain and have launched pilot projects using the technology.[18] While there is little information available about the benefits and risks that Blockchain technologies

15 Bacon et al., "Blockchain Demystified", 15.

16 Pisa and Juden, *Blockchain and Economic Development*, 49.

17 Smart contracts are a feature of Blockchain that will not be addressed in this chapter. For information on smart contracts, see: Michèle Finck, *Smart Contracts as a Form of Solely Automated Processing under the GDPR*, SSRN Scholarly Paper, Social Science Research Network, Rochester, NY, 8 January 2019: https://papers.ssrn.com/abstract=3311370.

18 For more information on the use of Blockchain in the humanitarian sector, see: Larissa Fast and Giulio Coppi, *Blockchain and Distributed Ledger Technologies in the Humanitarian Sector*, Humanitarian

bring in such cases, some of the following uses among Humanitarian Organizations have been proposed:[19]

Cash and Voucher Assistance (CVA).[20] Blockchain could improve the efficiency of CVA through a secure and well-structured transaction record-keeping system, which in turn increases transparency and provides added assurance that data stored in the system have not been tampered with. The application of Blockchain technology to CVA could allow Humanitarian Organizations to make digital cash payments cheaper, more efficient and traceable, as well as interoperable across multiple organizations. In addition, because Blockchain technology is said to provide operational resilience and to entail no single point of failure or compromise, it could make transactions more secure (See Section 15.5.4 – Data security, below for more information on Blockchain and security).

Optimizing and tracking logistics. Humanitarian supply chains are extremely complex and dynamic, which makes it difficult to monitor them properly. Blockchain technology may offer a way to introduce transparency into these operations. In the case of provision of medical supplies, for instance, a Blockchain may contain a near-immutable, time-stamped record of when the supplies left the warehouse, when they were transported out of the country of origin, when they arrived at the country of destination, when they were received by the local branch of the Humanitarian Organization and when they reached the destination hospital. Because a public Blockchain provides a publicly visible ledger, it can serve as a transparent data platform that traces the origins, use and destination of humanitarian supplies.

Tracking donor financing. Peer-to-peer tracking and monitoring of donations may make it possible to scale up finance models that cut out the traditional "middleman"[21] (or trusted Third Party).[22] Such models could reduce transaction costs associated with international humanitarian financing and improve the tracking of donations, including from the general public. However, Blockchain technology could be used to make anonymous donations. This could pose a challenge for Humanitarian Organizations with stricter funding policies that require the donating party to be identified.

Enhancing shared situational awareness in conflicts. The Whiteflag Protocol[23] (in which the ICRC is collaborating) aims to provide a neutral means of communication

Policy Group Report, ODI, London, , February 2019: https://odi.org/en/publications/blockchain-and-distributed-ledger-technologies-in-the-humanitarian-sector.

19 Examples taken from Ko and Verity, *BlockChain for the Humanitarian Sector*.

20 See for example: IFRC, *Blockchain Open Loop Cash Transfer Pilot Project*, ALNAP, 1 September 2018: www.alnap.org/help-library/blockchain-open-loop-cash-transfer-pilot-project.

21 Ko and Verity, *BlockChain for the Humanitarian Sector*, 13.

22 Finck, "Blockchains and data protection in the European Union", p. 18.

23 "WhiteflagProtocol", accessed 16 March 2022: www.whiteflagprotocol.org.

for all parties involved in a conflict. Whiteflag is designed to deliver a messaging system in which real-time information on emergencies, local dangers, landmines, population displacement and other issues can be shared in the knowledge that it has not been altered by a malicious party. In this arrangement, none of the participants need to trust one other. Although having this information publicly available could help to locate civilians and assess distinction and proportionality in attacks, it could also be used to target identified groups.

EXAMPLE:
In the Blockchain Open Loop Cash Transfer Pilot Project,[24] the IFRC and the Kenyan Red Cross Society used Blockchain to record cash-based transfers made to beneficiaries from households affected by drought. The idea behind the pilot was to explore the use and added value of Blockchain in CVA. The transfers themselves were made independently of the Blockchain, through a conventional partnership with a local mobile provider and an information management company. Using a private permissioned Blockchain, however, allowed transactions to be recorded almost immutably and in a distributed manner, thereby increasing transparency between the parties (the only ones allowed to access the Blockchain), creating an audit trail (as records were tamper-proof) and increasing record security (as there was no single point of failure or compromise).

Two notable challenges arose during the project. First, it proved difficult to change records when, for example, a disbursement was requested by mistake and a transaction needed to be reversed. Second, because beneficiaries could not receive assistance without Consent, it was questionable whether such Consent was freely given and informed.[25]

15.2 DATA PROTECTION IMPACT ASSESSMENTS

The use of Blockchain in humanitarian programmes may pose many data protection challenges that do not always occur in other contexts. This is one of the main reasons why it is important to carry out a Data Protection Impact Assessment (DPIA) before deciding to implement Blockchain systems. A DPIA can help identify whether it is necessary and proportionate to deploy such a system. If the organization does decide to proceed, the DPIA can also help to identify, address and mitigate the risks and challenges associated with the use of Blockchain. There are many templates and materials for conducting a DPIA,[26] but none of them have thus far been designed

24 IFRC, *Blockchain Open Loop Cash Transfer Pilot Project*.

25 See Section 3.2 – Consent.

26 See for example: French Data Protection Authority (CNIL), *Guidelines on DPIA*, 18 October 2017: www.cnil.fr/en/guidelines-dpia; UK Information Commissioner's Office (ICO), *Sample DPIA template*,

specifically for Blockchain in humanitarian contexts. Organizations therefore need to adapt existing DPIA models, or design Blockchain-specific ones.[27]

A DPIA is a systematic and adaptive process that covers both general questions relating to the Processing of Personal Data, and questions about the use of a specific type of technology (in this case, Blockchain). As discussed elsewhere in this chapter, Blockchain presents both advantages and challenges for Humanitarian Organizations. Despite the purported benefits, in most cases no effective improvements have been recorded. During the DPIA process, Humanitarian Organizations should therefore clearly identify the benefits, challenges and risks associated with using Blockchain, comparing them against other technologies. This approach is not new, but it is especially important for an emerging technology like Blockchain.

Since Blockchains can take many different forms, the DPIA must also cover the governance and design of each individual application. Because of the diversity of likely applications and the technical complexity of Blockchain, Humanitarian Organizations may also develop a decision-making framework to help them determine whether to implement Blockchain technologies, and if so, what protections they should implement. Some authors have suggested general decision-making frameworks for implementing Blockchain.[28] Yet these generic templates do not take into account the particular data protection concerns raised by Blockchain in the humanitarian sector. For this reason, an alternative Blockchain-specific decision-making framework is given in the annex to this chapter.

Conducting a DPIA can also be vital in identifying an appropriate legal basis for the use of Blockchain. The DPIA process should take into account the impact that a specific type of Blockchain (i.e. the one envisaged in a given situation) may have on Data Subjects' rights and the application of data protection principles. Based on this assessment, Humanitarian Organizations can choose the best solution to minimize potential risks.

The DPIA should give Humanitarian Organizations a clear picture of the impact Blockchain would have in terms of the proportionality of data Processing. Based on this assessment, an organization will be in a position to judge whether there are less intrusive means, such as traditional databases, that could fulfil its needs with less risk to beneficiaries.

Template, 22 June 2018: https://ico.org.uk/media/for-organizations/documents/2553993/dpia-template.docx?mc_phishing_protection_id = 28047-br1tehqdu81eaoar3q10.

27 More information about DPIA models and their design can be found in Chapter 5: Data Protection Impact Assessments (DPIAs).

28 Karl Wust and Arthur Gervais, "Do you need a Blockchain?", IEEE, 2018, 45–54: ieeexplore.ieee.org/document/8525392.

As well as assessing the technical design of the system, the DPIA process should also consider the issues and principles detailed in Sections 15.3 to 15.7 below.

15.3 DATA PROTECTION BY DESIGN AND BY DEFAULT

Data protection by design and by default involves designing a Processing operation, programme or solution in a way that implements key data protection principles from the outset, and that provides the Data Subject with the greatest possible data protections (see Chapter 6: Designing for data protection). The key data protection principles in this sense are:

- lawfulness, fairness, and transparency;
- purpose limitation;
- data minimization;
- accuracy;
- storage limitation (limited retention);
- integrity and confidentiality (security);
- accountability;
- support for Data Subjects' rights by design.

Refer to Chapter 2: Basic principles of data protection, for a general description of these principles, some of which are contextualized in the sections below.

At this stage, it is important to take into account the different types of Blockchain, as all options must be considered when designing a model that is compliant with data protection principles.

Private permissioned Blockchains (see Section 15.1.2 – Types of Blockchain, for definitions) are the most restrictive, since one or more parties define(s) who has the right to validate information on the Blockchain and who can access data on the ledger. It may therefore be easier to design private permissioned Blockchains in a way that is compatible with data protection principles.[29] Yet restricting the rights of participants might, in some cases, defeat the very purpose of Blockchain technology by reintroducing a trusted party and, potentially, a single point of failure or compromise.

Public Blockchains, in turn, should always be designed in ways that do not store Personal Data (this is always a preferred option, even for private ledgers). Personal Data could instead be stored "off-chain" (i.e. outside the ledger). Here, the public ledger merely contains a cryptographic pointer confirming that a specific document

29 Michèle Finck, *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?*, STUDY: Panel for the Future of Science and Technology, European Parliamentary Research Service (EPRS), 2019: www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

or piece of information has been stored in a different location (such as on a Humanitarian Organization's server).[30] The data themselves are not kept on the Blockchain. Yet even with this design, it is important to remember that public keys belonging to individuals included on the Blockchain will remain Personal Data. Whether or not cryptographic pointers also qualify as Personal Data is a matter of debate.[31]

15.4 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

Blockchains, as distributed ledgers, can involve a wide range of bodies and entities. Consequently, it can be difficult to ascertain which parties should be treated as Data Controllers and Data Processors. For clarification, the respective roles of each are detailed below:

Data Controllers determine the means and purposes of Processing. They are accountable for the Processing of Personal Data and are responsible for implementing Data Subjects' rights. They must comply with data protection principles and respond to individuals' requests to exercise their rights to access, rectification and erasure. If there are multiple Data Controllers in the Blockchain, or if new users considered Data Controllers join the Blockchain, their respective responsibilities for the Processing should be set out in a written agreement.

Data Processors follow the instructions of Data Controllers and are responsible for ensuring data security. They should also inform Data Controllers about which means are being used to process data, and about any problems or complaints that may arise with regard to data integrity, confidentiality and availability.

Each Blockchain architecture (as presented in Section 15.1.2 – Types of Blockchain) may have different implications when determining the roles played by different parties operating on the ledger. Importantly, when identifying the Data Controller, determining the purposes of the Processing is a more important factor than choosing

30 A cryptographic pointer (also known as a hash pointer) is the one-way mathematical transformation of any given input (a message or a document) into a fixed-length combination of letters and numbers (output). Every time a specific input is hashed, the output is the same, but any slight change to the input (e.g. adding or removing a comma) will produce a completely different hash (Pisa and Juden, *Blockchain and Economic Development*). Adding a hash pointer to the Blockchain, therefore, allows a person to verify that a document has been stored, since hashing that document again would produce the same pointer as the one contained in the ledger.

31 Finck, *Blockchain and the General Data Protection Regulation*, 30.

the means. With this in mind, and looking at the key parties in Blockchains, one could consider the following arrangements:

- In a permissioned Blockchain, it may be possible to identify a central party (or intermediary) that qualifies as the Data Controller (e.g. system operator that grants "writing" rights), and nodes would qualify as Data Processors.
- In a permissionless Blockchain, there will be no central intermediary, as the network is operated by all nodes in a decentralized manner. Here, every node could potentially qualify as a Data Controller, since they autonomously decide whether to join the chain and pursue their objectives.[32] However, there is no unanimity about this conclusion.

Some argue that nodes are Data Controllers because the fact that they join a Blockchain network can be considered tantamount to determining the purposes of the Processing.[33] Others argue that nodes are not Data Controllers.[34] It is also worth noting that nodes sometimes only see the encrypted version of the data and run a software program that does not allow them to alter the ledger. Consequently, they will be unable to "see" what data, including Personal Data, are being processed or make changes to the data and, therefore, cannot comply with data protection obligations of Data Controllers.

Users (organizations or private individuals deciding to use the Blockchain), in turn, can in some situations qualify as Data Controllers, since they clearly determine the purposes of the Processing (i.e. recording a specific piece of information onto the Blockchain).[35] Furthermore, users choose the means of Processing when selecting a specific version of Blockchain. This interpretation, however, will not apply to every type of Blockchain. This could be the case in a public permissionless Blockchain, but private permissioned Blockchains are more likely to be set up by a consortium of organizations, in which case the consortium will qualify as joint Data Controllers.

The French Data Protection Authority (CNIL) has sought to provide guidance on this matter. According to the CNIL:[36]

- Blockchain participants with "writing" rights will be considered Data Controllers when the data they enter are connected to a professional activity.
- Legal persons who "write" data on a Blockchain are considered Data Controllers.
- Miners (or nodes) who do not add data to the Blockchain, but only verify the authenticity of the data (by participating in the consensus protocol), are not Data Controllers because they do not define the means and purposes of the Processing;

32 Finck, "Blockchains and data protection in the European Union", pp. 26–27.

33 Ibid., p. 26.

34 Bacon et al., "Blockchain Demystified", 64–65.

35 Ibid., 64.

36 French Data Protection Authority (CNIL), *BLOCKCHAIN: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*, September 2018: www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf.

instead, they can be considered Data Processors, working under the instructions of the Data Controller.

Blockchain users, meanwhile, can be divided into two types:

- users who use Blockchain for commercial or professional purposes will qualify as Data Controllers;
- users who use the ledger for private purposes will not qualify as Data Controllers, since this would be considered a purely personal activity falling outside the scope of most data protection laws.

Considering the various interpretations and guidance on this matter, Humanitarian Organizations intending to use Blockchain technology must ensure that the governance of the chosen solution incorporates the concepts of Data Controller and Data Processor. They must also determine, as clearly as possible, the responsibilities of each party within a given Processing activity. If it becomes clear that, in a certain situation, it may be impossible for Data Controllers to fulfil their obligations (especially enabling Data Subjects to exercise their rights), an alternative solution should be sought, since the use of Blockchain will most likely be incompatible with data protection principles.

15.5 BASIC DATA PROTECTION PRINCIPLES

As explained above, reconciling the use of Blockchains with basic data protection principles can be challenging. In practice, compatibility between the two will depend on the architecture and design of each Blockchain solution. While this section provides general guidance, organizations must consider the specific features of each application when assessing its compatibility with data protection principles.

15.5.1 DATA MINIMIZATION

By their very nature, distributed ledgers would appear to run counter to the principle of data minimization, which states that the minimum amount of Personal Data should be processed in order to attain the objective and purposes of the Processing.[37] This is mainly because data in Blockchains can potentially be stored perpetually, and because a copy of the full ledger is stored in multiple nodes on numerous devices. However, there may be workaround solutions. Personal Data could be stored off the Blockchain while the ledger only keeps a cryptographic pointer to the data that are stored in a different location. In this case, the data will not be stored perpetually on the ledger or shared with all the nodes. The individual or organization that stores the data will retain full control over them and, therefore, will

37 For example, according to the General Data Protection Regulation (GDPR), Article 5(1)(c) and (e), Personal Data must be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed", and "kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed".

be able to apply the data minimization principle to the off-chain Processing of data without altering the ledger itself. Whether cryptographic pointers also qualify as Personal Data remains a matter of debate.[38]

15.5.2 DATA RETENTION

The fact that Blockchains are claimed to be immutable distributed ledgers also poses a challenge for the data retention principle.[39] Data stored on a Blockchain will be retained indeterminately on multiple computers. The best solution, therefore, would be not to store Personal Data on Blockchains. Personal Data should not, for instance, be stored in public ledgers, since this type of Blockchain can be accessed (or read) by anyone. In particular, Personal Data that are particularly sensitive – such as ethnicity and health records – should never be stored on Blockchains.

15.5.3 PROPORTIONALITY

Proportionality is a core principle of data protection. It generally requires consideration of whether a particular action or measure related to the Processing of Personal Data is appropriate to its pursued aim. Proportionality involves setting out the options and choosing the one that is the least intrusive with regard to the rights of Data Subjects. The complexity of Blockchains can make it difficult to determine whether a particular implementation is proportionate.

As with the data minimization and data retention principles, one way to address proportionality concerns in a public permissionless Blockchain could be to store Personal Data off-chain. Yet adding an off-chain database can mean reintroducing a trusted Third Party, such as a Cloud Service provider with whom the data will be stored. This, in turn, may negate the supposed benefits of using Blockchain in the first place. The proportionality requirement could, however, be satisfied if the characteristics of Blockchain are essential to achieve the envisaged objective (such as when there is an important need to improve the integrity, transparency and availability of an existing solution), and if that objective could not be achieved with a centralized database model (for instance, because the parties do not trust one another). The risks to Data Subjects, however, cannot be disproportionately high in comparison to the aim pursued.

15.5.4 DATA SECURITY

Data security is a key aspect of an effective data protection system.[40] Security is often related to three key principles:

- **confidentiality**: the data must only be accessible to authorized parties;
- **integrity**: unauthorized parties must not be able to modify the data, and the data must not be lost, destroyed or damaged;
- **availability**: the data must be available (to authorized parties) when needed.

38 Finck, *Blockchain and the General Data Protection Regulation*, 30.

39 See Section 2.7 – Data retention.

40 See Section 2.8 – Data security and Processing security.

Blockchains present both strengths and weaknesses when it comes to security across these three aspects. These are detailed, in turn, below.

On the issue of confidentiality, the distributed nature of Blockchains means that the same data are potentially replicated and distributed widely. This leads to increased access points and vulnerabilities. Moreover, even if a Blockchain system uses complex encryption and hashing techniques, advances in quantum computing mean that information could even be decrypted without the decryption key. If, in the future, encryption no longer guarantees the safety and anonymity of the data, all Personal Data stored on a public Blockchain could be exposed. And because, in most situations, data stored on a Blockchain cannot be deleted, the damage can be irreversible. This is yet another reason why it is not recommended to store Personal Data on the Blockchain itself.

With regard to integrity, the immutable character of Blockchain technology and the use of consensus protocols provide a security benefit over centralized databases, not least because "storing sensitive data on centralized servers creates a 'honeypot' for would-be hackers and a single point of failure".[41] In Blockchains, however, there is no single point of failure or compromise and, unless an attacker is able to gain control of enough nodes to control the consensus protocol, the system would most likely not be compromised.

On the question of availability, Blockchain is again beneficial because it consists of a distributed ledger stored simultaneously in multiple computers.

Resistance to a single point of failure or compromise is frequently said to be Blockchain's main added value in relation to security. If that is not an imperative for the organization, then traditional, non-Blockchain technology may be more efficient, faster and cheaper. Secret sharing techniques that are said to enhance the protection of encrypted data in distributed ledgers, for example, can also be used in traditional databases, i.e. they are not exclusive to Blockchain. The technology adds value when integrity and availability are important and when participants do not trust one another.

15.6 RIGHTS OF DATA SUBJECTS

Data Subjects are entitled to certain rights, which allow them to exercise control over their Personal Data. As explained below, however, it can be technically very difficult or impossible to implement these rights on Blockchains.

41 Pisa and Juden, *Blockchain and Economic Development*", 6.

15.6.1 RIGHT OF ACCESS

Individuals have a right to know whether their Personal Data are being processed by the Data Controller, and to obtain a copy of the Personal Data in question.[42] In the humanitarian sector, therefore, when Personal Data are stored on the Blockchain, Humanitarian Organizations should always participate as nodes that hold a full copy of the ledger. That way, they can ensure that the entire database is available at all times, and can inform beneficiaries which data are stored on the Blockchain.

When Personal Data are stored off-chain, meanwhile, the ledger only contains a pointer to the off-chain data. In such cases, the most likely scenario is that Humanitarian Organizations will store the data themselves and should be able to reply to Data Subjects' requests in line with the legal requirements.

15.6.2 RIGHT TO RECTIFICATION

Data Subjects have a right to have incorrect data about them rectified.[43] In a Blockchain, however, this can be problematic as it is technically very difficult, albeit not impossible, to change data once they are added to the ledger[44] (hence the term "immutable").

If Personal Data are stored on-chain, one way to uphold this right is to add the new, rectified data to the chain – by way of a supplementary statement – while making the previous data inaccessible (for instance by deleting the decryption key needed to access the incorrect data). However, there is no consensus over this solution among practitioners and academics. In some cases, it is also possible to insert a new transaction indicating that the old data need to be corrected. The problem with these options, however, is that instead of correcting the original data, they merely add more data to the chain. It is unclear whether this would be accepted as rectification.

In view of these limitations, the best way to deal with these challenges is to store Personal Data off-chain, where it can be rectified without altering the ledger itself. Note that this option would to a large extent reduce the integrity and availability advantages of the Blockchain described above. In other words, if integrity and availability are also important for Personal Data, then a Blockchain-based solution is not recommended.

42 See Section 2.11 – Rights of Data Subjects.

43 See ibid.

44 Daniel Conte de Leon et al., "Blockchain: Properties and misconceptions", *Asia Pacific Journal of Innovation and Entrepreneurship*, Vol. 11, No. 3, 4 December 2017, pp. 286–300: www.emerald.com/insight/content/doi/10.1108/APJIE-12-2017-034/full/html. And the example of the Ethereum hard fork to correct the DAO hack: https://blog.ethereum.org/2016/07/20/hard-fork-completed.

15.6.3 RIGHT TO ERASURE

The nearly immutable nature of Blockchain stands conceptually in conflict with the right to erasure.[45] Various options have been suggested to address this issue. One option, as mentioned above, is to make the data on the chain inaccessible, albeit still present on the chain. This can be achieved, for example, by deleting the decryption key needed to decipher encrypted data. Yet some scholars and practitioners argue that this approach is unsatisfactory because the Personal Data in question, although encrypted, are not deleted (as the right to erasure implies) but merely made inaccessible. This could prove problematic in light of advances in decryption technology (see Section 15.5.4 – Data security, above).

Since Personal Data stored off-chain can be rectified and deleted in line with data protection requirements without altering the distributed ledger itself, this is again the preferred option.

EXAMPLE:
If a Humanitarian Organization uses Blockchain for Cash and Voucher Assistance (CVA), it is likely to ask beneficiaries to have a "wallet" on the Blockchain. The wallet works in almost the same way as a public key, i.e. it can be compared against a username that does not, by itself, identify the beneficiary. The organization will, however, probably maintain an off-chain database or beneficiary management system that links every wallet to a unique beneficiary.

Every time cash is transferred to a beneficiary, a transaction will be added to the Blockchain specifying how much was sent, to which wallet and when. Once the transaction is validated by the consensus protocol, it is immutably stored in the Blockchain. If beneficiaries request that their data to be erased, it is technically impossible to delete their wallet (which, like a public key, constitutes Personal Data) from the chain. One option in this case would be to remove the person from the off-chain database or management system, since this is the only place where the wallet is associated with an individual. Once the personal profile is removed, immediate Reidentification should no longer be possible.

15.6.4 RESTRICTIONS OF DATA SUBJECTS' RIGHTS

The above discussion on access, erasure and rectification shows how difficult it can be to exercise data protection rights when using Blockchain technology. Since public permissionless Blockchains are mostly incompatible with Data Subjects' rights, it would seem that the only solution is to store Personal Data off-chain. Yet these rights are not absolute and can, therefore, be restricted. The Data Controller is allowed to take into account

45 Finck, "Blockchains and data protection in the European Union", p. 30.

available technology and the cost of implementation when Data Subjects request to exercise their rights. Importantly, however, these restrictions may be acceptable only in exceptional cases.[46] Chapter 2: Basic principles of data protection, explains and exemplifies the situations in which Data Subjects' rights can be restricted. Questions remain as to whether it is possible to have a "data-protection-compliant" Blockchain in specific use cases where the Processing legitimately involves derogation from Data Subjects' rights. Even if it is judged legitimate to restrict certain rights, all other data protection principles (data minimization, necessity, proportionality, security, etc.) still apply.

15.7 INTERNATIONAL DATA SHARING

Data processed in Blockchain applications will routinely flow across national borders – especially in public permissionless architectures, which anyone anywhere could potentially join. This raises questions about data protection in Blockchain applications when data are shared internationally.[47] Although contractual clauses and other recognized mechanisms exist, such measures may be all but impracticable in a Blockchain.

Determining applicable law and jurisdiction can also present challenges. The proper and targeted risk analysis as foreseen in Chapter 4: International Data Sharing, is impossible unless choice of jurisdiction and choice of law are clearly embedded in Blockchain governance (e.g. in private permissioned Blockchains that limit the geographical location of those who can join the chain).

International transfers can be problematic in certain types of Blockchain, such as unlimited public permissionless Blockchains like the one used by the cryptocurrency Bitcoin. Here, there is no central party with control over who joins the system and stores a copy of the ledger. Private permissioned and other architectures can, however, provide more control and therefore help to mitigate such risks. It is therefore possible to attempt to address the transfers issue through Blockchain governance, for instance by embedding data protection guarantees (including by hard-coding them in the Blockchain architecture).

Data Controllers also need to inform Data Subjects if their data have been shared with other parties or transferred to a third country. This is generally not possible – albeit with limited exceptions – in public permissionless Blockchains, since anyone in the world could potentially join the system and store a copy of the ledger. In permissioned Blockchains, however, Data Controllers have more control and should therefore be able to comply with this requirement.

46 See Section 2.11 – Rights of Data Subjects.

47 See Chapter 4: International Data Sharing.

15.8 ANNEX: DECISION-MAKING FRAMEWORK FOR BLOCKCHAIN IN HUMANITARIAN ACTION

The following decision-making framework is intended to guide Humanitarian Organizations through the process of implementing Blockchain in Humanitarian Action:

STEP 1:

This step is common to the deployment of any new technology and does not apply exclusively to Blockchain. It consists of an initial information-gathering and scoping exercise that should answer the following questions:

- What problem might a Blockchain solution address?
- To which programme will it apply, and what are the programme's needs?
- Is a Blockchain system the least invasive, most risk-averse and most controllable technology available to address the problem at hand?
- In what context will the Blockchain function?
- Where will it function (in one country or region, worldwide)?
- Who are the stakeholders (beneficiaries, local authorities, financial partners, mobile operators, other Humanitarian Organizations, etc.)?
- What are the objectives of the technology (increase internal efficiency, improve positioning, expand existing programmes, meet donor requirements, manage risks, etc.)?
- What are your existing governance arrangements and IT capacity? Can the technology be implemented, and can the associated risks be managed, under current arrangements and capacity?
- Is it clear how the technology will contribute to the local information ecosystem?

STEP 2:

Determine if a Blockchain-based system is necessary to attain the objective(s) of a humanitarian programme or other initiative, taking into consideration the advantages and challenges related to the technology, as identified above, in the particular context in which it will be implemented. Your organization should seek to understand what its needs are, whether or not Blockchain will fulfil those needs, how Data Subjects will experience the system, how their rights will be respected, and whether the same needs could be fulfilled by another system that better protects Data Subjects and their rights. You should ask the following questions:

- Does the order of (trans)actions matter?
- Is there a central authority you can trust?
- Do you need to store data?
- Is there buy-in from your governance/IT support team?
- Do you understand how your system will contribute to the local information ecosystem?

STEP 3:

If your organization decides that its objective can only be achieved with a Blockchain solution, you need to determine what type of Blockchain is most appropriate or necessary. Ask the following questions:

- Do you need to store state? This means whether or not your system needs to store the status and conditions of the system and not only to perform the action.
- Are there multiple contributors? This means contributors that can directly write data to the system. In a classical ecommerce use case where all users access the database through the merchant's website, the merchant is the single contributor as users cannot access the database without the merchant's control. Note that in the case of Blockchain, there are several roles to take into account.
- Can you use an "always-online" trusted Third Party (TTP)? A TTP is the entity that executes certain functions centrally, typically to validate the transactions.
- Are all contributors known?
- Are all contributors trusted?
- Is public verifiability required? It is important not to conflate public verifiability with the publication of audit or transparency report. It is meant here to have a provable verifiablity (in the mathematical sense) of the data.[48]

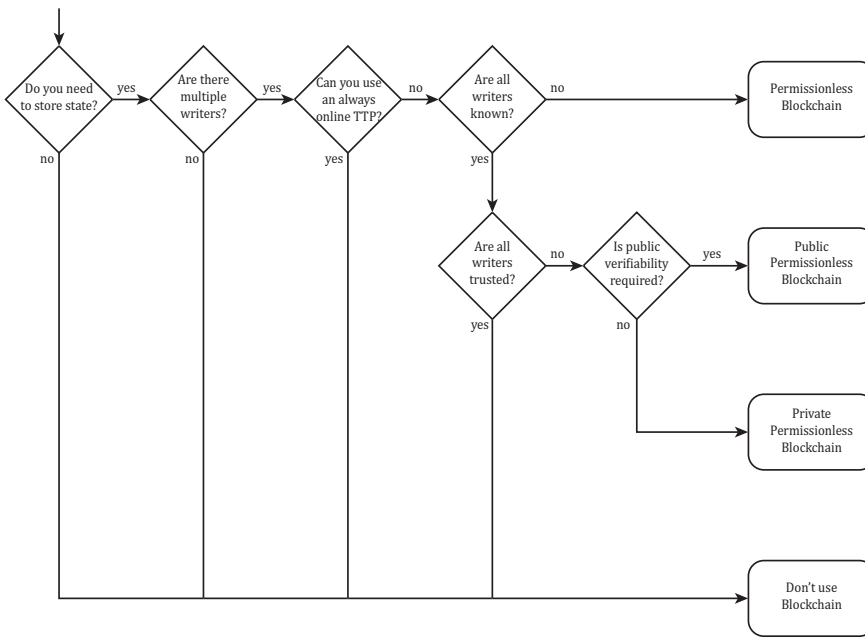

Figure 15.1 Decision tree.
Adapted from Wüst and Gervais, "Do you need a Blockchain?", IEEE, 2018.

48 Wust and Gervais, "Do you need a Blockchain?", IEEE, 2018.

STEP 4:

Consult your DPO, IT support and peers:

- Ask for guidance.
- Make use of the experience of others. For example, consult peers that have developed a similar system or used the off-the-shelf solution you intend to use, and seek advice from Blockchain experts.

STEP 5:

Conduct a DPIA to identify and assess Personal Data Processing impacts. A DPIA should include questions such as the following:

- What is the applicable law? Is it applicable to all stakeholders?
- What types of Personal Data are processed? Which of these are necessary for the transaction that will be stored on the Blockchain?
- Is the Processing fair, lawful and transparent?
- What are the alternatives to storing Personal Data on the Blockchain itself? Is off-chain storage possible?
- Are the Data Subjects able to fully exercise their rights? If not, are the restrictions lawful and proportionate?
- Who has the power to determine the governance of the Blockchain?
- How does the platform operate?
- Who can alter the platform and under what circumstances could entries on the ledger be updated?
- What are the risks posed by the chosen technology? How will each risk be treated and mitigated?
- How can individuals exercise their rights?

STEP 6:

Implement the principles of data protection by design and by default:

- Both principles require continuous monitoring and revision of technical and organizational measures, taking into account the following: available technology; the cost of implementation; the nature, scope and context of the Processing; the purposes of the Processing; and the risks (of varying likelihood and severity) to the rights and freedoms of natural persons posed by the Processing. A new DPIA should be conducted whenever there is a relevant change in the technology used or the type of data collected.
- Data protection by design involves considering factors such as:
  - compliance with data protection principles (lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality);
  - the rights of the Data Subject (e.g. notification, access, erasure, rectification);
  - other data protection obligations (e.g. accountability and security).

- Data protection by default involves considering factors such as:
  - what types and categories of Personal Data are processed;
  - the amount of Personal Data processed;
  - the purpose for which they are processed;
  - the storage period;
  - accessibility.

The above framework is summarized in the chart below. If, at the information-gathering stage, your organization concludes that other systems may be more appropriate than Blockchain, then you should not proceed past step 1.

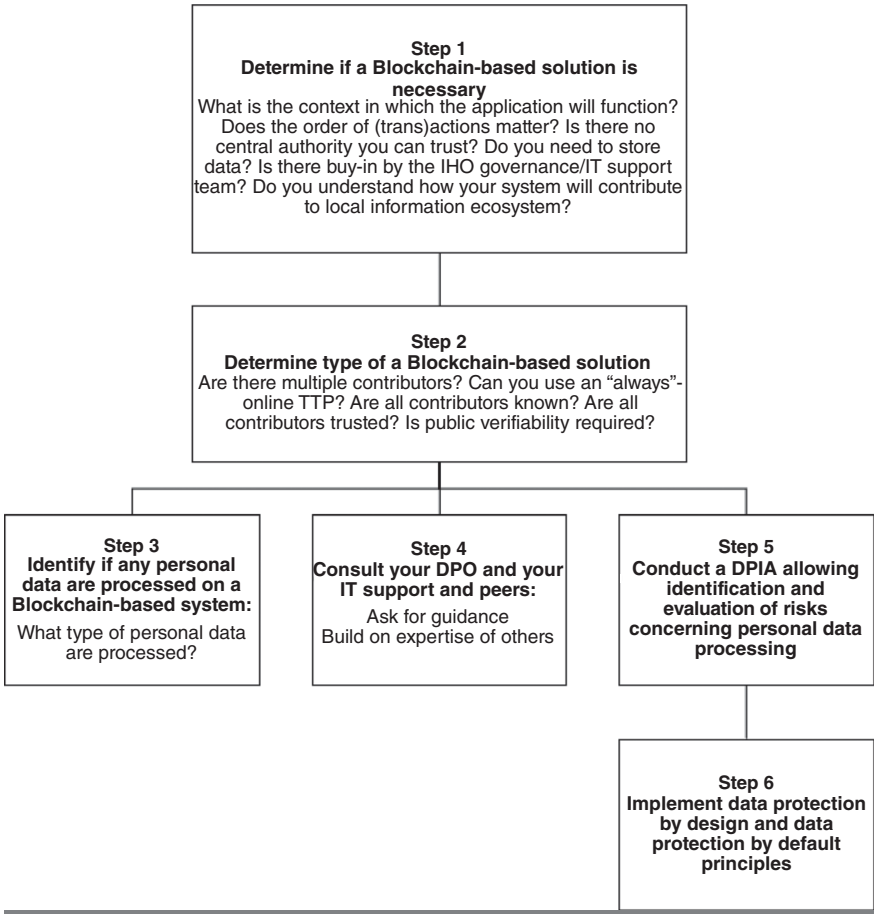

Figure 15.2 A Blockchain-based solution for humanitarian assistance.
Adapted from Wüst and Gervais, "Do you need a Blockchain?", IEEE, 2018.