node must process every transaction. Each time a transaction is added to a blockchain, the digital ledger is updated on all of the nodes simultaneously. Therefore, the goal of ensuring that data is stored and processed locally is automatically met. Requirements that take the form of government approval to transfer data would, however, have an impact on the ability of potential participants in the countries concerned to participate in blockchain consortia that bring together actors from various jurisdictions.

As for data privacy issues, Blockchain is often presented as an opportunity or catalyst for greater personal data protection and new forms of identity management. The use of various cryptographic tools gives users control over their personal data, allowing them to manage and share their personal data only with trusted parties.[27]

One must here distinguish between public and consortium/private blockchains. A specific feature of public blockchains, such as Bitcoin, which is often emphasized, is the fact that they allow transactions between parties without any party having to disclose their identity to any other party or to the public. While today, we mostly do not control who processes our personal data and how, public blockchains make it possible for the data subject to remain anonymous or to use a pseudonym and to control how their data is used. However, whereas it is true that no personal information, such as names, addresses or telephone numbers, is captured in the corresponding transaction data entries of the blockchain, one study showed that it is nevertheless possible to trace the IP address and thereby to de-anonymize clients – although the problem is not inherent to the technology and could be addressed by fixing the technical design of the blockchain (Biryukov *et al*., 2014).

While public blockchains enable the users themselves to implement the principle of "privacy by design" (Biryukov *et al*., 2014) at an individual level, consortium/private blockchains provide for this principle at the platform level: privacy levels are determined by the management of the platform. In such platforms, participants are known and identified, but permissions to read and write some of the data added to the platform can be restricted to certain participants in order to protect confidentiality (see Section 2.3). What is clear is that entities using a blockchain-based platform have to ensure that the technical design of the platform meets the requirements of the relevant regulatory framework(s), including data protection laws.

The deployment of the technology could, however, be limited by the rights granted to individuals under national data protection regulations. Much has been said, for example, about the possible incompatibility between the European General Data Protection Regulation (GDPR), which entered into force on 25 May 2018, and Blockchain, leading some to ponder whether the GDPR might not ultimately "block blockchain" (Toth, 2018).