nodes, which would be difficult in practice, although not impossible. In theory, a blockchain network can be compromised if a validator or pool of validators control more than 50 per cent of the network's computing power, which is called a "51 per cent attack". While the 51 per cent attack is a problem common to all types of blockchains, it is particularly critical in the case of public blockchains, given the difficulty of determining who effectively validates blocks.

A particular feature of public blockchains is the considerable amount of computational power that most of them require to validate transactions, in particular those using the Proof of Work consensus mechanism, such as Bitcoin (see the Annex for more information). Though wasteful in terms of energy expense, Proof of Work is required to ensure the safety of the consensus process. It makes the public blockchain mathematically very hard to hack as the cost of hacking becomes too high for a system where every node connected is synchronized with the entire blockchain network. Hence, although hacking the system is not impossible, it is economically inefficient and practically extremely hard. However, computing power capacity is increasingly being aggregated. The 51 per cent vulnerability is, to date, still subject to heated debates regarding the severity of its potential consequences.

Interestingly, most recent developments could render discussions on so-called "51 per cent attacks" obsolete. In a paper released in August 2018, Vitalik Buterin, Ethereum's co-founder, proposes a new consensus algorithm that, allegedly, requires just 1 per cent of the nodes to be honest and eliminates the risk of a 51 per cent attack (Buterin, 2018). In other words, an attacker who wanted to control the network would have to control 99 per cent of the nodes of the blockchain and not just 51 per cent. The 51 per cent attack may soon be called a 99 per cent attack.

(a) Blockchain versus distributed ledger technology (DLT)

Because it is simple and catchy, the term "Blockchain" is often used to refer to distributed ledgers whatever their specific features are. Blockchain, however, is only one type of distributed ledger technology (DLT) – one that compiles transactions in blocks that are then chained to each other. Blockchain is the most well-known and most tested distributed ledger technology, but an increasing number of models of transaction flows are being developed which, like Blockchain, use a blend of cryptographic techniques, but which are moving away from the concept of "blocks" – or even from both the concepts of "blocks" and "chain". "New kids not on the blocks" include IOTA,[11] Ripple[12] and Hashgraph.[13] Although these new models are not blockchains *per se*, the term "Blockchain" is now commonly used to refer to distributed ledger technology in general and to the phenomenon surrounding DLT. In order to facilitate reading, the present publication, like many others, will use the term "Blockchain" to refer more generally to "distributed ledger technology".