ledger, contained a fault that, under certain circumstances, allowed escrow accounts[5] to be emptied out (Brandon, 2016).

In spite of this unfortunate event, smart contracts are one of the blockchain characteristics that harness the most interest today in hundreds of applications in all domains because of their flexibility and the possibility to automate processes.

Over the last few years, an array of newer distributed ledger technologies has been developed to improve on the capabilities of the Bitcoin and Ethereum networks and promote new use cases[6] (see the next section for more information on the relationship between Blockchain and distributed ledger technology). IOTA, for example – which is a distributed ledger technology but not a blockchain *per se,* as it does not combine transactions in blocks, nor does it chain them in a linear manner – was launched in 2016 as a cryptocurrency platform designed for machine-to-machine communication.[7]

In addition, various consortia were formed to develop solutions tailored to the needs of businesses. The R3 consortium, for example, which brings together more than 200 companies, regulators and trade associations, developed its own distributed ledger platform called Corda, geared towards the financial world.[8]

Another well-known initiative is Hyperledger, which is hosted by the Linux Foundation, a non-profit organization that brings together industry leaders in finance, banking, Internet of Things (IoT) (i.e. machine-to-machine devices), supply chains, manufacturing and technology to advance cross-industry blockchain technologies. Hyperledger is a collaborative effort to develop enterprise blockchain-based frameworks and tools in open-source and related tools. Hyperledger is now widely used in various fields, including international trade.[9]

2. Blockchain 101

A blockchain is a digital record of transactions – or ledger – that is decentralized (no single entity controls the network – although "private" blockchains have emerged that provide for a greater degree of centralization – see Section 2.3), distributed (records are shared with all participants) and secured using a blend of proven cryptographic technologies. A blockchain is managed by computers or servers – called "nodes"* – on a peer-to-peer basis without the need for the intermediaries who traditionally authenticate transactions (such as banks in the case of financial transactions). Data added to the blockchain are shared with all participants in the network and are verified and validated by anyone with the appropriate permissions on the basis of the consensus protocol* of the blockchain (see Figure 1).