evidence, provided and validated by peers, moving away from single points of failure that exist in the traditional model of privacy (i.e. the banks in fiat currency[3] systems). The new model, Satoshi Nakamoto argued, solved the issue of "double spending" – the fact that digital currencies can be spent more than once because the digital file can be duplicated. Furthermore, the new system allowed for transactions to be public while the parties involved are anonymous, thus enhancing transparency while preserving privacy. Finally, the immutability and time-stamping* features of Bitcoin offered appealing assurances against fraud at a juncture where big players in the financial system were in the headlines for tampering with book-keeping and market metrics.

While Bitcoin was the first real-life application of Blockchain, blockchain technology is in fact a combination of several underlying techniques that have been in existence for at least four decades. For the five years that followed the creation of Bitcoin, the history of Blockchain remained nearly synonymous with the history of Bitcoin. It was only from 2013 that the blockchain technology started to make a name for itself as a result of its use in other cryptocurrencies, such as Ethereum (see Investoo Group, 2017), and more recently beyond the financial technology (fintech) industry.

The creation of Ethereum marked the second milestone in the history of Blockchain. In 2013, a 19-year old programmer, Vitalik Buterin, published a white paper that laid out his plan for a blockchain system that could also facilitate "decentralized applications" (Buterin, 2013). He proposed to achieve this in large part by building a programming language into Ethereum that developers could customize to fit their purposes.

Ethereum, sometimes referred to as "Blockchain 2.0", was released in late 2015. Ethereum's quantum leap lies in the concept of smart contracts*, i.e. computer programmes that self-execute the terms of a contract when specific conditions are met. Smart contract applications run exactly as programmed without fraud, third-party interferences, or delay. Automating transactions in this way constituted a revolution within the revolution and is one of the most valuable features of Blockchain for trade.

Probably the next most memorable milestone in the history of blockchain was the attack of Ethereum's decentralized autonomous organization[4] (DAO) in mid-2016. The DAO was meant to operate like a venture capital fund for the cryptographic space and was built as a smart contract on top of the Ethereum blockchain. A few weeks after its launch, the DAO was subject to a hacker attack that siphoned off millions of dollars' worth of assets and led to its collapse, leading many blockchain sceptics to question the very premises of the technology, i.e. its immutability and resistance to attack (see also Siegel, 2016). The problem was not the blockchain technology itself; it was the coding of the contract programmes that powered the DAO. The programmes, which had been built on top of the Ethereum blockchain