Endnotes

1. The concept of cryptographically secured chains of blocks was first described in 1991 by Haber and Stornetta (1991), but it was only in 2008-09 that the technology was effectively implemented.

2. A cryptocurrency is a digital currency that uses cryptography for security. See Nakamoto (2008).

3. A fiat currency is a currency that a government has declared to be legal tender, but that is not backed by a physical commodity such as gold or silver.

4. A decentralized autonomous organization (DAO) is an organization that is run autonomously through rules encoded in smart contracts. For more information, see: https://blockchainhub.net/dao-decentralized-autonomous-organization/

5. An escrow account is a special financial account for the temporary deposit of funds before they are paid out (or returned) at the conclusion of a specific transaction.

6. A use case is a software and system engineering term that describes how a user uses a system to accomplish a particular goal (definition from Techopedia).

7. See https://www.iota.org/

8. Corda is a shared ledger rather than a distributed ledger. Unlike blockchain networks, which replicate data across every member of the network, on the Corda platform, only those parties with a legitimate need to know can see the data within an agreement (see http://www.r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services).

9. See https://www.hyperledger.org/about.

10. The term “Blockchain” can refer to the blockchain technology itself, or to an application using the technology, i.e. a specific platform or network of users (called nodes) to provide a specific service.

11. Launched in 2016 as a cryptocurrency designed for the Internet of Things, IOTA is a public ledger with no chains, no blocks and no fees. It uses a new technology called the Tangle: instead of being compiled in blocks and chained to each other, IOTA’s transactions are connected in a big tangled web (see https://iota.readme.io/docs/what-is-iota).

12. Originally released in 2012, the Ripple protocol is meant to enable the near instant and direct transfer of money between two parties from any type of currency. While it is consensus-oriented, Ripple is technically not a blockchain. It summarizes the data into a single value rather than a block.

13. Hashgraph is a new consensus alternative to Blockchain that does not compile transactions in blocks. It uses a consensus protocol that, according to its developers, is faster, fairer and more secure than blockchains and has led many observers to ponder whether Hashgraph has made Blockchain obsolete. It is, however, not yet an open source, and proper analysis and benchmarking are still required before such claims can be upheld.

14. In fact, in the case of Bitcoin, the system as originally designed had anticipated that the transaction fee would be optional, at least as long as the miners are rewarded through Bitcoins (as Bitcoin was voluntarily designed to be deflationary, only a finite amount of Bitcoins can be generated in the system and the currency is bound to run out eventually). However, recent reports note that not only has a transaction fee become almost the only way for users to get their transactions into the