Glossary

Asymmetric key algorithms

One of the two types of algorithms used in encryption.* Asymmetric key algorithms use different keys to encrypt and decrypt the information and fall under the category of public-key cryptography. This type of encryption involves two keys that work in a paired fashion: a public key that is accessible to third parties, and a private key that is kept secret by the generator of the pair. The use of different keys makes this type of cryptography more convenient to implement than private-key cryptography, but increases the risk of malicious attacks. To mitigate this risk, an additional layer of security is provided by the introduction of security certificates, which are digital certificates that link a public key to a particular entity or individual, delivered by trusted certificate authorities.

Blockchain

A blockchain is a time-stamped and distributed digital record of transactions (or ledger) that is secured using various cryptographic techniques. It is a continuously growing list of records, called "blocks", which are "chained" to each other using cryptographic tools. Blockchain is the technology underpinning Bitcoin. The term is often used interchangeably with distributed ledger technology. Correctly speaking, however, blockchain technology is one type of distributed ledger technology.

Byzantine Fault

Byzantine faults or failures can occur because of software bugs or when a node is compromised, causing nodes to behave erratically. This type of fault was identified by Lamport *et al.* (1982) as the Byzantine General's Problem:

> "A group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the