CHAPTER 1 INTRODUCTION TO BLOCKCHAIN

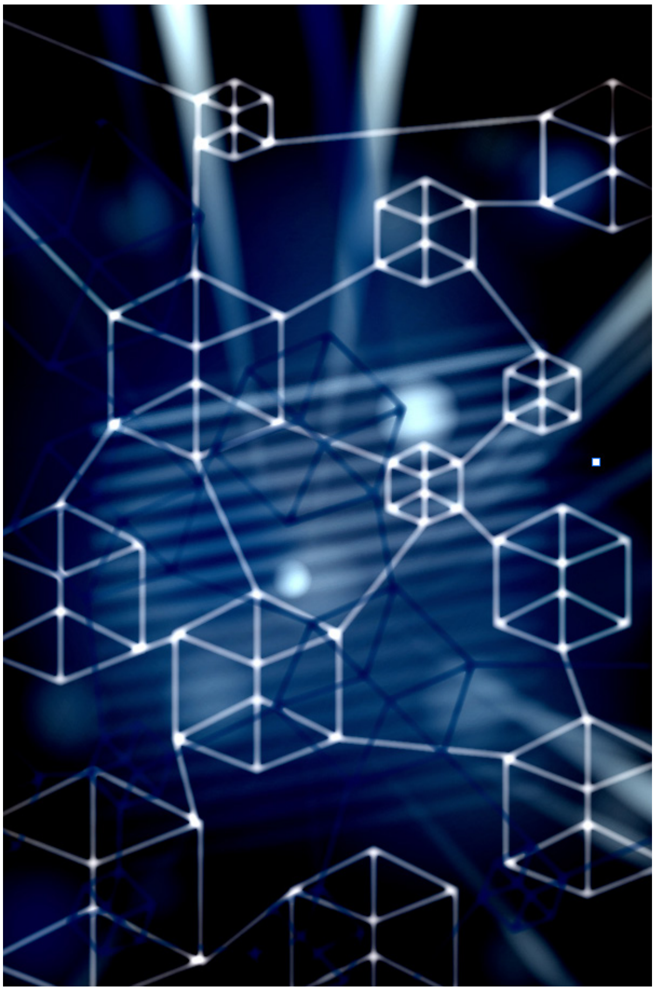
Blockchain technology is attracting a lot of interest as it offers the potential to improve data security in a variety of ways. Currently in an exploratory phase, blockchain experts are considering how the technology could be employed effectively across multiple industries.

EMERGENCE OF BLOCKCHAIN

While progress is fast, these experts need to remain vigilant and methodical since those who make their living from illegally accessing information are always looking for ways to overcome data security systems. Demand is high for blockchain experts. However, those experts were once beginners too. This book sets out to demystify the terminology and processes involved in blockchain technology and to consider some of its potential applications.

Blockchain is, at once, both infinitely simple and complex. Indeed, the concept is technologically simple enough that the earliest mention of the blockchain dates to 1982, with the oldest continuing blockchain released via publication in *The New York Times* in 1995 by Stuart Haber, W Scott Stornetta, and Dave Bayer under their company, Surety. This blockchain is still published each week in 2022.

Yet in the 2020s blockchain is still considered by many to be inscrutable, and hard to make sense of outside the IT and financial technology sectors. If this is the case, how can it have existed so long? The important thing to understand when thinking about the blockchain is that blockchain and digital currencies such as bitcoin are separate. They are related, but not the same. Once the concepts are looked at as separate entities, it is easier to think about what the blockchain actually is.

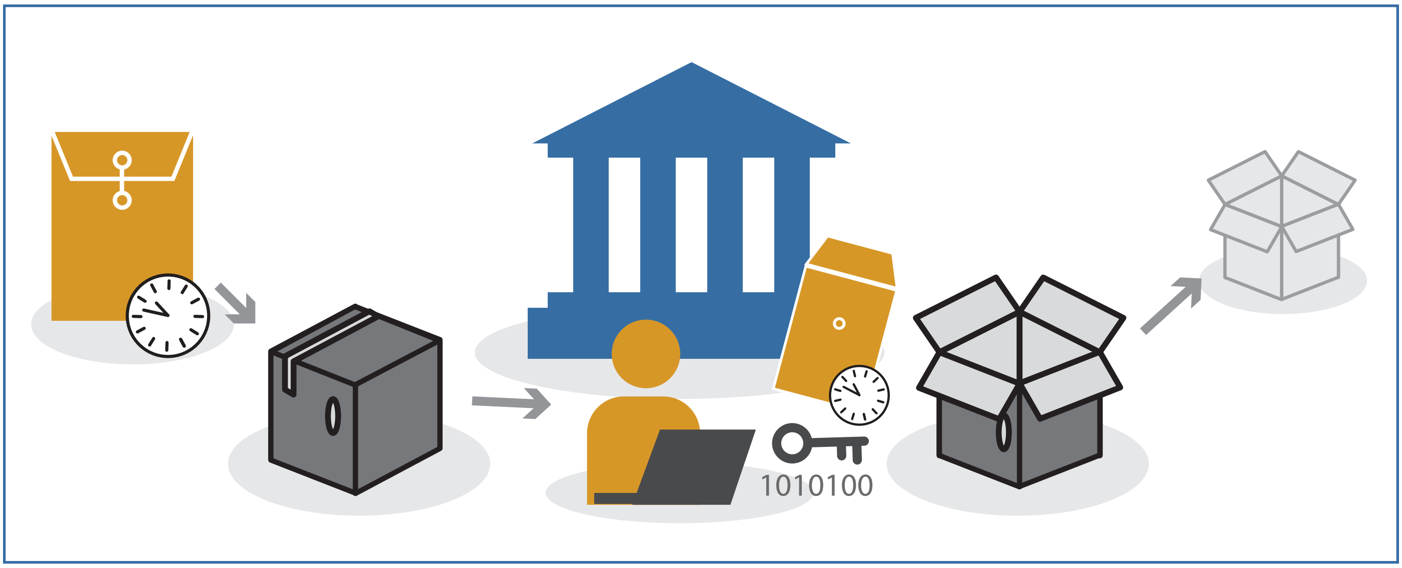


Conceptualising the Blockchain: A Method of Information Transfer

At base, the blockchain is about the movement of information. There is a simple analogue for this, one most people have experience with: the humble mailbox.

Mailboxes provide a way for packets of information — letters, parcels — to move from one person to another, one party to another, one organisation to another. This information could be a postcard from Steph to Megan, or a contract between Sara and her employer, GenTech. It could be a bank statement from Worldwide Bank to Small Flower Company, or a delivery of assets complete with a bill of lading, or even a cheque to transfer funds from Alice to Craig. Any of these things — all these things — are, in their most raw forms, types of information that pass-through mailboxes. It is important to remember, though, that mailboxes are used repeatedly. Each party has just one mailbox, one address, and it never changes.

The blockchain is also about the flow of information from one party to another. Unlike a regular mailbox though, it is comprised of single use blocks. To extend the mailbox analogy, the blockchain would be like having a series of custom-built mailboxes, with a new mailbox built for each individual packet of information that is sent out.



Example

Consider: Sara has a series of important transactions to complete with her bank. She needs absolute privacy for these transactions; she has been the victim of identity theft in the past and she does not want anyone else to intercept the flow of her information. Each time she sends out her data packet, she addresses it to a custom-built mailbox at a special address. Once Sara has sent her data packet, nothing in it can be changed or tampered with, which provides her with additional security.

The first data packet goes to Mailbox A, which the bank then unlocks with a special key and a code Sara has sent them. Once the data has been removed, Mailbox A is defunct.

The second data packet goes to Mailbox B, which the bank then unlocks with a special key and a code Sara has sent them. Once the data has been removed, Mailbox B is defunct.

The third data packet goes to Mailbox C, which the bank then unlocks with a special key and a code Sara has sent them. Once the data has been removed, Mailbox C is defunct.

Each mailbox is accessible only to Sara and the bank. Each data packet Sara sends out is time-stamped, so the bank knows when it was sent, and that the packet has not been tampered with.

Purpose building a mailbox takes time, though — it is not a low-stakes endeavour, so custom mailboxes would only be used for very special pieces of mail, like very sensitive personal information.

The blockchain works in essentially the same way — each new block added to the chain carries a new data packet. However, just like the mailbox example, using the blockchain for transferring information isn't a low-stakes endeavour either, and requires significant expenditure in terms of resources. This means it is only used for sensitive information or information for which some aspect of the blockchain is viewed as of greater benefit.

A key facet of the blockchain, however, is that rather than depending on just one person or organisation, the blockchain works with many — it crowd sources the flow of information, having each user check and agree the information is correct before sending. This type of crowdsourcing is referred to as a decentralised approach. A block is only added to the blockchain once the data in the block has been verified.

Why Use the Blockchain?

Knowing that the blockchain is difficult to use and resource intensive, why would someone choose to use it to transfer information when there are other, simpler ways available? Is it popular simply by virtue of its seeming newness? There are three core benefits in using the blockchain:

- Privacy
- Tracking
- Immutability

The blockchain can be leveraged into a variety of different use cases across industries, and the reasons for this always come down to one or more of the above three benefits in conjunction with the decentralised nature of the technology.

Privacy

The blockchain uses a cryptographic function to encode each block. Using a cryptographic function adds a layer of privacy.

The single-use feature of each block, however, means that there is a new cryptographic function for each block, which helps create additional layers of security. The decentralised nature of the blockchain and the consensus protocol, to be covered later, create even further layers of privacy.

This makes the blockchain desirable for a variety of different applications where privacy is required. These can range from individuals looking to minimise their digital footprint in more totalitarian regimes through to organisations handling large amounts of data through customer relationship management (CRM) systems looking to improve security practices and reduce the likelihood of data breaches, particularly in industries such as banking and securities.

Tracking

When each block in the blockchain is created, it is timestamped and “fingerprinted”; it carries a digital signature that’s generated as part of the process. This means the information can be tracked throughout its journey, each block can be tracked and confirmed. The data, although encrypted, is known to exist.

There is another layer to this, the cost of verification. This refers to the cost of verifying that something has happened e.g., a transaction, like a house sale, has actually occurred. Blockchain uses decentralised technology, depending on users to verify each block. When each user (or rather each user’s computer) agrees, a consensus is reached; it is only once this consensus has been reached that the block is added to the blockchain. This type of tracking is arguably less costly than traditional methods used in many sectors, *but it is also much more transparent and trackable* than traditional methods as blockchains are available for public viewing. It is only the data contained within the blocks that is inaccessible.

Immutability

Immutability is the quality of permanence, of being unchangeable. When a block is released on the blockchain, it is immutable, locked, and unchangeable. This means that the block is tamper-proof, and that the information can be considered secure. This is important when transferring information, and increased security is one of the reasons many industries have begun to explore the possibilities in this technology. To use the mailbox