Article Information

Author: Michael Bacina
Service: Blockchain

Beyond the Hype Cycle: Blockchain explainer

Piper Alderman's Blockchain Group has been at the forefront of the blockchain revolution, advising leading Australian and international projects using this exciting new technology to gain greater business efficiencies, forge new business models and disrupt incumbent intermediaries. We regularly present explainers on Blockchain, and in this article we set out a primer and some examples of how Blockchain technology operates, to assist you in understanding some key concepts in the technology.

What is a blockchain?

There are a variety of definitions emerging in legal systems. At a high level, a blockchain is a kind of distributed ledger technology, popularised by the cryptographic token known as "Bitcoin". We will use the Bitcoin Blockchain in our examples below, but you should keep in mind that cryptocurrencies such as Bitcoin are but one use of Blockchain technology, much as email is a useful application built on top of internet technology.

The critical concepts underpinning blockchain (as it relates to the Bitcoin blockchain) are:

1. It is a decentralised, as opposed to a centralised, network; with
2. A distributed validation of transactions occurring through the network; and
3. Those transactions are signed using public/private key cryptography and the use of hash records between blocks of records.

Centralised vs Decentralised Networks

Most of our interactions online, with or without our knowledge, involve us exchanging information, including our personal information and our financial details, when entering into a transaction. We regularly rely on intermediaries such as banks, online payment systems like PayPal, Dropbox and social media websites to store our information or transfer value (including funds).

All of this data is managed and controlled by central entities, usually at a single location or server. Such systems are susceptible to failure of that single point, via hacking, physical theft or fraud/corruption. These are what are known as "**centralised**" networks. The opaque nature of this kind of record keeping leads to adverse incentives in many business interactions (including within organisations themselves) and keeps the value of the data siloed. Data siloing may make sense in the short run, but in the long run makes it more costly to unlock the value in that data.

Blockchain promises a new era of transparency and censorship resistance, with new business possibilities and greater efficiencies. This is enabled in part by shifting from relying upon a central party in a network, to a more decentralised or even distributed network where a consensus of parties in the network co-operate together to enable the network to operate.

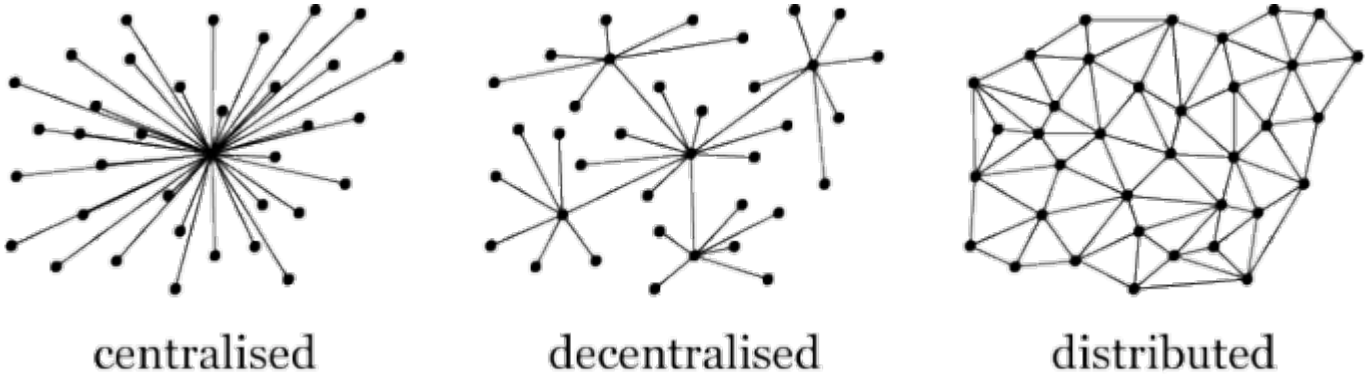


Figure 1: Centralised, Decentralised and Distributed Networks

Consider an example the following; once upon a time people would pay most bills using a quaint piece of paper called a "cheque" (or in the US/Canada a "check"). Payments made by cheque were processed (or "cleared") by a cheque being presented to a party for payment, and that cheque would ultimately find its way to the issuing bank, where a small army of clerks would verify that the account on which the cheque was drawn had sufficient funds available, and move those funds from the ledger of the party issuing the cheque to the ledger of the recipient thus "clearing" the payment.

In the example of the cheque, the bank and it's employed clerks would be referred to as a "centralised" system. Within the bank, internal processes govern which transactions will be escalated and how potential fraud is to be defeated. Computerisation and automation has now replaced these clerks, enabling much faster processing of payment requests, such that cheques are now rarely used in Australia.

In the same way a bank keeps track of transactions in its ledger, the Bitcoin blockchain (for example) simply records changes in a ledger which shows which wallets (i.e. the who) hold various amounts of Bitcoin (i.e. the what) and which transactions have occurred on the blockchain up to that point (i.e. the how).

However, the fundamental difference is that whereas a bank keeps a central record of transactions in its centralised ledger, the Bitcoin blockchain's ledger is stored on every single node in the network.

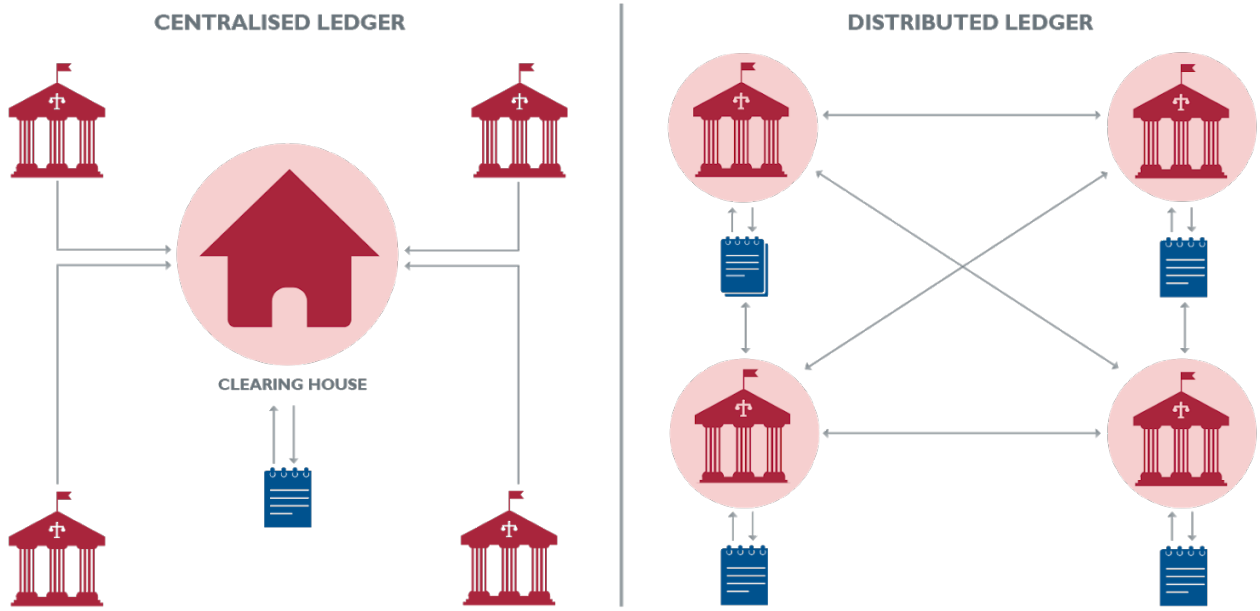
Anyone can set up a Bitcoin wallet and download the entire record of Bitcoin transactions (at the time of writing about 185GB of data) and anyone can set up a "mining rig" and run a machine which, in essence, provides that function which, once upon a time, a clerk employed by a bank performed. All those nodes check with each other that they have the correct copy of the blockchain they are storing, keeping the whole system secure.

The transactions validated by the miners on the Bitcoin blockchain are bundled up into "blocks" of transactions which are chained together using a hash leading to the name of the system.

In this way, the Bitcoin blockchain *is the bank*, leading to the slogan "be your own bank". Bitcoin has the longest track record of any cryptocurrency in use and security. The Bitcoin blockchain itself has never suffered a hack or loss of funds in the way that banks have collapsed due to internal fraud, but it has suffered the growing pains inherent in any new technology (and there are plenty of hacks focusing on users).

CENTRALISED OR DISTRIBUTED LEDGER?

A DISTRIBUTED LEDGER IS A NETWORK THAT RECORDS OWNERSHIP THROUGH A SHARED REGISTRY



Validation of Transactions

In order to validate a transaction in a ledger, the party performing that task needs to know the balance in the account/wallet the subject of the transaction. In a centralised system, this is pretty straightforward, as only one party has the ledger and can decide if a transaction submitted is approved. In a decentralised or distributed ledger, many parties need to agree on the "truth" of a transaction, that is reach a consensus, before it can be accepted as correct and true. Where there are multiple parties verifying transactions, the risk of a malicious actor entering the system is very real.

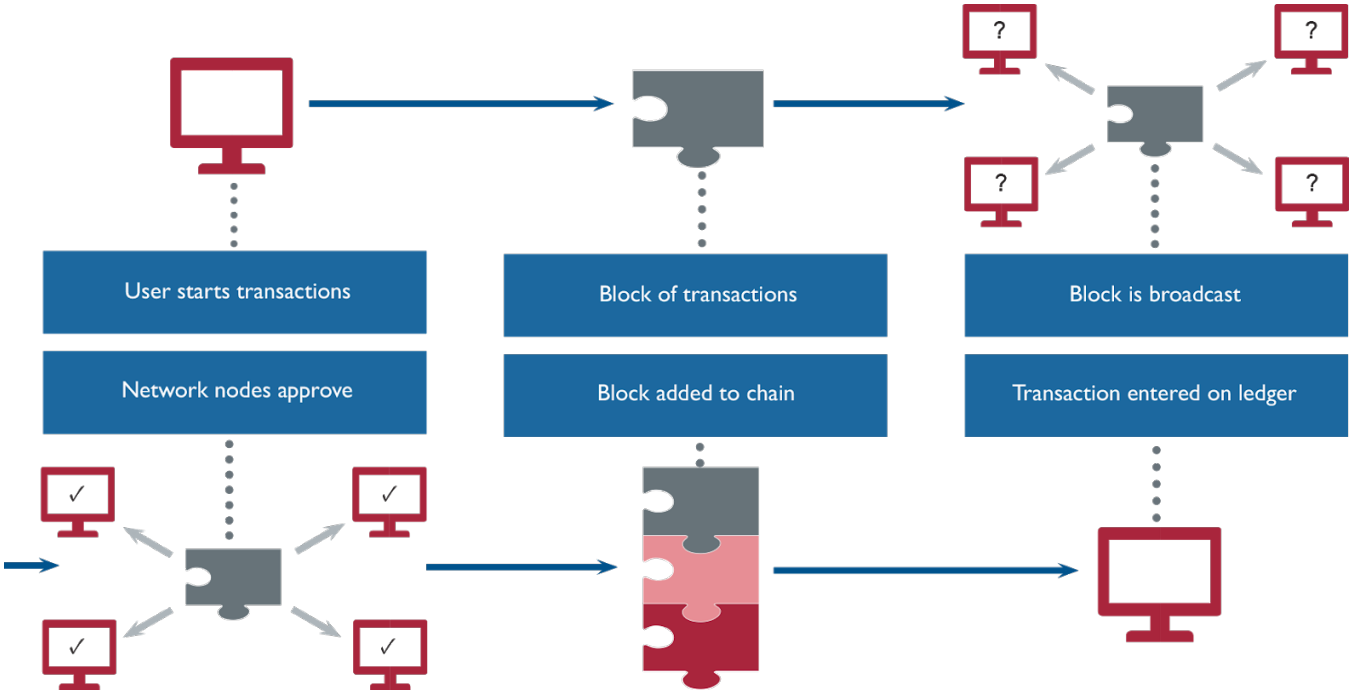
Consider an example using the childhood game of "Chinese Whispers" or "Telephone", where a circle of participants take turns passing on a phrase, by whispered it from one person to the next. When the circle has passed the phrase around it is revealed, together with the starting phrase.

The phrase has inevitably been changed at some point in the circle, by someone who either misunderstood, or deliberately alters, the phrase.

In the blockchain context, the person seeking to change the information would be considered a malicious actor. If there was no way for the parties seeking to verify transactions to communicate the information with each other, then a malicious actor could interfere.

The Blockchain equivalent of "Chinese Whispers" or "Telephone" would be each person, upon being told the phrase, shouting to the rest of the circle what the phrase is, so that as the information makes its way around the group, everyone can agree upon what the phrase is at each stage.

Similarly, transactions in the Bitcoin blockchain are broadcast to all the nodes in the network, which each node can then verify against their copy of the blockchain. Should enough nodes in the network agree, or reach "consensus" that a block of transactions is valid, then it is appended to the previous block.



Hashes, more than just something on Twitter

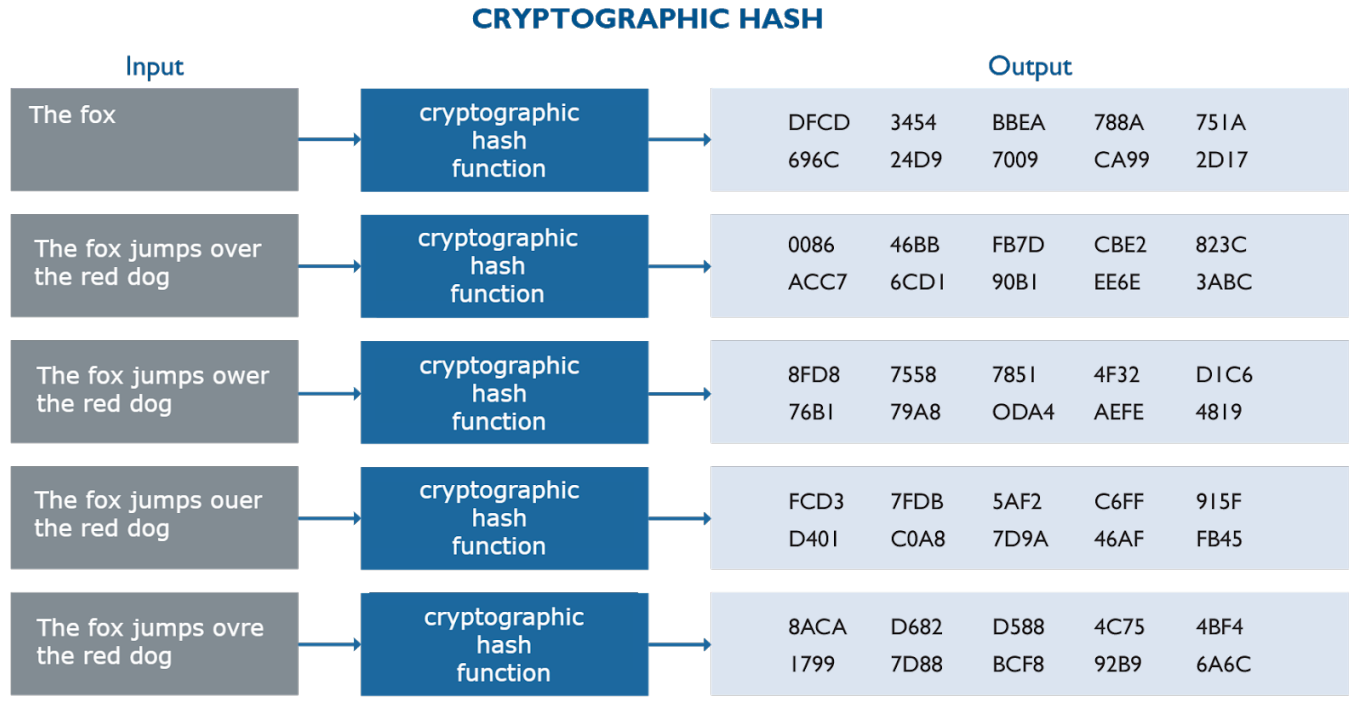
To go a little deeper, we are going to have to address cryptography. It is all well and good for a distributed network to compare transactions to a chain of previous transactions, but how can someone who downloads the blockchain know that the copy they downloaded is in fact correct and hasn't been tampered with?

The answer, is the use of hashing. Hashing is a process by which digital information is put through an, in effect, one way algorithm which generates a string of numbers and letters. It is next to impossible to take a hash and reverse it back into the input which generated it.

Cryptographic hashes were historically used to enable information to be stored by one party without that party knowing the content of that information, in a way that enables another party (who does know what that information is) to demonstrate that knowledge.

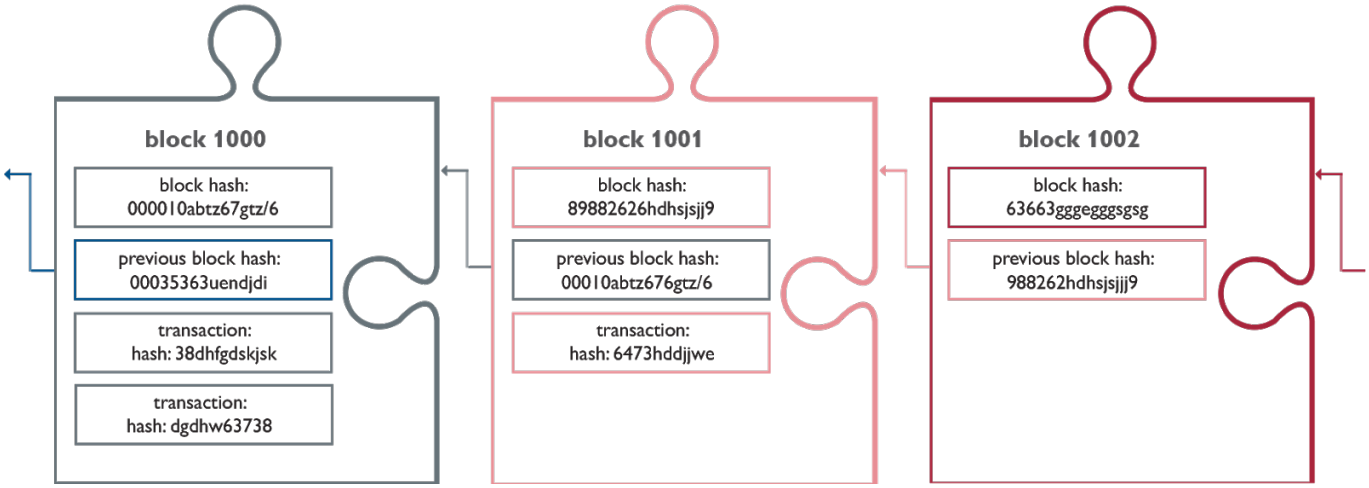
Consider the phrase "the quick brown fox jumps over the lazy dog". If, for example, this phrase was your password stored as plain text when you set up a website account, and the database was hacked, then your plain text password is in the hands of malicious actors, who can quickly use it to get the jump on your and access and misuse the information.

If, however, the phrase is put through a cryptographic hash algorithm first, then it will become just a string of numbers and letters. That is what is stored on the blockchain as your password. If the database is compromised, it is much more difficult for a malicious actor to discover your password as a result. The hackers would have to effectively guess your password to use the hash output to discover the input. Even small changes in the input to a hashing algorithm result in massive differences to the output.



How does this work in blockchain?

The transactions, when bundled together into "blocks" use a starting hash and a closing hash. The starting hash is taken from the block immediately prior and the closing hash is generated from the starting hash together with all of the data in that block.



If there is a change to a **single digit** of any part of the data in a block, the closing hash for that block will change, and since each block is dependent upon the block immediately prior in the blockchain, the change is instantly identifiable.

Practically, this means that the network of nodes can reject any blocks, or a copy of the blockchain, where the chain has been altered to "rewrite the past".

Public Private Key Cryptography

The final piece of the puzzle is how a user on a public blockchain like Bitcoin can move value around (i.e. the Bitcoins). A technology known as public private key cryptography is utilised here. In such a system each user has a pair of keys, one being their public key, which is generated via a one-way algorithm from that user's private key. For our purposes, the public key represents the address where a person is sending or receiving bitcoin (or another token on a different blockchain) to or from. While a person could receive bitcoin into their "wallet address" (i.e. their public key location) they can only send bitcoin from that address using their private key.

If the private key is lost, there is no way to recover it for a given wallet/public key, leading to another saying in the cryptocurrency world "your private key = your money, not your private key = not your money". This is very important to

understand if you are using a public blockchain as there is no technical support, or ability to "reset" a private key. There have been a number of unfortunate stories of significant sums of Bitcoin being lost when a user lost their private key. There are some hardware solutions which can store private keys, allowing users to access them with a PIN, but that is still not a fool proof solution.

What's next?

While we have used the example of the Bitcoin blockchain in the above article, it is very important to understand that blockchain technology is separate to and distinct from cryptocurrencies. Cryptocurrencies need blockchain to function, but there are almost limitless possibilities for blockchain deployments which do not require cryptocurrencies. As the most popular use of blockchain they do provide a valuable way to understand how blockchain technology works.

Blockchain technology is bringing serious disruption and efficiencies to those willing to learn and harness it. There are, however, a raft of legal issues which arise in relation to this technology (this is written by a lawyer!) which we will consider in future publications.