A Brief Study on Blockchain Technology

By Aslam Patel

a.patel54@edu.salford.ac.uk

What is a blockchain?

With the surge in popularity of cryptocurrencies based on blockchain technologies, blockchains have become extremely popular. A blockchain, as its name suggests, is a series of interconnected blocks that store data. A group of researchers first described this methodology in 1991, and it was first used in 1992.

Though, it went mostly unnoticed until Satoshi Nakamoto adapted it in 2009 to create the digital capital Bitcoin. But, first and foremost, what is a blockchain? What are their working principles, what issues do they tackle, and how may they be applied?

What is in a blockchain?

A blockchain is a decentralised ledger that everyone may access. They have an intriguing property: once data is stored on a blockchain, changing it becomes extremely difficult. It is meant to digitally timestamp documents so that they cannot be backdated or to interfere with them in any way. So how does that work? Figure 1. Shows basic properties of a 'block'.

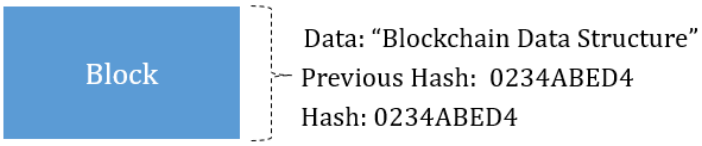

Figure 1 Block

Each block contains some data, as well as the block's hash and the preceding block's hash. The kind of blockchain determines the data that is contained within a block. For example, the Bitcoin blockchain contains information about a transaction, such as the sender, receiver, and quantity of bitcoin sent.

A hash is also a part of a block. A hash can be compared to a fingerprint. It uniquely identifies a block and all of its contents, exactly like a fingerprint. The hash of a block is determined after it is produced. The hash will change if something inside the block is changed. In other words, hashes are quite valuable for detecting block modifications.

The hash of the preceding block is the third element in each block. This essentially forms a chain of blocks, and it is this mechanism that ensures the security of a blockchain.

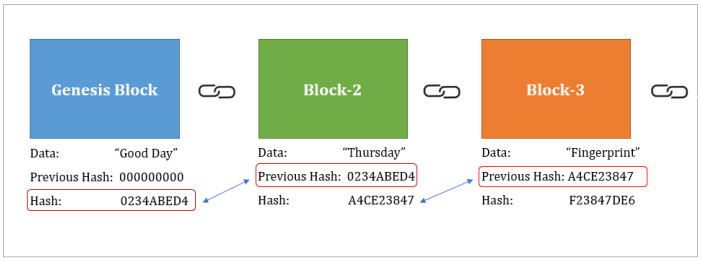

Figure 2 Three Blocks

A three-block chain diagram is shown in figure 2. As you can see, each block contains its own hash as well as the preceding block's hash. As a consequence, block number 3 refers to block number 2, while block number 2 refers to block number 1. Because it is the first, the first block is unique in that it cannot refer to prior blocks. This is referred to as the genesis block.

If you have tampered with the second block it causes the hash of the block to be altered as well. This would result in block 3 and all the forthcoming blocks to be invalid as they are no longer able to store a valid hash of the previous block. So

ultimately amending a single block will make all the following blocks invalid.

How does blockchain work?

However, hashes alone are insufficient to prevent manipulation. These days, computers are extremely fast, capable of calculating hundreds of thousands of hashes per second.

To make your blockchain legit again, you could effectively tamper with a block and recalculate all the hashes of other blocks.

Proof-of-work is a feature of blockchains that helps to alleviate this problem. It is a method that makes the building of new blocks take longer. In the instance of Bitcoin, calculating the requisite proof-of-work and adding a new block to the chain takes roughly 10 minutes.

Because tampering with one block requires recalculating the proof-of-work for all subsequent blocks, this approach makes it extremely difficult to tamper with the blocks. The proof-of-work process and the innovative use of hashing contribute to the security of a blockchain.

Properties of Secure Hash Algorithms

One example of a cryptographic hashing algorithm is SHA-256, which is used in Bitcoin. SHA-256 creates a 256-character hash result regardless of the size of the input data. The following features should be included in secure hash algorithms used in blockchain:

- *For the same input, the same hash value should be created every time.*
- *The hash should be calculated from the data, but the data should not be derived from the hash.*
- *Even a little change in the data should result in a full change in the hash value.*
- *The hash should be computed rapidly using the algorithm.*

Peer-to-peer networks/integrity

However, there is another way that blockchains protect themselves: they are distributed.

Instead, than relying on a central authority to maintain the chain, blockchains rely on a peer-to-peer network that anybody may join. Anyone who joins this network receives a complete copy of the blockchain. This may be used by the node to ensure that everything is still in working condition.

New blocks

When a new block is created by an individual everyone on the network receives the new block. The block is then verified by each node to ensure that it has not been interfered with. Each node adds this block to their own blockchain if everything checks up. This network's nodes come together to form an agreement. They have reached a pact on which blocks are genuine and which are not.

The block will be rejected by all nodes if the block has been tampered with.

How can this be exploited?

To effectively tamper with a blockchain, you will need to tamper with all of the chain's blocks, redo each block's proof-of-work, and gain control of more than half of the peer-to-peer network.

Then and only then will your modified block be acknowledged by the rest of the world. However, the good news is that this is a task which many security professionals would class as 'impossible' to implement.

Limitations of Blockchain

Because of the added complexity involved with consensus methods in blockchain, the performance of centralised systems significantly outpaces that of blockchain systems. For instance, Bitcoin presently has an output of about 7 transactions per second, but Visa, a centralised system, can manage 56,000 transaction communications per second.

Blockchain is still in its early stages. Legislators have yet to establish a legislative framework in

which blockchain technology may be properly implemented.

Evolution of Blockchain

Blockchains are likewise in a perpetual state of evolution. The establishment of smart contracts is one of the more recent advances. These contracts are basic scripts that may be used to automatically swap currencies based on certain conditions and are kept on the blockchain. Others soon recognised that the technology might be utilised for a variety of purposes, including preserving medical information, non-fungible tokens and even tax collection.

There are new and adapted blockchains that have been released by specific companies who have significantly improved on blockchains such as Bitcoin.

A prime example of this is the XRP ledger Blockchain by the company ripple. The table below aims to compare technical factors between early blockchain (Bitcoin) with New blockchain (XRP)

Features	Bitcoin	XRP
Transactions per second	7	1500
Speed of transaction	60+ Mins	4 sec
Average transaction fee	$0.5	$0.000003
Smart contracts	NO	YES
Energy Consumption	73.12 TWh	0.01 TWh
Mining	YES	NO

Figure 3 Table of comparison

Conclusion

Blockchain is becoming a more widespread technology, and the market for it is fast expanding. The worldwide blockchain technology market was $339.5 million in 2017. This market is expected to reach $2.3 billion by 2021.

Not only banking systems but Microsoft are one of the companies who are researching heavily into adapting their technologies around blockchain.

Ultimately, Blockchain allows for distributed data storage, as well as extra precautions to prevent unauthorised actors from altering stored data and decentralised validation to avoid fraud. It eliminates numerous human points of failure, offers a wide range of applications, and allows for automation at many levels of business operations.

With its constant adaptation and research, the full potential of blockchain is still to be discovered.

References

ResearchGate. 2021. (PDF) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. [online] Available at: https://www.researchgate.net/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends

Paladion.net. 2021. Evolution of Blockchain Technology | Paladion. [online] Available at: https://www.paladion.net/evolution-of-blockchain-technology

Ibm.com. 2021. What is Blockchain Security. [online] Available at: https://www.ibm.com/topics/blockchain-security

Binance Academy. How Does Blockchain Work? | Binance Academy. [online] Available at: https://academy.binance.com/en/articles/how-does-blockchain-work

Paladion.net. 2021. Evolution of Blockchain Technology | Paladion. [online] Available at: <https://www.paladion.net/evolution-of-blockchain-technology>