HOW BLOCKCHAIN WORKS?

CHETCUTI CAUCHI
ADVOCATES

ccmalta.com

How Blockchain Works?

Summary

Transactions requests are sent to a network of computers for validation. Each computer follows some software protocol(s) to ensure these transactions are valid. Once validated, transactions are combined together to make a block of data. Once the block of data is created, it is then recorded and kept in a digital register also called "Blockchain". Ultimately, copies of this register are distributed to the blockchain participants and secured by a cryptographic framework to ensure that records cannot be changed or altered.[1]

Analysis

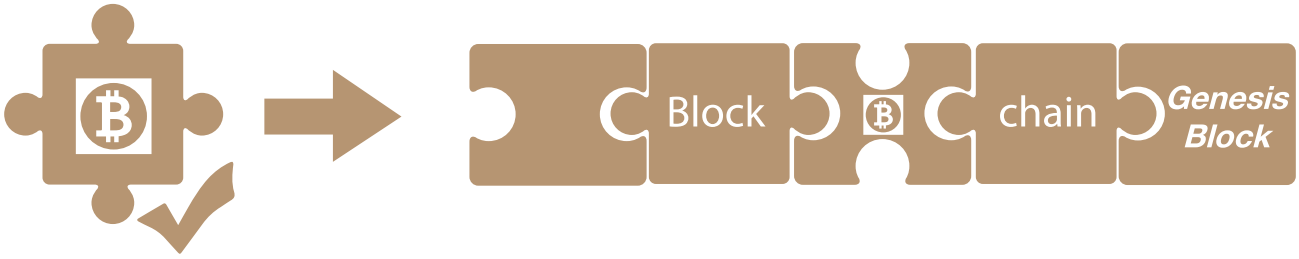
A blockchain consists of a distributed ledger on a peer-to-peer network. The ledger is made up of transactions which take place on the same network. Transactions do not necessarily have a monetary value, and the word transactions is to be interpreted widely to mean any type of data transfer across such network.

The data transactions are collected in blocks, and each block of transactions is confirmed by the majority of the network one after the other. Block confirmation times vary widely, with some networks such as Bitcoin taking up to ten minutes on average to confirm a block, and others taking mere seconds.
Each block is built onto the previous one, with all blocks being linked together onto one single chain. This is the origin of the term "Blockchain".[2]

How are blocks created?

Blockchain technology is a distributed, transparent cryptographic ledger, deemed unforgeable (to date), that keeps records of all transactions, without involvement of a central intermediary, each transaction being verified by the network participants. Each transaction that is verified will have a time stamp and the actual transaction data. A block will also contain two hash values: a hash value over all the transactions collected in the new block, and the hash value of the previous block.[3]

When a transaction is verified, it is added to a block of other verified transactions. The block is then immutably added to the distributed ledger in a linear and chronological order. All blocks are linked together onto one single chain.



[1] https://books.google.com.mt (Blockchain Basics: A Non-Technical Introduction in 25 Steps)
[2] https://blog.equinix.com/blog/2017/10/05/blockchain-a-new-type-of-internet/
[3] https://blockgeeks.com/guides/what-is-hashing/

The first block on a blockchain is known as the *Genesis block*.[4] All subsequent blocks are built on top of each other. With each confirmed block, the previous blocks grow stronger and more resistant to change, as in order to change one of the older blocks, one would need to change all the other blocks.

Consequently, the older the block, the more secure it is. Any attacker trying to change the data contained in older blocks would need to have an inordinate amount of power several times larger than that of the rest of the network. The computing power required is such, that all blocks would need to be changed at the same moment in time.

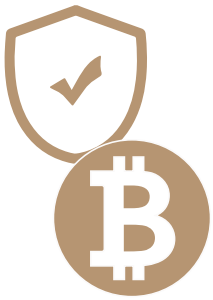
Block confirmation

Miners (as explained below) need to approve blocks through a simple majority vote. In essence, the first miner to solve a complex mathematical algorithm gets a block reward (which can be of a monetary nature) and broadcasts the solution to the rest of the network, who then in turn approve such solution and add the latest block onto their own chain. The process then starts all over again for the newest block. Miners constantly ensure that they are on the correct chain, which under normal circumstances is the longest chain which has the most recent block/s. The newest chain naturally is equivalent to the latest version of the distributed ledger.

Miners and users

On a basic blockchain network, there are two main participants - miners and users.[5]

Miners



Miners on a blockchain are not equipped with pick-axes. Instead, miners have a different role - they are there to confirm the blocks of transactions being processed constantly on the blockchain. The miners' role is important for two main reasons:

- they serve as validators for each and every transaction taking place on the network; and
- cumulatively they protect the network against any malicious external attacks.

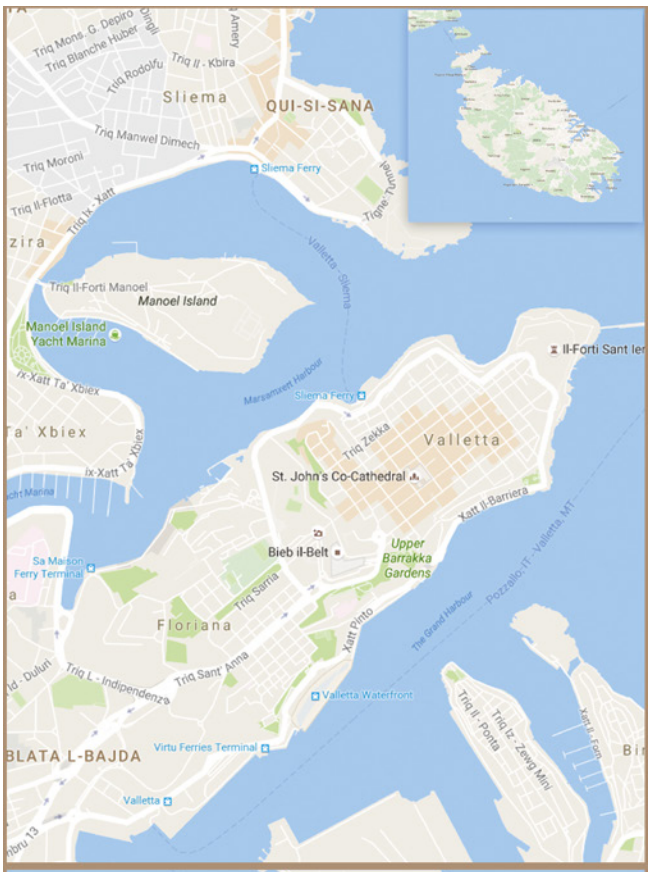
Miners are also the ones who have a voting right on any changes taking place in the network. The reason for this is that miners have an inherent interest in choosing the best options for the network, as doing otherwise would be akin to shooting themselves in the foot - any disruption in the network would hit them the hardest.

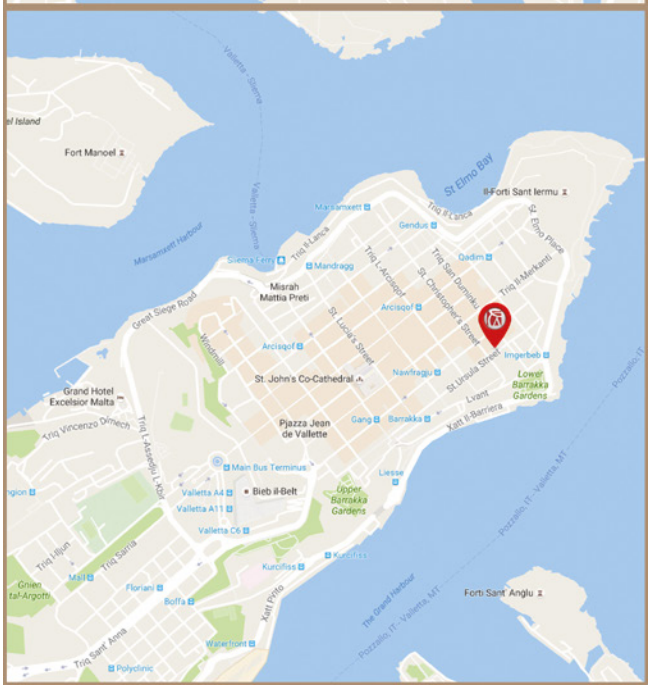
A third important role which is often overlooked is that of serving as a back-up. Miners are required to store a full copy of the ledger on their machines and therefore serve as decentralised back-up for the blockchain network.

Users

Users are the everyday participants who make use of the network, with the predominant use being that of transacting on the network. Anyone who makes use of the network such as being senders or recipients of transactions would qualify as blockchain users. Users, unlike miners, do not need to download a full copy of the ledger; it is enough if they are connected to the network via an Internet connection. Likewise, they do not have any voting rights due to their passive participation.

[4] https://en.bitcoin.it/wiki/Genesis_block
[5] https://bitmalta.com/blockchain-explanation/





CONTACT DETAILS

For more information, contact:

Dr. Maria Chetcuti Cauchi
B.A., LL.M.(Warwick), LL.D., TEP
Senior Partner & Founder, Financial Services

Skype: maria.chetcuti.cauchi
E: mcc@cclex.com • W: www.cclex.com

Dr Priscilla Mifsud Parker
B.A., M.A. (Fin. Serv.), LLD., TEP
Senior Partner – Financial Services

Skype: pmifsudparker
E: pmp@cclex.com • W: www.cclex.com

MALTA

CYPRUS

LONDON

ZÜRICH

HONG KONG

CHETCUTI CAUCHI
ADVOCATES

ccmalta.com