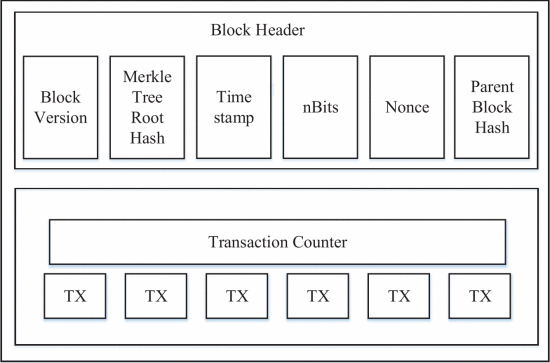
**O que é a blockchain e como funciona**

A *blockchain* é uma tecnologia que permite a transferência de bens entre usuários. Funciona como uma base de dados que armazena informação, organizando-a em blocos (*blocks*). À medida que a informação é armazenada, são criados novos blocos para armazenar a informação recente, que serão posteriormente ligados ao bloco anterior formando, assim, uma corrente, daí o seu nome. Um dos exemplos reais do uso da *blockchain* é a sua utilização para armazenar o histórico de transações de bitcoins entre entidades (Prathyusha, Kavya, Akshita 2018)



Constituição dos blocos - <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8029379>

Cada bloco nesta corrente é constituído por 2 partes essenciais: o *block header* e o *block body*. O block header contém: a versão do bloco; a sua hash especifica; a data da sua criação; uma nonce; um nBits e a hash do bloco anterior de forma a permitir a ligação deste bloco à corrente. O block body, por sua vez, contém toda a informação armazenada no bloco.

(Zheng et al 2017) <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8029379> (16/10)

Como vimos, no *block header* encontra-se presente uma *hash* especifica desse bloco. Essa *hash* é gerada utilizando um algoritmo (SHA256 cryptographic hash algorithm) e serve como identificadora do bloco. Está aqui também presente a hash referente ao bloco anterior. É a presença desta *hash* que permite “validar” o bloco criado e ligá-lo aos blocos anteriormente formados. Portanto, se essa *hash* corresponder à *hash* do bloco imediatamente anterior, valida-se esse bloco, juntando-o à corrente. (Antonopoulos 2014) (**pág. 163)**

Assim, uma blockchain é muitas vezes visualizada como uma “pilha” de blocos uns em cima dos outros, empilhados por ordem cronológica, em que cada bloco se refere ao bloco anterior através de *hashes*, criando uma corrente que liga todos os blocos, desde o mais recente, até ao bloco original ou *genesis block*. (Antonopoulos 2014)

**Ideologias da Blockchain: Peer-to-Peer (P2P) network e descentralização.**

A *blockchain* usa o sistema peer-to-peer (P2P). Este sistema é baseado numa rede onde não há hierarquias nem servidores centrais para onde são direcionadas informações ou dados. Neste sistema os computadores ligados à rede (nodos) são independentes, mas interligados entre si realizando todos as mesmas funções, recebendo e partilhando dados ao mesmo tempo. Assim, ao usar uma rede P2P, a blockchain é descentralizada, não existindo um servidor central para onde flui toda a informação, mas sim um conjunto de computadores com acesso total a toda a informação presente nessa mesma *blockchain*. (Antonopoulos 2014) **(pág. 139)**

Numa rede centralizada, a validação de uma dada transação dá-se por meio de uma entidade intermediária confiável. Por outro lado, num sistema descentralizado, cada transação é validada através do consenso entre nodos em relação à validade ou não de um bloco, conseguida com o uso de alguns protocolos. Alguns desses protocolos são o Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS) e Ripple.

O PoW é o protocolo usado no sistema da Bitcoin, pelo que será aprofundado mais adiante.

De acordo com (Mingxiao et al 2017) e (Zheng et al 2017), o protocolo PoS pode ter em conta 1 de dois fatores: o *coin age*, ou seja, o tempo que um nodo mantém a moeda em sua posse, ou a quantidade de posses que um nodo tem. No primeiro caso, quanto mais tempo um nodo mantém bens em sua posse, mais direitos tem, sendo as suas transações consideradas seguras. No segundo, acredita-se que quanto mais bens um utilizador tem, menor a chance de ele atacar a *network*, daí serem consideradas mais confiáveis.

Na DPoS os nodos que geram e validam blocos são eleitos democraticamente. Este protocolo permite uma rápida criação e validação de blocos. (Mingxiao et al 2017) <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8123011> (16/10)

**Blockchain associada às cripto moedas (bitcoin).**

A Bitcoin utiliza a tecnologia blockchain como forma de armazenar todas as transações realizadas. A forma como a bitcoin valida estas transações é através da validação do bloco, realizada pelos nodos conectados à rede bitcoin através do protocolo de PoW.

Assim, quando ocorre uma transação, esta é incorporada num bloco que, após estar completo, será enviado para todos os nodos da *network* para que este seja validado e posteriormente ligado à corrente de blocos. Os nodos que se ocupam desta avaliação são chamados de *miners*. Para conseguir provar a validade de determinado bloco os *miners* têm que descobrir a *hash* do bloco que esta a ser verificado através de um problema matemático baseado num algoritmo, cuja resolução é de elevada dificuldade, mas de fácil verificação, sendo o nome dado a esta atividade *mining*. O *miner* que conseguir determinar a *hash* envia-a para os outros *miners* para que estes possam verificar se essa é a solução correta, caso isso aconteça, valida-se o bloco e este é adicionado à corrente existente. A solução do problema (*hash*) é então incluída no *header* do novo bloco e serve como prova (Proof of Work) de que o *miner* resolveu o problema, permitindo-lhe receber bitcoins como recompensa. Após ser incluído na corrente, todas as transações incluídas no bloco são dadas como válidas permitindo o uso ou troca das bitcoins pelos novos donos. (Antonopoulos 2014). **(pág. 177)**

Muitas vezes vários blocos são validados ao mesmo tempo e, consequentemente integram a corrente na mesma altura. Isto pode causar um *Blockchain Fork*, ou seja, uma bifurcação da *blockchain* causando a formação de duas correntes às quais vão sendo adicionados blocos, “the blockchain literally split into two, with one half of the network adding blocks to one version of the chain, and the other half adding to the other. For the next six hours, there were effectively two Bitcoin networks operating at the same time, each with its own version of the transaction history” (Buterin 2013 <https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/> ). Na maioria das vezes este problema é resolvido rapidamente, havendo uma corrente mais longa que a outra, sendo essa corrente dada como a principal e os blocos presentes na corrente mais curta são removidos e reintegrados na *blockchain*. Mas, em escassos casos, estes *forks* podem durar até algumas horas, criando várias bifurcações ou até mesmo correntes inválidas de blocos, tendo como consequência perdas de informação e de blocos que, noutros casos, seriam validados integrados

**Segurança e imutabilidade desta tecnologia.**

A tecnologia da *blockchain* funciona com base na criptografia de informação armazenada permitindo um sistema seguro. Para além do uso de criptografia, a presença no *block header* da *hash* referente ao bloco imediatamente anterior permite aumentar a segurança e a imutabilidade dos dados, principalmente à medida que são adicionados novos blocos.

Como foi visto anteriormente, a forma de descobrir a *hash* de um determinado bloco é resolvendo um problema matemático de grande dificuldade, sendo necessário um grande poder computacional para o fazer. Assim, com a modificação da informação presente num dado bloco, a *hash* referente a esse mesmo bloco irá mudar. Vimos também que os blocos contêm a *hash* dos blocos imediatamente anteriores. Desta forma, com a alteração dos dados de uma dada transação e com a consequente mudança da *hash* os blocos serão incompatíveis entre si, sendo então detetada uma falha pelos nodos, o que lhes indica que foram realizadas alterações num dado blocopermitindo a sua correção. Para que a alteração ocorra sem ser detetada seria necessário recalcular as *hashes* de todos os blocos posteriores ao que foi alterado o que é praticamente impossível dado a necessidade da extremamente elevada capacidade computacional necessária para que esse cálculo fosse possível ocorrer antes da deteção da falha.

Fontes:

[http://academicscience.co.in/admin/resources/project/paper/f201803281522225610.pdf T.Prathyusha](http://academicscience.co.in/admin/resources/project/paper/f201803281522225610.pdf%20T.Prathyusha), M.Kavya, P.Sree Laxmi Akshita, 2018, Blockchain Technology

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8123011> Du Mingxiao\*, Ma Xiaofeng\*, Zhang Zhe\*\*, Wang Xiangwei\*, Chen Qijun\*, 2017, A Review on Consensus Algorithm of Blockchain

<https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/> 2013, Vitalik Buterin, Bitcoin Network Shaken by Blockchain Fork

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8029379> Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, 2017, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends

<https://unglueit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf>

Andreas M. Antonopoulos, 2014, Mastering Bitcoin: Unlocking Digital Cryptocurrencies