BTCBROS

INTRODUCTION TO BLOCKCHAIN - PART 1

EDUCATION VS ADVICE

How to/What is

What is ‘best’

Disclaimer: Nothing set forward in this guide is given as or should be constituted as financial advice. Everything within this guide is presented for educational and research purposes only.

INTRODUCTION

This guide is intended to be used as a reference point on the basics of Blockchain Technology. It's origin, workings, use and technical capacities. The guide has been constructed for beginners and those with continued interest in Cryptocurrencies and Blockchain technology.

This guide aims to educate in this field by providing a basic understanding. Further questions may be raised via the contact means indicated within this guide.

Note: This guide is not to be deemed as financial advice. Be aware that ANY type of financial investment carries a risk and you should always consult a professional for financial advice when making large investments. You are solely responsible for any financial investment made on the topics contained wherein.

ABOUT US

BTC Bros Ltd was formed in late 2016 by **Nathaniel Cole** and **Jonathan Powell**, with the help of **Len Gordon**, as a Blockchain & Cryptocurrency education and research consultancy.

The company also provides a range of **media and marketing** services **specifically aimed** at providing **awareness** for companies within the Blockchain and Cryptocurrency industry.

We have worked with a number of **Blockchain projects, brands, events and businesses**, on everything from concept formation to initial development.

We have helped **100's of individuals** to become aware of and **gain an understanding** of the **technologies, advancements** and **opportunities** within the space.

Our **signature development**, is an educational ecosystem built on Blockchain and Cryptocurrency principals, known as **ACE Economy.**

BTC Bros Ltd is a company registered in England & Wales.
Company No. 10759449

BLOCKCHAIN & DISTRIBUTED LEDGER TECHNOLOGY

Due to the complexity of the technical aspects of Blockchain technology, we have decided to split this guide into two parts. Part 1 tackles the basic functions of the Bitcoin Blockchain and it's comparison to legacy technologies. Part 2 focuses more on the technical processes of the Blockchain and their importance.

For those who have read our article, 'The History of Ledgers', you should already have an insight of how Blockchain progresses the history of not only financial book keeping, but also the keeping and organisation of records overall.

Please note that although you may hear discussion about Blockchain and Distributed Ledger Technology (DLT) being one and the same, they are in fact both the same and different.

DLT's derive much of their principles from Blockchain, however they can be totally different with regards to the way that they operate.

We will not go into DLT's or differences in this guide, instead this guide focuses solely on Blockchain, using the Bitcoin blockchain as the main example.

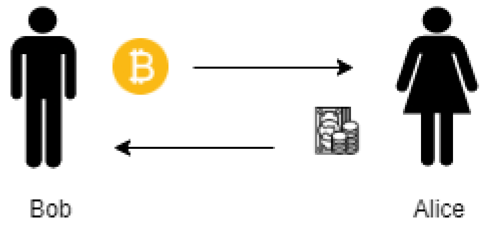
If you have not already, we strongly recommend that you read our 'Introduction to Cryptocurrencies' guide as a precursor to this one.

Thank you!

Blockchain Basics

There are some fundamental differences between the way that Bitcoin transactions work on the Blockchain, as opposed to how digital transactions work within our current financial system.

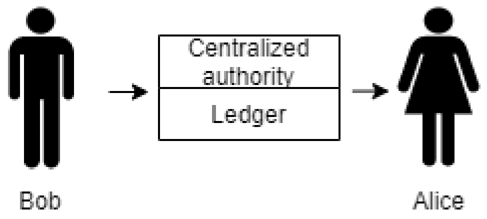
Before exploring the capabilities and technical of the blockchain, we must first look at this difference.



Crypto Transaction

Bitcoin transactions are **totally peer-2-peer (P2P)**, meaning that there **is no third party or centralized authority controlling the transaction.**

Transactions are recorded **publicly on the Blockchain**. However, in relation to our diagram, no one can tell that it is Bob and Alice doing the transactions. Instead both Bob and Alice's transactions are attributed to each of their **public keys**, respectively.



Bank Transaction

Traditional or 'Legacy' banking transactions are handled **by third party payment processors, other banks or 'clearing houses'.**

Each of these play a role in and **take a fee for account holders transacting between each other.**

Their ledgers are held on **centralised servers and entries are compared against each others ledger copies.**

Blockchain Basics cont'd…

Let's take a closer look at the transaction process to further breakdown some of the **important differences** in Blockchain and a standard ledger.

Crypto Transaction

In our diagram **Alice sends Bob some FIAT currency** and **Bob sends Alice some Bitcoin in return**, but wait, how did Bob know how to send that Bitcoin to Alice?

- Bob used Alice's **Public Key** to identify that the correct recipient wallet matches the one in which Alice has chosen to receive her Bitcoin.

- Using Alice's Public Key, Bob does not need to know any other information about Alice, not even her name. This is due to the **pseudo-anonymous nature of Bitcoins public Blockchain.**

In our **Introduction to Cryptocurrencies** guide, we gave a run down of the different types of Blockchain and their attributes. To make it **clear the Bitcoin blockchain falls into the category of Public, Open & Permissionless.**

To explain this even better, we first need to look into how both Bob and Alice acquired they're public keys.

Public Keys would have been generated for both Bob and Alice upon creation of their Bitcoin wallets.

A Public Key is a cryptographic identifier given to a wallet at the time of its creation.

The Public Key is similar to a **sort code/account number**, in comparison to what we would use in traditional banking. A users public key can be **shared with others to receive transactions and/or verify their wallet existence, balance and transactions.**

The sending/receiving of transactions between users happens via **Public Key Cryptography and a process called Hashing**.

Blockchain Basics cont'd…

Many people ask, where do I put my Bitcoins, or how do I know they're there?

Both the long and short answers to this are they aren't. Now don't panic and try not to get to confused, but here is an example:

When you put **CASH into your Bank Account**, you are given a receipt and you can see the value of your assets on a statement or online. You don't login and see live CCTV of all the notes and coins that you've deposited do you?!

That is because **once a deposit is received in your account it is recorded onto your banks ledger**, which in turn is recorded on the **sub-ledger** that they have **specific to your account**.

When you go to the bank and make a withdrawal**, the amount you are able to access depends on the amount of the most recent ledger balance**. This is checked, then if suitable or available, **you are given physical cash to denote the transaction**. The amount withdrawn is deducted from the ledger balance also. Sometimes, this can go wrong due to delayed clearances (remember we mentioned clearing houses on the previous page) or bank processes, which can lead to one of the most frustrating problems with legacy finance…**double spending**, but we'll talk about that in a later.

With Bitcoin, you are simply recording the ledger balance and **as cryptocurrencies are not physical, you do not need any cash to denote the transaction.** The ownership and transfer of X amount of Bitcoin is recorded and agreed on the Blockchain. When you send/receive Bitcoins, it is attributed/deducted either from or to your wallet respectively **and can be seen denoted in your wallet and on the Blockchain**.

It can take sometime to get your head around, but in reality it is very simple.

Some people have said because Bitcoin operates in a digital space, that it is backed by 'nothing but thin air'. However, we can see from the above example that **FIAT numbers on a screen**, is really only backed by **numbers on paper**.

In our intro, we explained what backs that paper…your government and banks word. With Bitcoin, it is **backed by the code and the code is backed by solid mathematical equation, which is governed by all the participants of the system, rather than a small group of bankers and politicians.**

This means that use of blockchain massively reduces, if not eliminates **centralisation, 'Bad actors', corruption and collusion** within the financial system, whilst promoting **trust, immutability and transparency**. The Bitcoin blockchain also provides opportunity for 'fair' distribution and governance, as anyone can be a participant on the chain.

Hash Function (Hashing) – Validating Data

Now we're going to get a little technical here, but still, we will keep it simple. To find out more about the **Hash Function**, look out for our upcoming **'Introduction to Blockchain – Part 2'** guide.

What is a Hash Function?

A hash function in cryptography is a **mathematical function that is most commonly used to verify the integrity of data**. This is achieved by transforming identical data to a unique, representative, fixed-sized digest, using specific types of computer algorithms.

Bitcoin uses the **SHA-256 algorithm** as part of it's protocol to complete hash functions.

What is meant by 'digest'?

In computing terms a digest is **a condensed data item, or variable length string used as an input, to create a (usually shorter) fixed-length string or summary**. The process normally comes from **'hashing'** the digest (input), using specific types of computer algorithms.

You can mess around **here** with hashing data inputs. Try typing in your name and see what you get!

Remember the Bitcoin algorithm is SHA-256.

Key Characteristics

- **The same input will always generate the same hash, provided we are using the same hashing algorithm.**
- **If there is any slight change in the input , then it will generate an entirely different hash output.**
- **If different inputs were to generate the same hash, we would refer to it as a "hash collision." This should never happen.**
- **It is nearly impossible to derive the input value from its hash output. Due to the fact that hash functions are extremely difficult to reverse engineer. For some technical reading on this check out this interesting thread (https://crypto.stackexchange.com/questions/45377/why-cant-we-reverse-hashes)**

PUBLIC KEY CRYPTOGRAPHY

Ok, hopefully the last two pages were not too complicated. Let’s take a **basic** look at how **Public Key Cryptography** works.

Both users have two sets of keys for their Bitcoin wallets:

- **Private Key – Must be kept private to the user**

- **Public Key – Is viewable by everyone. Really the address is public, but the public key it derives from will only be visible <u>when Bitcoin is spent.</u>**

When a user wants to send some Bitcoin to another user, they can use the users **PUBLIC KEY** to ensure that they are sending to the correct user. The receiving user will obviously need to give their **PUBLIC KEY** to make this possible.

Bitcoin is sent, by **User A (Bob)**, sending a message with the transaction details (amount) to **User B (Alice)**. When the message is sent, **the date and time are recorded on the blockchain, along with the transaction number and corresponding hash. Fig a.**

A **PRIVATE KEY** is used by the user to sign the message being sent to the other party. This serves to **authenticate the transaction**, as the private key should only be known to Bob.

The same thing happens when sending **digital assets** on the blockchain. **Fig b.**

In our example Alice sends Bob a **digital resource**, which could be many types of data, that only Bob can see. Only Bob can see this data, as he is the owner of the wallet with the **PUBLIC KEY** that Alice used to send it. Bob receives the data, but has to use his **PRIVATE KEY** to open his wallet and view it. Again, as Bob should be the only one with the **PRIVATE KEY** to that wallet, only he can receive/open/view the message.

Fig a.

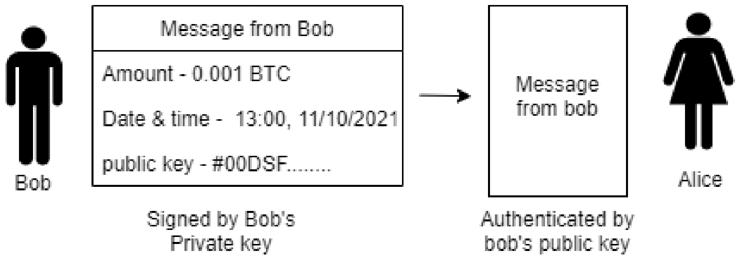
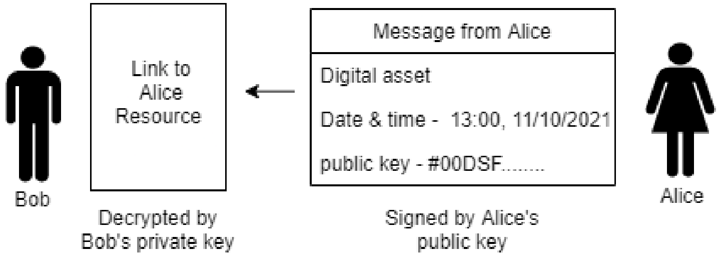

Bob
Message from Bob
Amount - 0.001 BTC
Date & time - 13:00, 11/10/2021
public key - #00DSF........
Signed by Bob's Private key
Message from bob
Authenticated by bob's public key
Alice

Fig b.


Bob
Link to Alice Resource
Decrypted by Bob's private key
Message from Alice
Digital asset
Date & time - 13:00, 11/10/2021
public key - #00DSF........
Signed by Alice's public key
Alice

THE BUILDING BLOCKS

Right, now that we know how **transaction data** is sent (**message**), let's explain how the message is processed on the blockchain (**on-chain**).

Blocks

Earlier we spoke about data being sent across the blockchain, however the name of the record of these actions (transactions) is called a **Block**, collectively known as **Blocks**.

What's in a Block?

A block is usually made up of a batch of transactions, containing **the cryptographic hash of the previous block, the block timestamp, and transaction data (message).**

The form that blocks use to represent this is called a **Merkle Tree**, which is something we will touch on in later blockchain guides.

These blocks are **chained** together and **timestamping** proves that the block and it's contained data **existed at the time it was first published to get to its hash**. Due to the fact that each block contains information about the block **previous to it**, they begin to form a **chain**. Hence the name **Blockchain**.

We will get into how this works a bit more on the next page

How are Blocks Created?

A block is created **every time data is sent on the blockchain**. These blocks go through a **validation process** to ensure that they **match the historical data** on the blockchain, before they can be allowed to be **accepted** by the blockchain. The operation of this validation or confirmation process is called **Mining**.

Chaining Blocks together

So, now we know a little bit about **Blocks** and some of the things they contain, lets take a slightly deeper look to see **how and why they are chained together.**

Block Header

Block Header

Block Number

Previous Block Hash

Bitcoin Version No.

Merkle Root

Nonce

Time Stamp

Every block on the Bitcoin blockchain has a **Block Header**. The block header serves to **identify a particular block on the blockchain** and contains **important meta data about each block.**

The **Merkle Root** comprises of all of the hashes in a block and them being hashed again.

The **Nonce** stands for **"Number only used once"**, which is the resulting number miners are solving problems for.

This number is added to the end of the hash, before being rehashed **to meet difficulty level requirements** of the blockchain.

Both of these processes add to the **security and trustworthiness** of the blockchain.

The diagram to the right is an example of how each block is then **chained together**.

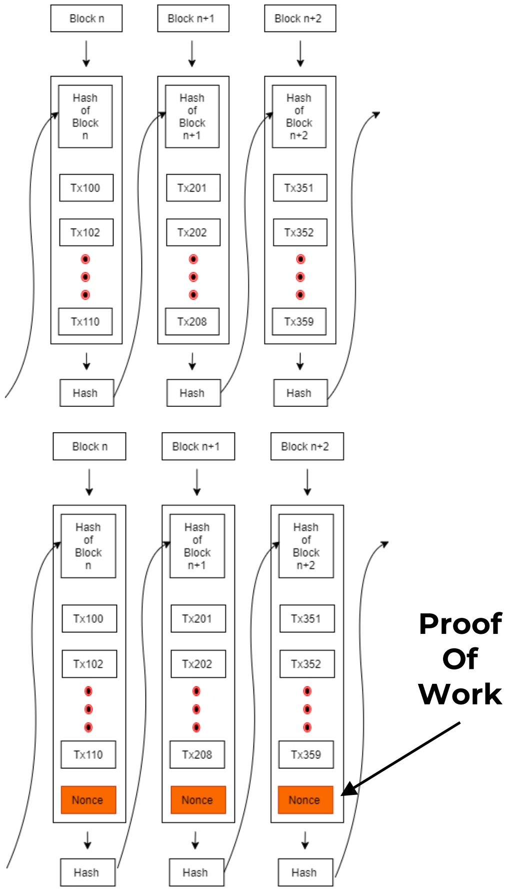
A block is created **containing multiple transactions, which each include their own individual transaction data.**

Each block is given a hash and a block header containing the previous hash and other important metadata.

The next block must **confirm to hold the same information and also the correct hash (remember each hash is unique)** to be confirmed as the next accepted block on the chain.

Each block carries the data and references **right back to the start of the chain**, which is the very **first bitcoin transaction**, known as the **Genesis Block.**

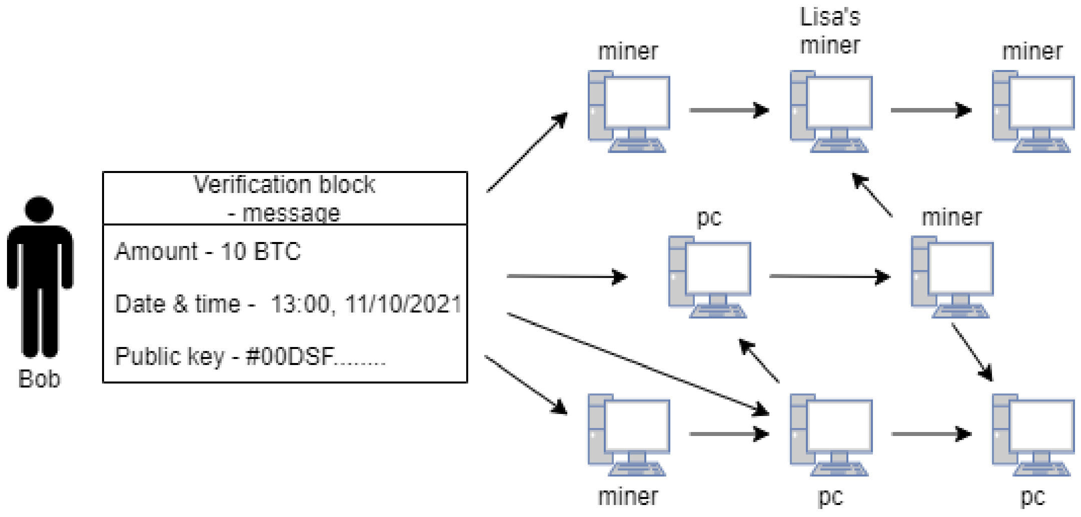
Chained Blocks



Proof Of Work

MINING

Mining is the process of confirming transactions on the blockchain using a computer to **validate and solve complex computational problems**, such as **confirming/validating** blocks on the blockchain.



Verification block - message

Amount - 10 BTC

Date & time - 13:00, 11/10/2021

Public key - #00DSF........

Every time a block is confirmed on the blockchain **Bitcoin is generated by the process**. This Bitcoin is **rewarded to all the miners involved in processing that block.**

This reward is **cut in half every 4 years** as the Bitcoin network goes through a process called "**Halving**". We will explain Halving in detail inside another guide.

Anyone can be a miner on the Bitcoin network, using a **computer processor, graphics card or an ASIC miner**.

ASIC stands for "Application Specific Integrated Circuit", which is a **powerful computer chip** commonly used by **professional Bitcoin miners** and **mining farms**.

With Bitcoin a **minimum of 6 confirmations** are needed to complete the transaction process. These confirmations are completed **by any miner or node (computer) on the network, provided all blockchain history and current copies on those computers are match.** Once a transaction is considered fully confirmed, **it cannot be reversed**.

If a computer tries to submit a record that is a **mismatch**, again the block will be **rejected** by the network, thus securing the **CORRECT** copy of the blockchain from corruption or "bad actors" going forwards.

Each miner is subject to **proving it's work** (adding the nonce) to the rest of the network. To achieve this, the Bitcoin network uses a cryptographic proving method called **'Proof Of Work (POW)'.** We'll discuss Proof-Of Work in part 2.

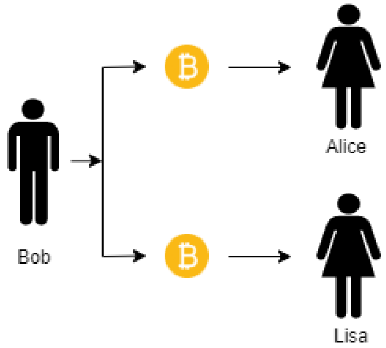
Each time someone sends Bitcoin, they pay a small fee for the transaction. These fees are distributed to miners on the network.

DOUBLE SPENDING

We spoke earlier about **“Double Spending”** being probably the biggest problem with legacy accounting.

For decades, **financial experts, mathematicians and economic gurus** have tried to solve the problem of double spending in accountancy...then Bitcoin and Blockchain came along!

Thank you Satoshi Nakamoto!



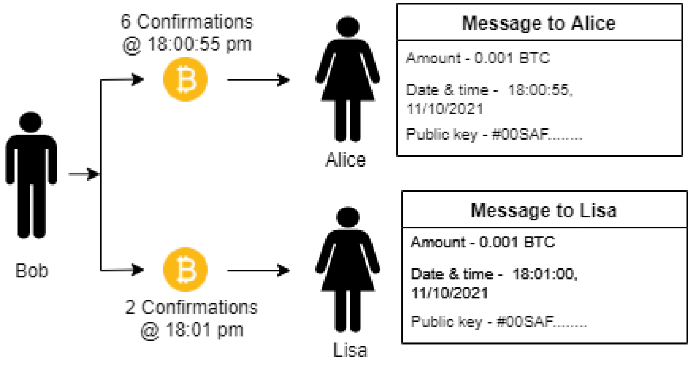
Double Spending occurs when a transaction is **recorded twice on a ledger.**

In **legacy accounting** this can lead to people being **debited twice for the same transaction**, people being **credited twice for the same transaction** and even used to embark upon **fraudulent activity** by **“fixing the books”.**

Because of the nature of how a blockchain works, double spending successfully is **not possible.**

If our user Bob only has **0.001 BTC**, he cannot send **0.001 BTC** to both Alice and Lisa. Even if both transactions were sent/processed at the same time, **the blockchain will still have to pick up one before the other.**

Lets say **Alice’s 1 BTC is confirmed on the blockchain first**, when the block containing **Lisa’s transaction** is presented to the chain, it will be **rejected by the miners and nodes**, as a successful transaction **has already been made to Alice**, which left Bob with **0.001 BTC** when it was confirmed. Therefore, because the **last block from/to Bob’s wallet** left him with **0 BTC**, there is **no way that he could possibly pay Lisa.**



Message to Alice

Amount - 0.001 BTC

Date & time - 18:00:55, 11/10/2021

Public key - #00SAF........

Message to Lisa

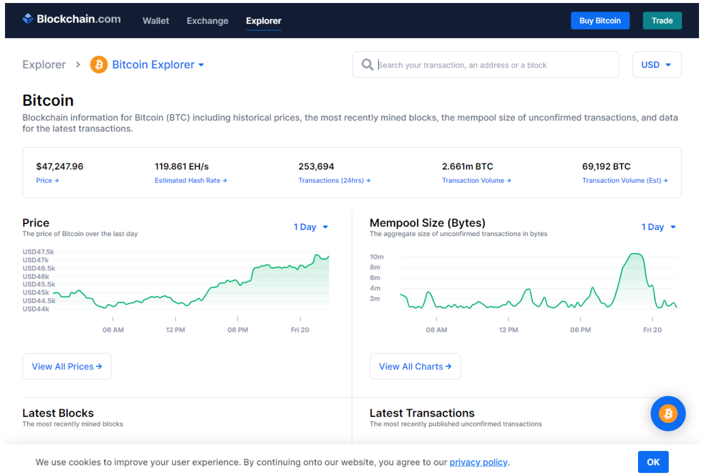
Amount - 0.001 BTC

Date & time - 18:01:00, 11/10/2021

Public key - #00SAF........

VIEWING THE BLOCKCHAIN

You might be wondering how everyone is able to view what is going on the blockchain. There are a number of ways to view the blockchain, but the easiest is via a **Block Explorer**.



Bitcoin

Blockchain information for Bitcoin (BTC) including historical prices, the most recently mined blocks, the mempool size of unconfirmed transactions, and data for the latest transactions.

$47,247.96	119.861 EH/s	253,694	2.661m BTC	69,192 BTC
Price →	Estimated Hash Rate →	Transactions (24hrs) →	Transaction Volume →	Transaction Volume (Est) →

Price

The price of Bitcoin over the last day

Mempool Size (Bytes)

The aggregate size of unconfirmed transactions in bytes

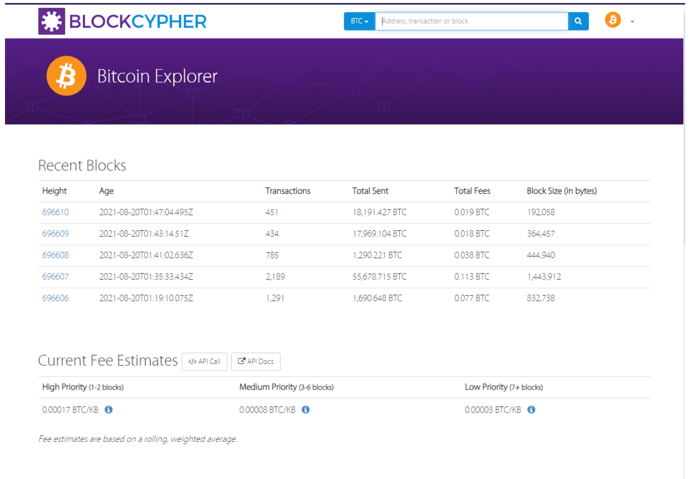
Latest Blocks

The most recently mined blocks

Latest Transactions

The most recently published unconfirmed transactions

We use cookies to improve your user experience. By continuing onto our website, you agree to our privacy policy.



Recent Blocks

Height	Age	Transactions	Total Sent	Total Fees	Block Size (in bytes)
696610	2021-08-20T01:47:04.495Z	451	18,191.427 BTC	0.019 BTC	192,058
696609	2021-08-20T01:43:14.51Z	434	17,969.104 BTC	0.018 BTC	364,457
696608	2021-08-20T01:41:02.636Z	785	1,290.221 BTC	0.038 BTC	444,940
696607	2021-08-20T01:35:33.434Z	2,189	55,678.715 BTC	0.113 BTC	1,443,912
696606	2021-08-20T01:19:10.075Z	1,291	1,690.648 BTC	0.077 BTC	832,738

Current Fee Estimates

High Priority (1-2 blocks)	Medium Priority (3-6 blocks)	Low Priority (7+ blocks)
0.00017 BTC/KB	0.00008 BTC/KB	0.00003 BTC/KB

Fee estimates are based on a rolling, weighted average.

Exploring the Blockchain

Block explorers are not only specific to Bitcoin. The vast majority of OPEN SOURCE blockchain projects, have Block explorers, on which you can view the networks transactions, transaction confirmations, fees and other useful statistical data.

When you **send/receive a transaction on the Blockchain**, you will generate a **Transaction ID**. This transaction ID can be used to **search for your transaction on the blockchain**. You can use this to **see if your transaction has been confirmed and has gone through or not**.

Some of the most popular Bitcoin Block Explorers can be found below:

Blockcypher – https://blockcypher.com

Blockchain.com – https://blockchain.com/explorer

Blockstream – https://blockstream.info/

Why not check out one of these explorers to see what a transaction looks like?

Just click on any **transaction ID** that you see and see if you can spot some of the things we've spoken about in this guide.

Conclusion

By reading this guide you have learned a number of things about **Blockchain Basics**. You should now have a basic knowledge of:

- **What a Blockchain is**
- **How/Why Blockchain was created**
- **The basic difference between Blockchain and Legacy Ledger operation**
- **The definition of Hash Function (Hashing)**
- **Basics of how a Hash Function is used**
- **Some basics of Public Key Cryptography**
- **What Blocks are and what they consist of**
- **The basics of how and why blocks are chained together**
- **The basics of Bitcoin Mining and a miners role on the Bitcoin network**
- **What Double Spending is and how the Blockchain solves it**
- **How to look up any transaction on the blockchain and understand basic transactional data**

This introductory guide can be followed up by any one of the guides on our **website** and is aimed at beginners. We encourage our users to **DYOR (Do Your Own Research)** and find out as much as possible, before deciding to have any involvement in the crypto markets.

THANKS FOR READING!

WE ARE @BTCBROS ACROSS ALL SOCIAL MEDIA!

BTCBROS

CONTACT US: ADMIN@BTCBROS.CO.UK

WWW.BTCBROS.CO.UK