What is Blockchain?

For one that doesn’t know anything about computers, databases, networks and cryptography, the easiest way to explain blockchain is by starting with something or some process that exists today and show how it can evolve to be blockchain.

Let’s use, for this example, the creation of a Social Security Number. The government maintains a huge database with SSN from everybody in US that is authorized to work. The number is tied to a name and the system has some more information about nationality, birth date, birth place, mother name and address.

|  |  |
| --- | --- |
| SSN | 123-45-6789 |
| Name | John Johnson |
| Nationality | American |
| Birth Date | 02/31/1990 |
| Birth Place | Springfield |
| Mother Name | Mary Johnson |
| Address | 1234 N Springfield Rd, Springfield, SD, 23456 |

Some facts about this arrangement:

1. The government creates and maintains the database (centralized)
2. Anybody that have access to your name and SSN can fake documents and pretend they are you. This is especially true for homonymous people. (not transparent)
3. If you need to change any information, you need to go through the government. (centralized)
4. Anybody that has access to your information can pretend they are you and change information in the government database. (can be changed without your knowledge)
5. Except by comparing several docs and information, there is no other way to prove that you are you. (trust)

Now imagine a scenario where anyone can create their own document, which still meets the needs of what the government needs, but it is totally controlled by the owner of the document.

1. Owner can create the document, by entering all the same information as above, without the need of going to a government facility.
2. The owner of the document has total control of the information and only those that receive the information from the owner can open it.
3. You can change the information as needed (within certain restriction controlled by the protocol like name or birth date).
4. Only you can change your information and nobody else.
5. You can always prove that you are you.

This can be done by using blockchain, and it would work as follow:

* You will enter your information in a form and upload all the proof documents, like birth certificate, proof of address, pictures and any other document that shows you are you. (note that, eventually, birth certificates and proof of address can also be in blockchain).
* The table will also contain a new field that determine if the specific information can or cannot be changed (this is part of the protocol to be used in the blockchain). For instance, the SSN can never be changed, whereas the name or mother’s name can change due to a new marriage.

|  |  |  |
| --- | --- | --- |
| SSN | 123-45-6789 | Immutable |
| Name | John Johnson | Mutable |
| Nationality | American | Mutable |
| Birth Date | 02/31/1990 | Immutable |
| Birth Place | Springfield | Immutable |
| Mother Name | Mary Johnson | Mutable |
| Address | 1234 N Springfield Rd, Springfield, SD, 23456 | Mutable |
| Proof document 1 | Birth Certificate | Immutable |
| Proof document 2 | Proof of Address | Mutable |
| Proof document 3 | Fingerprint file | Immutable |
| Other documents | Pictures | Mutable |

Once we know all the information to be in the table we have to find a way to make sure it only changes if we want and every time it changes we are made aware of it. We are going to add a “fingerprint” to it, which is called Hash and it is unique for the content in the table. If the content in the table changes, the Hash will change too.

|  |  |  |
| --- | --- | --- |
| SSN | 123-45-6789 | Immutable |
| Name | John Johnson | Mutable |
| Nationality | American | Mutable |
| Birth Date | 02/31/1990 | Immutable |
| Birth Place | Springfield | Immutable |
| Mother Name | Mary Johnson | Mutable |
| Address | 1234 N Springfield Rd, Springfield, SD, 23456 | Mutable |
| Proof document 1 | Birth Certificate | Immutable |
| Proof document 2 | Proof of Address | Mutable |
| Proof document 3 | Fingerprint file | Immutable |
| Other documents | Pictures | Mutable |
| Hash | w23g4mdnt58h2 | mutable |

The structure created in this table can be defined as a block of information. Let’s call it Block 1. In addition to the name, we add another component that we call Nonce. This number is added to the table and used as part of the cryptography of the chain. A Time stamp is also needed so it is known when the block was created.

|  |  |  |
| --- | --- | --- |
| Block # | 1 | Immutable |
| Nonce | 89752 | Immutable |
| Time stamp | 02/20/2021 | Immutable |
| SSN | 123-45-6789 | Immutable |
| Name | John Johnson | Mutable |
| Nationality | American | Mutable |
| Birth Date | 02/31/1990 | Immutable |
| Birth Place | Springfield | Immutable |
| Mother Name | Mary Johnson | Mutable |
| Address | 1234 N Springfield Rd, Springfield, SD, 23456 | Mutable |
| Proof document 1 | Birth Certificate | Immutable |
| Proof document 2 | Proof of Address | Mutable |
| Proof document 3 | Fingerprint file | Immutable |
| Other documents | Pictures | Mutable |
| Hash | w23g4mdnt58h2 | mutable |

Now we have a block that contains all the information about one person and can be used as a document for that person. This information is secure and if anything changes you can detect because the Hash will not match anymore.

Now, let say after a few years John Johnson changed his address and needs to update the block. He will make the update with his new address and the following will happen in this database:

|  |  |  |
| --- | --- | --- |
| Block # | 1 | Immutable |
| Nonce | 89752 | Immutable |
| Time stamp | 02/20/2021 | Immutable |
| SSN | 123-45-6789 | Immutable |
| Name | John Johnson | Mutable |
| Nationality | American | Mutable |
| Birth Date | 02/31/1990 | Immutable |
| Birth Place | Springfield | Immutable |
| Mother Name | Mary Johnson | Mutable |
| Address | 1234 N Springfield Rd, Springfield, SD, 23456 | Mutable |
| Proof document 1 | Birth Certificate | Immutable |
| Proof document 2 | Proof of Address | Mutable |
| Proof document 3 | Fingerprint file | Immutable |
| Other documents | Pictures | Mutable |
| Hash | w23g4mdnt58h2 | mutable |
|  |  |  |
| Block # | 2 | Immutable |
| Nonce | 68579 | Immutable |
| Time stamp | 12/2/2022 | Immutable |
| SSN | 123-45-6789 | Immutable |
| Name | John Johnson | Mutable |
| Nationality | American | Mutable |
| Birth Date | 02/31/1990 | Immutable |
| Birth Place | Springfield | Immutable |
| Mother Name | Mary Johnson | Mutable |
| Address | 5678 S Springfield Av, Springfield, MO, 18567 | Mutable |
| Proof document 1 | Birth Certificate | Immutable |
| Proof document 2 | Proof of Address | Mutable |
| Proof document 3 | Fingerprint file | Immutable |
| Other documents | Pictures | Mutable |
| Previous Hash | w23g4mdnt58h2 | Immutable |
| Hash | S9trkkn32stuvxi5 | Mutable |

A few things to be observed:

1. Block 1 is maintained as is (no changes) and a new block is added, creating a chain of blocks called blockchain.
2. The new block, Block 2, contains all the information from the previous block with the addition of one more not present in the first block. This information is the Hash of Block 1, or the Hash of the previous block (thus empty in Block 1). By adding this information in the subsequent block, it makes the chain very secure, because this is part of the Hash of the current block. If anybody changes information in Block 1 and recalculates the hash, it affects the hash of block 2 that will not match anymore. The bigger the chain the harder to change any information on it.
3. The Block #, Nonce, Time stamp, Address and Hash are all specific to this new block.

As one more example let’s say that John Johnson is recognized as a citizen of Mars. The database, or blockchain will be updated as follows:

|  |  |  |
| --- | --- | --- |
| Block # | 1 | Immutable |
| Nonce | 89752 | Immutable |
| Time stamp | 02/20/2021 | Immutable |
| SSN | 123-45-6789 | Immutable |
| Name | John Johnson | Mutable |
| Nationality | American | Mutable |
| Birth Date | 02/31/1990 | Immutable |
| Birth Place | Springfield | Immutable |
| Mother Name | Mary Johnson | Mutable |
| Address | 1234 N Springfield Rd, Springfield, SD, 23456 | Mutable |
| Proof document 1 | Birth Certificate | Immutable |
| Proof document 2 | Proof of Address | Mutable |
| Proof document 3 | Fingerprint file | Immutable |
| Other documents | Pictures | Mutable |
| Hash | w23g4mdnt58h2 | mutable |
|  |  |  |
| Block # | 2 | Immutable |
| Nonce | 68579 | Immutable |
| Time stamp | 12/2/2022 | Immutable |
| SSN | 123-45-6789 | Immutable |
| Name | John Johnson | Mutable |
| Nationality | American | Mutable |
| Birth Date | 02/31/1990 | Immutable |
| Birth Place | Springfield | Immutable |
| Mother Name | Mary Johnson | Mutable |
| Address | 5678 S Springfield Av, Springfield, MO, 18567 | Mutable |
| Proof document 1 | Birth Certificate | Immutable |
| Proof document 2 | Proof of Address | Mutable |
| Proof document 3 | Fingerprint file | Immutable |
| Other documents | Pictures | Mutable |
| Previous Hash | w23g4mdnt58h2 | Immutable |
| Hash | S9trkkn32stuvxi5 | Mutable |
|  |  |  |
| Block # | 3 | Immutable |
| Nonce | 85347 | Immutable |
| Time stamp | 2/30/2023 | Immutable |
| SSN | 123-45-6789 | Immutable |
| Name | John Johnson | Mutable |
| Nationality | American, Martian | Mutable |
| Birth Date | 02/31/1990 | Immutable |
| Birth Place | Springfield | Immutable |
| Mother Name | Mary Johnson | Mutable |
| Address | 5678 S Springfield Av, Springfield, MO, 18567 | Mutable |
| Proof document 1 | Birth Certificate | Immutable |
| Proof document 2 | Proof of Address | Mutable |
| Proof document 3 | Fingerprint file | Immutable |
| Other documents | Pictures | Mutable |
| Previous Hash | S9trkkn32stuvxi5 | Immutable |
| Hash | ç450hg3zpaqlgf9 | Mutable |

Notice the lines in red that are specific to this block. The previous hash is also part of the bloc. Going through each block you can see a history that tells what happened by when.

Now that the concept of blockchain is demystified, the question to be answered is “how can it be ensured that only the owner of the information can change it and he can decide who can have access to it?

To answer this questions there is the concept of private key, public key and signature.

Public Key and Private Keys are used together to encrypt/decrypt a message.

A person will have a public key and a private key. The public key is to be available to anyone. It can be considered as the person identity in the cyber space. The private key is for personal use and not to be distributed at all.

Let’s use an example. Let’s say that John Johnson has a public and a private key as below:

John’s Private Key: 2g8e5d6r8d6c8eg5saj5t45drd5ye90ss

John’s Public Key: alkjerjafnadieutpoz32oae09afjaajsafdsdjo0u9qamsafdu9weaf

And Anne has the following

Anne’s Private Key: 3iowuenmvaljaioqthajgojadjakljfljsadj

Anne’s Public Key: pariuanavdklhpah479akfdjq34tuajafnlaf 8q34tafjtoiuafpojaf0

The Public Key and the Private Key are used to generate a signature that validates a transaction. In our case, let’s assume that John wants to share his document with Anne, because he is applying for a loan.

John will request the Anne’s Public Key and will make a transaction to send the blockchain as follow:

Decrypted Blockchain

Encrypted Blockchain

Blockchain

John will send his blockchain containing his information, from his Public Key (similar to an address) to Anne’s Public key. His Private Key is used to encrypt the blockchain and ensures it was created by him. Anne will be able to decrypt the blockchain because her address is the destination. All this information is now captured as part of the blockchain and it is known who received the information from John.

Note how block 4 now contains information about the Public key that belongs to Anne, meaning that she is authorized and is able to decrypt the information.

|  |  |  |
| --- | --- | --- |
| Block # | 1 | Immutable |
| Nonce | 89752 | Immutable |
| Time stamp | 02/20/2021 | Immutable |
| SSN | 123-45-6789 | Immutable |
| Name | John Johnson | Mutable |
| Nationality | American | Mutable |
| Birth Date | 02/31/1990 | Immutable |
| Birth Place | Springfield | Immutable |
| Mother Name | Mary Johnson | Mutable |
| Address | 1234 N Springfield Rd, Springfield, SD, 23456 | Mutable |
| Proof document 1 | Birth Certificate | Immutable |
| Proof document 2 | Proof of Address | Mutable |
| Proof document 3 | Fingerprint file | Immutable |
| Other documents | Pictures | Mutable |
| Hash | w23g4mdnt58h2 | mutable |
|  |  |  |
| Block # | 2 | Immutable |
| Nonce | 68579 | Immutable |
| Time stamp | 12/2/2022 | Immutable |
| SSN | 123-45-6789 | Immutable |
| Name | John Johnson | Mutable |
| Nationality | American | Mutable |
| Birth Date | 02/31/1990 | Immutable |
| Birth Place | Springfield | Immutable |
| Mother Name | Mary Johnson | Mutable |
| Address | 5678 S Springfield Av, Springfield, MO, 18567 | Mutable |
| Proof document 1 | Birth Certificate | Immutable |
| Proof document 2 | Proof of Address | Mutable |
| Proof document 3 | Fingerprint file | Immutable |
| Other documents | Pictures | Mutable |
| Previous Hash | w23g4mdnt58h2 | Immutable |
| Hash | S9trkkn32stuvxi5 | Mutable |
|  |  |  |
| Block # | 3 | Immutable |
| Nonce | 85347 | Immutable |
| Time stamp | 2/30/2023 | Immutable |
| SSN | 123-45-6789 | Immutable |
| Name | John Johnson | Mutable |
| Nationality | American, Martian | Mutable |
| Birth Date | 02/31/1990 | Immutable |
| Birth Place | Springfield | Immutable |
| Mother Name | Mary Johnson | Mutable |
| Address | 5678 S Springfield Av, Springfield, MO, 18567 | Mutable |
| Proof document 1 | Birth Certificate | Immutable |
| Proof document 2 | Proof of Address | Mutable |
| Proof document 3 | Fingerprint file | Immutable |
| Other documents | Pictures | Mutable |
| Previous Hash | S9trkkn32stuvxi5 | Immutable |
| Hash | ç450hg3zpaqlgf9 | Mutable |
|  |  |  |
| Block # | 4 | Immutable |
| Nonce | 36247 | Immutable |
| Time stamp | 6/27/2024 | Immutable |
| SSN | 123-45-6789 | Immutable |
| Name | John Johnson | Mutable |
| Nationality | American, Martian | Mutable |
| Birth Date | 02/31/1990 | Immutable |
| Birth Place | Springfield | Immutable |
| Mother Name | Mary Johnson | Mutable |
| Address | 5678 S Springfield Av, Springfield, MO, 18567 | Mutable |
| Proof document 1 | Birth Certificate | Immutable |
| Proof document 2 | Proof of Address | Mutable |
| Proof document 3 | Fingerprint file | Immutable |
| Other documents | Pictures | Mutable |
| Shared with | pariuanavdklhpah479akfdjq34tuajafnlaf 8q34tafjtoiuafpojaf0 | Immutable |
| Previous Hash | ç450hg3zpaqlgf9 | Immutable |
| Hash | yplaneidgpwjdne | Mutable |

The last piece to make it all work together that the blockchain is stored in several computers. Everybody in the network has the access to the information. In the case of a document, like in our blockchain, the information about the person in the network will be encrypted and only possible to be decrypted by those who were addressed with the information (those are the white lines in block 5). Everything else will be visible in the network and will be validated by all those connected to the network through a consensus mechanism.

Why is blockchain revolutionary?

Blockchain has three pillars, which are decentralization, transparency and immutability. Those pillars allow for integrity to be added to transactions and also make it possible for people to take control of their own information.

Those characteristics are what makes it possible to fully eliminate middle mans from any transaction. Assets can be sent and received without the need of a bank as intermediary for instance. All the fees related to creating trust thought third parties are eliminated. Transactions can be done between two people or entities in any place as the ledge will contain all the information related to it and the leger is immutable.