WHAT IS DOUBLE SPENDING & HOW DOES BITCOIN HANDLE IT?

Sudhir Khatwani

Bitcoin is gaining rapid popularity and adoption across the globe. It is redefining the way we use the money by being the world's first fully functional digital currency.

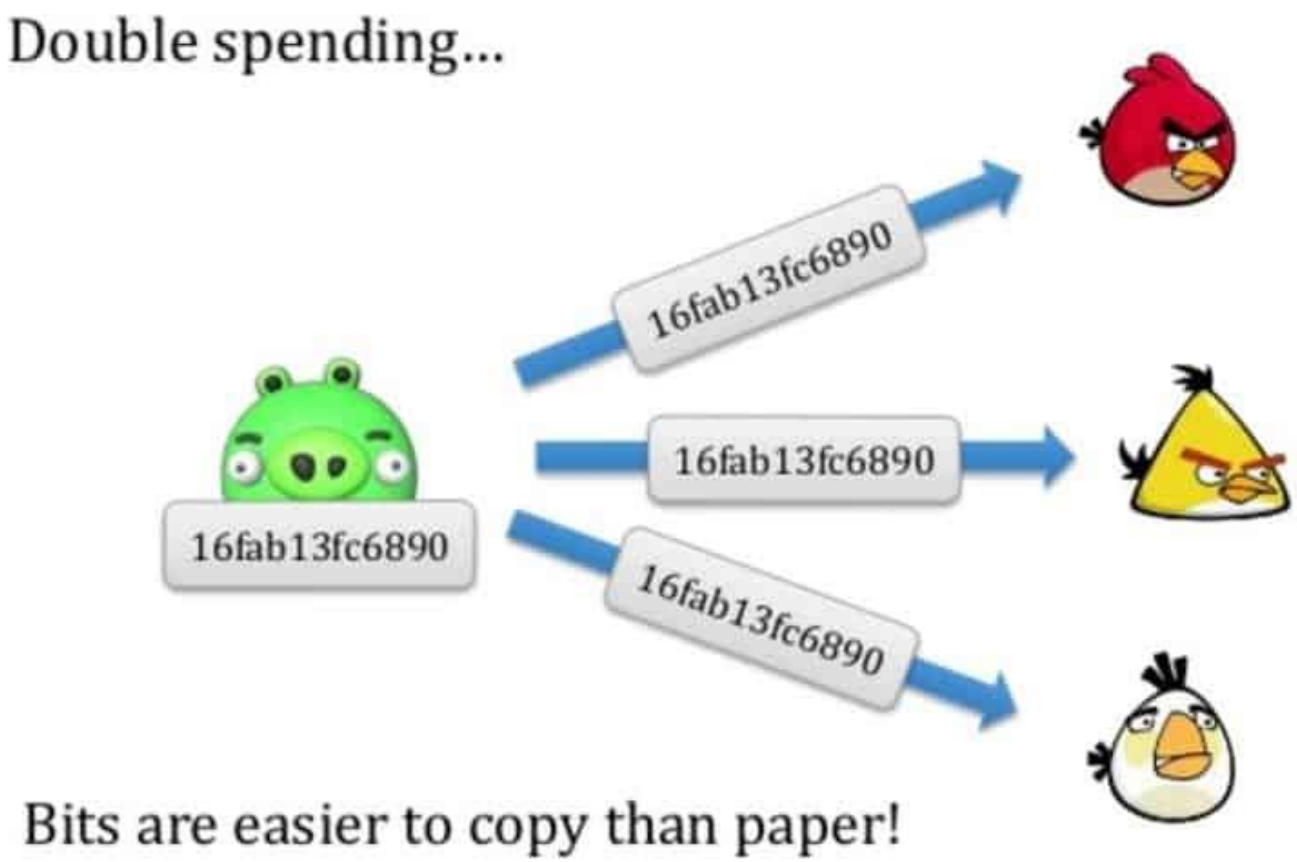
You might be surprised to know that even before Bitcoin, there were attempts to create a sustainable digital monetary system. But all those attempts **failed** because an obvious problem with digital money is that transactions can be copied and spent twice.

Let me simply the concept…

Bitcoin has been able to survive and thrive because it solves the *"double spending"* problem.

- Also read: What is Bitcoin? A Beginner's Guide.

WHAT DOES DOUBLE SPENDING MEAN?



Double spending means spending the same money twice.

Let's consider this example:

You go to Starbucks and order a cappuccino worth $10. You pay in cash. Now that $10 in cash is in the cash vault of Starbucks. By all means, you simply cannot spend the same $10 somewhere else to make another purchase.

Unless you steal it…!!!

As you paid with your $10 bill, the service provider at Starbucks instantly confirmed that you have paid, and you received your coffee in exchange for the money.

But Bitcoin is ***digital*** money, not physical cash. Hence, Bitcoin transactions have a possibility of being copied and rebroadcasted. This opens up the possibility that the same BTC could be spent twice by its owner.

How?

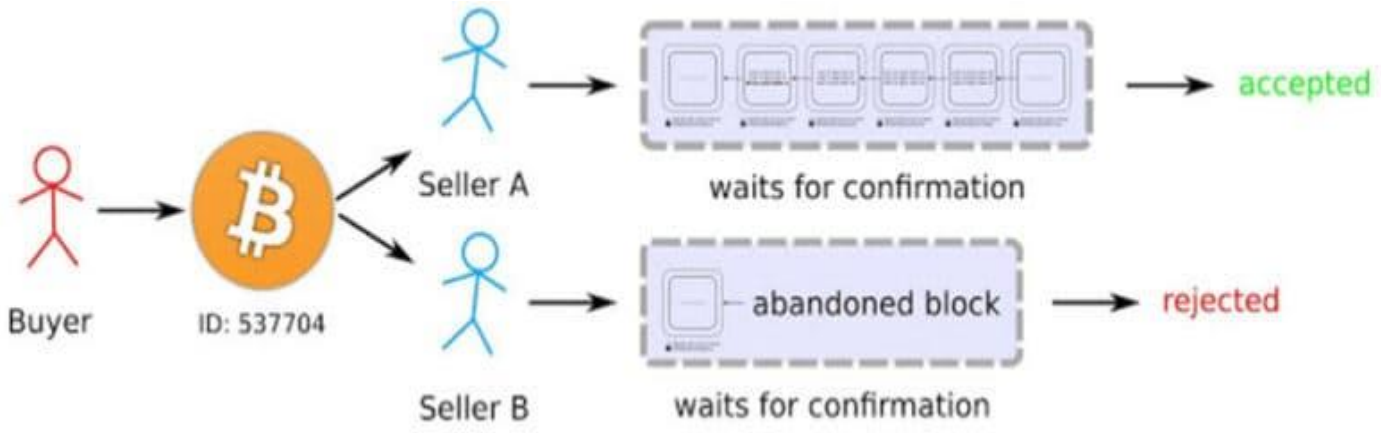
In our Starbucks example, you paid cash, so the payment was confirmed and verified instantly by another human. But with digital currency like BTC, if this verification mechanism is missing, it can lead to double spending.

Anyone can just copy that digital money and pay somewhere else.

And here is where the unique invention lies…

Bitcoin, although being a digital currency, **solves the problem** of being copied and getting spent twice.

How Bitcoin Handles The Double Spending Problem



Bitcoin manages the double spending problem by implementing a confirmation mechanism and maintaining a universal ledger *(called "blockchain"),* similar to the traditional cash monetary system.

Bitcoin's blockchain maintains a chronologically-ordered, time-stamped transaction ledger from the very start of its operation in 2009.

Every 10 mins, a block *(i.e. a group of transactions)* is added to the ledger. And all the nodes on the Bitcoin network keep a copy of this global ledger *(the blockchain).*

Let's see how the Bitcoin network prevents double spending:

Let's suppose you have 1 BTC which you try to spend twice.

You made the 1 BTC transaction to a merchant. Now, you again sign and send the same 1 BTC on another Bitcoin address to try and trick the merchant.

Both transactions go into the unconfirmed pool of transactions. But only your first transaction got confirmations and was verified by miners in the next block. Your second transaction could not get enough confirmations because the miners judged it as invalid, so it was pulled from the network.

But wait… what if both the transactions are taken simultaneously by the miners?

When miners pull the transactions simultaneously from the pool, then whichever transaction gets the maximum number of confirmations from the network will be included in the blockchain, and the other one will be discarded.

You might say that this is unfair for the merchant, as the transaction might fail in getting confirmations. Yeah, this can happen!!!

That's why it is recommended for merchants to wait for a **minimum of 6 confirmations.**

Here, "6 confirmations" simply means that after a transaction was added to the blockchain, 6 more blocks containing several other transactions were added after it.

"Confirmations" are nothing but more blocks containing more transactions being added to the blockchain. Each transaction and blocks are mathematically related to the previous one.

All these confirmations and transactions are time-stamped on the blockchain, making them irreversible and impossible to tamper with.

So if a merchant receives his/her minimum number of confirmations, he/she can be positive it was not a double spend by the sender.

Why can the merchant be assured?

Because to be able to double spend that coin, the sender has to go back and reverse all transactions in the 6 blocks that have been added *after* their transaction, ***which is computationally impossible.***

How Double-Spend Attacks Can Happen

- **Attack 51%**

If somehow an attacker captures 51% of the hash power of the network, double spending can happen.

"Hash power" means the computational power which verifies transactions and blocks. If an attacker has this control, he/she can reverse any transaction and make a private blockchain which everyone will consider as real.

But so far, no such attack has happened because controlling 51% of the network is highly cost intensive. It depends on the present difficulty of mining, the hardware price, and the electricity cost, all of which is infeasible to acquire.

- **Race Attack**

When an attacker sends the same coin in rapid succession to two different addresses, the obvious outcome is that only one of them will get included.

Now, if you as a merchant don't wait for confirmations of payment, then in a case like this, there's a 50% chance you got the double spent coin (and you won't receive that money).

Let's see how…

Your customer can trick you if he/she sends the same coins again to his/her address.

Once the customer does both transactions, both transactions go to an unconfirmed pool of transactions. Whichever transaction gets verified first and gets 6 confirmations will be accepted, and the other will be discarded.

As a merchant, you might get the 6 confirmations first, but if the attacker gets the confirmations first, then you won't receive your funds. That's why it is said to wait for a **minimum of 6 confirmations.**

So far, in the 8-year history of Bitcoin, no such attack has been successful. The Bitcoin mechanism of maintaining a universal transaction ledger based on confirmations has yet to be tricked.