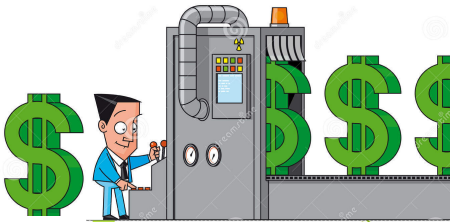
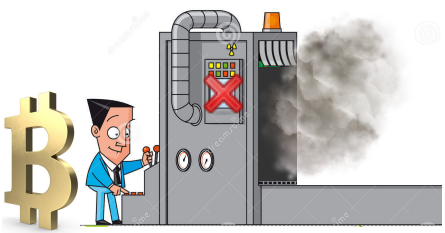
What is Bitcoin



In today's information age, almost anything can be duplicated. Money especially must be copy proof to ensure trade can happen fairly.

Cash is designed to be hard to counterfeit, but it isn't perfect. However, it is difficult enough that the average person won't bother to try.

We rely on the integrity of our government and democracy to guard the monetary system, but they leverage our trust to **counterfeit** legally

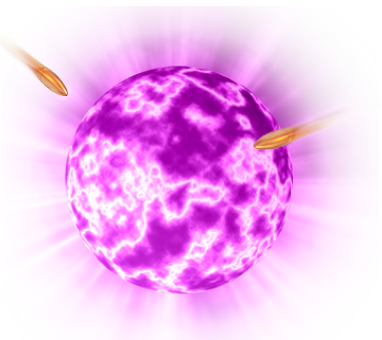


Bitcoin is the **discovery** of the **solution** to the **double spend problem**.

Everyone guards the system, and **no one** has the power to break or bend the rules or counterfeit.

There is no longer a need for a central trusted authority for money!

Similarly to a watch, the solution is composed of many parts which are precisely tuned. It relies on a mix of cost and hardware considerations: designed to allow as many participants as possible, and incentives: designed to create competition and promote harder security.



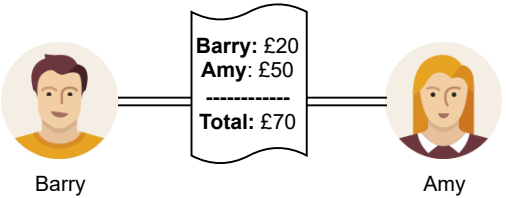
Over the years since January 2009, all attacks and attempts to break or corrupt Bitcoin have so far only made it stronger.

Incentives make it more profitable to participate in the network than attack it, and even coordinated propaganda has only helped to produce better learning material and rebuttals

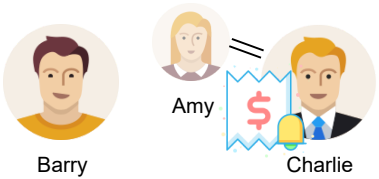
Lightning Wallets explained simply

This is Barry

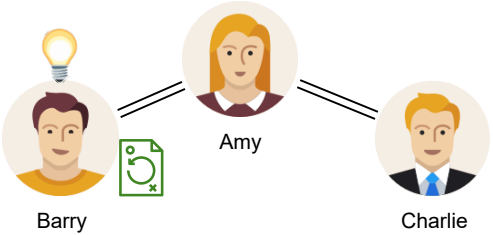
Barry has a few friends and business associates with whom he keeps money aside for.



Barry has a shared pot with Amy that is quick, and easy to update. Note: we call these "channels".

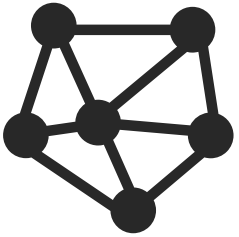


Barry needs to pay Charlie but wants to use the funds in the channels he has with his friends. Amy just so happens to have a channel with Charlie!



Barry makes a conditional update to his channel with Amy that ONLY completes if she can PROVE that she gave Charlie the funds. Barry agrees to include a tiny tip for Amy too.

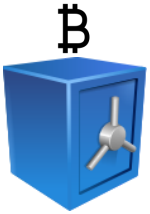
Payment complete!



Re-allocating funds within online digital pots became so convenient, it turned into a global peer to peer payments network atop Bitcoin.

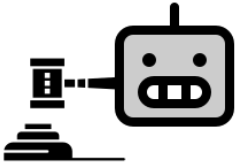
An honest, personable payment network that works without banks!

Why does it rely on Bitcoin?



Every address on the Bitcoin network is like a mini personal vault.

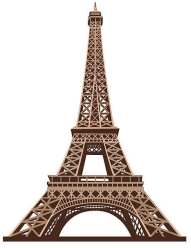
Bitcoin's "multisig" feature allows for vaults locked by 2 or more keys, creating joint accounts, or even ZERO TRUST pots between strangers.



Bitcoin's programmability allows users to define break clauses before depositing money into a multisig address. This allows shared pots to be closed fairly by either party if the other ever stops cooperating.

These features provide a sound foundation for the lightning network to run atop.

Zero trust multisig addresses with break clauses make the perfect shared pot to use.



The lightning network runs atop Bitcoin and only uses bitcoin locked in secure pots.

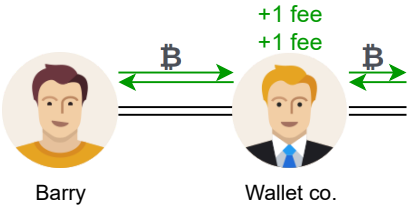
This enables faster and cheaper payments without introducing any **debt** or **credit** systems.

The lightning network complements Bitcoin's sound money properties. It was carefully designed to enhance its utility without compromising your uniquely independent control over it.

What's the catch?

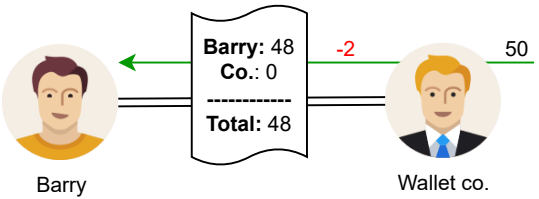
Businesses need to make money, nothing is truly free, so how do lightning wallets work?

This section focuses on user-friendly commercial wallets. Technical users may find cheaper alternative solutions and maybe even business opportunities of their own.



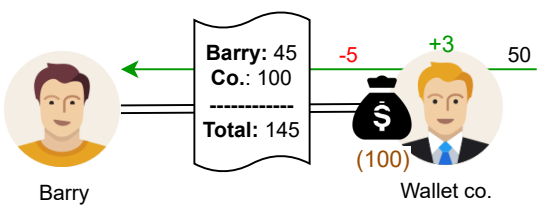
Most wallets connect you to a corporate channel; one between you and them.

This enables a smooth, reliable experience; but it also means that they are always there to collect a fee from every incoming and outgoing payment.



Although not a catch, when you receive your first deposit, a channel needs to be created. The cost for this will be taken from **your** deposit; it's only fair.

But a channel with 0 balance on the company side is not very useful if you want to receive more money later on.

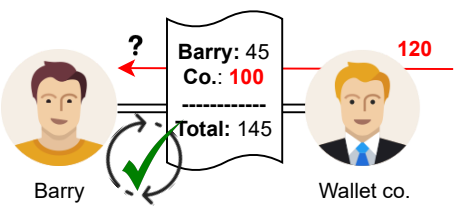


Companies will add some of their own funds to the channel so that they have a balance too. This allows for some incoming payments without having to create more channels at further cost.

Companies will charge a fee for this as it requires them to reserve and **lock** some of **their** capital.

The **good news**, is that the best apps are **open source**. Companies do this to gain reputation, allowing experts to verify that there are **no tricks** up their sleeves, that **they aren't deceiving you**, and all control is kept **on your device**, not hidden away on their servers.

Be sure to ask a knowledgeable friend what wallet they recommend that's open source! There are a handful of good ones.



One thing to note, is that whenever you receive more than your channels will allow, most wallets will automatically create a new channel for you instead of failing; taking a fee from the deposit once again.