Wrapping your head around Bitcoin

Introduction

How does one wrap their mind around Bitcoin? Let's see if we can answer this question in a very short, concise and to laymen friendly way. In order to help the reader grasp the important points we'll highlight them in big letters when they come up.

What you are familiar with

Ask yourself, why do you use your national currency? Whichever one you use, the answer is the same. You use it because you can exchange it for something that you want/need? Next question you should ask yourself is why do other people take your national currency from you in exchange for whatever? Again the answer is the same no matter which national currency you use; they take it because they know they'll be able to use it to get something in exchange for it that they themselves will want/need.

So basically people use national currencies because based on what they observed in the past they assume tomorrow they'll be able to get something they'll want/need in exchange for it.

National currencies are used because they are used

But wait a second, why does this system work? Ignoring the history of how it came to be, this system works primarily because everyone knows that the national currency they use is popular within a region, meaning you're likely to find someone who'll accept it, it's plentiful meaning there's not just 1 note somewhere in someone's hand, many people have this currency, but it's also not too plentiful meaning it kind of keeps its value in the short term(and usually only slowly and steadily loses its value in the medium term) and people cannot just make more of it (well.. besides people in central banks). And to top it all off, governments force people through legal tender laws and tax laws to use it for payment of legal debts and taxes.

So it's pretty clear all these aspects are guaranteed by laws of governments and by actions of central banks and the banking system. One could say it's an entire money system behind your national currency that provides it and provides it in a form that people consider as useful for the role of money.

Now let's innovate

Bitcoin is an entirely new money system

The difference between the Bitcoin money system and the money system we just examined is profound and you must make note of it if you want to properly wrap your head around Bitcoin. The difference is that while the national currency money systems are governed by men (men who run governments, central banks and the banking system) the Bitcoin money system is governed by computer code. Where national currency money systems are built upon agreements between men, the Bitcoin money system on the other hand is a technology and the money system is built upon this technology in a functional state.

And it's not just any kind of technology, it is a first of its kind technology. You may have heard that Bitcoin is a digital currency and shrugged it off thinking it's nothing new and it has been done before but you'd be making a huge mistake doing so.

Bitcoin, from a technological standpoint, has never been done before

Similar to national currency money systems the Bitcoin technology encompasses more than just a currency. With national currency money systems we could draw an analogy to national currency being the blood that runs through banks and financial institutions which would then be the veins.

The same analogy could be applied to the Bitcoin money system within which there is both a digital currency called bitcoins - the blood - and a payment system called Bitcoin that handles this currency exclusively - the veins - both which are governed by the Bitcoin technology.

Bitcoin is both a currency and a payment system

Before I explain how this technology works, let's look at what principles were chosen to be built into it. Because as we've seen with national currencies, money needs to function under certain principles and with certain properties, otherwise it wouldn't work because no one would want it or have a use for it. Plus keep in mind using Bitcoin is entirely voluntary as opposed to national currencies meaning it must be that much more appealing if anyone would ever voluntarily decide to use it.

So for better or for worse (there's a lot of debate which principles are preferred in money), in no particular order of importance, here is a list of 10 principles the Bitcoin money system is built upon:

1. FINITENESS - unlike the infinite possible supply of fiat currencies the total supply of bitcoins that will ever exist is forever arbitrarily limited and fixed
2. TANGIBILITY - issuing new bitcoins requires labor in the form of finding a specific number by solving a cryptographic mathematical problem
3. TRANSPARENCY - all Bitcoin transactions are public and forever stored in a transaction log called the blockchain which anyone can read and examine
4. ANONYMITY - all Bitcoin transactions are only between cryptographical pseudonyms without the need to have their owner's true identity revealed
5. SECURITY - all confirmed Bitcoin transactions are with mathematical certainty irreversible, all bitcoins are with mathematical certainty non-counterfeitable
6. DECENTRALIZATION - Bitcoin has no central authority and is voluntarily run by consenting autonomous peers in a peer to peer network
7. SELF-OWNERSHIP - only the owner of a pseudonym gets the password to spend his bitcoins in effect making them his property unless he chooses otherwise
8. INTEGRITY - all bitcoins are counted equally(are fungible), virtually can’t be frozen or blocked from being spent
9. PRACTICALITY - Bitcoin works anywhere, for anyone, non-stop, and the protocol allows for many practical layers on top, just like email, http..
10. RATIONALISM - the Bitcoin software is written under the MIT open source license and is not anyone's logically inconsistent intellectual property but merely organized information everyone can use as they wish

One can easily see how people would value such a money system, right?

Bitcoin is used because of the principles it's built upon

Yeah, that's right.. just like national currency money systems. So when you're scratching your head and asking yourself why would anyone cough up national currencies, or anything else of value for that matter, in exchange for some bitcoins, here's your answer; they do it because they value those principles and the properties bitcoins have because of them.

And it really isn't more complicated than that. Plus now after running for four years Bitcoin has also developed a bit of a history, perhaps just enough so that an online "region" has grown accustomed to bitcoins having value to other people within this same community and so many of these people now assume they will be able to find someone tomorrow who will exchange something they'll want/need for bitcoins.

But does it deliver?

Well, you will now likely think, those principles sure sound nice for a money system but how can I know that won't change, how can I know that tomorrow suddenly someone won't find a way to break one or more of those principles and steal from me? That's a reasonable concern.

Remember, Bitcoin is a first of its kind technology. The building blocks actually aren't very new and were already used independently for quite some time now which is also a reason why it's easy to think Bitcoin can work. But it is how these building blocks are put together into a functioning whole that transforms them into something completely new. And what this new thing is, is a technology that is practically impossible to cheat.

It is practically impossible to cheat the Bitcoin technology

What does this mean? And why practically? Well we want to be accurate.. Theoretically it is possible but we'll see in a minute why that is so highly unlikely that for all intents and purposes it is impossible.

Again, remember that Bitcoin is a first of its kind technology, so when asking the question how exactly it works the best answer most likely is to change this question and instead rather ask who is Bitcoin. That is much easier to answer because Bitcoin can essentially be anyone with a computer or some other device connected to the internet. The only condition is that they install the Bitcoin software, and bam, they are part of Bitcoin.

More precisely when someone does that this software then connects their computer to other's who also run this software and so connected to each other all Bitcoin users form a person to person network. Next, when you run the Bitcoin software on your computer what it also does is it listens to what other users and their Bitcoin software are transmitting and the brilliant part about this process is that it is coded to simply hear those other users that follow the same rules as you.

Let's look at an analogy to understand the ramifications of this. See what happens is pretty much like if you were sitting in a school classroom full of your classroom mates and a teacher. And because you are "coded" to hear and understand only English, when a French exchange student sits next to you and starts talking to you in French, you simply don't understand what he is saying and so you ignore him, and so does everyone else in the classroom. You don't need the teacher to control you and tell you to not talk with him, it's because you and the French exchange student are communicating under different rules that no communication can take place.

Same goes for the Bitcoin peer to peer network and it's why the rules can't change. If someone would do so, they would simply get ignored by the rest.

> Bitcoin simply ignores those who don't follow its rules

And there you go. The only way the Bitcoin rules could ever change is if you can get all users to simultaneously download a new version of a Bitcoin application, something that is practically impossible since the code is open for everyone to examine, there is no autoupdate and there is no single Bitcoin application but there are many different versions developed by different people.

So as long as there are just a few people running a Bitcoin application under the original rules Bitcoin can function and the rules can't change. The real trick in all of this is that being able to merely fake your Bitcoin software follows the rules is made impossible by the laws of mathematics, specifically cryptography.

The renowned cryptographer Bruce Schneier even eloquently said that in order to fake following these rules the chances of succeeding doing it are: ".. infeasible until computers are built from something other than matter and occupy something other than space."

To be able to really understand this we'd have to delve into some pretty advanced math but suffice it to say that the same cryptographic principles that protect military, banking and government secrets is also used in Bitcoin and if it fails for Bitcoin it will also fail for all those other organizations.

> Faking obeying Bitcoin rules is made impossible by laws of math

Conclusion

So in summary, when you take all of the above into account you are left with a first of its kind potently highly disruptive technology that is a new money system with both a currency and a payment system, built on top of arguably very desirable principles and is practically impossible to cheat. Truly understanding this will give you a new perspective and will open up a whole new world to you, a world in which you:

- are in full control over your finances at all times
- define how public you want your ID information to be within a transaction
- are protected from anyone being able to freeze or seize your money
- receive money without having to pay any fees
- don't face any risk of money system fraud
- can preserve your purchasing power through ensured limitedness of bitcoins
- can send any amount to anyone, anywhere, anytime without having to ask for anyone's permission

Bitcoin is important because it represents:

- ✓ freedom
- ✓ honesty
- ✓ progress
- ✓ complete control over your finances

Basically if you care about any of this there's nothing on this planet that comes even close to it.