Ruben explains Bitcoin.

Ok, print this out and read it before bed or anytime you have a minute to contemplate what I am about to explain. Because if Bitcoin has an Achilles heel, it's that it is not trivial to understand. But, just like driving was an intimidating concept when you were 14, but today you just drive, so Bitcoin can forever change the way we all think about money once you get past some basics.

Actually driving is a good analogy, as cars are horribly complicated machines, but you don't need to understand timing chains and fuel air mixtures to drive.. So, I will start with what you need to know to "use" bitcoin, then we will talk about how it works and what makes it simply amazing and revolutionary.

To use bitcoin, you need a "digital wallet" to store your bitcoin, and some bitcoin to spend (literally, that's it, no forms to fill out and no waiting days/weeks to get started :). Transactions happen very similar to things like ApplePay, Google wallet, or any of the other electronic transactions we are becoming accustomed to. You present your smartphone to either a teller machine at a checkout or an ATM, or just interact with another digital wallet directly (smartphone apps are the best way to keep a digital wallet, as they are both portable and can use things like the onboard camera and NFC to conduct transactions).
Most bitcoin transactions use "QR codes". QR codes are those funny little square "bar" codes you see on so many things these days. (QR codes can represent different things, like web pages, business cards or in our case digital wallet accounts)

To exchange bitcoins with another party, the sender uses their digital wallet to scan a QR code generated from the recipients' wallet and enters how much bitcoin to send.
That's it, again pretty simple. Now, there are other ways to store or transfer bitcoin, you can imbibe value to some physical objects such as coins and even just printouts, but they must have a Public/Private Key on them (we will discuss this in a minute when we talk about what's under the hood in Bitcoin. But you can add any value (up to as much bitcoin as you own) into a simple coin,

or piece of paper.

Ok, now for the fun part, how does Bitcoin work, and why is it better than the currency system we have now?

<Warning: Math ahead, you have been warned.>

Bitcoin is simply math, now we are talking some pretty impressive math, and I mean Einstein, Tesla, Leonardo da Vinci brilliant! Whoever put all this together to create Bitcoin is well ahead of their time (we don't know who exactly came up with the idea, but that's another story ;).

The basic math concept at work here is called "Hashing" (not to be confused with recreational substances gaining popularity in Colorado ;). Hashing is a math function such that you put in a string of numbers and out comes a fixed length number. Sounds pretty mundane, but there is one interesting property, when you change what numbers you put in, what comes out is not at all related to what came out from the previous input number. Let me explain, if you entered the number 1, and hashed it, you might get out the number 1983546. And if you entered the number 2 you might get out 0000006. So just knowing what comes out does not give you any idea about what went in. But the process is repeatable, not random, so if I enter 2 and hash it, it would always come out 0000006.

So the application here is, if I have a Bitcoin wallet "Private key" that holds the value of my bitcoin, I will hash this "account number" and out will come a "Public key". And here is where the magic comes in, everyone can keep a copy of these public keys in a "ledger" that is Bitcoin, recording every transaction and verifying every account value by its public key. Since public keys do not give you any authority to spend value, only verify and deposit, everyone can know my public key which will identify my account without any risk of someone taking my bitcoin!

Quick step back, I said ledger previously, lets take a closer look at that, because it is the this ledger (Called the blockchain) that is what makes Bitcoin work and also provides the amazing potential for money in the future.
The blockchain is a record of transactions. Every transaction that has ever happened in bitcoin is recorded in the blockchain. Anyone and everyone is entitled to keep a copy of this "ledger". But how do you keep someone from "cooking the books" by fabricating transactions adding or subtracting from people's account. Well, here is where the magic of hashing takes on another role. Every transaction that goes into the blockchain has to be verified by using the previous block (page in the ledger). If your account went up in value, you have to show where that bitcoin came from by subtracting it from someone else's account that already had it (and you would need the private key of that account to authorize that). So you can't fabricate value, and without the private key you can't take it (remember the blockchain is a record of public keys which does not give you any information on the private keys that are needed to have the authority to spend). Finally, once all the transactions are verified and a new page of the blockchain is complete it is "sealed" by hashing it, and the result of that hash goes in to become the seed to the next block (page). So once you spend bitcoin you can't go back and undo a transaction (no chargebacks here) and if you tried to spend the same coins again, the sealed block (page) of the ledger would show you already spent them.

Ok, so we have established that the blockchain is tamperproof, but where do bitcoins come from? If we need to get bitcoin from someone else's account to increase our own, where do these people get bitcoins from in the first place? Here is where we talk about “miners”. Miners are people who work on creating the next block (page) of the blockchain. Miners collect all the transactions that have not yet been verified and sealed and put them together and hash them with the seed from the previous block. Whoever does this creates a new block and is awarded bitcoin for their effort (currently 25 bitcoin given per new block). Now those of you paying attention may realize 25 bitcoin is worth thousands of dollars! Who would not want to make the next page, and how do we decide who gets the privilege of going next? Again, we go back to our old friend the hash, if we hash all the unverified transactions and the seed from the previous block out comes some number, now we know if we add any additional number the outcome from the hash will be very different. So in order to have the privilege of writing the next page you have to adjust the hash to meet certain criteria (certain number of leading zeros), and we do this by adding a nonsense number that has no purpose other than to change the output of the hash. this number is called a “nonce” and miners must make many many guesses changing the nonce in a race against all the other miners until the hash results in a number with the correct number of leading zeros, once this is found, it is presented to the network to be verified, and if correct, a new block is created, 25 bitcoins is awarded to the miner who created it and the process begins again for the next block.

Ok, it’s time to make your head hurt with math. The number space we deal with for Bitcoin is an enormous number, we don’t have words to describe numbers this big.
(As an example, here is a bitcoin wallet “account number” expressed in decimal :
79,997,772,847,639,216,672,418,180,991,860,902,976,156,612,091,045,226,626,673,405,579,803,985,222,202)
The quantity of possible unique numbers is simply unfathomable (2^96 for the curious). Saying it is billions of billions upon billions still not describe this number space.
This unimaginable pool of numbers helps bitcoin in several ways. First, when you want a new bitcoin address, you just pick one, you don’t check if anyone else has that account number already, because they don’t and never will. Let me give you an example, let’s say you wanted to have 2 bitcoin wallets, as a level of security if you believe someone could steal the money from one (Stealing is possible, but it requires the thief to get ahold of your private key, either via hacking or negligence on your part) ok, what if I told you you could have a million wallets. What if I told you you could have a million wallets every minute. What if I told you you could have a million wallets every minute for every minute you were alive! What if I told you that if all 7 billion people on the planet did the same thing, we would still have lots of wallets left unused! There ya go, now you're getting the idea of scale here. It’s this pool that makes “guessing” a private key impossible (yes, if I could guess your private key, I could spend your money, no passwords, no authentication, simply security through obscurity). However, as an example, the theoretical perfect super computer, computing at the speed of light, would not be able to “guess” your account number before the sun burned out in billions of years!

Ok, now back to the blockchain, when a miner randomly changes the “nonce” the hash will change, but as we are still in this same expansive number space, it may not be the value required after one, two, millions or even billions of “guesses”.
Bitcoin automatically adjusts the “difficulty” or number of leading zeros required from the hash to create a successful result, to maintain that a new block is created only every 10 minutes or so. So depending on the difficulty of the block many hashes will be required before an acceptable solution is found. At first when the difficulty was low, personal computers were sufficient to solve the block every 10 min. But as this is a race, people began finding faster and faster ways of hashing. CPU’s can hash at about tens of thousands of hashes per second, pretty impressive till you realize a video card can do hundreds of thousands of hashes per second. But seeing as the payout for a new block is worth thousands of dollars, it’s worth finding something even faster. Enter the ASIC (Application Specific Integrated Circuit) chip. ASIC are hardware chips that do only one thing, HASH! So they do it very quickly, the first ASIC chips were able to make millions of hashes a second, running them in parallel, larger “rigs” were able to do billions of hashes a second, and today it is possible to buy miners that are capable of a hashing TRILLIONS of times a second! As each generation of chips gets faster, and as more and more people try their hand at the “free money” that is given out for mining, the difficulty continues to rise, till an equilibrium is reached.

Hang on, we are almost done, now that you understand bitcoins, and the blockchain, there is one more important facet. Bitcoins are only the tip of the iceberg. The blockchain can be used to “represent” almost anything and still works in the same impressive way. Let’s say stocks, I could make stock in a company available via a blockchain. Let’s call it stockcoin. You could sell stockcoin to people and they keep them like bitcoins, their ownership would be represented in the blockchain and would be completely transparent and public, anyone could trade shares without the need for an exchange, they would simply exchange them as we do bitcoins. The only difference would be incentivizing the miners to keep making the Blocks (ledger pages) as with stockcoin unlike bitcoins the company would start out owning all the shares and transactions would all begin from the company's account to the investors. One solution would be for the company to pay “shares” to miners to keep the blockchain, or you could make transaction fees which would go to the miners for keeping up the blockchain. Ownership would be pseudo anonymous with only public keys as metrics, but each share and each transaction would be recorded and trading could happen around the clock and around the world!

Finally, Bitcoin is very robust, the protocol allows for many useful things like setting up multiple keys to release funds (Escrow). Bitcoin also has a self limiting production (There will only ever be 21 Million bitcoins produced to combat deflation), This, and the fact that the software is “open source” such that it can be modified in the future to adapt to needs not foreseen today (Changes must be adopted by consensus, and cannot be forced upon the system by lone agents).

There is much more to Bitcoin, but this concludes my primer. I would suggest further reading and understanding, as components of Bitcoin if not the entire system will be part of how we use money in the future.

Ruben Guardiola