Lets really kickstart this section, in this lecture I want to explain what the blockchain actually is. So you may have heard the term blockchain thrown around in this course already.

But for a real basic definition of how the blockchain works - just to kick things off, imagine two metaphors: a fly trapped in amber, and a magical, automatically synchronizing book that keeps every single transaction in every single copy.

Now, you might have scratched your head, or asked yourself… One of two questions:

First… “Isn’t this all ridiculously inefficient?” After all, just imagine all the terabytes of data that are wasted by storing the entire Blockchain thousands and thousands of times. And think about all of the wasted computing power created by the miners having to perform advanced cryptography and agree on every single transaction. And actually, you’re right: Blockchain technology is extremely wasteful. Not only because of all the duplication, but also because a lot of the very complex computing-power intensive calculations that miners do, end up getting thrown out or invalidated.

But let’s leave that aside for a second, because the truth is, no matter how you cut it, Blockchain is still extremely wasteful - by design. You see, it turns out that precisely because Blockchain is so wasteful, it’s also extremely secure. While it may not make sense from an efficiency standpoint to keep every transaction on every single full node, it makes the Blockchain literally impenetrable. The same goes for the extremely challenging - and increasingly complicated - cryptography that goes into each block. Just as all of this is extremely wasteful for the miners and the ecosystem as a whole, so, too, is it extremely challenging and cost ineffective to try and alter a block. You’d have to somehow simultaneously fool thousands and thousands of computers, and redo the work the’ve done, which together form the most powerful computing network the world has ever known. A heist of that scale would cost thousands of times more than you’d be able to steal from it - if it were even technically feasible.

And that, my friends, is the incredible power of Blockchain.

Blockchain technology, and cryptocurrencies like Bitcoin in particular, offer us much more than impenetrable security in an increasingly vulnerable digital world, though. In fact, that’s just a small part of their true potential.

Perhaps even more exciting are the new possibilities they unlock: They allow us to collaborate with people and things we don’t even trust.

In the past, in order to do business with someone, you had to, well, you know… TRUST them. You had to be sure that they were actually going to deliver the products or services they promised, or your could lose your money. You had to trust in the legal system and in the contract that you created with them - that it didn’t have any “holes” in it, and that the courts would side with you in the event of a grievance. In fact, you had to trust in lots of third parties, like governments, that the fancy piece of paper you’d been given was authentic legal currency, and actually worth what people say it is. You had to trust in the bank - and in the government - that they wouldn't steal or seize that money once you deposited it. And you had to trust in the entire system - that that fancy piece of paper would be worth something tomorrow. All in all, you had to trust in a lot of people, systems, and things before you could collaborate with someone - even if that meant that you both would trust a so-called “trusted third party.” And, as cryptocurrency luminary Nick Szabo loves to remind us… “Trusted third parties are security holes.”

How many times have banks, credit card companies, retailers, and even governments been hacked, exposing your information to the preying eyes of criminals? How many of us have had our credit card number stolen because we trusted an online retailer, or been cheated by an unscrupulous business person who didn’t pay up?

With Blockchain, Bitcoin, and some of the additional technologies being built on top of it such as digital smart contracts baked directly into the blockchain itself, both these vulnerabilities, and your need to trust these so-called trusted third parties like banks, courts, or governments, go away.

In fact, with Blockchain, you don’t even have to know the other parties involved in a transaction - much less trust them. All you need to trust in is math - the sophisticated mathematical and cryptographic operations being done by the network, and maybe trust that the entire internet won’t go out…. Though, even if it does, you can rest assured that your money, contract, or anything else is securely stored in a distributed ledger - safely kept on thousands and thousands of computers, and completely untouchable.

All of this is very exciting, not just for money, but also for all of the sensitive and secure data that humanity needs to keep safe. But, that’s another topic for us to explore in another lecture. For now, at least, I hope you guys understand why exactly Blockchain is such a tremendous innovation, and why it is already changing the world as we know it.

See you in the next lecture, where I’ll be differentiating private and public blockchains for you.