What is Blockchain Anyway?

A simple guide to how blockchain works

A TranSolutions Inc. Publication
By Vanessa Glavac

Learn more about TranSolutions' claim management software at www.TransolutionsInc.com

How Does Blockchain Work, Anyway?

There's a lot of buzz right now about blockchain and how it could revolutionize the supply chain industry. But before you can speculate on new uses for blockchain, you need to understand how it works.

Most explanations we found seem to go one of two ways – either they're so detailed that you need a computer science degree to understand them, or they gloss over the process in a sentence or two. We've done our best to present a plain-language explanation of the major principles. Most of the information here relates to the blockchain behind Bitcoin – there are different types of blockchains just like there are different types of databases or TMS's, but this will serve as a starting point for how blockchains in general work.

The Basics – What is a Blockchain?

A blockchain is essentially a ledger – a list of transactions. In the case of bitcoin, the blockchain tracks financial transactions, but the same principles could be used to track other exchanges, such as the flow of goods through the supply chain.

In traditional financial systems, the ledger is stored by a trusted 3rd party such as a bank, who manages the ledger as well as some backups. In the case of banking, you can see your own transactions, but you cannot see the full ledger. Moreover, you rely on the bank to process transactions. This works fine if the bank is trustworthy. However, banks, governments, and financial institutions have historically been prone to corruption and mismanagement. In fact, Bitcoin was developed as a result of the 2008 financial crisis.

What makes blockchain unique is that the ledger is decentralized – instead of relying on a trusted third party, it relies on a peer-to-peer network. No single entity stores or manages the ledger or transactions. Instead, the full record of all transactions are stored on the computers of anyone who wants to download it. This also means that the transactions are fully transparent – anyone can see every transaction since the beginning of the blockchain (although the users and accounts may be anonymous).

The distributed nature of the blockchain means that transactions cannot be faked, altered, or destroyed. Once you make a transaction on the blockchain, a record of that transaction will be stored on every computer in the network.

Calculating Balances & Sending Transactions

The blockchain keeps of a record of every transaction that has ever happened since the beginning of the blockchain. To determine how much money you have in your account, a computer program reviews every transaction that has ever happened between every account, and then calculates how much money you have.

To make a transaction, you send a message out to the network. That message tells the network that you want to update the ledger and move money from your account to another person's account. When it reaches another computer, (or "Node"), that computer updates its copy of the ledger, and then sends your transaction out to its neighboring nodes. Those nodes then do the same thing, and your transaction propagates throughout the network.

Keeping All Ledgers Consistent

But if there are multiple ledgers on multiple computers, what if there's a difference between some of them? How do you know which one is the true copy?

This is where the problem of "Double Spending" comes into play. Let's say a freight thief orders your product. To pay you, he sends a transaction throughout the network. He has $10,000 in his account, and the order costs $10,000, so he has enough for the transaction to go through.

But, it takes time for that transaction to propagate throughout the network. The transaction will reach some nodes before it reaches others, so the thief can take advantage of this. Immediately after that first transaction, the freight thief could send that same $10,000 to another account he owns. That second, contradictory transaction would reach some nodes before the first transaction. In fact, because different transactions reach different nodes at different times, they can't be timestamped.

So, how does the network know which is the "real" transaction? What's to stop the thief from spending the same money twice and ripping you off after you ship your product?

Putting the "Block" in "Blockchain"

The solution is to balance the ledger and then create consensus throughout the entire network. The network does this through the creation of "blocks". A block is a group of transactions. Since transactions can't be timestamped precisely, all transactions within a block are considered to have happened at the same time. Transactions are unconfirmed until they're included in a block. Once a transaction is included in a block, it's recorded within the blockchain.

Each time a block is created, it's tied to the previous block, forming a chain, which is what gives us the term "blockchain". This chain of blocks forms the ledger of all transactions that have ever happened.

Very new blocks can be rewritten in some cases, but once a transaction is six blocks deep, it is permanent and cannot be undone.

Now, back to our freight thief. Even though his intents are malicious, neither of his transactions are more correct than the other. It's perfectly valid for him to transfer his money to another account instead of paying you; as long as only one transaction goes through, you will either have your money, or you can keep your product and sell it to someone else. All that matters is that the ledger balances.

Miners: The Workers Behind the Blockchain

The work of balancing the ledger to create the block is done by people known as "miners". There isn't one correct way to balance the ledger – one possible solution would be to accept the thief's payment to you and reject his other transaction as invalid. Another solution would deem his payment to you as invalid. Combine this with all the instances of possible transactions, and this leaves us with many possible solutions.

In addition to balancing the ledger, the miners must also solve a very difficult and arbitrary math problem – this is known as "solving the block". The only way to solve the math problem is to test possible solutions at random. However, although it's very difficult to find a correct answer, once you have the answer, it's very easy for others to verify if the solution is correct or not.

The first miner to solve the block propagates the solution out to the network, who check to see if it's correct. Once the network agrees on the block, the block is added to the blockchain, and the transactions in that block are confirmed. Then the miners start working on solving the next block, and the process continues.

To motivate miners to do the work of balancing the ledger, the miner who solves the block is given a financial reward (which is where the term "miner" comes from).

Difficult and arbitrary math? It's high school all over again!

So if the math problem is just arbitrary, why do the miners need to solve it instead of just balancing the ledger? It's that useless?

From an accounting perspective, it *is* useless. But it's essential from the perspective of psychology and economics.

At a glance, balancing the ledger for all transactions in a block sounds like a large task. However, compared to the computing power available in the network, it's actually a very easy task – too easy, in fact. This means that multiple miners would solve the block simultaneously – and then the network would have to decide which block to accept.

Say 100 blocks were generated at the same time – which block should be chosen? Each miner wants their own block to be chosen. And since block creation is fast and easy, why should a miner submit the first solution they find? Instead, the miner could be a little more selective about what transactions are included in the block. What's to stop a company from creating blocks that exclude their competitor's transactions? What's to stop our freight thief from manipulating the block creation in order to scam people? And then, while the network is trying to decide among the first 100 possible blocks, other miners could create even more blocks, each trying to throw their hat in the ring, making reaching consensus even more difficult.

Remember: the blockchain is based on a peer network, and no one has more say in voting then anyone else. There's no overarching entity that can just make a decision to speed up the process.

Blockchain is also designed so that it doesn't require goodwill or trust to work. The blockchain is designed to work even when people in the network aren't altruistic or well-intentioned.

Saved by a Make-Work Project

To alleviate these issues, the task of balancing the ledger is made artificially difficult. The problem is so difficult that with all the computing power of all the miners on the network, a block is only generated every ten minutes, on average. Because each miner is just trying random solutions to the math problem, no one knows for sure that they're going to solve the block. Suppose our freight thief could reverse his payment through careful creation of the blocks. The odds that he'll win this block are very low. The odds are much better that his payment to you will just go through, in which case he's lost money. The odds increase with his computing power, but computer powering is expensive, especially when you're competing with the entire network. Essentially, the costs of trying to cheat the system become very, very expensive, which is a major deterrent to fraudulent behavior.

Also, because blocks are solved less frequently, there aren't as many options for the network to choose from, making consensus easier to reach. Sure, miners can still hold out and refuse to accept the block. Instead, they can try to find another solution to the block so that they can win the reward. But remember: with this setup, solving a block is enormously difficult. To win the reward, the miner not only has to have the good luck of solving the block before the other block is chosen, they also need the network to choose their block after the first one has a head start. The odds are against him, so it makes more sense for the miner to get right to work on solving the next block, and hope he finds it first.

So, while this arbitrary math problem appears to be a make-work project, it actually plays a very important role in the functioning of the blockchain. In fact, if the miners buy more powerful computers so they can solve the problem faster, the problem is actually adjusted to be even more difficult. The only constant is that blocks should always take an average of 10 minutes to solve.

Further Reading

This is a very basic explanation of how blockchain works. While we read dozens of sources to arrive at this explanation, the following are the main sources for this ebook, and the best sources for further reading:

How Does the Blockchain Work? By Michele D'Aliessi

Discusses the process described here in greater depth, and touches on topics like security and encryption, and when blocks can be rewritten.

The Proof-of-Work Concept by Daniel Krawisz

A further explanation of the need for the miners to solve an artificially difficult math problem.

Bitcoin Hash Functions Explained by Corin Faife

More detailed information on the miner's math problem.

Disclaimer

The information in this ebook is for informational purposes only; neither TranSolutions Inc nor the author accept responsibility or liability for its content.