Don Tapscott and Alex Tapscott

Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World

Blinkist

These key insights in blinks were written by a team of experts at Blinkist. We screen the world of nonfiction to choose the very best books. Then, we read them deeply and transform them into this concise format that brings you the most inspiring ideas from the text.

Maybe these blinks will inspire you to dig deeper, or maybe they're enough to start you thinking and then on to something new. However you read blinks, we hope they help you become an even brighter you.

What's in it for me? Delve into the new and promising world of blockchain technology.

In 2008, in the wake of the world financial crisis, someone using the name Satoshi Nakamoto found a new way to handle money and other kinds of data. It was a method that soon spread like wildfire among computer scientists, privacy advocates, anarchists, media theorists and banks – anyone who had wrestled with the question of how to establish trust among two parties on the internet.

We don't know who the person behind the name Satoshi Nakamoto is. The name could even hide several people. But this is beside the point. What is important is the new idea that Nakamoto suggested: the Bitcoin and, with it, *blockchain technology*.

These blinks will introduce to you to this technology. You will learn what the blockchain is, how we can use it and why it has the potential to turn the world upside down.

In these blinks, you'll learn

- why banks might soon become redundant;
- why Airbnb and Uber aren't actually part of the sharing economy; and
- which is faster: Sending an anvil to China or sending money through the banking system?

The blockchain is a decentralized database technology that is secure and trustworthy.

Let's say you're looking to buy a house, but the seller insists that no banks or notaries get involved. You'd probably be pretty skeptical about such a seller's trustworthiness.

This is why we've come to rely on middlemen – intermediaries that ensure the transaction is legitimate, allowing both buyer and seller to rest easy.

Banks have long served this purpose by authenticating transactions and keeping track of property titles to confirm who owns what. More recently, businesses such as Uber and Airbnb have begun filling the role of middleman platforms and now vouch for the reliability of a driver or apartment owner.

However, history shows us that middlemen themselves aren't always the most trustworthy.

Banks can go bankrupt and lose your money by making bad deals and companies like Uber can sell customer data without getting consent. And with more and more cases of unwarranted surveillance, even governments can seem untrustworthy – and they're certainly capable of going bankrupt themselves.

So where does the internet fit into all this? Well, until recently, most people would say that the internet lacked the proper security for big transactions involving money or property. But there's a new technology that might change this conception for good.

It's called *blockchain*, and it comes with a protocol that allows buyers and sellers to bypass traditional central authorities like banks.

It does this by making every transaction a transparent process. Everyone using the blockchain has access to, and thus compose the management of, an incorruptible decentralized database.

When a transaction is made, it gets timestamped and added to the database. When it clearly doesn't corrupt the system and is agreed upon by the majority of all parties involved, it gets legitimized.

With this level of transparency and verification protocol, there's no opportunity for hackers or thieves to make changes that will go unnoticed. Plus, the system doesn't allow for changes to old entries.

Since no one entity controls the blockchain, everyone can trust it.

"Whereas most technologies tend to automate workers on the periphery doing menial tasks, blockchains automate away the center."

The blockchain is a tamper-proof technology.

So you might be wondering, why is it called "blockchain"?

First of all, every record, which might contain multiple transactions, is called a *block* on the ever-growing database. And each new block is linked to all the previous ones, not unlike a chain – hence, "blockchain."

This construction of linked blocks is part of what makes the system so secure.

New blocks are created by special nodes called *miners*, which not only contain the new transactions being added, but also a link to the previous block, which in turn contains a link to the previous one and so on down the line.

So when a block gets added, the new miner will broadcast its data to the

network of other nodes in the database, triggering a *consensus algorithm* that will make sure everything is in perfect agreement.

This is how miners can replace traditional middlemen; the algorithms protect the blockchain from any funny business or tampering within the chain.

The *proof-of-work algorithm* is the most popular one for blockchains as it makes it next to impossible for someone to add a block that contains altered information.

It requires miners to make complex mathematical calculations that demand massive amounts of computer resources. Meeting this demand means the additional block is valid because one of the inputs to the calculations is a link to the chain's previous transaction-history, which must match-up perfectly.

It also ensures that, when a new block is added, someone can't roll back the chain, remove an old transaction, create a new block to cover up the wrongdoing *and* make the chain one block bigger.

Pulling that off would require a criminal to create new blocks faster than the combined speed of the entire network, with enough computing power left over to solve the massive math puzzle.

This is next to impossible; the cost of the computing requirements to do something like that would outweigh any benefits that might be gained through the manipulation. In short, the blockchain is quite secure.

The combined processing power of the Bitcoin network is hundreds of times bigger than that of the top 500 supercomputers in the world.

Blockchain makes finances faster, cheaper and more inclusive than traditional banks.

Here's a question that doesn't require a supercomputer to answer: Which would arrive first on a journey from the United States to China, an anvil being sent through the mail or a ten dollar bill being sent by a bank?

Believe it or not, the anvil would get there first. And this is part of the problem with today's financial system. Banks are just unnecessarily complicated and slow; in fact, many of them are still using mainframe computers from the 1970s!

Since we do a lot of online banking already, you'd think money would be able to travel as fast as an email, but the system is bogged down by a ridiculously large number of middlemen.

These middlemen not only slow things down; they make things more expensive in an effort to boost their own bank accounts.

Middlemen include credit card companies, investment banks, stock exchanges, wire services like Western Union, accounting and security firms and so on.

But none of this is necessary for a currency that uses blockchain, which is how *Bitcoin* operates.

Bitcoins take around 10 minutes to be transferred from one account to another, which is all the time it takes to add a new block to the chain. So there's no need to pass through five different intermediaries, which is what happens when you use a credit card to pay for a cup of coffee at Starbucks.

The complex and expensive way banks operate also makes them essentially

useless for the poorest populations.

Due to the complicated banking system, payments under 20 cents aren't profitable for banks, even though 2.2 billion people live on less than a dollar a day. It's no wonder that 2.5 billion people don't have a bank account.

Blockchain, on the other hand, could make for a great alternative since it handles small payments and provides many of a bank's services at no cost.

Anyone with an internet connection can use blockchain and join the global economy.

Blockchain technology can also be used to reduce corruption and improve contracts.

The blockchain that manages the Bitcoin currency is now the longest blockchain in existence and is overseeing $16 billion dollars worth of currency.

But one of the great things about blockchain is that it can do much more than deal with money.

Blocks can also keep track of land ownership or intellectual property, such as the ownership of songs or other copyrighted material.

And with its public transparency, the system offers a way to reduce corruption, which could be useful in countries where bribery and fraud continue to be a systemic problem in government.

Property law is especially in need of reform. It's estimated that 70 percent of the world's population has no enforceable claim to the land they own.

But this may soon change. There is already a unique blockchain called *Ethereum* that specializes in dealing with contractual agreements.

Ethereum's blocks store small mini-programs, called *smart contracts*, which are programmed to react to certain transactions in the blockchain.

Such a transaction will automatically prompt the parties involved to enforce contractual agreements. So, if someone is supposed to get paid a certain amount when a property is sold, a payment might be automatically delivered to that person in Bitcoins.

And since this contract is already part of a blockchain's history, it cannot be altered, canceled or otherwise avoided.

This is great for other kinds of agreements as well, especially for small payouts that can otherwise be a hassle to maintain.

For example, when a large number of individuals pool their resources into an investment, everyone can automatically be paid out, no matter how small their contribution.

Often this is seen as a hassle since the cost of keeping track of small investments often outweighs the payout – but, without the need for a middleman, blockchain technology can make it worthwhile.

This concept has already resulted in *The DAO,* an investment fund managed entirely by blockchain smart contracts, which has so far raised $168 million from 10,000 different, and anonymous, contributors.

Depending on the requirements, blockchains can enforce transparency or privacy.

Over the course of the past decade or so, the internet and digital technology have been at the center of the debate over privacy rights and how safe our personal data is.

This is another reason why blockchain could end up being so useful for everyone: its transactions allow for both privacy and transparency, depending on what is called for.

One way blockchain users can choose their level of privacy is through the use of cryptographic keys, which can also act as a signature on a transaction.

While the average citizen could protect their privacy by always using a new signature, NGOs, governments and other public organizations could always use the

same identifiable signature. This way, anyone could easily track their spending.

This could be of great service to the institutions that have struggled to regain public trust.

For instance, after a massive earthquake struck Haiti in 2016, people around the world donated around $500 million to the Red Cross. Yet a large portion of that money simply vanished. Had it been donated through blockchain, every single dollar could have been easily tracked and accounted for.

The same could happen if government departments began using blockchain, and taxpayers would get a much better idea of how their money is being spent.

Along with this new level of transparency would come a similar level of privacy.

Blockchain allows you to manage your own presence through specially designed

smart contracts, meaning you can pick and choose which data is private and which data is available to those whom you choose to provide access.

So if you get pulled over by a traffic cop, you could grant the police temporary access to your personal information, which they could then bring up in their copy of the database to see that you have a clean criminal record.

If you wanted to make some money, you could even rent out valuable bits of personal data to an advertising corporation. Or if you're feeling more charitable, you could donate it to medical researchers, all while keeping your identity under lock and key.

The flexibility of blockchain could lead to an increase in small businesses and new ways of generating revenue.

Has the thought of mountains of paperwork prevented you from following through on a great business idea? Well, if you had had access to blockchain technology at the time, things might have turned out differently.

Blockchains and smart contracts can make it a lot easier to start and operate your own company.

Many steps, including raising capital, making payments, protecting assets and allowing real-time audits can all be handled through blockchains. And the ease with which this can be done, along with the security that comes with it, may encourage many entrepreneurs to enter the market – especially in areas that are plagued by corruption.

We could also see a rise in more pay-per-use businesses.

Previously, charging individuals a tiny fee wasn't a practical business model. But since this is possible through smart contracts and micropayments, media companies could start doing things like charging viewers for every minute of content, or even every second!

What's better for customers, though, is that blockchain allows for companies to build a decentralized method of distribution that will make it faster and more secure to share their services.

You may have heard companies such as Airbnb and Uber call themselves part of a new "sharing economy," but these companies don't really share; they aggregate the resources of others. And this allows them to reap the profits while claiming ownership of customer data.

Through a blockchain, similar yet cheaper, faster and more secure platforms could be built that wouldn't require a central authority.

In fact, a great many things could become securely shareable through a blockchain, such as the processing power of your smartphone, the excess storage on your computer or even the electricity created by a solar panel.

This technology has the potential to engage billions of more people in the global economy.

Micropayments could finally end spam: if everyone had to pay 0.001 cent per email, spam would instantly become unprofitable.

Blockchain use poses new challenges, but solutions are in sight.

At this point, you might be wondering whether blockchain is perhaps too good to be true.

Indeed, there are challenges that need to be overcome, but the solutions to those problems are also in sight.

One of the big challenges is getting the general public to understand how it works, because, without everyone's participation, it's full potential will never be met.

Governments are also notoriously slow in understanding the implications of new technology, which means that blockchain could be poorly regulated. Or worse, the government could decide to use it against the public by creating an unprecedented surveillance state.

But this is why it's even more important that the public be educated. This, of course, is no small undertaking since it requires a certain level of computer savvy and a complete change in the way we approach routine functions.

Another concern is the amount of energy it takes to maintain blockchains.

Currently, the massive bitcoin blockchain costs around $100 million in electricity every year.

However, it should be noted that every currency costs money to maintain or obtain, and rare metals like gold actually derive their value from how costly it is to extract them from the earth. And let's not forget that our current financial system has its own gigantic costs, from the expensive banking skyscrapers, to the maintenance of underground vaults and armored trucks.

Finally, there's the question of jobs that would become largely automated by blockchain technology.

Indeed, many jobs could be replaced by computer code as blockchain's shared financial ledger could automate the work of the army of employees working in the accounting sector.

However, by reducing corruption and setting strict conditions for good governmental services, it could also create fertile ground for many more businesses to operate and create jobs.

So it's true that there are a few stumbling blocks on the way to a blockchain economy, but these are challenges to be overcome, not permanent barriers to a better future.

Final summary

The key message in this book:

Blockchain is a technology that enables the direct transaction of rights or assets between two parties and eliminates the need for superfluous third parties and intermediaries. This has far-reaching implications for commerce as blockchains promise to bring billions of poor people into world commerce. It also has the potential to build a true sharing economy, where value is created and distributed in a fair manner directly from those who own the resources. Furthermore, it can do all this in an open and transparent fashion, making it possible to greatly reduce corruption and fraud.

Actionable advice

Get some Bitcoins and play around.

When the internet emerged, one of the best ways to understand its usefulness was to set up an email account and send out your first message. Similarly, the best way to understand and prepare for the blockchain revolution is to find out how you can earn and spend your first Bitcoins.

Got feedback?

We'd sure love to hear what you think about our content! Just drop an email to remember@blinkist.com with the title of this book as the subject line and share your thoughts!

Suggested further reading: *Wikinomics* by Don Tapscott & Anthony D. Williams

Wikinomics shows how Wikipedia-like mass collaboration of individuals is revolutionizing society and business, and why this is actually good for companies and the public.

Nice work! You're all done with this one.

We publish new books every week at blinkist.com.
Come and see – there's so much more to learn.

Inspired to read the full book?

Get it here.