

Stephen P. Williams

Blockchain: The Next Everything

Made by 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? Embrace the radical potential of blockchain technology.

These days, everyone from finance gurus to conceptual artists is talking about blockchain. Initially devised as a platform for Bitcoin, blockchain went unnoticed for years until technologists realized that its potential far exceeds the realm of cryptocurrencies. Now, the hype around this new technology has amounted to some philosophers calling it the next enlightenment.

But what exactly is blockchain? Simply put, blockchain is a digital ledger software that is unhackable and unchangeable. Its distributed technology offers an unprecedented amount of transparency and accountability that poses a threat to traditional intermediary authorities such as banks, businesses, and even governments.

If that sounds confusing, don't worry. In this these blinks, you'll learn how the technology works, how it's being applied to business, finance, climate change, and the arts, and what it could mean for the future of society.

In these blinks, you'll learn

- why blockchains become more secure as more people join them;
- how blockchain could lead to a fleet of autonomous self-driving cars; and
- why blockchain is giving people hope for a brighter future.

The blockchain is a new, revolutionary kind of ledger.

If you look up the definition of blockchain, you'll learn that it's a digital *ledger*, or book in which accounts or monetary transactions are recorded.

If that sounds boring, look at it this way: ledgers are the foundations of civilization. Without them, we wouldn't have been able to build cities or efficient markets. They are the means by which we do everything from keeping track of our finances and demonstrating ownership of a house to verifying our status as citizens.

For hundreds of years, the world economy has been based on a ledger system called double-entry bookkeeping. These ledgers have two columns for information: debit and credit. As long as the credit and the debit for a transaction

match in both the buyer's and the seller's books, that transaction is error-free.

In order to establish trust in the system and ensure that a transaction is true and accurate, double-entry accounting requires middlemen. Brokers, bankers or other intermediaries get a fee to certify the legitimacy of transactions.

However, history has shown us that this system isn't always reliable. In the aftermath of the 2008 financial crisis, it was revealed that many large corporations, like Enron and Lehman Brothers, had effectively been keeping extra sets of books, which they used to conceal the true nature of their financial operations. For years, these companies were able to manipulate the system to launder vast amounts of money.

Ever since the dawn of the Internet, many have hoped that it would bring an end to these kinds of transgressions. But until now, the Internet's susceptibility to

hackers has posed security issues when it comes to large financial transactions.

However, the blockchain might change all that. The blockchain was originally created as a platform for the cryptocurrency Bitcoin. By tracking every purchase or sale, the blockchain ensures that a digital coin can never be spent twice. Transactions are all online for everyone to see; all you need to join is an Internet connection.

In addition to credit and debit, the blockchain has a third column in its digital ledger: verification. This eliminates the need for intermediaries. Instead, trust is built into the very system.

Blockchain technology is already being developed in ways which might revolutionize everything from the way that artists can certify the provenance on their work to the way we value currencies such as the U.S. dollar. It

could even eliminate the possibility of tampering or lost ballots when it comes to voting.

But how can we be sure that this technology is so trustworthy? That's because unlike other ledgers, the blockchain is unhackable and unalterable. In the next blink, we'll take a closer look at how it actually works.

Blockchain technology is unhackable and unchangeable.

Picture yourself gazing up into the sky on a clear night. Beams of light link each star to the next, forming a celestial network. That's what a blockchain looks like: a network of phones, computers and other devices, forming a supercomputer that runs the blockchain.

The blockchain system is secured through the construction of linked blocks that represent information. Say you want to record the number of rubber trees in the Amazon rainforest. The data would be entered into a digital collection called a "block." After a block reaches its capacity it's ready to be added to the chain of linked blocks, or the "blockchain."

However, before it can be added, the new block must be approved by every *node* – meaning every device linked to

the chain – in a process known as the *protocol*. That’s why blockchain is called a distributed technology: everyone on the chain has equal decision-making power.

There are various protocol methods, but the most common one is called “proof of work.” With proof of work, every new block comes with a complex mathematical problem, which must be solved before the block can be added to the chain. This is done by special nodes called *miners* that compete to solve the problem in order to win Bitcoins. Thanks to proof of work, adding blocks to the chain requires substantial computational resources, which helps prevent malicious actors from manipulating the blockchain.

Part of solving the problem generates a cryptographic *hash*, or a code made up of a long string of numbers and letters. In addition to its own hash, each block contains a timestamp as well as the hash

from the previous block, aligning it with the rest of the blockchain.

You might be wondering why it's possible to mine Bitcoins, but not to hack into the blockchain and change a block's information – to say that someone else's Bitcoin actually belongs to you, for instance.

That's because changing a single block's information would render the entire chain's hashes out of sync and automatically signal a break-in. Not only would hackers have to change the hashes for every block in the chain, but they would also have to do this for every single node, since the blockchain is copied onto every node's device. The computing power required to achieve such a task increases exponentially with every node added to the chain.

In other words, the more nodes there are on a chain, the stronger the chain becomes.

In theory and practice, distributed applications built on the blockchain have radical potential.

Unless you're a computer programmer, you'll probably never come across a blockchain code. What you will see and interact with is what blockchain enables - namely, distributed applications, or "dapps."

The potential for these dapps is endless.

One example is *smart contracts*. A smart contract is essentially an automated contract on a blockchain with terms agreed upon by both parties. Once the terms of the contract are carried out, an algorithm delivers the payment in cryptocurrency and documents the transaction on the blockchain. Smart contracts thus automate bureaucracy, eliminating the need for centralized authorities to verify the transaction.

Many dapps already use smart contracts. On Ethereum, a public blockchain that supports smart contracts and uses a cryptocurrency called Ether, you can find dapps that use smart contracts to do things like record the origin of a work of art or time-stamp an idea you have for a film, creating an official document of your intellectual property.

Other possibilities for smart contracts require only that we use our imagination.

Currently, Uber uses a centralized app to connect drivers with customers and ensure payment. A blockchain dapp equivalent could use smart contracts to enable taxis to connect to customers directly, and bypass any centralized intermediary.

Let's take that one step further. Say that at some point in the near future you buy a self-driving car. Smart contracts could allow you to set the car up to run itself as a taxi 24/7.

If the car is low on gas, for instance, a smart contract between you and the car would be activated, and the car would drive itself to get its tank filled. Similarly, if the car has a flat tire, another smart contract would kick in and the car would drive itself to get the tire fixed.

Eventually, your car will have earned enough money to purchase another self-driving car. The second car may then earn enough money to purchase another car all by itself. This process would continue until there was an entire fleet of autonomous taxis functioning without owners.

Such a business model is called a DAO, or distributed autonomous organization. We can't be sure right now whether such a model could be successfully realized. But the mere idea of it goes to show how blockchain offers radical potential.

Distributed technology signals a paradigm shift away from centralized hierarchies.

The hype around blockchain might sound familiar to anyone who remembers the utopian ideas surrounding the Internet in the 1990s. Although the Internet did make people more connected, it failed to bring about the egalitarian society that many had hoped for, as corporations like Facebook were quick to monopolize the network for their own growth. However, with blockchain, things may be different.

That's because distributed systems intrinsically shift accessibility and power to the masses.

Think of investing. For most of history, it has been exclusive to the elite. Banking fees, credit histories, and limited access have undermined the ability of the lower classes to participate in this lucrative

activity. But anyone can join a blockchain like Bitcoin or Ethereum, meaning anyone can invest with them.

Some even envision that cryptocurrencies will overtake the central banking system. That's something that many people have dismissed, but since the US dollar no longer stands for a tangible asset such as gold, cryptocurrencies are really no less valid than dollars, or in fact any other currency. As more people start valuing cryptocurrencies, the vision of a future free of big banks might not be such a stretch after all.

For the time being, the United Nations, the World Economic Forum, and the Rockefeller Foundation are all already developing ways for blockchain technology to empower disadvantaged farmers, disenfranchised voters, and underprivileged people without banking access.

Blockchain technology itself, of course, has no moral agenda. But the distributed system that it represents encourages a rethinking of hierarchies, creating a more equitable version of capitalism.

In the same way that smart contracts could eliminate the need for Uber, blockchain dapps have the potential to enable other kinds of trading, like that around rented accommodation. Instead of paying fees to Airbnb as a central arbitrator, as the owner of a property you could set up a smart contract with a renter that would run the venture for you. Depending on your agreement, if guests overstayed their visit, the smart contract would either lock them out of the house or automatically charge them for a longer stay. This peer-to-peer system would mean a true sharing economy.

*"With blockchains, we are
becoming a hive."*

Blockchains champion an unprecedented degree of transparency while enabling privacy.

In one episode of TV series *Portlandia*, the protagonists Peter and Nance interrogate their waiter about the life of the chicken they are considering ordering. Asking questions such as whether the chicken had any friends, the show pokes fun at the rising demand for transparency about where our products are coming from.

In the future, you might be able to check your turkey's journey from farm to table on your phone. Cargill, the company that owns the brand The Honeysuckle White, has already tested a blockchain dapp that lets people track exactly where their turkeys on Thanksgiving came from.

This is not the only way in which blockchain is paving a way for a future of unprecedented transparency.

Fura, Everledger and DeBeers are three companies devising blockchains to avert blood-diamond trafficking. With the technology, once the certification for a conflict-free diamond is entered onto the blockchain, it follows that diamond all the way up the supply chain, as its location is updated at each step.

Not only would this mean that buyers could recognise and refuse blood diamonds at the point of purchase, it would also enable diamond miners to track where their stones end up, and even give them a chance to communicate with people at the top of the supply chain. In that system, the diamond miner would be just as important as the buyer at the top of the supply chain, and would have a real voice to influence how the system is run.

At the same time as making transparency possible, blockchains also enable unparalleled privacy.

Intimate is a dapp that enables pornography vendors and sex workers to offer their services using cryptocurrency and anonymous addresses. The dapp enables users to keep their identities private while making their reputation recognizable across the platform, making conditions for all participants safer.

Up until this point, we've been discussing public blockchains. But some blockchains are private, invitation-only platforms.

This kind of maximum privacy is essential for businesses, such as health care operators, that deal with confidential information, but it's also being embraced by businesses in general. Computer behemoth IBM has already engaged private blockchains for major business operations using the Hyperledger Fabric framework, and other corporations are sure to follow.

Still, the fact that corporations might opt out of transparency won't affect

blockchain's utopian promise; the public chains will remain under the control of the public.

Environmental friendly solutions for blockchain are underway.

As we've seen, blockchain has the potential to affect issues ranging from farming to investment opportunities. But here's the catch: as of yet, blockchain networks require an extortionate amount of energy.

This is especially true for the Bitcoin proof-of-work protocol. When Bitcoin was first released, you could mine coins from your desktop computer. Today, there is so much competition on the Bitcoin blockchain that it requires an assembly of computers drawing large amounts of energy. The business is so lucrative that professional bitcoin mining farms have been set up around the world.

All this means that on some days the bitcoin network requires as much energy as the entire country of Denmark.

That being said, for most blockchain applications, proof of work isn't the most efficient way of authenticating new blocks for the blockchain. One example is the Ethereum blockchain. It has been experimenting with a "proof of stake" protocol, which does without mining entirely. Rather, nodes called *validators* place a stake or bet that they will be given the next block to validate. If they do catch the next block, they gain a financial reward. The hope is that such alternatives will reduce blockchain energy consumption levels as well as make transactions faster.

Looking at the problem from another angle, there are many ways in which blockchain technology could become a tool in the quest for climate change solutions.

One environmental application for blockchain is in the carbon-trading market. By turning carbon emissions into

a tradable good, carbon-trading markets provide a financial incentive to offset air pollution. Beijing-based Energy Blockchain Lab, working with IBM, has already used the open-source Hyperledger blockchain to develop a new, more efficient platform for carbon asset trading in China.

Another green use of blockchains could be the use of a reliable and transparent ledger to track greenhouse gas emissions. This would be essential to monitoring the progress made by nations pledged to the carbon reduction targets of the 2016 Paris Agreement.

Blockchain could also be used to track endangered species, make the ultimate destination of donated funds more transparent, and certify land ownership to counter deforestation.

The possibilities are endless. It's up to us to embrace this new technology and continue to think of creative ways in

which blockchain could make the world a better place.

Final summary

The key message in these blinks:

Blockchain is so much more than Bitcoin or any other cryptocurrency. Computer scientists are pushing this unhackable, distributed digital ledger technology to do everything from revolutionizing business to tackling climate change. While the actual uses of the technology will depend on the groups and individuals who use it, it intrinsically encourages an unprecedented degree of transparency, as well as challenging the inequalities inherent in traditional hierarchical systems.

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!

What to read next: *Digital Gold*, by Nathaniel Popper

As you've just learned, blockchain was a by-product of the invention of Bitcoin. But there's more to the story of that cryptocurrency than the elusive engineer who developed it. Until recently, however, the details of Bitcoin's sudden rise have been largely confined to obscure forums on the internet.

In *Digital Gold*, Nathaniel Popper tells the untold history of Bitcoin. While its value skyrocketed from zero to \$1 billion, Bitcoin's early days were marked by difficulties. To learn how cypherpunks, gamblers, visionaries, nerds, and investors were behind the rise of the world's leading cryptocurrency, we highly recommend the blinks to *Digital Gold*.

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.](#)

Copyright © 2014 by Blinks Labs GmbH.
All rights reserved.