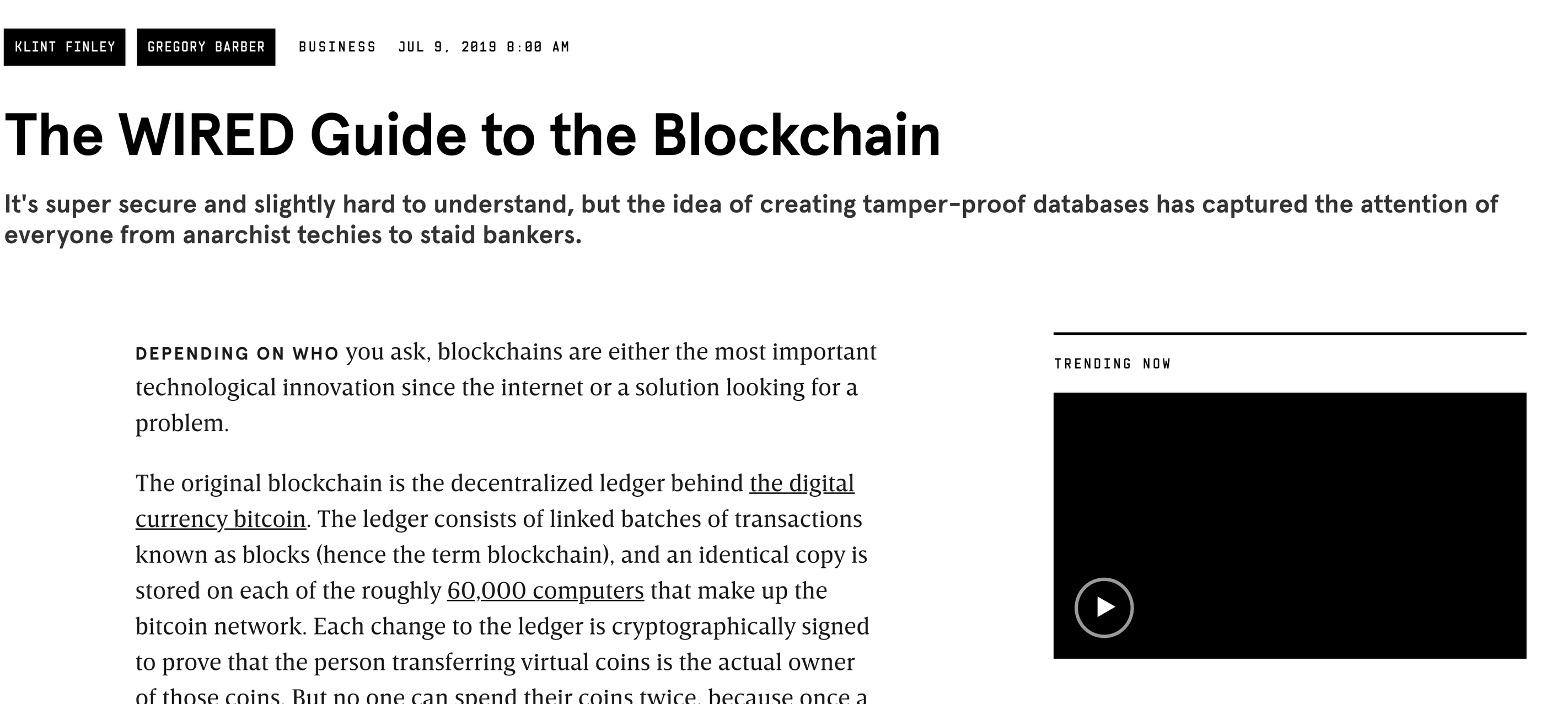

ILLUSTRATIONS: RADIO

KLINT FINLEY GREGORY BARBER

BUSINESS JUL 9, 2019 8:00 AM

The WIRED Guide to the Blockchain

It's super secure and slightly hard to understand, but the idea of creating tamper-proof databases has captured the attention of everyone from anarchist techies to staid bankers.

DEPENDING ON WHO you ask, blockchains are either the most important technological innovation since the internet or a solution looking for a problem.

The original blockchain is the decentralized ledger behind the digital currency bitcoin. The ledger consists of linked batches of transactions known as blocks (hence the term blockchain), and an identical copy is stored on each of the roughly 60,000 computers that make up the bitcoin network. Each change to the ledger is cryptographically signed to prove that the person transferring virtual coins is the actual owner of those coins. But no one can spend their coins twice, because once a transaction is recorded in the ledger, every node in the network will know about it.

Who paved the way for blockchains?

DigiCash (1989)

DigiCash was founded by David Chaum to create a digital-currency system that enabled users to make untraceable, anonymous transactions. It was perhaps too early for its time. It went bankrupt in 1998, just as ecommerce was finally taking off.

E-Gold (1996)

E-gold was a digital currency backed by real gold. The company was plagued by legal troubles, and its founder Douglas Jackson eventually pled guilty to operating an illegal money-transfer service and conspiracy to commit money laundering.

B-Money and Bit-Gold (1998)

Cryptographers Wei Dai (B-money) and Nick Szabo (Bit-gold) each proposed separate but similar decentralized currency systems with a limited supply of digital money issued to people who devoted computing resources.

Ripple Pay (2004)

Now a cryptocurrency, Ripple started out as a system for exchanging digital IOUs between trusted parties.

Reusable Proofs of Work (RPOW) (2004)

RPOW was a prototype of a system for issuing tokens that could be traded with others in exchange for computing intensive work. It was inspired in part by Bit-gold and created by bitcoin's second user, Hal Finney.

The idea is to both keep track of how each unit of the virtual currency is spent and prevent unauthorized changes to the ledger. The upshot: No bitcoin user has to trust anyone else, because no one can cheat the system.

Other digital currencies have imitated this basic idea, often trying to solve perceived problems with bitcoin by building new cryptocurrencies on new blockchains. But advocates have seized on the idea of a decentralized, cryptographically secure database for uses beyond currency. Its biggest boosters believe blockchains can not only replace central banks but usher in a new era of online services that would be impossible to censor. These new-age apps, advocates say, would be more answerable to users and outside the control of internet giants like Google and Facebook.

Unless, of course, Facebook runs away with the idea itself. In June, Facebook announced Libra, a new blockchain that will support a digital currency. Unlike the thousands of anybodys who run Bitcoin nodes, it will be controlled by an association comprised of just 100 companies and NGOs. Libra is certainly a challenge to central banks, not least because it's a privately controlled monetary system that will span the globe. But replacing government with corporations is not exactly the revolution that enthusiasts imagined blockchain would bring. So far, the crypto community is divided on whether Libra is a good thing. Some see Facebook's effort as a corruption of a technology designed to ensure that you don't need to trust your fellow users---or any central authority. Others are celebrating it as the moment that blockchain goes mainstream.

Other so-called "private" blockchains, like Libra, are growing in popularity. Big financial services companies, including JP Morgan and the Depository Trust & Clearing Corporation, are experimenting with blockchains and blockchain-like technologies to improve the efficiency of trading stocks and other assets. Traders buy and sell stocks rapidly using current technology, of course, but the behind-the-scenes process of transferring ownership of those assets can take days. Some technologists believe blockchains could help with that.

Blockchains also have potential applications in the seemingly boring world of corporate compliance. After all, storing records in an immutable ledger is a pretty good way to assure auditors that those records haven't been tampered with. This might be good for more than just catching embezzlers or tax cheats. Walmart, for example, is using an IBM-developed blockchain to track its supply chain, which could help it trace the source of food contaminants. Many other experiments have emerged: Voting on the blockchain. Land records. Used cars. Real estate. Streaming content. Hence the phrase "xxx on the blockchain" as a catch-all for the enduring hype cycle. The question is, if one organization (say, Walmart) has control of the data, did it really need blockchain at all?

It's too early to say which experiments will stick. But the idea of creating tamper-proof databases has captured the attention of everyone from anarchist techies to staid bankers.

TRENDING NOW

Most Popular

SECURITY
Apple's Killing the Password. Here's Everything You Need to Know
MATT BURGESS

GEAR
Octopus Energy Is the Answer to a Broken, Inefficient Market
SIMON HILL

GEAR
Everything Apple Announced: iPhone 14, Apple Watch Ultra, and More
GEAR TEAM

GEAR
Apple's New 'Ultra' Watch Goes Toe-to-Toe With Garmin
ADRIENNE SO

The First Blockchain

The original bitcoin software was released to the public in January 2009. It was open source software, meaning anyone could examine the code and reuse it. And many have. At first, blockchain enthusiasts sought to simply improve on bitcoin. Litecoin, another virtual currency based on the bitcoin software, seeks to offer faster transactions.

One of the first projects to repurpose the bitcoin code to use it for more than currency was Namecoin, a system for registering ".bit" domain names. The traditional domain-name management system---the one that helps your computer find our website when you type *wired.com*---depends on a central database, essentially an address book for the internet. Internet-freedom activists have long worried that this traditional approach makes censorship too easy, because governments can seize a domain name by forcing the company responsible for registering it to change the central database. The US government has done this several times to shut sites accused of violating gambling or intellectual-property laws.

Namecoin tries to solve this problem by storing .bit domain registrations in a blockchain, which theoretically makes it impossible for anyone without the encryption key to change the registration information. To seize a .bit domain name, a government would have to find the person responsible for the site and force them to hand over the key.

What's an "ICO"?

Ethereum and other blockchain-based projects have raised funds through a controversial practice called an "initial coin offering," or ICO: The creators of new digital currencies sell a certain amount of the currency, usually before they've finished the software and technology that underpins it. The idea is that investors can get in early while giving developers the funds to finish the tech. The catch is that these offerings have traditionally operated outside the regulatory framework meant to protect investors. Since the first tidal wave of ICOs in 2017, the SEC has said that virtually all violated securities law. Newer companies are increasingly looking for regulatory loopholes: a more common practice these days to raise money the traditional way (through VCs) and "airdrop" coins to users for free.

In 2013, a startup called Ethereum published a paper outlining an idea that promised to make it easier for coders to create their own blockchain-based software without having to start from scratch, without relying on the original bitcoin software. In 2015 the company released its platform for building "smart contracts," software applications that can enforce an agreement without human intervention. For example, you could create a smart contract to bet on tomorrow's weather. You and your gambling partner would upload the contract to the Ethereum network and then send a little digital currency, which the software would essentially hold in escrow. The next day, the software would check the weather and then send the winner their earnings. A number of "prediction markets" have been built on the platform, enabling people to bet on more interesting outcomes, such as which political party will win an election.

So long as the software is written correctly, there's no need to trust anyone in these transactions. But that turns out to be a big catch. In 2016, a hacker made off with about $50 million worth of Ethereum's custom currency intended for a democratized investment scheme where investors would pool their money and vote on how to invest it. A coding error allowed a still unknown person to make off with the virtual cash. Lesson: It's hard to remove humans from transactions, with or without a blockchain.

Blockchains had other limitations, too. The security protocols that allow people to trust blockchain systems without a central overseer are notoriously slow (not to mention energy-intensive). Ethereum gave developers the tools to write applications, but the tech couldn't yet handle the fancy graphics of your new decentralized computer game or the volume of users needed to make your open social network useful. Dozens of competitors have since hatched out of academic labs and start-ups, each purporting to have a novel technical solutions. Ethereum is working on scaling up its technology too. But so far, no clear winner has broken through.

That sluggishness also gave an opening to corporate blockchains. Even as cryptography geeks plotted to use blockchains to topple, or at least bypass, big business, the big guys began their own experiments with blockchains. Many corporate experiments involve "private" blockchains that run on servers within a single company and selected partners. In contrast, anyone can run bitcoin or Ethereum software on their computer and view all of the transactions recorded on the networks' respective blockchains. But big companies prefer to keep their data in the hands of a few employees, partners, and regulators. Private blockchains are also substantially faster because they don't require the intensive security protocols used by Bitcoin and Ethereum. Tech firms like IBM and Intel offer private blockchains to companies interested in things like supply chain tracking.

Recently, there's also been renewed interest in using private blockchains to fulfill its initial use case: buying things. While the dream of using Bitcoin as a medium of exchange has largely died out, due to high transaction costs and extreme volatility, some have been interested in using private blockchains to support "stablecoins"---cryptocurrencies pegged to real-world assets. JP Morgan recently announced Quorum, its private blockchain, would start supporting such a coin. And then, in June, Facebook announced Libra.

Most Popular

SECURITY
Apple's Killing the Password. Here's Everything You Need to Know
MATT BURGESS

GEAR
Octopus Energy Is the Answer to a Broken, Inefficient Market
SIMON HILL

GEAR
Everything Apple Announced: iPhone 14, Apple Watch Ultra, and More
GEAR TEAM

GEAR
Apple's New 'Ultra' Watch Goes Toe-to-Toe With Garmin
ADRIENNE SO

The Future of Blockchain

Despite the blockchain hype---and many experiments---there's still no "killer app" for the technology beyond speculation and (maybe) payments. Blockchain proponents admit that it could take a while for the technology to catch on. After all, the internet's foundational technologies were created in the 1960s, but it took decades for the internet to become ubiquitous.

That said, projects like Facebook's Libra, which is supposed to launch in 2020, indicate the technology is here to stay, but perhaps not in the form its early champions imagined. Libra is designed to enable users to make payments, with a "stablecoin" that will be backed by a number of real-world assets. The idea is to initially support things like cross-border payments and in-app purchases. But it could also be the starting point for building out all sorts of blockchain-based applications. For example, Facebook says it's interested in exploring things like digital identity tied to the Libra blockchain. At some point, you might use that identity to log in to apps, open bank accounts, apply for jobs, or prove that your emails or social-media messages are really from you.

Those services could also be built on one of the original "public" blockchains, which continue to evolve. Ethereum is currently trying to move from the slow, energy-intensive security scheme it has historically been to a sleeker approach that could make the platform more useful. Bitcoin has the Lightning Network, an experimental technology that enables cheaper payments by cutting down on some of the intensive computations. Even Facebook has promised to begin moving Libra toward a truly decentralized model within the next five years, pending technological breakthroughs.

Advocates are particularly excited about the possibility of building other financial services directly on the blockchain, an area known as "decentralized finance," or DeFi. Smart contracts could be used to issue peer-to-peer loans, for example, without an overseeing authority, or even handle more complicated applications like insurance. Some believe blockchains can also help automate many tasks now handled by lawyers or other professionals. For example, your will might be stored in a blockchain. Or perhaps your will could be a smart contract that will automatically dole out your money to your heirs. Or maybe blockchains will replace notaries.

Bitcoin proved that it's possible to build an online service that operates outside the control of any one company or organization. The task for blockchain advocates now is proving that that's actually a good thing.

Learn More

- **The Ambitious Plan Behind Facebook's Cryptocurrency, Libra**
  Facebook has designed a blockchain and cryptocurrency that it won't fully control, but that will uniquely benefit Facebook.
- **New to Blockchain: Turning In-Game Virtual Goods into Assets**
  Companies like Forte and Animoca want to use blockchain technology to allow players to trade skins and other in-app purchases.
- **I Sold My Data for Crypto. Here's How Much I Made**
  How I became my own data broker on the blockchain—and sold my digital soul in the process.
- **The Decentralized Internet Is Here, With Some Glitches**
  Blockchain-based applications aren't vaporware: you can use them today. But they're often buggy, counter-intuitive, and risky. Hey, early adoption always comes with a cost.
- **A $50 Million Hack Just Showed That the DAO Was All Too Human**
  The DAO heist didn't just show how human error can undermine automatic systems. The schism it caused in the Ethereum community shows how hard it is to remove messy human politics from software.
- **The Dark Web's Favorite Currency Is Less Untraceable Than It Seems**
  Bitcoin is encrypted, but that doesn't mean it's anonymous. Monero is one of several blockchain-based currencies trying to build a more private alternative, but don't count on being totally anonymous. Yet.
- **Why Wall Street Is Embracing the Blockchain—Its Biggest Threat**
  It may seem weird that financial institutions are experimenting with blockchain applications when part of the idea of blockchains is to make these companies obsolete. But it turns out that blockchains---or something like them---could make life easier for Wall Street.
- **An AI Hedge Fund Created a New Currency to Make Wall Street Work Like Open Source**
  Traditionally, a hedge fund's trading methods are a closely guarded secret. But the hedge fund Numerai is using a new cryptocurrency to encourage data scientists to work together to build algorithms that make the fund more valuable.

This guide was last updated on July 7, 2019.

Enjoyed this deep dive? Check out more WIRED Guides.

Klint Finley is a contributing writer for WIRED covering tech policy, software development, cloud computing, and more.
CONTRIBUTOR

Gregory Barber is a staff writer at WIRED covering energy and the environment. He graduated from Columbia University with a bachelor's degree in computer science and English literature and now lives in San Francisco.
STAFF WRITER

TOPICS WIRED GUIDE BLOCKCHAIN

MORE FROM WIRED

Crypto and the US Government Are Headed for a Decisive Showdown
A crop of lawsuits could finally settle the question of whether most digital assets are illegal securities offerings.
GILAD EDELMAN

The Future of the Web Is Marketing Copy Generated by Algorithms
The killer app for GPT-3 could help marketers lure clicks and game Google rankings.
TOM SIMONITE

Meet the Lobbyist Next Door
What do a Real Housewife, an Olympic athlete, and a doula have in common? They're all being paid by an ad-tech startup as influencers—peddling not products but ideologies.
BENJAMIN WOFFORD

Data Centers Are Facing a Climate Crisis
Companies are racing to cool down their servers as energy prices and temperatures soar. And the worst is yet to come.
CHRIS STOKEL-WALKER

Volodymyr Zelensky on War, Technology, and the Future of Ukraine
In a one-on-one interview with WIRED, the embattled president expresses clarity amidst the chaos.
GEOFFREY CAIN

The iRobot Deal Would Give Amazon Maps Inside Millions of Homes
Why is the Roomba company worth $1.7 billion to Amazon? It's not the dust, it's the data.
KHARI JOHNSON

The Speedy Downfall of Rapid Delivery Startups
Companies that promise groceries delivered in 15 minutes surged during the pandemic—but are now in retreat.
ARIELLE PARDES

Big Takeaways From the FBI's Mar-a-Lago Raid
The fact that a search of Donald Trump's Florida home was even necessary says a lot.
GARRETT M. GRAFF