THE HUNT FOR DARK MATTER AXIONS
PAGE 46

WHY LONELINESS IS SO TOXIC
PAGE 60

HOW SNAKES CAME TO SLITHER
PAGE 66

SCIENTIFIC AMERICAN

THE FUTURE OF MONEY

Cryptocurrencies cut banks and governments out of financial networks

Will they fix a flawed system—or could they make it worse?

PLUS

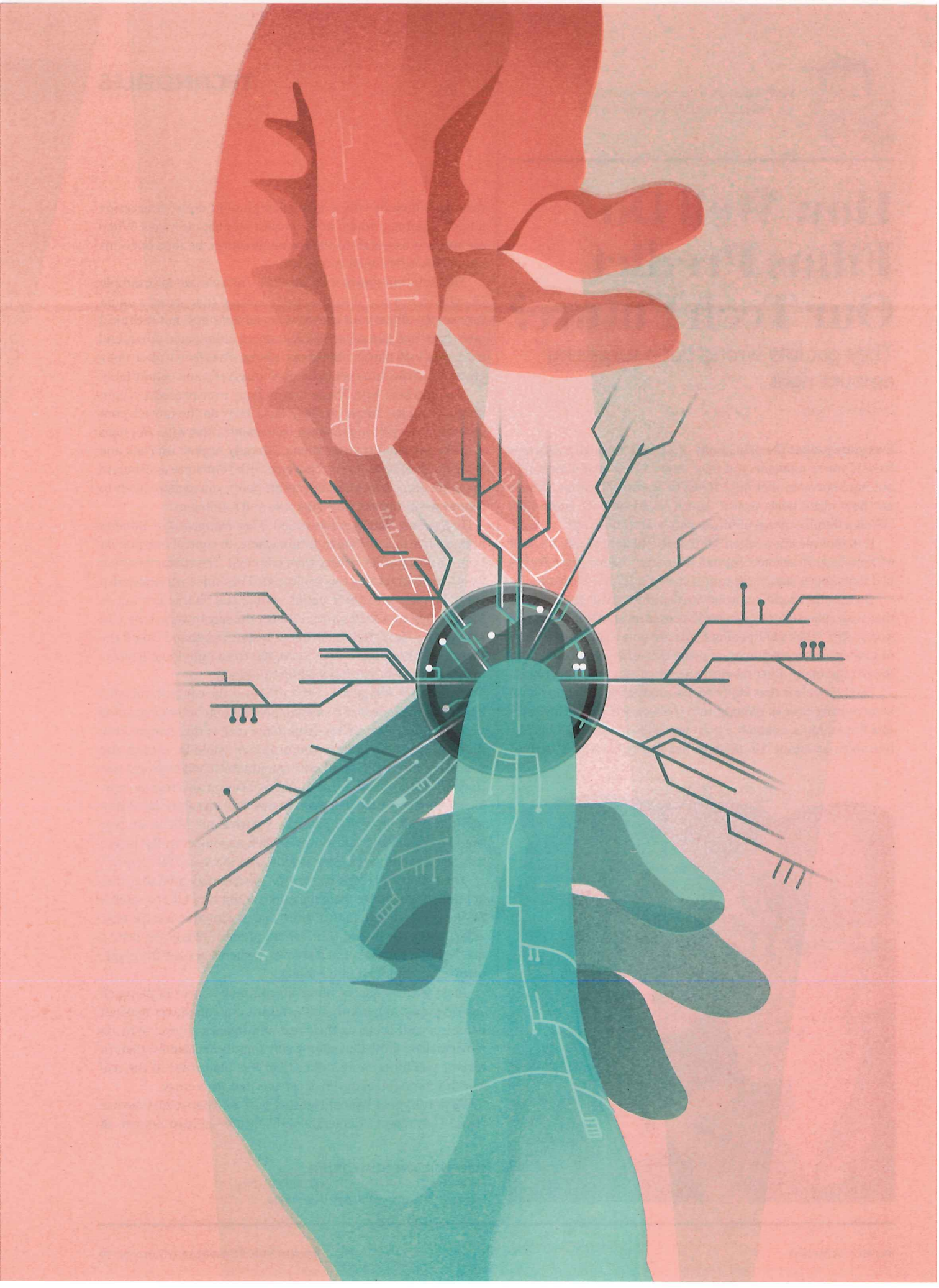
THE RACE TO SAVE THE CORALS
Helping them adapt to warmer oceans
PAGE 38

JANUARY 2018

9 770036 873145 01>

U.K. £4.99 $6.99 U.S.

ScientificAmerican.com



THE FUTURE OF MONEY

SPECIAL REPORT

BITCOIN WAS ONLY THE BEGINNING. MACHINES THAT BROKER trust without human intermediaries could fix the financial system's biggest flaws, but they also raise unnerving questions. Are we ready for a world in which any asset—from currency to personal identity—can be traded and tracked in an indelible ledger? What if a technology designed to strip banks and governments of power ends up giving them unprecedented control? —*The Editors*

Illustrations by Borja Bonaque

THE FUTURE OF MONEY

BREAKING THE BANK

NEW FINANCIAL NETWORKS COULD STOP THE CONCENTRATION OF WEALTH AND INCREASE PARTICIPATION IN THE ECONOMY—BUT ONLY IF USED WITH CARE

BY ALEXANDER LIPTON AND ALEX "SANDY" PENTLAND

IN BRIEF

The modern financial system has become dangerously complex. Increasing transparency would reduce risk, but that requires modeling the monetary circuit at a level of detail beyond the capacity of current technology.

New technologies such as digital currencies are now making it possible to simulate every trade and transaction. These tools could build more efficient financial networks and decentralize the control of money. People could exchange directly with one another instead of relying on banks.

The potential for sweeping change is real, but there are many uncertainties. These digital networks will only promote equity and accountability if they are properly built and responsibly used. They could just as easily lead to extreme levels of centralized control.

ON A SPRING DAY MORE THAN 5,000 YEARS AGO IN THE MESOPOTAMIAN CITY OF UR, A FOREIGN merchant sold his wares in exchange for a large bundle of silver. He didn't want to carry the bundle home because he knew he'd be back in Ur again to buy grain at the end of harvest season. Instead the merchant walked to the local temple, where valuables were often stored, and asked the priest to hold onto the silver for him.

Shortly after, the priest's nephew showed up to ask for a loan. The young man wanted to buy seed to grow his own crops, a wish that tugged at his uncle's heartstrings. So the priest loaned him some of the silver, reasoning that if his nephew failed to repay him by the time the merchant needed the silver back, he could fill in the missing amount with his personal funds or borrow it from friends. By using a long-term contract with the foreign merchant to support a short-term loan to his nephew, the priest doubled the number of commercial transactions by using the same money twice. In other words, he invented fractional banking.

Based on archaeological evidence, we know that some scenario like this one occurred in Mesopotamia, and it profoundly changed the financial environment in two ways. First, it increased the overall productivity of the economy, because the nephew could now afford seed. Second, it introduced risk: the nephew might not be able to pay the money back in time.

A few millennia later the emergence of government-backed central banks in 17th-century Europe connected this "double spending" with taxation. The king would borrow money from merchants to fight wars or build roads, and he would use it to pay arms manufacturers, purveyors and troops. That money began circulating, generating economic activity and profits, and at each step the amount of money was doubled—or more. The king typically repaid the loans with taxes imposed on profits, launching a prototype monetary circuit that marks the beginning of the banking system we use today.

Distilled to its simplest form, the modern circuit works along these lines: First, firms borrow money from private banks like JPMorgan Chase or HSBC to pay workers' salaries and other expenses. This is the step where money is created. Second, consumers purchase goods produced by firms or deposit the money as savings in banks. Finally, those firms use the money they receive to repay banks, and the cycle is complete. At this stage, the originally lent money is destroyed, but the interest stays in the system forever. That's how private banks can jump-start economies by creating money "out of thin air." Their power to do so is regulated in part by central banks, which impose limits on the amount of capital and liquidity private banks must always have to back lending activities.

If only it were so simple. Unfortunately, the monetary circuit introduces some fundamental problems into society. For one thing, it inevitably creates a handful of billionaires who control a high concentration of total wealth. It is also distressingly common to see leveraged money creation without sufficient understanding of (or care for) the risks. Which is how we get financial crashes, such as the one in 2008: when bankers and politicians spurred an insatiable demand for mortgages, it was met by a significant increase in the amount of money created—along with an even more significant increase in risk.

It may seem obvious to blame the monetary circuit itself for these problems. But it's not the root of the issue. Leveraged money creation works well as long as we can understand and control its inherent risks while suppressing undesirable wealth concentration. Today, however, a tangled web of factors, such as a booming population, global trade and powerful computers, makes the system far too complicated to manage and regulate, let alone understand.

What's more troubling is that the prevailing framework we use to guide macroeconomic activity is based on outdated paradigms. Models that are typically used to govern money creation and interest rates, for example, still treat private banks as simple intermediaries, ignoring the fact that they are big, active, money-creating elements unto themselves. That banks have their own motivations and profit-making strategies injects major opacity into the system. It's no wonder that the 2008 mortgage crisis was difficult to see coming.

Today's supercomplex monetary circuit needs to be modeled in unprecedented detail for us to actually understand it. Technological limitations have long prevented such a gargantuan task. But big data and the emergence of digital currencies and digital contracts are finally changing that. Rather than using historical averages to estimate what might happen in any economic system, it is finally becoming possible to completely simulate every individual trade and transaction and analyze all potential outcomes. The prospect of this feat is shaking up the functionality and ideology of global finance, and its implications could make economic security much better—or much worse.

Alexander Lipton is founder and CEO of StrongHold Labs and Connection Science Fellow at the Massachusetts Institute of Technology. Previously he served at Bank of America in senior managerial roles, while holding visiting professorships at the University of Oxford and Imperial College London. In 2000 he received the first Quant of the Year award.

Alex "Sandy" Pentland is a professor at M.I.T., one of the most cited authors in computer science and a member of the U.S. National Academies. In 2011 *Forbes* named him one of the world's seven most powerful data scientists. His most recent book is *Social Physics* (Penguin Books, 2015).

THE RISE OF DIGITAL CURRENCIES

NEW TECHNOLOGIES that make it feasible to reinvent our financial system have exploded on the scene in only the past decade. Most everyone has heard of Bitcoin, but that's only one piece of an up-and-com-

ing financial-technology industry characterized by buzz and speculation. What is important to know is that the core invention is a "distributed ledger," a database shared and managed by multiple participants. Think of it as a communal, digital bookkeeping system. It represents the foundational technology that has made cryptocurrencies—simply, digitally encrypted currencies—such as Bitcoin possible. Its underlying data structure, called a blockchain, is held in a series of sequentially encrypted blocks. To make those blocks reliable and secure, they are consensually updated by a variety of "proving" mechanisms that involve both humans and computers.

Conceptually speaking, blockchains and distributed ledgers are not new—blockchains, for instance, naturally occur whenever power, land or property changes hands. What *is* new is the marriage of the two concepts in a tamper-resistant computer system that can be applied to a wide range of practical problems. New technologies for blockchain-based distributed ledgers are making it possible to create digital currencies that are far more efficient than the U.S. dollar and more efficient than even Bitcoin.

These tools could enable us to monitor and analyze transactions at such a granular level that we can finally understand the monetary circuit. With a whole new level of clarity, we could learn to recognize and act on early-warning signals that arise from within the trillions of transactions recorded in the ledger, thus increasing system stability and safety. This kind of open-book, real-time monitoring is also safer for the community as a whole. In the 2008 crash, for example, there was not enough bureaucratic capacity to deal with the individual losses of tens of millions of citizens. As a consequence, regulators focused mostly on triaging the much smaller number of big banks, leaving ordinary people to suffer the most.

As this rapidly evolving technology gets tapped for an expanding range of applications, confusion abounds. Because Bitcoin is currently the most well-known (some might say notorious) form of digital currency, it is worth backing up to explore its origins and its weaknesses and how it is different from more promising forms that are now being pursued. Bitcoin was designed as a peer-to-peer digital payment system that operates without central authority. Anyone can join, which is both a strength and a weakness. Users make financial transactions with one another directly, without the help of intermediaries. These transactions are recorded in a publicly distributed blockchain ledger, for all participants to (theoretically) see. Since Bitcoin's inception in 2009, its price has gone up several orders of magnitude, making it the darling of speculators.

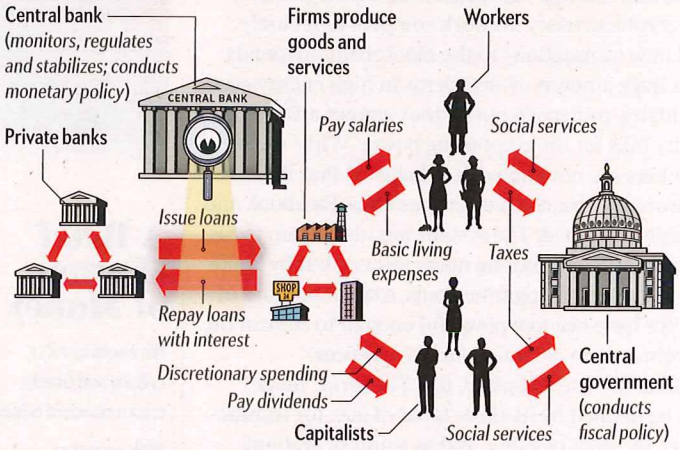
Bitcoin's promises are grand. Its proponents—mostly techno-savvy idealists and libertarians but also some criminal types—expect it to become a global currency that eventually supplants national cur-

Three Types of Financial Systems, Visualized

The current monetary circuit has become too complicated to understand. Emerging "blockchain technologies," such as the one driving Bitcoin, decentralize (and defog) the system. New networks are in development.

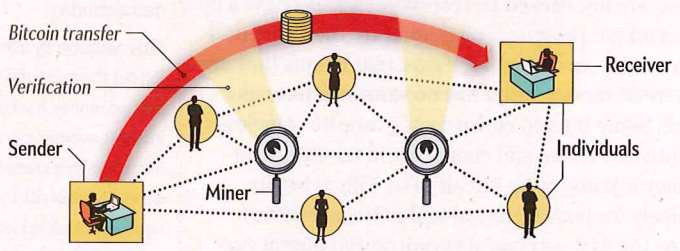
Fractional Banking (current monetary circuit)

Banks create money "out of thin air" when they issue loans to firms. Firms pay salaries and dividends to households. Households buy goods and services from firms. When loans are repaid, the "created" money is destroyed, but interest stays in the system for good.



Peer-to-Peer Bitcoin Network

Transactions are made directly between users, without the help of designated intermediaries. They are publicly broadcast and recorded in a blockchain. Consensus is maintained by random validators. Bitcoin has no value, so its price is inherently unstable.



Peer-to-Peer Tradecoin Network

As with Bitcoin, transactions would be made directly between users and are publicly recorded in a blockchain. But consensus is maintained by designated validators. Tradecoin's value is backed by real assets supplied by sponsors, so its price is relatively stable.

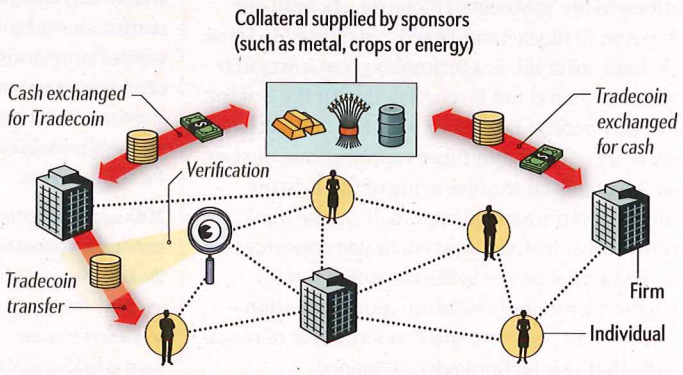


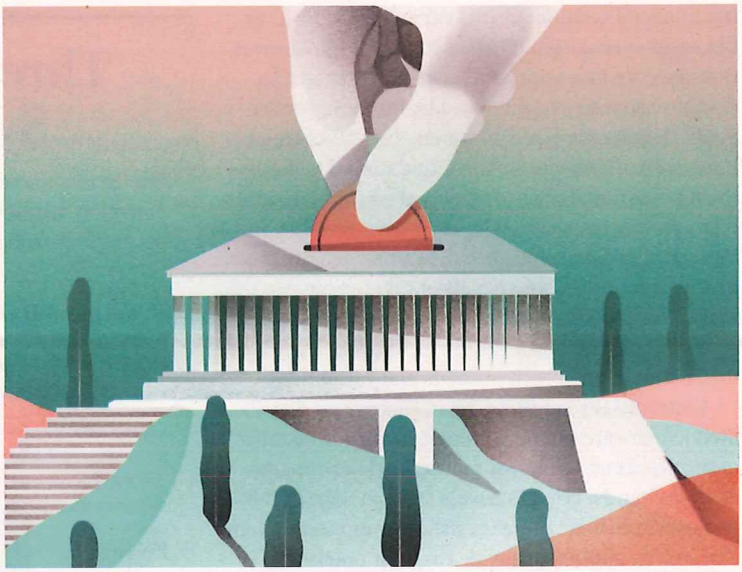
Illustration by Peter and Maria Hoey

rencies, which, in their minds, can be easily manipulated. Some enthusiasts even believe that Bitcoin is the digital version of gold, perhaps forgetting that gold gains stability both from its physical attributes and from billions of stakeholders and that in the digital world, good technologies are routinely overtaken by better ones.

Bitcoin is actually not the first digital currency, and it's very likely not the last major one either. It also has serious logistical constraints. For example, the number of transactions that can be handled per second is approximately seven, compared with the 2,000 on average handled by Visa. It's an energy suck, too: mining—the process by which nodes of the cryptocurrency network compete to securely add new transactions to the blockchain—depends on a huge amount of electricity. In high energy-cost countries, miners go bust if they cannot afford the utility bills for the computing power. While exact numbers are not known, it is believed that Bitcoin consumes as much electricity as eBay, Facebook and Google combined. The system was also set up to distribute authority among many miners, but by banding together into gigantic pools, a small number of groups have become powerful enough to control the Bitcoin system. So much for peer-to-peer!

Bitcoin's use is limited, too. The term "money" can be defined by its three types of use: for transactions, for store of value, and as a unit of account. Because Bitcoin's price versus the U.S. dollar (and other government-designated legal tender) is extremely unstable, it is difficult to use on a day-to-day basis. Bitcoin and Ether, another major digital currency, are not backed by real-world assets or even by government promises; consequently, they are purely speculative. In colloquial terms, that means they are not "real" money: what has no value can have any price. Some Bitcoin enthusiasts frame its valueless nature as a virtue and claim that in the future all money is going to be Bitcoin-like. This is highly unlikely for both technical and political reasons.

As the first successful decentralized digital currency, though, Bitcoin is an impressive breakthrough. The underlying technology and the philosophy of an unregulated, peer-to-peer financial system are innovative, and Bitcoin poses practical solutions to big problems. Of course, it's only one application of blockchain-based distributed ledgers. Blockchain, after all, is a technology, not a singular ideology: it should not be conflated with the driving philosophy behind Bitcoin or with the motivations of any of its current and future applications. Just as it has the potential to solve some of the existing problems of our financial system, it can be used to entrench them instead. And when you consider that a key element of power is the control of money—both existing money and future money creation—we can already peek into the Pandora's Box of moral hazards that this technology has opened.



A Brief History of Money

7th century B.C.: Lydians and Greeks create standard coinage.

14th century: Merchant banks such as the Medicis expand involvement in multistate finance, trade and manufacturing.

17th century: By loaning out the value of deposited money, bankers increase economic productivity while creating new sources of risk that regularly result in local crashes and even widespread depressions. Central banks emerge, linking banking with taxation.

18th century: The gold standard evolves from previous tactics in which circulating money was loosely controlled by a reserve of precious metals. This lowers risk.

20th century: The gold standard is replaced by the Basel Accords, which say that holding easily sold assets is just as good as holding gold.

Take the central banks of the major reserve currencies such as the U.S. Federal Reserve and the Bank of England. Trust is often associated with size—the bigger, the more trustworthy—but these players have proved such thinking to be a grave mistake. They have repeatedly chosen to make the "little guys" poorer by diluting their financial obligations through inflation, suppressing interest rates and other policies. Recently they have been testing negative interest rates and contemplating ways to get rid of cash.

What is more alarming is that some central banks are discussing the possibility of making *all* of their currency digital and recording purchases directly on a ledger. This could bypass input from private banks and give the government absolute control over the economy. It would also mean that the government has a record of everything you buy—including the stuff you currently purchase with cash to intentionally avoid a paper trail. This is increasingly looking like a possible scheme, and countries such as China, the U.K., Singapore and Sweden have announced plans for studying and potentially implementing such a strategy. The critical takeaway here is that although the technology itself is decentralized by design, it can be used to create centrally controlled systems.

TOWARD A MORE STABLE FINANCIAL SYSTEM

IT IS CLEAR that the invention of blockchain and distributed ledgers won't eradicate problems like financial crashes and unhealthy inflation—at least not in the short term. But it does enable the creation of legitimate alternatives to the big, powerful players. Technology now makes it possible to form specialized global currency systems that previously would not have had sufficient scale, trust or political stability to compete. That is why a natural next step is for the little guys—such as emerging economies or large num-

bers of individual citizens—to band together to form alternatives to central banks.

With that possibility in mind, our lab at the Massachusetts Institute of Technology is working on creating a digital currency suitable for large-scale transactional purposes. Called Tradecoin, it will be indelibly logged on a blockchain and anchored at all times to a basket of real-world assets such as crops, energy or minerals. Doing so will help stabilize its value and make it easier for the public to trust it. The core idea is that a broadly useful currency needs both human trust and efficient trade systems.

A digital Tradecoin built on a distributed ledger can allow alliances of small nations, businesses, commercial traders, credit unions or even farmers to put together enough assets to back a large, liquid currency that would potentially be as trustworthy and at least as efficient as the national currencies used by the World Bank and the International Monetary Fund. This would give the Tradecoin alliance members some protection from the selfish policies of the big players. The cryptographic structure makes it much easier, safer and cheaper for them to engage in international trade. If the alliance members are geographically and politically diverse, they could have greater immunity from the risk of default than if they were backed by a single large entity. Indeed, this is exactly how the Bank of England got started in 1694: as an alliance of merchants.

By design, the principles behind currencies such as Tradecoin are fundamentally different from cryptocurrencies like Bitcoin, which are not backed by real-world assets and do not involve alliances. Tradecoin can also avoid the energy-intensive process of mining by using a preapproved network of diverse and trusted "validators." Participants can choose a set of validator nodes who are sufficiently diverse so that no one can bribe 51 percent of the validators all at once. The result is a fast, fully scalable, reliable and environmentally friendly financial instrument. It combines the most recent technologies with the very old idea of a gold coin having intrinsic value, giving it the necessary trust to be used far away from its place of origin.

Currencies such as Tradecoin can be even safer than today's currencies because they can be designed to make the details of the monetary circuit visible for supervision. Oversight by human stakeholders is still necessary, much as ICANN oversees the Internet system or regulators such as the Federal Reserve Board oversee the banking system in the U.S. They allow for easy distributed accounting, which means we can more reliably model and predict risks. Right now this kind of transparency is impossible because the details of financial transactions and contracts are tightly restricted. But if such a system had been in place in 2008, it could have monitored the extreme concentration of some traders in mortgage-backed credit-default obligations and "simulated" in detail the consequences of changes in home values. Instead of hidden packages of bad mortgage deals, there could have been bright red flags.

We are taking on these transparency challenges. For instance, we are building "trust network" software systems for European Union nations and major U.S. financial companies to use as pilot programs. They will allow recording and "playback" of transactions and contracts among different parties without exposing proprietary data or violating privacy. This software is also the core system for Tradecoin. We are exploring how to pilot two Tradecoin currencies: one that is intended for international commerce and backed by an alliance of small nations and another that is backed by farmers for use in commodity markets. We are now recruiting alliance members to test the idea.

It is exciting that for the first time ever, there is the possibility of worldwide digital currencies that are largely immune to selfish policies of the rich central banks that control much of the money. Indeed, a flurry of new alternatives is likely to emerge, and a few might ultimately rise to compete with the biggest reserve currencies. That we can now create monetary systems that are truly understandable means we can potentially build the tools for minimizing risk, avoiding crashes, and maintaining individual freedom from intrusive governments and overly powerful corporations. And because they will be backed by (and convertible into) traditional assets, they have a real baseline value. That means they are less likely to be targeted for speculative attacks and will be strongly resistant to both political manipulation and inflation caused by the problems of single nations.

Taken together, next-generation cryptocurrencies such as Tradecoin could dramatically reduce frictions in global trade, even amid the chaos of the current political and economic climate. As a result, major currencies such as the dollar might become less dominant, or else the U.S. financial system might become better behaved. The hope is that these distributed systems, backed by broad alliances of diverse players, can bring more transparency, accountability and equity to the world.

MORE TO EXPLORE

The Macroeconomics of Central Bank Issued Digital Currencies. John Barrdear and Michael Kumhof. Staff Working Paper No. 605. Bank of England, July 2016.

Modern Monetary Circuit Theory, Stability of Interconnected Banking Network, and Balance Sheet Optimization for Individual Banks. Alexander Lipton in *International Journal of Theoretical and Applied Finance*, Vol. 19, No. 6, Article No. 1650034; September 2016.

Trust::Data: A New Framework for Identity and Data Sharing. Edited by Thomas Hardjono, David Shrier and Alex Pentland. Visionary Future, 2016.

FROM OUR ARCHIVES

After the Crash. The Editors; Science Agenda, December 2008.

scientificamerican.com/magazine/sa

THE FUTURE OF MONEY

THE WORLD BITCOIN CREATED

THE FIRST BIG DIGITAL CURRENCY GAVE US A GLIMPSE OF A NEW ECONOMIC ORDER—ONE THAT RAISES MORE QUESTIONS THAN ANSWERS

BY JOHN PAVLUS

John Pavlus is a writer and filmmaker focusing on science, technology and design. His work has appeared in *Bloomberg Businessweek*, *MIT Technology Review*, and *The Best American Science and Nature Writing* series. He lives in Portland, Ore.

BITCOIN. CRYPTOCURRENCIES. SMART CONTRACTS. MANY PEOPLE HAVE NOW heard of the rapidly changing ecosystem of financial technology, but few have wrapped their heads around it. Hundreds of central banks and corporations are incubating a game-changing technology called blockchain—and investors are betting billions on it. Yet only 24 percent of global financial services professionals surveyed in 2017 by PricewaterhouseCoopers (PwC) described themselves as "extremely" or "very" familiar with it. Much of the public is unsure if any of this is legal, if they understand it at all. Evangelists say it has the power to upend entire economic systems; others, such as Emin Gün Sirer, a blockchain researcher at Cornell University, warn that while the technical core is "fascinating and disruptive, there's also a lot of hokum out there." How to parse the nuance—or get a handle on what a blockchain is?

It all starts with Satoshi Nakamoto, the world's most reclusive pseudonymous billionaire. In October 2008 Nakamoto published a paper via an obscure Internet mailing list detailing a design for the world's first blockchain: a public database distributed and synchronized every 10 minutes across thousands of computers, accessible to anyone and yet hackable by no one. Its purpose? To provide a decentralized, bulletproof record of exchange for a new digital currency Nakamoto called Bitcoin.

Until that point, the trouble with "peer-to-peer electronic cash" was that nobody could reliably prevent you from spending it twice. Blockchain technology changed all that by inscribing every transfer of Bitcoin into a "distributed ledger"—a kind of digital spreadsheet that, thanks to the laws of mathematics and cryptography, was more inviolable than carving it in stone. The *Economist* dubbed it "the trust machine."

The technology that underpins Bitcoin quickly outgrew it, driving a frenetic period of innovation. Think of blockchain as a scaffolding that can hold any data that need secure provenance: financial histories, ownership documents, proofs of identity. This "worldwide ledger"—as Don Tapscott, co-author of *Blockchain Revolution,* calls it—is a blank slate. But the technology, imperfect as it is, can be tapped for evil, too, and some are pumping the brakes on the frenzy. Here's a guide to the digital landscape that Satoshi Nakamoto—whoever he is—has thrust before us.

CORE CONCEPTS

CRYPTOCURRENCY A form of digital currency that relies on the mathematics of cryptography to control how and when units of the currency are created and to ensure secure transfer of funds.

PEER-TO-PEER (P2P) NETWORK A web of computers linked in a decentralized way, such that any computer can communicate directly with any other without going through a central server or other administrator. Napster, the network for sharing music files that launched in the late 1990s, popularized the concept.

NODE A computer connected to a P2P network. The Bitcoin network currently has thousands of nodes spread across the globe.

DISTRIBUTED LEDGER A list of recorded, time-stamped transactions that is simultaneously broadcast, copied and verified via consensus across many different computers in a P2P network. If every node in the network has an identical copy of the ledger, falsified entries or corrupted versions can be easily detected.

BLOCK A grouping of individual transaction records on a blockchain. On the Bitcoin network, new blocks are added to the chain every 10 minutes.

HASHING A cryptographic method that uses a mathematical function to condense any amount of data into a unique string of alphanumeric characters of a certain fixed length—called a hash value. This creates an easily verifiable digital fingerprint for the hashed data. If even a single bit of the original data is changed or corrupted, the fingerprint that emerges from the hash function will be drastically different, making it easy to detect errors or tampering. Hashes are also "one-way"—the data cannot be reassembled or extracted from the fingerprint.

MINING The process by which nodes of a cryptocurrency network compete to securely add new blocks of transactions to a blockchain. Units of the currency are the reward—and hence, a financial incentive to ensure security. Mining involves downloading the latest version of the blockchain's transactions for verification, then using brute-force computation to randomly search for the solution to a difficult mathematical puzzle created via hashing. The first node to discover the correct solution "mines" that block, adding it to the blockchain and claiming the reward associated with it. Humans control nodes, but the competition has nothing to do with skill: simply, the more raw computing power a miner applies toward the solution, the more likely he or she is to find it—a process called proof of work.

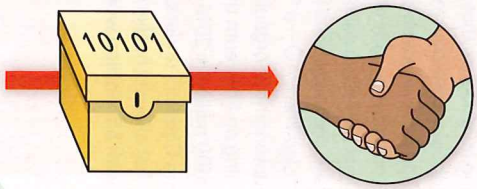
Illustrations by Peter and Maria Hoey

HOW BLOCKCHAIN WORKS

How does digital currency—or any data—reliably pass back and forth on a decentralized network full of strangers that don't have a reason to trust one another at all? By generating a permanent ledger of transactions that can't be changed by any single network member.

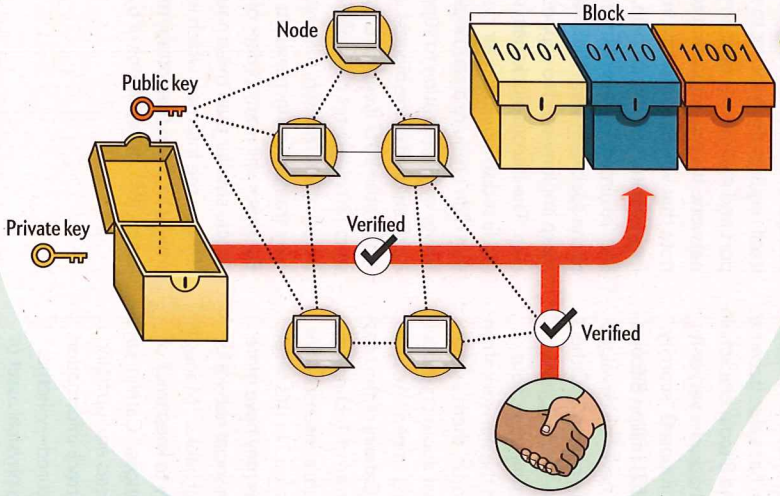
1

A blockchain transaction begins with one party agreeing to send data to another. These data could be anything. But because the point of a blockchain is to create a permanent, verifiable record of exchange, the data usually represent some valuable asset. Common examples: units of a cryptocurrency or other financial instrument; contracts, deeds or records of ownership; medical information or other identity data.



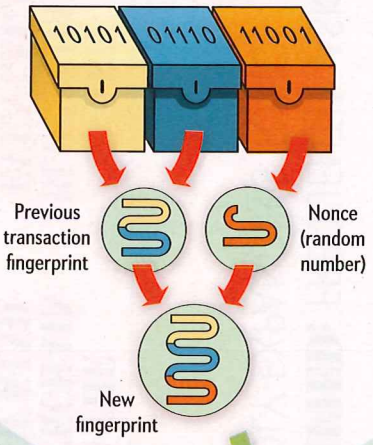
2

The transaction is broadcast for verification to a peer-to-peer network of computers operating the blockchain. Every node on the network is equipped with a procedure for verifying whether the transaction is valid or not. (In a Bitcoin transaction, for example, the network would verify whether those paying actually have the amount of Bitcoins they say they do.) Once the network has reached a consensus, algorithms package up the validated transaction with other recent transactions into a block.



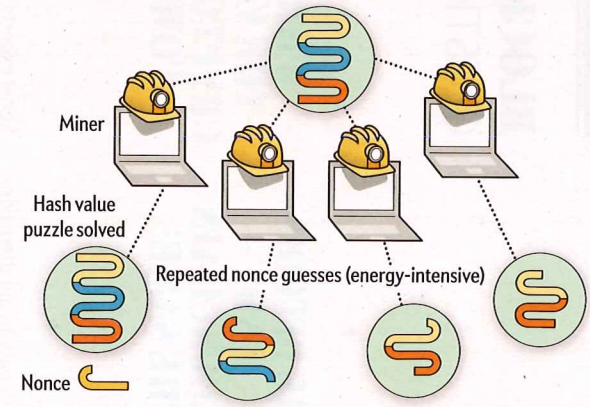
3

Software creates a "fingerprint" for the new block by hashing the data inside it, together with two other pieces of information: the fingerprint of the preceding block and a random number called a nonce.



4

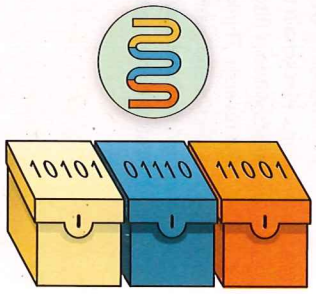
Special nodes called miners begin competing with one another for the right to add the new block to the blockchain. Their computers perform a tedious set of hash-based calculations over and over again by trial and error, hoping to generate a solution that satisfies an arbitrary rule defined by the network. (On the Bitcoin blockchain, the miners are searching for solutions—or "hash values"—that have a particular number of zeros at the beginning.) Whoever is first to complete this proof-of-work process and find the matching solution successfully "mines" that block, earning a financial reward.



AS AN ALTERNATIVE: Proof-of-work mining is energy-intensive, so some new blockchains are doing away with it, instead using a preapproved network of "validator" nodes who can notarize transactions via an alternative process called proof of stake. Because this process doesn't rely on difficult hashing calculations, it uses much less computing power (and much less electricity).

5

The validated block is added to the blockchain with a digital fingerprint that also mathematically encodes the validated fingerprints of every block preceding it. These nested fingerprints make the blockchain increasingly secure with every new block that gets added because altering a single bit of information anywhere in the blockchain would drastically change not only the fingerprint of that particular block but every subsequent one in the chain as well.



BLOCKCHAIN DEMYSTIFIED: FREQUENTLY ASKED QUESTIONS ABOUT A RAPIDLY EXPANDING TOPIC

1.

ARE BITCOIN AND BLOCKCHAIN THE SAME?

No, but it's easy to get them confused because they both came into public awareness in 2008, when Satoshi Nakamoto published his paper describing how to implement them simultaneously. Bitcoin is one type of cryptocurrency. What people call "blockchain" is a technology that makes Bitcoin possible—an infrastructure that can be used for tracking many types of transactions. Blockchain technology exists without Bitcoin—but not the reverse. Think of Bitcoin as a kind of application that runs "on" the blockchain, much like Web sites run on the Internet.

2.

WHERE DOES THE VALUE OF A CRYPTOCURRENCY COME FROM?

Some experts say that a cryptocurrency like Bitcoin has value because of its security (the Bitcoin blockchain has never been hacked—yet) or its mathematically imposed "scarcity" (a fixed supply of 21 million Bitcoins means they can never be devalued by "printing more money"). Others say that they have intrinsic value because mining them is tedious work that makes the network stronger—in other words, there's value in effort. But what about cryptocurrencies that aren't mined? According to Christian Catalini of the Massachusetts Institute of Technology, "value comes from consensus. We all *agree* it has value." In this sense, cryptocurrencies may have more in common with social networks than with central banks. "Money is a way for society to keep track of checks and balances," Catalini says. "If cryptocurrencies end up being a better way to track information," their value is secured—whether they represent a physical asset or just a number.

3.

IS THE BLOCKCHAIN A NEW KIND OF INTERNET?

Not quite, because the blockchain itself requires the Internet to support and maintain its peer-to-peer network. It's also important to note that when people talk informally about "the" blockchain, they're almost always referring to the specific system that Nakamoto implemented to support Bitcoin. The Bitcoin blockchain was the first distributed ledger system that didn't require a centralized server or organization to support it. It's still one of the biggest: as of November 2017 it contains more than 130 gigabytes (140 billion bytes) of information, and every new transaction increases its size. But that's still many orders of magnitude smaller than the amount of data on the Internet, which is estimated to be on the yottabyte scale (10^{24}, or septillions of bytes).

4.

ARE BLOCKCHAINS EVEN LEGAL?

Yes. But their decentralized nature and association with Bitcoin—which has been used in illegal transactions such as drug and arms sales—can give blockchains an "outlaw" reputation it doesn't necessarily deserve. Blockchains can be used for many different purposes, good or ill, just like Facebook, e-mail or any other Internet technology.

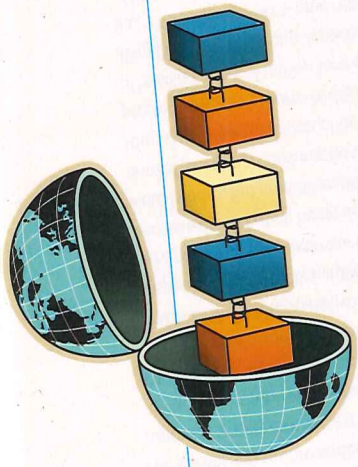
5.

HOW ARE CRYPTOCURRENCIES SECURE AND TRUSTWORTHY?

Because they're ultimately nothing but software, the trustworthiness of a cryptocurrency "comes from the code base," says M.I.T. researcher Catalini. Anyone can gin up a cryptocoin and raise funds by selling it through an initial coin offering—even Paris Hilton did it, lending her name to promote an obscure token. But it's no coincidence that the two most popular cryptocurrencies, Bitcoin and Ether, were engineered by computer-programming savants. That said, even coins with impressive technical bona fides can be risky. The DAO—a "decentralized autonomous organization" running on Ethereum that raised over $100 million in 2016—"had a bug" (in Catalini's understated terms) that allowed hackers to make off with $50 million worth of Ether.

10%

Predicted amount of the world's gross domestic product that will be stored in blockchain-based technology by 2025, according to a 2015 survey report from the World Economic Forum.



WHO IS USING BLOCKCHAIN TECHNOLOGY?

It's not just for cyberlibertarians, and it goes way beyond finance. Here's an incomplete lineup:

- **FINANCIAL INSTITUTIONS:** Global banks and investment institutions are researching and pursuing blockchain projects, sometimes joining forces in consortiums. Since 2012 Ripple has been a thriving, blockchain-based system for settling international transactions among banks. Start-ups such as Bloom intend to deploy blockchains to credit reporting, hoping to end data breaches like the Equifax hack.
- **GOVERNMENTS:** Delaware and Illinois use distributed ledgers for birth certificates. A Vermont law allows blockchain technology to verify the authenticity of legal documents. Dubai integrated blockchains into many of its administrative services, such as obtaining licenses. In 2016 Tunisia began issuing a blockchain-backed version of its digital national currency called the eDinar.
- **TECH ENTREPRENEURS:** The Ethereum network—which was designed to support new applications, rather than just a digital cash ecosystem like Bitcoin—is like an App Store for blockchain start-ups. Hundreds of projects and businesses are running on it. One notable: WePower wants to let households buy and sell renewable energy (from, say, roof-mounted solar panels) directly to one another.
- **COPYRIGHT AND IP HOLDERS:** U.K. musician Imogen Heap started Mycelia, a tech incubator that tracks metadata associated with creative works, cutting out intermediaries like iTunes.
- **NONPROFITS AND AID GROUPS:** The BitGive Foundation is boosting the accountability of philanthropic giving. And the United Nations World Food Program is streamlining how it tracks and delivers assistance to Syrian refugees in Jordan.
- **ACADEMIC INSTITUTIONS:** Forget sheepskins. The Blockcerts project wants to make all manner of academic and professional credentials more trustworthy and shareable.
- **ASSET MANAGERS:** London-based Everledger is targeting the diamond industry by recording the attributes and provenance of each precious stone. Fine wine and art are tracked, too.
- **JOURNALISTS:** To push back against fake news, Civil gives news makers a platform to create ad-free, inalterable journalism that's immune to outside interests (Russia; Facebook) and supported by readers.
- **REGULAR PEOPLE:** For migrant workers who send money to their families back home, using Bitcoin costs less than using Western Union, which is why an estimated 20 percent of international remittances between South Korea and the Philippines now rely on it.

WHY WOULD YOU USE A CRYPTOCURRENCY INSTEAD OF A NATIONAL CURRENCY?

Imagine holding a $100 bill that buys only $50 worth of goods. In Venezuela, where the official currency is crashing in value, that scenario is a reality. "You're losing something like half of the value of your net income every year to hyperinflation," says venture capitalist Morris. "People are thinking: 'How can I stop that?' And they're buying Bitcoin."

Why would a hard-to-understand cryptocurrency with no government guaranteeing its value as "legal tender" seem like a better bet than a more traditional value-holding commodity such as gold? For one thing, converting Venezuelan bolivars into Bitcoin is simply a lot easier for ordinary folks—anyone with access to the Internet can do it. Because Bitcoin has no physical form, you don't have to stash it somewhere unsafe—like a mattress or, in Venezuela's case, a bank. Of course, Bitcoin doesn't have a stable value, either. But while the bolivar has nose-dived, the value of a Bitcoin is at least trending ever upward. In a country where inflation is expected to exceed 2,300 percent in 2018 (according to the International Monetary Fund), it seems like a reasonable risk to take.

Zimbabweans have the opposite problem. After ditching its own currency for the U.S. dollar, the country now relies on currency imports to run its economy—and it's facing a shortage. Bitcoin is now common enough that it's even accepted by car dealers.

77%

of the global financial services industry is expected to adopt blockchain as part of a production system or process by 2020, according to PwC.

SO, BITCOIN: THE FUTURE OR A FLASH IN THE PAN?

Bitcoin is the world's most popular digital currency. But it's also wildly speculative, and many financial experts point to its legendary volatility: the currency's value has risen more than 10-fold since 2016, but it lost 40 percent of its value in a span of two weeks in September 2017—only to regain (and surpass) it just as quickly. (Who knows what it will be by the time you read this.) To others, the network's technical limitations—it is sluggish at handling transactions—combined with its unsustainable mining costs make it the equivalent of a financial time bomb. "We don't bet on Bitcoin," says Charlie Morris, chief investment officer of Next-Block Global, a firm that invests in blockchain technology.

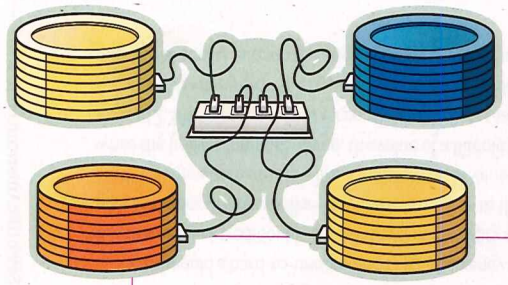
Bitcoin legitimized the basic economics of a global cryptocurrency. But the next-largest "altcoin" may have more staying power: Ether is less a cashlike currency than a "blockchain asset," as Morris calls it, used to power and secure the Ethereum network. Much like renting virtual servers in Google's "cloud," developers who want to create applications using Ethereum's blockchain must pay for access in tokens of Ether. The more useful Ethereum becomes as a mainstream platform, the more stable and valuable Ether becomes, too. New currencies and platforms are very likely to emerge—the race for prominence has only just begun.

ARE WE FACING THE END OF CASH?

It may seem that printed money is headed for the same fate as newspapers. But experts say that cash is far from dead. "We're still using great piles of paper to pay for things like international shipping of sea containers," says Vinay Gupta, CEO of Mattereum, a legal services firm for smart contracts. "The system is not so broken that people are willing to tear it up." The trouble with Bitcoin and Ether is that while they can function as a store of value or unit of exchange, they're not accepted as legal tender in enough places to compete with cash.

In places such as Kenya, where few people have traditional bank accounts and "mobile money" services such as M-Pesa have made saving and sending money by phone much easier than exchanging physical cash, cryptocurrencies might seem like a natural fit. But mining still requires a lot of processing power—not a common resource in Africa, where inexpensive feature phones outsell smartphones and not many own PCs. The computations required to secure blockchain transactions could, in theory, happen on "your old Nokia SIM card," Gupta says. Still, cold, hard paper won't soon disappear.

3 4 5



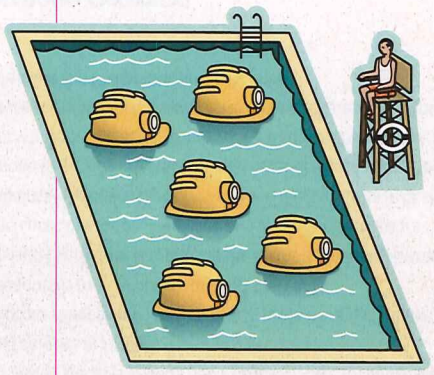
IS THE BLOCKCHAIN A NEW KIND OF INTERNET?

IF CRYPTOCURRENCIES ARE DIGITAL, WHAT POWERS THEM?

Just because cryptocurrencies have no physical attributes doesn't mean that there's no cost to using them. The intentionally effortful process by which new Bitcoins are "mined"—how new transactions are added to the ledger—requires that the entire P2P network cycle through a mind-boggling number of random computations to validate blockchain transactions. All of that processing requires energy.

How much energy? Start with the amount of computation. In late 2017 the Bitcoin network's "hash rate" was around 10 exahashes—that's 10 million trillion calculations—per second. Deriving a precise energy estimate from that figure is impossible because the network, being decentralized, can't account for individual nodes. But credible estimates peg the Bitcoin network's annual electricity consumption at around 27 terawatt-hours—roughly equivalent to that of Ireland. To put that in perspective, producing a year's worth of Bitcoin alone requires the equivalent of burning about 11 million tons of coal, which pours nearly 29 million tons of carbon dioxide into the atmosphere. Fueling Bitcoin by solar power would require harnessing more than half of the entire U.S.'s annual utility-scale solar capacity.

Ethereum's creator, Vitalik Buterin, is currently transitioning the network's blockchain to a different validation mechanism called proof of stake, which doesn't rely on mining at all. Bitcoin's larger, more decentralized network is unlikely to make a similar move anytime soon. But Vinay Gupta, who designed Dubai's blockchain strategy, believes that the same greed that motivates miners to turn kilowatts into cryptocurrency will ultimately spur them to innovate their way out of this scalability problem. Venture capitalist Charlie Morris thinks that as proof-of-stake cryptocurrencies prove their mettle in the market, "mining will become like a little blip in history," he says. "People will say, 'Remember when we all did that—wasn't that ridiculous?'"



WHERE DOES MINING ACTUALLY OCCUR?

71%

of Bitcoin is mined in China; the next most active country is India, at 4 percent. Tip: Don't try mining at home—alone. The task is now dominated by giant mining pools akin to the ones in China, so the chances of a solo node mining a block today is about one in eight million. Lone operators would spend far more on energy bills than they'd get in profits. Want to become a mining hobbyist? Join a public mining pool.

ARE BLOCKCHAINS EVEN LEGAL?

HOW ARE CRYPTOCURRENCIES SECURE AND TRUSTWORTHY?

WHAT DOES THE PUBLIC THINK ABOUT BLOCKCHAIN?

62%

of Americans believe cryptocurrencies are used for illegal purchases or don't know what they're used for at all, according to a 2017 YouGov survey.

59%

of global consumers polled in a 2017 HSBC survey said they had never heard of blockchain technology; 80 percent of those who had heard of the technology still don't understand what it is.

39%

of senior executives at large U.S. companies indicated they had little or no knowledge about blockchain technology, according to a 2017 Deloitte survey.

HOW WILL THIS TECHNOLOGY BE USED IN THE FUTURE?

Anyone building on blockchain technology is, by definition, a futurist. Once distributed ledger technology gets out of its training-wheels phase, what might we create with it?

- **SELF-DRIVING, SELF-OWNING CARS:** Instead of driving for Uber, your car would drive itself while you work or sleep. Blockchain-backed smart contracts could remove middlemen like Uber and Lyft from the car-sharing equation by automating their two basic functions—matching cars with riders and facilitating payments. You could also own "shares" of a car represented by cryptocurrency tokens.
- **PORTABLE MEDICAL DATA:** The same technology that allows two people to exchange units of Bitcoin without necessarily trusting each other could also vouchsafe medical information, putting control firmly in the hands of patients, says Brian Behlendorf, executive director of the Linux Foundation's Hyperledger project, a tool kit for building blockchain applications. Patients would receive a "'health wallet" with their data and histories. A doctor could go to a ledger and request your blood type, generating an access request on the user's phone. "You get an audit trail of who you shared that data with and the option to delete it when the treatment is over," Behlendorf says.
- **A GLOBAL SUPERCOMPUTER:** Linking your devices to thousands of others in a P2P network—and using a blockchain to pay you for their use—would create a financial incentive to support a worldwide, decentralized supercomputer. While you sleep, your laptop and phone could be rented by scientists who want to run models, for example. A project called Golem is already working on it. "The number of idle laptops is so much larger than the computing power of the data centers," Gupta says. "Artificial intelligence, climate modeling—all of that stuff could be accelerated 1,000-fold."

4

WHAT ARE THE LIMITATIONS AND DANGERS OF BLOCKCHAIN?

"Blockchains provide a substrate that, if certain assumptions are held to, is very difficult to modify ex post facto," says Cornell blockchain researcher Emin Gün Sirer. "But that doesn't mean that everything recorded to a blockchain is true or desirable. If I get hacked and someone steals my cryptocoins and tries to use them, I would very much like to undo that transaction. That's where immutability becomes a liability." It's also easy to confuse a blockchain's theoretical immutability with actual data security: public blockchains like Ethereum and Bitcoin don't actually encrypt any information. The Linux Foundation's Brian Behlendorf goes one step further: "The ledger should never be used to store personal data or anything sensitive, not even in encrypted form," he says, "because we know that no matter what we encrypt today, probably in 40 or 50 years we'll be able to decrypt it" with more advanced technology. Some advocates speak of blockchain as a panacea for any social problem involving trust, but that's blindly optimistic. For more on the limitations of blockchain as a societal savior, see page 34.

HOW DO YOU REGULATE A DECENTRALIZED SYSTEM?

Given the Wild West reputations of decentralized digital currencies, it's easy to assume that they were created to dismantle or avoid financial regulation. But that's not quite accurate. Bitcoin is full of regulations, after all—they're just defined and enforced by source code (and the collective activity of its P2P network) rather than by governments or financial institutions. "The whole innovation about Bitcoin is in eschewing social governance of record keeping," says Patrick Murck, a lawyer who researches blockchain policy and regulation at Harvard University's Berkman Klein Center for Internet and Society. Ethereum's stated purpose—to support the deployment of autonomous smart contracts—is essentially regulatory. A blockchain is arguably nothing *but* regulation: a mathematically enforced system of rules about what can and cannot be done with records in a database.

What always matters about financial regulation, decentralized or not, is who gets to do the regulating and how. "If you have a system that's decentralized, there's nowhere to attach regulation—but wherever that system gets reintermediated [by third parties], regulation will follow," Murck says. In 2013 China banned cryptocurrencies from its banking system, and last September it ordered all domestic Bitcoin exchanges to shut down. The U.S. and Japan are moving to regulate cryptocurrency exchanges and "initial coin offerings" with the same vigilance they apply to stock trading and investment banking.

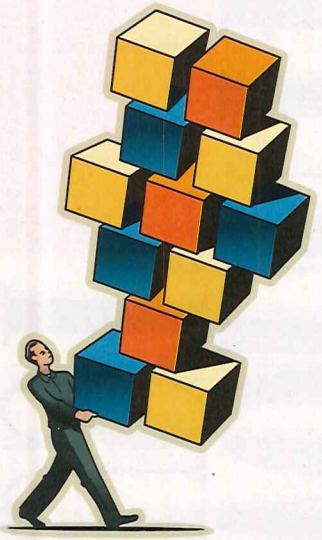
One future application of blockchain technology is in securing digital identity records, and according to venture capitalist Charlie Morris, new cryptocurrencies may emerge that marry identity data with financial information. They wouldn't have the anonymity of Bitcoin (Morris estimates the number of Bitcoin holders who pay honest taxes on them to be mere hundreds). But as digital money goes mainstream, the trade-off in perceived security and stability may make oversight tolerable—or even desirable. Says Murck: "If I'm trusting you with some property to hold on my behalf and transact with it—whether it's Bitcoin or Beanie Babies—then you're either regulated or about to be regulated."

5

CAN BLOCKCHAINS FAIL?

To date, the Bitcoin blockchain—the world's first and at present its largest and most widely used—has never been compromised or hacked. But that doesn't mean that every blockchain is invulnerable by definition. "There's no such thing as a perfect technology," says Cornell's Gün Sirer, co-director of the Initiative for Cryptocurrencies and Contracts. Here are three gaps in a blockchain's armor:

51% ATTACK: Blockchain-backed cryptocurrency networks rely on two bottomless resources for security: the speed and greed of their miners. But it's theoretically possible to overpower both. To subvert the blockchain's consensus mechanism, hackers would need to gain control over a majority of nodes in the network. This would give them the power to control how and which blocks get mined. They could reverse new transactions, allowing them to double spend digital currency. Or they could prevent other people's transactions from being validated. Bitcoin's P2P network, with thousands of nodes worldwide, seems unlikely to fall prey to such an attack. But smaller "altcoins" are at risk: one called Krypton was hit in 2016 by a group called the 51 crew. Even blockchains that don't use mining are vulnerable because they still rely on an "assumption that a majority of nodes in their network are benign," Gün Sirer warns.



GOOD OLD-FASHIONED HUMAN ERROR: It may take the computing equivalent of moving mountains to compromise the blockchain itself. But anything built on it or attached to it is just as vulnerable as it is now. Mt. Gox, a Bitcoin currency exchange (that is, an intermediary that lets people convert traditional currencies—like dollars—into Bitcoin) plagued by mismanagement and faulty code, lost 850,000 Bitcoins (worth $620 million at the time) in 2014. Ultimately blockchains are just distributed ledgers with no help desk—so if you have a digital wallet full of cryptocurrency and you lose the password, that money is almost certainly gone. There is rich irony in the fact that some cryptocurrency users keep a hard copy of their pass codes (or even the currency itself, stored on a USB drive) in a safety deposit box at the bank—a practice known as cold storage.

"BLOCKCHAIN BLOAT": This is less of a vulnerability than a natural consequence of blockchains working too well. Because every new block essentially revalidates every block before it, that means every node performing the validation needs a copy of the latest version of the entire chain to deal with every new transaction. At more than 130 gigabytes and growing, the Bitcoin blockchain is already getting unwieldy. Ethereum's ledger, designed to be more flexible (so that it can act as a platform for more sophisticated transactions such as smart contracts), is already bigger than Bitcoin's—if everyone were to start using it, would only high-performance supercomputers be able to handle the load? That could effectively decentralize the network, defeating the purpose of the distributed ledger in the first place.

THE EVOLUTION OF TRUST

THE ULTIMATE SOCIAL IMPACT OF BLOCKCHAIN TECHNOLOGY DEPENDS ON WHO CONTROLS OUR DIGITAL IDENTITIES

BY NATALIE SMOLENSKI

IN BRIEF

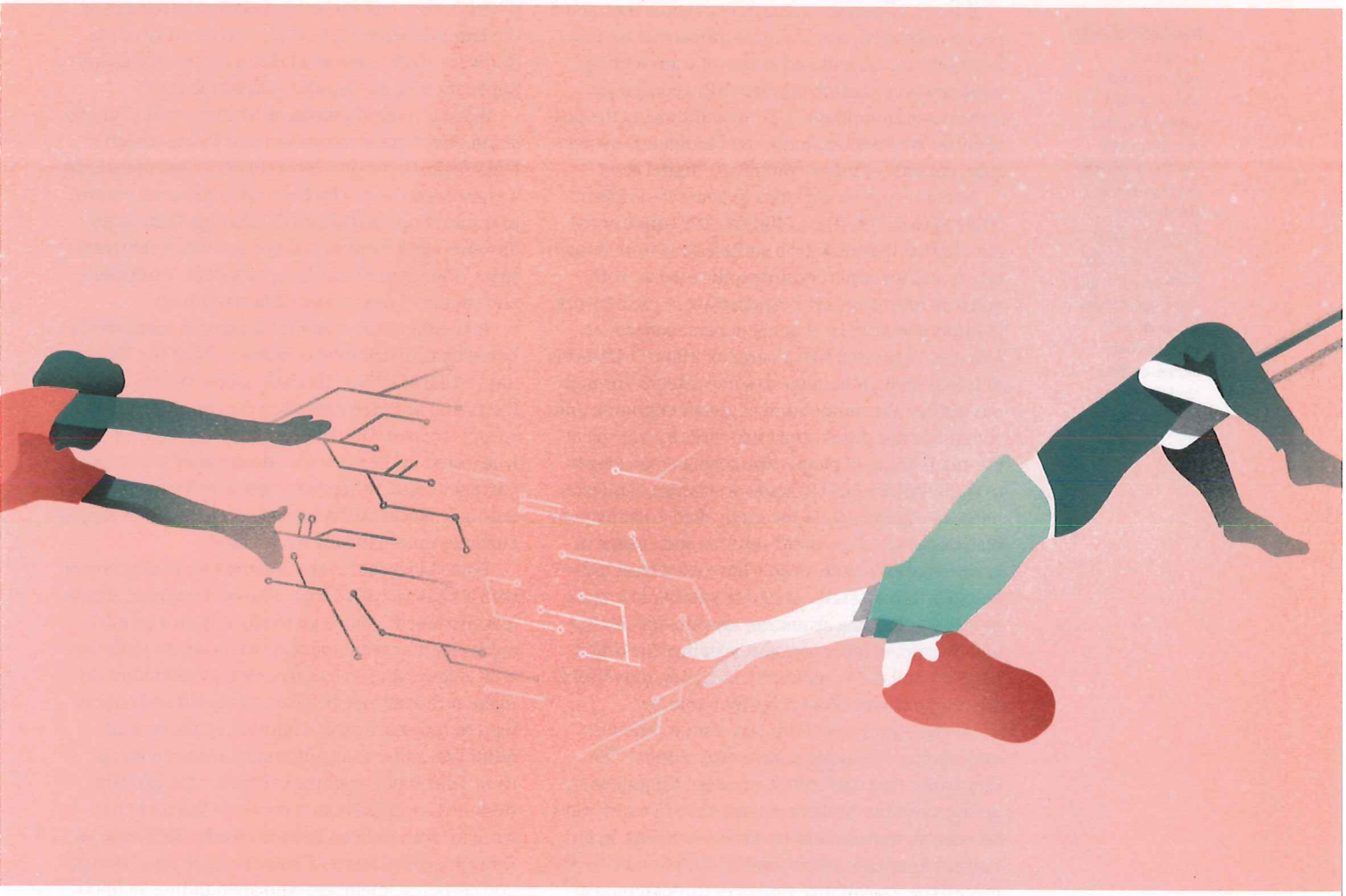
Banks and governments have in many ways failed to broker trust for the global economy, especially in the past few decades. Ordinary people have grown wary of centralized power and are seeking alternatives.

Bitcoin—and blockchain technology in general—allows the brokering of trust to be shifted toward machines and away from human intermediaries such as bankers. This technology could design exploitation out of the system instead of punishing it later.

Blockchains lend themselves both to human emancipation and to an unprecedented degree of surveillance and control. How they end up being used depends on how the software handles digital identity.

TO PARTICIPATE IN TODAY'S GLOBAL ECONOMY, ordinary people must accept an asymmetrical bargain: their lives are transparent to states, banks and corporations, whereas the behavior and inner workings of the powerful actors are kept hidden. The boundaries between the consumer and the citizen have irreversibly blurred. Harvard University social scientist Shoshana Zuboff has called this one-sided, extractive interaction "surveillance capitalism," and it is a major structural issue. The very institutions whose charter is brokering social trust—banks and governments—have in many parts of the world spectacularly failed to do so, especially during the lifetimes of those younger than 35.

The 2008 financial crash and its aftermath gave



shape to a kind of ambient helplessness. Of the legal cases that were brought to court, most were settled at shareholders' expense rather than resulting in jail time for high-ranking bankers, which convinced many that the wealthy and powerful collude for their own benefit. The issues run much deeper than the fallout from bad mortgages. An analysis of a 2007 database listing 37 million companies and investors across the world yielded the conclusion that 1 percent of these companies control 40 percent of the network, and most of the 1 percent are financial institutions. Over the past three decades investment earnings have become the chief source of economic growth in most countries, far outpacing income growth and making the top tier of wealthy people even wealthier. In the meantime, two billion people are still unbanked, excluded even from a far from perfect network that in principle facilitates access to capital. There is no agreement about whether or how these trends should be transformed to promote greater economic equality and inclusion without compromising individual autonomy.

That brings us to a historic moment in which mistrust of authority in the forms of power and wealth grows against a background of economic life that is inescapably global and mobile. If there's an impulse to retreat from it all in protest, there's also an acknowledgment that doing so is a recipe for economic self-sabotage. These constraints have led technologists around the world to imagine alterna-

Natalie Smolenski is a cultural anthropologist who writes and speaks about the intersections of identity, technology and government. She also leads business development for Learning Machine, a firm that makes applications for issuing and verifying official records on the blockchain using the Blockcerts open standard.

tives that simultaneously scale trust while making it more intimate and reciprocal. It's no coincidence that the world's first successful digital currency, Bitcoin, emerged on the scene in 2009: it represents a reaction to this growing desire for transparency, access and empowerment.

Bitcoin, of course, is a currency that is transacted via a blockchain—a new digital infrastructure that functions as a distributed ledger of transactions, validated according to mathematical consensus rather than by humans. It is revolutionizing the possibilities for direct exchange and individual ownership, not only of money but of any digital asset.

Bitcoin—and blockchains in general—is often referred to as "trustless." But this isn't quite accurate. Rather trust has been shifted away from human actors and toward a cryptographic system, with material incentives for participating in the network. In other words, trust is being depersonalized. At first, this may seem like a paradox. Haven't all forms of trust relied on humans to some extent? Throughout history, the momentum of global migration and commerce has driven trust networks to scale from the small group of people any given person knows to communities largely made of strangers and enemies. To expand across the earth, feed growing populations, wage wars, build empires and engage in knowledge exchange, people have used trust technologies that evolved out of one another in a more or less overlapping sequence: kinship and gift giving, division of labor, account keeping (the origin of credit and debt), hierarchy, currency, universalizing religions and, most recently, banking.

At the beginning of the 21st century, trust is undergoing yet another stage of evolution. The very banks that underwrote modern capitalism by acting as secure brokers of trust have in many ways become an impediment to its development. In our current financial system, policy and law tend to disincentivize exploitative practices through punishment. In the future, blockchains could simply design those practices out of the picture.

BUILDING FROM A BLOCKCHAIN

BITCOIN'S CONSENSUS PROTOCOL, which sets out the incentives and requirements that frame participation in the network, is exceptionally good at maintaining a distributed, open, peer-to-peer system of governance. Its transactions are public, though pseudonymous, and its code is open-source and maintained by a global network of volunteer core developers. The Bitcoin blockchain also doesn't store identity data; it uses public/private key pairs, rather than accounts, as addresses.

But blockchain-based transactions are more traceable than cash, which means that once a key pair is tied to a known identity, network analysis can, for example, aid police in tracking down criminal actors. This reality runs counter to the assumption that cryptocurrencies are more suited to criminal activity than other types of currency. In fact, it reintroduces the specter of surveillance capitalism. Interestingly, blockchains have properties that lend themselves both to human emancipation and to an unprecedented degree of surveillance and control. Whether they end up being used for the former or the latter depends on how the architecture of the "software stack"—the blockchain protocol and the application layer—handles digital identity.

When it comes to protocol, it's important to understand that there is more than one way to design a blockchain. Generally, "blockchain" is used to describe a type of system in which a single, universal record of transactions is replicated, although there is no absolute agreement on a set of necessary characteristics. Countless chains have now been introduced, and they are built to solve different things.

Take Ethereum, a public blockchain that aims to be a global, distributed computer called the Ethereum Virtual Machine. Its chain stores smart contracts that are executed when the conditions they specify are met. Unlike Bitcoin, the users most highly invested in the network—determined via cryptocurrency security deposits—get to collectively validate new blocks. Misbehaving users have their cryptocurrency automatically confiscated.

Some blockchains are designed for communities with a higher level of trust among their users. These "permissioned" chains generally rely on a central authority that grants specific users access to the system so they can serve as transaction validators. To make sure everyone behaves, permissioned chains tend to rely more on disciplining by the central authority rather than automated material incentives. One major example is Ripple, a blockchain designed specifically to serve as a settlement network for transactions between banks. Similarly, the Enterprise Ethereum Alliance is made up of nearly 200 corporate members who are building an open-source tool kit so businesses can design their own permissioned versions of the Ethereum blockchain.

Still other blockchainlike initiatives are referred to as distributed ledgers because they may lack one or all of the underlying features of blockchains. They are generally permissioned, with many of their transactions also kept private. A major distributed ledger is R3 Corda, developed by a consortium of banks to facilitate consensus regarding financial agreements.

Permissioned blockchains and distributed ledgers arose in part to include some type of identity vetting for validators and transactors on the network. (By design, there is no native identity validation in the Bitcoin blockchain protocol.) The field of identity is the terrain on which the emancipatory or oppressive characteristics of blockchains will be socially realized. The easier it is to tie someone's transactions to an identity—and the more central-

ized and externally controlled an individual's digital identity becomes—the more the possibilities for abuse multiply.

PROMISE AND PERIL

THE AVERAGE PERSON cannot use any blockchain directly, in the same way that the Internet cannot be used directly. Rather the individual uses applications that make use of the underlying blockchain in one way or another. The application layer is where untold confusion and often outright bad faith can reign. The history of Bitcoin, for example, is littered with cryptocurrency exchanges and wallet providers who left gaping security flaws in their applications, leading to high-profile hacks and accusations of embezzlement. In the case of the Ethereum network, vulnerabilities have resulted in the theft or loss of millions of dollars in its Ether cryptocurrency, with virtually no recourse for users. In general, using any application built by a trusted third party to hold your blockchain-based digital assets is still a highly insecure proposition.

This is the crux of blockchain's catch-22: the public won't use blockchains without user-friendly applications. But user-friendly applications often achieve that ease through centralization, which replicates the conditions of control that blockchains sought to circumvent.

If blockchains are to become widely useful, though, some correlation of identity with transactions is necessary. Perhaps identity will not require a full disclosure of who you are. As some in the Bitcoin community have argued, the current fixation on identity verification is largely misplaced; generally, what people want to know is whether a particular claim about you is true: Are you over 21? Did you really get a Ph.D. from M.I.T.? Are you a U.S. citizen? We are habituated by the incentive structures of surveillance capitalism to believe that giving up sweeping personal data is necessary to get by in the world. Changing that presupposition is one of the most radical influences that blockchain technologies may have.

Imagine, for instance, a future of digital voting. An election board must be able to correlate the casting of a vote to a registered voter so that person's vote is marked as "spent." But that process doesn't necessarily have to identify the individual to the board: it could simply verify that the voter is registered to participate in that election and record that he or she has cast a ballot after that person has done so—all without correlating the vote to the voter.

Projects that minimize the dispersal of so-called personally identifiable information are still rare, in part because they are not easy to monetize—either in financial currency or in the "currency" that is personal data. One example is Blockcerts, a series of free reference libraries developed by the M.I.T. Media Lab and Learning Machine, where I work. Blockcerts allows individuals to hold their digital assets in a private wallet that is hosted on their own device. The documents issued to a person are not associated with any identity profile unless the recipient chooses to do so. All the code is open-source, so it can be inspected for integrity and used by anyone to build his or her own applications for sending, storing, sharing and verifying official documents. This claims-based approach is a step toward what some in the digital identity space have called "self-sovereign identity," which means that individuals have administrative control over their own data.

We are habituated by the incentive structures of surveillance capitalism to believe that giving up sweeping personal data is necessary to get by in the world. Blockchain technologies may change that.

Blockchains are indeed a disruptive trust technology. But if blockchain-based applications are not designed with a commitment to digital self-sovereignty, there is nothing, in principle, preventing human beings from being treated as so many objects in a supply chain, with every movement and activity recorded, perhaps permanently. Creating digital identities whose existence is independent from governments and corporations is the next grand challenge that blockchains both pose and could help solve.

MORE TO EXPLORE

Debt: The First 5,000 Years. Updated edition. David Graeber. Melville House, 2014.

The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order. Michael Casey and Paul Vigna. St. Martin's Press, 2015.

Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. Shoshana Zuboff in *Journal of Information Technology*, Vol. 30, No. 1, pages 75–89; March 2015.

FROM OUR ARCHIVES

A Calculus of Risk. Gary Stix; May 1998.

scientificamerican.com/magazine/sa