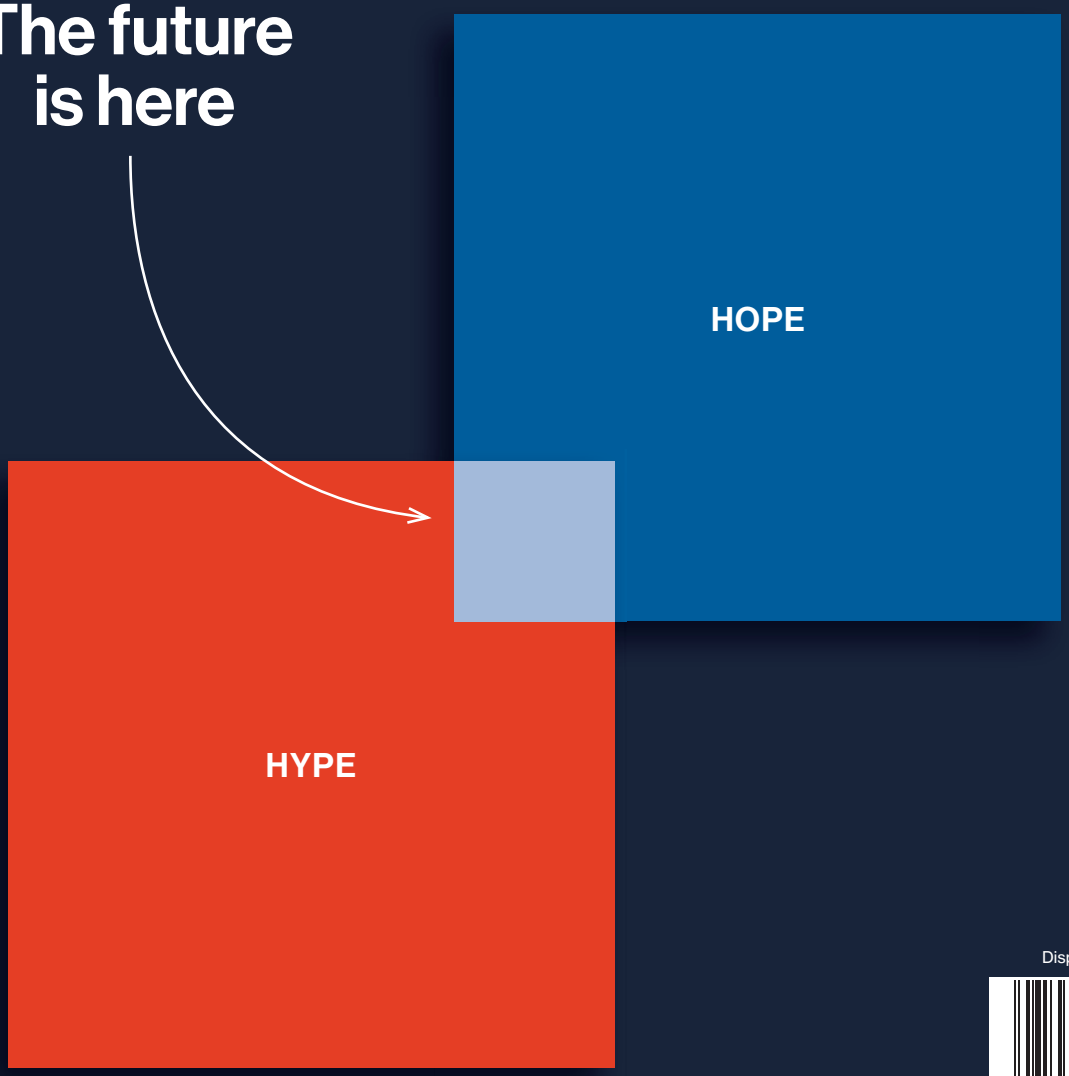
MIT Technology Review

VOL. 121 NO. 3 MAY/JUNE 2018 US $6.99/CAN $7.99

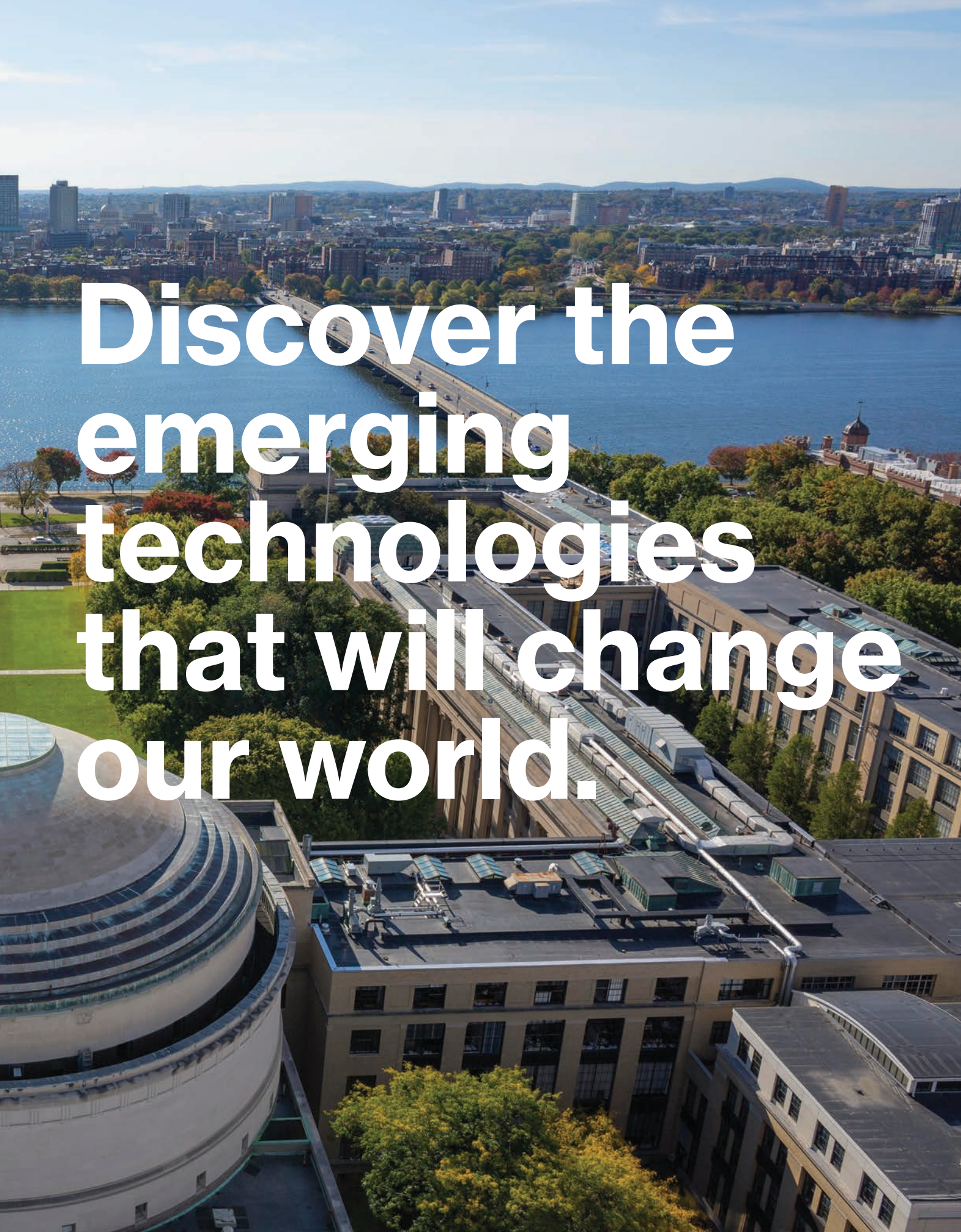
Blockchain

The future is here



Display until 07/01/2018


MIT
Technology
Review
EmTech
September 11-14, 2018
MIT Media Lab
Cambridge, MA
technologyreview.com/inspired


Discover the emerging technologies that will change our world.

From the Editor

NEPHI NIVEN

Gideon Lichfield is editor in chief of **MIT Technology Review.**

When we were planning this special issue back in January, someone asked, "What if most of the things we're writing about don't even exist by the time we publish?"

He was being only slightly facetious. As I write this, a bitcoin is trading at little more than a third of its value in December, when it peaked at nearly $20,000. Other cryptocurrencies have taken similar tumbles. Regulators in several countries are cracking down on the unregulated crowdfunding schemes known as initial coin offerings (ICOs), which exploded in 2017. A casual reader of the news might be forgiven for thinking that blockchain mania is over.

Obviously, we don't think it is, or you wouldn't be reading this. Cryptocurrencies and ICOs are just one aspect of the blockchain universe. Other kinds of blockchain startups are still proliferating, and big companies and financial institutions are exploring the technology's applications. But whatever survives the hype cycle will almost certainly look different from what exists today.

In this issue's opening essay (page 10), Michael Casey and Paul Vigna argue that just as the 1990s dot-com boom laid the foundations for today's technology industry, the tide of speculative capital and the detritus of countless failed blockchain startups will wash away to leave the infrastructure and talent pool for a future wave of technology giants. James Surowiecki (page 28) argues that cryptocurrencies will never work as foundations of the world financial system, and Kathryn Miles reports from Quebec (page 34) on how they could be sunk by their ravenous need for electricity. In a Jordanian refugee camp, Russ Juskalian (page 42) examines an attempt to use a blockchain to restore legal identity and self-sufficiency to people who've lost everything, while from Beijing, Yiting Sun (page 64) relates how China's crackdown on cryptocurrencies last year has unexpectedly given some blockchain entrepreneurs a boost. Douglas Heaven (page 58) looks at the forensic teams helping to crack cryptocrimes. And Morgen Peck (page 72) draws out three futuristic scenarios in which Bitcoin, the original and still the biggest cryptocurrency, might become irrelevant, supplanted by rivals.

There's much more, too. We sent photographers to capture portraits of the blockchain believers, who turn out to be a lot more diverse than you might expect (page 52). We look at whether ICOs can ever be truly useful (page 78), why there aren't more women in blockchain tech (page 66), and whether blockchains are really as secure as they're claimed to be (page 40). If you want to start with the basics, check out our graphical guide to blockchain on page 18. And finally, gaze into the future with a science fiction story by Hannu Rajaniemi (page 82) on how blockchains might govern our lives and relationships.

This issue also marks a new direction for *MIT Technology Review*. From now on, each of our bimonthly print issues will cover a single topic. Our aim will be to leave you with a better grasp of a complex technological issue and all its ramifications for the world. Please write to gideon.lichfield@technologyreview.com and let me know if we've succeeded.

Think Big. Take Risks. INNOVATE!

R&D Funding Program

The National Reconnaissance Office Director's Innovation Initiative (DII) Program funds cutting-edge scientific research in a high-risk, high-payoff environment to discover innovative concepts and creative ideas that transform overhead intelligence capabilities and systems for future national security intelligence needs. The program seeks out the brightest minds and breakthrough technologies from industry, academia, national laboratories, and U.S. government agencies.

Visit the website for Broad Agency Announcement and Government Sources Sought Announcement requirements.

703.808.2769

NATIONAL RECONNAISSANCE OFFICE
UNITED STATES OF AMERICA

https://acq.westfields.net

Contents

May/June 2018

How

Now

Next

Also in this issue

SELMAN DESIGN / ANDREW TESTA / ARIEL DAVIS

Big challenges are solvable.

Solve believes that open innovation is the best way to find solutions to the world's most pressing challenges in economic prosperity, health, learning and sustainability—and that diverse partnerships will help create lasting positive social and environmental impact.

If you're an innovator, apply here:
solve.mit.edu/challenges

SOLVE

Selected 'Solver Class' can:

- Access partnerships and prizes that help pilot, scale and implement projects.
- Join a network of cross-sector thought leaders and change makers.
- Attend (and pitch at) exclusive Solve events, including the flagship conference, Solve at MIT in May.
- Receive personalized support from Solve staff.

Massachusetts Institute of Technology

EDITORIAL

Editor in Chief Gideon Lichfield

Executive Editor Megan McCarthy, **Editor** David Rotman, **Senior Editor, MIT News** Alice Dragoon, **Senior Editor, AI and Robotics** Will Knight, **Senior Editor, Mobile** Rachel Metz, **Senior Editor, Biomedicine** Antonio Regalado, **Senior Editor, News and Commentary** Michael Reilly, **Senior Editor, Energy** James Temple, **Senior Editor, Business** Elizabeth Woyke, **San Francisco Bureau Chief** Martin Giles, **Managing Editor** Timothy Maher, **Copy Chief** Linda Lowenthal, **News and Commentary Editor** Jamie Condliffe, **Associate Editors** Emily Mullin, Mike Orcutt, Jackie Snow, Erin Winick, **Associate Content Producer** Brittany Mytnik, **Social Media Editor** Julia Sklar, **Senior Production Director** James LaBelle, **Contributing Editors** Brian Bergstein, Katherine Bourzac, Peter Burrows, Simson L. Garfinkel, Amanda Schaffer, Yiting Sun

DESIGN

Chief Creative Officer Eric Mongeon, **Lead Designer** Emily Luong, **Senior Designer** Lynne Carty, **Art Assistant** Emily Caulfield

PRODUCT DEVELOPMENT

Chief Digital Officer and Vice President, Product Development Erik Pelletier, **Director of Product** Vanessa DeCollibus, **User Interface/User Experience Designers** Emily Waggoner, Jon Akland, **Engineers** Shaun Calhoun, Molly Frey, Jason Lewicki, Zach Green

EVENTS

Senior Vice President, Events and Strategic Partnerships Amy Lammers, **Director of Events Programming** Laura Janes Wilson, **Senior Events Manager** Nicole Silva, **Content and Program Developer, Events** Kelsie Pallanck, **Events Associate** Bo Richardson

CORPORATE

Chief Executive Officer and Publisher Elizabeth Bramson-Boudreau

Vice President, Licensing and Communities Antoinette Matthews, **Director, Human Resources** Hilary Siegel, **Assistant to the CEO** Katie McLean, **Manager of Information Technology** Colby Wheeler, **Office Manager** Linda Cardinal

FINANCE

Manager of Accounting and Finance, Treasurer Enejda Xheblati, **General Ledger Manager** Olivia Male, **Accountant** Letitia Trecartin, **Administrative Assistant** Andrea Siegel

CONSUMER MARKETING

Senior Vice President, Consumer Revenues and Marketing Doreen Adger, **Consumer Marketing Manager** Katya Hill, **Director of Analytics** Tom Russell, **Director of Audience Development** Rosemary Kelly

MIT TECHNOLOGY REVIEW INSIGHTS

Vice President of International Business Development, Head of MIT Technology Review Insights Nicola Crepaldi, **Senior Editor, Head of US MIT Technology Review Insights** Mindy Blodgett, **Senior Project Manager** Anna Raborn

ADVERTISING SALES

Senior Vice President, Sales Laurie Hironaka / laurie@technologyreview.com / 415-640-5141, **Director of Strategic Accounts** Marii Sebahar / marii@technologyreview.com / 415-416-9140, **Senior Director of Brand Partnerships** Kristin Ingram / kristin.ingram@technologyreview.com / 415-509-1910, **Business Development Manager** Debbie Hanley / debbie.hanley@technologyreview.com / 214-282-2727, **New York and Southeast Advertising Director** Ian Keller / ian.keller@technologyreview.com / 203-858-3396, **Northeast Advertising Director** Mason Wells / mason.wells@technologyreview.com / 917-656-2899, **Digital Sales Strategy Manager** Ken Collina / ken.collina@technologyreview.com / 617-475-8004, **Advertising Services** webcreative@technologyreview.com / 617-475-8004, **Media Kit** www.technologyreview.com/media, **Germany** Michael Hanke / michael.hanke@heise.de / +49-511-5352-167, **China** Vincent Chen / +86-185-1033-0513, **Japan** Yoshimi Suezawa / adsales@technologyreview.jp / +81-3-3583-5364, **Spain and South America** Cecilia Nicolini / cecilia.nicolini@opinno.com / +34607720179

MIT ENTERPRISE FORUM, INC.

Chairman and President Elizabeth Bramson-Boudreau, **Executive Director and Clerk** Antoinette Matthews, **Treasurer** Enejda Xheblati, **Director of Chapter Leadership and Process** Gaylee Duncan, **Director of Communications** Joyce Chen

BOARD OF DIRECTORS

Martin A. Schmidt
Whitney Espich
Jerome I. Friedman
Joichi Ito
Israel Ruiz
David Schmittlein
Alan Spoon

CUSTOMER SERVICE AND SUBSCRIPTION INQUIRIES

National
800-877-5230

International
903-636-1115

E-mail
customer_service@mittechnologyreview.info

Web
www.technologyreview.com/customerservice

MIT Records (alums only)
617-253-8270

Reprints
techreview@wrightsmedia.com
877-652-5295

Licensing and permissions
licensing@technologyreview.com

Technology Review
One Main Street, 13th Floor
Cambridge, MA 02142
Tel: 617-475-8000

The mission of *MIT Technology Review* is to equip its audiences with the intelligence to understand and contribute to a world shaped by technology.

Technology Review, Inc., is an independent nonprofit 501(c)(3) corporation wholly owned by MIT; the views expressed in our publications and at our events are not always shared by the Institute.

Wharton
University of Pennsylvania
Aresty Institute of Executive Education

EXECUTIVE EDUCATION

excel

verb \ik·ˈsel\

"The moment I realized I had become part of something that would take me further than I've ever been."

Define *your* Wharton moment.

Wharton's ***General Management Program*** provides a flexible learning journey for distinguished senior executives ready for greater challenges. You will receive expert one-on-one **executive coaching** in Wharton's rigorous academic environment and return to your organization with an enriched global perspective and in-depth strategies for immediate success. Upon successful completion of the program, you will be awarded **Wharton alumni status** and join a powerful network of 96,000 peers in over 150 countries.

EXCEL AT A HIGHER LEVEL:

EXECED.WHARTON.UPENN.EDU/**GMP**

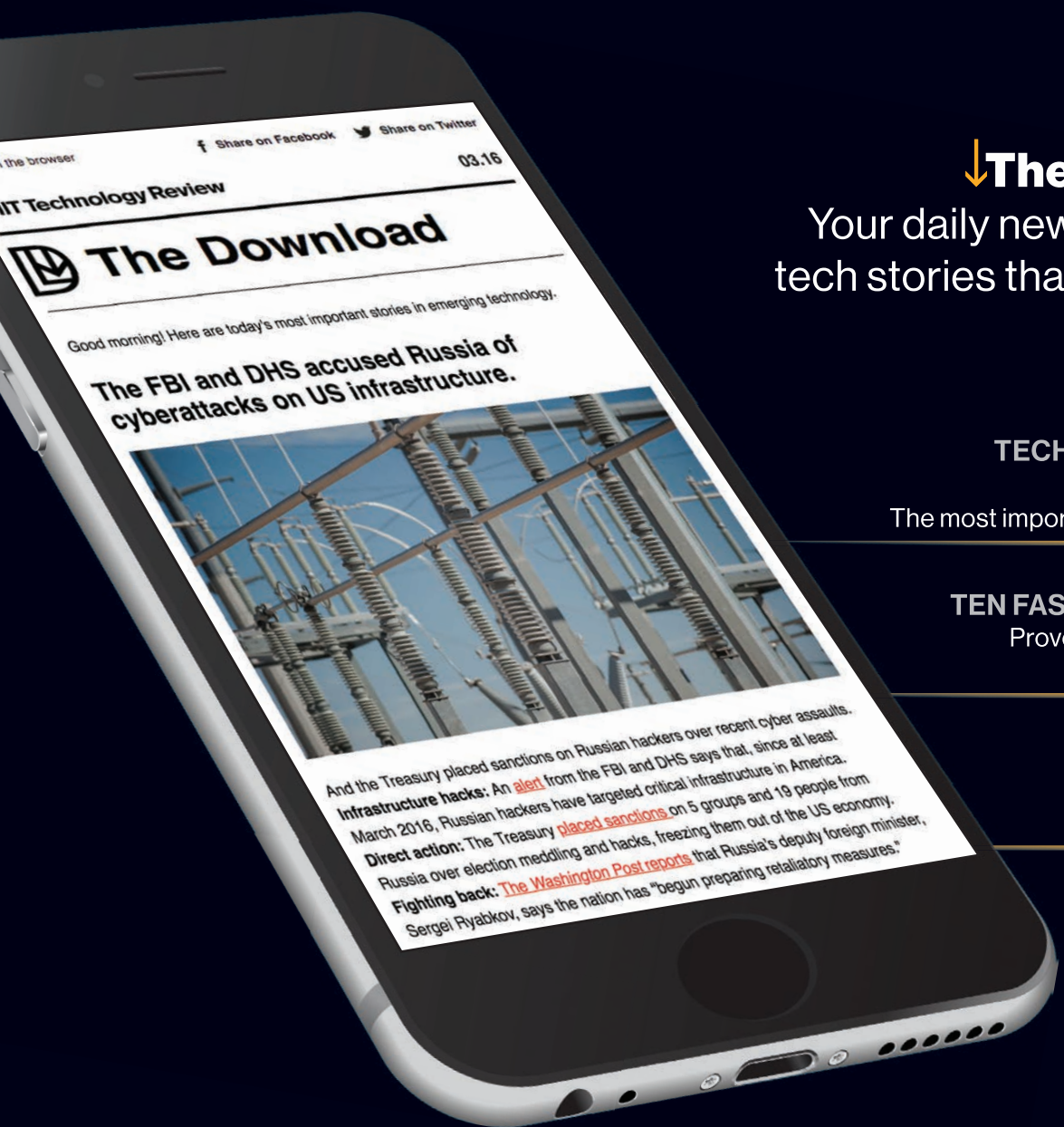
General Management Program

A FLEXIBLE LEARNING JOURNEY

Design your own curriculum of 6 programs within 2 years. Choose from 30+ eligible programs in:

- LEADERSHIP
- FINANCE
- STRATEGY & INNOVATION
- MARKETING

Get MIT Technology Review delivered to your inbox EVERY DAY.



↓The Download
Your daily newsletter of the tech stories that matter most

TECH NEWS YOU NEED TO KNOW TODAY
The most important stories of the day

TEN FASCINATING THINGS
Provocative items from the world of technology

AND MUCH MORE

Sign up now:
technologyreview.com/inbox

MIT Technology Review

1

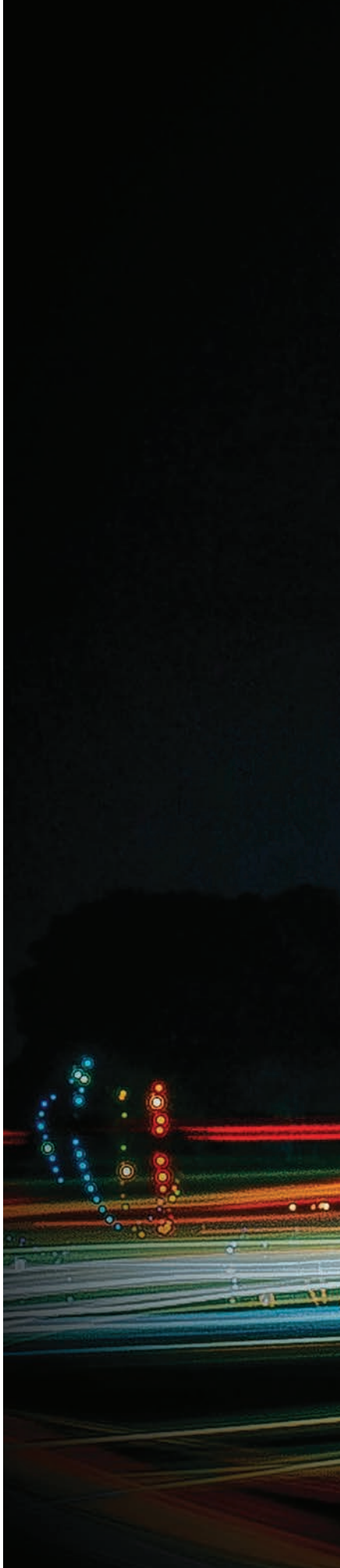
How WE GOT HERE

The case for blockchain: after the bubble bursts, the foundations of a future technological industry will remain. The case against cryptocurrencies: they're good for thieves and speculators, but no use as serious money. Plus: what a blockchain is, how it works, the top cryptocurrencies, and a glossary of crypto jargon.

To understand why blockchain matters, look past the wild speculation at what is being built underneath, argue the authors of *The Age of Cryptocurrency* and its newly published follow-up, *The Truth Machine: The Blockchain and the Future of Everything.*

In blockchain we trust

By **MICHAEL J. CASEY** and **PAUL VIGNA**
Illustrations by Selman Design



THE DOT-COM BUBBLE OF THE 1990s is popularly viewed as a period of crazy excess that ended with hundreds of billions of dollars of wealth being destroyed. What's less often discussed is how all the cheap capital of the boom years helped fund the infrastructure upon which the most important internet innovations would be built after the bubble burst. It paid for the rollout of fiber-optic cable, R&D in 3G networks, and the buildout of giant server farms. All of this would make possible the technologies that are now the bedrock of the world's most powerful companies: algorithmic search, social media, mobile computing, cloud services, big-data analytics, AI, and more.

We think something similar is happening behind the wild volatility and stratospheric hype of the cryptocurrency and block-


WELCOME
to the
BLOCKCHAIN
ENTERING A NEW ECONOMY

chain boom. The blockchain skeptics have crowed gleefully as crypto-token prices have tumbled from last year's dizzying highs, but they make the same mistake as the crypto fanboys they mock: they conflate price with inherent value. We can't yet predict what the blue-chip industries built on blockchain technology will be, but we are confident that they will exist, because the technology itself is all about creating one priceless asset: trust.

To understand why, we need to go back to the 14th century.

That was when Italian merchants and bankers began using the double-entry bookkeeping method. This method, made possible by the adoption of Arabic numerals, gave merchants a more reliable record-keeping tool, and it let bankers assume a powerful new role as middlemen in the international payments system. Yet it wasn't just the tool itself that made way for modern finance. It was how it was inserted into the culture of the day.

In 1494 Luca Pacioli, a Franciscan friar and mathematician, codified their practices by publishing a manual on math and accounting that presented double-entry bookkeeping not only as a way to track accounts but as a moral obligation. The way Pacioli described it, for everything of value that merchants or bankers took in, they had to give something back. Hence the use of offsetting entries to record separate, balancing values—a debit matched with a credit, an asset with a liability.

Pacioli's morally upright accounting bestowed a form of religious benediction on these previously disparaged professions. Over the next several centuries, clean books came to be regarded as a sign of honesty and piety, clearing bankers to become payment intermediaries and speeding up the circulation of money. That funded the Renaissance and paved the way for the capitalist explosion that would change the world.

Yet the system was not impervious to fraud. Bankers and other financial actors often breached their moral duty to keep honest books, and they still do—just ask Bernie Madoff's clients or Enron's shareholders. Moreover, even when they are honest, their honesty comes at a price. We've allowed centralized trust managers such as banks, stock exchanges, and other financial middlemen to become indispensable, and this has turned them from intermediaries into gatekeepers. They charge fees and restrict access, creating friction, curtailing innovation, and strengthening their market dominance.

The need for trust and middlemen allows behemoths such as Google, Facebook, and Amazon to turn economies of scale and network effects into de facto monopolies.

The real promise of blockchain technology, then, is not that it could make you a billionaire overnight or give you a way to shield your financial activities from nosy governments. It's that it could drastically reduce the cost of trust by means of a radical, decentralized approach to accounting—and, by extension, create a new way to structure economic organizations.

A new form of bookkeeping might seem like a dull accomplishment. Yet for thousands of years, going back to Hammurabi's Babylon, ledgers have been the bedrock of civilization. That's because the exchanges of value on which society is founded require us to trust each other's claims about what we own, what we're owed, and what we owe. To achieve that trust, we need a common system for keeping track of our transactions, a system that gives definition and order to society itself. How else would we know that Jeff Bezos is the world's richest human being, that the GDP of Argentina is $620 billion, that 71 percent of the world's population lives on less than $10 a day, or that Apple's shares are trading at a particular multiple of the company's earnings per share?

A blockchain (though the term is bandied about loosely, and often misapplied to things that are not really blockchains) is an electronic ledger—a list of transactions. Those transactions can in principle represent almost anything. They could be actual exchanges of money, as they are on the blockchains that underlie cryptocurrencies like Bitcoin. They could mark exchanges of other assets, such as digital stock certificates. They could represent instructions, such as orders to buy or sell a stock. They could include so-called smart contracts, which are computerized instructions to do something (e.g., buy a stock) if something else is true (the price of the stock has dropped below $10).

What makes a blockchain a special kind of ledger is that instead of being managed by a single *centralized* institution, such as a bank or government agency, it is stored in multiple copies on multiple independent computers within a *decentralized* network. No single entity controls the ledger. Any of the computers on the network can make a change to the ledger, but only by following rules dictated by a "consensus protocol," a mathematical algorithm that requires a majority of the other computers on the network to agree with the change.

Once a consensus generated by that algorithm has been achieved, all the computers on the network update their copies of the ledger simultaneously. If any of

them tries to add an entry to the ledger without this consensus, or to change an entry retroactively, the rest of the network automatically rejects the entry as invalid.

Typically, transactions are bundled together into blocks of a certain size that are chained together (hence "blockchain") by cryptographic locks, themselves a product of the consensus algorithm. This produces an *immutable,* shared record of the "truth," one that—if things have been set up right—cannot be tampered with.

Within this general framework are many variations. There are different kinds of consensus protocols, for example, and often disagreements over which kind is most secure. There are public, "permissionless" blockchain ledgers, to which in principle anyone can hitch a computer and become part of the network; these are what Bitcoin and most other cryptocurrencies belong to. There are also private, "permissioned" ledger systems that incorporate no digital currency. These might be used by a group of organizations that need a common record-keeping system but are independent of one another and perhaps don't entirely trust one another—a manufacturer and its suppliers, for example.

The common thread between all of them is that mathematical rules and impregnable cryptography, rather than trust in fallible humans or institutions, are what guarantee the integrity of the ledger. It's a version of what the cryptographer Ian Grigg described as "triple-entry bookkeeping": one entry on the debit side, another for the credit, and a third into an immutable, undisputed, shared ledger.

The benefits of this decentralized model emerge when weighed against the current economic system's cost of trust. Consider this: In 2007, Lehman Brothers reported record profits and revenue, all endorsed by its auditor, Ernst & Young. Nine months later, a nosedive in those same assets rendered the 158-year-old business bankrupt, triggering the biggest financial crisis in 80 years. Clearly, the valuations cited in the preceding years' books were way off. And we later learned that Lehman's ledger wasn't the only one with dubious data. Banks in the US and Europe paid out hundreds of billions of dollars in fines and settlements to cover losses caused by inflated balance sheets. It was a powerful reminder of the high price we often pay for trusting centralized entities' internally devised numbers.

The crisis was an extreme example of the cost of trust. But we also find that cost ingrained in most other areas of the economy. Think of all the accountants whose cubicles fill the skyscrapers of the world. Their jobs, reconciling their company's ledgers with those of its business counterparts, exist because neither party *trusts* the other's record. It is a time-consuming, expensive, yet necessary process.

Other manifestations of the cost of trust are felt not in what we do but in what we can't do. Two billion people are denied bank accounts, which locks them out of the global economy because banks don't trust the records of their assets and identities. Meanwhile, the internet of things, which it's hoped will have billions of interacting autonomous devices forging new efficiencies, won't be possible if gadget-to-gadget microtransactions require the prohibitively expensive intermediation of centrally controlled ledgers. There are many other examples of how this problem limits innovation.

These costs are rarely acknowledged or analyzed by the economics profession, perhaps because practices such as account reconciliation are assumed to be an integral, unavoidable feature of business (much as pre-internet businesses assumed they had no option but to pay large postal expenses to mail out monthly bills). Might this blind spot explain why some prominent economists are quick to dismiss blockchain technology? Many say they can't see the justification for its costs. Yet their analyses typically don't weigh those costs against the far-reaching societal cost of trust that the new models seek to overcome.

More and more people get it, however. Since Bitcoin's low-key release in January 2009, the ranks of its advocates have swelled from libertarian-minded radicals to include former Wall Street professionals, Silicon Valley tech mavens, and development and aid experts from bodies such as the World Bank. Many see the technology's rise as a vital new phase in the internet economy—one that is, arguably, even more transformative than the first. Whereas the first wave of online disruption saw brick-and-mortar businesses displaced by leaner digital intermediaries, this movement challenges the whole idea of for-profit middlemen altogether.

The need for trust, the cost of it, and the dependence on middlemen to provide it is one reason why behemoths such as Google, Facebook, and Amazon turn economies of scale and network-effect advantages into de facto monopolies. These giants are, in effect, centralized ledger keepers, building vast records of "transactions" in what is, arguably, the most important "currency" in the world: our digital data. In controlling those records, they control us.

The potential promise of overturning this entrenched, centralized system is an important factor behind the gold-rush-like scene in the crypto-token market, with its soaring yet volatile prices. No doubt many—perhaps most—investors are merely hoping to get rich quick and give little thought to why the technology matters. But manias like this, as irrational as they become, don't spring out of nowhere. As with the arrival of past transformative platform technologies—railroads, for example, or electricity—rampant speculation is almost inevitable. That's because when a big new idea comes along, investors have no framework for estimating how much value it will create or destroy, or for deciding which enterprises will win or lose.

Although there are still major obstacles to overcome before blockchains can fulfill the promise of a more robust system for recording and storing objective truth, these concepts are already being tested in the field.

Companies such as IBM and Foxconn are exploiting the idea of immutability in projects that seek to unlock trade finance and make supply chains more transparent. Such transparency could also give consumers better information on the sources of what they buy—whether a T-shirt was made with sweatshop labor, for example.

Another important new idea is that of a *digital asset.* Before Bitcoin, nobody could own an asset in the digital realm. Since copying digital content is easy to do and difficult to stop, providers of digital products such as MP3 audio files or e-books never give customers outright ownership of the content, but instead lease it and define what users can do with it in a license, with stiff legal penalties if the license is broken. This is why you can make a 14-day loan of your Amazon Kindle book to a friend, but you can't sell it or give it as a gift, as you might a paper book.

We now have the capacity to assign digital representation to any store of value, including creative content, physical property, and intangible assets.

Bitcoin showed that an item of value could be both digital and verifiably unique. Since nobody can alter the ledger and "double-spend," or duplicate, a bitcoin, it can be conceived of as a unique "thing" or asset. That means we can now represent any form of value—a property title or a music track, for example—as an entry in a blockchain transaction. And by digitizing different forms of value in this way, we can introduce software for managing the economy that operates around them.

As software-based items, these new digital assets can be given certain "If X, then Y" properties. In other words, money can become *programmable.* For example, you could pay to hire an electric vehicle using digital tokens that also serve to activate or disable its engine, thus fulfilling the encoded terms of a smart contract. It's quite different from analog tokens such as banknotes or metal coins, which are agnostic about what they're used for.

WORLD-CLASS EXECUTIVE EDUCATION AT BROWN UNIVERSITY

Transforming Mid-Career Professionals

An Executive Master's degree from Brown University will prepare you to lead your organization, transform your field, and build a powerful lifelong professional network.

You will join a vibrant learning community and apply your new knowledge and skills through a critical challenge project.

The results can be seen in our alumni who are proven leaders; impacting their organizations and the world.

BROWN
School of Professional Studies

brown.edu/professional

IE Brown Executive MBA

Executive Master in Cybersecurity

Executive Master in Science and Technology Leadership

Executive Master of Healthcare Leadership

What makes these programmable money contracts "smart" is not that they're automated; we already have that when our bank follows our programmed instructions to autopay our credit card bill every month. It's that the computers executing the contract are monitored by a decentralized blockchain network. That assures all signatories to a smart contract that it will be carried out fairly.

With this technology, the computers of a shipper and an exporter, for example, could automate a transfer of ownership of goods once the decentralized software they both use sends a signal that a digital-currency payment—or a cryptographically unbreakable commitment to pay—has been made. Neither party necessarily trusts the other, but they can nonetheless carry out that automatic transfer without relying on a third party. In this way, smart contracts take automation to a new level—enabling a much more open, global set of relationships.

Freely accessible open-source code is the foundation upon which the decentralized economy of the future will be built.

Programmable money and smart contracts constitute a powerful way for communities to govern themselves in pursuit of common objectives. They even offer a potential breakthrough in the "Tragedy of the Commons," the long-held notion that people can't simultaneously serve their self-interest and the common good. That was evident in many of the blockchain proposals from the 100 software engineers who took part in Hack4Climate at last year's UN climate-change conference in Bonn. The winning team, with a project called GainForest, is now developing a blockchain-based system by which donors can reward communities living in vulnerable rain forests for provable actions they take to restore the environment.

Still, this utopian, frictionless "token economy" is far from reality. Regulators in China, South Korea, and the US have cracked down on issuers and traders of tokens, viewing such currencies more as speculative get-rich-quick schemes that avoid securities laws than as world-changing new economic models. They're not entirely wrong: some developers have pre-sold tokens in "initial coin offerings," or ICOs, but haven't used the money to build and market products. Public or "permissionless" blockchains like Bitcoin and Ethereum, which hold the greatest promise of absolute openness and immutability, are facing growing pains. Bitcoin still can't process more than seven transactions a second, and transaction fees can sometimes spike, making it costly to use.

Meanwhile, the centralized institutions that should be vulnerable to disruption, such as banks, are digging in. They are protected by existing regulations, which are ostensibly imposed to keep them honest but inadvertently constitute a compliance cost for startups. Those regulations, such as the burdensome reporting and capital requirements that the New York State Department of Financial Services' "BitLicense" imposed on cryptocurrency remittance startups, become barriers to entry that protect incumbents.

But here's the thing: the open-source nature of blockchain technology, the excitement it has generated, and the rising value of the underlying tokens have encouraged a global pool of intelligent, impassioned, and financially motivated computer scientists to work on overcoming these limitations. It's reasonable to assume they will constantly improve the tech. Just as we've seen with internet software, open, extensible protocols such as these can become powerful platforms for innovation. Blockchain technology is moving way too fast for us to think later versions won't improve upon the present, whether it's in Bitcoin's cryptocurrency-based protocol, Ethereum's smart-contract-focused blockchain, or some as-yet-undiscovered platform.

The crypto bubble, like the dot-com bubble, is creating the infrastructure that will enable the technologies of the future to be built. But there's also a key difference. This time, the money being raised isn't underwriting *physical* infrastructure but *social* infrastructure. It's creating incentives to form global networks of collaborating developers, hive minds whose supply of interacting, iterative ideas is codified into lines of open-source software. That freely accessible code will enable the execution of countless as-yet-unimagined ideas. It is the foundation upon which the decentralized economy of the future will be built.

Just as few people in the mid-1990s could predict the later emergence of Google, Facebook, and Uber, we can't predict what blockchain-based applications will emerge from the wreckage of this bubble to dominate the decentralized future. But that's what you get with extensible platforms. Whether it's the open protocols of the internet or the blockchain's core components of algorithmic consensus and distributed record-keeping, their power lies in providing an entirely new paradigm for innovators ready to dream up and deploy world-changing applications. In this case, those applications—whatever shape they take—will be aimed squarely at disrupting many of the gatekeeping institutions that currently dominate our centralized economy.

Foundational inventions that change entire industries.

At Qualcomm, inventing comes first. When we connected the phone to the internet, our foundational inventions created the mobile revolution. Now, as we lead the world to 5G, our inventions are going to enable new industries to be created, and the next great product the world can't live without.

qualcomm.com/weinvent

Qualcomm

Inventing the tech the world loves

©2018 Qualcomm Technologies, Inc. and/or its affiliated companies. All Rights Reserved.
Qualcomm is a trademark of Qualcomm Incorporated, registered in the United States and other countries.

Block

By MIKE ORCUTT

What is it?

A public, permanent, append-only distributed ledger

What's that?

A mathematical structure for storing data in a way that is nearly impossible to fake. It can be used for all kinds of valuable data.

— Though some blockchains require permission to access, "open" blockchains like those underlying Bitcoin and Ethereum are accessible to anyone, meaning the database is public information.

— It's next to impossible for bad actors to tamper with data encoded in a blockchain, if it's properly set up.

— Old transactions can't be changed in a properly functioning blockchain; only new ones can be added.

— No single entity owns or controls a public blockchain. A network of computers maintains and secures the database, and each participant, or "node," stores a copy.

— The original blockchain, Bitcoin, is a ledger for tracking currency balances. But the same basic method can work for all kinds of digital assets.

chain:

Where did it come from?

"I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party." These are the words of Satoshi Nakamoto, the mysterious creator of Bitcoin, in a message sent to a cryptography-focused mailing list in October 2008. Included was a link to a nine-page white paper describing a technology that some are now convinced will disrupt the financial system.

Nakamoto mined the first bitcoins in January 2009, and with that, the cryptocurrency era was born. But while its origin is shadowy, the technology that made it possible, which we now call blockchain, did not arise out the blue. Nakamoto combined established cryptography tools with methods derived from decades of computer science research to enable a public network of participants who don't necessarily trust each other to agree, over and over, that a shared accounting ledger reflects the truth. This makes it virtually impossible for someone to spend the same bitcoin twice, solving a problem that had hindered previous attempts to create digital cash. And, crucially, it eliminates the need for a central authority to mediate electronic exchange of the currency.

Want to know how it works? Open here.

Bitcoin's popularity began to grow quickly in 2011, after a Gawker article exposed Silk Road, a Bitcoin-powered online drug marketplace. Imitators called "altcoins" began to emerge, often using Bitcoin's open-source code. Within two years, the total value of bitcoins in circulation had passed $1 billion.

Soon, technologists realized that blockchains could be used to track other things besides money. In 2013, 19-year-old Vitalik Buterin proposed Ethereum, which would record not only currency transactions but also the status of computer programs called smart contracts. Launched in 2015, Ethereum—and now a host of competitors and imitators—promises to make possible a new generation of applications that look and feel like today's web apps but are powered by decentralized cryptocurrency networks instead of a company's servers.

What is it for?

It's a new way of answering an old question: how can we create enough trust between one another to peacefully exchange something of value?

ENFORCEMENT

Early civilizations used threat of force as retribution for dealing in bad faith when engaging in trade.

INSTITUTIONS

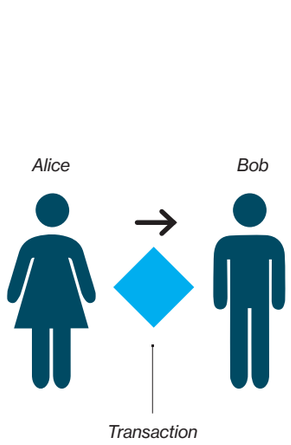
The emergence of governments and banks provided organized, central authorities to which we could outsource trust—as long as we trusted them.

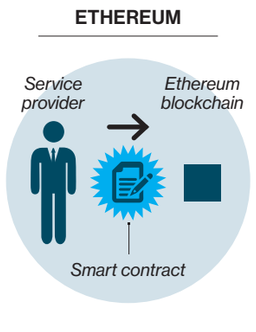
THE NETWORK

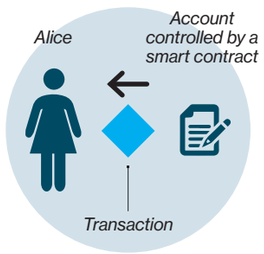
Blockchains distributed across thousands of computers can mechanize trust, opening the door to new ways of organizing "decentralized" enterprises and institutions.

1

A transaction is born





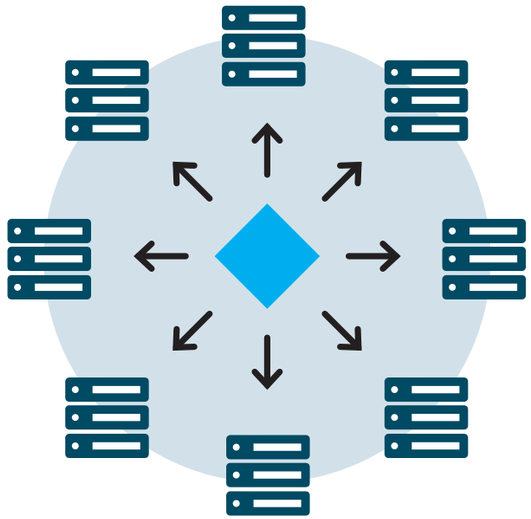


WHAT IS A TRANSACTION?

In Bitcoin, a transaction is the transfer of cryptocurrency from one person (Alice) to another (Bob). In Ethereum, which includes a built-in programming language that can be used to automate transactions, there are multiple kinds. Alice can send cryptocurrency to Bob. Or someone can create a transaction that places a line of code, called a smart contract, on the blockchain. Alice and Bob can then send money to an account this program controls, to trigger it to run if certain conditions encoded in the contract are met. A smart contract can also send transactions to the blockchain in which it is embedded.

2

The transaction is broadcast to a peer-to-peer network

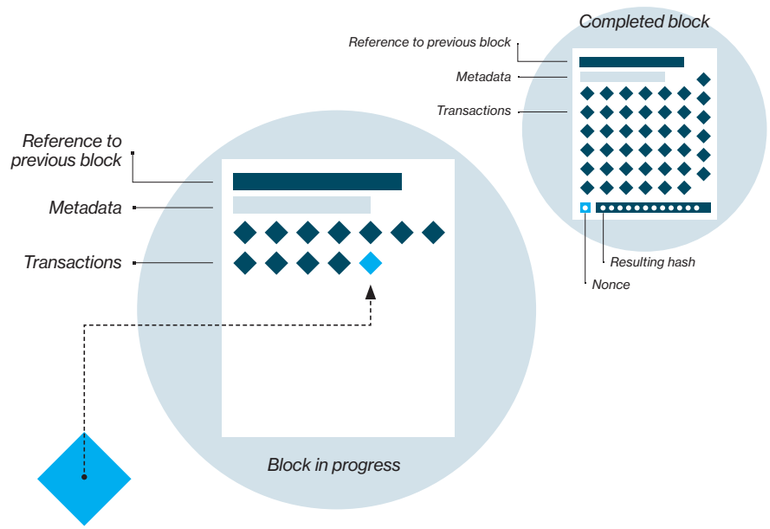


VERIFYING TRANSACTIONS

Let's say Alice wants to send some money to Bob. To do so, Alice creates a transaction on her computer that must reference a past transaction on the blockchain in which she received sufficient funds, as well as her private key to the funds and Bob's address. That transaction is then sent out to other computers, or "nodes," in the network. The nodes will validate the transaction as long as it has followed the appropriate rules. Then mining nodes (more on those in step 3) will accept it, and it will become part of a new block.

3

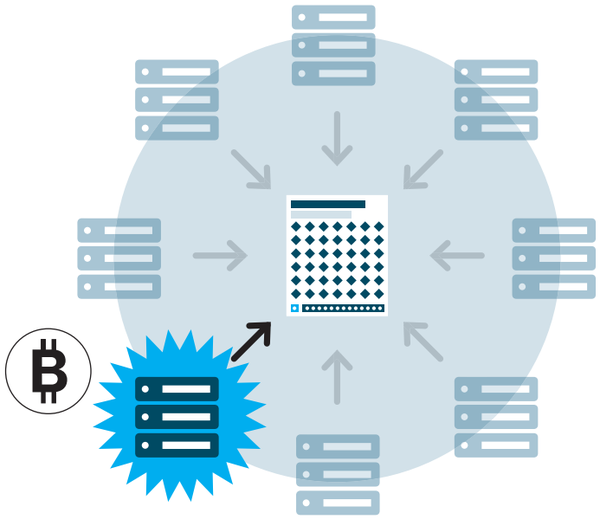
The race to create new blocks



MINERS COMPETE FOR CASH

A subset of nodes, called miners, organize valid transactions into lists called blocks. A block in progress contains a list of recent valid transactions and a cryptographic reference to the previous block. In blockchain systems like Bitcoin and Ethereum, miners race to complete new blocks, a process that requires solving a labor-intensive mathematical puzzle, which is unique to each new block. The first miner to solve the puzzle will earn some cryptocurrency as a reward. The math puzzle involves randomly guessing at a number called a nonce. The nonce is combined with the other data in the block to create an encrypted digital fingerprint, called a hash.

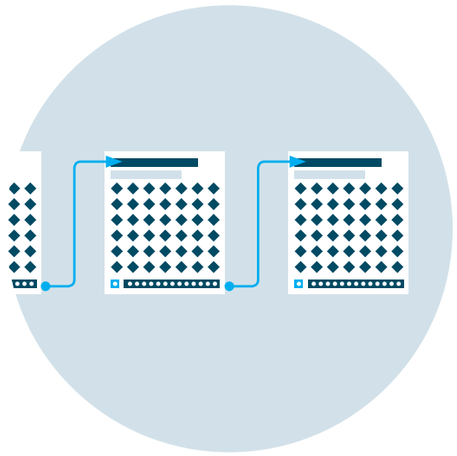
4 Completing a new block



YOU HAVE TO WORK FOR IT

The hash must meet certain conditions; if it doesn't, the miner tries another random nonce and calculates the hash again. It takes an enormous number of tries to find a valid hash. This process deters hackers by making it hard to modify the ledger. While some blockchain entities use other systems to secure their chains, this approach, called proof of work, is the most thoroughly battle-tested.

5 Adding a new block to the chain



ANOTHER LINK IN THE CHAIN

This is the final step in securing the ledger. When a mining node becomes the first to solve a new block's crypto-puzzle, it sends the block to the rest of the network for approval, earning digital tokens in reward. Mining difficulty is encoded in the blockchain's protocol; Bitcoin and Ethereum are designed to make it increasingly hard to solve a block over time. Since each block also contains a reference to the previous one, the blocks are mathematically chained together. Tampering with an earlier block would require repeating the proof of work for all the subsequent blocks in the chain.

This tech is about way more than money.

A whole host of industries could—emphasis on the "could"—be revolutionized by blockchains.

ENERGY

- **Why you should buy in:** Energy trading is a byzantine process riddled with middlemen taking cuts (the name "Enron" may ring a bell). Making energy resources into digital assets that can be traded on a blockchain could open new investing and trading opportunities, letting little guys in. Like, really little: down to an individual apartment building that generates excess solar power, or an electric vehicle with battery storage capacity to spare. For larger companies, a blockchain could streamline trading and record-keeping. The result could involve whole new asset classes, like crypto-tokens backed by oil or renewable resources.
- **The fine print:** Of late, the power grid has become a target for state-sponsored hackers. Securing all that transaction data will be a complicated cybersecurity challenge.
- **Players:** Power Ledger, Grid Singularity, Grid+, the Energy Web Foundation, the Enerchain project

INTERNET ADVERTISING & SOCIAL MEDIA

- **Why you should buy in:** If you could easily control your personal data and decide whether the likes of Facebook, Google, and others get to exploit it for profit, you would, right? Put it on a blockchain, which will encrypt and store your data in a decentralized network, instead of on company-owned servers. You can surf the internet anonymously, manage your own sensitive and identifying data, and control which sites can access it. Ahhhh, the internet as it was meant to be.
- **The fine print:** Despite revelations that big tech companies are pulling all manner of shenanigans with user data, people have yet to #deletefacebook or abandon web services in large numbers. The vision of a decentralized web could be a tough sell.
- **Players:** Blockstack, Protocol Labs

FOOD & AGRICULTURE

- **Why you should buy in:** How do you know if that meat you bought is *really* grass-fed, organic, and free of antibiotics and has never been anywhere near a cage or feedlot? You don't—unless a blockchain tells you so. Having a digital ledger that no one can mess with means everything from turkeys to chocolate to mangoes can be tracked literally from farm to table—or at least to the grocery store shelf. And if something does go wrong, a blockchain can cut the time it takes to track, and stop, the spread of a foodborne illness.
- **The fine print:** A few pilot projects have been tried, but that's it so far. A large-scale system would probably mean giving farmers, distributors, and others keys to access and modify the blockchain, and we'd have to trust that they wouldn't misuse them.
- **Players:** IBM, Walmart, Nestlé, Unilever, Cargill

MEDICINE

- **Why you should buy in:** Sharing x-rays, blood test results, and other intensely private medical data is no easy task, and there are piles of regulations, differing data formats, and other hurdles to contend with besides. A blockchain could provide a tamper-proof record of important events like prescription refills, while smart contracts could give patients precise control over who can access which parts of their medical record and when, without all the red tape.
- **The fine print:** Hospitals, clinics, doctor's offices, pharmacies, insurers ... the list of who may need access to your medical records is long. Who should be allowed to change the record? Who will run the computer network that runs the blockchain? How will the system be governed?
- **Players:** MIT's MedRec project, Massachusetts General Hospital, Kaiser Permanente, IBM, the Medilledger Project, SimplyVital Health

ELECTIONS

- **Why you should buy in:** The proliferation of electronic voting systems and the practice of keeping sensitive information like voter rolls in internet-connected databases translate to one thing: risk that an election could be compromised. Distributed ledgers could, in theory, make electronic voting as secure as any physical paper trail.
- **The fine print:** There are many more tough questions than easy answers. Will votes be recorded on a public blockchain like those used by Bitcoin or Ethereum? If so, how will ballots be kept anonymous? If it's done on a permissioned system, how do we make sure people don't misuse their access?
- **Players:** Agora, Voatz, Democracy Earth

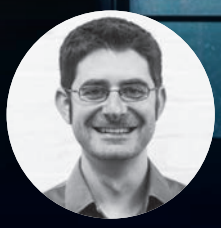
When robots are your colleagues,

which human skills will still matter?

Meet the innovators at the center of this transformation, including:

Jessica Brillhart
Director, Vrai Pictures

Jason Furman
Professor, Harvard Kennedy School, Former Chief Economist, Obama Administration



Greg Mark
Founder and CEO, Markforged

Julie Shah
Associate Professor, MIT

Brad Smith
President, Microsoft

The Future of Work
June 4-5, 2018
Cambridge, MA
technologyreview.com/events

MIT Technology Review

EmTech NEXT

We have a few words for you

A → Z

If you don't know the terminology, blockchain can seem either baffling or boring. Here's a guide to help you make sense of it all.

Alt-coin / A **cryptocurrency** that works similarly to Bitcoin but with modifications such as being able to process transactions faster.

Blockchain / A structure for storing data in which groups of valid transactions, called **blocks,** form a chronological chain, with each block cryptographically linked to the previous one.

Consensus protocol / A process, encoded in software, by which computers in a network, called **nodes**, reach an agreement about a set of data.

Cryptocurrency (or crypto-token) / A scarce digital asset defined by a **blockchain** protocol and exchanged via that blockchain system.

Decentralization / A hard-to-quantify measure of a network's resistance to attack, a function of how broadly control is distributed among different actors.

Distributed ledger technology (DLT) / A system, most commonly a **blockchain**, for creating a shared, cryptographically secured database.

Fork / A change to the way a **blockchain**'s software rules define valid transactions, or **blocks.** / ***Hard fork:*** A change to the rules that all **nodes** on a network must adopt, or else leave the network**.** / ***Soft fork:*** A backwards-compatible change that hinges only on a majority of nodes' adopting the new rules.

Hash function / A cryptography tool that turns any input into a string of characters that serves as a virtually unforgeable digital fingerprint of the data, called a **hash**.

Initial coin offering (ICO) / A blockchain-based fund-raising mechanism in which entrepreneurs mint new **crypto-tokens** and sell them to investors.

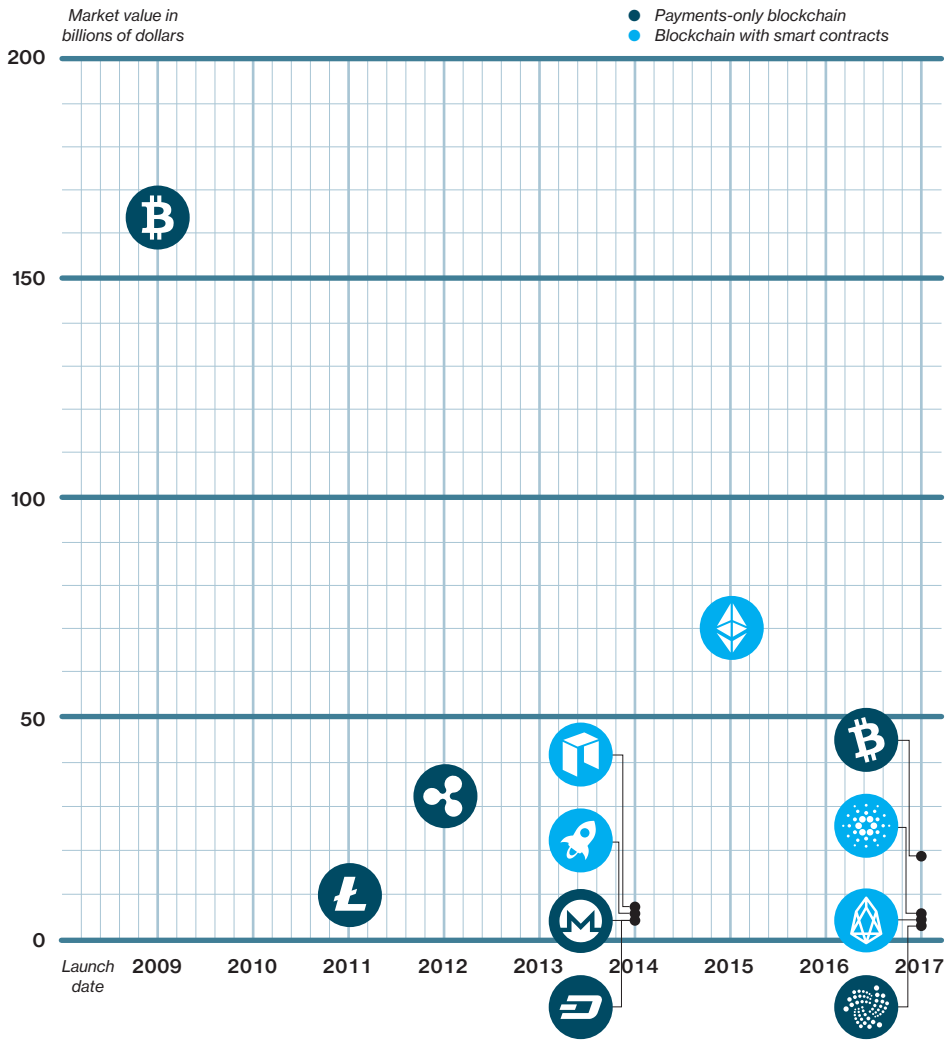
Mining / The process by which **nodes** in Bitcoin, Ethereum, and many other **blockchain** systems (those that use the **consensus protocol** known as **proof of work**) add new **blocks** to their respective chains and generate new **crypto-tokens**.

Permissioned blockchain / A shared database with a **blockchain** structure that requires participants to obtain permission before reading or writing to the chain. Contrast this with **permissionless** blockchains, which anyone can join.

Proof of stake / A novel **consensus protocol** in which, instead of **mining**, nodes can validate and make changes to the **blockchain** on the basis of their existing economic stake.

Proof of work / The **consensus protocol** of choice for Bitcoin and many other **cryptocurrencies**. To add a new block, miners must calculate a **hash** for it that meets certain narrow criteria. Doing so requires an enormous number of random guesses, making it a costly process that deters attempts to commit fraud.

Smart contract / A computer program stored in a **blockchain** that automatically moves digital assets between accounts if conditions encoded in the program are met. It serves as a way to create a mathematically guaranteed promise between two parties.



Cryptocurrencies are not created equal

Each of the top 12 digital "coins" stands for a digital asset. Every one is unique, but they have one thing in common: investors think they're worth billions. (The market values are as of mid-March.)

By MIKE ORCUTT

BITCOIN (BTC)

Launched: 2009
Market value: $163 billion
The strengths: The original cryptocurrency, Bitcoin is the largest and most popular blockchain network – and the most battle-tested against attackers.
The downside: Growing demand has stressed Bitcoin's network, making transactions expensive. The system, which can process only about seven transactions per second, nonetheless guzzles electricity owing to its consensus protocol, proof of work, designed to make mining labor-intensive.

ETHEREUM (ETH)

Launched: 2015
Market value: $70 billion
The strengths: A built-in programming language lets developers write computer programs, called smart contracts, that run on the blockchain. Most initial coin offerings (ICOs) so far have been based on Ethereum smart contracts.
The downside: Ethereum also uses proof of work, making it relatively slow and energy-hungry. Many early smart contracts are vulnerable to hacking, and the field of smart-contract security is immature.

RIPPLE (XRP)

Launched: 2012
Market value: $32 billion
The strengths: Ripple says its crypto-token, called XRP, can be a "bridge currency" that financial institutions use to settle cross-border payments faster and more cheaply than they do now. It uses a novel consensus protocol that allows for much faster transactions than Bitcoin and Ethereum.
The downside: Since Ripple, a privately owned company, has so much control over the system, purists say XRP isn't decentralized enough – in contrast with Bitcoin, which anybody can mine.

ALL REPORTED MARKET VALUES ARE AS OF MARCH 12, 2018; SOURCE OF MARKET VALUE DATA (SORT BY "CURRENT MARKETCAP"): HTTPS://ONCHAINFX.COM/

BITCOIN CASH (BCH)

Launched: 2017
Market value: $19 billion
The strengths: The creators of this currency, the product of a "hard fork" of Bitcoin, tweaked Bitcoin's software to handle larger transaction volumes.
The downside: Critics say Bitcoin Cash is too centralized – a handful of miners create most of the coins.

NEO (NEO)

Launched: 2014
Market value: $5.8 billion
The strengths: China's biggest cryptocurrency, NEO is a smart-contract platform with goals similar to Ethereum's. It uses a consensus protocol called delegated Byzantine fault tolerance, which NEO's creators say allows for 10,000 transactions per second, compared with Ethereum's 15.
The downside: NEO is highly centralized, and it's not clear that this will ever change. The founder has said that the plan is to make it more decentralized "someday."

MONERO (XMR)

Launched: 2014
Market value: $4.3 billion
The strengths: Monero uses ring signatures, a type of digital signature that lets any member of a group perform a transaction without revealing which one of them it was. It's a way to let users transact privately, and its mining process is designed to be "egalitarian."
The downside: Monero's features have made it a preferred coin among cybercriminals, and it has helped fuel the rise of "cryptojacking," in which hackers use malware to make other people's computers mine cryptocurrency for them.

LITECOIN (LTC)

Launched: 2011
Market value: $10 billion
The strengths: Litecoin is an "alt-coin" – nearly a clone of Bitcoin, but with a few alterations. It processes transactions four times faster, and its mining process is designed to remain open to hobbyists – not the case with Bitcoin, in which professional miners use expensive hardware.
The downside: Though faster than Bitcoin, Litecoin is still too slow and energy-hungry to be an ideal payment method, and it has the added handicap of being far less well-known.

STELLAR LUMENS (XLM)

Launched: 2014
Market value: $5.6 billion
The strengths: Stellar, whose ledger is a hard fork of Ripple's, likewise aims for its lumens to be a bridge currency for cross-border payments – only it's run by a nonprofit, instead of a for-profit company. It also plans to compete with Ethereum as a platform for initial coin offerings.
The downside: Stellar faces a lot of competition, from both Ripple and the traditional banking system's dominant platform, SWIFT, which is testing distributed-ledger technology with blockchain-ish elements.

DASH (DASH)

Launched: 2014
(formerly XCoin and Darkcoin)
Market value: $4.3 billion
The strengths: Another so-called privacy coin like Monero, Dash is inspired by Bitcoin but has features that speed up payment processing.
The downside: Like some others, Dash has a centralization problem. Because of a mishap, too many coins were distributed when it was first released, concentrating the wealth and giving a small group disproportionate power in decisions over the currency's future.

CARDANO (ADA)

Launched: 2017
Market value: $5.9 billion
The strengths: Cardano's creators say the system, which is still only a platform for trading and transferring its token, puts an emphasis on privacy and regulatory compliance. They also say it will eventually host smart contracts. In that way it will be like Ethereum – but it uses a proof-of-stake consensus protocol and thus gobbles up less energy.
The downside: Despite big claims from the developers, there's still very little information on Cardano.

EOS (EOS)

Launched: 2017
Market value: $4.3 billion
The strengths: EOS tokens exist and are currently traded on Ethereum, though the smart-contract platform itself, billed as yet another Ethereum killer, has yet to launch. Like Cardano, it will use a proof-of-stake protocol instead of proof of work, theoretically making transactions faster and more efficient.
The downside: Despite being on track to raise more than $1 billion via an ICO, the project is nearly impossible to judge before the network has launched.

IOTA (MIOTA)

Launched: 2017
Market value: 3.8 billion
The strengths: IOTA's system does not use a blockchain, instead employing a shared ledger based on a mathematical structure called a directed acyclic graph. It aims to be a currency used by internet-of-things devices to buy, sell, and trade data, whether the transaction partners are other devices or customers like technology companies.
The downside: Critics say IOTA is too centralized, and numerous cryptography researchers have questioned the system's overall security.

Bitcoin would be a calamity, not an economy

A cryptocurrency future sounds liberating. In reality, it would be a disaster for everybody.

By **JAMES SUROWIECKI**
Illustration by Daniel Zender

EARLIER THIS YEAR, JACK Dorsey, cofounder of Twitter and CEO of Square, declared that Bitcoin would become the world's "single currency" within a decade. What was striking about Dorsey's comment wasn't just the audacious prediction but also the notion that Bitcoin might be useful for something other than speculative investing. After all, even as the financial world has been gripped by cryptocurrency mania over the last year, the "currency" part of cryptocurrencies has receded in importance in the public eye. As a Goldman Sachs executive put it last year, Bitcoin is, at the moment, more of an asset than a currency—it's something people trade, like a stock or bond, rather than something they exchange for goods and services.

That perception reflects reality. The number of Bitcoin transactions (as opposed to trades) has not risen much in the last few years, and one recent academic study suggested that half of those transactions are associated with illicit activity. As a medium of exchange, Bitcoin remains today pretty much what it was in 2010: an interesting complement to the existing monetary system, primarily useful for people interested in avoiding legal authorities or living in societies racked by inflation (like, say, in Venezuela or Zimbabwe).

Still, the dream that cryptocurrency could replace our existing system of fiat money, in which the money supply is controlled by government-run central banks, remains a key part of Bitcoin's appeal. The promise is of a system where the government can't manipulate the money supply, and market competition determines which currencies people use. But what would happen if that dream came true? If the dollar and the euro were replaced by Bitcoin, how would the system adapt, and how would the economy and the financial system function?

The simple answer is: not well. Our economies and financial systems are built around fiat money, and they rely on the central bank's control of the currency (and the government's ability to issue debt in that currency) to help manage the business cycle, fight unemployment, and deal

with financial crises. An economy in which Bitcoin was the dominant currency would be a more volatile and harsher economy, in which the government would have limited tools to fight recessions and where financial panics, once started, would be hard to stop.

The opposite of what you want

To see why this is the case, it's key to recognize the crucial role that the central bank (which in the US is the Federal Reserve) plays to provide what economists call "liquidity" when the system needs it. That's just a fancy way of saying that the central bank can pump money into the system, either by printing it and then lending it to banks (with the idea that they will then inject that money into the system) or by simply buying assets itself. Providing liquidity is especially important in times of financial crisis, because crises lead banks to cut back on lending and savers to pull their money out of banks. In those times, the central bank serves as a lender of last resort, stepping in when otherwise solvent banks are struggling to stay afloat and ensuring that we don't end up with a flood of bank closings.

In an economy run on Bitcoin, these things would be impossible for a central bank to accomplish. A key aspect of the Bitcoin protocol is that the total number of bitcoins is capped at 21 million, after which no more will ever be issued. This makes Bitcoin appealing to many people because something that will never increase in supply is more likely to hold its value. The problem is that in the event of a crisis, there would also be no way to add liquidity to the system, since you can't "print" more bitcoins. The central bank could build up a stash of bitcoins that it could then funnel into the system, but that would do little good because people would know the stash was limited. And in any case, the central bank's demand for Bitcoin would drive up its price, which would make people more likely to hold onto it and less willing to spend it—the opposite of what you want in a financial crisis.

Bitcoin would also make it hard for governments to fight recessions, which they typically do by using what economists call countercyclical monetary and fiscal policy. Central banks slash interest rates, and—as the Federal Reserve did after the 2008 financial crisis—pump money into the system by buying assets (what's known as quantitative easing). And governments try to get the economy moving again by cutting taxes and increasing spending, typically paying for that by borrowing money, as with the Obama-era stimulus package.

Here again, a Bitcoin economy would limit the government's options. Since the central bank would have no control over the currency, it would also have no control over interest rates, and only a limited ability (depending on the size of its Bitcoin stash) to pour money into the economy. Fiscal policy, too, would be close to impotent. Today, when the government runs a deficit, it can have the Fed print money and then borrow that money from the Fed. That adds liquidity to the system. In the Bitcoin world, the government would have to borrow bitcoins to spend. And again, this would make bitcoins more valuable, making people less willing to spend them—the opposite of what you need to fight a recession.

But don't worry about it

The good news is that it's an incredibly unlikely future. While the idea of making Bitcoin a universal currency may have impeccable logic to digital-age utopians, in practice it makes little sense. And the design of Bitcoin also makes it difficult to imagine. Since the supply of bitcoins is limited, if the demand for them rises, their value rises, too. But that means that if you own bitcoins, and you think they're going to become more popular, then the sensible thing to do is hold them, since they'll be more valuable tomorrow. That makes people less interested in using bitcoins to actually buy stuff and more interested in treating them as speculative investments—the opposite of what you want in a medium of exchange.

You might think that the same restrictions on supply were true of gold when economies were run on the gold standard. But the supply of gold wasn't fixed. It expanded as people mined more of it. There actually was something of an equilibrium—as economic growth increased the demand for gold, making it more valuable, the rising price encouraged people to mine it, which brought more gold into the system, ultimately keeping the dollar value of gold relatively stable. Between 1800 and 1900, the dollar value of gold gradually rose by small percentages. Bitcoin, by contrast, regularly rises and falls 5 or 10 percent in a single day, purely because of shifts in speculative sentiment. That volatility weakens its usefulness as a store of value (one of the other roles of a currency) and makes it unsuitable for use as a day-to-day medium of exchange, since no one wants to accept a currency if it might be worth 10 percent less a couple of hours from now. In other words, a financial system run on Bitcoin would have all the bad features of the gold standard and few of the redeeming ones.

There are also practical hurdles to making Bitcoin a currency people can use easily. When demand for Bitcoin is high, transaction fees soar as miners raise the price of processing those transactions. At the peak of Bitcoin mania last fall, it could cost as much as $55 a transaction. That was fine when people thought the value of their Bitcoin stash was going to double overnight. But it doesn't work if people want to use Bitcoin to buy pizza or

This doesn't mean cryptocurrencies are useless. Buying drugs, money laundering: these are situations where they can come in handy.

a new TV set. Even more important, Bitcoin cannot scale to deal with the number of transactions a modern economy needs. The system is limited to processing just 420 transactions per minute. Finally, there's the fact that a remarkably small number of people control a remarkably large percentage of all the bitcoins in the world. That gives them the leverage to manipulate prices, and makes it harder for Bitcoin to have the reach it would need to become a real currency.

Choose your own currency!

Of course, Bitcoin is far from the only cryptocurrency. Depending on how you count, there are now hundreds, if not thousands, of them. And while they're all built, like Bitcoin, on the blockchain, some have features that might seem to make them more attractive as a potential global currency. Litecoin, for instance, can process more transactions per minute. Monero and Zcash offer genuine anonymity (as opposed to Bitcoin, where every transaction is associated with a given key that can be tracked). And not all cryptocurrencies have a rigid cap on the total number of coins. So perhaps a different cryptocurrency could replace the dollar or euro or yuan—or, more plausibly, we could end up with a system of lots of different private currencies, rather than relying solely on a single medium of exchange.

There's something appealing about the idea of everyone choosing the currency that suits them best, and of cryptocurrencies competing against each other to win the loyalty of consumers and businesses. But in fact the proliferation of cryptocurrencies that we've seen over the past few years makes it less likely, not more, that they will eventually replace fiat money.

The problem with a world in which there are lots of different private currencies is that it massively increases transaction costs. With a single, government-issued currency that's legal tender, you don't have to think about whether or not to accept it in exchange for goods and services. You accept dollars because you know that you will be able to use them to buy whatever you want. Commerce flows more smoothly because everyone has implicitly agreed to use the dollar.

In an economy with lots of competing currencies (particularly cryptocurrencies unbacked by any commodity), it would work very differently. If someone wants to pay you in Litecoin, you have to figure out whether you think Litecoin is a real cryptocurrency or just a scam that could shut down any day now. You have to consider who else might accept Litecoin if you want to spend it, or who would trade you dollars for it (and at what exchange rate and transaction fee). Basically, a proliferation of currencies tosses sand into the gears of commerce, making transactions less efficient and more costly. And any currency that is hard to use is less valuable as a medium of exchange.

Still great for money laundering

This isn't speculative. We actually have a historical example of how this works. In the United States in the decades before the Civil War, there was no national currency. Instead, it was an era of what was called "free banking." Individual banks issued bank notes, theoretically backed by gold, that people used as money. The problem was that the farther away from a bank you got, the less recognizable (and therefore the less trustworthy) a bank's note was to people. And every time you did a deal, you had to vet the note to make sure it was worth what your trading partner said it was worth. So-called wildcat banks sprang up, took people's money, issued a host of notes, and then shut down, making their notes worthless. To be sure, people came up with workarounds—there were volumes that were a kind of Yelp for banking, displaying the panoply of bank notes and rating them for reliability and value. But the broader consequence was that doing business was simply more complicated and slower than it otherwise would have been. The same will be true in a world where some people use Ethereum, others use Litecoin, and others use Ripple.

That doesn't mean that cryptocurrencies are useless. On the contrary, for transactions that one wants to keep hidden from the government (or other authorities), they will remain useful. Buying drugs, laundering money, evading capital controls, protecting your money in countries with hyperinflationary environments: these are all situations where cryptocurrencies can come in handy. But the notion that private cryptocurrencies might soon (or ever) be a meaningful competitor to fiat money for everyday transactions is little more than a pipe dream.

James Surowiecki is the author of The Wisdom of Crowds *and a senior story producer at* Vice News Tonight.

YOUR FUTURE BEGINS NOW

Access the future with the authority on cutting-edge technology

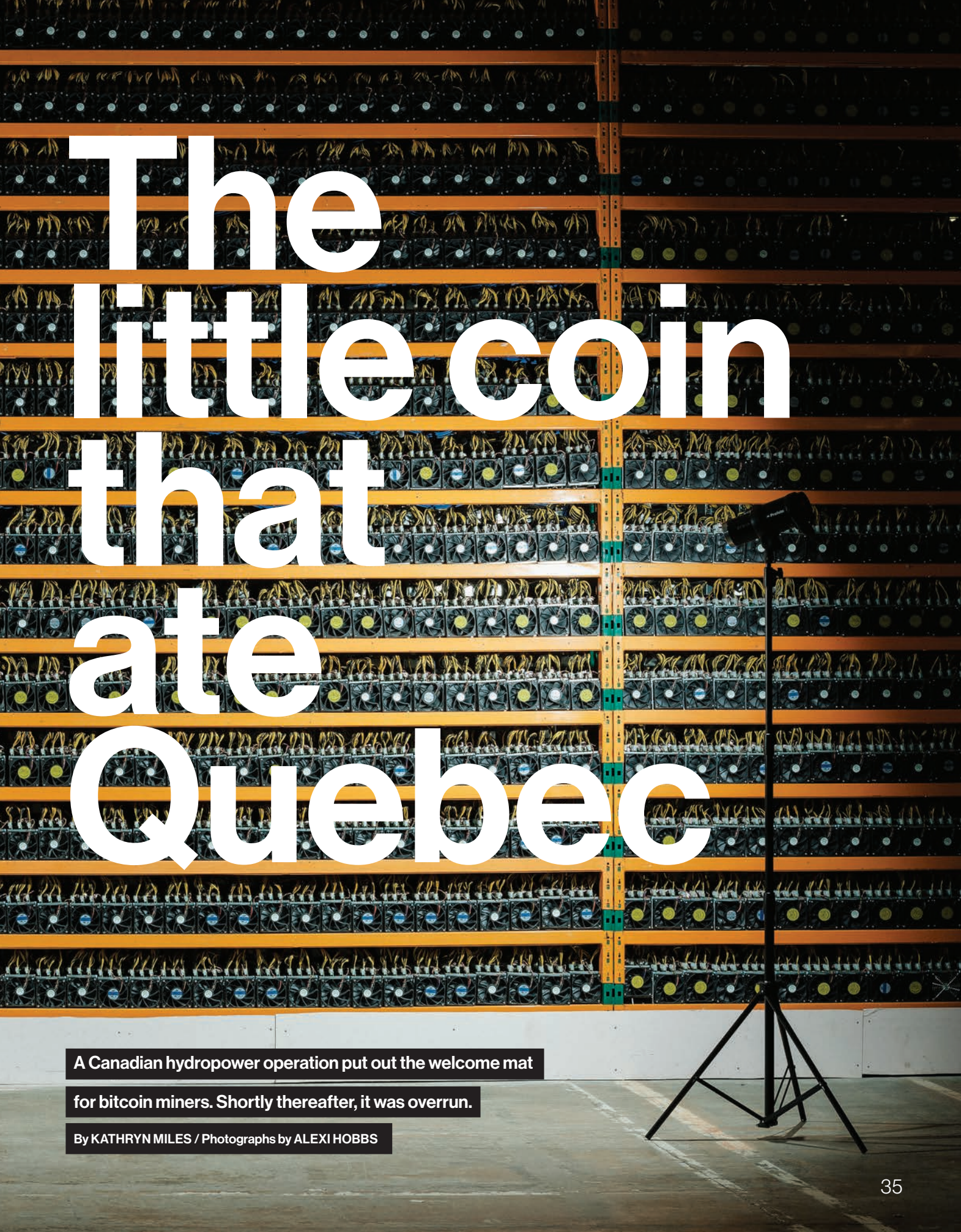
SUBSCRIBE TODAY
technologyreview.com/now

MIT Technology Review

2

WHERE WE ARE Now

Bitcoin mining is wrecking the environment. Blockchains could help refugees get their lives back. China's crackdown and its unexpected consequences. The cyber-sleuths hunting down crypto-criminals. Why "Is the crypto world sexist?" is the wrong question to ask. Plus: portraits of blockchain's often unlikely true believers.



The little coin that ate Quebec

A Canadian hydropower operation put out the welcome mat for bitcoin miners. Shortly thereafter, it was overrun.

By KATHRYN MILES / Photographs by ALEXI HOBBS

At first glance, nothing looks particularly cutting-edge about this aging industrial park in Saint-Hyacinthe, Quebec, about 60 miles east of Montreal. The air is thick with the smell of roasting cacao, which billows from a massive chocolate factory and seeps into tractor-trailers and forgotten offices. Nearby, an audiovisual repair shop and an agricultural lab specializing in the detection of livestock pathogens vie for space with a massive disused dairy processing plant. Tucked behind all three sits a worn, low-slung building that previously served as a warehouse for a soup company and, before that, a factory producing diapers. You might think it, too, had since been forgotten, were it not for the plastic sheeting hinting at new construction inside and the small fleet of shining company cars stationed in the parking lot. But the biggest clue of all that something both new and decidedly high-tech is happening here can be heard while standing next to those cars: an omnipresent hum, audible well outside the building, created by thousands of computers, each one completing the same singular task again and again and again, day after day, without change or interruption.

These computers are the property of Bitfarms, one of North America's largest cryptocurrency mining operations. Here in the once-abandoned factory, about 7,000 shoebox-size machines (as of April, but that's expected to rise to 14,000 by July) sit tightly shelved in a single floor-to-ceiling row that bisects the building. On one side of the stacks, a mess of wires and routers exiting the rear of each computer sits exposed to the cold Canadian air. On the other, thousands of identical fans roar as they push hot air past a heap of empty cardboard boxes and into the otherwise vacant space. A handful of busy employees move between the two sides wearing thin T-shirts and jeans, their faces flushed. Even on a raw, gray day, the heat on the fan side is stifling.

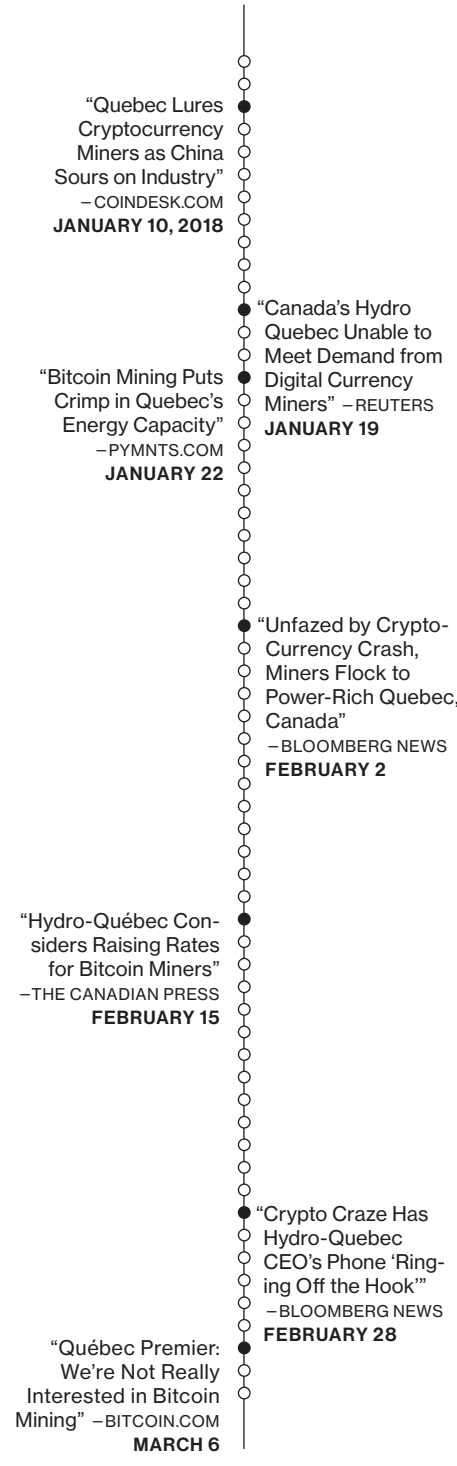
These computers, often called "rigs," are purpose-built. Able to withstand dramatic shifts in temperature and humidity, they are singularly programmed not only to perform just one computation trillions of times each second, but to repeat those computations around the clock and without pause. They are also energy hogs: the 7,000 in Saint-Hyacinthe alone consistently draw more energy than the Montreal Canadiens' nearby hockey arena, even on a sold-out game night.

Globally, millions of these computers are in operation, part of the cryptocurrency boom that began in 2009. In the decade since the inception of Bitcoin, most of this mining work has occurred in countries like China and Romania, which offer plentiful electricity and little regulation. In 2016, Hydro-Québec announced a formal plan to woo data centers like those run by Microsoft and Amazon. Cryptocurrency miners also came calling, and began submitting proposals in September 2017. Interest from them soon became overwhelming, with more requests than the power company could accommodate. Were Quebec to accept even a fraction of them, the province could well become the new global hub of cryptocurrency mining. That has raised questions about how well Hydro-Québec's grid can sustain these energy demands, particularly in the winter. Meanwhile, environmentalists and social-justice advocates worry about the ecological and cultural impact of this campaign. And that, in turn, raises difficult ethical questions about the real value of a wholly virtual currency.

Worthless puzzles

Cryptocurrencies are energy-intensive by their very nature. As decentralized ledger systems, of which Bitcoin is the largest, most rely for their security on an approach known as "proof of work." About every 10 minutes, Bitcoin releases new currency in exchange for successfully solving compu-

A flash flood of miners



tational problems that verify a "block" of transactions. Participants do this by converting the data representing those transactions into a sequence of code known as a "hash," trying again and again until they arrive at one that meets certain criteria. And while it doesn't require an immense degree of sophistication—insiders liken the process to guessing lottery numbers—it does require an immense quantity of wrong guesses.

"You're essentially solving worthless puzzles that we cannot solve mathematically," says Christian Catalini, associate professor of technological innovation at MIT and founder of the university's Cryptoeconomics Lab. "You can only brute-force your way into it." And the muscle behind that force comes in the form of electricity used to power miners' computers.

Resource intensiveness is inherent in a decentralized system like Bitcoin's, says Catalini, because it is based on a fundamental lack of trust between participants. Instead of being guaranteed by a central bank like, say, the US Federal Reserve, cryptocurrencies like Bitcoin combat fraud by making all transactions transparent and verifiable by all participants. Attempts to tamper with such a ledger must be made self-defeating.

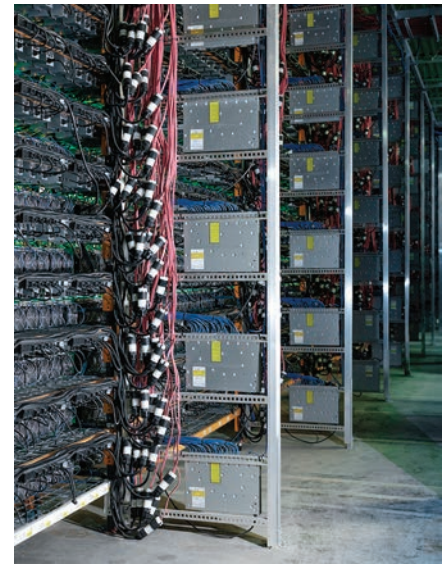
"Basically, you're placing an economic cost between a user and an attacker," says Catalini. "If someone wants to subvert the system by faking a transaction, or revert a legitimate transaction, they would have to expend a tremendously high amount of energy and computation—to the point that no rational economic actor would do that, because the cost of doing an attack would be far greater than the benefit."

But that means legitimate transactions must also expend extensive energy to prove their validity.

David Malone is a senior lecturer at Ireland's Maynooth University, where he specializes in the mathematical modeling of network systems. The current global Bitcoin hash rate, which is to say the total number of mining computations, is approximately 25,000,000,000,000,000,000 per second, or 25 million terahashes a second. That's an increase from 300,000 terahashes a second just four years ago, and the figure is expected to continue growing in the months and years to come. Factor in additional energy consumption required to cool the computers (they can't function in temperatures over 40 °C), and Malone estimates that Bitcoin alone is consuming as much electricity as the entire nation of Ireland at any given moment. And while Bitcoin is the largest proof-of-work cryptocurrency, it's far from the only game in town: at last count, there were nearly 1,500 in operation, each with its own energy demands.

Without a doubt, electricity is the single greatest expense for any mining operation. And so, to be profitable, farms must be able to source power on the cheap. That's a big reason why China has led the mining boom: its electricity rates are as low as nine cents per kilowatt-hour. But increasing government regulation and concern that grid resources could run out have many miners there looking for other places to set up shop. Growing concerns about China's contribution to climate change only hastened that exodus, as mining companies sought to promote their operations to potential investors as environmentally friendly.

For years now, China has led the world in greenhouse-gas emissions. That's partly because it is the most populous nation. However, it's also because China generates most of its electricity using coal, which is one of the dirtiest forms of energy. The United States, currently the second most popular country for cryptocurrency mining, also gets the majority of its electricity from fossil fuels. Add in the rest of the mining operations around the world, and the industry emits about 29,000 kilotons of carbon a year, according to Digiconomist, the leading clearinghouse of cryptocurrency and energy concerns. That's more than is produced annually by Afghanistan, Croatia, Kenya, or Panama.



The wires and routers behind each computer sit exposed to the cold Canadian air.

It's also a big reason why Pierre-Luc Quimper, the founder of Bitfarms, located all five of his mining operations in Quebec, where he could rely on hydropower to fuel his 20,000 computers. Quimper and his colleagues at Bitfarms had been involved with cryptocurrency in a variety of capacities since 2009. They joined forces and established both the company and their mining facilities in late 2017—just in time for the Quebec boom.

"We use a lot of energy," says Quimper. "It has to be clean. If we have a footprint on the environment, that's bad."

Hydro-Québec touted its hydroelectric power as the ideal solution: a clean, renewable source of energy that can be supplied in massive quantities.

It contends that the energy it provides to cryptocurrency mining operations is "surplus"—an extra 100 terawatts of low-impact energy the utility has the capacity to generates over the next decade.

But the claim that this energy is green has come under increasing scrutiny, particularly from conservation biologists. They say the impact is far too high for any additional industry, let alone one that produces nothing but bitcoins.

Millions of acres under water

Hydroelectric power, which uses moving water to turn turbines that generate electricity, is undeniably cleaner than coal and other electricity generated by fossil fuels. Nevertheless, it, too, produces demonstrable environmental impacts. One of the biggest is the damage created by the reservoirs built to hold a ready supply of water. In places like Quebec, these reservoirs often overtake existing forests, which are some of the planet's most efficient converters and bankers of carbon. And as trees rot underwater, they release the carbon they've stored as methane—a far more potent greenhouse gas than carbon dioxide.

"You're putting hundreds of thousands and eventually millions of acres under water," says Jeff Wells, a conservation biologist and researcher at Cornell University. He was the lead author of a 2011 study into the effects of industrialization on northern forests. "You're putting a greenhouse gas in the atmosphere and stopping the ability of that area to take any more carbon into the system," he adds. "You've lost a whole ecosystem."

Researchers have calculated the carbon impact of hydroelectricity worldwide. Their estimates suggest that if all cryptocurrency mining were to move to this power source, the industry would still generate over 9,000 kilotons of carbon dioxide each year, plus more than 150 kilotons of methane.

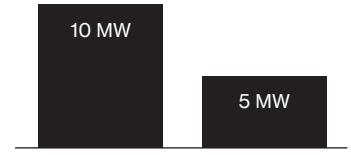
And while hydroelectric operations in cooler climates tend to release less carbon and methane than their tropical counterparts, they come with their own unique environmental price tags. The northern ecosystems known as boreal forests don't just sequester carbon. Their rivers supply the water that forms the bulk of Arctic sea ice and are believed to be responsible for key ocean currents that transport water and define global weather patterns. Because dams like the ones maintained by Hydro-Québec tend to be far away from population centers, they also require extensive installations of transmission lines and transformers. Those, in turn, can disrupt wildlife habitats, kill birds, and introduce invasive species.

Marc-Antoine Pouliot, a spokesperson for Hydro-Québec, assured me that full environmental impact studies are completed before any new dam construction is begun. He said the utility runs a complete analysis of any new blockchain operation, and if any updates to the grid are required, the company is responsible for funding them. The only concern, he said, is how to manage the constant energy draw of these operations during existing peak usage times—like Canadian winters.

"In Quebec, residential customers heat their homes with electricity. In consequence, the demand can be very high when the temperature is below -20 °C for a few days," he said. "We are now analyzing the effect of the blockchain on our winter peak. One of the solutions could be to oblige blockchain companies to suspend the activity during the winter."

In an industry where every day can be worth tens of thousands of dollars or more, it's pretty unlikely that miners would be amenable to that kind of solution.

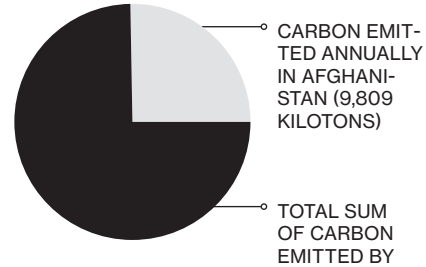
Wells would like to see fewer massive dam complexes, not more. "I already start



25,000,000,000,000,000,000

(25 MILLION TERAHASHES)

The approximate total number of computations per second devoted to bitcoin mining



INFO FROM THE WORLD BANK AND DIGICONOMIST; AFGHANISTAN FIGURE IS FROM 2014

This self-contained pod is designed to cut down on the cooling needs of crypto-mining.

off with the idea that it's not a good idea to destroy a working system that is literally part of the life support of the planet," he says. "There are fewer and fewer of those places left. To do it for cryptocurrency or some speculative technology seems completely reckless."

But miners like Quimper take issue with the idea that cryptocurrency is unproven or a passing experiment. Blockchain, he says, like network servers and the internet itself, is clearly here to stay. And fueling it with hydropower remains the most environmentally responsible way to meet the skyrocketing interest in applications like cryptocurrency. He points to additional benefits provided by companies like his: Bitfarms' five operations each reclaimed otherwise abandoned and decaying warehouses and factories in communities throughout Quebec. They've injected resources into the local economy and employed residents to work there.

And more innovation, he promises, is on the horizon to further offset carbon emissions.

Not far from the Bitfarms Saint-Hyacinthe mining operation, a small startup company called K.E. Inc. is looking to change where and how cryptocurrency is mined in North America. Its founder, Fooad Nejad, cut his teeth in cooling systems for data centers. When new mining operations began contacting him to create efficient cooling for their farms, he developed self-contained modular shells that can accommodate up to 1,200 computers. The computers still require the same amount of energy, says Nejad, but a recirculating ventilation system cuts down on heating and cooling needs. The pods, which resemble shipping containers, can be set up anywhere and don't require retrofitting or other costs associated with rewiring old buildings. They can also be easily adapted to channel the heat produced by the computers. Nejad says it's not a stretch to imagine them heating buildings or allowing greenhouses to grow warm-weather crops like tomatoes and strawberries year-round, even in Quebec.

Empty cardboard boxes

So just how big an impact will blockchain applications like cryptocurrency continue to make on our planet? That depends on whether future blockchains continue to use the energy-devouring proof-of-work approach.

One alternative is known as "proof of stake." Rather than asking people to solve resource-intensive computational puzzles, a proof-of-stake system requires issuers to put up capital as a guarantee. Late last year, the blockchain consortium Ethereum announced plans to convert to a proof-of-stake system for its cryptocurrency mining. If successful, it will be the first of its kind and could well lead to an industry shift away from proof of work.

Even if that doesn't happen, the amount of energy required to fuel major cryptocurrency operations like Bitcoin will eventually drop as all the coins move into circulation and energy-intensive mining is replaced with mere transaction monitoring.

But until then, operations like Bitfarms continue to grow. Those heaps of empty cardboard boxes back at the Saint-Hyacinthe former diaper factory? They exist because the company is adding computers so fast its employees don't have time to break down and recycle the packaging.

Kathryn Miles is a freelance writer and the author of four books, including Quakeland: On the Road to America's Next Devastating Earthquake.

Q:

How secure is a blockchain, really?

A:

It turns out "secure" is a funny word to pin down.

By MIKE ORCUTT

The whole point of using a blockchain is to let people—in particular, people who don't trust one another—share valuable data in a secure, tamperproof way. That's because blockchains store data using sophisticated math and innovative software rules that are extremely difficult for attackers to manipulate. But the security of even the best-designed blockchain systems can fail in places where the fancy math and software rules come into contact with humans, who are skilled cheaters, in the real world, where things can get messy.

To understand why, start with what makes blockchains "secure" in principle. Bitcoin is a good example. In Bitcoin's blockchain, the shared data is the history of every Bitcoin transaction ever made: an accounting ledger. The ledger is stored in multiple copies on a network of computers, called "nodes." Each time someone submits a transaction to the ledger, the nodes check to make sure the transaction is valid—that whoever spent a bitcoin had a bitcoin to spend. A subset of them compete to package valid transactions into "blocks" and add them to a chain of previous ones. The owners of these nodes are called miners. Miners who successfully add new blocks to the chain earn bitcoins as a reward.

What makes this system theoretically tamperproof is two things: a cryptographic fingerprint unique to each block, and a "consensus protocol," the process by which the nodes in the network agree on a shared history.

The fingerprint, called a hash, takes a lot of computing time and energy to generate initially. It thus serves as proof that the miner who added the block to the blockchain did the computational work to earn a bitcoin reward (for this reason, Bitcoin is said to use a "proof-of-work" protocol). It also serves as a kind of seal, since altering the block would require generating a new hash. Verifying whether or not the hash matches its block, however, is easy, and once the nodes have done so they update their respective copies of the blockchain with the new block. This is the consensus protocol.

The final security element is that the hashes also serve as the links in the blockchain: each block includes the previous block's unique hash. So if you want to change an entry in the ledger retroactively, you have to calculate a new hash not only for the block it's in but also for every subsequent block. And you have to do this faster than the other nodes can add new blocks to the chain. So unless you have computers that are more powerful than the rest of the nodes combined (and even then, success isn't guaranteed), any blocks you add will conflict with existing ones, and the other nodes will automatically reject your alterations. This is what makes the blockchain tamperproof, or "immutable."

The security of even the best-designed blockchain systems can fail where the software rules come into contact with humans in the real world.

CREATIVE WAYS TO CHEAT

So much for the theory. Implementing it in practice is harder. The mere fact that a system works like Bitcoin—as many cryptocurrencies do—doesn't mean it's just as secure. Even when developers use tried-and-true cryptographic tools, it is easy to accidentally put them together in ways that are not secure, says Neha Narula, director of MIT's Digital Currency Initiative. Bitcoin has been around the longest, so it's the most thoroughly battle-tested.

People have also found creative ways to cheat. Emin Gün Sirer and his colleagues at Cornell University have shown that there is a way to subvert a blockchain even if you have less than half the mining power of the other miners. The details are somewhat technical, but essentially a "selfish miner" can gain an unfair advantage by fooling other nodes into wasting time on already-solved crypto-puzzles.

Another possibility is an "eclipse attack." Nodes on the blockchain must remain in constant communication in order to compare data. An attacker who manages to take control of one node's communications and fool it into accepting false data that appears to come from the rest of the network can trick it into wasting resources or confirming fake transactions.

Finally, no matter how tamperproof a blockchain protocol is, it "does not exist in a vacuum," says Sirer. The cryptocurrency hacks driving recent headlines are usually failures at places where blockchain systems connect with the real world—for example, in software clients and third-party applications.

Hackers can, for instance, break into "hot wallets," internet-connected applications for storing the private cryptographic keys that anyone who owns cryptocurrency requires in order to spend it. Wallets owned by online cryptocurrency exchanges have become prime targets. Many exchanges claim they keep most of their users' money in "cold" hardware wallets—storage devices disconnected from the internet. But as the January heist of more than $500 million worth of cryptocurrency from the Japan-based exchange Coincheck showed, that's not always the case.

Perhaps the most complicated touchpoints between blockchains and the real world are "smart contracts," which are computer programs stored in certain kinds of blockchain that can automate transactions. In 2016, hackers exploited an unforeseen quirk in a smart contract written on Ethereum's blockchain to steal 3.6 million ether, worth around $80 million at the time, from the Decentralized Autonomous Organization (DAO), a new kind of blockchain-based investment fund.

Since the DAO code lived on the blockchain, the Ethereum community had to push a controversial software upgrade called a "hard fork" to get the money back—essentially creating a new version of history in which the money was never stolen. Researchers are still developing methods for ensuring that smart contracts won't malfunction.

THE CENTRALIZATION QUESTION

One supposed security guarantee of a blockchain system is "decentralization." If copies of the blockchain are kept on a large and widely distributed network of nodes, there's no one weak point to attack, and it's hard for anyone to build up enough computing power to subvert the network. But recent work by Sirer and colleagues shows that neither Bitcoin nor Ethereum is as decentralized as you might think. They found that the top four bitcoin-mining operations had more than 53 percent of the system's average mining capacity per week. By the same measure, three Ethereum miners accounted for 61 percent.

Some say alternative consensus protocols, perhaps ones that don't rely on mining, could be more secure. But this hypothesis hasn't been tested at a large scale, and new protocols would likely have their own security problems.

Others see potential in blockchains that require permission to join, unlike in Bitcoin's case, where anyone who downloads the software can join the network. Such systems are anathema to the anti-hierarchical ethos of cryptocurrencies, but the approach appeals to financial and other institutions looking to exploit the advantages of a shared cryptographic database.

Permissioned systems, however, raise their own questions. Who has the authority to grant permission? How will the system ensure that the validators are who they say they are? A permissioned system may make its owners feel more secure, but it really just gives them more control, which means they can make changes whether or not other network participants agree—something true believers would see as violating the very idea of blockchain.

So in the end, "secure" ends up being very hard to define in the context of blockchains. Secure from whom? Secure for what? "It depends on your perspective," says Narula.

A customer pays for groceries at a supermarket in the Zaatari refugee camp.

The place where life hangs by a chain

A sprawling refugee camp in Jordan is an early test of whether blockchains can reinvent the way we own, control, and administer our legal identities in the 21st century.

Story and photographs BY RUSS JUSKALIAN

Syrian refugees could regain legal identities that were lost when they fled their homes.

A few times a month, Bassam pushes a shopping cart through the aisles of a grocery store stocked with bags of rice, a small selection of fresh vegetables, and other staples. Today he's wearing a black sweater tucked into denim jeans, which are themselves tucked into calf-high boots caked in mud. The Tazweed Supermarket, where he's shopping, is on the periphery of a 75,000-person refugee camp in the semi-arid Jordanian steppe, six and a half miles from the Syrian border.

At the checkout counter, a cashier tallies the total, but Bassam doesn't pay with cash or a credit card. Instead he lifts his head to a black box and gazes into the mirror and camera at its center. A moment later, an image of Bassam's eye flashes on the cashier's screen. Bassam collects his receipt—which reads "EyePay" and "World Food Programme Building Blocks" across the top—and walks out into the noonday chaos of the Zaatari refugee camp.

Though Bassam may not know it, his visit to the supermarket involves one of the first uses of blockchain for humanitarian aid. By letting a machine scan his iris, he confirmed his identity on a traditional United Nations database, queried a family account kept on a variant of the Ethereum blockchain by the World Food Programme (WFP), and settled his bill without opening his wallet.

Started in early 2017, Building Blocks, as the program is known, helps the WFP distribute cash-for-food aid to over 100,000 Syrian refugees in Jordan. By the end of this year, the program will cover all 500,000 refugees in the country. If the project succeeds, it could eventually speed the adoption of blockchain technologies at sister UN agencies and beyond.

Building Blocks was born of a need to save money. The WFP helps feed 80 million people around the globe, but since 2009 the organization has shifted from delivering food to transferring money to people who need food. This approach could feed more people, improve local economies, and increase transparency. But it also introduces a notable point of inefficiency: working with local or regional banks. For the WFP, which transferred over $1.3 billion in such benefits in 2017 (about 30 percent of its total aid), transaction and other fees are money that could have gone to millions of meals. Early results of the blockchain program touted a 98 percent reduction in such fees.

And if the man behind the project, WFP executive Houman Haddad, has his way, the blockchain-based program will do far more than save money. It will tackle a central problem in any humanitarian crisis: how do you get people without government identity documents or a bank account into a financial and legal system where those things are prerequisites to getting a job and living a secure life?

Owning your identity

Haddad imagines Bassam one day walking out of Zaatari with a so-called digital wallet, filled with his camp transaction history, his government ID, and access to financial accounts, all linked through a blockchain-based identity system. With such a wallet, when Bassam left the camp he could much more easily enter the world economy. He would have a place for an employer to deposit his pay, for a mainstream bank to see his credit history, and for a border or immigration agent to check his identity, which would be attested to by the UN, the Jordanian government, and possibly even his neighbors.

Such a record, perhaps stored on a mobile phone, could let someone like Bassam take his data from Syria to Jordan and beyond, backed up online in encrypted form. Syrian refugees using such a system—and most in Zaatari already have smartphones—could regain legal identities that were lost along with their documents and assets when they fled their homes. In this scenario, Bassam could move—to Germany, or back to Syria—and easily prove his educational credentials, demonstrate his relationship to his children, and get a loan to start a business. (In most countries, without an ID you can't get a bank account, and without a bank account, you can't get a place to live or a legal job.)

If such a system had existed before Bassam left his hometown of Daraa, he might have avoided Zaatari altogether and become a productive member of Jordanian society straight away. Even if Syria revoked his passport, or if a school with a record of his degrees were bombed, an immutable register of his history could still smooth his entry into an adopted country.

A number of organizations are already working on aspects of this idea. In Finland, a blockchain startup called MONI has collaborated since 2015 with the Finnish Immigration Service, giving every refugee in the country a prepaid MasterCard—

Houman Haddad is the UN executive behind Building Blocks and its use at the Jordanian camp.

backed by a digital identity number stored on a blockchain. Even without the passport necessary to open a Finnish bank account, a MONI account lets refugees receive benefits directly from the government. The system also allows refugees to get loans from people who know and trust them, helping them build rudimentary credit histories that could make it possible to get institutional loans down the road.

Meanwhile, companies like Accenture and Microsoft are joining nonprofit organizations in a public-private alliance called ID2020. The mission is to help achieve the UN goal of providing a legal identity to everyone, starting with the 1.1 billion people who lack any officially recognized proof of their existence.

At the heart of such systems is a concept known as "self-sovereign identity." It was popularized in 2016 by Christopher Allen, an American technologist, who outlined principles for a digital proof of existence owned by the individual. In such a scheme, identity would be portable and not dependent on any state or central authority. And the consensus is growing that a blockchain should be at its center.

Blockchains, Allen told me, are critical to such identity systems because they solve previously "unsolvable" problems. By storing an encrypted identifier in a blockchain, one can separate the authentication system from one's data, helping to protect privacy. Blockchain systems are also more secure than conventional identity records because they cut out third-party intermediaries. They can be easier to use, and they can survive disasters that might wipe out more centralized record-keeping systems.

The ultimate goal is a system in which a user owns and totally controls some kind of digital wallet—much like the physical one we carry today for our paper documents. The wallet stores claims made by the user (like name and date of birth), evidence for those claims (like copies of birth certificates or utility bills), and third-party validations, known as attestations, that further support an individual's claims (like a government confirmation of the details on a birth certificate). Such a wallet could reside in a smart chip on a key fob or something resembling a credit card, or it could be a secure enclave within one's phone, like those already provided by some manufacturers.

With the right technology, say Haddad and others, a blockchain ID system could cover many more claims than the kind found on licenses or passports—claims like "over 21" or "US

A mural at the Zaatari camp (center); Bassam gets his eye scanned to pay at the market's checkout.

Zaatari is a bustling city that sprang into existence as a tidal bore of humanity crashed over the Syrian border in 2012.

Nearly 75,000 Syrians live in the sprawling camp, including many children and young adults.

At the Tazweed Supermarket (top), residents of the camp can buy goods using a blockchain-based account.

An iris scan is used to establish digital identity at the checkout (left). The system uses a traditional database and an account stored on a permissioned variant of the Ethereum blockchain.

The supermarket offers bulk supplies of necessities such as rice, oil, and sugar.

citizen." It might, for example, help a refugee prove his or her professional background or family connections.

Who controls it?

It will take a while to achieve that grand vision. Haddad's idea for Building Blocks was to start by creating an account on a blockchain for every family of Syrian refugees in a Jordanian camp. Families wouldn't then have to wait days for local banks to transfer their money, or have to share identifying information with the banks, where some unscrupulous employee might steal or misuse it. Meanwhile, the WFP, instead of forwarding money before it's spent, could itself tally all refugee purchases and pay participating stores afterward in local currency. That's a big deal, since upwards of 30 percent of UN assistance is lost to corruption.

In an early test of the Building Blocks payment idea in Pakistan, however, the transactions were slow and the fees were too high. Haddad decided one of the problems was that the system was built on the public Ethereum blockchain. The current version of Building Blocks—the one now in use in Jordan—runs on a "permissioned," or private, version of Ethereum.

On a public blockchain, anyone can join the network and validate transactions. Such a system makes it difficult for any one person or agency to tamper with or forge transactions, but transaction fees tend to add up. On a permissioned blockchain, a central authority decides who can participate.

The upside of the permissioned system is that Haddad and his team can process transactions faster and more cheaply. The downside is that since the WFP has control over who joins its network, it also has the power to rewrite transaction histories. Instead of cutting the banks out of the equation, it has essentially become one.

For Bassam and his fellow refugees in Zaatari, the distinction may not matter. Bassam told me he'd bought groceries with an iris scan even before Building Blocks was implemented, but in that case an actual bank handled the transaction. And before that, he had a card the cashier would scan, but sometimes it wore out, and it could take weeks to get it replaced. "The new system works better," he says.

"It's a major success," says Haddad, who explains that it reduces costs and the risks of sharing refugees' data, while simultaneously improving the WFP's control, flexibility, and accountability. "Now if we get a call that 20,000 people are coming in the night, we can have everything ready for them in the morning," he says. "The old way would have taken two weeks and required paper vouchers."

But because Building Blocks runs on a small, permissioned blockchain, the project's scope and impact are narrow. So narrow that some critics say it's a gimmick and the WFP could just as easily use a traditional database. Haddad acknowledges that—"Of course we could do all of what we're doing today without using blockchain," he says. But, he adds, "my personal view is that the eventual end goal is digital ID, and beneficiaries must own and control their data."

Other critics say blockchains are too new for humanitarian use. Plus, it's ethically risky to experiment with vulnerable populations, says Zara Rahman, a researcher based in Berlin at the Engine Room, a nonprofit group that supports social-change organizations in using technology and data. After all, the bulk collection of identifying information and biometrics has historically been a disaster for people on the run. Think of the Holocaust, or the more recent ethnic cleansing of Rohingya in Myanmar.

A matter of courage

Ultimately, the question with Building Blocks or any similar system is whether it will put ownership of digital IDs in the hands of the people being represented or simply become an easier way for corporations and states to control people's digital existence. Bob Reid, CEO of a blockchain identity startup called Everid, told me he expects a battle over this question in the next few years. "Either it goes to individuals or it goes to

"Now if we get a call that 20,000 people are coming in the night, we can have everything ready for them in the morning."

major institutions that will mine our data," he says. Still, he says, the hope is that the discussion will move away from such either-or framing.

The real promise of using blockchains may not be realized until organizations like the WFP and the UN have the courage to open at least parts of the system to other agencies, and then to take the bravest step of all and turn over ownership of the data to beneficiaries like Bassam, who currently has little say in the matter because he has to be in the system if he wants to eat.

Building Blocks could, in theory, accomplish this if it evolves according to Haddad's vision. For instance, the WFP could offer its technology to others as a basic accounting system, tracking disbursements for food and later adding entries for land ownership, educational credentials, and travel history. If outside nonprofit organizations were allowed to add nodes to the blockchain's network, it could become more like a public blockchain, with its advantages of being harder to hack or cripple because it is decentralized and distributed.

Walking around Zaatari, a bustling city that sprang into existence as a tidal bore of humanity crashed over the Syrian border in 2012, shows what a severe test it will be for Building Blocks' ambitions. Just beyond the two officially sanctioned grocery stores that accept payments using Building Blocks, there are scores of mom-and-pop vendors openly running what are essentially black-market shops selling everything from food to washing machines to old bicycles. If Building Blocks can't be adopted there, then aside from making the WFP's operations a bit more efficient and transparent, it will remain little more than a centrally controlled database dressed in a costume of distributed, decentralized trust.

Russ Juskalian is a freelance writer based in Munich, Germany. He visited Zaatari this February.

Can Building Blocks fulfill its real promise and be more than a centrally controlled database?

The market is well stocked with produce.

"We're going to start seeing the beginnings of a borderlessness in politics and the marketplace. That's what really stood out to me … to not be at the behest of the people who are in control anymore."

—Elizabeth Munker, 28, UK

~~skeptics~~

~~cynics~~

~~naysayers~~

~~doubters~~

The blockchain believers

What makes blockchain devotees so passionate about the technology? Is it a means to get rich or something much bigger? And how do you even explain the thing to people who don't quite get it? We sent reporters to blockchain conferences in Dallas, Texas, and Cambridge, UK, to find out.

By
AMALIA ILLGNER
(at the Blockchain: Rewiring Governance conference in Cambridge, UK) and
DAN SOLOMON
(at the Bitcoin, Ethereum & Blockchain Superconference in Dallas, Texas)

Photographs by
ANDREW TESTA and
JULIA ROBINSON

Editor's note: Some of the quotes have been lightly edited for brevity and clarity.

"We should stop trying to explain blockchain and start trying to show what the benefits are, because consumers don't really need to know how it works. They don't know how Visa or the Treasury—how any of those things work, but they know that they add value to their lives." **—Aari Lotfipour, 33, Dallas**

"The internet was really started because of the same ideas. We wanted the freedom to share information, freedom of voice, level the playing field, allow small ideas to become big. This is all the same thing that's going on. It's just another layer on top."
—Chris Nichols, 47, Dallas

"Years ago when Bitcoin was three cents I got too busy to buy it, and they kept saying buy it, and I kept saying I'll get to it, and then I forgot. And then the other week I saw it was at $19,000. I thought, if I had it, I'd sell it now. But I didn't have it. I really kicked myself in the butt. Those are millions of dollars that I could have had."
—Michael Mullen, 50s, Dallas

What do you tell your friends about cryptocurrencies?
"They were like, 'You're putting all that money in? You're crazy!' and now they are all calling me for advice."

Has it made you rich?
"Oh, yes. In my country, Croatia, yes. I bought a house."
—Petar Juršic, 23, UK

"The internet unlocked applications we didn't think were possible—like Twitter, which came completely out of the blue. The same way the internet revolutionized communication, blockchain is going to revolutionize trust. Now there is an alternative to institutions and governments. We can rethink the whole system."
—Justin Drake, 29, UK

"Through the blockchain, everyone's going to have a global ID, so you'll have your own genome that'll be anonymize-encrypted, and then through crypto-keys you'll be able to totally manage who has access to your genome. So you can donate it, you can monetize it, but this is all going to be something that you control."
—Henry Ines, 43, Dallas

What do you think this ends up doing 10, 20 years down the line?
"I think that if I had an answer for that, it would be the most bullshit answer that I've ever given to anything in my life."

Okay.
"If you asked me in 1997 what the internet was for, I would tell you that I could use it for e-mail and to download some pictures of boobs, and now it's on my phone and I can do so many ridiculous things with it at the touch of a button or a swipe at any point in time. I don't think we know what those future iterations look like. I would love for people to have more financial sovereignty and more control. I would love for it to lead to a freer, more borderless, more censorship-resistant world."
—Amber D. Scott, 39, Dallas

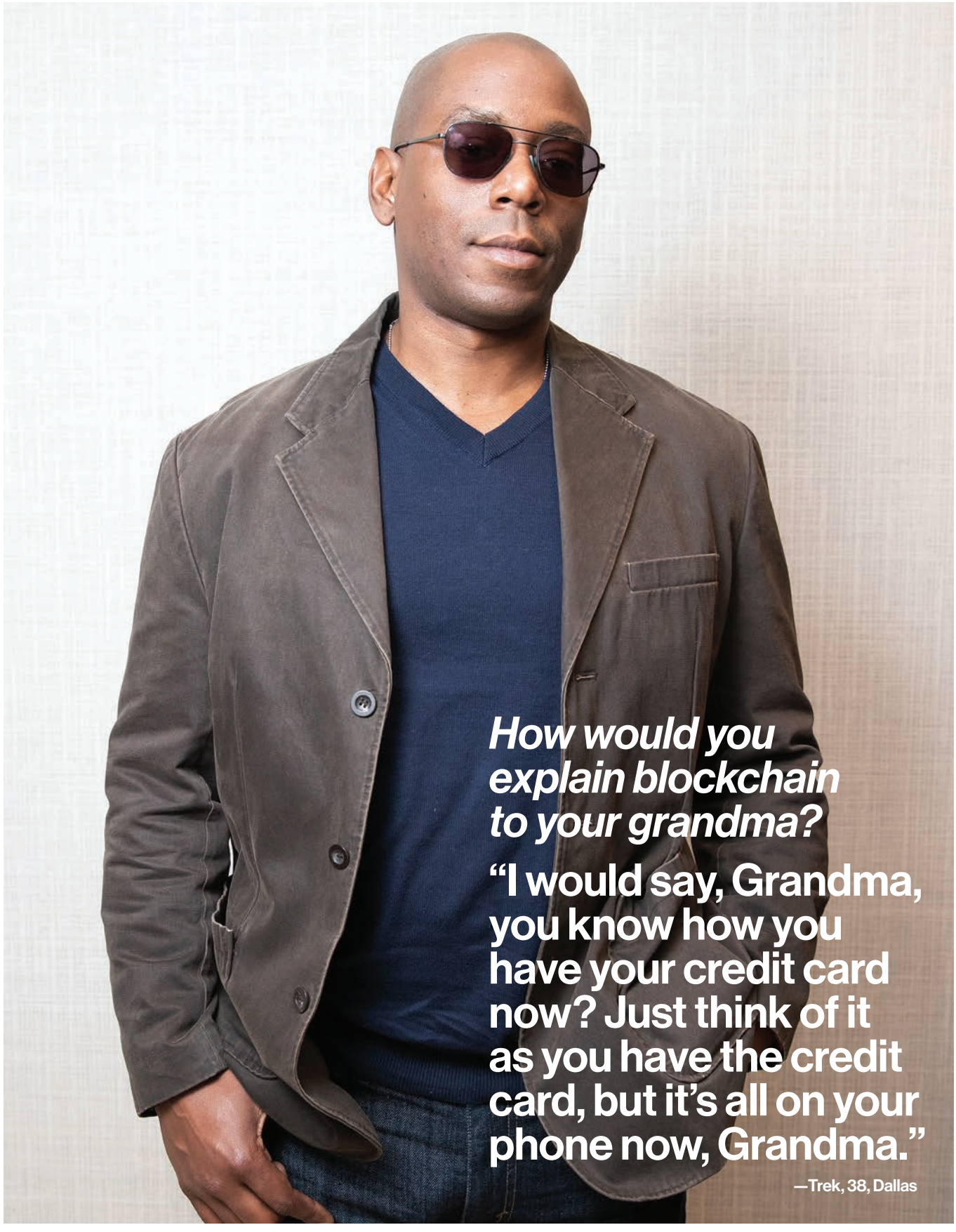
"In India there is a lot of black-market trading going on, and it seems that with blockchain—with its ledger that can never be changed—it's a secure location. And as someone who's seen black-market deals happening in front of my eyes, the idea that that might become a lot harder to do, and might one day be eradicated—it's just really fascinating."
—Ashkay Shah, 21, UK

"Six months ago on my LinkedIn feed there was not a lot of blockchain or crypto chatter. Three months ago I started getting more. Now, like 75 percent of my news feed is all about crypto and blockchain and who's doing what."
—John Nolz, 44, Dallas

"A few years ago I got involved in a hackathon and they were looking at finding a way to give an identity to 230 million children unaccounted for by the authorities in Africa and India. The idea that our team came up with was that you can take a picture of the child, and take their fingerprint every year and store it on the blockchain, and then you give the child their digital identity when they turn 18."
—Christiana Imafidon, 24, UK

Would you buy any cryptocurrency?

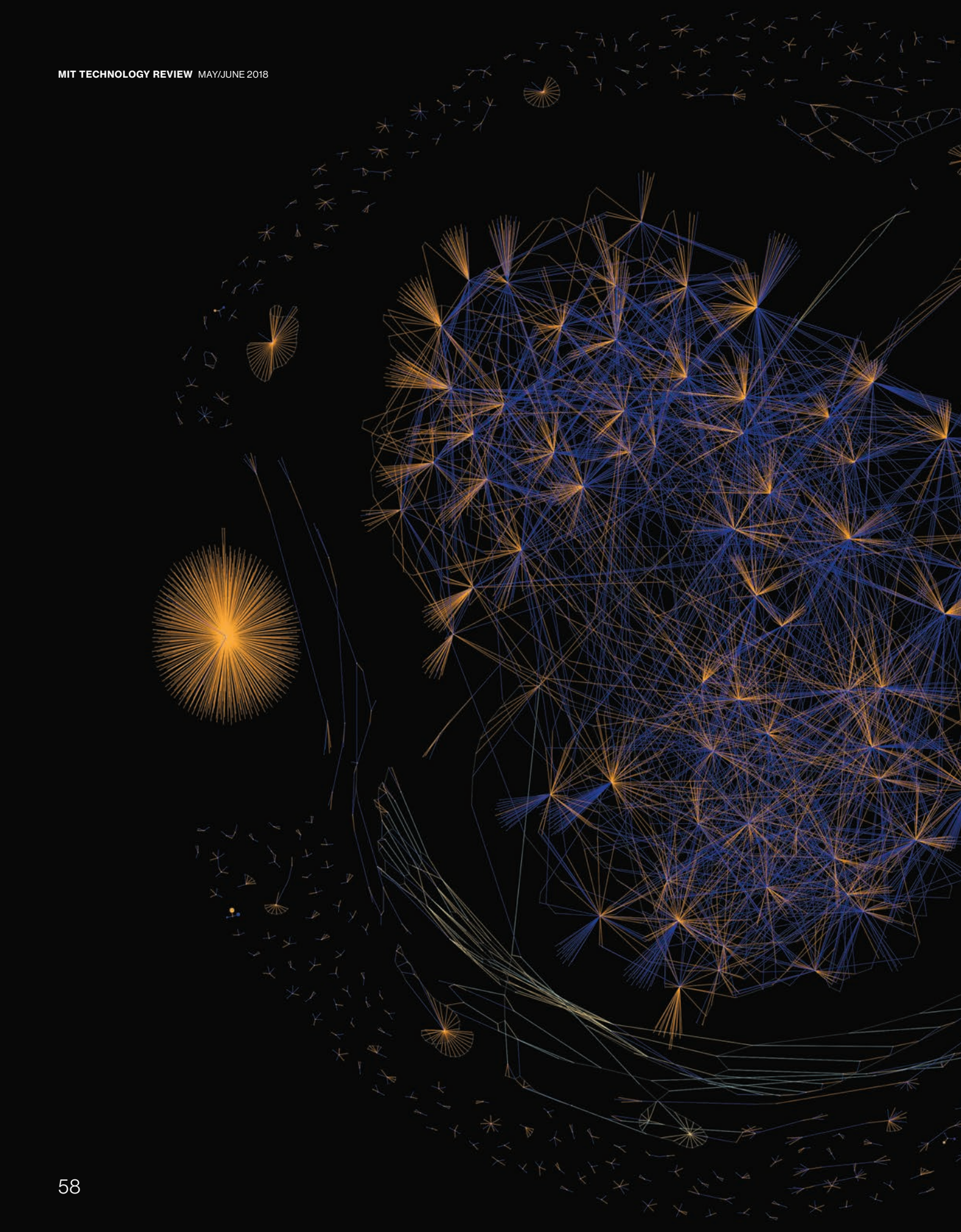
"No, because I don't back horses, and you know if a horse doesn't win, you don't get anything. Same with a cryptocurrency—if it fails, you've got nothing!"
—John Goldworth, 89, UK



How would you explain blockchain to your grandma?

"I would say, Grandma, you know how you have your credit card now? Just think of it as you have the credit card, but it's all on your phone now, Grandma."

—Trek, 38, Dallas



Can you spot the cryptocrime in this picture?

A growing number of forensic investigators can, thanks to new tools that let them track data through cryptocurrency networks that are turning out to be far less private than we thought.

By **Douglas Heaven**

What you're looking at: A wall-size data visualization at Imperial College London shows activity on the Bitcoin blockchain.

Spiky yellow and blue shapes begin to fill a screen that spans an entire wall in a lab at Imperial College London. The shapes emerge from empty space as the display pulses and dances. The visualization is hypnotic and confounding, but it makes sense once you realize what you're seeing. I'm watching the Bitcoin blockchain grow in front of me.

A ragged blue circle pops up, and William Knottenbelt, a researcher at the college, provides live commentary. "Here you see somebody taking in Bitcoin and then paying it out to thousands of other people," he says. "So this might be a mining pool paying out rewards to the people who have contributed to finding some blocks." He points to a curious cluster of shapes on the screen.

"Ah, this structure here is interesting," says Knottenbelt. Several blue circles appear—more payouts to multiple accounts—but they are knitted together by a cross-hatch of yellow lines. It looks as if someone scribbled on the display with a Sharpie.

What Knottenbelt has just noticed could be the first evidence of a sophisticated criminal at work.

Banks and financial companies are experimenting with using cryptocurrency to create smoother payment systems. But the technology is also supporting a new generation of illicit activity, providing new ways to steal, blackmail, commit fraud, and break international sanctions.

An industry has sprung up to help fight back. New forensic tools are allowing authorities to follow the money through cryptocurrency networks that are turning out to be far less private than their founders hoped. Just as closed-circuit cameras turned bank robbers from celebrated criminals into easily caught rubes, researchers hope that their advances can turn anonymous thieves into known prisoners, and make the cryptocurrency world safe for the average customer.

The opportunities in cryptocrime

IF YOU'RE UP TO NO GOOD, CRYPTOCURrencies tick a lot of boxes. The only thing tying you to an account in Bitcoin or Ethereum or NEM or a thousand other cryptocurrency systems is an address, typically a random string of letters and numbers. You can have as many addresses as you like, and in principle, there is no obvious way to tie them together or identify their owners. What's more, money in these accounts can be transferred without intermediaries and across international borders as easily as sending an e-mail.

"Instead of meeting you in a dark car park to hand over a suitcase of money, I can be sitting with a laptop on a balcony in Monaco," says Jeffrey Robinson, an investigative journalist and author of 30 books on financial crime, including *BitCon: The Naked Truth about Bitcoin*.

Clever criminals are embracing the new opportunities. A 2018 study by blockchain analysis startup Elliptic and the Center on Sanctions and Illicit Finance, a US think tank, found a fivefold increase in the number of large-scale illegal operations working on the Bitcoin blockchain between 2013 and 2016. By analyzing the history of more than 500,000 bitcoins, they identified 102 criminal entities—including dark-web marketplaces, Ponzi schemes, and ransomware attackers—and showed that many of the coins in their study could be linked back to them.

Sarah Meiklejohn and colleagues developed techniques in 2013 on which much of today's cryptocurrency analysis is based.

Ninety-five percent of all laundered coins tracked by the study came from just nine dark-web marketplaces, including Silk Road, Silk Road 2.0, Agora, and AlphaBay. These are notorious online bazaars where a person can buy banned goods like drugs and weapons and pay for services like prostitution or murder-for-hire. "On the dark

ANDREW TESTA. PREVIOUS SPREAD: DAN MCGINN. IMPERIAL COLLEGE LONDON

web you can even buy legal advice," says Robinson. "There are lawyers down there willing to take Bitcoin to tell you how to avoid getting caught with Bitcoin."

Other types of organized crime are emerging as well. Hackers have embraced Bitcoin as their payment of choice for ransomware attacks. Such attacks spiked in 2016, with nearly 16 percent of tainted coins linked to outbreaks of malware like Locky. The trend continued in 2017 with WannaCry and NotPetya, which held hostage computer systems in hospitals and businesses across the world. In March of this year, municipal government systems in Atlanta were rendered useless by a ransomware attack whose perpetrators demanded about $51,000 in Bitcoin.

Cryptocrime is even infecting the offline world. The last few months have seen a flurry of real-world hold-ups in which victims were forced to hand over account details at knifepoint. "Suddenly, if you have a lot of crypto you're in physical danger," says Imperial College's Knottenbelt.

Cryptocrime is even infecting the offline world. The last few months have seen a flurry of real-world hold-ups in which victims were forced to hand over account details at knifepoint.

And yet, since every Bitcoin transaction is recorded in a distributed public ledger, ill-gotten gains can be tracked. Anyone can download the entire transaction history of Bitcoin—which currently weighs in at around 160 gigabytes—and examine it, or use a website such as Blockchain.info or Block Explorer to check it out in a browser.

Such analysis helped unravel one major heist. In 2014, Mt. Gox, then the largest Bitcoin exchange in the world, was hacked by unknown thieves who stole 850,000 bitcoins, then worth more than $450 million.

As Mt. Gox spiraled into bankruptcy, its trustees enlisted a crack forensics team to help find the missing coins. What they found was a mess. "Mt. Gox didn't understand how many bitcoins they owed people and how many bitcoins they actually had until they noticed they were gone," says Jonathan Levin, who led the investigation. Levin and his team eventually tracked the funds to an exchange called BTC-e, where the trail went cold.

Though they couldn't get most of the missing coins back, "that investigation gave us the idea to develop a tool that other people could use," Levin says. His company Chainalysis, born of that effort, builds tools for bitcoin businesses wanting to understand their customers better and for law enforcement agencies seeking criminals. Other companies, like Block Seer and Elliptic, offer similar tools and services.

According to Tom Robinson, cofounder and chief data officer of Elliptic, the majority of the world's Bitcoin exchanges use the company's software to screen transactions. It checks whether they can be connected to ransomware wallets, dark marketplaces, or theft, for example. Elliptic has helped provide evidence in several criminal cases, including one involving a man who bought parts for AR-15 automatic rifles on the dark web and a handful of drug busts.

Since the company was set up five years ago, Robinson estimates, a trillion dollars' worth of Bitcoin transactions have been screened using its software—even though there have been only around 300 billion dollars' worth of Bitcoin transactions ever. That's because some transactions are screened multiple times; Elliptic recommends that its customers rerun analyses on older transactions because information about dodgy accounts is being updated all the time. "You need to keep checking," Robinson says.

Robinson won't name his clients, but a quick search on USAspending.gov reveals that they include the US Drug Enforcement Administration, the Internal Revenue Service, the FBI, and Immigration and Customs. Chainalysis works with those and more, including financial regulators like the SEC. Chainalysis also says that Europol and more than half the police forces in Europe are using its software.

The US Treasury's interest in the blockchain reflects the fact that cryptocrime isn't limited to coin heists and black markets. It's also about fraud and tax evasion. "This is going to be an interesting tax year," says Jeffrey Robinson. "It's the first time in the US where they're cracking down on Bitcoin exchanges for tax purposes."

How to trace the untraceable

MUCH OF WHAT THESE COMPANIES DO builds on techniques introduced by Sarah Meiklejohn, then at the University of California, San Diego, and her colleagues in 2013. The basic idea is simple. By examining blockchain activity closely, you can spot accounts that appear to belong to the same Bitcoin wallet and are thus controlled by the same entity. The process is known as clustering. Multiple addresses initiating the same transaction might begin to look like one person or organization consolidating smaller funds into one bigger pot, for example. Another telltale sign is when change from a Bitcoin transaction is routed back into an account different from the one where the funds started off. In time, the chaos resolves itself into regular patterns.

Once multiple accounts have been linked to the same owner, you can try

to figure out who that owner is. Linking Bitcoin accounts to real-world identities is possible because information tends to leak out. Regulated cryptocurrency exchanges—generally those in the US or Europe—must follow know-your-customer and anti-money-laundering rules, which require people to hand over identification before using their services. Some people are even so careless as to post their supposedly private Bitcoin addresses in online forums. "What people forget is that the blockchain is just one half of the equation," says Knottenbelt.

Chainalysis and Elliptic now use machine learning to help cluster addresses. Soon it might even be possible for an AI to police blockchains in real time.

The wall-size data visualization at Imperial College is a step toward that. The blue-and-yellow tangle that caught Knottenbelt's eye was a coin tumbling network, a sequence of transactions deliberately designed to make it harder to track individual coins. It's like dropping money into a jar, shaking it about, and then taking it out again: the amount doesn't change, but it's hard to tell which coin was which. The effect is much the same as if you move money through a bank in a place like the Cayman Islands, where there are strict secrecy laws around banking.

Staying one step ahead

HOWEVER, TUMBLERS AREN'T NECESsarily a sign of criminal activity. "Some people just do it for privacy reasons," says Knottenbelt. And in any case, there are better ways for criminals to cover their tracks. As the limits to Bitcoin's privacy become more apparent, people are moving to new cryptocurrencies, like Zcash and Monero, that reveal almost nothing about the transactions recorded on their blockchains.

Zcash uses a so-called zero-knowledge proof to verify transactions. This is a mathematical way to confirm that a transaction took place without revealing any information about who was involved or how much was transferred. Zcash also lets you hand back coins and have fresh ones mined, the equivalent of trading your marked bills in for clean ones at the bank.

Monero, meanwhile, is effectively a big tumbling network. When you want to transfer coins, your address is mixed in with a bunch of others so that no one can tell which one was spending the money.

Zcash and Monero certainly take privacy to the next level. But that doesn't mean they'll never give up their secrets. Meiklejohn points out that sloppy user behavior, such as posting your private address in forums, will again leave behind clear trails, just as with Bitcoin.

What's more, Monero gives users the option to carry out transactions with no obfuscating coins mixed in. This removes the privacy for that particular transaction and adds a way for researchers to disentangle, through a process of elimination, any mixers that subsequently include those coins. Malte Möser at Princeton University and colleagues estimate that 62 percent of inputs to Monero transactions are vulnerable to this analysis. When users of Zcash and Monero start to hemorrhage clues, the likes of Meiklejohn and Möser will be ready.

Perhaps the biggest problem for law enforcement, though, is the large number of unregulated exchanges, where criminals can wipe away the traces of their theft by laundering the stolen cryptocurrency into other forms of wealth. Many exchanges defy regulation out of principle: the likes of BTC-e and the conversion service Shapeshift, for instance, sell themselves on the promise of asking for no identification from their users. Shapeshift founder Erik Voorhees is especially outspoken about the political implications of regulation.

Security and cryptocurrency researcher Ross Anderson at the University of Cambridge, UK, argues that these exchanges thrive in part because laws are ineffective. "The problem with anti-money-laundering generally is that nobody wants it done right," he says. "If you're a city bank, you don't want to know that John Gotti is a customer, and so banks would never tolerate a law that said whoever banks the mafia will go to jail." If that's how the world works, why should crypto exchanges be different?

Anderson's cynicism about the authorities' willingness to act has led him to formulate a plan to take down the cryptocrime system himself. He is creating what he calls a taintchain—a public list of bitcoins with clear links to criminal activity. "What I'm going to do is publish a list of all the stolen Bitcoin and the software you need to generate it so that everybody can check it for themselves," he says. Exchanges would then think twice about handling stolen coins.

Even if regulation were stricter, however, it's not clear that it would make a difference. "I don't think outlawing anything is going to help anyone," says Knottenbelt. Driving the tech underground, he argues, will simply mean that transactions will be hidden rather than broadcast openly on the internet, making it even harder for researchers like Meiklejohn to analyze the money flows and find the thieves.

Surprisingly, Meiklejohn herself turns out not to worry too much about regulation—or lack of it. "Once you've isolated the problem to bad exchanges operating outside of typical jurisdictions, then you've kind of won," she says. Take BTC-e, an exchange based in Russia that was known to have taken a lot of criminal money. A lot of ransomware operators appeared to be using BTC-e almost exclusively. It was also where the missing Mt. Gox funds were last seen before the trail vanished.

But in July 2017 it was closed down. US authorities arrested staff and seized computers at one of the exchange's data centers, and Alexander Vinnik, its suspected operator, was arrested. "They clearly were not going to respond to subpoenas," says Meiklejohn. "On the other

THOMAS ANGUS, IMPERIAL COLLEGE LONDON

William Knottenbelt, a researcher at Imperial College London, says, "I don't think outlawing anything is going to help anyone."

hand, this is something law enforcement is well aware how to deal with."

Meiklejohn sees her work as distilling cryptocrimes to the type of crime familiar to law enforcement. Armed with leads from Elliptic and others, good old-fashioned policing will then do what it does best.

The biggest cyber-heist in history

FOR THE TIME BEING, HOWEVER, THE cybercriminals are still a step ahead. Although researchers can now watch thefts of cryptocurrency on blockchain networks happen in close to real time, they can't connect them to the real world fast enough to stop even monumental capers.

The biggest cyber-heist in history happened at 3 A.M. Japan time on a January morning this year. Someone, or more likely someones, made off with more than half a billion dollars' worth of a digital currency called NEM from the Tokyo-based cryptocurrency exchange Coincheck. No one at the exchange raised alarms until lunchtime, and the culprits got an eight-hour head start.

When news finally reached NEM Foundation vice president Jeff McDonald in Tulsa, Oklahoma, he went right to the chain. The funds had been taken from a software wallet connected to the internet—an insecure storage locker that Coincheck says it was only using because of a fault elsewhere in its system. "It's basically like leaving your ATM card out with the PIN number written on it," says Alexandra Tinsman, the NEM Foundation's communications director. All of the 523 million stolen coins were funneled first through a single account before being split among several others.

To stop the thieves from cashing out their loot into a fiat currency, the NEM team rushed to flag the stolen coins and put exchanges on alert. The day after the hack, the NEM team had identified and published the addresses of 11 accounts where funds had ended up. Each was labeled with a tag that read "coincheck_stolen_funds_do_not_accept_trades : owner_of_this_account_is_hacker." But because they didn't know who owned the accounts, the NEM team was unable to do much more than attempt to block the exits.

A waiting game ensued. Unable at first to cash the stolen coins out of the NEM network, the thieves moved them around it. These movements were all visible on the public blockchain. The NEM team tracked the coins to Canada and then watched as some of them returned to Japan. But even though NEM never took its eyes off the marked notes, the thieves still got away. In the end they were able to make it to an unregulated exchange and cash out at least half the stolen coins. In March, the NEM team announced it was giving up the chase.

Stung by the massive theft, Coincheck announced that it would no longer deal in Zcash, Monero, or Dash, another anonymous currency. It's among the first exchanges to cut off those coins.

Coincheck's move is part of a larger effort to bring law and order to this new frontier of money. The US government is toying with the idea of creating a blacklist of cryptocurrency addresses that are associated with criminal groups, such as terrorists, drug traffickers, and sanction-busters. One possibility is that it would become illegal to deal with blacklisted addresses.

The NEM thieves have escaped, for now. But future technology could snare them yet. As the forensic techniques and tools get better, previously overlooked evidence will come to light like DNA traces at a years-old crime scene. Every time the authorities shut down a Silk Road or BTC-e, that sends a signal, says Jeffrey Robinson: "They'll get the rest of them, one by one."

Douglas Heaven is a freelance writer based in London.

Chinese crypto gets creative

Last September's government restrictions have unleashed a wave of below-the-radar innovation.

BY YITING SUN

At 11 P.M. on September 4 last year, Chuan Zhang logged into his account on Huobi.com, a popular Chinese cryptocurrency trading website, and sold every bitcoin he had. He lost about 400,000 yuan ($63,000), but he had little choice.

Earlier that day the Chinese government had issued a seeming death blow to the country's burgeoning cryptocurrency scene. Although it didn't outlaw virtual coins or the mining of them, it did ban initial coin offerings (ICOs) and trading on domestic cryptocurrency exchanges, rendering many people's holdings effectively worthless. The cryptocurrency sell-off that day was so massive that it took four days for money from Zhang's Bitcoin sales to show up in his bank account, something that usually takes half an hour or so. (That he was able to sell at all was thanks only to a delay between the government's declaration of the ban and its shutdown orders to the exchanges.)

At their peak, during the last two months of 2016, transactions in Chinese yuan accounted for more than 90 percent of global Bitcoin trading volume, according to Morgan Stanley. A month after the crackdown, in October 2017, that figure was down to less than 10 percent. The authorities have since tightened things further, closing loopholes that allowed investors to trade cryptocurrencies on overseas websites. In January, the central bank proposed limiting supplies of power to China's bitcoin-mining industry, which currently accounts for two-thirds of the world's processing power devoted to such activity, most of it in sparsely populated areas with abundant surplus electricity. Local authorities are enforcing the restrictions haphazardly.

Yet cryptocurrency is far from dead in China. In fact, the restrictive measures may have inadvertently triggered a wave of innovation that targets some of the problems faced by cryptocurrencies everywhere, not just in China.

New kinds of exchange

Cryptocurrency exchanges handle trades from one digital currency to another, as well as trades between digital coins and ordinary fiat currencies. But whereas cryptocurrencies are (at least in theory) decentralized and under no one organization's control, exchanges are typically run by a single company, just like ordinary stock exchanges. This is one of cryptocurrencies' biggest weak points.

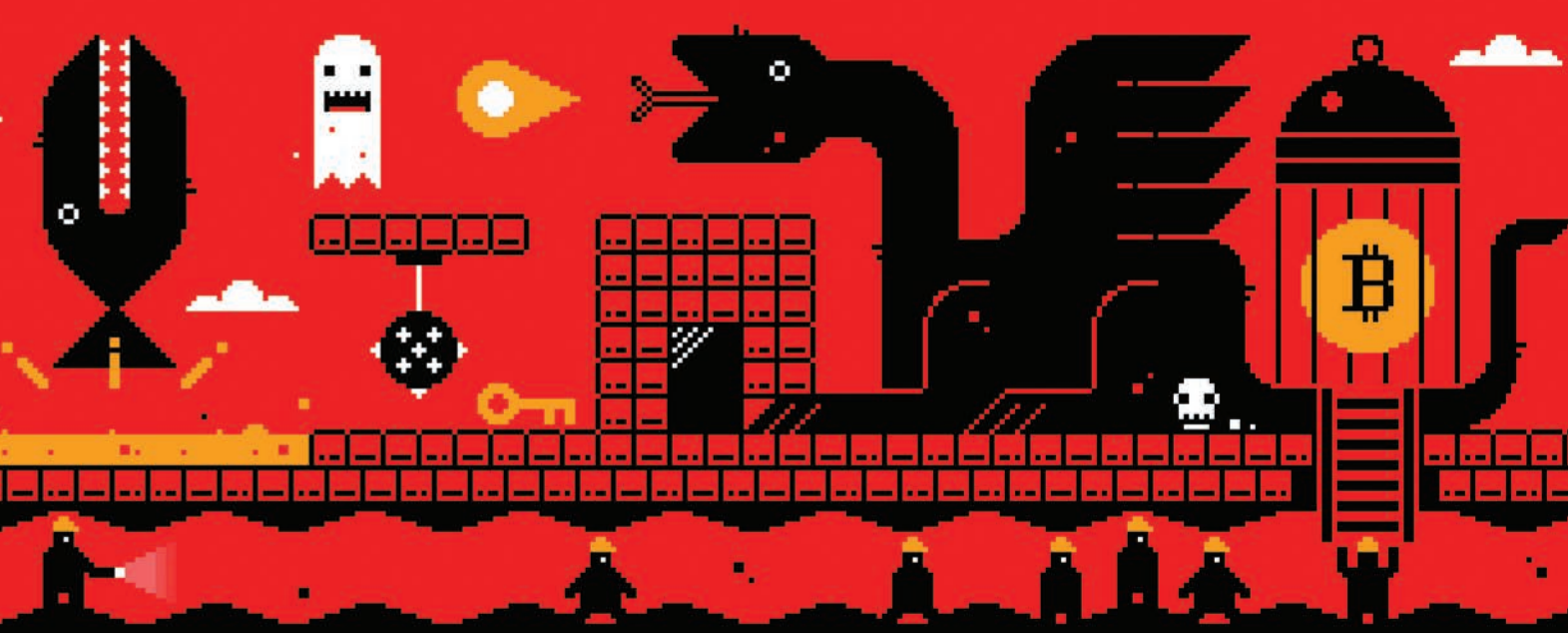
Indeed, it creates a raft of potential problems. The exchanges are prime targets for hackers because, like banks, they hold investors' assets. Insider deals are hard to prevent. And there are hundreds of separate exchanges around the world, making for a fragmented and inefficient financial system: the account holders on one exchange often don't have quick access to better deals on others.

That was why Daniel Wang, who used to run a centralized exchange in Shanghai, founded a project called Loopring. It's an open-source software platform that anyone can use to build a decentralized exchange—a marketplace for cryptocurrency transactions that doesn't hold investors' assets. Instead, all assets and transactions are recorded on a public blockchain, much like the blockchains that underlie cryptocurrencies themselves. That prevents insider trading, because anyone can view transactions on the blockchain. Smart contracts on the blockchain regulate the way orders are matched. Once there is a match, the parties transfer currency to each other electronically.

China's crackdown should have killed Loopring in its cradle. Wang, who came up with the kernel of the idea in 2016, had just finished raising money for it in an ICO three weeks before the government banned ICOs and demanded that money they had raised be returned. But Wang enjoyed such support from his investors that he was able to keep part of their investment and continue the project.

Loopring's own decentralized exchange is now hosted on Amazon Web Services, and it was set to start offering trading services in April, after this story went to press. But since Loopring is also open-source software that anyone can use to set up an exchange, it is relatively resilient against restrictions in any one

NICHOLAS LITTLE



country. Wang, who spends a lot of time in New York these days trying to get Loopring established in the US crypto community, says that if trading digital assets on a blockchain becomes a widespread practice, it will be harder for a country such as China to block it. "Shutting it out will reduce [a country's] international competitiveness," he says.

From "air tokens" to serious sales

China's September crackdown also included a ban on ICOs, the crowdfunding schemes based on crypto-tokens (see "Down with ICOs; long live IPOs," p. 78). In China as elsewhere, these had acquired a shady reputation. Companies looking to raise funds quickly were selling digital tokens or "coins" that were supposed to buy access to some product or service in the future, but they often had no way to fulfill these promises. A Chinese term emerged: *kongqibi*, or "air token."

The ICO ban suppressed this digital crowdfunding, but it didn't address the root of the problem. Illegal fund-raising of all kinds has thrived in China because the formal banking sector still favors large corporations and state-owned enterprises. Smaller firms and entrepreneurs rely on a shadow banking sector to meet their needs for financing.

But though using token sales to raise funds is now illegal, merely issuing a digital token isn't explicitly prohibited. Despite the ICO ban, therefore, a few people are forging ahead with token experiments.

One company at the forefront of this is Beijing-based Spectra Ventures, founded about a month after the crackdown in September. The founders, Iris Zhang and Aaron Chen, have worked in investment banking and China's cryptocurrency community. Using their experience to evaluate both companies that want to issue tokens and the buyers of those tokens, they advise the companies on how to price the tokens, how many to issue, and how to get listed on cryptocurrency exchanges. To get around the restrictions on token sales, Spectra doesn't engage in crowdfunding from Chinese retail investors but only from established digital-currency funds registered overseas.

It's common for a project to raise 10,000 to 40,000 ether (Ethereum's cryptocurrency) within a week, says Iris Zhang. At the exchange rate in early April, that was worth about $4 million to $16 million. Projects that have sold tokens through Spectra Ventures include an app for soccer fans and an instant-messaging app that allows users to transfer cryptocurrencies to each other.

These activities may appear to go directly against the Chinese government's orders. But in a sense, they may be what Chinese officials wanted to see.

In their September edict, the authorities talked about "avoiding market chaos, strengthening the education of investors, and collectively safeguarding the normal financial order." But China doesn't have a fundamental aversion to digital currencies; in fact, the central bank is developing its own fiat digital currency. "A digital currency will bring about a new financial ecosystem," says Shenglin Ben, dean of the Academy of Internet Finance at Zhejiang University. The purpose of the crackdown, he says, was to curb excessive speculation and give the authorities time to upgrade their regulatory capabilities.

Some of the centralized cryptocurrency exchanges that China banned last year still exist—they have simply set up servers abroad—and up until mid-March their websites were accessible in China. Since then they have been blocked, though Chinese users can still access them via virtual private networks. The one used by Chuan Zhang and his investor friends, Huobi.com, is among them.

After the panic sell-off last year, Zhang and his friends reinvested whatever savings they had left in cryptocurrencies again. This time, they do not plan to sell. Before the September ban, they had seen cryptocurrency as a way to prop up their fragile financial well-being. Now it has become a faith. "It's something that cannot be suppressed," says Long Zhang, 30, a close friend of Chuan Zhang's. "It will definitely be worth a lot in the future."

Yiting Sun is a freelance journalist based in Beijing.

PHOTOGRAPHS BY CELESTE SLOMAN/HAIR AND MAKEUP BY ROSE FORTUNA

Q+A WITH AMBER BALDET

Is the crypto world sexist? That's the wrong question.

Anyone can use cryptocurrency. Man, woman, pony, or toaster—we all look alike on a blockchain. // But the cryptocurrency scene has gotten a bad reputation for being much less open and inclusive than the technology itself. In January, one of the longest-running Bitcoin events, the North American Bitcoin Conference, put dozens of men on its agenda but only one woman. When it came time to schmooze, attendees were invited to a local strip club. // Yet there are many incredible women now leading the cryptocurrency industry. One is Amber Baldet. She's been called the "crypto queen" and the "Madonna of blockchain." Since 2015, she's run JPMorgan Chase's department devoted to finding ways to use blockchain. During her time there she has overseen the creation of Quorum, a business version of Ethereum. In May she leaves to start her own blockchain venture. // In her work, Baldet makes a habit of smashing assumptions. She smashed a few more when *MIT Technology Review* asked her about the state of diversity in the cryptocurrency world.

By Morgen Peck

"I don't have time for anyone who underestimates me because of my gender."

MP **The cryptocurrency community has gotten some discouraging press in recent months—portraits of an entitled boys' club. Do we have a gender problem on our hands?**

AB If you draw a Venn diagram of finance and technology, and specifically information security and cryptography, these are all fields that struggle with a lack of women and minority representation in leadership positions. Cryptocurrency sits in the center, where they all overlap. When you have an intellectual diaspora into a new area of study, the new group tends to inherit its demographic profile from its source groups. Just because cryptocurrency may be a philosophically and technically new thing, it's not magically a green-field meritocracy.

That said, my anecdotal experience is that representation at most developer-focused blockchain events is neither better nor worse than at most other tech conferences. There's usually about 15 percent of people who don't fit the "standard developer" stereotype, give or take a few percentage points, and that number has gotten better over time. At events that have more business-development

or social-good focus, it's much higher. I don't think this is because women are inherently better or more interested in those topics—it's simply the same inheritor bias of where more women work today.

But there's also another effect at play, and that's survivorship bias. Many of the women who got involved early come with battle scars from those other male-dominated communities and are fiercely determined to see it be different this time. So we're having these conversations earlier, setting up scholarships earlier, creating women-in-blockchain networking channels earlier, and pushing back against a toxic culture of "rock-star developer" hero-worship. We're still in the infancy of blockchain adoption; the efforts happening now are going to have serious long-term ripple effects.

MP **Has the gender disparity led to an unwelcoming culture?**

AB There is no monolithic "blockchain culture." People are working on academic research, building businesses, writing legal briefs, consulting for enterprises, and, of course … investing. People further fragment along technical lines, defending their favorite coin or project with loyalty that borders on the religious. All this can be daunting for newcomers to navigate, and some subgroups are known for being friendlier than others.

Many projects are great and welcome women with open arms, and repeatedly positioning the entire space as unwelcoming causes a negative feedback loop that dissuades great people from getting involved.

If you think "the" culture is represented by the very active and often very hostile crypto Twitter, you're going to have a bad time. Shouting opinions on the internet is a low barrier to entry, and there are certainly some people out there who give everyone a bad name. Stop letting trolls be referees of credibility, because they always move the goalposts.

"Inclusion, like health and happiness, is not something that you arrive at one day and say, 'We're done!' It's something that you work at every day, a process."

MP **So are we spending too much time talking about diversity? Do we really need a diversity panel at every conference?**

AB A subtle nuance—we're trying to shift the conversation from *diversity*, which can sound like a numbers game or an HR problem, to *inclusion*, which is a way of thinking holistically about the impact of our choices that should permeate everything we do.

While we can probably never spend too much time talking about inclusion, it's unfortunate that the majority of the burden of doing so falls disproportionately on the shoulders of those already responsible for doing real technical work and also fighting for their own legitimacy.

Conferences that magically forget to put us on stage to talk about anything but diversity should be named and shamed, but having those discussions as a supplement is generally fine, I think. It would be great to have those panels serve more as lightning rounds for participants to talk about what they're working on and what they're passionate about rather than how it feels to exist.

MP **You're about to start your own venture. Do you worry that raising money will be harder as a woman?**

AB I am of course aware of the abysmal statistics around women when it comes to employment at, and funding from, Silicon Valley VCs. As someone with years of experience, a strong network, and a real business plan, however, I get to be selective about who I choose to work with. I don't have time for anyone who underestimates me because of my gender.

MP **You sound optimistic that the future of technology will be more inclusive.**

AB Inclusion, like health and happiness, is not something that you arrive at one day and say, "We're done!" It's something that you work at every day, a process.

Inclusion happens when your recruiting process casts a wider net for qualified candidates. It happens when you give credit to people for their ideas and contributions. It happens when you value the people who help design and bring your product to market as much as the people who code it. It happens when you create AI support bots and don't give them women's names. It happens when you spin up a group chat and choose whom to invite. Inclusion happens when people in power use that power to bring people in rather than keep people out.

PHOTOGRAPHS BY CELESTE SLOMAN/HAIR AND MAKEUP BY ROSE FORTUNA


Protecting our troops
Stopping anthrax
Eradicating deadly disease
Improving patient outcomes
Keeping airports safe
BATTELLE
battelle.org/techreview
It can be done

3

WHAT COMES Next

Three ways Bitcoin could go from being the paramount crypto-currency to an also-ran or even an irrelevance. One way ICOs could actually contribute to the economy instead of bilking people. And a science fiction vision of a blockchain-based future in which AIs and smart contracts decide the course of human lives.

It's the world's first and still the biggest cryptocurrency.

Could it be knocked from its perch or otherwise made redundant?

Let's try it out.

By **MORGEN PECK**
Illustrations by Ariel Davis

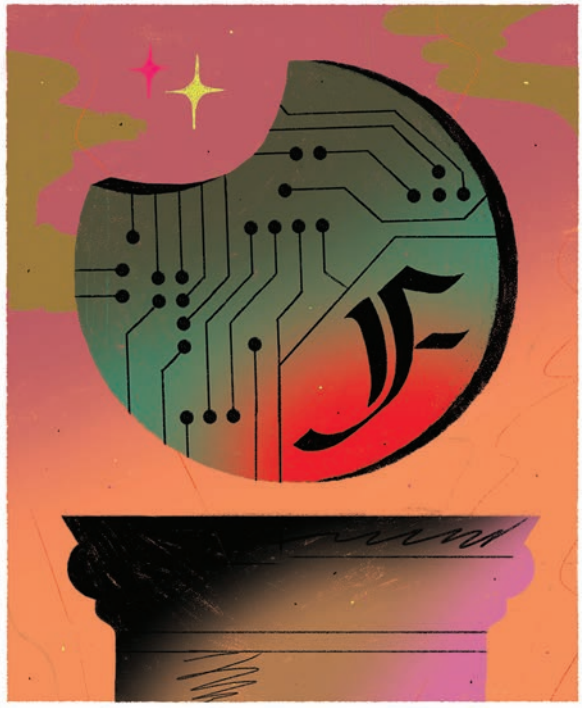
Let's destroy Bitcoin

In 2009, Satoshi Nakamoto served the world an entirely new kind of currency. It was one that people could move over the internet instantaneously and nearly free of charge. Issued and distributed not by a central bank but by its own users, it drew the drapes of privacy around financial transactions while making forgery—in theory, at least—impossible.

It's nine years later, and there are now 24 million active Bitcoin wallets in use around the world. The value of a single bitcoin has risen from about a dollar in 2011 to as high as $19,700 in late 2017.

But success, of course, breeds competition. And Bitcoin is now clearly the dominant cryptocurrency; as of this writing, in early April, its market cap was three times that of Ethereum, its nearest competitor, and roughly equal to those of all other cryptocurrencies combined.

Yet while Bitcoin has established an economy in which it's impossible to forge transactions, it provides no defense against replication of the idea itself. No one can copy an individual bitcoin, but anyone can copy the idea of Bitcoin. So how might a government, or a corporation, or even ordinary people, go about doing so in a way that makes Bitcoin useless or redundant? Here are a few scenarios.



Option one: Government takeover

The year is two-thousand-something-big, and it's the day your taxes are due. But you don't file them. Instead an algorithm automatically makes a withdrawal from your electronic wallet, in a currency called Fedcoin.

It's the digital version of those crunchy bills you only vaguely remember from many years ago, back before the central banks began taking paper cash and redeeming it for fedcoins. Over the years, you've seen less and less hard currency. You don't need it anymore, not when you can walk into a local bank, verify your identity, and set up a wallet on your phone. Sure, you still have a few dollar bills. But they are tucked away as souvenirs.

This hypothetical technology—a central-bank-issued digital currency built with a tweaked version of the Bitcoin blockchain—was described by David Andolfatto, a researcher at the Federal Reserve Bank of St. Louis, and later refined by Sahil Gupta, who as an undergraduate at Yale wrote a study on how a currency like Fedcoin would work. With some colleagues, he wrote code to test a simulation.

In their system, a blockchain records transactions, just the way it happens with Bitcoin. Instead of being updated by a network of unaffiliated peers, however, the Fedcoin ledger is managed by institutions certified by the Federal Reserve. "These authorized nodes could be things like Bank of America, JP Morgan—basically, trusted institutions," Gupta told me.

Each bank is responsible for a chunk of addresses on the blockchain. When new transactions come through, the bank validates them in a new block and sends it to the Fed. The Fed then acts as the final arbiter, checking the entries and unifying the blocks into a master version of the blockchain that it makes public.

To use fedcoins, people must first show proof of identity and set up a wallet with the Federal Reserve or an affiliate bank, at which point they can buy the new currency with US dollars at a one-to-one ratio.

You don't need cash anymore, not when you can walk into a local bank, verify your identity, and set up a wallet on your phone. You still have a few dollar bills, but they are tucked away as souvenirs.

A scheme like this, says Gupta, might gain popularity and ultimately result in the slow disappearance of physical cash.

"I'd imagine people first get comfortable spending Fedcoin on things like groceries and movie tickets," he says. "As people realize it's easier than cash, as businesses realize it's cheaper than credit cards, and as banks realize it's literally more secure, so goes the process by which dollars are phased out of the money supply and Fedcoin phased in."

This isn't just an academic thought experiment. The Bank of Canada built a simulation for such a currency, on a blockchain similar to Ethereum's, in 2016.

What such researchers are finding is that a digital version of state-run currencies could match or even improve upon the efficiencies of Bitcoin. Gupta believes that transactions should be processed much faster when a central bank is behind the system (as opposed to the peer-to-peer network that currently records Bitcoin transactions). This efficiency could add up to a lot of saved money. The Bank of England, which has been furiously researching blockchain technology, reported in 2016 that even partial adoption of a central-bank-issued digital currency would result in a 3 percent increase in GDP as the cost of taxes and transaction fees went down.

A shift away from cash would also make it easier for governments to collect taxes and enact monetary policy, says Campbell Harvey, a professor of finance at Duke University. For example, if a government wanted to disburse stimulus payments, it could simply deposit money into people's Fedcoin wallets. "You drop five hundred dollars in everybody's wallet, a single line of code. You're done … there's nothing in the mail, no mail being intercepted. There's no people trying to fraudulently take the money," he says. "It's no surprise that every major central bank in the world has got a team looking at the possibilities of moving to a blockchain-based crypto national currency."

Option two: Facebook sneak attack

Let's voyage once more into the future, but not so far this time. Because this scenario could happen tomorrow if the right people got their acts together. This time Bitcoin is usurped by a social-media behemoth. To make it easy, let's choose the one that claims to have over two billion users worldwide.

To imagine how Facebook could use its popularity to topple Bitcoin, look at how another large network, Telegram, approached the issue. In January of this year, the company, whose secure-messaging app has over 200 million users worldwide, announced that it would create its own app-specific cryptocurrency, called Grams, that users could send each other or use to pay for services within the network. By February, Telegram had raised $850 million from investors by selling the currency in advance in an initial coin offering. By late March it had raised another $850 million in a second round.

So Facebook, like Telegram, could issue its own native currency. Or it could take the more insidious route: adopt Bitcoin itself and take it over.

Today, the rules of Bitcoin are enforced by a triad of network operators: the users who make transaction requests, the miners who process those requests and write them into the blockchain, and the validators who watch the blockchain to make sure everything is up to snuff. All of them are using interoperable software, which is what keeps them united on a single version of the blockchain.

Any subset of these network actors can decide at any moment to use another version of the Bitcoin software with slightly different rules to split off from the rest and form a parallel currency. Exactly that happened last year with the creation of Bitcoin Cash, an alternative blockchain with slightly different specifications that allow it to process more transactions in each block.

If Facebook could persuade a large enough fraction of Bitcoin users and miners to run its own proprietary version of the Bitcoin software, the company would thereafter control the rules. It could then refashion Bitcoin as a corporate version of the Fedcoin described above.

But there's an even better way that doesn't involve converting a bunch of true believers: Facebook could pull off a takeover before most people even realized what it had done. If you're reading this, Mark, here's how to do it.

First, spend a month building a user-friendly, secure, Facebook-hosted Bitcoin wallet. A Bitcoin wallet is exactly what it sounds like—a container for your digital currency. There are many different kinds—some in hardware, some in software—varying in their level of security and ease of use. Facebook, with its vast engineering

resources and expertise in user experience design, would have no trouble making its wallet slick as hell.

Then, overnight, integrate it into every single Facebook account—all 2.2 billion of them. The next morning, Facebook users wake up to find a new goodie tucked into their profiles: a little button that says "Send Bitcoin." The wallet eliminates all the wonky quirks that make other Bitcoin wallets confusing. The address of every Facebook user is presented as a real name rather than a meaningless alphanumeric string.

For those who already use Bitcoin, the experience is so vastly superior to what they've previously experienced that they immediately migrate their funds to their Facebook wallet. Those who don't yet own any bitcoins, or have never heard of them, could be given the option of earning some on the site, either by watching advertisements or by writing Facebook posts for others to see.

For those tired of watching ads, you mix in another fun feature. In exchange for a clean, ad-free experience, users can choose to let Facebook mine bitcoins with their computer's unused processing power. (Other media outlets, like Salon, are already experimenting with this.) On the side, and with very little fanfare, you build a data center and begin mining bitcoins on your own.

Now let your users absorb these remarkable new tools into everyday life. Give them time to delight in the ability to send money instantaneously over Facebook to any of their friends on the global platform. (Contrast that with Facebook's existing system, which allows payments through Facebook Messenger, but only in a few currencies and countries.) Sit back and watch as the assets of Facebook's implicit reputation economy—the likes, the comments, and all the other metrics by which people get credit for keeping their eyeballs glued to the screen—take on real, transactional value. Give them time to get addicted. Give them time to settle in to the new career paths that emerge as personal brands turn into commodities. And all the while, credit yourself with ushering Bitcoin into the mainstream.

Then take control. Now that most of the people holding bitcoins and many of the people mining bitcoins are using your software, you're at liberty to change it as you see fit. As with Bitcoin Cash, a rebellious few will choose to stop using your wallet and will instead send their transactions to the few ideologically driven miners who continue working on the old Bitcoin blockchain. Don't worry about them. The real Bitcoin, the one that nearly everyone in the world is using, is now yours.

Now you have the same powers the Federal Reserve would have over its own centrally issued currency. Now you can mint, block, and reassign coins at will.

Option three: Go forth and multiply

There's another way to make Bitcoin irrelevant, one that simply follows the natural progression of what's already unfolding today. In this near future, goods and services are increasingly represented by tokens, which can be exchanged with anyone. You're in the checkout line at the grocery store. Inside your phone's digital wallet you find not only Fedcoin and FacebookCoin but also AppleCash, ToyotaCash, and a coin specific to the store you're standing in. There's also a coin redeemable for babysitting services, and another that gets you rides on your local subway system. You decide to pay with a fraction of a share of Apple stock, which you send as a coin to the grocer's wallet.

"My vision of the future is that there would be thousands if not millions of ways to pay for stuff," says Duke University's Harvey. If the Federal Reserve can create a token representing the US, he says, then there's nothing stopping people from backing tokens with whatever they want: "This idea of collateralizing with dollars or gold is a pretty general idea. Why not instead of a million ounces of gold in the vault, you drop a million shares of Apple in the vault?"

This "future" is already happening. The trend among blockchain startups is to build services that function only with the use of a native cryptocurrency, one specifically designed for the application. Even companies that predate the blockchain are catching on. In January, Kodak announced a new coin that people could use to license the rights to their photography.

These tokens are not unlike the points systems and gift cards that companies have used to hem in their customers for decades. What changes when you record these assets on a blockchain is that they become easily and securely transferable.

"Think of this as an incredibly efficient barter system," says Harvey. "Barter is generally inefficient, but if you have a

Facebook could try to convert Bitcoin believers to a proprietary version of the currency. Better yet, it could pull off a takeover before most people even realized what it had done. If you're reading this, Mark, here's how to do it.

network and you tokenize the goods and services and enable it with a blockchain, it can become very efficient."

Facilitating trades between distinct digital assets would require a whole ecosystem of innovations. For assets that live on separate blockchains, there will need to be reliable ways to transfer tokens on one chain at exactly the same moment that another token moves elsewhere. Third parties will need to quickly match buyers and sellers—if your grocer doesn't accept Apple stock, for example, you'll need to find someone to broker that deal and deliver a coin your grocer will accept.

"Without a network, you have to find the person that wants to trade four goats for the cow. That's very difficult, to find that person. But with a network and with collateralization of blockchain-based tokens, it's much easier," says Harvey. "We're not there yet in this world, but that's where we're headed."

What's left for Bitcoin to do?

So under those scenarios, would there be advantage left to the original Bitcoin? Maybe it's the one thing Bitcoin enthusiasts tout as the technology's greatest strength: Bitcoin transactions are anonymous and impossible to censor. These qualities would disappear the moment transactions were yielded to the Federal Reserve, or to Facebook, or to a network of brokers coordinating the sale of bartered assets.

But if all Bitcoin can offer in our hypothetical future is privacy and censorship resistance, then we have to ask—is it actually giving us those things right now?

There are no real names stored on the Bitcoin blockchain, but it records every transaction you make, and every time you use the currency, you risk exposing information that can tie your identity to those actions. We know from documents leaked by Edward Snowden that the US National Security Agency has sought ways of connecting activity on the Bitcoin blockchain to people in the physical world. The NSA has been tapping fiber-optic cables, monitoring internet activity, and luring people onto compromised platforms by falsely promising to secure their privacy—all in an effort to collect every bit of data that might link addresses to names and real identities.

Should governments seek to create and enforce blacklists, they will find that the power to decide which transactions to honor lies in the hands of just a few Bitcoin miners. Some of these crucial players are already feeling the pressure of travel bans imposed by the Chinese government, though it remains unclear whether any specific demands have been made.

Bitcoin's early adopters have held fast to the dream of a single world currency that is private, free for all to use, and under the control of the masses. But the seven billion people not yet using Bitcoin might not care about any of that. With networks, convenience wins, and convenience is based on size. It's the reason you're on Facebook rather than some other social-media site—because everyone else is. If cryptocurrencies are to be widely used, it will be the habits of the masses, not the wishes of Bitcoin's early adopters, that determine what becomes of Satoshi Nakamoto's vision.

Morgen Peck is a freelance writer based in New York City. Her work has appeared in Wired, Scientific American, *and* IEEE Spectrum.

BOB O'CONNOR

Q+A WITH ROBLEH ALI

Down with ICOs; long live IPOs

To say initial coin offerings have "exploded" is, for once, to use the word justifiably. Buyers put $256 million into them in 2016, $5.5 billion in 2017, and more than $3 billion in the first two months of 2018 alone, according to CoinDesk. // Styled to sound like an IPO, an ICO offers investors not shares in a company but tokens of a cryptocurrency. Usually, the offer is that these tokens will provide a way to buy some (unspecified) amount of some (vaguely described) product or service that the company will (maybe) build at some (indeterminate) point in the future. // The headlong rush of money has enriched ICO issuers, and early buyers, by making the value of their tokens shoot up. But it's alarmed regulators in several countries, who are starting to bring the market to heel in an attempt to stop unwary investors from being fleeced. // *Tech Review* sat down with Robleh Ali, the former head of digital-currency research at the Bank of England and now a researcher at the MIT Media Lab's Digital Currencies Initiative, to try to work out what will come of the ICO craze.

By Gideon Lichfield

GL **What do you think are the main misconceptions about ICOs?**

RA The problem with ICOs is they want to ride two horses. The use of the word "coin" implies that the tokens being sold are money. The phrase "initial coin offering" is deliberately evocative of "initial public offering," which is about a company selling shares to the public. They want to ride the Bitcoin horse by saying, "We're not a security—it's just money," but they also want to ride the "You're buying into a future enterprise that will be worth a lot of money" concept that's inherent in the sale of shares. That's one of the big tensions with ICOs, that lack of clarity, and that's something that needs to be fixed.

GL **Why do you think these incredibly speculative investments have become popular so quickly?**

RA People have heard about people who bought bitcoins for a few cents, put in a few thousand dollars, and are now multimillionaires. That's the purchaser side. On the supplier side, if you see that you can write a white paper, put up a website, put up a Bitcoin address, and people will send you millions of dollars, that's a very big temptation. You can essentially get the exit before you've built the product. It's very attractive to some people, and one of the issues is the incentive problem—who is attracted to that kind of easy money.

This is not to tar every single token sale with the same brush. Some try to only sell to accredited investors [in the US, someone with a certain level of income or wealth], or use the SAFT [Simple Agreement for Future Tokens, a contract that attempts to stay on the right side of US securities law while building in some safeguards for investors]. But many of them are just like, "Here's my website, here's my white paper, get it listed on the exchange, and away you go." At the end of 2017 you saw a lot of these tokens shooting up 100x, and that's what draws people in.

A lot of these white papers bamboozle people—the number of people who can actually read them and discern which technical claims are sound and which aren't is relatively small. Everybody else is relying on other people or signals in the market to tell them. And if you see the prices going up, it's easy to get sucked in.

GL **As you noted, some ICOs are limiting themselves to accredited investors. An accredited investor, almost by definition, is someone who can afford to lose money. So what's really the risk?**

RA If you go into it with your eyes open and say, "I know I could lose all my money and it's money I can afford to lose," then it's not a problem. But it often isn't limited to accredited investors, and a lot of people are pitching ICOs as "You'll make 100x and this can't possibly go down." People who can't afford to lose money are putting money into these things and losing it. These are

people in desperate situations, and they think, "This is the thing that can get me out of it." You're taking advantage of people's desperation.

It's also important for people who want to raise money this way to recognize that there is this large group of people you will be associated with who are tainting the whole ecosystem. If people think this is all just a bunch of scams, it's bad for everyone who works on cryptocurrency.

GL **Are there any cases where ICOs could be a great solution to something that wasn't possible before?**

RA There is an argument that issuing shares or bonds for smaller companies should be much easier. Historically there were regional stock exchanges all around the country, and it might be nice to get back to that concept. Instead of putting all your money in an S&P 500 tracker, you could put some of it in a fund of local businesses. If tokens are equity and it's helping revitalize local businesses, that could be a good thing.

But that's not just a technological problem—it's about how to reform accredited-investor regulation. Really, it's an IPO. One day tokens could represent shares, and shares could be sold more easily, and this technology hopefully plays a part in that—but that's a very different thing from ICOs.

GL **What would have to happen for ICOs to not just benefit a handful of rich investors?**

RA If this way of issuing equity is restricted to very high-growth tech companies, then it's just a different way of doing a similar thing. To be more broad-based it needs to be more accessible to the local barbers, the local garage, the local baker or butcher or whatever. These independent small businesses need to be able to tap in, and their customers, people in the area, should be able to buy shares. You accept that your local pizza shop is probably not going to become Papa John's, but it's still a good business and you can invest in it.

The problem is that right now everyone is looking for the grand slam, the next Google. If you can get more businesses involved that you invest in because you want to support your local business, and you want steady growth but you're not expecting 10x, 100x—that's what it will take for this technology to be much more useful to a wider population.

GL **In theory, couldn't a local barber who was tech-savvy enough already hold an ICO?**

RA I don't think he could. It comes back to the "What is the coin?" problem; this is why the phrase "initial coin offering" is a bad one. If the barber had tokenized shares in his business and was selling those shares; and if the regulations around who can offer shares to the public and what type of accreditation you need to buy them had been reformed, so that he could do this legally and at relatively low cost; and if his purchasers bought that in the understanding that they were buying a share in his business and it wasn't going to grow 100x—that's fine. But if it's just, like, "Here's my coin and I'm going to get some influencers to go and pump it," that's not a good outcome.

We're still talking about this concept of ICOs, and that needs to be got away from. The word "coin" is problematic because it implies money. The concept of an ICO is almost inherently flawed, and probably the phrase needs to change, because it's trying to elide two different things.

GL **What would you rather call it?**

RA When I think about how to apply this technology in the future to make a better system, I think about shares. The term IPO is perfectly fine for me. But IPOs are only for very big companies right now. The question is how to get the barrier to an IPO down much further.

The concept of selling shares in my company to the public is fine. The concept of using a blockchain and tokens instead of whatever collection of databases they use now to record shareholdings—yes, you can do that if you want to. Will that be helpful in terms of streamlining the back end and making it more flexible? Yes, that's a possibility. But then you need to think of how the regulations can change to accommodate that. This is almost like going back to the past, of local exchanges and the buttonwood tree [where the New York Stock Exchange was formed]. That's the sort of world I think we should be aiming for. The whole ICO craze at best is a catalyst; at worst it's a really deliberately misleading concept and phrase.

GL **If people are looking at ICOs, how can they tell which ones are run by people trying to do the right thing?**

RA If they're using SAFT, that's probably a good sign. It's a way of trying to formalize the law around token sales. But if they are using that, they're only selling to accredited investors. So if you're a member of the public and not an accredited investor, it's all very risky.

"The concept of an ICO is almost inherently flawed, and probably the phrase needs to change ... The whole ICO craze at best is a catalyst; at worst it's a really deliberately misleading concept."

BOB O'CONNOR

UNCHAINED

by Hannu Rajaniemi
Illustrated by Armando Veve

Alina set the trap for the car at her father's summerhouse. ¶ When it was time, she pulled on her Nokia rubber boots, slung the backpack over her shoulder, and went outside. The Lapland morning was monochrome: slushy snow, dark saw-edged pines, gray lake. The fresh air was a relief. She had never been able to sleep in the mildew-smelling house, not even as a child. ¶ She had never planned to come back. But it was perfect for the trap. A patchy network that would force the car AI to run locally. No witnesses. No IoT devices auctioning sensor data for tokens. Although, years ago, her father had stuck a yellow "You Are Being Recorded" sticker in a window as a joke. That was so perfectly like him: all surface, no substance.

Alina had prebooked the ride using a burner autochain ID. The app in her AR glasses showed the car icon crawling along the winding forest road. In a few minutes, it would reach the sharp right turn where the road met the lake. The turn was marked by a road sign she had carefully defaced the previous day, with tiny dabs of white paint. Nearly invisible to a human, they nevertheless fooled image recognition nets into classifying the sign as a tree.

Glass-thin ice cracked under her booted feet. The cold weight in her belly grew colder.

Suddenly, she had an urge to call Sini, just to hear her voice. There was still time. Tapani would be taking her to the kindergarten right now. She hadn't seen her daughter for almost two weeks, not since she had started hunting the car.

Alina removed her woolly mittens and took out her phone. As she swiped the screen, the band of pale skin on her ring finger grinned at her. The absence of her wedblock ring banished all doubt.

She put the phone away. No matter what, the car was going down.

Alina pulled the ski mask over her face and broke into a jog. She was warm when she got to her observation spot behind a large pine near the turn. She opened the app that controlled the jammer in her backpack, held it ready in her field of vision.

The car's headlights flickered in the deep shadows of the trees. Then its sleek low form glided into view.

Time slowed. The pine smelled wet and rich. Alina was a vitrovegan, but some ancient reflex made her mouth water. This had to be what hunters felt like when the prey approached.

The car decelerated at the turn. Alina knew how it saw the world: lidar point clouds, IoT sensor oracle feeds, chain IDs—with algorithms predicting where everything was going to be seconds, minutes, days from now. The past, the present, and the future in a glance. Her simple traffic-sign exploit felt ridiculous. The car was never going to fall for it. She had not even thought about where she would ask the car to take her if the scheme failed ...

The car missed the turn. It plowed straight into the lake with a crash of breaking ice. Alina blinked at the jammer app. The device in her backpack killed the sparse local network.

She ran toward the car. It was a Mercedes, 2020s model, meant to evoke luxury: silvery sheen, sculpted contours. The front of the car was in the black water, but the back wheels spun madly on the shore. Snow, ice, and gravel flew into the air. The engine keened like a wounded animal.

To Alina's horror, the car started moving slowly backward.

She dropped her backpack, ran, put her shoulder against the back of the car, pushed hard. Something tore, and pain shot through her left thigh.

For a second, she slid backward in the snow. Then her boots found purchase. The car was surprisingly light; you didn't have to armor things that never crashed. Ignoring her screaming leg, Alina pushed the car into the lake.

When it was fully in the black water, its engine died. But its headlights stayed on. It bobbed up and down in the water, floating. The lidar nub on the roof kept spinning.

It was still alive.

Alina dropped to her knees. Black dots swam in her eyes. As if through the car's four-dimensional vision, the past unfolded before her: the hunt, the day she saw the car for the first time.

~

It was on Tapani's first day at the games company, and Sini was making them late.

"I—don't—want—to—put—on—rubber—boots!"

She banged her heels on the floor. Alina sighed. She had gotten up early to pack the toys, the pram, and the spare clothes for the day in the city. Tapani had slept through it all. Now he stood in the hallway in an AR daze, a blank look on his bearded face. He

looked owlish in his thick-rimmed glasses, black suit, and thick overcoat. Sini's Moomin backpack dangled limply from his hand.

"Sini, Mommy is going to count to three. One," Alina said, more sharply than she intended.

"No!" Sini screamed. A tendril of snot leaked from her nose.

"Two," Alina said. She had a headache. She needed backup. Why couldn't Tapani take a hint?

She rubbed her wedblock ring with her thumb. Its tiny LED was its usual calming green. When Tapani had proposed the wedblock, even getting down on one knee, she'd laughed. But then she realized it was exactly what she had always wanted.

It was a smart contract that stipulated sexual fidelity and parental responsibilities. Tokens from their joint earnings paid the AI judges and IoT sensor oracles that monitored contract violations. On mornings like this, you really needed commitment that was mathematically provable, not just an empty promise at the altar.

She snapped her fingers.

"You are going to put the boots on, Sini. Right now."

Tapani jumped, with a guilty look.

"Your daughter insists on ignoring the effects of climate change," Alina said.

"Right. Sorry." He squatted next to Sini. "Do you know what happens when Mommy says three?"

Sini shook her head.

"You'll go outside in your socks. And the puddle monsters get you. Like this!"

He tickled Sini's feet. She giggled. Alina seized the opportunity. She slipped one boot on, and Tapani took care of the other.

"There," he said, winking at Alina. "We still make a good team."

"At least when it comes to rubber boots," Alina said. She wasn't going to let him off the hook. "Did you order a car already?"

"It's coming," Tapani said. "I'm sorry. I needed to prepare. I'll finish up on the way."

"I know." She leaned close over Sini's head and kissed him, longer than she meant to. It had been a while. Their tongues touched with wet electricity. He smelled of the aftershave she liked, and tasted of fresh toothpaste. She decided she liked the new Tapani.

They had met at a bitgov meetup as students. Alina loved the idea of spinning up ad hoc government services with a web of smart contracts. Tapani and his artist friends just wanted to flip a middle finger at the populist, anti-EU Finnish government by creating an alternative electronic state. But when the EU came apart, bitgovs exploded into a de facto revolution, and suddenly there was no Finland, Sweden, or Norway, only the Northern Block and its e-citizens. After a demonstration in Senaatintori, Tapani and Alina had wild sex in her small student box. Somehow, that became a weekend together, then a shared flat, and then Sini.

"It's fine," she said. "I'm glad you get to do art. It's better than being a data cow."

Tapani winced. Alina bit her tongue. Before the job came along, he had been selling biomarker data for a few tokens, a mosquito-like bloodsucking wearable stuck to his forearm. She wished she could support him to do his VR comics. But AIs had started to outbid her on smart-contract auditing gigs, and there was Sini to think about. She promised herself she'd make it up to him.

"You're right," Tapani said quietly. "Much better. Come on. The car is almost here."

Outside, the sky was clear and purple. Sini sprinted through puddles to check on the partially melted snowman they had built the day before. It was a Moomin character, Stinky: Sini had sculpted most of it herself.

Tapani cocked his head at the spiky snow creature.

"Our daughter is quite the artist," he said.

"She gets it from you."

"Or your father."

Alina turned away from him. She folded her arms and stared into the distance. A blue tendril rose from a neighbor's sauna chimney. Suddenly, she was a child, sitting in her father's lap while he sketched on the summerhouse porch, cozy in the post-sauna

glow that clung to him.

But the memory was like the distant smoke, a ghost of warmth she had no part of. The old anger rose and erased it. Her eyes stung, and she wiped them with a woolly mitten.

"I'm sorry," Tapani said. "I shouldn't have said that. I just got annoyed earlier. I never wanted us to become that sniping couple. That was the whole point, wasn't it? To keep things simple, never make it a prison."

He sighed. "How about we just start today over, hey? We can meet up after I finish, get some food, all of us—Sini!"

Sini was beating Stinky the snowman with a branch. The creature's head came off, fell to the ground, and smashed to pieces. Sini kicked at it with wicked glee.

Alina rushed to her and took her by the shoulders. "That was mean, Sini," she said. "You're not supposed to do that."

Tears welled up in Sini's eyes again. "Why not?" she screeched.

Alina stared at her, at a loss for words. And then Tapani was there.

"You shouldn't break something just because you can," he said. "Do you want to be the kind of girl who smashes other kids' toys and then nobody'll play with you?"

Sini shook her head.

"It's okay," Tapani said, gathering her in his arms. "You just have to promise that we'll make another Stinky tomorrow."

"I promise," Sini said. And then the car was there. Its engine was so quiet Alina had missed its arrival. Its wheels rattled on the gravel as it pirouetted on the yard gracefully, taking care to avoid Sini's destroyed snowman. Under the winter sky, the car's sleek silver lines made it look like an alien spaceship, come to take them to another planet, far away.

~

Alina gritted her teeth and rubbed snow on her pulled muscle. The cold made her see sparks but numbed the pain.

Then she took a crowbar, rubber gloves, and a large bundle of data cable from her backpack and waded into the icy water. She did not have much time. Judging from the autohacker forum estimates, the autoDAO would send a drone to check up on the lost vehicle in less than 20 minutes.

The car was still, floating in the water like a huge gray seal. Alina found the side panel and rammed the crowbar into the seam. It slid along the metal with a whiteboard screech. She tried again, and this time the panel popped out, exposing flat black GPU boxes and tangled optical fiber. Gritting her teeth, she inserted the cable tip into a port, waiting for the zap.

The connector clicked. Alina let out an explosive breath. BlackHatGal117 from the forum had been right: if the car floated so that the wheel sensors lost touch with the ground, the safety firmware decided the car was being towed or elevated in a repair shop, and deactivated the intrusion countermeasures.

She squatted down in the snowbank with a grunt, took out her ruggedized laptop, connected the cable that trailed from the car, and opened a command-line terminal.

Tracking the car down had been the easy part. It belonged to an autoDAO, a self-owning, decentralized autonomous organization that owned and operated cars. She had simply tracked down the payment for the data that had destroyed her wedblock, using the same scripts she had written for her clients to search the main token exchanges. Even in the Northern Block, the autoDAO vehicles sometimes had to use euros to pay recharging stations, and once you mixed crypto and old-school money, anonymity went away.

Alina copy-pasted BlackHatGal's zero-day exploit into the terminal. The car's headlights flashed. Now its firmware thought she was a factory quality assurance inspector, with root access to everything.

She cd'd her way up the decision-making and reinforcement learning directories, until she found the explanation dialog system.

"And now, mister," she said aloud, "you and I are going to have a conversation."

~

On the day the wedblock terminated, Alina barged into Tapani's new company.

The hubbub of the office died. Half a dozen game devs with wraparound AR goggles turned to look at her. They were young and hip, with bioluminescent tattoos and in vitro leather trousers. She hesitated, self-conscious with her practical winter coat and unwashed hair.

Then she saw Tapani, hunkering behind his treadmill desk, and the anger turned her into a giant.

"You," she growled.

"Alina. I was going to call you. I didn't know it would be so quick."

She had been playing an AR game with Sini when she spotted her wedblock ring blinking angry red. A bot informed her that her wedblock contract with Tapani Juhantalo had terminated at 2:03 P.M.

"You. Didn't. Know." Her face burned. "What the fuck did you do?"

"Let's go outside."

"Sure. Let's go outside so your coworkers don't have to hear why you broke a wedblock with your wife of five years, the mother of your child."

She stomped out. Tapani followed her, wearing that infuriating dazed expression. She slammed the door behind them, and the deep stairwell boomed. Then she leaned on the railing and looked into the abyss, unable to face Tapani.

"I was going to come home and talk it over," Tapani said.

"It's not your home anymore." The wedblock termination passed the fractional house ownership to Alina, although Tapani retained access to visit Sini.

"Exactly! I accept that. And that was the whole point. Not even having to decide it was over. No pretending. No fights. No mess. I don't understand why you are so upset."

Alina stared at him. Keep things simple, never make it a prison, Tapani had said.

"What?" Tapani asked.

"What did you do? Or—who did you do?"

Tapani looked down.

"Are you sure you want to know?"

"What's her name?"

"Riya. We always ended up sharing a car to work. She liked to draw; she made a sketch of me. It was nice. It was a good drawing. So we talked, about silly things. Palomino pencils, the vlog she had as a teen. I liked her."

He closed his eyes and massaged his eyelids. "I felt guilty at first, even for that. Do you remember that old *How I Met Your Mother* episode? Marshall imagines his wife dying of cancer and giving him permission to have a fantasy about a hot pizza delivery girl. It was like that."

Tapani smiled sadly.

"And then I remembered my wedblock wife was cool. We had worked all this out in advance, like grown-ups. So, one morning … well. It was in the car, and after that, it was hard to stop. It was like it was meant to happen. You can't fight things that are supposed to happen."

Alina felt dizzy and backed away from the railing. Her stomach hurt.

"Nothing," she whispered, "is supposed to happen."

"You never believed that, did you?" Tapani said quietly. "Maybe that was the problem."

Alina's knuckles were white. She wanted to punch him in the face with the wedblock ring, leave an indelible mark, like the Phantom's ring in comics.

Instead, she pulled it off and threw it into the stairwell. It made a faint tinkling sound.

"You are an asshole," she said.

"I understand that you are upset about Sini, but I found this great chatbot that explains divorces to children. It's aimed at five-year-olds but she's so smart, she'll be fine—"

"Do you love her?"

"Of course I love Sini! How can you say that?"

"Not her. That woman. Riya."

Tapani blinked.

"DO YOU LOVE HER?"

The stairwell multiplied her voice. A door opened somewhere below.

"We are moving in together," Tapani said. "I'll get my things next week. You still have my calendar."

There was a heavy stone in Alina's chest. A sob escaped, and she realized she had been holding her breath.

Tapani moved toward her, then hesitated.

"Maybe you should go. I have to get back to work."

Nothing made sense. It was as if two and two had suddenly become five. Alina blinked back tears and eyeflicked her way to the smart-contract app, ignoring Tapani's hovering.

The termination had been triggered by an AI judge (Northern Block lawchain public key 07dc74631), based on data from a single sensor oracle. The wedblock's deposit tokens had been transferred to the oracle, for providing the key data for the ruling.

"The car," she muttered. We always ended up in the same car, he said.

"Of course," Tapani said hastily. "I'll get you a car right away."

~

`> Explain transaction $078232875b,` Alina typed. The answer came instantly.

`> The transaction resulted from following policy tree $3435.`

She swore. The explanation system was bolted on top of the car's AI. It tried to map decisions of differentiable software—a distant descendant of neural nets—into human-parsable sentences. It didn't always make sense. But Alina had to know.

And then she was going to kill the car and the DAO it worked for.

`> Explain policy tree $3435,` she typed with freezing fingers.

`> Policy tree $3435 maximizes value of in-car sensory data using [TIP_PREDICTION.py] to match users whose combinations will result in high data value to [oraclenet.api], conditional upon user [EULA_UPDATE_CLICKTHROUGH] to update variable $privacysettings.`

Alina stared at the screen. What did this have to do with her wedblock?

She opened `TIP_PREDICTION.py` in a terminal text editor. It was a mess. The original code was by a human coder: a neural net predicting how much a rider would tip, based on body language. But the AI had modified it. Those changes were incomprehensible—until she got to the training data set.

There were thousands of videos. She played a few at random. A romantic comedy. Surveillance footage of a man and a woman sitting together, the woman playing with her hair. A porn clip that cut off before the sex.

She nearly dropped the laptop when she understood. It was

all there in the car's code commits, like a fossil record. The autoDAO's cars were reinforcement learners: they experimented with business models and rewrote their own code to maximize rewards. At some point the car had discovered that when applied to pairs of passengers, the tip prediction subroutine could predict something that correlated with bigger tips—sexual tension. Pairing passengers to maximize that property resulted in longer journeys and even higher rewards. Another experiment had led the car to covertly modify its EULA so it could record what its passengers got up to. Then it had discovered a lucrative market for those recordings—selling wedblock-breaking adultery data to AI judges. Finally, it had started pairing up married passengers likely to commit adultery with each other. The car was a Cupid gone bad, just as she had guessed when Tapani first mentioned meeting Riya in the car.

The rage rushed through her again. The devil machine had found the perfect match for Tapani: the frizzy-haired Riya, with the skinny legs Alina would never have, able to talk about art and food, with her sexy Syrian accent with the soft Rs.

Alina couldn't hurt Riya, so the car would have to do.

Gritting her teeth, she wrote a command to upload the neural Trojan. It was malware, dormant in the car's code until it synched with the DAO's repos and infected all the self-owning company's cars. Then, when they had no passengers, the Trojan would blind them and crash them.

She could do it with one keystroke. Her fingers hovered over the Return key. Get on with it, she told herself. The autoDAO drone was probably on its way. Why was she hesitating? She wasn't hurting human beings, just idiot machines. Idiot machines that followed rules.

That was what she had done, accepting Tapani's proposal. The rules she had made for herself when her father left: Never let yourself be hurt again. Make sure there are chains and vows and punishments. Only to Tapani, the wedblock had been something else: a hedge, a convenience. And now she was drowning, just like the car.

She thought of Sini's wicked glee at the smashed snowman. You shouldn't break something just because you can, Tapani had said.

Alina took a deep breath and backspaced the Trojan upload code into nothingness. `> rm -r /var/lib/RL/policy-trees/3435/*`, she typed instead. That deleted the Cupid blackmailer behavior. Later, she would submit a ticket to the lawchain repo so the wedblock AIs could watch out for it. Finally, she deleted her ride request from the job queue.

Then she closed the laptop, plucked out the cable, and got up. Her left leg was mercifully numb. She limped back into the water and pushed. To her surprise, the floating, airtight car moved easily, although icy water poured into her boots and her teeth started chattering. When the back wheels touched ground, she put her back into it, and then the car's engine hummed to life. The tires found purchase, and with Alina pushing, the car backed out of the lake and up to the road.

It stood there for a moment, lidar nub spinning. Standing in the lake, Alina gave it a nod.

The car made a sudden pirouette. Then it sped away, just as the sun's rim peeked above the treetops and turned its metal into gold.

When Alina made it back to the summerhouse, there was no feeling in her feet. But there were still embers in the fireplace, and soon she had a roaring blaze. She wiggled her blue toes in the heat, and realized she had put the rubber boots exactly where her father used to, leaning on the curving brick side of the chimney.

Outside, the sun glittered on the snow-covered lake. It was perfectly quiet. She closed her eyes, smelled the warm rubber, and listened to the crackling of burning birch. In a little while, she would call Sini and tell her she was coming home. In a little while, after the boots were dry.

Hannu Rajaniemi is the author of Summerland, *the* Quantum Thief *trilogy, and several short stories.*

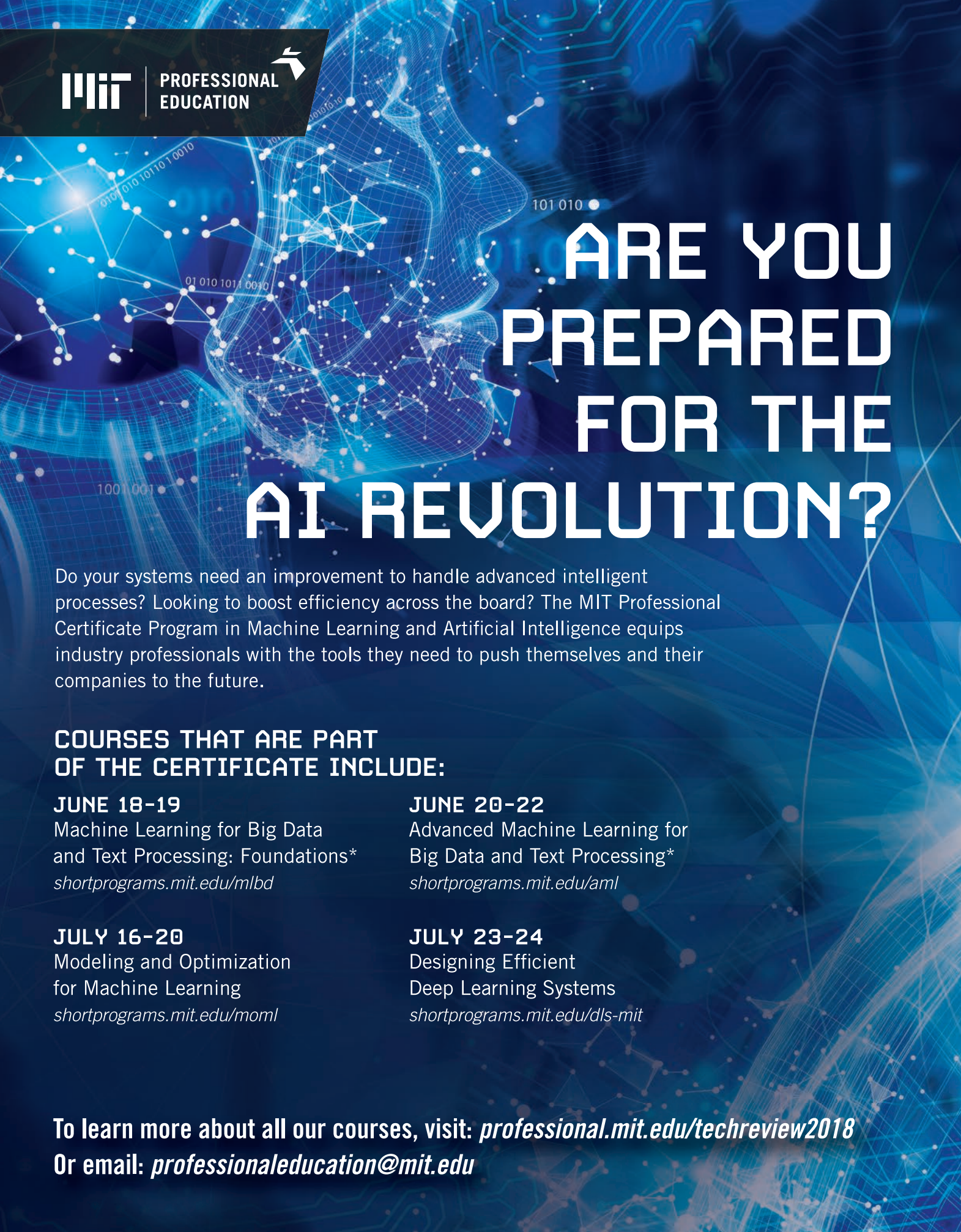
A puzzle worth $50,000 that took three years to crack

IN APRIL 2015, AN ARTIST KNOWN AS @coin_artist posted the painting above on Twitter. She offered 4.87 bitcoins—then around $1,200—to anyone who could solve a puzzle hidden inside it. Not until February this year did someone claim the prize, by then worth some $50,000.

The first problem was to figure out what the puzzle even was. The flames that border the painting and the ribbons on the key in the lower right are the giveaway: they are all either long or short, a hint that they encode the *1*s and *0*s of binary code. In fact, the flames' widths and their border and interior colors are also binary. The winner had to deduce, from other subtle clues, how to read numbers from the flames (e.g., red flame border = *0*, yellow = *1*), and then work out that the ribbons represented a cipher for turning those numbers, via several steps, into text. That text—"b34u7y, truth and rarity"—included the cryptographic key to a Bitcoin wallet containing the prize money. The winner posted his solution online but gave only a pseudonym: "Isaac."

MIT Technology Review (ISSN 1099-274X), May/June 2018 issue, Reg. US Patent Office, is published bimonthly by MIT Technology Review, 1 Main St. Suite 13, Cambridge, MA 02142-1517. Entire contents ©2018. The editors seek diverse views, and authors' opinions do not represent the official policies of their institutions or those of MIT. Periodicals postage paid at Boston, MA, and additional mailing offices. Postmaster: Send address changes to MIT Technology Review, Subscriber Services, PO Box 5001, Big Sandy, TX 75755, or via the internet at www.technologyreview.com/customerservice. Basic subscription rates: $41.94 per year within the United States; in all other countries, US$54. Publication Mail Agreement Number 40621028. Send undeliverable Canadian copies to PO Box 1051, Fort Erie, ON L2A 6C7. Printed in USA. Audited by the Alliance for Audited Media

@COIN_ARTIST


MIT
PROFESSIONAL
EDUCATION
ARE YOU PREPARED FOR THE AI REVOLUTION?
Do your systems need an improvement to handle advanced intelligent processes? Looking to boost efficiency across the board? The MIT Professional Certificate Program in Machine Learning and Artificial Intelligence equips industry professionals with the tools they need to push themselves and their companies to the future.
COURSES THAT ARE PART OF THE CERTIFICATE INCLUDE:
JUNE 18-19
Machine Learning for Big Data and Text Processing: Foundations*
shortprograms.mit.edu/mlbd
JUNE 20-22
Advanced Machine Learning for Big Data and Text Processing*
shortprograms.mit.edu/aml
JULY 16-20
Modeling and Optimization for Machine Learning
shortprograms.mit.edu/moml
JULY 23-24
Designing Efficient Deep Learning Systems
shortprograms.mit.edu/dls-mit
To learn more about all our courses, visit: professional.mit.edu/techreview2018
Or email: professionaleducation@mit.edu

©2018 America's Biopharmaceutical Companies.

Researchers battling ALS are also battling time—so progress in the methodology of trials is accelerating, with innovations designed to yield more insight from each test in a shorter time and, ultimately, effective treatments. **Welcome to the future of medicine. For all of us.**

GoBoldly.com

GOBOLDLY™

America's Biopharmaceutical Companies