THE WORLD BITCOIN CREATED

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

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

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

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

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

CORE CONCEPTS

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

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

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

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

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

HASHING A cryptographic method that uses a mathematical function to condense any amount of data into a unique string of alphanumeric characters of a certain fixed length—called a hash value. This creates an easily verifiable digital fingerprint for the hashed data. If even a single bit of the original data is changed or corrupted, the fingerprint that emerges from the hash function will be drastically different, making it easy to

detect errors or tampering. Hashes are also “one-way”—the data cannot be reassembled or extracted from the fingerprint.

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

HOW BLOCKCHAIN WORKS

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

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

- 2 The transaction is broadcast for verification to a peer to peer network of computers operating the blockchain. Every node on the network is equipped with a procedure for verifying whether the transaction is valid or not. (In a Bitcoin transaction, for example, the network would verify whether those paying actually have the amount of Bitcoins they say they do.) Once the network has reached a consensus, algorithms package up the validated transaction with other recent transactions into a block.
- 3 Software creates a “fingerprint” for the new block by hashing the data inside it, together with two other pieces of information: the fingerprint of the preceding block and a random number called a nonce.
- 5 The validated block is added to the blockchain with a digital fingerprint that also mathematically encodes the validated fingerprints of every block preceding it. These nested fingerprints make the blockchain increasingly secure with every new block that gets added because altering a single bit of information anywhere in the blockchain would drastically change not only the fingerprint of that particular block but every subsequent one in the chain as well.
- 4 Special nodes called miners begin competing with one another for the right to add the new block to the blockchain. Their computers perform a tedious set of hash based calculations over and over again by trial and error, hoping to generate a solution that satisfies an arbitrary rule defined by the network. (On the Bitcoin blockchain, the miners are searching for solutions—or “hash values”—that have a particular number of zeros at the beginning.) Whoever is first to complete this proof of work process and find the matching solution successfully “mines” that block, earning a financial reward.
  AS AN ALTERNATIVE: Proof of work mining is energy intensive, so some new blockchains are doing away with it, instead using a preapproved network of “validator” nodes who can notarize transactions via an alternative process called proof of stake. Because this process doesn’t rely on difficult hashing calculations, it uses much less computing power (and much less electricity).

BLOCKCHAIN DEMYSTIFIED: FREQUENTLY ASKED QUESTIONS ABOUT A RAPIDLY EXPANDING TOPIC

1. ARE BITCOIN AND BLOCKCHAIN THE SAME?

No, but it’s easy to get them confused because they both came into public awareness in 2008, when Satoshi Nakamoto published his paper describing how to implement them simultaneously. Bitcoin is one type of cryptocurrency. What people call “blockchain” is a technology that makes Bitcoin possible—an infrastructure that can be used for tracking many types of transactions. Blockchain technology exists without

Bitcoin—but not the reverse. Think of Bitcoin as a kind of application that runs “on” the blockchain, much like Web sites run on the Internet.

10% Predicted amount of the world’s gross domestic product that will be stored in blockchain based technology by 2025, according to a 2015 survey report from the World Economic Forum.

WHO IS USING BLOCKCHAIN TECHNOLOGY?

FINANCIAL INSTITUTIONS: Global banks and investment institutions are researching and pursuing blockchain projects, sometimes joining forces in consortiums. Since 2012 Ripple has been a thriving, blockchain-based system for settling international transactions among banks. Start-ups such as Bloom intend to deploy blockchains to credit reporting, hoping to end data breaches like the Equifax hack.

GOVERNMENTS: Delaware and Illinois use distributed ledgers for birth certificates. A Vermont law allows blockchain technology to verify the authenticity of legal documents. Dubai integrated blockchains into many of its administrative services, such as obtaining licenses. In 2016 Tunisia began issuing a blockchain-backed version of its digital national currency called the eDinar.

TECH ENTREPRENEURS: The Ethereum network—which was designed to support new applications, rather than just a digital cash ecosystem like Bitcoin—is like an App Store for blockchain start-ups.

Hundreds of projects and businesses are running on it. One notable: We Power wants to let households buy and sell renewable energy (from, say, roof-mounted solar panels) directly to one another.

COPYRIGHT AND IP HOLDERS: U.K. musician Imogen Heap started Mycelia, a tech incubator that tracks metadata associated with creative works, cutting out intermediaries like iTunes.

NONPROFITS AND AID GROUPS: The BitGive Foundation is boosting the accountability of philanthropic giving. And the United Nations World Food Program is streamlining how it tracks and delivers assistance to Syrian refugees in Jordan.

ACADEMIC INSTITUTIONS: Forget sheepskins. The Blockcerts project wants to make all manner of academic and professional credentials more trustworthy and shareable.

ASSET MANAGERS: London-based Everledger is targeting the diamond industry by recording the attributes and provenance of each precious stone. Fine wine and art are tracked, too.

JOURNALISTS: To push back against fake news, Civil gives news makers a platform to create ad-free, inalterable journalism that’s immune to outside interests (Russia; Facebook) and supported by readers.

REGULAR PEOPLE: For migrant workers who send money to their families back home, using

Bitcoin costs less than using Western Union, which is why an estimated 20 percent of international remittances between South Korea and the Philippines now rely on it. It’s not just for cyber libertarians, and it goes way beyond finance. Here’s an incomplete lineup:

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

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

Why would a hard-to-understand cryptocurrency with no government guaranteeing its value as “legal tender” seem like a better bet than a more traditional value-holding commodity such as gold? For one thing,

converting Venezuelan bolivars into Bitcoin is simply a lot easier for ordinary folks—anyone with access to the Internet can do it. Because Bitcoin has no physical form, you don't have to stash it somewhere unsafe—like a mattress or, in Venezuela's case, a bank. Of course, Bitcoin doesn't have a stable value, either. But while the bolivar has nose-dived, the value of a Bitcoin is at least trending ever upward. In a country where inflation is expected to exceed 2,300 percent in 2018 (according to the International Monetary Fund), it seems like a reasonable risk to take.

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

2 WHERE DOES THE VALUE OF A CRYPTOCURRENCY COME FROM?

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

77% of the global financial services industry is expected to adopt blockchain as part of a production system or process by 2020, according to PwC.

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

Bitcoin is the world's most popular digital currency. But it's also wildly speculative, and many financial experts point to its legendary volatility: the currency's value has risen more than 10-fold since 2016, but it lost 40 percent of its value in a span of two weeks in September 2017—only to regain

(and surpass) it just as quickly. (Who knows what it will be by the time you read this.) To others, the network's technical limitations—it is sluggish at handling transactions—combined with its unsustainable mining costs make it the equivalent of a financial time bomb. "We don't bet on Bit-coin," says Charlie Morris, chief investment officer of Next-Block Global, a firm that invests in blockchain technology.

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

ARE WE FACING THE END OF CASH?

It may seem that printed money is headed for the same fate as newspapers. But experts say that cash is far from dead. "We're still using great piles of paper to pay for things like international shipping of sea containers," says Vinay Gupta, CEO of Mattereum, a legal services firm for smart contracts. "The system is not so broken that people are willing to tear it up." The trouble with Bitcoin and Ether is that while they can function as a store of value or unit of exchange, they're not accepted as legal tender in enough places to compete with cash. In places such as Kenya, where few people have traditional bank accounts and "mobile money" services such as M-Pesa have made saving and sending money by phone much easier than exchanging physical cash, cryptocurrencies might seem like a natural fit. But mining still requires a lot of processing power—not a common resource in Africa, where inexpensive feature phones outsell

smartphones and not many own PCs. The computations required to secure blockchain transactions could, in theory, happen on “your old Nokia SIM card,” Gupta says. Still, cold, hard paper won’t soon disappear.

3. IS THE BLOCKCHAIN A NEW KIND OF INTERNET?

Not quite, because the blockchain itself requires the Internet to support and maintain its peer-to-peer network. It’s also important to note that when people talk informally about “the” blockchain, they’re almost always referring to the specific system that Nakamoto implemented to support Bit-coin. The Bitcoin blockchain was the first distributed ledger system that didn’t require a centralized server or organization to support it. It’s still one of the biggest: as of November 2017 it contains more than 130 gigabytes (140 billion bytes) of information, and every new transaction increases its size. But that’s still many orders of magnitude smaller than the amount of data on the Internet, which is estimated to be on the yottabyte scale (1024, or septillions of bytes).

IS THE BLOCKCHAIN A NEW KIND OF INTERNET?

IF CRYPTOCURRENCIES ARE DIGITAL, WHAT POWERS THEM?

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

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

Bitcoin’s larger, more decentralized network is unlikely to make a similar move anytime soon. But Vinay Gupta, who designed Dubai’s blockchain strategy, believes that the same greed that motivates miners to turn kilowatts into cryptocurrency will ultimately spur them to innovate their way out of this scalability problem. Venture capitalist Charlie Morris thinks that as proof-of-stake cryptocurrencies prove their mettle in the market, “mining will become like a little blip in history,” he says. “People will say, ‘Remember when we all did that—wasn’t that ridiculous?’”

WHERE DOES MINING ACTUALLY OCCUR?

- 71% of Bitcoin is mined in China; the next most active country is India, at
- 4 percent. Tip: Don’t try mining at home—alone. The task is now dominated by giant mining pools akin to the ones in China, so the chances of a solo node mining a block today
  is about one in eight million. Lone operators would spend far more on energy bills than they’d get in profits. Want to become a mining hobbyist? Join a public mining pool.

4. ARE BLOCKCHAINS EVEN LEGAL?

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

ARE BLOCKCHAINS EVEN LEGAL?

WHAT DOES THE PUBLIC THINK ABOUT BLOCKCHAIN?

- 62% of Americans believe cryptocurrencies are used for illegal purchases or don't know what they're used for at all, according to a 2017 YouGov survey.
- 59% of global consumers polled in a 2017 HSBC survey said they had never heard of blockchain technology; 80 percent of those who had heard of the technology still don't understand what it is.
- 39% of senior executives' at large U.S. companies indicated they had little or no knowledge about blockchain technology, according to a 2017 Deloitte survey.

HOW WILL THIS TECHNOLOGY BE USED IN THE FUTURE?

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

SELF-DRIVING, SELF-OWNING CARS: Instead of driving for Uber, your car would drive itself while you work or sleep. Blockchain-backed smart contracts could remove middlemen like Uber and Lyft from the car-sharing equation by automating their two basic functions—matching cars with riders and facilitating payments. You could also own "shares" of a car represented by cryptocurrency tokens.

PORTABLE MEDICAL DATA: The same technology that allows two people to exchange units of Bitcoin without necessarily trusting each other could also vouchsafe medical information, putting control firmly in the hands of patients, says Brian Behlendorf, executive director of the Linux Foundation's Hyperledger project, a tool kit for building blockchain applications. Patients would receive a "'health wallet" with their data and histories. A doctor could go to a ledger and request your blood type, generating an access request on the user's phone. "You get an audit trail of who you shared that data with and the option to delete it when the treatment is over," Behlendorf says.

A GLOBAL SUPERCOMPUTER: Linking your devices to thousands of others in a P2P network—and using a blockchain to pay you for their use—would create a financial incentive to support a worldwide, decentralized supercomputer. While you sleep, your laptop and phone could be rented by scientists who want to run models, for example. A project called Golem is already working on it. "The number of idle laptops is so much larger than the computing power of the data centers," Gupta says. "Artificial intelligence, climate modeling—all of that stuff could be accelerated 1,000-fold."

WHAT ARE THE LIMITATIONS AND DANGERS OF BLOCKCHAIN?

"Blockchains provide a substrate that, if certain assumptions are held to, is very difficult to modify ex post facto," says Cornell blockchain researcher Emin Gün Sirer. "But that doesn't mean that everything recorded to a blockchain is true or desirable. If I get hacked and someone steals my cryptocoins and tries to use them, I would very much like to undo that transaction. That's where immutability becomes a liability." It's also easy to confuse a blockchain's theoretical immutability with actual data security: public blockchains like Ethereum and Bitcoin don't actually encrypt any information. The Linux Foundation's Brian Behlendorf goes one step further: "The ledger should never be used to store personal data or anything sensitive, not even in encrypted form," he says, "because we know that no matter what we encrypt today, probably in 40 or 50 years we'll be able to decrypt it" with more advanced technology. Some advocates speak of blockchain as a panacea for any social problem involving trust, but that's blindly optimistic. For more on the limitations of blockchain as a societal savior, see page 38.

5. HOW ARE CRYPTOCURRENCIES SECURE AND TRUSTWORTHY?

Because they're ultimately nothing but software, the trustworthiness of a cryptocurrency "comes from the code base," says M.I.T. researcher Catalini. Anyone can gin up a cryptocoin and raise funds by selling it through an initial coin offering—even Paris Hilton did it, lending her name to promote an obscure token. But it's no coincidence that the two most popular cryptocurrencies, Bitcoin and Ether, were engineered by

computer-programming savants. That said, even coins with impressive technical bona fides can be risky. The DAO—a "decentralized autonomous organization" running on Ethereum that raised over $100 million in 2016—"had a bug" (in Catalini's understated terms) that allowed hackers to make of with $50 million worth of Ether.

HOW ARE CRYPTOCURRENCIES SECURE AND TRUSTWORTHY?

HOW DO YOU REGULATE A DECENTRALIZED SYSTEM?

Given the Wild West reputations of decentralized digital currencies, it's easy to assume that they were created to dismantle or avoid financial regulation. But that's not quite accurate. Bitcoin is full of regulations, after all—they're just defined and enforced by source code (and the collective activity of its P2P network) rather than by governments or financial institutions. "The whole innovation about Bitcoin is in eschewing social governance of record keeping," says Patrick Murck, a lawyer who researches blockchain policy and regulation at Harvard University's Berkman Klein Center for

Internet and Society. Ethereum's stated purpose—to support the deployment of autonomous smart contracts—is essentially regulatory. A blockchain is arguably nothing but regulation: a mathematically enforced system of rules about what can and cannot be done with records in a database.

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

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

CAN BLOCKCHAINS FAIL?

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

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

GOOD OLD-FASHIONED HUMAN ERROR: It may take the computing equivalent of moving mountains to compromise the blockchain itself. But anything built on it or attached to it is just as vulnerable as it is now. Mt. Gox, a Bitcoin currency exchange (that is, an intermediary that lets people convert traditional

currencies—like dollars—into Bitcoin) plagued by mismanagement and faulty code, lost 850,000 Bitcoins (worth $620 million at the time) in 2014. Ultimately blockchains are just distributed ledgers with no help desk—so if you have a digital wallet full of cryptocurrency and you lose the password, that money is almost certainly gone. There is rich irony in the fact that some cryptocurrency users keep a hard copy of their pass codes (or even the currency itself, stored on a USB drive) in a safety deposit box at the bank—a practice known as cold storage.

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