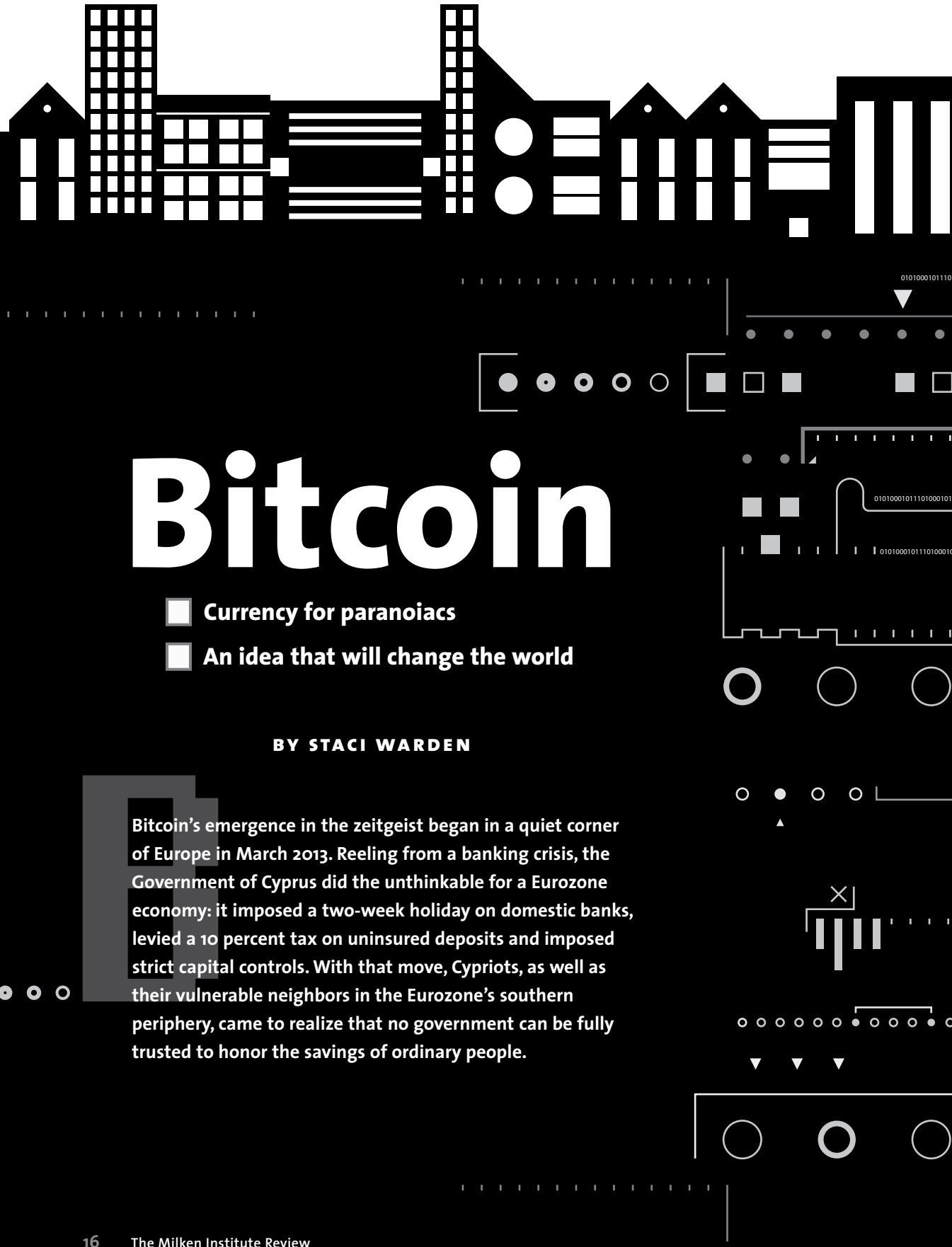
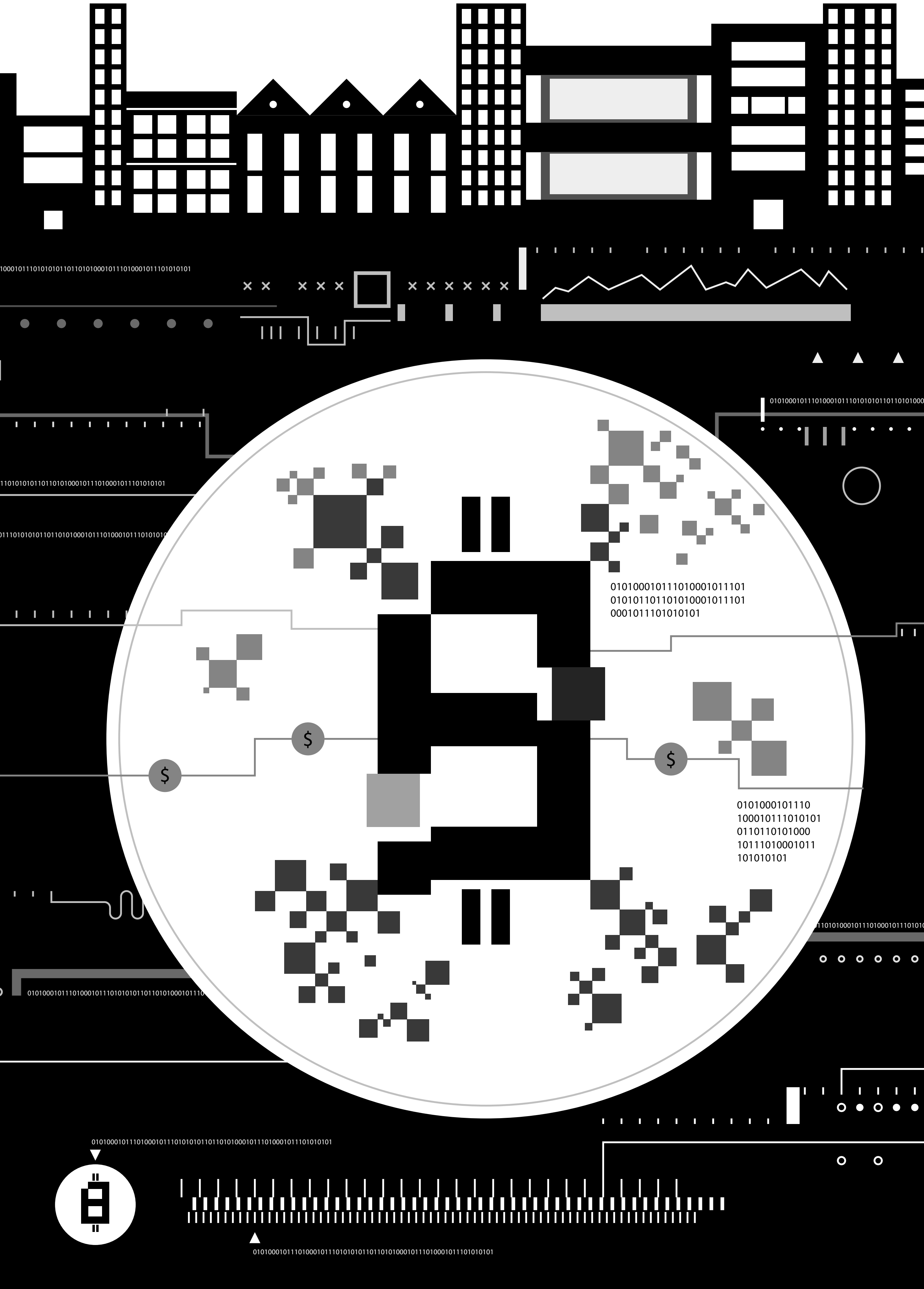


Bitcoin

- Currency for paranoiacs
- An idea that will change the world

BY STACI WARDEN

Bitcoin's emergence in the zeitgeist began in a quiet corner of Europe in March 2013. Reeling from a banking crisis, the Government of Cyprus did the unthinkable for a Eurozone economy: it imposed a two-week holiday on domestic banks, levied a 10 percent tax on uninsured deposits and imposed strict capital controls. With that move, Cypriots, as well as their vulnerable neighbors in the Eurozone's southern periphery, came to realize that no government can be fully trusted to honor the savings of ordinary people.



$
$
$
0101000101110100010111101
0101011011010100010111101
0001011101010101
0101000101110
100010111010101
0110110101000
10111010001011
101010101

In response, the most wary investors around the world turned to bitcoin and began buying the virtual currency. Its price rose eight-fold and the value of all bitcoin in circulation topped $1 billion for the first time. (Grammarians take note: going forward, we'll use "bitcoin" to refer to the unit of currency itself and "Bitcoin" to mean the concept behind the currency.)

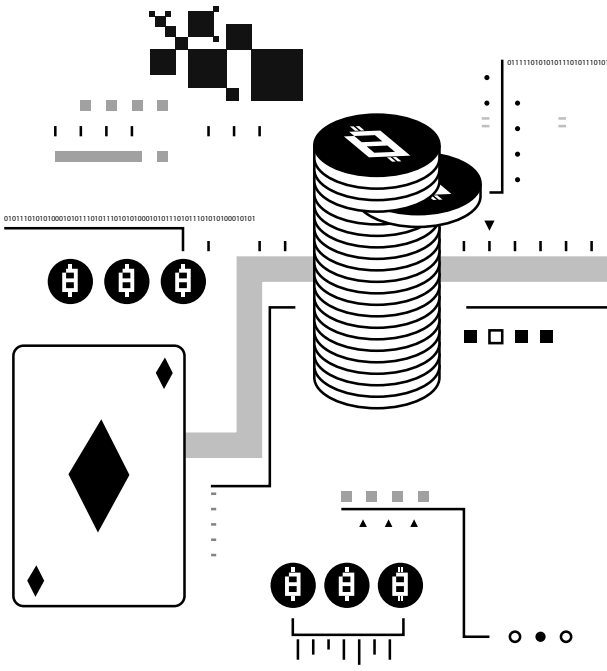
Today, Bitcoin's main features are well-known even to casual followers of the phenomenon:

- It is virtual – there are no actual coins.
- Bitcoin allows you to buy and sell things without revealing your personal identity.
- Your holdings can't be inflated away by government policy (but they can certainly change in value).
- Your money can't easily be confiscated.

Anarchists, libertarians and tech-savvy criminals may have spotted Bitcoin's advantages first. Bitcoin was used to fund Wikileaks when it was cut off by traditional payment processors after the Julian Assange affair. But the currency's ongoing popularity has been driven in part by regular people living in countries in which financial repression is the norm.

Chinese savers, for example, discovered Bitcoin's potential early on. No doubt driven by the opportunity to escape negative real returns on their deposits at state-owned banks and restrictions on hard-currency transactions, Chinese participation fed the virtual currency's meteoric rise throughout 2013. Today, despite a severe government crackdown, 80 percent of all bitcoin exchange transactions are into or out of the Chinese renminbi.

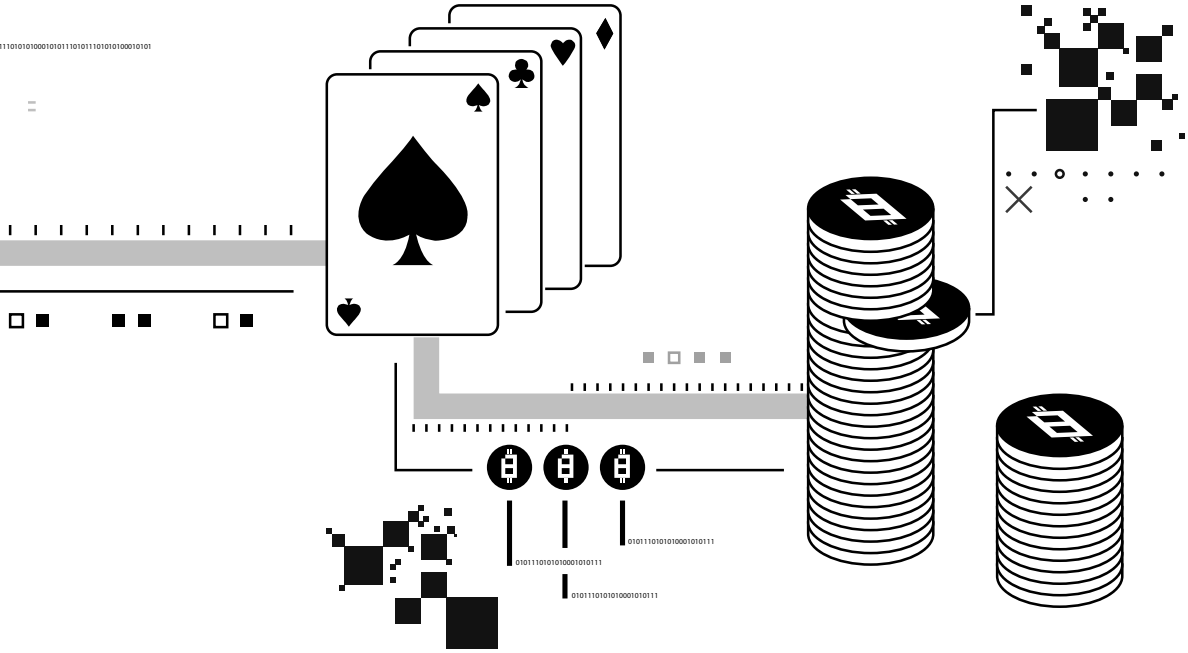
STACI WARDEN, a former banker at JPMorgan Chase, is the executive director of the Center for Financial Markets at the Milken Institute and chair of the Rwandan Capital Markets Authority.



In Argentina, where the peso trades at a deep discount to official rates in the black market and the government levies a 35 percent tax on foreign-currency credit card purchases, bitcoin activity far exceeds that of any other country in Latin America. Back in Europe, bitcoin transaction volume has tracked the euro crisis. The day of the Greek referendum on the European austerity package in July, bitcoin's price rose to a four-month high.

Bitcoin advocates argue that the virtual currency can bring freedom to those living under repressive systems of all kinds, be they political dissidents or women trying to keep earnings out of the hands of husbands or brothers. By the same token, advocates argue, Bitcoin can have a profound social effect by opening the door to the financially marginalized. Some two billion people still operate outside of the formal global financial system. But anybody with a mobile phone can use bitcoin, and these days, a remarkably large number are connected wirelessly. In Africa, for example, two out of three people have mobile

PREVIOUS PAGE AND THIS PAGE: ERIC FROMMELT



You need a pretty strong stomach to hang onto an asset that has seen daily price volatility of 35 percent on more than one occasion.

phone subscriptions, while just 20 percent have bank accounts.

That said, Bitcoin's core value proposition as a substitute for regular currencies is, frankly, questionable. Critics of Bitcoin – and they are numerous – emphasize, first, that unlike "fiat" currencies issued by governments, a bitcoin has no inherent value. The U.S. dollar, as legal tender, can, most importantly, be used to pay taxes, and because of that fact, be thought of as a claim on the U.S. government that is backed by the productive capacity of the nation as a whole. Bitcoin, by contrast, has value purely from the collective will to accept it as payment. And, despite Bitcoin's steady growth in popularity, the community of believers remains small. At the peak, the value of all bitcoins – its total market capitalization – was about equal to the market cap of the stock market in Slovenia.

Moreover, bitcoin's roller-coaster volatility undermines its potential as a store of value. You need a pretty strong stomach to hang onto an asset that has seen daily price volatility of 35 percent on more than one occasion. Anybody who bought bitcoin at its 2014 high of $1,250 has seen 80 percent of that wealth go up in smoke.

Even as a medium of exchange, Bitcoin's convenience factor is fighting the headwinds of a revolution in hard-currency payment technologies, from ApplePay in the United States to WeChat in China to MPesa in Kenya. And last year's IRS ruling that bitcoin

is property, not currency, doesn't help. This designation means that capital gains taxes must be calculated (by the law-abiding, anyway) each time bitcoin is used to make a purchase.

More fundamentally, many economists – among them, Paul Krugman – argue that Bitcoin's mechanism for determining the money supply encourages hoarding that not only creates severe wealth inequalities favoring early adopters, but undermines Bitcoin's potential as a medium of exchange. It's true that an outsized amount of bitcoin is, in fact, held for speculative purposes, and the high-profile merchants who have chosen to accept it in payment (Overstock.com, Expedia, Dell) have yet to see the transaction volumes they expected.

Yet, despite these weaknesses – not to mention the Silk Road arrests, the high-profile blowup of Mt. Gox (the once-dominant bitcoin exchange that lost the equivalent of $500 million to hackers), and the wary approach of regulators – the venture capital industry is on track to invest $1 billion this year in the Bitcoin ecosystem. Venture capital is pouring into everything from exchange houses to merchant services to investment funds to retail offerings. In fact, Bitcoin-related businesses and nascent competitors handling other virtual currencies are multiplying so rapidly that it's extremely difficult to keep abreast of them.

SO, WHAT'S THE BIG DEAL?

Actually, Bitcoin's core value proposition is not convenience or even anonymity; it's more fundamental. Satoshi Nakamoto, Bitcoin's elusive creator, explained it in a post on a crypto-currency blog in 2009:

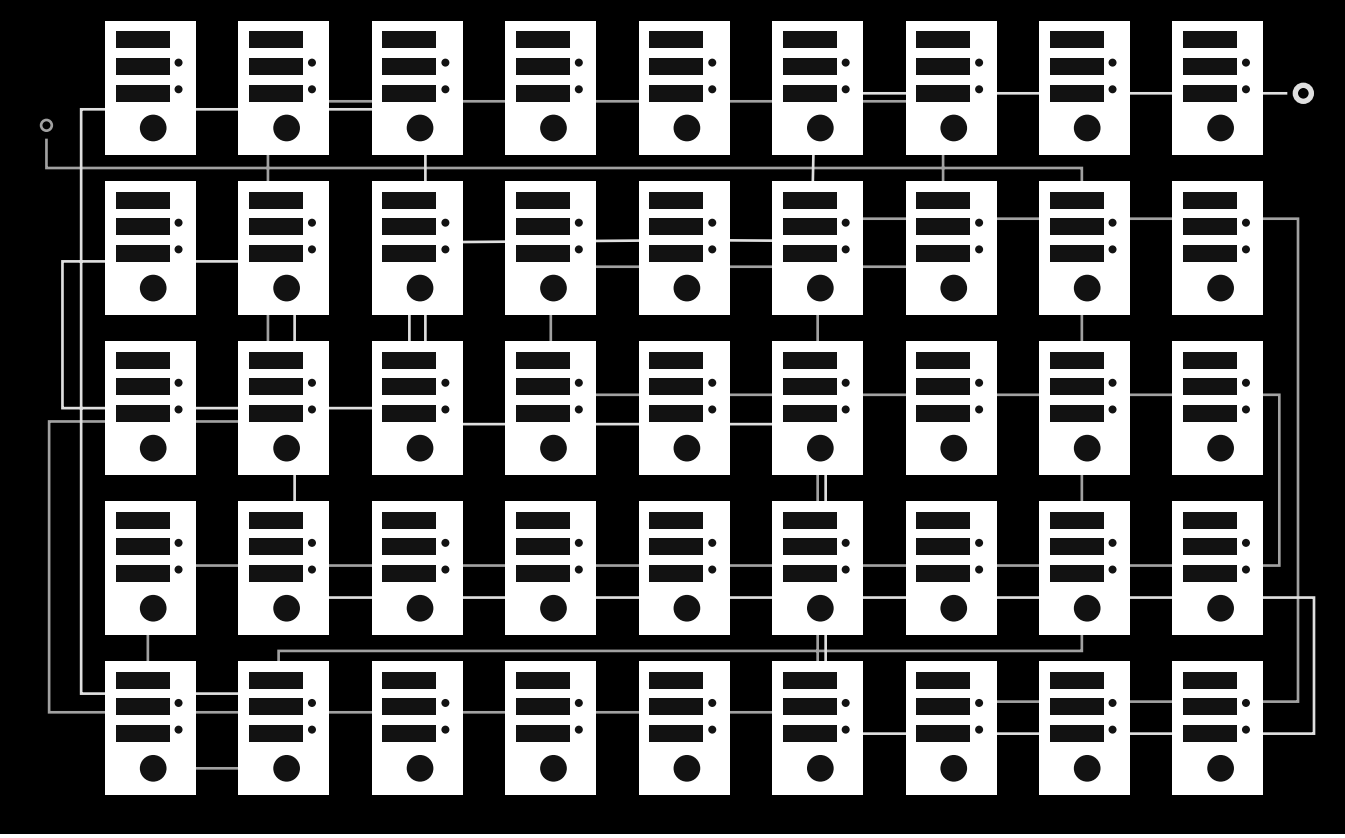
> The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. … With e-currency based on cryptographic proof, without the need to trust a third-party middleman, money can be secure and transactions effortless.

His point was not just that trust is often abused, but that the need for trust itself makes for an inefficient and costly system of exchange. Because people don't trust one another, they need banks to make payments, brokers to transfer securities, lawyers to write contracts and courts to settle disputes. But these middlemen extract fees for these services, and these fees add up to gigantic sums. Gil Luria at Wedbush Securities estimates that trust-based service provision in the United States accounts for about 21 percent (no misprint) of GDP.

If a currency system could eliminate the need for trusted intermediaries, the ramifications would be enormous. The $260 billion that merchants paid in card fees in 2013 would be up for grabs. A global remittance system that functioned without intermediaries would save an estimated $30 billion for some of the world's poorest people. Moreover, the savings would go beyond money. The identities of shoppers would be protected from data breaches at their credit card companies – or, for that matter, at Target or Home Depot.

THE BITCOIN REVOLUTION

On October 31, 2008, one month after the collapse of Lehman Brothers – no coincidence, surely – Satoshi Nakamoto (a pseudonym for an individual or group) posted a nine-page paper to the Cypherpunk mailing list explaining an electronic cash system that



If a virtual currency is to live on thousands of independent computers instead of on one in-house system, somehow all those computers need to be in constant collective agreement about who owns what, without having to trust one another.

did not require trust. Not in government, not in the banking system, not in credit card companies, not between buyers and sellers. And with that paper, he (she? they?) ushered in the world's first popular virtual currency.

The problem Satosho Nakamoto solved is not trivial. In order to eliminate the need for trust from a financial exchange system:

• Changes in the money supply need to be rule-based, not discretionary.

• Transactions need to be irreversible after a very short period to eliminate the risk of disputed charges.

• The historical record of all transactions needs to be publicly available and thus broadly verifiable.

• The ledger of credits and debits needs to reside "nowhere and everywhere" so that it can't be shut down.

• Most important, the system needs to eliminate any form of centralized authority that makes rules or enforces them.

It's that last part that's really hard. Not technically hard, mind you; decentralization can be achieved with any old peer-to-peer network. And, in fact, both the idea and the core requirements for a decentralized virtual currency – the Internet, databases shared across multiple computer networks, and the public/private key cryptography that enables secure payments – have been around since the 1990s. What's hard about eliminating centralized authorities is that centralized authorities decide things, and, in particular, they

ERIC FROMMELT

decide the validity of alleged transactions. If a virtual currency is to live on thousands of independent computers instead of on one in-house system, somehow all those computers need to be in constant collective agreement about who owns what, without having to trust one another, and without any one of them having the authority to lay down the law.

Financial institutions have put in place a lot of sophisticated processes to determine who owns what. But as a general rule, winners in what amount to competing transactions are determined on a first-come-first-served basis. If I have $100 in my bank account and I try to make two payments of $100, my bank will cash the first one it receives and bounce the second. But what if there were no bank? What would stop me from spending the same $100 twice?

In the Bitcoin system, payment transactions are blasted out electronically to all the nodes (computers) in the network, first for verification and then to be added to the collective ledger that stipulates ownership. That's not quite an answer, though. What if I try to spend money I don't have by making two payments in rapid succession (all I have to do, after all, is press a button twice)? What if some computers pick up my first transaction and invalidate the second, but other computers pick up the second transaction and invalidate the first? How could an authoritative record possibly establish that only one of those payments is valid, and how could it do so in such a way that thousands of independent entities would never question that decision, now or in the future?

What Satoshi Nakamoto did was to solve this "double payments" problem. In techspeak, he created a decentralized database where the order of transactions is agreed upon by everybody. As Richard Brown, who has the job moniker Executive Architect for Banking Innovation in the UK at IBM enthused in an interview in 2013:

> Even five years ago, I would have told you that Bitcoin's core architecture was impossible. You could never solve the problem of coming to a global consensus without trust. But now it's here.

Because Satoshi Nakamoto solved this problem, he (I'm going to stick with the convention) belongs in the pantheon of technology geniuses. But here's the kicker: because he solved this problem, Bitcoin's potential as a paradigm-shifting operating system far outshadows its realistic potential as a substitute for global currencies.

HOW BITCOIN WORKS

As noted, Bitcoin is just a very broadly shared public ledger of credits and debits that records ownership, with the security of payments guaranteed by the use of private/public cryptographic key technology. A user sets up one or more public addresses to receive bitcoin, and can spend that bitcoin if she has the private key to prove the address belongs to her. Back in the day, users would download the entire Bitcoin ledger to their computers and store their private keys on their hard drives. Today, an entire industry exists to make accessing Bitcoin easy for everyday users. Bitcoin exchanges such as Coinbase will store your private key for you and issue you a password-protected "wallet" so that you can access your money. The downside: many also require you to provide personal details.

Now comes the truly nerdy part. Transactions, once made, are blasted out to the Bitcoin network, and every 10 minutes there is a contest among nodes of the network to see who can be the first to add the newest block of transactions to the Bitcoin ledger. (This is why the technology is called a blockchain.)

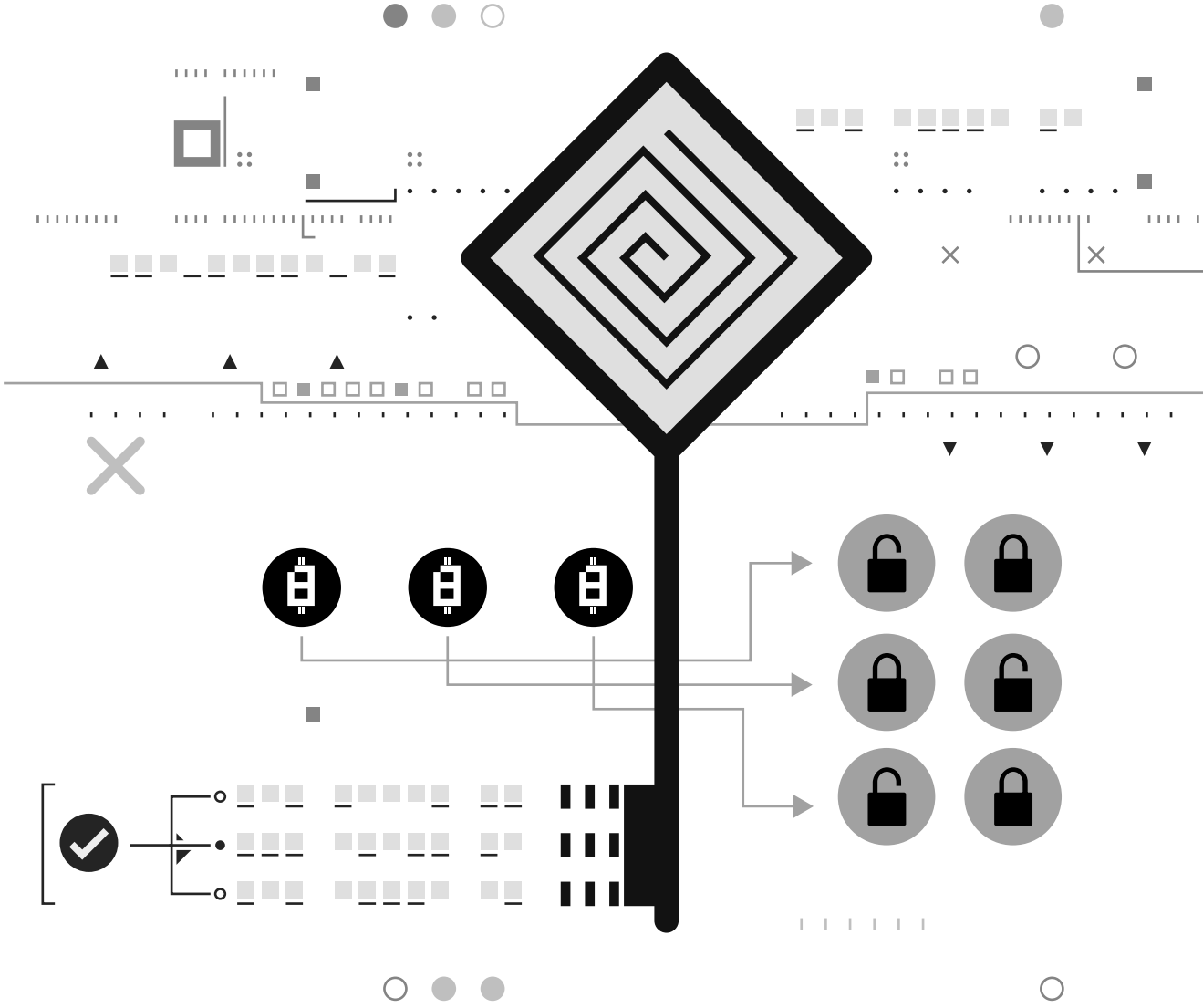
ERIC FROMMELT

Each node scoops up as many transactions as it can, adds a time stamp, a "pay me if I win the contest" line, and a reference to the previous block in the ledger. It then hashes this all together in a series of cryptographic functions using what is known as a Merkle tree. (Don't ask.)

The first node to do this publishes its hash to the network, and the other nodes check it by running the same inputs through the same hash function. If they get an identical result, they validate the block and it is appended to the ledger. The winning node is then paid in bitcoin. When bitcoin launched, miners were paid 50 bitcoin for appending blocks. That payment is cut by half every four years until all 21 million bitcoins are mined (expected by 2140). Miners are now paid 25 bitcoin, the fixed rate until 2016.

This process of verifying transactions and racing to see who can append them first is called "mining" bitcoin, a term no doubt used to evoke gold mining. This analogy is not, strictly speaking, correct, however, because unlike in gold mining, an increase in bitcoin mining effort does not bring a commensurate increase in the bitcoin supply (which, as noted above, is limited to 21 million).

Bitcoin uses the SHA-256 cryptographic hash function. As you'd expect from any self-respecting cryptographic function, it takes all this transaction information and turns it into

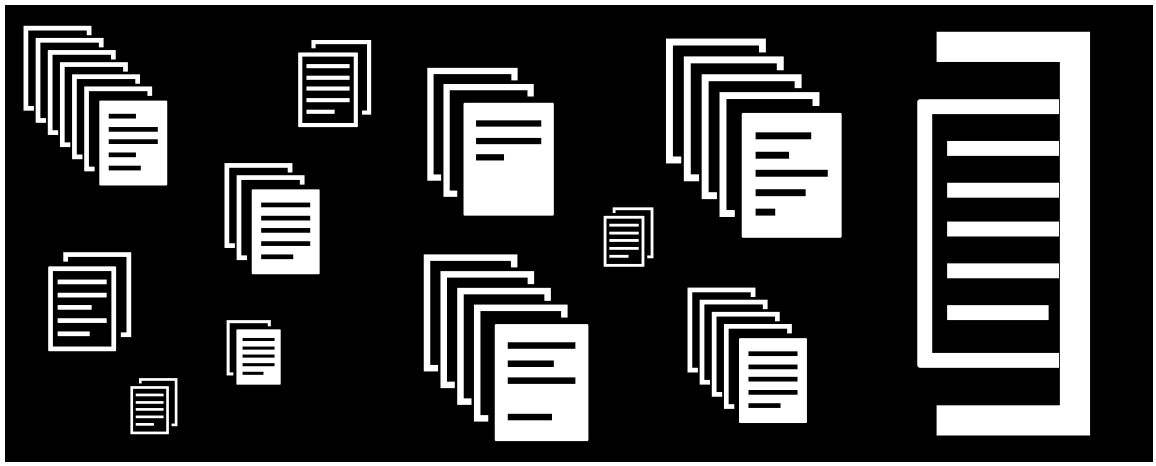


complete gobbledygook. In the case of SHA-256, the gobbledygook is always 64 characters long. In fact, you could run "Hello, world!" or the entirety of *War and Peace* through SHA-256, and in both cases you would get 64 characters of nonsense. The input information is protected because it's impossible to figure out the original content by looking at the resulting hash value. But if I choose to tell you that the output of my hash function is *War and Peace*, you can easily check if I'm telling the truth by getting the book and running it through the hash function yourself. If I am, you will get exactly the same output.

Actually, it's no big deal to run a cryptographic hash function. This is important for minimizing the effort required of other nodes to check the winner's work, but it is problematic for running the contest in the first place. It's just too easy to win. And if it's too easy to win, there will be multiple winners. If I try to make a double payment, the node that picks up my first transaction and the node that picks up my second transaction could both win. This would cause a fork in the chain, and when it came to validating the work, some nodes would validate the first fork and some the second. In an easy contest there would be multiple forks with each block, and very soon we would have complete chaos.

Satoshi Nakamoto's solution to this problem was to make the contest extremely difficult. According to the Bitcoin protocol, the contest should last 10 minutes. So, if the computers get faster and they start solving the cryptographic problem in less than 10 minutes, then the problem is recalibrated to make it harder.

Nakamoto's theory was that, if in order to earn the right to append the next block to the blockchain (and thus earn bitcoin) each node would have to undertake significant effort, the likelihood of ending up with just one winner would be markedly increased. And if there was just one winner, it wouldn't matter how many duplicate payments were sent out. Each node individually knows how to reject

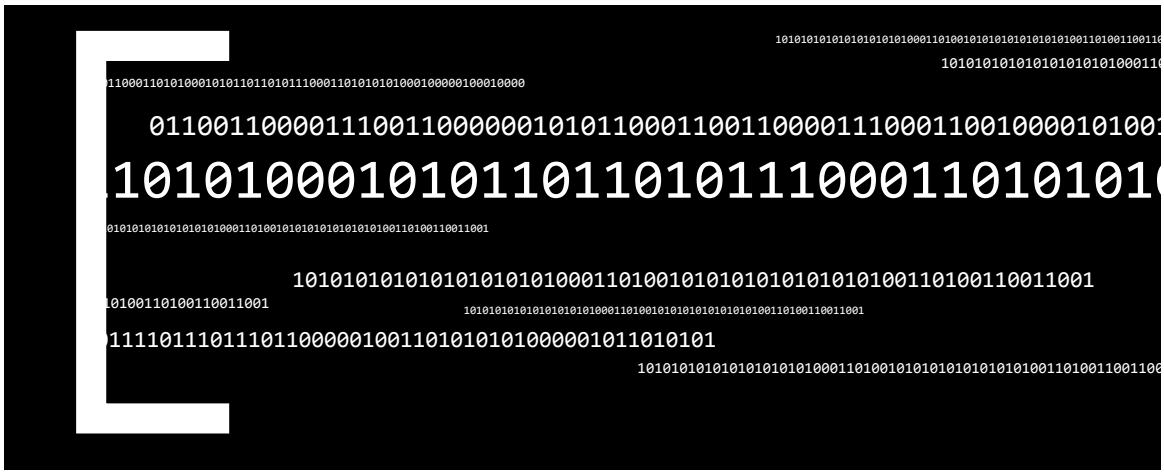


You could run "Hello, world!" or the entirety of *War and Peace* through SHA-256...

ERIC FROMMELT

duplicates and only one node would win the contest. One of my payments would be appended, and the rest would be thrown away.

To make the contest hard, he borrowed a trick that is used to protect email servers against incoming spam. He requires a "proof of work," determined by CPU usage (computer power). In the Bitcoin protocol, the proof of work is this: not only do miners have to create a cryptographic hash value out of all



and in both cases you would get 64 characters of nonsense.

these transactions, but the hash value must be small. That is, it has to start with a certain number of zeros. If the hash value a miner gets after scooping up 10 minutes' worth of transactions isn't small enough, it has to keep adding *something else* to the mix to try to shrink it. Basically, it keeps adding different random numbers, over and over again, until it comes upon one (by luck) that gives it a small enough hash value.

It's not conceptually or technically difficult to find a really small hash value, but it can take a lot of computing power. Nor is it impossible that there will be two simultaneous winners, and thus a fork in the ledger. The beauty of the Bitcoin protocol, though, is that this problem does not endure. In the next round, the new winning miner will simply append its block to one of the forks (it doesn't matter which one) making that fork the longer of the two (or, more accurately, the fork that contains the most amount of work). In the round after that, the miners, by agreement, append to the fork that contains the most work. So after a couple of rounds at most, the runt fork is completely ignored and all the unconfirmed transactions go back in the pool to be picked up later.

All of them, that is, except my other, fraudulent, payment. That one is rejected because all nodes on the network can see that those bitcoin have already been spent in a transaction with an earlier time stamp (because it was picked up in a previous block). With every block added, previous blocks become exponentially more secure, so that tampering with the ledger becomes impossible. Even the most prudent users of Bitcoin maintain that

after an hour (six blocks), bitcoin payments can be reliably said to be irreversible.

Got all that? If you didn't, remember the bottom line: no central referee is settling these disputes. It's just that the rules are clear and everybody has a potent incentive to follow them.

The elegant thing about Satoshi Nakamoto's system is that, by doing this work to verify transactions, Bitcoin miners are maintaining the integrity of the ledger itself. And in return for this maintenance work, they are paid in bitcoin that become part of the bitcoin money supply the way Federal Reserve deposits in private banks become part of the supply of dollars. The contest is fair because every 10 minutes all miners have an equal shot at winning, but the winner is most likely to be the miner that has exerted the most effort in terms of computer processing.

ERIC FROMMELT

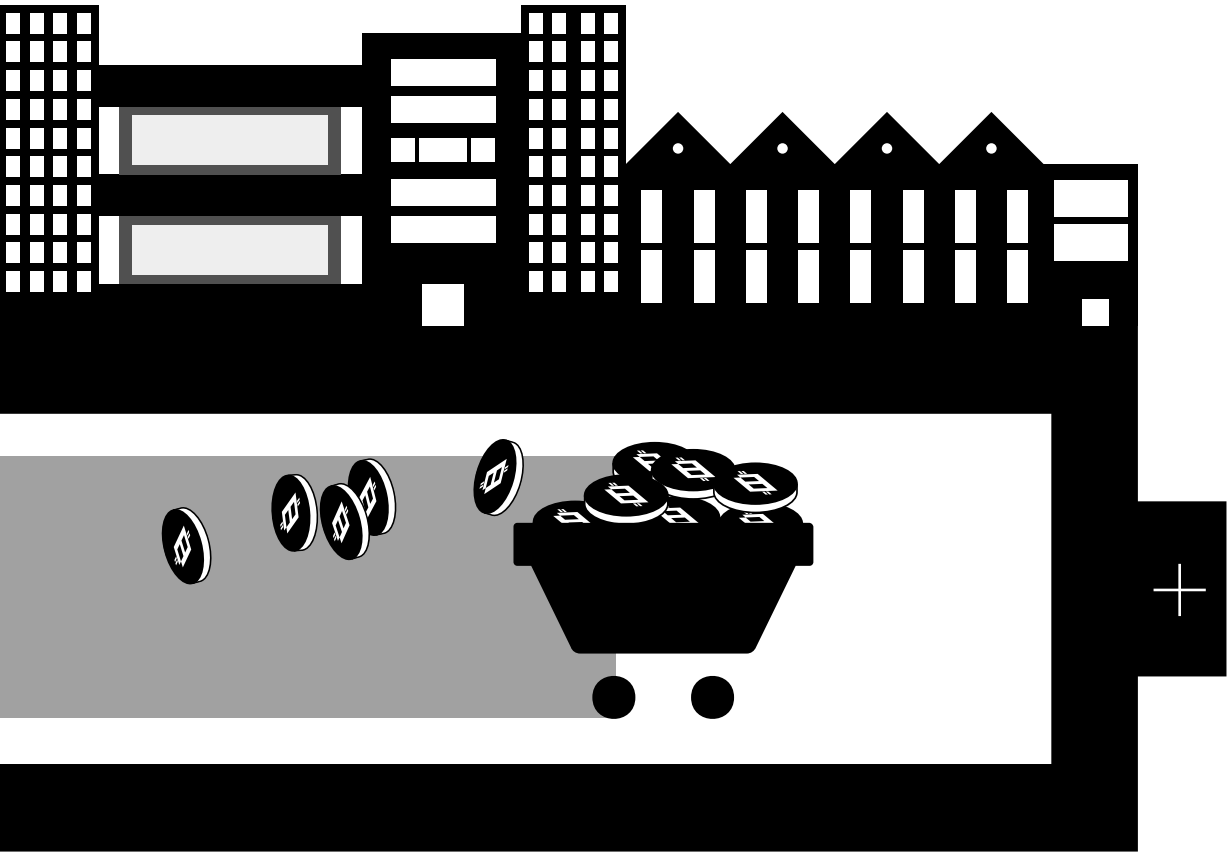
CRITICISMS AND COPYCATS

As a result of Bitcoin's unique incentives to encourage mining, miners worldwide are locked into an ever-escalating arms race of computing power to solve hash functions and win bitcoin. Once the domain of amateur enthusiasts, Bitcoin mining is now a big business requiring expensive, highly specialized equipment. The numbers are mind-boggling. The average hash rate at the time of this writing is 400 million gigahashes per second (a gigahash is a billion hashes!). The total electricity consumption by Bitcoin miners has reached an estimated 1.46 billion kilowatt-hours per year. This is roughly enough electricity to power a small American city.

To keep energy costs low, many Bitcoin miners locate where coal is cheap, or in places with geothermal sources of energy, like Iceland. Critics denounce both the energy wasted and the geopolitical risks associated with the many locations where energy is subsidized (two-thirds of miners are located in China and another 20 percent are in parts unknown). Supporters counter that the energy efficiency of mining is on the rise – and in any case, the energy used to power the Bitcoin ecosystem should be compared to the energy requirements for running the various components of the global banking system.

At any rate, the race continues, and might be on the edge of transformation into a different sort of contest. For example, the tech startup 21 Inc., while extremely secretive about its business plan, made big headlines in Bitcoinland recently by raising a staggering $116 million in pre-launch VC funding. 21 Inc. has released only two tweets in its short corporate history. But the first one reads, "A bitcoin miner in every device and in every hand."

Critics including Kevin Dowd and Martin Hutchinson note that, because each miner ignores the social costs it imposes on the system

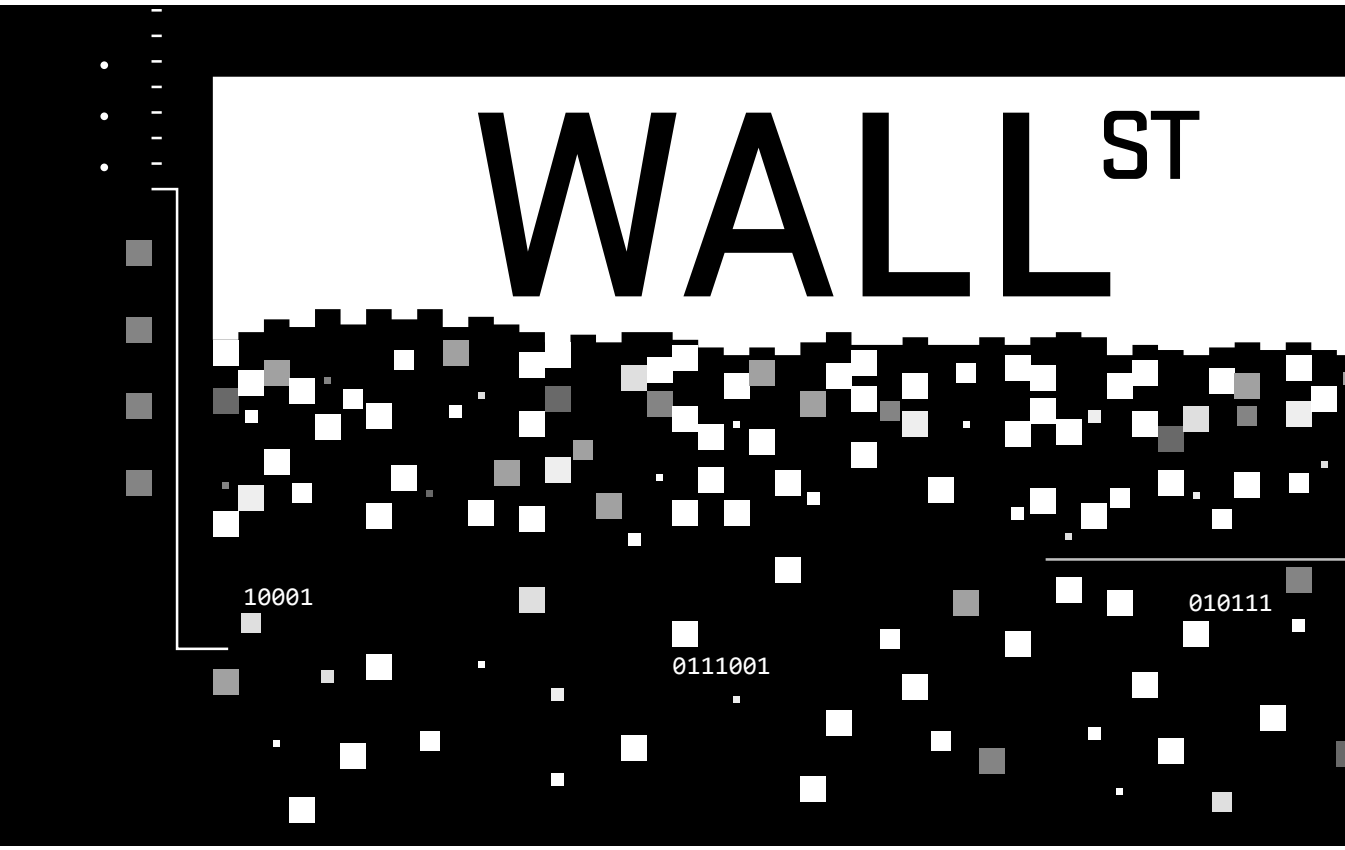


The total electricity consumption by Bitcoin miners has reached an estimated 1.46 billion kilowatt-hours per year—roughly enough electricity to power a small American city.

(the arms race) and because there are no social benefits to that arms race (the total bitcoin supply is fixed), the Bitcoin system is subject to economies of scale that will inevitably lead to consolidation. And if a node or group of nodes were to eventually amass a majority of the total computing power, it could control the system, perhaps for nefarious purposes.

The possibility of a "51 percent attack" is the most discussed potential weakness of the Bitcoin protocol, and the Ghash.io mining pool did, in fact, amass 51 percent of the computing power for a few hours in 2014. Several members immediately left the pool, though, in order to reduce its size, and its CEO quickly stated, "We never have and never will participate in any 51 percent attack." Great, but still, doesn't that inject the need for trust into a system that is supposed to operate perfectly without trust?

Much the way the floodgates opened to new runners in the wake of Roger Bannister's shattering of the four-minute mile back in 1954, hundreds of "alt-coins" have now been developed. The idea is to try to improve in some way on the core Bitcoin protocol. Some of the most interesting are Litecoin (which has a proof-of-work script that limits hashes per second to conserve mining energy), Peercoin (which has a "proof of stake" to reward miners for owning Peercoin), Dogecoin (fun, philanthropic and introduces controlled inflation to



Why bother with financial services at all? A company that wants to make an initial public offering of securities, for example, could simply issue its own shares and then sell those shares directly through the blockchain.

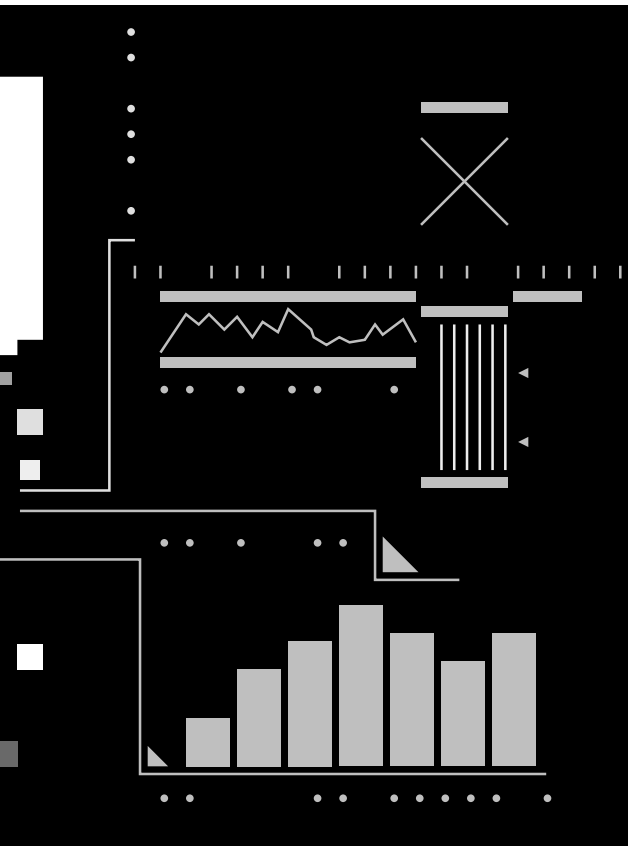
discourage hoarding), Freicoin (which has a holding tax to discourage hoarding), Darkcoin and Zerocoin (which make the "audit trail" even more difficult), and Primecoin (which makes the proof-of-work a search for prime numbers, thus making mining scientifically useful).

The most successful variant on Bitcoin, the Ripple protocol, is a decentralized system of nodes that already trust one another, so that group verification is less costly. But Ripple is mostly trying to work within the established banking system, not necessarily to compete with it.

THE POWER OF THE BLOCKCHAIN

One bitcoin is divisible into a hundred million units, thereby enabling extremely small micropayments (0.00000001 BTC is called – you guessed it – a Satoshi). As a result, a whole new world can be opened up to charge for things currently priced at zero that would be more efficiently allocated at very low prices. For example, micropayments can be charged for

ERIC FROMMELT



things like webpage or blog views. And, these payments can be automated on the blockchain. So, for example, a coffee shop could automatically start charging by the minute (or, for that matter, by the second) for wifi usage as soon as you sat down with your latte.

But, amazingly, micro-units of bitcoin can be used for entirely different purposes, as vessels for transferring and recording ownership of digital property of all kinds. For example, the owner of a given bitcoin could assert that it now represents something else in addition to the bitcoin itself – say, title to 100 shares of Apple stock, an ounce of gold, or a house the bitcoin owner possessed – and then use the same blockchain technology to register and/or transfer ownership of that asset at extremely low cost in a way that can't be tampered with or reversed. As Marc Andreessen, one of Silicon Valley's most successful venture capitalists, put it:

> Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. The consequences of this breakthrough are hard to overstate.

Imagine the possibilities. For starters, any institution that confers ownership, transfers ownership and settles disputes about ownership is in some ways up for grabs. Land registries keep track of titles, custodians keep track of securities and the phone company allocates telephone numbers. On the blockchain, all of these central authorities can be avoided because the job of record-keeping can be done on a decentralized basis. The blockchain effectively crowdsources the validation of ownership and transfer.

Today, trade and post-trade processes (matching, clearing, collateral management, settlement, custody, etc.) require a complex offsetting of credits and debits across multiple balance sheets, subject to multiple access rules, with giant sums to be reconciled at the end of each day. But these agreements and obligations among firms could be recorded on a shared ledger at the industry level. Research by Santander Innoventures estimates that the banking sector could save $15-20 billion by 2022 using a decentralized ledger technology. Blockchain technology would enable direct (and irreversible) settlement, moving settlement times from two days in many cases to milliseconds. Financial institutions are beginning to pour money into these ideas. Indeed, Nasdaq is planning to open a business that will issue or transfer securities using blockchain technology by the end of 2015.

But why bother with financial services at all? A company that wants to make an initial

public offering of securities, for example, could simply issue its own shares and then sell those shares directly through the blockchain. A bitcoin in this case could equal, say, 100 shares of stock, and all the rights (dividends, voting) would transfer automatically with it. Going forward, the company would then use the blockchain to track any changes in ownership and pay dividends to the public addresses showing ownership on that date. It would not even need to know the identities of its shareholders (though there is speculation that the SEC might insist). It could issue debt in the same way.

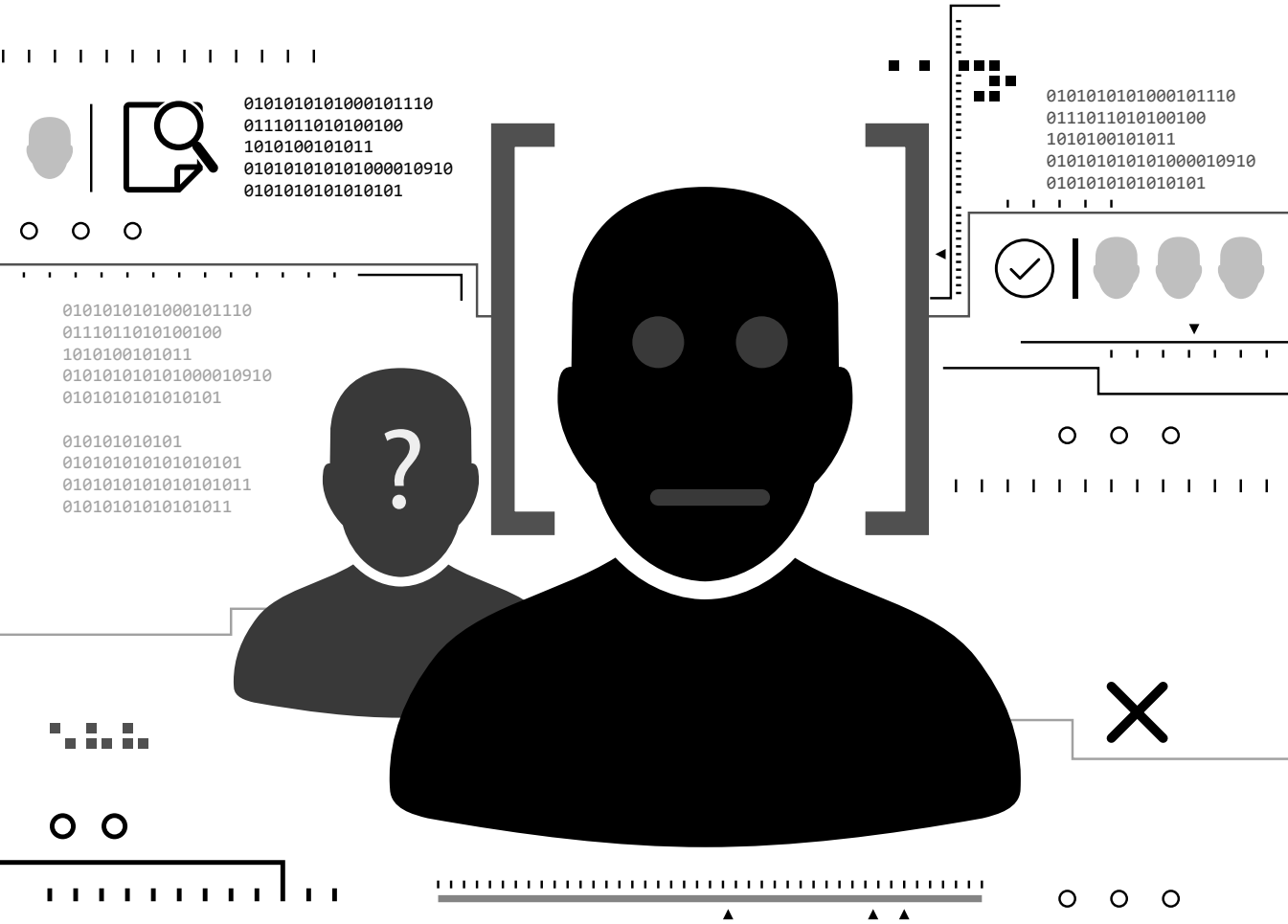
Another possibility, "forward auditing," has lots of interesting potential uses. Philanthropists donating bitcoin, for example, could verify that the recipient charity spent the funds in accordance with agreed terms. Because forward auditing provides important clues to a person's spending patterns and therefore identity, Bitcoin is considered, strictly speaking, to be pseudonymous rather than anonymous. The FBI was able to track down the ringleader of the Silk Road illicit drug marketplace with some heavy-duty blockchain sleuthing (and subpoenaing). The difference between anonymity and pseudonymity has never been lost on the Bitcoin enthusiasts who closely monitor the nearly one million bitcoin thought to be mined by Satoshi Nakomoto in the early days for clues to his whereabouts and identity. Alas, not one of these bitcoins has ever been spent.

Because the blockchain contains a certain and verifiable record of every bitcoin transaction, it could also be useful in verifying an object's provenance and legitimizing ownership, in, say, the art world or for secondary sales of entertainment tickets. In both cases, the blockchain would independently verify that the seller owned and had the right to sell the item in question. In the same way, the transfer of copyright through the blockchain could help avoid intellectual property violation. Most importantly, perhaps, there is an estimated $10 trillion in undocumented assets in developing countries that could be pseudonymously collateralized for credit, if property title could be established, verified and secured.

Because forward auditing provides important clues to a person's spending patterns and therefore identity, Bitcoin is considered, strictly speaking, to be pseudonymous rather than anonymous.

Interestingly, some institutions that are inherently untrustworthy already see the blockchain as a way to tie their own hands in order to instill trust. Start-up software developers speak of using blockchain technology as a way to precommit to delivering service forever (even if they go out of business) because the protocol runs autonomously, once unleashed. Voting is another oft-cited example. To clearly demonstrate a fair voting process, a voting registry could distribute a wallet and a private key to each registered voter. Voters would then "send" their votes to wallets that candidates held in their names. An up-to-the-minute accurate, tamper-proof vote count could be maintained, while still assuring voter anonymity.

One of the earliest and most ingenious ex-



amples of hand-tying was Satoshi Dice. In gambling, one never can be 100 percent certain that the dealer isn't fixing the game. The risk is compounded in online gambling, as the random-number generator program that rolls the dice or deals the cards sits on the gambling house's own server. Using the blockchain, Satoshi Dice was able to provide random and verifiable number generation and payout rules. By 2012, Satoshi Dice accounted for half of all bitcoin transfers in volume terms – not because the odds it offered were better than with traditional gambling platforms, but because they were provably fair.

BLOCKCHAINS AND SMART CONTRACTS

Smart contracts are automated contingency contracts based on "if-then" statements. And because Bitcoin is essentially just computer code, many rules can be written on top of a Bitcoin transaction. One of the most immediately useful is multi-signature authentication. For example, a buyer and seller can stipulate that two private-key signatures are required to make payment on an item that needs to be delivered, and then give a trusted third party the right to one of those signatures. If the item is delivered as expected, the buyer and seller both sign and the payment goes through. But if there is a dispute, the third party provides (or doesn't) the second signature to release the funds. The cost and hassle of formal escrow services are avoided.

In finance, credit default swaps (contracts that pay off when a counterparty defaults on its debt), insurance contracts (that pay off

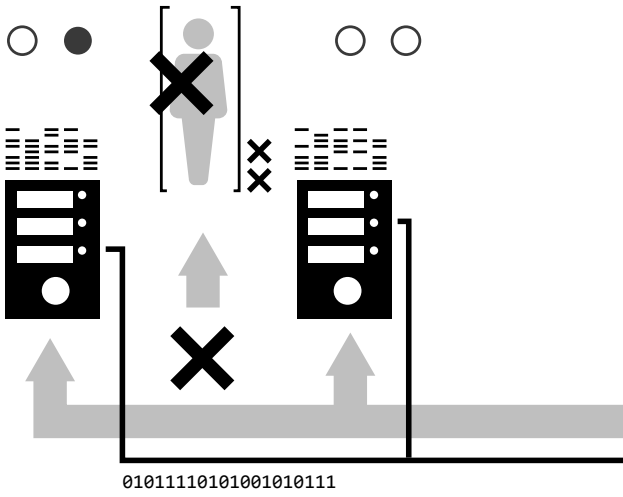
ERIC FROMMELT

when a state of the world occurs), contracts-for-differences (that pay off based on how the price of an asset relates to a reference price) and assurance contracts (that pay off when pre-agreed funding levels are met) are straightforward examples of if-then contracts that can be designed to self-execute automatically on the blockchain. You could also imagine combining the assurance contracts of crowdfunding platforms such as Kickstarter with equity self-issuance capabilities, so that initial investors could participate in the upside of successful ventures instead of just getting a free tee-shirt.

More broadly, these kinds of automated assurance contracts could turn communities of all kinds into equity holders, potentially becoming an important way to fund public goods. Travellers could fund the construction of a new road, for example, provided funding goals were met.

Things get even weirder when you combine the power of the blockchain with the Internet of Things. For example, you could buy a car on the blockchain (a digital asset representing ownership of the car, really). The car would monitor the blockchain so that it knows when its ownership has been transferred. When you buy it, it updates its ownership information to your public address, and you activate it using your private key to that address.

Of course, you could also buy the car over time. In this case, the car would monitor your monthly payments, and if you skipped one, it would simply transfer itself back to its previous owner and render itself unusable to you. From a financial inclusion perspective this is interesting because people with bad credit histories, or people who live in countries with banking regimes that won't bear the cost of credit assessment, could enter these contracts. As the repo cost is considerably reduced for



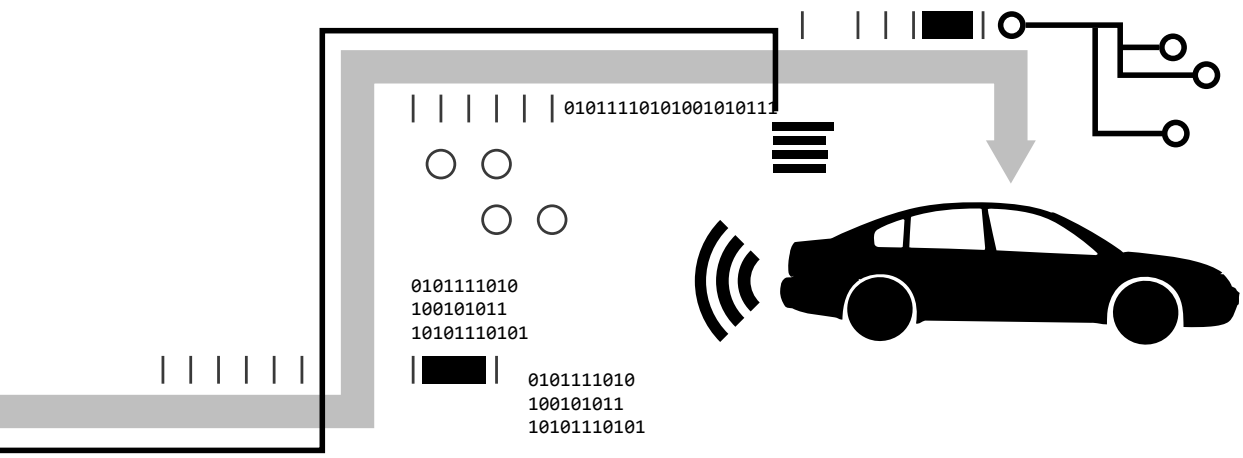
sellers, they may be more willing to take on the credit risk. For that matter, they may not even care who you are.

The futurists go further still, pointing out that you don't really need to be a person to get yourself a public address on the blockchain. Any computer that can generate a random number can do that. And this opens up a whole new world of autonomous agents, also referred to as decentralized autonomous corporations (DACs).

Self-running programs have existed for a long time. But on the blockchain they could potentially buy and sell services and enter into contracts without human intervention. A straightforward example is computers trading storage capacity or Internet bandwidth among themselves. In theory, though, your refrigerator could also trade electricity on the spot market with your neighbor's dishwasher. Mike Hearn, one of Bitcoin's core developers, imagines a car that can sell ride services for bitcoin, use its profits to hire humans for upkeep, have children (buy other cars for its fleet) and then sell itself for parts at the end of its useful life. Seriously.

A lot of this is fanciful, perhaps, but Vitalik Buterin, the 21-year-old founder of much-

ERIC FROMMELT



talked-about development platform Etherium, warns:

> If there is a centralized service on the Internet right now, you can bet that it will eventually be replaced by a DAC. Everything from YouTube to Facebook is fair game, and it will be difficult for these centralized institutions to keep up with distributed applications that have little to no overhead.

BEST IDEA SINCE SLICED BREAD?

Most of the above now exists only in the minds of some very clever technologists. But well over a billion dollars in venture and institutional money is being spent on developing applications that either sit on top of the Bitcoin blockchain or build similar decentralized protocols. The Colored Coin protocol (you "color" your coin by declaring that it represents another asset) is the most well known of the former, and Etherium is probably the most exciting example of the latter.

Still, caution is advised. The history of innovation is full of examples of first-mover misfires (witness Marc Andreessen's own Netscape browser venture). And Bitcoin faces formidable challenges as both a store of value and a medium of exchange. It has an outsized environmental footprint and scalability limitations in its current form. It may also have fatal vulnerabilities inherent in its current design, as the recent turmoil over increasing the maximum block size recently demonstrates. The regulatory environment is still uncertain. (And exactly how, by the way, would you regulate that self-owned car?)

Moreover, as the *Financial Times*'s *Alphaville* blog – a reliable critic of everything Bitcoin – points out, the fundamental flaw in the Bitcoin story may be that people actually value real live intermediaries. The whole point of entrusting monetary policy to humans, for example, is that the money supply should not be rule-based, but elastic to changes in aggregate demand. People willingly outsource trust because it's useful to do so.

Only time will tell whether Bitcoin or one of its copycats will become an important global currency, or whether the blockchain will evolve into a truly disruptive core infrastructure. But once you start learning about the blockchain, it's hard not to be awed by the enormity of the problem that Satoshi Nakamoto solved, the elegance with which he solved it, and the possibilities that his solution offers. After all, on the blockchain, nobody knows you're a toaster.