Cover | Computing | Networks

28 Sep 2017 | 15:00 GMT

Blockchains: How They Work and Why They’ll Change the World

The technology behind Bitcoin could touch every transaction you ever make

By **Morgen E. Peck**

Blockchain World

Bitcoin was hatched as an act of defiance. Unleashed in the wake of the Great Recession, the cryptocurrency was touted by its early champions as an antidote to the inequities and corruption of the traditional financial system. They cherished the belief that as this parallel currency took off, it would compete with and ultimately dismantle the institutions that had brought about the crisis. Bitcoin’s unofficial catchphrase, “In cryptography we trust,” left no doubt about who was to blame: It was the middlemen, the bankers, the “trusted” third parties who actually couldn’t be trusted. These humans simply got in the way of other humans, skimming profits and complicating transactions.

Photo: The Voorhes

Jump to Sections in this Feature

Bitcoin sought to replace the services provided by these intermediaries with cryptography and code. When you use a check to pay your mortgage, a series of agreements occur in the background between your financial institution and others, enabling money to go from your account to someone else's. Your bank can vouch that your money is good because it keeps records indicating where every penny in your account came from, and when.

Bitcoin and other cryptocurrencies replace those background agreements and transactions with software—specifically, a distributed and secure database called a blockchain. The process with which the ownership of a Bitcoin token will pass from one person to another—wherever they are, no matter what government they live under—is entrusted to a bunch of computers.

Now, eight years after the first blockchain was built, people are trying to apply it to procedures and processes beyond merely the moving of money with varying degrees of success. In effect, they're asking, What other agreements can a blockchain automate? What other middlemen can blockchain technology retire?

Can a blockchain find people offering rides, link them up with people who are trying to go somewhere, and give the two parties a transparent platform for payment? Can a blockchain act as a repository and a replay platform for TV shows, movies, and other digital media while keeping track of royalties and paying content creators? Can a blockchain check the status of airline flights and pay travelers a previously agreed upon amount if their planes don't take off on time?

If so, then blockchain technology could get rid of Uber, Netflix, and every flight-insurance provider on the market.

Those three proposed applications aren't hypothetical—they're just a few of the things now being built on Ethereum, a blockchain platform that remotely executes software on a distributed computer system called the Ethereum Virtual Machine. In the blockchain universe, Ethereum, which has its own cryptocurrency, called ethers, is by far the project that is most open to experimentation. But zoom out and a diverse collection of potentially disruptive innovators floods into view. New groups are pitching blockchain schemes almost daily. And the tech world's titans don't plan to miss out: Microsoft is offering its customers tools to experiment with blockchain applications on its Azure cloud. IBM, Intel, and others are collaborating on an open-source blockchain initiative called Hyperledger, which aims to provide the bones for business-oriented blockchains. Meanwhile, many of the largest banks—the very institutions that blockchain pioneers were trying to neutralize—have cobbled together their own version of the technology in an attempt to stay ahead of the curve. And even Bitcoin, which runs on the first and most successful blockchain, is being retrofitted for applications its designers never dreamed of.

PEOPLE

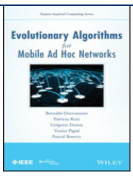
Satoshi Nakamoto

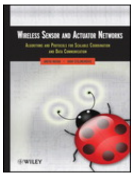
If the blockchain were a religion, Satoshi would be God. This anonymous hacker is responsible for writing the Bitcoin white paper, releasing the first Bitcoin code, and inspiring legions of blockchain developers. Many have sought to reveal his/her/their identity, but to this day that information remains secret.

Pretty much without exception, these new blockchain projects remain unencumbered by actual mass adoption. No single blockchain concept or strategy has yet revolutionized any industry. Bitcoin itself is used by no more than 375,000 people in the entire world on any given day, according to Blockchain.info. But the investor dollars are pouring in, and proposals are floating and colliding like tectonic plates on a hot undercurrent of hype and intrigue.

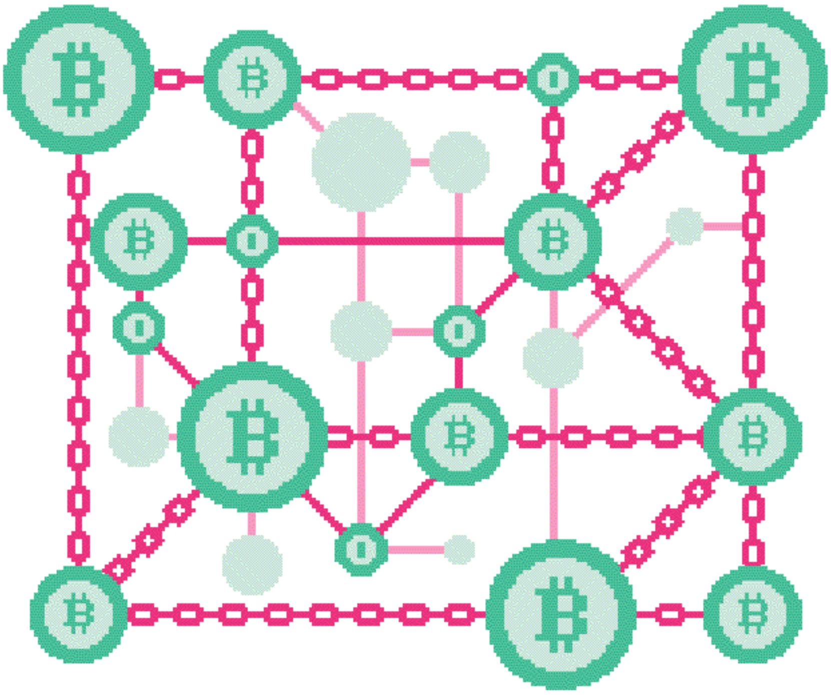
When the mantle cools, which blockchain platforms will persist, and which will slowly sink back beneath the surface? To make any kind of prediction, you've got to understand what a blockchain really is and what it does. The place to start, logically enough, is with Bitcoin.

Suggested Wiley-IEEE Reading





How Do Blockchains Work? The Bitcoin Example



All illustrations: Nicholas Little

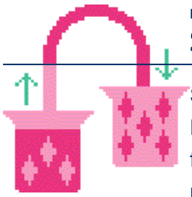
In 2009, an anonymous hacker (or group of hackers) going by the name of Satoshi Nakamoto unveiled the first entirely digital currency. The technology worked on the principle that, at its foundation, money is just an accounting tool—a method for abstracting value, assigning ownership, and providing a means for transacting.

Cash is the historic means of accomplishing these chores. Simply possessing the physical tokens—bills, coins—equals ownership, and it's up to the individuals to negotiate transactions among themselves in person. As long as cash is sufficiently difficult to replicate, there is no need for a complete accounting of who owns what portions of the money supply, or for the details of who the various holders were of a single $50 bill going back to when it was printed.

However, if you could piece together a running tabulation of who held every bill, then suddenly the physical representations would become unnecessary. Banks and payment processors have already partially sublimated our physical currency into digital records by tracking and processing transactions within their closed systems.

Bitcoin completed the transformation by creating a single, universally accessible digital ledger, called a blockchain. It's called a chain because changes can be made only by adding new information to the end. Each new addition, or block, contains a set of new transactions—a couple of thousand in late August—that reference previous transactions in the chain. So if Helmut pays Hendrieke a bitcoin, that transaction appears at the end of the chain, and it points to the transaction in which Helmut was previously paid that coin by Helche, which in turn points to the time before that when Helche was paid the coin by Halfrid, and so on.

Bitcoin's blockchain, unlike the ledgers maintained by traditional financial institutions, is replicated on networked computers around the globe and is accessible to anyone with a computer and an Internet connection. A class of participants on this network, called miners, is responsible for detecting transaction requests from users, aggregating them, validating them, and adding them to the blockchain as new blocks.



HACKS & HEISTS

2016

Shortly after the Distributed Autonomous Organization debuted on the Ethereum blockchain, someone siphoned US $60 million in ethers from this autonomous version of a venture-capital fund. In a bold move, the Ethereum developers rewrote the blockchain code to return the money.

Validation entails both verifying that Helmut actually owns the bitcoins in his transaction and that he has not yet spent them elsewhere. Ownership on the Bitcoin blockchain is determined by a pair of cryptographic keys. The first, called the public key, resides in the blockchain for anyone to see. The second is called the private key, and its owner keeps it safe from view. The two keys have a special mathematical relationship that makes them useful for signing digital messages. Here's how that happens: Helmut takes a message, combines it with his private key, does some calculations, and ends up with a long number. Anyone who has the original message and knows the corresponding public key can then do some calculations of their own to prove that the long number was in fact created with the private key.

In Bitcoin, transactions are signed with private keys that correspond to the public key most recently associated with coins being spent. And when the transaction gets processed, those coins get assigned a new public key.

But the main role of miners is to ensure the irreversibility of new transactions, making them final and tamperproof. The method they use for doing so is thought to be the most significant contribution that Satoshi Nakamoto—whoever he or she is—made to the field of computer science.

Ensuring irreversibility becomes necessary only when you invite anyone and everyone to take part in the curation of a ledger. If the Bitcoin blockchain were being run by a single bank with a set of known validators operating under a single jurisdiction, then enforcing the finality of transactions would be as simple as writing it into company policy and punishing anyone who didn't follow the rules.

But in Bitcoin, there is no central authority to enforce the rules. Miners are operating anonymously all over the world—in China, Eastern Europe, Iceland, Venezuela—driven by a diversity of cultures and bound by different legal systems and regulatory obligations. Therefore, there is no way of holding them accountable. The Bitcoin code alone must suffice. To ensure proper behavior, Bitcoin uses a scheme called proof of work.

How Does Proof of Work Secure Blockchains?

First, let's be a bit more specific about the problem that public blockchains are trying to solve with proof of work. In this open peer-to-peer network, miners—whoever is running the bitcoin code—are receiving news of transactions and gathering them to create a new block. They are doing so in competition with one another, because the first to create a valid block gets paid (in bitcoins) for that service. In this situation, what's to stop a miner from deleting previous transactions in the blockchain after they have been added? While this type of reorganization does not enable a miner to steal coins, it could be used to spend the same coins multiple times. For instance, I could go to some unwitting merchant and pay for a cup of coffee with bitcoins. If I were a miner, I could later go into my version of the Bitcoin blockchain, remove the transaction, and send the modified chain out to my peers, thereby redepositing the bitcoins I spent back into my own pocket.

Therefore, it is crucial that all miners on the Bitcoin network have the same copy of the blockchain, and that all changes and transactions are irreversible. "The fact that they're all playing the same music is very important for the music to sound good," says Stefan Thomas, a developer for Ripple, a bitcoin-inspired digital currency.

To keep all the musicians in sync, the Bitcoin mining software makes it very expensive—in terms of computing power and, therefore, electricity—to add new blocks and even more expensive to change blocks further back in the record.

Any miner trying to add a new block must also provide a cryptographic proof to go along with it. In order to produce the proof, the miner digests the new block through multiple rounds of a hash function—a computation that takes a chunk of data of arbitrary length and reduces it to a meaningless alphanumeric string with a fixed length, called a hash. To make the process more challenging, the blockchain algorithm demands that the resulting hash start with a certain number of zeroes. The difficulty comes from the fact that there is no way to predict what hash any given data set will spit out, and so miners run the computation over and over on their validated blocks, each time inserting a random number into the data set. When that number is changed, a new hash results. When at last the miners get the correct number of zeroes, they're done.

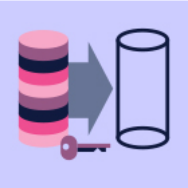
The first miner who finds a satisfactory hash then announces the new block to the other miners, who check it and append it to the full version of the blockchain that they are harboring on their computers. For performing all this work, miners collect a reward of newly minted bitcoins as well as any mining fees, which users voluntarily tack onto their transactions in hopes of pushing to the head of the line.

Think of hashing as a way of locking the blocks on a chain. Suppose you have a lock that requires a key to close. You also have a huge pile of keys at your disposal, but you don't know which one will work. You have to try them one by one. When you finally find the correct key, you leave it in the lock so that anyone can check that it's the right fit.

THINGS TO DO WITH A BLOCKCHAIN

Self-Driving Cars

Cars can now drive themselves (sort of). Isn't it about time they got an allowance? The blockchain startup Oaken Innovations is looking into equipping self-driving cars with cryptocurrency wallets for minor expenses like paying tolls and buying oil changes.



See illustration: **Miners & Signers**

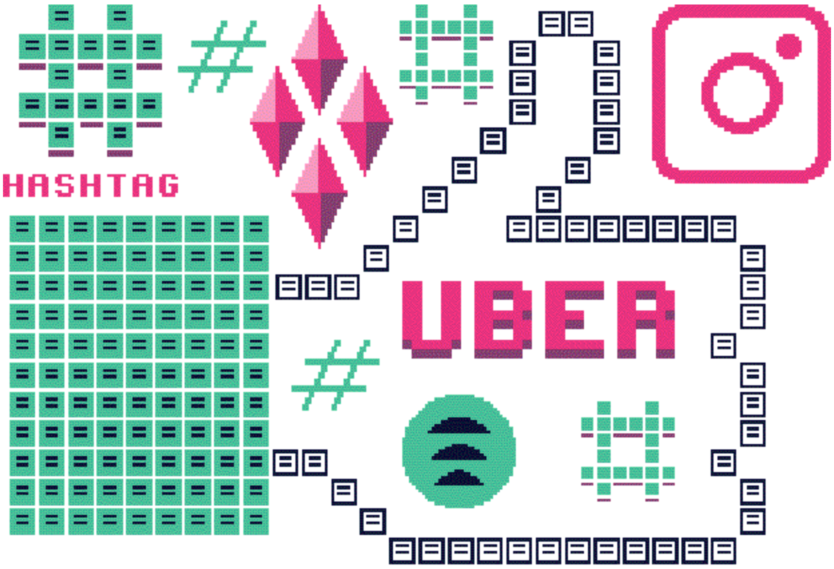
Theoretically, this work and the payoff that miners receive act as incentives for good behavior. Bitcoin miners are heavily invested in the network that they serve, both in the electricity they consume and in the hardware they buy. Therefore, the thinking goes, they should be disinclined to damage the currency in any way, including by taking any actions, such as double-spending, that might call into question the integrity of Bitcoin and devalue the currency.

Such attacks are further thwarted because the cost of changing the contents of old blocks is compounded by each new block that gets added to the chain. When a new block is made, it contains the hash of the one before it. Any changes in old blocks will result in invalid hashes for all subsequent blocks. Therefore, it is impossible to insert bogus modifications into a previous block without having to repeat all the work that was performed after that block. In that lock analogy, it's as though the design for the lock at the end of the chain depends on all the locks that came before it. So changing one lock in the middle of the blockchain means having to find new keys for every lock after it.

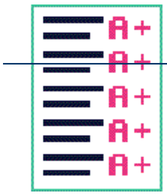
Bitcoin "deters misbehaving parties because the damage a misbehaving party can do is bounded by how much [computational] power he has," says Emin Gün Sirer, a codirector of Cornell University's Initiative for CryptoCurrencies & Contracts (IC3).

By forcing miners to provide costly proofs and then repaying them for their work, Satoshi created the first viable peer-to-peer digital currency. But he also solved a more general problem that had vexed computer scientists for decades—consensus. Bitcoin, which has never been knocked off-line for any substantial period of time over the past eight years, reliably incentivizes a network of potentially dishonest participants to process transactions and secure a single version of those events. The result is an ever-growing chain of data that anyone with an Internet connection can inspect and add to, and one that has proven remarkably impervious to attack.

How Can You Use a Blockchain to Do Other Things?



It turns out that such a system may be useful for much more than just money. Almost as soon as Bitcoin debuted, people began imagining what other kinds of applications you could run on a blockchain if you generalized the technology. When miners validate transactions, they are really running small programs that process the data and deliver a thumbs-up or a thumbs-down on the transaction request. But what if they could run more complex programs, like the software for a social media network? And what if the blockchain were used to represent data other than simple currency transactions, like messages on an online forum?



THINGS TO DO WITH A BLOCKCHAIN

Educational Records

Educational Records: Most people would change some detail of their school records if they could. Today, principles and the fear of being caught keep us honest. But tomorrow it might be the blockchain. Sony and IBM are creating a new blockchain for tracking and storing diplomas, transcripts, and other kinds of educational records.

Although these ideas were around from Bitcoin's inception, it would take several years and a 19-year-old computer science student in Toronto to make them popular. In 2013, Vitalik Buterin devised an entirely new blockchain called Ethereum. The goal of Ethereum was to take what Bitcoin had done for currency and expand it into other realms.

Like Bitcoin, Ethereum uses a blockchain that has its own currency, called ethers. Unlike Bitcoin, Ethereum uses transactions that are miniprograms, called smart contracts, that can be written with an unlimited amount of complexity. Users can then interact with programs by sending them transactions loaded with instructions, which miners then process.

In practice, this means that anyone can embed a software program into a transaction and know that it will remain there, unaltered and accessible for the life span of the blockchain. Theoretically, with Ethereum, you could replace Facebook, Twitter, Uber, Spotify, or any other digital service with new versions that would be invulnerable to censors and transparent in their policies, and which could operate indefinitely in the absence of the people who created them.

"The amazing thing is you can put a computer program on that network…and, similar to Bitcoin, everybody on the system can agree on exactly what happened and when it happened…I think that's a profound idea," says Joseph Lubin, a founder of Ethereum, who now runs Consensys, a Brooklyn-based incubator for decentralized applications.

What's a Permissioned Ledger?

Concurrent with Buterin's attempts to use blockchain technology to make a world-spanning computer, another trend was pushing the technology in the opposite direction, toward a more closed and controlled iteration of Satoshi's masterpiece. In September of 2014, a group of financial institutions—including Barclays, Goldman Sachs, and J.P. Morgan—formed a consortium, called R3, to explore how blockchains might improve the efficiency of payments between banks. [To see how far this has gone, read "Wall Street Firms to Move Trillions to Blockchains in 2018," in this issue.]

It didn't take long for these institutions to realize that the open structure of blockchains like Bitcoin and Ethereum ran counter to their needs. Of primary concern was the anonymity of users, who on open blockchains are represented by alphanumeric public addresses, providing no indication of their real-world identities. Banking laws in the United States and elsewhere forbid such anonymity. "We have to know particularly who our participants and counterparties are on these platforms," says Tim Swanson, the director of market research at R3.

Financial institutions are also legally required to protect customer data and control its export across national or regional lines. Given that public blockchains replicate the entire transaction record on every computer in the network, it's impossible to restrict the chain of custody while using them.

Thus was born the "permissioned ledger" approach to blockchain technology. In a permissioned ledger, the identity of people adding blocks is known, and data in the system is viewable only by selected parties. Because the right to create new blocks is assigned by the people who run the code rather than by a lottery, there is no need for proof-of-work mining or a cryptocurrency to pay for it.

This kind of system is intended to be used in situations where all participants on a blockchain already have a small degree of trust among them but want to simulate the services of a neutral third party, as might be the case with banks when settling international wire transfers.

Last year, R3—which recently raised US $107 million from more than 40 institutions—released its first permissioned ledger, Corda. And Corda already has a competitor; J.P. Morgan, which left the R3 consortium this past spring, has released its own permissioned ledger, called Quorum.

The permissioned-ledger approach has also spread beyond banks to other industries that find themselves serving as guardians to sensitive customer data. Many of these projects are built with tools provided by Hyperledger, an open-source project hosted by the Linux Foundation and backed by big tech firms. Hyperledger is building products for companies that want to work with smart contracts but are hesitant to embrace open blockchains like Ethereum and Bitcoin.

“People have to understand the actual concerns and the regulatory requirements that entities such as banks, insurance, and the health care industry have to adhere to. They cannot afford the risk and uncertainty that is introduced by some of the open systems,” says Jonathan Levi, creator of Hacera, an access-control management system for blockchains.

How Are Smart Contracts Really Going to Work?

Regardless of what flavor of blockchain wins in the end, the smart contracts that will run on it will need a variety of supporting technologies. These supplementary technologies are now being developed, to little fanfare, in the shadow of the blockchain carnival. And they will be absolutely crucial to the expansion of blockchain technology.

“Once you’ve got smart contracts, a whole host of problems arise,” says Ari Juels, a codirector of Cornell University’s IC3. These problems fall into a couple of categories.

For one thing, blockchains can’t store much data. That’s going to be a problem for the many projects that, for example, propose to live-stream video over the blockchain—there’s nowhere to put the video content.

The Bitcoin blockchain records the inputs and outputs of every coin on the network, as well as the content of an additional field that allows for up to a mere 40 bytes of metadata per transaction. That’s all.

See illustration: **How Smart Contracts Work**

Another problem with putting contracts on blockchains is that blockchains by themselves don’t know what’s going on in the real world. That’s a problem if, say, your smart contract is a flight insurance system, because it needs to know when your flight really takes off and lands. Blockchains were never designed to query websites. “Anything they learn about the outside world has to be injected into them,” says IC3’s Juels.

Ideally, developers will devise schemes for storing and accessing data in ways that do not reintroduce the weaknesses—vulnerability to censorship and a reliance on potentially dodgy humans—that blockchains were invented to avoid. To accomplish that, developers will have to carefully consider which “trusted parties” they can actually trust.

The problem of storing static data might be solved with distributed file sharing services, such as Protocols Labs’ Interplanetary Database or Storj Labs’ decentralized cloud storage system. These are systems that would enable people all over the world to rent out surplus space on their hard drives. Such schemes would work for a blockchain-based smart contract system because the data would be redundantly stored on multiple computers around the world, and thus would always be available and difficult to censor.

As for importing real-time data into a blockchain, this could be handled by what blockchain developers are calling “oracles.” These are services that get paid for reliably querying sources of real-time data and feeding it to smart contracts on the blockchain.

At IC3, Juels has implemented an automated oracle called Town Crier [PDF]. It's meant to ensure that data injected onto a blockchain comes from a trustworthy source and hasn't been tampered with. It uses a "trusted software" enclave on Intel processors. The chips run code behind a cryptographic shield but still provide proof that the program was executed as promised.

Where's All the Money for This Stuff Coming From?

If the many digital services that modern society has come to rely on are to be rebuilt on blockchain technology, then someone is going to have to pay for all of the engineering and research that will have to be done.

But how do you get money for those functions when what you're trying to do is create a technology that—if it succeeds—will destroy the valuable data many enterprises survive on? Ideally, open blockchains, like Ethereum, entrust custody of data to the people who created it, giving them the option to choose how they share it. In such an environment, it is no longer feasible for a company to survive off a business model that harvests and sells its customer's browsing behavior, purchasing history, or location data. Nor could blockchain companies rely on the restricted possession of their intellectual property, as programs on an open blockchain are there for everyone to see.

Nevertheless, a potential funding mechanism for blockchain-based businesses has already emerged: A new trend in blockchain funding called initial coin offerings (or ICOs, after initial public offering, or IPO) has turned out to be wildly lucrative, although legally questionable.

Groups that choose to fund their projects with ICOs design their smart contracts in such a way that a user must own an app-specific coin in order to use the app. These groups then create a bunch of the coins before their launch and sell them on the open market.

In the nondigital world, it would be like someone opening a laundromat where you could use only custom coins to run the machines. And so, instead of just getting investors, the owner stamps out a bunch of coins to sell to the public, which can then be traded at prices determined by the value of the laundry service.

To date, over half a billion dollars has flooded into blockchain companies by way of token sales, and the last few months have seen an eye-popping acceleration in the rate and price of new offerings. This July, a blockchain project called Tezos set a record by raking in over $200 million with an ICO.

Such astronomical investments have led some observers to complain that there is a grim hypocrisy at work. "The blockchain entrepreneurs who are pushing these schemes are really demonstrating all the avarice and cupidity which they ascribe to standard financial services" and government-backed currencies, says Preston Byrne, the cofounder of Monax Industries, an open platform for blockchain developers. "So, when the money starts flowing in their direction, they're becoming equally careless about the public—whom they once were."

However, others argue that the ICO, as a new class of investment vehicle, is just as disruptive as the applications being funded.

"Money is not the root of all evil. Equity is the root of all evil," says Joel Monegro, who left Union Square Ventures to start Placeholder, a new fund devoted exclusively to blockchain technologies.

His argument, which is often repeated by blockchain startup leaders, is that giving founders and employees equity in a company encourages them to hoard that wealth rather than use it to improve their products.

An app-specific coin, on the other hand, is not only a financial instrument but the means for accessing a technology. It follows that the more people use a service, the more demand there will be for the token required to access that service.

“My incentive as a company is not to extract more profits but to get more usage, because the token appreciates in value with the usage of the service. You completely flip the incentives,” says Monegro.

In the United States at least, the ICO binge has likely come to an end. In late July, the U.S. Securities and Exchange Commission sent a chill through the startup scene. It issued a warning that many of the ICOs reviewed by the department fell into the category of securities and would therefore be bound by its rules.

Nevertheless, the trailing edge of the tsunami of ICO cash is still washing up on the shores of the industry. Only time will tell if it’s put to good use.

“Times have changed, and very quickly. Some of us early adopters, who struggled financially three and four years ago but held onto their beliefs and their coins, are very well off now,” says Hacera’s Levi. “We still need Bitcoin and Ethereum to operate at larger scales, and enterprises need to decentralize more and secure their sensitive data. We are now facing a new and different kind of a challenge: Given the vast amounts of money invested, it remains to be seen how many old-timers and newcomers will stay true to the cause and continue to work to change the world with the technology that already changed theirs.”

SPECIAL REPORT: BLOCKCHAIN WORLD

PREVIOUS
< Browse All Stories

NEXT
How Smart Contracts Work >