Attendee enters Inside Bitcoins conference, New York City, United States.

The Internet of Trust

Created to avoid banks, bitcoin's blockchain technology may end up helping them

Andreas Adriano and Hunter Monroe

THE greatest thing about cash is the simplicity of transactions. You just hand it over and receive something. Nobody asks your name, address, phone number, date of birth, social security number, salary, how long you've been in your current job … Cash produces instant *trust* between buyer and seller.

Because it's impractical to move large amounts of hard cash around, paper-based and later electronic payment systems were created. However, establishing this trust without cash is complex and expensive. Acquiring a credit or debit card requires the applicant to answer numerous questions—and the issuing bank to verify the answers and the applicant's credit. Using the card demands a complex infrastructure to ensure that transactions are fast, reliable, and safe—and costs the merchant a percentage of each sale.

Domestic transfers between banks depend on payment systems operated by central banks, while international transfers may involve other commercial banks between the sender's and the receiver's banks. Furthermore, these transactions can take several days. As another example, although we associate modern stock markets with nearly instantaneous electronic trades, settling transactions can take two to three days and requires additional players, including custodians, notaries, clearinghouses, and central securities depositories. Until the transactions have settled, financial institutions must set aside significant amounts of cash or other liquid assets to cover their positions if someone along the line does not pay.

Simpler and cheaper

Could technology make things simpler and cheaper again? Enter bitcoin, the digital currency that some claim will spell the end of banks but others view as a Ponzi scheme and a financial vehicle for criminals. Bitcoin—or more precisely, the underlying technology that allows it to function, called distributed ledgers, or blockchain—could allow what many see as radical rewiring of the financial sector (see Box 1).

Bitcoin's story is well known: it started when Satoshi Nakamoto—the name used by the inventor, whose actual identity is still uncertain—posted a paper and software on

an email discussion list of activists who believed that cryptography could bring about social and political change ("cypherpunks"). Others became interested and soon started to develop the idea online. Bitcoin started trading in 2009, with an exchange rate against the U.S. dollar of $0.0007 per bitcoin. In February 2011, it reached parity with the dollar. In November 2013, the value of bitcoin peaked at $1,242, and it has been trading above $400 for most of 2016. The value of bitcoin in circulation is about $6 billion (compared with about 1.5 trillion U.S. dollars in circulation worldwide).

In the beginning, bitcoin grabbed the imagination of libertarians who wanted to get rid of, or at least have an alternative to, banks and central banks. While the exchange rate surge triggered something of a gold rush, bitcoin's relative anonymity and ease of trading attracted drug dealers and other criminals, leading to a heavy law enforcement crackdown during 2013 and 2014 that landed some early entrepreneurs in jail and gave the whole initiative a bad reputation.

Tech entrepreneurs and the financial industry soon realized that the real news was under the hood—bitcoin's underlying distributed ledger technology. Essentially, this is a technology for verifying and recording transactions on a peer-to-peer basis without a central authority. It upends a very basic tenet of payment systems: having one central, independent, and trusted bookkeeper that stores and validates all transactions—a role often played by central banks (see chart).

With bitcoin, everyone on the Internet can validate and record transactions in their own copy of the ledger. They group the transactions during a given period into a block, which is followed by a tamper-proof stamp. Each transaction block links to a block for the previous period—hence the term "blockchain." Completing the block for a period requires

Box 1

You got money

Several start-ups are already delivering small payments and remittance services at low cost using bitcoin as a payment system, not a currency. Rather than charging 8 percent to send remittances, the start-up Circle Internet Financial, for example, performs the service free. Its sleek mobile app incorporates social media features like sending pictures and emojis together with a payment notification—appealing to a younger demographic accustomed to expressing itself in smileys.

Users link their profile to a bank account or card on each end of the transaction and simply "text" money to each other anywhere in the world. Transactions are conducted via bitcoin, but the user doesn't need to know how it happens. If the receiver is not in the bitcoin system, the money can still be retrieved with other "digital wallets" (apps that allow the storage of bitcoin or other currency on a smartphone) or at the counters of remittance companies for a small fee, provided they also deal in bitcoin.

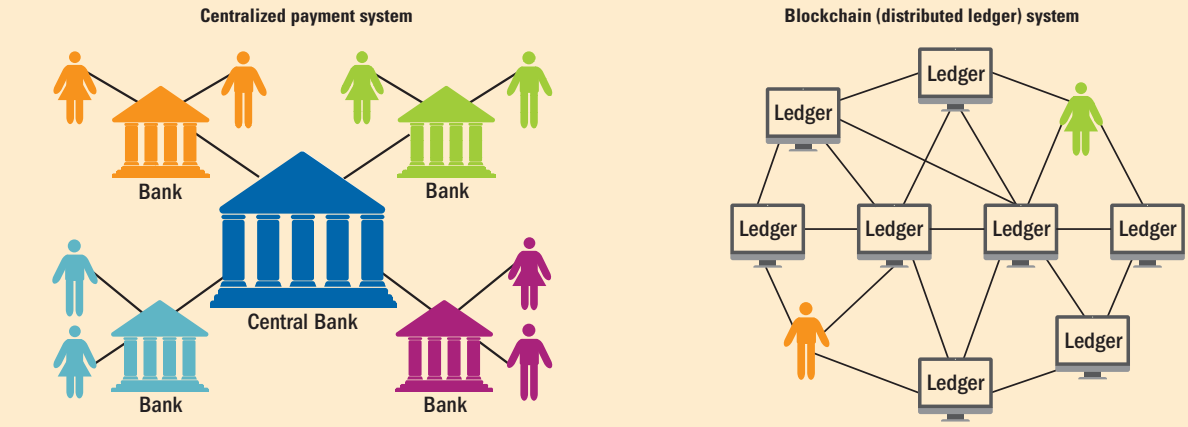
"It's like with sending an email," says the Circle CEO, Jeremy Allaire. "You don't care about how the message is routed through the Web." He explains how his Filipino nanny in California used to spend about $50 for each remittance home and now pays $0.75, and that much only because her family at the other end of the transaction doesn't use Circle. Because transactions happen very quickly, bitcoin's well-known volatility is not really an issue.

Circle combines the digital appeal with some good old "real" features. It is registered as a money service business, which allows it to provide many banking services, except lending and investing clients' money, and enjoys deposit protection from the U.S. government. It recently became licensed in the United Kingdom and formed a partnership with Barclays Bank.

Like many start-up honchos in the Internet's early days, Allaire, whose coffers are well funded by venture capitalists, is not concerned with short-term profitability. "Our business is entering a market that generates trillions of dollars of revenue a year for retail banks. There's absolutely huge amounts of market share to be disrupted or to be accessed with digital banking products," he says. Didn't many companies fail in the early 2000s by focusing too much on acquiring customers and too little on monetizing them? "The most significant Internet companies, they all started by focusing relentlessly on providing a free consumer utility that really delivered a lot of value for consumers. And they did it for several years until it got to a meaningful scale," he adds.

Spreading the burden

In traditional banking, the central bank tracks payments between clients; in blockchain banking, transactions are recorded on multiple network computers and settled by many individuals.



some computational work, with a reward in bitcoin—so the people competing to complete blocks are called "miners." Thus bitcoin, by combining a peer-to-peer approach with cryptographic security, became the first successful digital currency, after several decades of failures.

So how big a deal is that? U.S. entrepreneur Marc Andreessen explained it this way: "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," he said in a *New York Times* article in January 2014.

Andreessen was an Internet pioneer, who while still in college in 1993 founded Netscape, the first widely used Web browser. He now runs Andreessen Horowitz, one of Silicon Valley's most influential venture capital funds. Venture capitalists make money by finding the next big thing before it's even a thing. Andreessen and many other venture capitalists who funded the creators of the Internet as we know it are now betting on bitcoin and the underlying blockchain technology. They see this technology as a breakthrough that can establish, between unknown and physically separated participants, the same trust as a cash transaction. Some predict that this capability to disintermediate any trusted third party will be the most disruptive technology since the Internet. The (overused) word "disruptive" refers to new technologies that shake up, or even destroy, traditional business models. Think Amazon and bookstores, or Uber and taxis. Disrupting the financial industry, the most regulated business in the world, is a whole different game. It is possible and even desirable, as the *Financial Times*' Martin Wolf wrote recently, given the industry's many shortcomings, but very complicated in all aspects: legal, fiscal, financial, and operational.

Traditionally, the financial industry has tried to solve the problem of creating trust by acting as a trusted intermediary between individuals and companies who do not know each other, with central banks and regulators backing up this trust by supervising banks and through deposit insurance. Individuals and companies pay banks to conduct their transactions, for example through credit cards and wire transfers, because other banks and the central bank recognize each other as trustworthy counterparts. It's great business for them: according to a McKinsey&Company report, banks extract an astonishing $1.7 trillion a year, 40 percent of their revenue, from global payment services. Even more surprising, despite all technological innovation, the cost of financial intermediation in the United States has not changed significantly since the beginning of the 20th century, according to research cited by the Bank of England's chief economist, Andrew Haldane, in a recent speech. In a 2012 report, the European Central Bank (ECB) estimated that, aside from the fees everybody pays, the indirect costs are as high as 1 percent of GDP, which in the European Union alone translates to about €130 billion a year. And the cost of sending remittances to another country is even higher—nearly 8 percent according to the World Bank. However, a number of start-ups, many using bitcoin, make sending payments as simple and inexpensive as sending an email (see Box 2).

Transforming the financial sector

According to its proponents, bitcoin's blockchain technology can be used to transform the financial sector fundamentally, for example by reducing the settlement time for securities transactions. With faster settlement, less money needs to be set aside to cover credit and settlement risks—just as collateral is not needed for a cash transaction.

The list of potential uses is even longer. Think property titles, for example—home buyers in the United States usu-

Box 2

Bitcoin FAQs

Q: Is bitcoin the only digital currency?

A: No, there are over 700 so-called cryptocurrencies out there. Bitcoin is the best known, with the highest market value, liquidity, and acceptance. Ethereum is a distant second.

Q: Are cryptocurrencies safe?

A: Episodes of hacking, stealing of bitcoin, and even bankruptcy of exchanges and wallet providers have occurred, but less frequently over time.

Q: How volatile are they?

A: Cryptocurrencies can be very volatile. Bitcoin has hovered just above $400 during 2016; it was trading below $300 in May 2015, but was above $1,200 in 2013.

Q: If it's so volatile, is it a good investment?

A: It is a very speculative investment. And it's not guaranteed by a central bank or backed by a government. Investors are totally on their own.

Q: Is it a good payment system?

A: It's cheaper than many conventional options for remittances or money transfers and can be very convenient for instance for smartphone payments. To the extent that transactions are settled quickly, volatility is less of a problem.

Q: How can I buy bitcoin or other cryptocurrency?

A: There are many exchanges that sell and buy bitcoin, such as Coinbase, Localbitcoins, and CoinDesk. There are also a growing number of physical automated teller machines, or ATMs, that will convert hard currency into bitcoin.

Q: How do I store them?

A: The most practical way is to download a digital wallet to a smartphone. As with a real wallet, these are good for small purchases. Storing large amounts is more complex. Some users have a dedicated offline computer (one not connected to the Internet all the time) and use encryption and very strong passwords to protect their funds.

Q: Where can I use them?

A: Acceptance is still limited but is increasing. A few online retailers accept bitcoin, as do some brick-and-mortar stores.

"There's nothing in the current technologies preventing instant settlement."

ally buy insurance to protect against liability originating from an unexpected claim on the property they are buying—or the process for buying, registering, and paying taxes for a car. A blockchain could provide digital, unforgeable proof of ownership along with a complete record of the chain of possession. There is also substantial excitement about smart, self-executing contracts—for instance, travel insurance that pays automatically if a flight is cancelled, or a car loan that disables the ignition if payments are missed. Blockchain technology also powers an alternative to bitcoin called Ethereum (with a currency worth about $800 million), which has lately been attracting some mainstream attention. Unlike bitcoin,its paternity is known: Vitalik Buterin, a 22-year-old Russian-Canadian college dropout.

Jerry Cuomo, IBM's vice president for blockchain technologies, also sees potential applications of purpose-built private blockchains to improve transparency through compliance and auditing, in sharp contrast to bitcoin's reputation as secretive and anonymous. "Bitcoin decided to be anonymous by design," he says. However, "it's perfectly possible to have a blockchain with different levels of access, in which participants don't see what others are doing, but auditors and regulators come in at a higher level and see everything," he explains.

Although much of the experimentation with blockchain technology is occurring in the start-up world, IBM is one of a number of big businesses dipping a toe into this water. Last December, it joined the Linux Foundation to disseminate blockchain technology with open source software (meaning any programmer can work on it, as opposed to proprietary systems like Windows). Large banks such as JPMorgan Chase & Co. and technology companies like Cisco and Intel are collaborating on the initiative. In February, the Tokyo Stock Exchange joined IBM to test blockchain use in recording trades in low-transaction markets, and the Australian Stock Exchange has asked Digital Asset Holdings, a start-up, to develop distributed ledger technology for clearing and settlement. A consortium of 42 global banks is working with a new company called R3 to develop distributed ledger standardized technologies for the financial industry.

Setting standards will be crucial here. It is typical of a new innovation cycle that different companies come up with different ways to do something, leading to a patchwork of technological approaches. Some worry that this could undo years of effort to integrate the financial industry globally. For example, under the Single Euro Payments Area (SEPA) initiative, it took European authorities 12 years from the launch of euro notes and coins in 2002 to integrate technological platforms and business procedures to make cross-border payments among the 35 participating countries as simple and inexpensive as a domestic transfer.

As the ECB's director general of market infrastructure and payments, Marc Bayle oversees SEPA and other continental integration initiatives, such as TARGET2, the euro area cash payment settlement system, and T2S, its equivalent for securities. He follows blockchain developments with interest, but is not impressed by some of the promises, like shorter settlement times. "There's nothing in the current technologies preventing instant settlement. The problem is the structure of markets. If a fund manager in Miami wants to invest in Frankfurt, there will be many legal, operational, tax, and financial considerations to be taken into account, and they might prefer to work with intermediaries providing such expertise in a cross-border context between the United States and the EU/Germany," Bayle says.

Useful in central banks?

He does not rule out the possibility that blockchain or similar distributed ledger technologies might evolve to become useful in central banks, despite their current limitations and the conceptual tension between distributed and central ledgers. While the use of blockchain to replace the ECB's main settlement systems is not really envisioned now, it is being considered in certain niches to foster secondary markets for more exotic securities. "We have to see whether this technology can be useful for us, if it can help lowering costs and having more resilient systems. But also, we have to think how it affects financial intermediation, the role of banks and other market participants, as well as our capacity as regulators," Bayle adds. Some are asking whether bitcoin and other blockchain applications could eventually undermine monetary policy and financial stability—but the consensus is that there is no immediate risk.

It is probably too early to say whether blockchain is "the next Internet" or just an incremental evolution. Silicon Valley is paved with overhyped ideas that later proved unviable and with revolutionary companies that disappeared in a few years, but still in some cases had some impact. Andreessen's Netscape Web browser was acquired by AOL in 1999 for over $4 billion. AOL itself, today a ghost of its lavish previous self, was acquired for about the same amount in 2015 by Verizon. It's not impossible to think that bitcoin or other blockchain technology could implode because of a still unknown design flaw or the work of a, well, disruptive hacker.

The blockchain game is only beginning. As Bill Gates once put it: "We always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten." ■

Andreas Adriano is a Senior Communications Officer in the IMF's Communications Department, and Hunter Monroe is a Senior Economist in the IMF's Monetary and Capital Markets Department.