Hutchins Center Explains: How Blockchain could change the financial system

By David Wessel

Editor's note: If you want to know more about blockchain and disruptive financial services technologies after reading this Q&A, watch the Hutchins Center's live discussion this Thursday at 1:15 p.m. EST. You can register here to receive a reminder about the event. It will be webcast live on the same page.

Bitcoin, the stateless virtual currency, often sounds like something between fad and fraud. But the technology undergirding bitcoin and other cryptocurrencies—both the software protocols that make them work and a "distributed ledger" innovation known as the "blockchain"—may prove to be enduring, a development that could significantly alter the way money changes hands around the world.

As Bank of England economists put it in a recent essay, "The key innovation of digital currencies is the 'distributed ledger' which allows a payment system to operate in an entirely decentralized way, without intermediaries such as banks." This could turn out to be a highly disruptive technology, one that challenges the dominance of the big players in payment systems and that significantly reduces the cost of financial transactions and the speed with which they are completed.

But the evolving technology faces risks and obstacles. Some of these stem from the public impression of bitcoin, a currency created with this new technology. These problems include hacking attacks on bitcoin wallets, governance challenges, threats to consumer protection, money-laundering concerns, resistance from entrenched financial institutions and raised regulatory eyebrows. It could turn out to be an infant technology, one that most of us don't yet understand, one that is about to change the world; think the Internet before browsers. Or it could fizzle out.

"Blockchain is a bit like gluten," says Tim Swanson, head of research at R3CEV, a New York start-up backed by 40 banks. "Everyone is talking about it but no one knows what it is in great detail." Here's an effort to address that.

Q. Is this about substituting bitcoin or some other virtual currency for the U.S. dollar?

A. No. While some enthusiasts of bitcoin focus on its use as a currency or an asset class for investment, the use of bitcoin as a substitute for dollars, euros or yen as a medium of exchange can be separated from other applications of the underlying technology, which moves value from one party to another across the Internet through a universal system of record, a feature that has rich potential outside payments, such as recording property deeds.

Q. What is a payment system? And how does ours work today?

A. There have been many different forms of money over the years—gold, silver, coins, paper, checks, electronic debits and credits. People use money to pay for purchases; that's a medium of exchange. Once upon a time, people physically traded gold or coins of other precious metals for goods and services. In the 16th century, goldsmith banks emerged. They held the gold, issued paper receipts (a precursor of paper currency) and recorded transactions in their ledgers. This worked only for people who used the same bank. Over time, the appetite for payments among individuals who used different banks created a need to make and record payments between banks. That, in turn, led to the emergence of a central clearing bank at which all the banks kept accounts.

Although we no longer use gold as a medium of exchange, modern payment systems operate on much the same model. Whether you pay with a debit or credit card or a new app on your phone like ApplePay or Venmo, the funds ride along a variety of electronic paths—like differing gauge rail lines—and wind up being settled centrally at a bank. "Payments are made by reducing the balance in a customer's account and increasing the balance in the recipients account by an equivalent amount—a process that has not changed fundamentally since the 16th century," the Bank of England economists observe. Today, ledgers are kept electronically, but there still is a central ledger, usually at the central bank, that keeps track of payments between banks, and ledgers at each bank to keep track of individuals' payments.

The payment system is an essential part of the plumbing of the U.S. economy and, as the Federal Reserve noted in a January 2015 report, the U.S. payment system is at "a critical juncture" in its evolution. "Technology is rapidly changing many elements that support the payment process. High-speed data networks are becoming ubiquitous, computing devices are becoming more sophisticated and mobile, and information is increasingly processed in real time. These capabilities are changing the nature of commerce and end-user expectations for payment services. Meanwhile, payment security and the protection of sensitive data, which are foundational to public confidence in any payment system, are challenged by dynamic, persistent and rapidly escalating threats. Finally, an increasing number of U.S. citizens and businesses routinely transfer value across borders and demand better payment options to swiftly and efficiently do so."

Q. So how does a "distributed ledger" work?

A. Any payments system needs trust. People won't accept payments if they can't count on the payments being of value; a loss of trust in a currency or in other intermediary institutions can trigger a destabilizing run. The question is how to generate that trust if banks aren't at the center of the system. A problem with any electronic payment system is ensuring that two people can't claim the same money. With coins or dollar bills, the physical act of possession means one can't spend the same money twice. A payment system that relies on digital records must have a way of preventing "double spending" because we all know that digital records can be edited, altered or copied. That is at odds with the key feature of money. Once you trade it away, you no longer

have it. Modern banks maintain ledgers that are the definitive record of an individual's balances. "Those holding ledgers," the Bank of England economists write, "have the ability to prevent any transaction they deem to be invalid. In order to use the system, people must trust that these centralized ledgers will be maintained in a reliable, timely and honest manner."

Bitcoin and its many look-a-likes do away with that centralized ledger. Instead, there's a decentralized ledger distributed among all participants and a process in which all the users agree on changes to the ledger. Most such ledgers are built with a blockchain, a database that consists of chronologically arranged bundles of transactions known as blocks. "Since anybody can check any proposed transaction against this [shared] ledger, this approach removes the need for a central authority and thus for participants to have confidence in the integrity of any single entity," the BoE economists write. A distributed ledger allows people to exchange electronic money with someone else without necessarily having the transactions settled centrally through a bank. Members of the system police transactions. The technical details are complicated, but essentially a network of computers uses cryptography to secure, update and maintain the integrity of the ledger. It is, as The Chain Blog puts it, "a collection of mathematical, recordkeeping and communications procedures that makes it possible to trade digital assets securely." The ledger "is immutable, distributed, and cryptographically secure...When you commit to the idea that the record of trades is the money, there is no separate clearing or settlement step needed. The trade is its own settlement."

Q. But do you need bitcoin or some other cryptocurrency to make this system work?

A. Not in all circumstances. A cryptocurrency *is* needed if transactions are being conducted over a ledger maintained by a public or "permissionless" network, one to which anyone has access, such as bitcoin's. That's because the computer owners who participate in those networks need a financial incentive to contribute their computing power and because the use of such as token of value deters fraud by making it prohibitively costly to seize majority control of what has become a very large network. But even in a permissionless system, it's possible for users to splinter the bitcoin into a tiny, immaterial amount (so they're essentially worth almost nothing) and then attach other information to that transaction in order to assert or transfer a claim on a valuable asset.

If, on the other hand, the ledger is maintained by a well-defined pool of participants whose membership is not open to the public – an approach known as "a permissioned system" – then some aspects of the technology can be deployed without bitcoin or other cryptocurrency. Thirty banks, for instance, have partnered with R3CEV, to deploy distributed-ledger technology without bitcoin to handle financial transactions among banks. Nasdaq OMX Group Inc. is testing the technology to record trades in privately held companies; it's "a natural evolution for managing physical securities," says Nasdaq CEO Robert Greifeld. Goldman Sachs recently applied for a patent for a virtual currency it calls "SETLcoin" that it says would offer "nearly instantaneous executive and settlement" of stock and bond trades."

Q. What are the advantages of all this?

A. Proponents of the new technology, which has drawn substantial interest from payments systems leaders in Silicon Valley and others outside of traditional finance, say the advantages include the immutability of its ledger, the much lower cost for financial transactions and its greater speed – even cheaper, safer and faster than mobile-phone apps used to move money today. In some forms, the technology could primarily serve to improve efficiency in the back offices of financial institutions and exchanges. Several start-ups have been founded with that that objective. Or the technology could be the means by which new players unseat entrenched institutions. Coinbase, for instance, offers a way for merchants to accept payment in bitcoin. Circle, a smartphone app, uses bitcoin to allow individuals to send cash around the world, but the users don't have to hold bitcoins or bear bitcoin/dollar exchange-rate risk. The threat from start-ups utilizing this new technology is already putting pressure on big banks and other financial institutions to reduce transaction costs and speed transactions with existing technologies and institutions.

The new technology is particularly appealing in niches where the financial system is a bit creaky. One start-up, Ripple, is using distributed-ledger technology to help banks move money more efficiently across currencies and national borders, eliminating the need for putting the money through what are known as correspondent banks. Spanish banking giant Santander is an early adopter. A start-up founded by JP Morgan veteran Blythe Masters, Digital Asset Holders, for instance, sees the instant-transaction aspect of the technology as a way to eliminate the lag between the sale of, say, a share of stock and the final settlement of the trade and to eliminate all-too-frequent errors in the records of sellers, buyers and middlemen Another start-up, Everledger, uses the technology to protect luxury goods; it will record data about a stone's distinguishing attributes, providing unchallengeable proof of its identity should it be stolen. If the technology drives transaction costs down far enough, new business models might emerge: newspaper websites, for instance, might use a permissionless or public network to charge just a few cents if you wanted to click on a particular story, essentially selling their content one story at a time, a feature that would be possible only on a permissionless or public network (today, the cost of charging a transaction to a credit card today makes such low-price sales difficult.) Low transaction costs and fast settlement could also be a boon to poor people who often face high fees to transfer money, and need quick access to their income to cover daily needs.

Q. What are the risks to of embracing distributed ledger technology?

A. Any network faces operational risks. ("The system is down. Please try again later.") A distributed ledger system is designed so records are stored on many computers around the world so they're less vulnerable to a failure of one node.

But there are still risks, some common to all payment systems and some unique to this new technology. Is it robust enough to handle large volumes? How will it resolve disputes? Will new

players be as reliable and trusted as banks and other institutions that handle financial transactions today? As the Committee on Payments and Market Infrastructure of the Bank for International Settlements warned in a recent report, "The system's decentralized setup and its open and flexible governance structure mean that it may be difficult to anticipate possible disruptions (e.g. hacking attacks on exchange platforms.)" Because any changes to the permissionless or public strains of a new payment system require consensus of the participants – recall there is no central authority – responding quickly to an unanticipated development could be difficult. Economist David S. Evans, a business consultant, observes that the savings promised by advocates of distributed ledger could shrink if, as is likely if the technology spreads, new players are burdened with some of the costs of regulation and governance that existing players bear.

Q: So what are regulators worried about?

A: Regulators of the financial system are (or should be) seeking to balance two important objectives: (1) maintaining the safety and stability of the payments system and the rest of the financial system, which involves deciding what kind of network is in the public interest and to what extent it should be decentralized and (2) encouraging the development of new technologies that could have social and economic benefits even if they hurt the businesses of existing financial institutions. That's easier said than done. As with any new technology – and particularly with a huge cast of new entrants – the regulators are asking about robustness, reliability and stability and how to apply or alter existing rules and legal frameworks, including consumer protection, to this new-fangled finance. Government authorities charged with combatting terrorism and money-laundering have an obvious interest in restraining any new technology that bad guys might use as an end-run around the traditional financial system to avoid detection – or in finding ways this new technology might be used to catch bad guys.

Q: And how might this affect the Fed and other central banks?

A: In most countries, including the U.S., the central bank oversees the payments system because it is essential to the functioning of a modern economy. In light of widespread technological ferment and the proliferation of start-ups, the Fed has established a Faster Payments Task Force comprised of representatives of industry and consumers. It is charged with identifying and evaluating alternative approaches for "a safe, ubiquitous, faster" U.S. payments system.

Bitcoin and its cousins aren't likely to unseat the dollar or government-issued currencies in the foreseeable future, despite the hype that sometimes suggests otherwise. Some central bankers speculate that if digital currencies take off, they might produce their own. But this is not going to happen in the near-term.

The author thanks Michael S. Barr, Jerry Brito, Michael J. Casey and Seth F. Wheeler for helpful comments. Any errors or oversimplifications are his responsibility alone.

References

Bank of England, "Innovations in Payment Technologies and the Emergence of Digital Currencies." Quarterly Bulletin, 2014: Q3.

The Chain Blog, "The Magic of the Blockchain." *The Chain Blog*, n.d.

Circle, "About," 2016.

Coinbase, "Coinbase," 2016.

The Economist, "The Great Chain of Being Sure About Things," *The Economist*, October 31, 2015.

David S. Evans, "Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms," Coase-Sandor Working Paper Series in Law and Economics (Chicago, IL: Universiry of Chicago Law School, 2014).

Federal Reserve Banks, "Faster Payments Task Force," *Federal Reserve Banks*, 2015 (Circle, "About," 2016.

Federal Reserve System, "Strategies for Improving the U.S. Payment System." January 26, 2016.

Bradley Hope and Michael J. Casey, "A Bitcoin Technology Gets Nasdaq Test," *The Wall Street Journal*, May 10, 2015.

Jennifer Hughes, "Goldman Sachs Files Patent for Virtual Settlement Currency," *Financial Times*, December 3, 2015.

Phillip Stafford, "Blockchain for Banks Still at the 'Gluten' Stage," *Financial Times*, December 9, 2015.

Tim Swanson, "Consensus-as-a-service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems." *R3CEV*, April 6, 2015.

Paul Vigna and Michael J. Casey, *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order*. St. Martin's Press, 2015.

Paul Vigna and Michael J. Casey, "Coinbase Raises $75 Million in Funding Round," *The Wall Street Journal*, January 20, 2015.

David Yermack, "Corporate Governance and Blockchains": Working Paper 21802 (Cambridge, Mass.: National Bureau of Economic Research, December 2015).