

Financial Insights

Created by The Financial Institution Relationship Management Group

Blockchain Technology Disrupting Traditional Records Systems

by Christoffer Koch and Gina C. Pieters

Blockchain technology, popularized by the digital currency bitcoin, is a decentralized digital ledger that has become a disruptive force in the financial industry and elsewhere. A blockchain acts as a distributed database or joint global register of all transactions, bypassing traditional, centralized channels such as banks. The technology underlies the recent surge in cryptocurrencies—digital currencies that, like bitcoin, rely on cryptography, or encryption, to ensure the legitimacy of their transactions.

Blockchain has the potential to revolutionize payment systems as well as peer-to-peer lending, document verification, ride-sharing and crowdfunding, among other applications. The blockchain behind bitcoin has no ownership and is publicly viewable by design. However, public availability of records is not a requirement of the blockchain technology in general, and many commercial applications do not necessarily incorporate it. This Financial Insights will give a high-level overview of the core features underlying the disruptive potential of blockchain technology and some of its limitations.

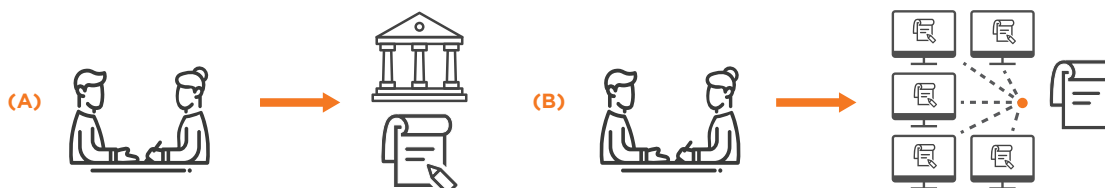
Why Are Blockchains Useful?

Digital currencies are susceptible to double spending: The same accounting units have the potential to be fraudulently claimed and spent multiple times due to the near-zero replication costs of digital units. Within a traditional currency system, a central authority or accounting intermediary keeps track of time-stamped transfers and balances (*Chart 1A*) and then permits the transaction to proceed after verifying account ownership and sufficient balances.

The bitcoin payment system succeeded because it automated and decentralized this process. It verifies ownership through digital signatures—a private–public key system—and employs the blockchain to verify sufficient balances, thus removing the need for a centralized ledger. Blockchain records are distributed across multiple computers (nodes) in self-organizing connected networks (peer-to-peer networks). Each individual node contributes to maintaining and verifying the blockchain (*Chart 1B*). Because the ledger is distributed across multiple computers in connected networks, there are no vulnerable centralized files or databases.

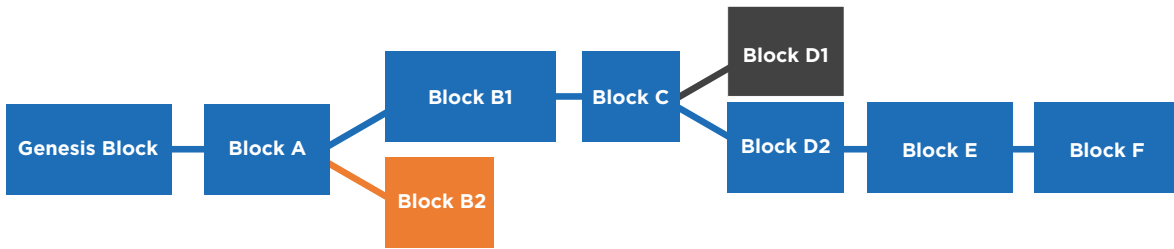
Chart 1

Maintaining a Ledger in a Traditional, Centralized System and a Decentralized Node Network



The private–public key system is widely used in online transactions, such as those using HTTPS (hypertext transfer protocol secure). Bitcoins reside in what is known as the bitcoin address, indexed by a unique, alphanumeric public ID called the public key—for example, 1CeWXYf239hqpxuo6B2Q1aX7FjWWXtYPXW. Associated with each public key is a private key, which is required to authorize any movement of bitcoins between public keys. The public key is akin to a checking account number; the private key is a unique authorizing signature. Authenticating whether an agent

Chart 2 A Stylized Formation of the Blockchain



has sufficient funds boils down to verifying that the particular public key has sufficient funds.

The public blockchain ledger permits the construction of a current balance as well as past balances for each public key by summing the value of transactions associated with the key using the fully recorded transaction history. As long as the blockchain record is correct, double spending is impossible.

How Are Blockchain Transactions Executed?

If two agents wish to engage in a transaction, they create and “sign off” on the transaction using the agents’ private keys. This marks the transaction as genuine. Their transaction is time-stamped and broadcast to the blockchain network, joining all other pending transactions. All pending transactions known to a node are collected into a new block—a collection of transactions that are encrypted using cryptographic techniques. Each block links back to the previous block of time-stamped transactions, creating a chain of blocks, or blockchain.

To create a block, a node must find the cryptographically correct nonce—an alphanumeric string—so that the new block satisfies certain criteria. The difficulty of finding the nonce, and thus creating the new block, is adjusted by the system to ensure a new block is created about every 10 minutes. The first node to uncover the nonce for a block broadcasts its solution to the decentralized network. Verifying that the “winner” node is indeed correct is computationally fast once the nonce solution is known. If the nonce and the transactions contained within the block are valid, the newly created block is then added to the blockchain by the winning node. This extends the length of the blockchain by one block.

It is possible that two nodes nearly simultaneously broadcast a new block—blocks B1 and B2 in Chart 2 both claiming to be the next in the chain—but the blocks themselves are slightly different for some reason. Typically, the block that results in the longest blockchain, B1, is judged to be the correct one. If both blocks are the same length but contain slightly different transactions—blocks D1 and D2 in Chart 2—some nodes add block D1 and others add block D2. The nodes continue working to create the next block, E. Suppose that block E associated with D2 finishes first. Then the chain A → B1 → C → D2 is longer than chain A → B1 → C → D1 and becomes the accepted consensus blockchain. The subsequent blocks—E, F, etc.—are added to

D2 and not D1. If the network ever wants to follow D1 instead, it must recalculate the new versions of blocks E, F, etc.

As nodes are constantly computing blocks of transactions, and building on previous transactions by continuously presenting their solutions, nodes are effectively both voting on and verifying the correct record of bitcoin transactions. A block can be added to the blockchain but be altered a few minutes later because the majority of nodes working on the transactions block reach different solutions. Editing any completed block involves redoing all the blocks after it as well, making retroactive editing of the blockchain a rapidly impossible task after consensus is reached. This is why blockchains are considered secure and prevent transaction fraud.

What Are Potential Vulnerabilities?

If the majority of nodes are honest, the honest blockchain will grow the fastest, outpacing competing dishonest chains that contain falsified transactions. A dishonest node trying to edit a past block would need to simultaneously redo both the block in question and all blocks based upon the edited block, and surpass the work of all the honest nodes to create the longest chain. This becomes exponentially more difficult as subsequent blocks are added. A vulnerability in this system arises, however, if a cartel forms.

In principle, a cartel of dishonest nodes could undermine the blockchain.¹ It could double spend bitcoin if it were to become large enough as dishonest nodes to exceed honest nodes. When a cartel manipulates a blockchain and it ceases to be an accurate register of transactions, it is dubbed a “51% attack.” Even then, a cartel cannot send bitcoins between arbitrary accounts, a “Sybil attack,” because it does not have the associated private keys. However, the cartel can alter records of transactions that were initiated, preventing transactions from being properly recorded, or by rewriting the blockchain to exclude past recorded transactions. A cartel member could pay Alice in bitcoin, receive goods and then force consensus on a blockchain that instead shows the bitcoin being paid to Bob, who may be a member of the same cartel. A record on the blockchain showing Alice’s bitcoin transaction would not exist. While this problem is fundamental to blockchain, it is easily detected and remedied if the nodes are publically viewable and competitive.

New Blockchain Technology Applications

The blockchain of bitcoin and of similar cryptocurrencies described above has been designed to have no ownership and be publicly viewable, allowing anyone to verify transactions. In contrast, commercial blockchain models differ in their approach to visibility and how consensus on blocks is achieved to avoid the 51% attack.

Corda, developed by the R3 consortium of over 70 major financial companies (Barclays, Credit Suisse, Royal Bank of Scotland, J.P. Morgan, Bank of America, etc.), is only loosely rooted in blockchain. Corda is not copied to all nodes—only parties in the transaction can vote on the block.

An alternative approach employs an interledger protocol, such as the one developed by Ripple. The Ripple protocol allows the Ripple blockchain and traditional ledger systems to communicate. Therefore, established financial institutions such as banks and credit unions can use the Ripple blockchain for transfers outside their institution while retaining their own proprietary and private ledger system. The Ripple protocol is being adopted by Accenture, UBS and other banks and was tested by Western Union to speed up cross-border transactions.²

More broadly, blockchains enable the codification of any agreement. Fabric is a blockchain developed by IBM to facilitate smart contracts—codifying legal contracts—and divides nodes into validating and nonvalidating peers to avoid the 51% attack.

Blockchain Possibilities and Limitations

While blockchains have the potential to revolutionize transactions, understanding their limitations is crucial for policymakers and users. Any individual or company that uses a blockchain technology must understand how ultimate control of the nodes is distributed—who will decide the ledger's accuracy. In many regards, the innovators of the technology intended for decentralization and democratization of transactions, thus revolutionizing the way payments are made, assets are exchanged and contracts are recorded.

Koch is a senior research economist in the Research Department and Pieters is an assistant professor of economics at Trinity University.

Notes

¹ For further details, see "Bitcoin: A Peer-to-Peer Electronic Cash System," by S. Nakamoto, bitcoin.org, 2008, <http://bitcoin.org/bitcoin.pdf>.

² For an application of cryptocurrencies to estimating capital controls, see "Bitcoin Estimate Capital Controls and Unofficial Exchange Rates?" Gina C. Pieters, 2016, Federal Reserve Bank of Dallas Globalization Institute Working Paper 292, and "Financial Regulations and Price Inconsistencies Across Bitcoin Markets" Gina C. Pieters and Sofia Vivano, 2017, Information Economics and Policy, vol. 39(C), June 2017, pp. 1–14.

Noteworthy Items

Federal Reserve Releases Federal Open Market Committee Statement

June 14, 2017

Fed Governor Jerome Powell: "Thoughts on the Normalization of Monetary Policy"

June 1, 2017

Powell asserts that after a tumultuous decade, the economy is now close to full employment and price stability. Despite what some have predicted, accommodative monetary policy is one of the main reasons for this return. The plans to unwind the Fed's balance sheet has been outlined by the Federal Open Market Committee in 2014. Powell reviews the different paths the Fed may take toward normalization.

Fed Chair Janet Yellen: "So We All Can Succeed: 125 Years of Women's Participation in the Economy"

May 5, 2017

Yellen reflects on the history of working women at the celebration of the 125th anniversary of women being admitted to Brown University. In her speech, she asserts that the integration of women into the economy has benefited society as a whole, using the women of Brown University as

examples. She also highlights the struggles many women still face despite the great progress that has been made, emphasizing the need for changes in the workplace that would increase female participation in the labor force as well as improve conditions for workers overall.

Dallas Fed President Rob Kaplan's Essay: "Assessment of Current Economic Conditions and Implications for Monetary Policy"

May 22, 2017

President Kaplan discusses his assessment of economic conditions in the U.S. and globally and their implications for monetary policy. He discusses key secular trends that can have a powerful influence on unfolding economic conditions: the aging workforce in the U.S., the global debt supercycle, globalization and technology-enabled disruption.

Eleventh District Banking Conditions Survey Results


May 2017


The Federal Reserve Bank of Dallas conducts the Banking Conditions Survey twice each quarter to obtain a timely assessment of activity at banks and credit unions headquartered in the Eleventh Federal Reserve District.

Dallas Fed Resources

Calendar of Upcoming Events

 **July 17**
Southwest CUNA
Management School
(SCMS)
FORT WORTH, TEXAS

 **Aug. 18**
Banker Roundtable
AMARILLO, TEXAS

 **Aug. 28–29**
Banking On the Leaders
of Tomorrow (BOLT)
Program
ALBUQUERQUE,
NEW MEXICO

Did You Know?

Congress established the Fed in 1913 to provide the country with a safer financial system.

Economic Updates

Texas—“Texas Economy Strengthens”

The Texas economy is growing at a moderate pace.

U.S.—“U.S. Economic Picture for First Half of 2017 Changes Little”

Economic indicators released in May and June point to continued moderate growth and a mostly unchanged outlook for the U.S.

International—“Output and Inflation Improves Across the International Economy”

The outlook for the global economy has slightly improved since early May.

Publications

Community Banking Connections

The Community Banking Connections publication is a nationwide Federal Reserve System resource for community banks.

Dallas Beige Book—May 31, 2017

A summary of anecdotal information about recent economic conditions and trends in the Eleventh District.

Economic Letter—“Bank Asset Concentration Not Necessarily Cause for Worry”

U.S. banking assets have become substantially more concentrated within a few large institutions.

Southwest Economy—“Texas Economy Shifting into Second Gear in 2017”

The first quarter 2017 issue looks at soaring home prices in Texas, the state’s 2017 economic outlook and Dallas’ strong job growth.

Surveys and Indicators

Agricultural Survey

The Dallas Fed conducts the quarterly Agricultural Survey to obtain a timely assessment of agricultural credit conditions in the Eleventh Federal Reserve District.

Texas Business Outlook Surveys—Manufacturing, Service Sector, Retail

The Dallas Fed conducts recurring surveys of over 900 business executives in manufacturing, services, energy, and ag lending across Texas and the broader Eleventh Federal Reserve District.

Eleventh District Banking Conditions Survey Results

The Federal Reserve Bank of Dallas conducts the Banking Conditions Survey twice each quarter to obtain a timely assessment of activity at banks and credit unions headquartered in the Eleventh Federal Reserve District.

Texas Economic Indicators

Texas economic indicators suggested continued growth in May.

About *Financial Insights*

Financial Insights is published periodically by FIRM—Financial Institution Relationship Management—to share timely economic topics of interest to financial institutions. The views expressed are those of the authors and should not be attributed to the Federal Reserve Bank of Dallas or the Federal Reserve System.

FIRM Staff

Tom Siems
Assistant Vice President
and Senior Economist
Tom.Siems@dal.frb.org

Matt Davies
Assistant Vice President
Matt.Davies@dal.frb.org

Steven Boryk
Relationship Management
Director
Steven.Boryk@dal.frb.org

Pam Cerny
Payments Outreach Analyst
Pam.Cerny@dal.frb.org

Donna Raedeke
Payments Outreach Analyst
Donna.Raedeke@dal.frb.org

Preston Ash
Economic Outreach
Specialist
Preston.Ash@dal.frb.org