



Bitcoin and Blockchain

By Olga Kharif & Matthew Leising | Updated June 2, 2017 10:28 PM UTC

When bitcoin broke into [public consciousness](#) in 2013, it couldn't have been sexier: a digital currency being used to buy everything from drugs to cupcakes. Now there's a new wave of excitement about an aspect of bitcoin that is a bit less sexy: public online ledgers. [Blockchain](#) – the technology used for verifying and recording transactions that's at the heart of bitcoin – is seen as having the potential to reshape the global financial system and possibly other industries.

The Situation

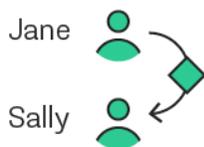
After years of volatility, the price of bitcoin reached a [new high](#) in early 2017, a surge tied in part to increased interest in China, where bitcoin is seen as protection against currency controls. But efforts to bring investing in the digital currency into the mainstream were set back when the U.S. Securities and Exchange Commission [rejected](#) an application to open a bitcoin-based exchange-traded fund that would have opened the field to more retail investors. Meanwhile, more than 50 banks including Barclays Bank Plc and JPMorgan Chase & Co. have joined the [R3 consortium](#), created to find ways to use blockchain as a decentralized ledger to track money transfers and other transactions. R3

has made its software code publicly available, which could hasten its broader adoption. Nasdaq Inc. is already using blockchain – with help from startup Chain.com – for trading securities in private companies. The Australian Stock Exchange is working [with blockchain startup Digital Asset Holdings to speed up](#) its clearing and settlement services in the cash equities market. Blockchain is also being tested by retailers like Wal-Mart Stores Inc. for [ensuring food safety](#), as industries ranging from healthcare to natural-resource management are exploring what advantages the technology might hold over traditional databases. Meanwhile, ether, a newer digital currency tied to the ethereum blockchain, began to take a [bigger share](#) of the cryptocurrency market, and more than [40 new types of digital coins](#) were issued in the first five months of 2017.

How Blockchain Works for Bitcoin

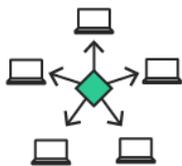
When payment is made with a physical coin, the person who handed it over can't spend it again. Preventing "double spending" in a digital currency is more complicated.

Transaction



Jane uses bitcoin to buy a cup of coffee at Sally's internet café, using her private key to transfer ownership of the currency.

Mining network



Word of the transaction is sent through the bitcoin network to "miners" with powerful computers.

Block



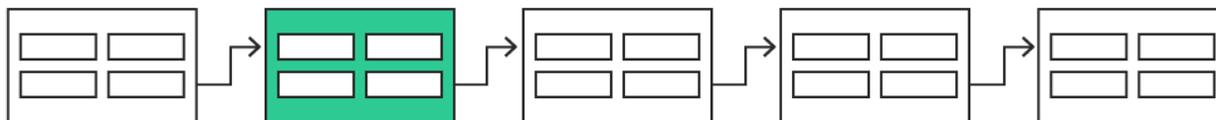
Miners use trial-and-error computations to solve a puzzle created by combining data about recent transactions. The first to find the unique number that unlocks the puzzle earns the right to bundle the transactions into a confirmed batch known as a block.

Verification



The winning miner is rewarded with newly minted bitcoin – but only after other miners confirm that the block's transactions don't contain any attempts to spend the same funds twice.

The Chain



Blockchain acts as a public ledger showing all transactions, though the identities of participants are obscured. Each block has a cryptographic link to the previous one. Every addition of a new, linked block to the chain makes it harder for a rogue miner to steal Sally's bitcoin by rewriting the sequence of transactions.

The Background

Virtual currencies aren't new – online fantasy games have long used them – but the development of a secure digital currency without a central issuer rightly turned heads. The [person or people](#) who created the bitcoin system under the pseudonym Satoshi Nakamoto solved a problem central to any currency –preventing counterfeiting – and did it without relying on a government's authority. The software also solved one specific hurdle for digital money – how to stop users from spending the same unit of currency twice. The breakthrough [idea](#) was blockchain, a publicly visible, anonymous online ledger that records every single bitcoin transaction. It's maintained by a network of bitcoin “miners” whose computers perform the calculations that validate each transaction, preventing double-spending. The miners earn a reward of newly issued bitcoin. The pace of creation is limited, and no more than [21 million](#) will ever be issued.

The Argument

Since bitcoin first boomed, there's been no shortage of critics to call its rise a [bubble](#) and to argue that the currency has no intrinsic value. But entrepreneurs in the field say that focusing on the price of bitcoin is missing the point – its value is as proof of concept for a new kind of payment system not reliant on third parties like governments, big banks or credit-card companies. Promising applications of blockchain include moving money abroad, signing contracts, clearing complex financial transactions and as a medium for [micro-payments](#) in emerging countries. Others say blockchain advocates are hyping what amounts to no more than a new kind of database. Proponents of ether respond that the etherium blockchain does far more than let bitcoin users send value from one person to another. Its advocates think it could be a [universally accessible machine](#) for running businesses, as the technology allows people to do more complex actions in a shared and decentralized manner.

The Reference Shelf

- A Bloomberg Businessweek [article](#) looking at how interest in blockchain is surpassing that in bitcoin.
- Bloomberg Television has a [video primer](#) as part of its “The 12 Days of Bitcoin” series
- Bloomberg Markets [traced the interest](#) of Silicon Valley investors in bitcoin.

- CoinDesk has a Bitcoin [price index](#); [Bitcoincharts.com](#) has a range of data.
- Two explainers, one aimed at [kindergarteners](#) and the other a [you-too-can-mine-bitcoin](#) project, plus an exploration of the [double-spending problem](#).
- The New Yorker looks at [Dark Wallet](#), a project meant to speed the spread of bitcoin, from the law student who invented the printable gun.

To receive a free monthly QuickTake newsletter, sign up at bloombergbriefs.com/quicktake

FIRST PUBLISHED OCT. 3, 2013

To contact the writers of this QuickTake:

Olga Kharif in Portland at okharif@bloomberg.net

Matthew Leising in Los Angeles at mleising@bloomberg.net

To contact the editor responsible for this QuickTake:

John O'Neil at joneil18@bloomberg.net



MORE [QuickTake](#) TOPICS

