

The Internet of Finance

Unleashing the Potential of Blockchain Technology

APRIL 16, 2015



HIGHLIGHTS

- The blockchain—the power behind Bitcoin—is widely recognized as a foundational technology and the key disruptive innovation in the Bitcoin protocol.
- Blockchain technology in effect removes the need for a clearing house or financial establishment to act as intermediary during a transaction and in doing so *transfers control and power from a central authority to the many*, facilitating quick, secure, and inexpensive exchanges of value.
- The innovation has potentially significant implications for companies in the payments space, including those involved in money transfer and credit card transactions, as well as for trade, commerce, and the financial system as a whole.
- A broad range of developers have recognized the potential of the blockchain and have started designing next-generation platforms such as Colored Coins and Ethereum.
- There are numerous obstacles facing the technology's widespread adoption in the real economy, including regulatory uncertainty and the enormous computational power and the high energy costs required to maintain the system. Critics also warn of the risk of eventual breakdown.

Despite concerns about potential risks, virtual currencies remain high on the list of new technologies that have the potential to transform financial services. [Bitcoin](#)—a decentralized cyber currency and payment system released in open-source software in 2009—is the [largest](#) and best-known on several measures (Chart 1).¹ However, bitcoin has faced numerous barriers to widespread adoption, including its lack of liquidity and volatility (Chart 2), as well as uncertainty surrounding potential future regulation. Such concerns have contributed to a significant decline in Bitcoin's market capitalization since the end of 2013 (Chart 3). Nevertheless, many observers predict that Bitcoin's underlying technology—the distributed public ledger, or “blockchain”—will play a significant and positive role in the financial services industry regardless of whether bitcoins become general-purpose currency. This CMM research note examines the technology's potential to alter the financial landscape.

WHAT'S A BLOCKCHAIN?

Bitcoin's blockchain is widely recognized as a foundational technology and the key disruptive innovation in the Bitcoin protocol. It is a cryptographically authenticated record of bitcoin transactions that offers confirmation of ownership for each bitcoin at any given time. Furthermore, the blockchain allows each bitcoin to be identifiable by its unique transaction history. Users maintain

The *Capital Markets Monitor* and other IIF publications are available on the Institute's website: <http://www.iif.com>

Questions or comments regarding this publication may be addressed to:

Dennis Ferenzy

Senior Research Analyst, CEM
1-202-857-3643
dferenzy@iif.com

Hung Tran

Executive Managing Director
1-202-682-7449
htran@iif.com

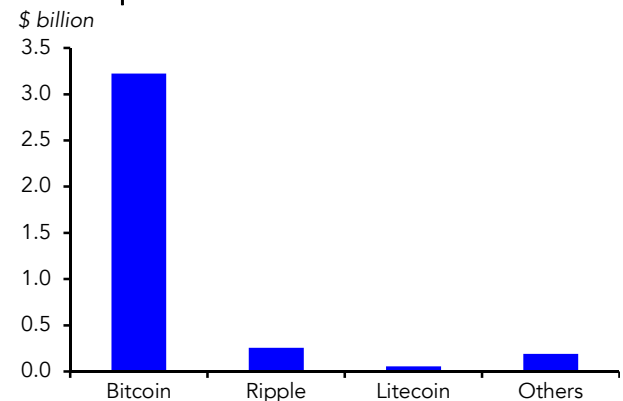
Conan French

Senior Technology Advisor
1-202-857-3624
cfrench@iif.com

Sonja Gibbs

Director, CEM
1-202-857-3325
sgibbs@iif.com

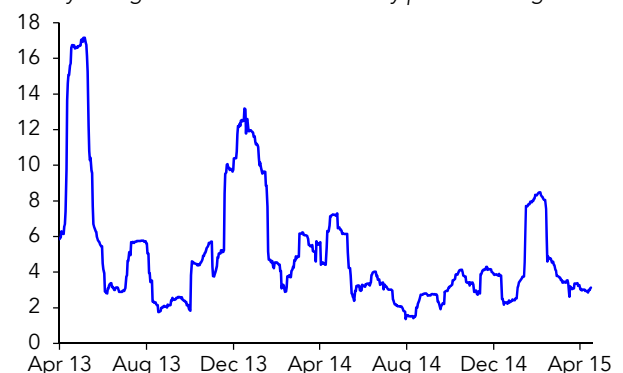
Chart 1
Market Capitalization of Internet-based Currencies



Source: www.coinmarketcap.com, IIF.

Chart 2
Bitcoin Price Volatility

30 day rolling standard deviation of daily percent change



Source: www.bitcoincharts.com, IIF.

1) Please see the CMM Bitcoin [Special Feature](#) from last year and our subsequent update on the topic from the IIF's [Weekly](#) for more information.

this distributed system through a process called “mining” whereby multiple node computers validate transactions by verifying the cryptographic hashes and transaction records which identify the block and coin. Payees can offer transaction fees to “miners” to incentivize verification, and these fees may become necessary to receive rapid confirmation in the future.

“Mining” is also the term used to describe the process for new blocks of coins to be found and added to the chain. The miners’ node computers solve increasingly complex calculations. The resulting “proof of work” for successful solutions, and the cryptographic hash, establish the new block of coins and are added to the blockchain.² The computational power and energy required for these proofs will also continue to increase as the system expands, and miners may seek compensation for their verification services.³

Finally, while the blockchain is most often referred to in the context of the Bitcoin platform, it is not technically dependent upon it. Other applications can, and have, incorporated the technology.

DISRUPTIVE TECHNOLOGY: MOVING TOWARDS AN “INTERNET OF FINANCE”

Because the financial industry’s foundation is built on the tracking and guaranteeing of assets as they travel from one centralized ledger to another, blockchain technology, which has been adopted by many other cryptocurrency systems, could dramatically alter the industry. Blockchain technology in effect removes the need for a clearing house or financial establishment to act as intermediary during a transaction and in doing so transfers control and power from a central authority to the many, facilitating quick, secure, and inexpensive value exchanges. This innovation has potentially significant implications for companies in the payments space, including those involved in money transfer and credit card transactions, as well as for trade, commerce, and the financial system as a whole.

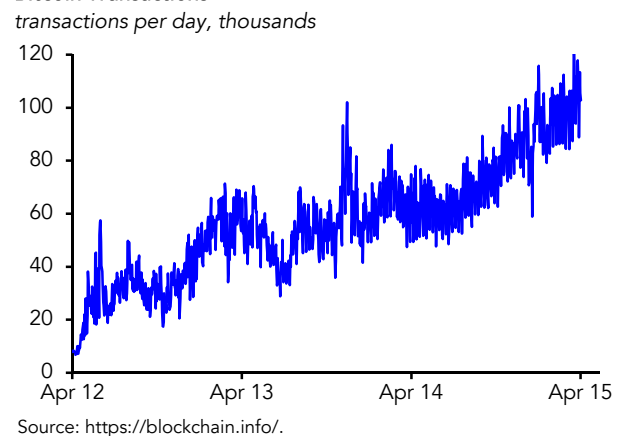
Cryptocurrencies utilizing blockchains show that digital transaction records can be managed securely without a central authority. Because most of today’s financial instruments exist electronically and because the current financial system is comprised of a set of digital records, many observers reason that blockchain technology could eventually supplant the current market infrastructure, where centralized ledgers are held and controlled by large institutions. However, for this to occur on a significant scale, various obstacles, including the blockchain’s requirement for enormous computational power and the associated high energy maintenance costs would need to be addressed.

A number of analysts believe that these obstacles can, and will, be overcome and that blockchain technology could be as disruptive as the Internet thanks to its ability to transfer value as seamless and low-cost as the Internet made the transfer of information. Indeed some commentators use the term “Internet of Money” to describe innovative cryptocurrency protocols. However, according to the Bank of England report, “[Innovations in payment technologies and the emergence of digital currencies](#),” because the blockchain’s function could extend beyond just payments, it may be even more appropriate to describe the technology as a “first attempt at an ‘Internet of Finance.’”

Chart 3
Bitcoin Market Capitalization



Chart 4
Bitcoin Transactions



2) For a more detailed summary, please see “[How does Bitcoin work?](#)”

3) New companies such as [21](#) seem to be focused on solving these constraints.

Blockchain technology, proponents argue, could lead to the removal of intermediaries in stock trading, contracting, and lending. All these functions could in theory be performed and documented on decentralized computer servers around the world. As a result, there could be myriad potential uses for blockchain technology, as noted in a [special report](#) in The Economist. For instance, the blockchain could lay the foundation for an updated commodity futures market, where trades are processed quickly and at very low cost. It could also facilitate the exchange of information required to corroborate a physical transaction, such as providing proof of authenticity for artwork and diamonds. Furthermore, the blockchain could also enhance transparency and improve regulatory supervision in various markets, as the technology provides greater visibility on the movement of funds.

SMART PROPERTY, SMART CONTRACTS, AND NEXT-GENERATION PLATFORMS

Advocates claim that the blockchain concept and the wave of innovation it has unleashed—commonly referred to as “next-generation platforms”—have nearly endless functions. [Colored Coins](#), for instance, enables the storage and transaction of “[smart property](#)” on top of the blockchain. Smart property is property whose ownership is controlled via the blockchain using “[smart contracts](#),” which are contracts enforced by computer algorithms that can automatically execute the stipulations of an agreement once predetermined conditions are activated. Examples of smart property could include stocks, bonds, houses, cars, boats, and commodities. By harnessing blockchain technology as both a ledger and trading instrument, the Colored Coins protocol functions as a distributed asset management platform, facilitating issuance across different asset categories by individuals as well as businesses. This could have a significant impact on the global economy as the technology permits property ownership to be transferred in a safe, quick, and transparent manner without an intermediary. Visionaries see many other exciting opportunities too, including linking telecommunications with blockchain technology. This could, for example, provide car-leasing companies the ability to automatically deactivate the digital keys needed to operate a leased vehicle if a loan payment is missed.

Entrepreneurs and developers are working diligently to realize the blockchain’s potential. For instance, [Ethereum](#)—an open-source development project that provides a platform for developers to create and publish next-generation distributed applications—uses blockchain technology to facilitate the trading of binding smart contracts that can act as a substitute to conventional business documents. The technology allows the contracts to be traced and used to confirm business deals without the need to turn to the legal system. In addition to a variety of contracts and agreements, the project’s website emphasizes that the platform can be used to “codify, decentralize, secure and trade just about anything: voting, domain names, financial exchanges, crowdfunding, company governance, intellectual property, and smart property.”⁴

BARRIERS TO WIDESPREAD ADOPTION

Many, however, remain skeptical. Critics maintain that there are numerous obstacles facing blockchain technology’s widespread adoption in the real economy, many forecasting an eventual breakdown. The enormous computational power and the associated high costs required to maintain the system would become increasingly difficult to overcome as it expanded. In the Bitcoin ecosystem alone, there are already hundreds of thousands of high-powered computers that have been specifically developed for mining activities. Bitcoin miners now have 13,000 times more combined calculating capacity than the world’s 500 most powerful supercomputers. It is estimated that the combined electrical consumption of these computers is enough to power approximately 135,000 American households. More striking still is that the Bitcoin system processes only about 100,000 transactions per day (Chart 4)—a small fraction of Visa’s 150 million. The computing power, energy, and carbon footprint required to process all the transactions of the global financial network using blockchain technology would be colossal. It is unclear whether today’s technology would be able to process even a fraction of that amount.

Other obstacles to widespread adoption include two central components of the blockchain’s functionality—an incentive system that motivates a dispersed workforce to validate and record transactions on the public ledger and a governance system that provides rules and structures for the platform. It remains unclear how these two systems would develop and function as blockchain technology evolves, and what would be the ramifications for the economic and operational efficiency of these blockchain models in the conventional economy. Furthermore, legal and regulatory hurdles will no doubt pose challenges too; legislative bodies, regulators, and law enforcement agencies around the world cite tax evasion, money laundering, and financing of illicit activities as concerns associated with the novel technology.⁵ Moreover, important

4) For more information on next-generation platforms please see “[Great Chain of Numbers](#).”

5) Please consult the University of Chicago Law School’s paper, “[Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms](#)” for more information on the barriers facing the expansion of the technology from a small niche area to the mainstream economy.

questions related to smart property and smart contracts would also need to be addressed. For instance, would they be accepted by the courts, and if so, how would they operate within the traditional legal system?

BETTER REGULATION AND ADVANCES IN TECHNOLOGY COULD HELP

While the aforementioned hurdles are valid concerns, advocates point out that technological advances and enhanced regulatory measures should be able to solve them. On the regulatory front, the case is often made that since the new technology provides a public record of every transaction that takes place on the system, the movement of funds and assets could theoretically be traced by law enforcement bureaus and regulators. With appropriate monitoring and investigation, it should ultimately prove difficult to conceal criminal activity, as each asset on the system would be identifiable by its unique transaction history. With regard to technological challenges, proponents argue that with the foundation established and continued advances in technology, it is only a matter of time before a viable, cost-effective, and efficient blockchain model is in place, given the significant expected benefits of widespread adoption.

Indeed, innovation is ongoing and a wide range of alternatives to Bitcoin's blockchain model are being developed. For instance, [Gridcoin](#), which utilizes blockchain technology to crowdsource scientific computing ventures, requires far less electricity and computing capacity to function. Additionally, [Ripple](#) and [Stellar](#), open-source global payments protocols that claim to facilitate the secure transfer of currencies in real time and at virtually no cost, completely eliminate mining and instead use other mechanisms, such as voting, to update their respective system's ledger. Several banks, including Germany's Fidor and U.S.-based CBW and Cross River Bank, have embraced the Ripple platform, illustrating the potential start of a gradual move towards cryptolegder technology in the mainstream economy. Moreover, Reuters recently reported that International Business Machines Corp (IBM) is considering leveraging blockchain technology to design a digital cash and payment system for several key fiat currencies. Reuters claims that IBM has met informally with various central banks, including the U.S. Federal Reserve, about the possibility of creating a blockchain-tied cash network, and that the tech giant plans to build the platform for the endeavor should central banks approve the idea. The proposed system, however, would be overseen by central banks and therefore would not be decentralized like Bitcoin.

STILL EARLY DAYS—LOOKING FOR MORE FUNCTIONALITY, BETTER PLATFORMS

The Bitcoin protocol and its underlying blockchain technology are currently in an evolutionary phase, comparable to when Internet protocols were still nascent. Like the PC and Internet in their early days, the cryptoprotocol ecosystem today should be viewed as a work in progress with immense potential. A broad range of developers have recognized the promise of the blockchain and have started developing applications that move away from a cryptocurrency-only network to ventures that have added functionality. Some developers are building directly on the Bitcoin blockchain, while others question whether it provides the most optimal platform for continued experimentation in the complex digital universe—and have created new protocols based upon its underlying principles. While no one is certain how or in which direction blockchain technology will evolve, it is clear that the Bitcoin protocol has unleashed a wave of financial innovation. Some of these new platforms may flourish, others may collapse. In fact, it is possible that the platform that can spearhead this technology into the mainstream economy has not yet been designed.

Finally, blockchain proponents argue that like the Internet in its beginning, the technology should not be over-regulated, as that would impede its advancement. Had the Internet been over-regulated during its early development, many of today's useful and far-reaching innovations would be non-existent. The same concept, advocates argue, is applicable to the blockchain. As both international and national regulators consider the potential implications of the blockchain for financial stability, supporters continue to urge recognition of the important distinction between the technology itself and the applications that operate on it.

CONCLUSION

It remains to be seen whether the innovative blockchain technology underpinning many of today's Internet-based currencies and digital projects will be adopted widely enough to become a disruptive force in the global economy. For this to happen, present-day blockchain technology would require technical modification and improvements to its design that address fundamental concerns, including incentive and governance procedures, as well as the enormous computational power required to maintain the system and the associated costs. However, if the mathematicians, entrepreneurs, programmers, and developers that support the blockchain are able to address these challenges—as well as potential problems that arise during the course of development—blockchain technology could very well revolutionize the financial landscape, making the "Internet of Finance" a reality.