DEPTH. FOCUS. SERVICE.

MERCATOR ADVISORY GROUP

UNDERSTANDING BITCOIN'S IMPLICATIONS FOR CREDIT UNIONS

A Mercator Advisory Group Research Brief Sponsored by CO-OP Financial Services

April 2015

Introduction

In 2014, Oxford Dictionaries online included for the first time the definition of the word "cryptocurrency":

"A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank"

This succinct definition captures three key facets of cryptocurrency, of which Bitcoin is the first and most widely used example. These are characteristics that separate cryptocurrencies from fiat currencies such as dollars or yen. The generation of fiat currency is strictly regulated by a central authority in charge of monetary policy, such as the Federal Reserve. A cryptocurrency such as Bitcoin, on the other hand, is essentially just a globally shared ledger book of accounts that keeps track of who has what. The generation of new Bitcoin is strictly governed by mathematical rules, and the total number of bitcoins in circulation will never exceed 21 million. And finally, this entire system functions independently of any central authority. Anyone can have a copy of the public ledger and enter into the complex mathematical puzzle-solving process that determines who gets to update it with the latest transactions every 10 minutes.

More on each of these aspects later. First some key terms needed to understand how Bitcoin works:

- A **Bitcoin public address** is analogous to a bank account number and is used to store bitcoins. But unlike a bank account, a Bitcoin address can be randomly generated and is not associated with a user's personally identifiable information (PII). (Note that capitalized "Bitcoin" is used to signify the concept or network, while lowercase "bitcoin" commonly refers to the currency or digital "coins."[i])

- **Private key** is like a personal identification number (PIN) and is a text string that is required in order to authorize any transaction of bitcoins from a Bitcoin public address.

- **Bitcoin wallet is** a collection of Bitcoin public addresses and the private keys associated with them.

- The **blockchain** is the ledger recording all Bitcoin transactions in blocks, which are formed roughly every 10 minutes.

- **A Bitcoin miner** is akin to a bookkeeper of sorts. A Bitcoin miner competes with other miners to solve a computational puzzle that authorizes him or her to update the blockchain with the latest transaction. For these efforts, the miner is rewarded with new bitcoins and possible transaction fees.

- **Proof-of-work problem** is a computational puzzle that Bitcoin miners must perform in order to add to the blockchain.

What Problem Does Bitcoin Solve?

Currencies have historically served three functions—as a store of value, a medium of exchange, and a unit of account. New currencies are invented every day, from Starbucks rewards to Amazon Coins. Most of these don't last very long. The fundamental innovation of Bitcoin is not the fact of its inception as a digital currency but the blockchain algorithm that makes its circulation possible, all without the need for a trusted central authority. The term "blockchain" denotes the public ledger that is a log of every single transaction made using Bitcoin since it was first proposed and executed by its pseudonymous founder (or group of founders), who goes by the name Satoshi Nakamoto. This ledger can be seen and held by anyone running a Bitcoin "client," the software necessary to generate the private key necessary for every Bitcoin user and for security. The ledger is updated approximately every 10 minutes when a new block is added by a bitcoin "miner" who succeeds in solving a computationally complex cryptographic "proof-of-work" problem. This new block, which contains a record of Bitcoin transactions that have been completed since the last block was sealed, is linked to the previous block once other miners in the network verify its legitimacy.

Since each block is "chained" to the preceding block and is sealed with immense computational work, it is nearly impossible to engineer variations in the blockchain once a block has been added and its associated transactions have been logged. This is an incredibly clever solution to the "double-spending" problem, a way to ensure that no one can send a store of digital value twice (the value is digital since the Bitcoin transactions are after all dealing with bits of data and not bars of gold or notes of fiat currency). Traditionally, the solution to the double-spending problem has been to appoint a central authority to ensure transaction fidelity. For instance, when someone sends money from one PayPal account to another, both parties trust PayPal to accurately debit and credit the two accounts. Bitcoin decentralizes the solution to this problem: Each transaction is checked against the public ledger before it can be added to the next block, to ensure that the person sending the bitcoins has not already spent them. The elimination of a central authority minimizes transaction costs although it does not negate them. It also makes Bitcoin resilient to systemic attacks and enables applications that utilize the blockchain in a variety of public proof applications.

To incentivize Bitcoin miners to play their crucial bookkeeping role, a predetermined set of new bitcoins gets unlocked and transferred to the possession of the successful miner with the addition of each new block. The size of this set of new bitcoins, initially 50, is continuously halved every 210,000 blocks, which ensures that the total number of bitcoins in circulation will never exceed 21 million. When this limit is reached, which is anticipated to occur in the year 2140, the Bitcoin architecture allows for transaction fees—currently optional—to play a larger role. Nevertheless, many Bitcoin wallet providers already pay a transaction fee to miners. Coinbase, for instance, reportedly pays a transaction fee of 0.0002 BTC (as of March 12, 2014, worth about 6 cents) to miners to ensure that its users' transactions are logged to the blockchain as soon as possible.[ii] There is concern that this transaction fee may increase in the future to compensate miners for the diminishing number of bitcoins released into circulation.[iii]

State of the Bitcoin Ecosystem: Key Metrics

Bitcoin is not the only cryptocurrency game in town. It is, however, the mostly widely known and enjoys the greatest market capitalization (see Figure 1). Bitcoin-enabled startups have also attracted tremendous interest and investment from venture capitalists. In 2014, the Bitcoin ecosystem attracted $238.9 million of funding, a 143% increase over the previous year.[iv] By contrast, venture capital investment as a whole grew by 61% in 2014 compared to the previous year.[v]

Figure 1: Market Capitalization of Top 10 Cryptocurrencies (as of December 2014)

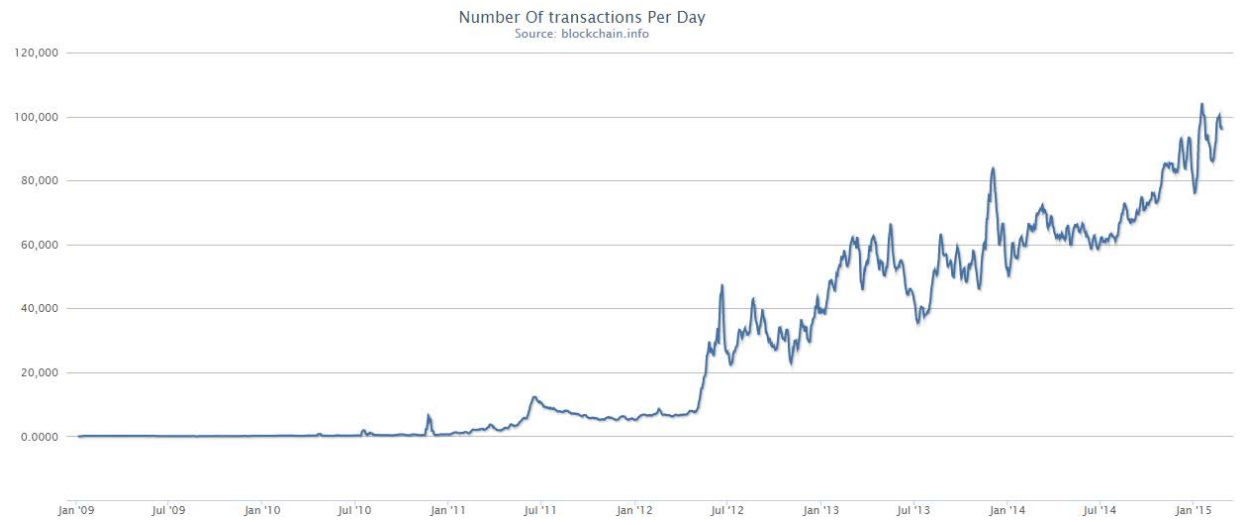
Rank	Name	Market Cap
1	Bitcoin	$ 4,132,670,815
2	Ripple	$ 706,795,764
3	Litecoin	$ 79,521,355
4	BitShares	$ 38,420,086
5	PayCoin	$ 35,959,731
6	MaidSafeCoin	$ 23,917,169
7	Nxt	$ 18,392,947
8	Stellar	$ 17,713,142
9	Dogecoin	$ 17,145,911
10	Peercoin	$ 11,573,821

Source: CoinDesk "State of Bitcoin 2015"

Bitcoin trading volume hit $23 billion in 2014, up 57% from the year before.[vi] The total number of merchant locations accepting Bitcoin rose to over 82,000 by the end of 2014, a 128% increase year over year.[vii] The number of Bitcoin wallets in use also rose by 149% over the same year, to 7.9 million.[viii]

Perhaps the most important metric for Bitcoin ecosystem is the number of transactions recorded per day. In January 2015 that number averaged around 100,000 (see Figure 2). In comparison, PayPal handles over 10 million transactions every day.[ix]

Figure 2: Number of Bitcoin Transactions per Day Is Growing



Source: Blockchain.info (https://blockchain.info/charts/n-transactions)

The other key statistic to note with regard to Bitcoin is the volatility of its price. Today the cost of a single bitcoin is around $260, a far cry from the close $1,000 plus valuations we saw briefly in late 2013. Bitcoin's volatility index calculation is estimated at around 4% today, far higher than most major fiat currencies, which range between 0.5% and 1.0%.[x]

Bitcoin's Value Proposition for Payments

Bitcoin evangelists will tell anyone who will listen that the days of credit and debit card networks are numbered. However, a closer examination of the applicability of Bitcoin for retail payments suggests that the payment system run by the likes of Visa, MasterCard, and American Express has some undeniable benefits, especially for consumers, which Bitcoin-backed retail payment services will find tough to mimic.

Mercator Advisory Group is of the opinion that Bitcoin is not likely to replace credit cards in retail payments for the foreseeable future. For the consumer, there are few discernible benefits to using Bitcoin for everyday transactions. For the merchant, lower fees may be attractive, but they doesn't compensate for the fact that a Bitcoin transaction takes approximately 10 minutes to get "confirmed" on the blockchain (whereas card transactions are authorized instantaneously, although their settlement takes longer). This makes accepting payments for purchase transactions via Bitcoin at the point of sale completely unfeasible for any sort of brick- and-mortar retail business that involves high turnover and nonnegligible transaction sizes.

Figure 3: Comparing Bitcoin vs. Card Networks for Retail Transactions

	Pros	Cons
Card Networks	High acceptance	Chargeback risk for merchants
	KYC compliance	Settlement lag
	Excellent consumer protection	Risk of data breach of personally identifiable information
	Immediate authorization	Processing fees
Bitcoin	Immediate settlement	Regulation unclear
	Low fees and irreversible	Hacking risk
	Increased security for personally identifiable information (PII)	Extreme volatility

Source: Mercator Advisory Group

The essential difference between the two systems in the context of retail payments is that card transactions are essentially "pull" transactions: The merchant is authorized to make a claim to the cardholder's bank or credit union, which authorizes the transaction and then releases the funds. From the merchant's point of view, this process is slow (it often takes 2 to 3 days for the funds to reach the merchant) and expensive (each credit card transaction comes with a 2–3% interchange fee to the merchant). Bitcoin, in contrast, operates entirely through "push" transactions: Once bitcoins are moved from one address to another, the transaction is irreversible (although it is possible to engineer third-party solutions that hold the funds in an escrow account). This is undeniably beneficial to merchants (assuming they have a way to hedge away all the foreign exchange risk), but, for the most important stakeholders in the ecosystem—consumers—the benefit is unclear (see Figure 3).

There is, however, another important category of consumer payments in which Bitcoin would have immediate relevance—international remittances. In 2012, residents in the United States sent $123.27 billion abroad.[xi] The World Bank estimates that the global average cost of a remittance (as a percentage of the transaction) was about 7.9%. Mercator Advisory Group's analysis of a Bitcoin-backed remittance service operating in the U.S.-Philippines corridor reveals that it is considerably cheaper—by over 1200 basis points—to send small dollar amounts (less than $50) through Bitcoin than through services provided by Western Union, Remitly, Xoom, and the like.[xii]

The makers of Ripple, another promising cryptocurrency platform similar to Bitcoin, are building infrastructure necessary for banks and credit unions to be able to offer real-time international payments at a fraction of the cost that correspondent banking arrangements currently involve.[xiii]

Bitcoin 2.0: Blockchain Applications Beyond Payments

The distributed public ledger known as the blockchain which underpins Bitcoin has all sorts of interesting applications that go beyond payments. Mercator Advisory Group has identified three that we see as having the greatest potential in the near term. These are digital asset trading, smart contracts, and identity management.

Digital asset trading refers to the use of Bitcoin for representing any sort of real asset such as a stock certificate or a land title. Since the entire transaction history of a single bitcoin can be traced from the point of its inception by analyzing the blockchain, it is possible to verify and transfer ownership of any asset whose value is represented in bitcoins. This opens up radical possibilities. The title to a house, for instance, could be represented in Bitcoin (assuming the supporting legal statues are in place) and transferred in exchange for equivalent bitcoins. This transaction would be as simple to complete as buying a cup of coffee with the Starbucks app.

Smart contracts refer to the creation of algorithms that have programmatic access to Bitcoin addresses created by interested parties who wish to engage in a contract. To clarify this idea, consider the following example: Let's say a person, Bob, approaches his bank for financing the purchase of a new car. Bob has poor credit history and would, under normal circumstances, fail to secure a loan. However, in a world with Bitcoin and interconnected devices, new possibilities emerge. Bob and his bank could enter into a smart contract stipulating that on a particular day of each month, if Bob's designated Bitcoin address did not forward the necessary payment to a Bitcoin address the bank set up to receive the payment, then the algorithm would begin to restrict Bob from accessing his car. This could mean that the Near Field Communication (NFC) "token" that Bob uses every day to unlock his car with his phone (this would be a world where physical keys are a thing of the past) would no longer work. The issuance of this token (or random sequence of characters) would be managed by the smart contract's algorithm. As one can imagine, the Bitcoin-distributed public ledger could revolutionize the whole business of credit issuance through innovative use of smart contracts.

Finally, **identity management** is another exciting potential area of application for blockchain technology. Currently, most of the vital documents we use in our lives—driver's license, passport, workplace ID—are paper-based and easy to lose, steal, or forge. Bitcoin's public key cryptography, where every user has both a public address and a private key, can be extremely effective tool to verify identity. A traveler passing through the immigration checkpoint at an airport, instead of being asked for a passport, could be asked to use his or her private key to encrypt a given message to create what is known as a "digital signature." Using that person's publicly known address, which the government would keep track of and associate with the person's social security number, it then becomes possible to decrypt the message and verify that the private key and its associated signature are indeed genuine and associated with a known public address. This would be a foolproof method of identity verification as long as each person was aware of how to keep the private key secure.

Conclusion: Implications for Credit Unions

Assuming the volatility of Bitcoin drops considerably to what is considered normal for currencies, and that security concerns around how best to secure private keys are resolved, we could see the proliferation of a host of new financial services backed by Bitcoin, many of which are directly associated with the core businesses of credit unions today. Since Bitcoin addresses can be generated at will, and each can function as a store of bitcoin currency, the cost of acquiring new account holders can be expected to decline considerably. As discussed in this paper, Bitcoin's value as an infrastructure to support payments could be especially relevant to international remittance transfers. Credit unions whose clientele includes a large number of migrant workers may want to consider partnerships with regulated Bitcoin-backed exchanges such as CoinX or Coinbase to explore the possibility of offering a competitive international remittance product to their customers.

It's much more difficult to see Bitcoin's value in everyday retail transactions, where consumers much prefer the ubiquity and protections offered by a card network scheme led by well-known and established organizations like Visa, MasterCard, and American Express, which fund the protections and consumer incentives via interchange.

As for adding Bitcoin functionality to a credit union's wallet, it is unclear whether the costs involved in offering such functionality in a manner that is secure (security being a huge ongoing concern) are justified by the benefits. The primary "use-case," if you can call it that, for buying and holding bitcoins today is purely speculation. This particular use-case is limited to a very small number of cryptocurrency enthusiasts and is unlikely to find much traction among the broader mainstream of CU account holders.

There are undeniably many thousands of very smart people worldwide building all sorts of interesting applications that use Bitcoin technology on the back end. These projects range from digital asset exchanges to smart contracts, but they are all still very much in their infancy and their utility to credit unions is yet to be determined. Nevertheless, while watching and waiting to see what benefits they will offer, it would be highly worthwhile for credit unions to keep abreast of these Bitcoin 2.0 innovations that go beyond payments. At Mercator Advisory Group, cryptocurrency applications are a continuing part of our Emerging Technologies Advisory Service research agenda, and we continue to engage our clients on this front to keep their leadership informed.

At its core, Bitcoin represents a profoundly simple innovation in maintaining an indisputable history of its transactions as represented by the blockchain. This cryptographically sealed history cannot be altered and will be very difficult to destroy as long as such a thing as the Internet exists. This will have profound implications for the financial services industry, and beyond. Predicting what exactly these implications will be, however, is a bit like trying to grasp the significance of the Internet would have been in 1995—these are early days still.

Endnotes

[i] https://bitcoin.org/en/vocabulary

[ii] https://support.coinbase.com/customer/portal/articles/815435-does-coinbase-pay-bitcoin-miner-fees

[iii] http://www.coindesk.com/new-study-low-bitcoin-transaction-fees-unsustainable/

[iv] http://www.coindesk.com/research/state-of-bitcoin-2015/

[v] http://venturebeat.com/2015/01/17/vcs-invested-48-3b-in-2014-highest-level-since-2000/

[vi] http://www.coindesk.com/research/state-of-bitcoin-2015/

[vii] Ibid.

[viii] Ibid.

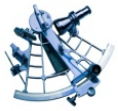
[ix] https://www.paypal-media.com/about

[x] https://btcvol.info/

[xi] World Bank Bilateral Remittance Matrix 2012: http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTDECPROSPECTS/0,,contentMDK:22759429~pagePK:64165401~piPK:64165026~theSitePK:476883,00.html

[xii] See Mercator Advisory Group research report "*A SWIFT Disruption? Bitcoin and Peer-to-Peer Models Challenge the Remittance Business*": http://www.mercatoradvisorygroup.com/Reports/A-SWIFT-Disruption_-Bitcoin-and-Peer-to-Peer-Models-Challenge-the-Remittance-Business/

[xiii] https://ripple.com/integrate/executive-summary-for-financial-institutions/



About Mercator Advisory Group

Mercator Advisory Group is the leading independent research and advisory services firm exclusively focused on the payments and banking industries. We deliver pragmatic and timely research and advice designed to help our clients uncover the most lucrative opportunities to maximize revenue growth and contain costs. Our clients range from the world's largest payment issuers, acquirers, processors, merchants and associations to leading technology providers and investors. Services include *Banking Channels, Credit, Commercial and Enterprise Payments, Debit, Emerging Technologies, International, and Prepaid practices*, which provide research documents and advice; *CustomerMonitor Survey Series*, which report and analyze primary data collected in our biannual consumer surveys; and *Consulting Services*, which enable clients to gain actionable insights, implement more effective strategies, and accelerate go-to-market plans; offerings include tailored project-based expertise, customized primary research, go-to-market collateral, market sizing, competitive intelligence, and payments industry training. Mercator Advisory Group is also the publisher of the online payments and banking news and information portal PaymentsJournal.com. Visit www.mercatoradvisorygroup.com.

About CO-OP Financial Services

Based in Rancho Cucamonga, Calif., and founded in 1981, CO-OP Financial Services is the nation's largest credit union service organization in terms of number of credit unions and members served. The company helps credit unions compete by providing products and services that make it more convenient for credit union members to do business with their credit unions. With a motto of "Be There. Be More," CO-OP's products and services fall into three business lines, including "Locations," (ATM, shared branching and call center services); "Card Payments" (debit and credit processing) and "Mobile/Virtual" (mobile, online, check imaging, bill pay services). To learn more visit www.co-opfs.org.