DAVID WENDELL ASSOCIATES, INC.
INVESTMENT COUNSEL

P.O. Box 21980
325 Corporate Drive
Portsmouth, N.H. 03802
(603) 427-0200
www.davidwendell.com

First Quarter, 2014

A Bit about Bitcoin

"We have proposed a system for electronic transactions without relying on trust."
Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008

In recent weeks, Bitcoin has been the topic of many conversations both on and off Wall Street. One of the founders of the early internet company Netscape announced investing more than $50 million in Bitcoin-related businesses and plans to invest hundreds of millions more in the coming years. Even here in New Hampshire, the leading article in a Sunday edition of a local newspaper focused on the digital currency. But the disappearance and possible theft of millions of dollars in Bitcoins and the bankruptcy of several of the exchanges where it was traded is good reason for users, merchants, investors and traders all to pause.

The concept for Bitcoin was first proposed in a paper posted to a cryptography website five years ago. Cryptography in the digital world is the study of secure communications in which a trusted third party vouches for the other two parties. The paper's author was Satoshi Nakamoto but none of the site's members had ever heard of him. His online profile stated he lived in Japan but his email address was from a free service in Germany. Nakamoto emailed the site sporadically and then stopped completely in 2011.

As Bitcoin developed and gained more enthusiasts, the mystery surrounding his identity deepened. Some assumed the name was a pseudonym, noting that "Satoshi" means "intelligent, clear thinking, quick witted or wise" in Japanese. Others thought it was derived from the brand names SAmsung, TOSHIba, NAKAmichi and MOTOrola. Still others speculated it was really a group of Google employees working on a secret project. Last month, a national magazine announced it had identified Bitcoin's creator but he denied involvement, as have others sharing the same name.

Under the Bitcoin framework, users run special software that forms a network on the internet. Every time a purchase is made using Bitcoins, the software broadcasts it to the network where it is added to a permanent chain of transactions. Known as the "block chain," it acts as a kind of ledger, tracking old transactions and validating new ones. In cryptographic terms, the block chain is the "trusted third party." This is in contrast to a currency backed by a government.

- - - - -

The information provided herein represents the options of David Wendell Associates and is not intended to be a forecast of future events, a guarantee of future results, nor investment advice.

The block chain structure addresses the primary problem of digital currencies -- fraud. A digital dollar is basically a piece of information that can be copied, cut and pasted just as easily as any piece of text. Theoretically, anyone can "spend" a digital dollar as many times as they wish and this is known as the "double-spending" problem. With the Bitcoin ledger maintaining all transactions in a chain that is open to scrutiny and verification by all Bitcoin users, the double-spending problem is effectively eliminated.

In the early days, there was no market for Bitcoins, just enthusiasts of cryptography sending them back and forth to each other. The first real world transaction took place in early 2010 when two pizzas were purchased for 10,000 Bitcoins. Then the price slowly started rising and by mid-2011, it had reached $31 but then plummeted to $2 by year's end. Last year, the price of a Bitcoin began to increase 5-10% each day as more and more people wanted in on the action. By October, a Bitcoin was valued at $200 and by the end of November, it was more than $1,100. Since then, Bitcoins seem to have settled at about $600 each. There are two ways of obtaining Bitcoins: through a trading exchange or through "mining" them.

Bitcoins can be traded for dollars and other government-backed currencies on Bitcoin exchanges, such as the now-bankrupt Mt. Gox, or they can be traded for goods with online merchants who accept Bitcoins, such as Overstock.com. Also, two Bitcoin ATM machines have been installed in Massachusetts and the one-way cash-to-Bitcoin transaction takes about 30 seconds. A regular ATM has many more functions. For people who do not have digital wallets already installed on their devices, the ATM machine will issue a paper wallet with two Quick Response ("QR") codes -- similar to bar codes -- used to import the Bitcoin to a digital wallet. However, Massachusetts state regulators recently warned consumers to proceed with caution, stating "if you can't afford to lose the money you have, you should not buy Bitcoins."

The process used to create Bitcoins is called "mining," where users try to solve a complex mathematical puzzle built into the software. The puzzle is related to the number of Bitcoins already in existence and the reward for being the first to solve the increasingly difficult puzzle is 25 Bitcoins, which are added to the ledger and stored on the mining computer hardware. Currently, about 25 Bitcoins are being mined every 10 minutes. Based on the software's algorithm, there are 21 million potential Bitcoins and about half are already in circulation. The algorithm ensures that the supply of Bitcoins expands gradually, in contrast to the perceived effects of quantitative easing programs by central banks around the world.

In the early days, mining for Bitcoins could be done easily using laptop and desktop computers. But the puzzle has become complex enough to strain the standard semiconductor chips found in personal computers.

A recent *Bloomberg BusinessWeek* article showed a young miner in his living room, surrounded only by cables and computers strewn about the floor. Despite the Spartan setting, he spent more than $20,000 on hardware and racks up over $400 a month in electric bills. He constantly has to monitor the temperature of the room as the chips work better when they are hot but if they get too hot, they will overheat and malfunction. He estimates that his two fastest computers will each earn him about $150,000 in Bitcoins this year -- "It takes up a lot of time, but I have no kids. I have no life. I have a cat."

The same article also described some new companies that are trying to manufacture chips specifically designed to solve the Bitcoin algorithm. One such start-up, HashFast, bills itself as "The World's Fastest Bitcoin Miner" and according to the company's founder, "It would take 70,000 of Intel's fastest chips to match one of ours." So far, the company has missed a string of its own production deadlines but does plan to ship its first product soon.

Another start-up, MegaBitPower, claims it is "North America's largest Bitcoin Miner." The founder of this company states he generates 100 to 300 Bitcoins each day using his own specialized chips. He plans on selling his equipment to other enthusiasts -- charging up to $1 million for gear than can mine $150,000 Bitcoins each day -- but has yet to find takers. He plans on keeping the Bitcoins he mines, betting they will only go up in value: "I am riding this Bitcoin wave."

Despite the hoopla, digital currencies are not new. In the early days of internet shopping, many thought consumers would be reluctant to enter their credit card numbers into computers and send them off into cyberspace. A number of companies developed methods to facilitate internet transactions but all relied on real world banks within the established financial system to process the transactions. Two of the original electronic cash companies were CyberCash and DigiCash, both founded in the early 1990s and both highfliers during the internet boom.

CyberCash provided an electronic software wallet to consumers that was downloaded onto computers to safeguard credit card numbers. When the consumer found a merchant that accepted CyberCash, the merchant's CyberCash software would obtain an encrypted credit card number from the wallet and the transaction would proceed.

DigiCash ran a trial eCash program with the Mark Twain Bank of St. Louis and its technology was unique in that it allowed for anonymous transactions over the internet. In fact, DigiCash's founder, David Chaum, developed a number of sophisticated cryptographic protocols and some observers today believe that he may be the real "Satoshi Nakamoto" due to his background and expertise in cryptography.

Despite the belief that consumers would be paranoid about internet shopping, they actually became increasingly comfortable and internet shopping flourished. At the same time, MasterCard and Visa engaged in major marketing efforts to leverage their name recognition and set low limits for liability in the event of credit card fraud. By the early 2000s, both CyberCash and DigiCash had filed for bankruptcy, the credit card companies were firmly established on the internet and digital currencies basically had entered the realm of solutions searching for problems.

The past few weeks have seen a couple of Bitcoin exchanges filing for bankruptcy, including Mt. Gox, based in Japan, and FlexCoin, based in Canada. Mt. Gox had become the major Bitcoin exchange and it announced that some $500 million and possibly more in Bitcoins that had been stored on the site's hardware were stolen, representing about 750,000 Bitcoins owned by customers and 100,000 owned by the company.

Mt. Gox originally was formed as an online platform for a trading card game called *Magic: The Gathering*, similar to other fantasy role-playing games such as *Dungeons and Dragons*. The name "Mt. Gox" is actually an acronym for "Magic: The Gathering Online Exchange." In 2010, the platform's creator switched the site over to handling Bitcoin-to-U.S. dollar trades and it became hugely popular. In 2011, he sold it to Tokyo-based Mark Karpeles who then steered Mt. Gox to become one of the most trusted entities in the Bitcoin world.

The story behind the Mt. Gox bankruptcy is still developing but at this point it appears likely that lax security and inadequate software stemming from its gaming origins played a prominent role. The company just announced it had found 200,000 Bitcoins worth some $114 million that were held in an "old-format wallet" used before mid-2011. FlexCoin announced its bankruptcy after hackers reportedly used a trick once popular against ATMs -- withdrawing cash faster than FlexCoin could rectify its accounts. The hackers figured out how to double-dip into the exchange's available Bitcoin balances.

With concerns mounting over Bitcoin cyber-thefts, some companies are addressing the problem the old fashioned way: real world physical vaults. One start-up called Xapo just raised $20 million in venture funding to construct a network of underground vaults that will be placed in mountainous regions around the world. The secret vaults deep in the earth will store Bitcoins on computer hard drives, becoming the Fort Knox of cyber currencies. "Trust in the participants, trust in the technology, trust in the ecosystem as a whole -- this is a really important block for the Bitcoin ecosystem," according to one venture capitalist backing the company. A far cry from what Nakamoto originally envisioned!

Ironically, a number of observers think that what may save Bitcoin, and the eight other crypto-currencies currently in existence, is government regulation -- the bane of most enthusiasts. The Internal Revenue Service just ruled that it will treat Bitcoin as property subject to capital gains taxes and extensive record-keeping rules and not as currency. Additional regulations should further clarify what crypto-currencies are and are not.

As the price of Bitcoin soared past $1,100, some on Wall Street began asserting that Bitcoin is in fact an asset class. This would mean that Bitcoins would have a place in investors' portfolios along with stocks, bonds and money market funds. We prefer to stick to our discipline of investing in high-quality, growing companies with experienced management teams and established track records. In other words,

"Whew! There will be no Bitcoin for you in your portfolio."

William H.L. Mitchell
Karen Wendell