Bitcoin: a first assessment

FX and Rates | Global
05 December 2013

Bank of America Merrill Lynch

David Woo +1 646 855 5442
FX and Rates Strategist
MLPF&S
david.woo@baml.com

Ian Gordon +1 646 855 8749
FX Strategist
MLPF&S
ian.gordon@baml.com

Vadim Iaralov +1 646 855 8732
FX Strategist
MLPF&S
vadim.iaralov@baml.com

Tamper-proof, limited supply and divisibility

We believe Bitcoin can become a major means of payment for e-commerce and may emerge as a serious competitor to traditional money transfer providers. As a medium of exchange, Bitcoin has clear potential for growth, in our view.

Store of wealth for the underground economy?

It has been reported that Bitcoin may help users avoid high taxes, capital controls, and confiscation. The correlation between CNY's share of volume of all Bitcoin exchanges and price of Bitcoin is high and rising (Chart 1). That said, the fact that all Bitcoin transactions are publically available and that every Bitcoin has a unique transaction history that cannot be altered may ultimately limit its use in the black market/underworld.

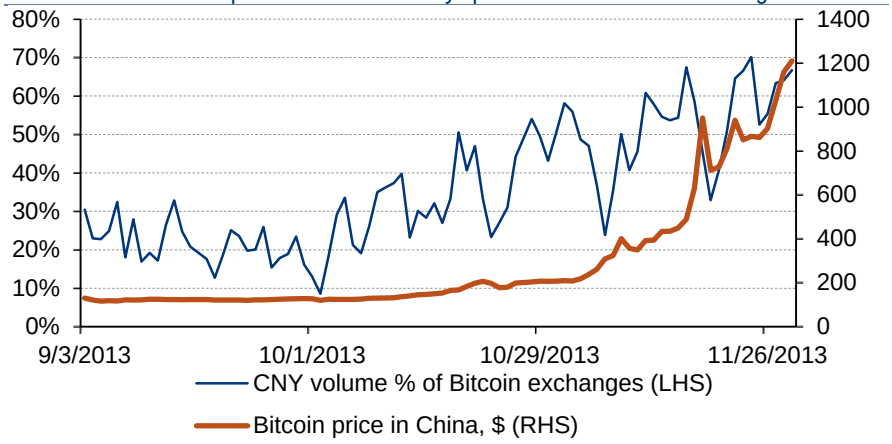
Volatility

Bitcoin's role as a store of value can compromise its viability as a medium of exchange. Its high volatility, a result of speculative activities, is hindering its general acceptance as a means of payments for on-line commerce.

Fair value?

Is Bitcoin a bubble? Assuming Bitcoin becomes (1) a major player in both e-commerce and money transfer and (2) a significant store of value with a reputation close to silver, our fair value analysis implies a ***maximum market capitalization of Bitcoin of $15bn (1BTC = 1300 USD)***. This suggests that the 100 fold increase in Bitcoin prices this year is at risk of running ahead of its fundamentals.

Chart 1: Recent Bitcoin price action is driven by speculation on Chinese exchanges



Source: BofA Merrill Lynch Global Research

Table of Contents

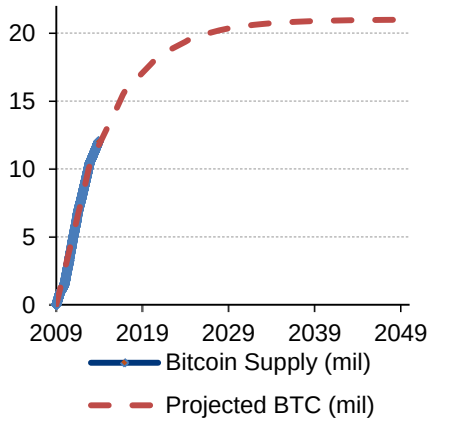
Refer to important disclosures on page 13 to 14. Link to Definitions on page 12.

Vadim Iaralov +1 646 855 8732

What is Bitcoin?

Bitcoin is a digital currency designed by Satoshi Nakamoto, a pseudonym, in January 2009. Bitcoin allows users to send payments within a decentralized, peer-to-peer network, and is unique in that it does not require a central clearing house or financial institution clearing transactions. Users must have an internet connection and Bitcoin software to make payments to another public account/address.

Chart 2: Bitcoin supply to taper to 21m by 2140



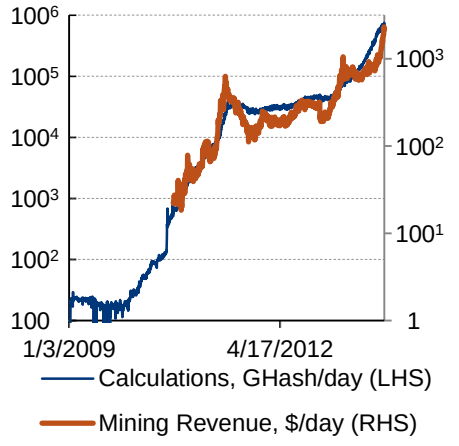
Source: BofA Merrill Lynch Global Research

Satoshi is the smallest unit of Bitcoin; 1 Bitcoin contains 100 million Satoshi. By design, the supply of Bitcoins cannot exceed 21 million Bitcoins (2,100 trillion Satoshi). The total amount of Bitcoin in circulation will increase predictably, based on its underlying code, until reaching the cap in 2140. The current supply is 12 million Bitcoins or 57% of the eventual total (Chart 2).

A **public history of all transactions** is continuously updated and verified by "miners" who gather batches of new transactions into blocks and attach these blocks to the end of the "Blockchain." This public history forms a ledger of transactions where every single Satoshi is tracked from its first owner to the present owner. Having the full history publicly available guarantees that a buyer actually owns the number of Bitcoins he or she wants to spend, preventing fraud.

Bitcoin supply is increased with every new block of transactions added to the public history (i.e. Blockchain). The verification of new transactions by miners is relatively easy and many transactions can be easily compressed in a single block. However, there is a computational task for each block of a high degree of difficulty designed to constrain the increase in the money supply, no matter how slow or fast the overall mining network is. If no external transactions are outstanding, a block with a single transaction to pay the miner would be produced. Indeed, the first several thousand blocks simply paid the miner and contained no other transactions (presently blocks contain a record of hundreds of transactions). This way the initial seed currency was distributed to miners who bore the speculative risk in the Bitcoin's success.

Chart 3: Mining industry has grown exponentially



Source: BofA Merrill Lynch Global Research

As a rough analogy, suppose competing journalists (**miners**) are asked to document the national news on each given day for the National Archives[1]. The journalist is asked to write down the events (**transactions**) in a book (**block**) and the Archive will eventually buy one such book for a fixed fee. To determine which of the books the Archive will buy the archive has an additional requirement for journalists that the book contains the fingerprints of 10 people whose birthday was on that particular day. Note that the list of people isn't related to the national news (**transactions**) but is simply meant to control the supply of books coming out per day. As more journalists collaborate to find people, the Archive increases the number of fingerprints required.

Exchanges allow the conversion between real-world fiat currencies and Bitcoin (Chart 1). The participation in exchanges requires consumers to take on credit risk by transferring Bitcoins from a personal account to a third-party's account, which is similar to entrusting real-life cash to depository institutions. However, unlike banks, Bitcoin third-party accounts are not regulated nor do they provide FDIC protection. While personal accounts are easy to secure, start-up exchanges in overseas jurisdictions with online digital wallets are often targeted by hackers. Exchanges also have some risk of the operator absconding with the money

[1] Mathematics plays the role of the Archive as there is no central authority.

before the currency conversion is completed. Major exchanges ordered by volume are BTC China (CNY), OkCoin (CNY), Mt.Gox (USD, EUR, GBP, JPY, AUD), FXBTC (CNY), Bitstamp (USD), Bter (CNY), BTC-E (USD), BTCTrade (CNY), VirtEx (CAD).

Chart 4: Tech advances favor computational prowess

Source: BofA Merrill Lynch Global Research

Bitcoin as a medium of exchange, distinct from speculative transactions on exchanges, initially gained popularity with companies involved within the Bitcoin ecosystem. For example, miners can purchase specialized chips with Bitcoins. To facilitate transactions, payment processors such as Bitpay provide software to merchants, and absorb FX volatility risk by guaranteeing exchange rates and sending daily bank payments. Since April 2013 significant investment was made into start-ups that develop and promote Bitcoin as a means of exchange for merchants (as opposed to speculation investment on the exchange). For example, CoinLab has received seed money to incubate other Bitcoin start-ups like mining companies and exchanges. The most notable company to accept Bitcoins may be Baidu, a major Chinese portal, which began accepting Bitcoin for its online security services in October 2013.

The rapid rise in BTC prices (292% a year) has generated a comparable exponential growth in **mining revenue**, which in turn has attracted **large capital investment**. Indeed, the number of computations has grown 521% a year (Chart 3), requiring expensive, heavy-duty Bitcoin-mining chips. The competition for revenues has taken away the low-hanging fruit and each dollar mined is now hundred times “deeper” (Chart 4). Electricity costs are also going up as miners use more computers. We describe the miner’s challenge and the mining industry in the Appendix.

Ian Gordon +1 646 855 8749

A cost-benefit analysis

Money/currencies are generally thought to have three distinct roles: as a unit of account, medium of exchange, and store of value. To the extent that Bitcoin offers users many benefits and efficiencies as a medium of exchange, this means it possesses some fundamental value that may increase over time as it gains wider use. However, as a unit of account and store of a value, it has considerable shortcomings which we believe will ultimately hinder it from ascending to international currency status. In this section we will review Bitcoin’s advantages and disadvantages in more detail.

Advantages

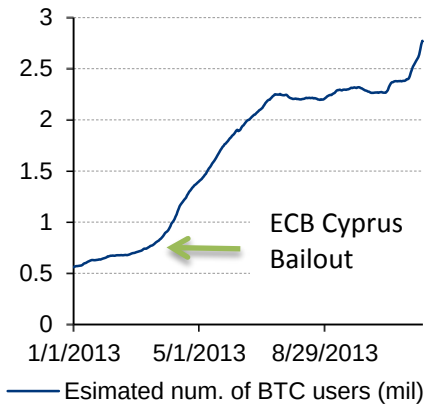
As a medium of exchange, Bitcoin is attractive as it offers low transaction costs. It does so by eliminating the need for a central clearing house or financial institution to act as a third party to financial transactions. Using a decentralized, peer-to-peer network, transactions are verified independently by network users (i.e., miners) who are rewarded for their work with newly minted Bitcoins. In addition, it provides an alternative payment method to users who may not have access to credit or debit cards, or, other forms of electronic payments.

Bitcoin offers an attractive alternative to cash in terms of security, transparency of transactions, and counterfeiting. Bitcoins reside in an encrypted format on their owner’s computer, making it difficult, though not impossible, for hackers to access and steal electronically. Physical Bitcoin theft is also possible, but it seems no easier to carry out on a large scale than for cash.

In addition, given their digital format, Bitcoins are much easier to carry than cash, which could be a particular benefit in economies where large scale transactions are conducted in cash. Bitcoin also offers the benefit of being easier to track than cash given that each coin contains an electronic record of each transaction that coin has gone through since it was created. Not only is each transaction recorded on each Bitcoin, but all transactions are recorded in an online public ledger, offering a level of transparency that is not available with cash. Such transparency offers regulators means to track potentially illicit activity. Lastly, the digital format with automatic verification also makes it impossible to counterfeit[2].

There is a finite supply of Bitcoins. The design of Bitcoin seeks to mimic the supply of gold in that the system will create a finite supply of the currency, which its proponents see as a way to protect its value from profligate governments or central banks. The system is designed such that the supply of Bitcoins will increase over time until it reaches a total supply of 21 million. In order to achieve this target, the incremental supply of new Bitcoins will decrease geometrically by 50% every four years.

Chart 5: BTC user base has grown 5- fold YTD



Source: BofA Merrill Lynch Global Research

Bitcoin's relative anonymity is advantageous to citizens of crisis countries. It has been reported that some believe Bitcoin can be used by those seeking to avoid evade high taxes, capital controls, and confiscation. For example, there was a sharp increase in Bitcoin interest on March 16 when Cypriot authorities, as part of their European assistance package, were prepared to implement a private sector haircut of deposits (Chart 5). Additionally, China has also seen a sharp increase in Bitcoin activity and now accounts for a majority of transactions when broken down by currency, likely reflecting the currency's value as an outlet for those wanting to avoid capital controls or potential confiscation (Chart 1).

"Winner Takes All" market ensures that increasing acceptance and popularity of Bitcoin increases likelihood of success. As Bitcoin becomes more popular, competitors will face higher barriers to entry, making it less likely they will be successful in supplanting Bitcoin's market share. Several other digital currencies with similar features to Bitcoin have been introduced with limited success. However, we believe the structure of the digital currency market is one of "winner takes all" whereby as Bitcoin becomes more popular and is easy to use, consumers will have much less incentive to experiment with an alternative currency with similar features.

Bitcoin offers large benefits (from an asset allocation perspective) given its negative correlation with risk sensitive assets, much like gold. For example, following the October FOMC meeting in which the market interpreted the statement as suggesting a less accommodative stance of policy than was anticipated, gold fell as much as 1% in the aftermath while Bitcoin fell 3%.

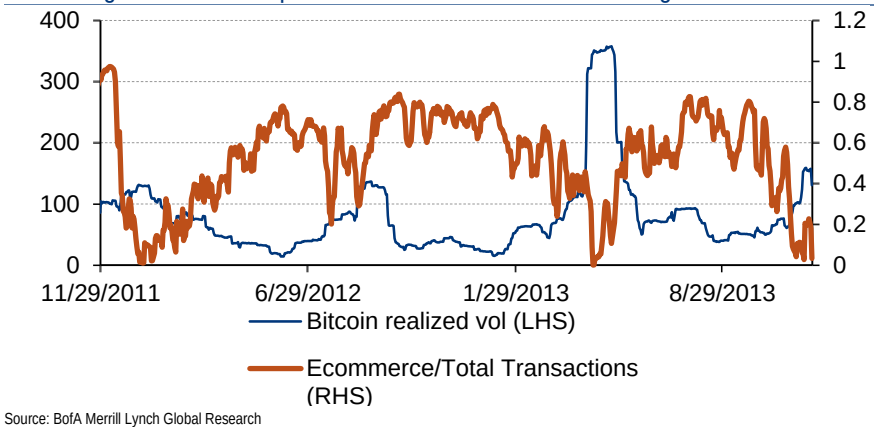
Disadvantages

Bitcoin's role as a store of value is seriously compromised by its elevated price volatility. The dollar price of Bitcoin has moved 10% on a daily basis since its inception including days when the price moved 190% from that day's highs to lows. It can be argued that these swings reflect shifts in estimates about the fundamental value of Bitcoin as more people become aware of it, or, use it. For example, the Bitcoin's dollar price increased 50% to $785 following a Senate

[2] An attacker with 51% of the network may attempt double-spending, similar to passing a bounced check but cannot inflate fake supply as the initial recipient won't be able to tender it. The vast size of the mining industry's computing power makes 51%-attack unprofitable relative to receiving revenue from honest mining.

Hearing on November 18th after which a couple regulators took a more positive stance towards the use of Bitcoin as another form of payment.[3] This is consistent with indications from European officials on Bitcoin. However, it is more likely a function of the highly speculative nature of the market which produces such unstable returns amidst very low circulation and poor liquidity as investors are enticed by the extreme return opportunities. High volatility also undermines Bitcoin's role as a medium of exchange as large retailers are much less likely to accept it as a form of payment with prices so volatile (Chart 6). Stores accepting it now are effectively internalizing the costs of this volatility and not passing it onto consumers, but we would not expect such likely unprofitable practices to last.

Chart 6: High Bitcoin vol compromises its role as a medium of exchange



Source: BofA Merrill Lynch Global Research

Regulators could try to impose controls that would increase the transaction costs for using Bitcoin despite its efficiency and the transparency relative to cash. Firstly, the government is unlikely to want to promote a new currency that could be viewed as one that could help facilitate "black market" activities, or, tax evasion. As a result, regulators are currently thinking about how Bitcoin will fit into the broader payment and tax system, and what makes sense in terms of regulation. The bottom line is any new regulation will raise Bitcoin's transaction costs, offsetting and/or eliminating one its main benefits. In addition, the ease with which Bitcoin can be used internationally increases the need for international regulatory coordination. While coordination raises the risk of an uneven regulatory landscape for Bitcoin, stringent regulation by a few large countries/regions would significantly increase the costs of using Bitcoin, thus limiting its usefulness as a medium of exchange.

The quality of Bitcoin exchange security, where consumers exchange dollars for Bitcoins (and vice versa) is suspect. For Bitcoin users not able to mine their own Bitcoins, their only alternative is to exchange their local currency for Bitcoins at an exchange. Aside from the FX risks these customers take, a large number of Bitcoin exchanges have been hacked with large amounts of customer Bitcoins stolen. In one reported case Bitcoinica, an exchange, lost 18,547 Bitcoins from its deposits after its systems were hacked. More recently, a European exchange called BIPS lost 1,295 Bitcoins (or $990,000) following a security breach.[4] As the vast majority of potential Bitcoin users cannot mine their own Bitcoins, exchanges will be critical for linking local currencies with Bitcoin. Without deposit (FDIC) or investment (SIPC) protection, Bitcoin users/investors have little recourse to retrieve stolen funds so in addition to investment risk they are also carrying credit risk.

[3] Regulators See Value in Bitcoin, and Investors Hasten to Agree (http://dealbook.nytimes.com/2013/11/18/regulators-see-value-in-bitcoin-and-investors-hasten-to-agree/?_r=0)
[4] http://siliconangle.com/blog/2013/11/26/bips-bitcoin-exchange-cleaned-out-in-990k-virtual-heist/

Seigniorage[5] is currently accruing to the "miners" of Bitcoins who have the fastest CPUs. Over time this will undercut seigniorage as a source of revenue for the government as they do not control the creation of Bitcoins. This means the government will have an incentive to crack down on Bitcoin if it becomes too big.

A 50 minute wait before payment receipt confirmation is received will prohibit wider use. Fifty minutes is the time needed for enough additional blocks to be added to the chain to protect against double spending. This is less of an issue for two parties that know each other because they trust the other will not double spend, but when dealing with an anonymous counterparty this creates a high level of unhedgeable risk. As a result, in the absence of a central counterparty verifying transaction/clearing Bitcoin is likely to remain illiquid, and will prevent it from becoming a significant international currency.

Bitcoin's use as an international currency will likely be hindered by the fact that it is not a legal tender. Unlike fiat money, nobody is under any obligation to accept Bitcoins as a mean of payment. Therefore, its value is only as good as the perception of its worth by its users. Without a backstop buyer, Bitcoin could disappear very quickly should perceptions of its usefulness decline. Repeated bouts of volatility and further cyber-attacks which put consumer and investor money in jeopardy will certainly inform this perception even as Bitcoin does offer many benefits. Some aspects of the characteristics of Bitcoins (e.g., it is not centrally cleared and there is a confirmation delay) makes us doubtful about its potential in the OTC market (where most FX trading turnover is executed), even though we cannot rule out that a non-deliverable forward market could emerge.

David Woo +1 646 855 5442

How to assess Bitcoin's fair value?

The value of Bitcoin has risen 100 times over the past year, raising the question of whether it is a bubble. To answer this question, we need to be able to assess its intrinsic value. We don't offer a forecast for Bitcoin, but below are our preliminary thoughts on how to approach the fair value question. Bitcoin's is both a medium of exchange as well as a store of value. In our view, it is easier to think about fair value by treating these two purposes separately.

Value as a medium of exchange

As we have argued already, Bitcoin has some attractive attributes as a medium of exchange, especially for e-commerce. What could be the fair value of Bitcoin if it were to become a dominant medium of exchange for e-commerce that accounts for, let's say, 10% of all the payments for B2C transactions? Let's do the following exercise:

- US personal consumption expenditures totaled $11trn in 2012
- Household checking deposits and cash totaled $0.7trn in 2012
- Dividing the former by the latter, we get 0.07 (which we will refer to as velocity from now on)
- Velocity has been rising since 2008, likely reflecting cash hoarding behavior that is likely temporary. To smooth it, we take an average of the velocity of the past ten years to arrive at 0.04 -- we assume US households are holding 4 cents in their cash/near cash balances for every $1 spent over the course of the year

[5] Seigniorage is the revenue earned by the government from issuing money. http://www.bankofcanada.ca/wp-content/uploads/2010/11/seigniorage.pdf

- In 2012, total B2C e-commerce sales in the US totaled $224bn
- If we were to assume that the velocity for on-line sales is the same as the velocity for all US household spending, then households would want to set aside $10bn for their on-line shopping
- Given the assumption that Bitcoin will grow to account for the payment of 10% of all on-line shopping, this would suggest that US households would want to have a balance of $1bn worth of Bitcoins
- What about for the whole world? US GDP is about 20% of World GDP. If we were to assume the same degrees of penetration of e-commerce for the rest of the world and that spending by households outside the US has the same velocity, we get to **$5bn worth of Bitcoins** for the total desired cash/non-cash balance of global on-line shopping.

The above is a very rough calculation and we have made a lot of big assumptions. Moreover, B2C is only one dimension of total e-commerce and we cannot rule out that Bitcoin can become a dominant medium of exchange for B2B transactions. Nevertheless, the exercise shows that if Bitcoins remains only as a medium of exchange, there appears to be a clear upside limit for its value.

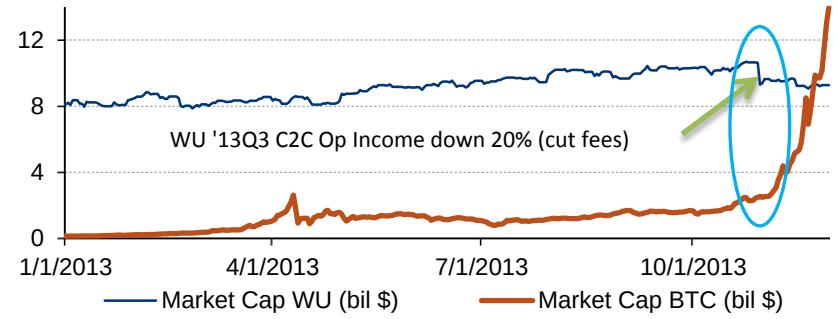
It has been argued that Bitcoin may become a popular means of payment for illicit trade. We don't have an informed view on this subject but the fact that all Bitcoin transactions are publicly available (and therefore can be tracked in theory by law enforcement agencies) and that every Bitcoin is defined by its unique transaction history (making it difficult for criminals to cover their tracks[6]) may limit the growth of its use in the black market/underworld.

In addition to its role as a mean for payment for on-line commerce, Bitcoin can be used for transfer of money (e.g. immigrant worker in the US sending remittances back home). This can be done very cheaply and fast (online settlement in under 10min if the sender is trustworthy like family member or 50min settlement for strangers). How do we assign a maximum fair value to this role of Bitcoin?

Western Union, MoneyGram, and Euronet are the three top players in the money transfer industry (with about 20% of the total market share). Let's assume that Bitcoin becomes one of the top three players in this industry. What does that mean for Bitcoin valuation? Given Bitcoin's supply is fixed, when one buys a Bitcoin, one is acquiring not only a medium of exchange but also an investment in the enterprise value of Bitcoin. From this point of view, Bitcoin's market capitalization could be viewed, with a little leap of faith, as its enterprise value. With the average market capitalization of Western Union, MoneyGram and Euronet at about **$4.5bn**, we will add this number to the maximum market capitalization of Bitcoin's role as a medium of exchange.

[6] Reid and Harrigan (2011) used passive analysis of the public history to identify 60% of the users related to the WikiLeaks donations address. They also validated and traced an alleged theft of 25,000 Bitcoins from a shared mining account despite attempts to launder and reshuffle the money. Law enforcement could do better with subpoenaed IP logs from signups at the exchanges as well as planting and following "marked coins."

Chart 7: BTC surpasses Western Union in market capitalization



Source: BofA Merrill Lynch Global Research, Bloomberg

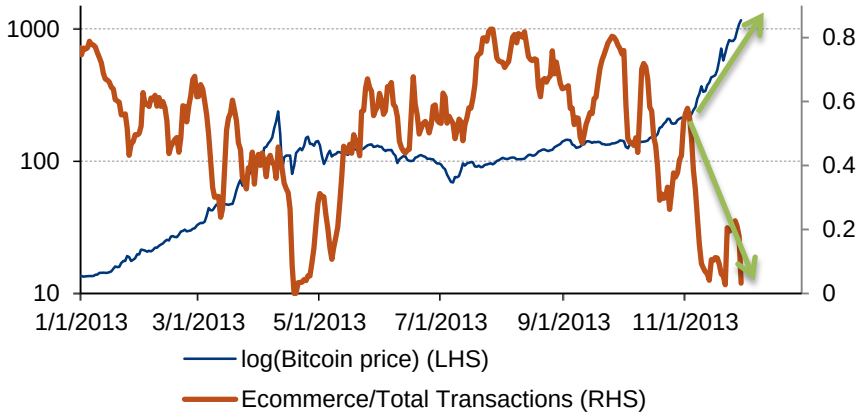
Bottom-line: maximum market capitalization for Bitcoin's as a medium of exchange = $5bn (for B2C e-commerce) + 4.5bn (means for payments) = $9.5bn

Interestingly, our $9.5bn estimate is below the current actual market capitalization of Bitcoin at $13bn. This suggests that the current market value of Bitcoin assumes either that Bitcoin will account more than 10% of market share for e-commerce, will have more than 10% market share of the money transfer industry (Chart 7)., or will have significant value as a store of value.

Value as a store of value

The value of Bitcoin has been recently outstripping the growth of the non-speculative transactions using it (Chart 8). This fact alone would suggest that the price appreciation has been more about Bitcoin as a store of value or investment than as a medium of exchange.

Chart 8: Fewer transactions outside exchanges as prices rose



Source: BofA Merrill Lynch Global Research

How can we assign a value to Bitcoin's role as a store of value? This is a very difficult question. Given Bitcoin does not pay any interest and that there are no investment instruments (equities or bonds) that are denominated in Bitcoin, the value of its store of value role appears limited. From this point of view, as a store value, its closest cousins are probably precious metals or cash (Table 1), in our view.

Table 1: Value of Bitcoin substitutes

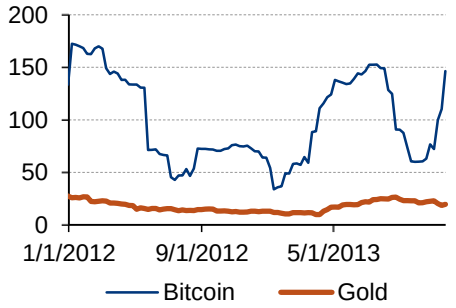
Value of large denomination $+€ bills	Value of gold bar/coins/ETFs in private hands	Deposits of foreigners with Swiss banks
$1.5trn	$1.3trn	$50bn

Source: BofA Merrill Lynch Global Research

Bitcoins and gold have three important common attributes: neither pays any interest, the supply of both is limited, and both are more difficult to trace than most financial assets (except cash). The current outstanding value of gold bar/coins/ETFs is about $1.3trn. Can Bitcoin reach the same market capitalization as gold? We are doubtful.

First of all, Bitcoins are much more volatile than gold, which makes Bitcoins a riskier asset to own. Over the past two years, the volatility of Bitcoin has been on average five times higher than that of gold (Chart 9). All else being equal, this means Bitcoins are five times riskier than gold. Unless Bitcoin volatility declines sharply or gold prices increases sharply, it is reasonable to think that it will be difficult for the market capitalization of Bitcoins to go above $300bn.

Chart 9: Realized vol of Bitcoin versus gold (52w rolling window)



Source: BofA Merrill Lynch Global Research

Furthermore, the reputation of gold as a unique and safe store of value has been growing for the past ten thousand years. It will take some time for Bitcoins to acquire that reputation. We don't know how to quantify the value of gold's reputation, but this reputation is probably the main reason that its value is 60 times that of silver. If we were to assume that Bitcoin were to eventually acquire the reputation of silver (which is an extremely ambitious assumption), this suggests that Bitcoin market capitalization for its role as a store of value could reach $5bn.

By the way, $5bn is not too far from the current value of total US silver eagles minted (since 1986), in our view probably the most relevant comparison to Bitcoin, that is around $8bn (12k tons).

Bottom-line: maximum market capitalization for Bitcoin's as a store of value = $5bn

Bitcoin's has one advantage over gold in that it is easier to transfer. That said, we don't think this is a big advantage given the advent of gold ETFs and the ability to move such ETFs in-between accounts. We would not assign any additional value for Bitcoin in this respect.

Clearly, market perception of the Bitcoin's fair value also depends importantly on the outlook for unconventional monetary policy. If Federal Reserve's quantitative easing does not end over the next year, as is generally expected, the demand for safe haven assets (like gold and Bitcoins) would increase supporting their value. We expect Fed tapering to begin in Q1 next year and the USD to slowly regain its credibility as the world's reserve currency, especially as the US continues to reduce its fiscal deficit that will likely fall below 4% of GDP next year. Bitcoin as a store of value likely will struggle to gain traction if our bullish USD view for 2014 turns out to be correct.

Final tally:

When we add our estimated maximum market capitalization for Bitcoins for its role as a medium exchange with that for its role as a store of value, we get a number that is somewhere around $15bn. Although this does not mean that Bitcoin price cannot rise further (as an object of speculation), we think the recent rise of Bitcoin price could soon run ahead of its fundamentals. Our current view implies a:

Maximum market capitalization for Bitcoin = $15bn

Maximum fair value of Bitcoin = 1300 USD

Conclusions

We believe Bitcoin could become a major means of payment for e-commerce and may emerge as a serious competitor to traditional money-transfer providers. As a medium of exchange, Bitcoin has clear potential for growth, in our view.

There is much speculation that Bitcoin may help avoid high taxes, capital controls, and confiscation. The correlation between CNY's share of volume of all Bitcoin exchanges and price of Bitcoin is rising. That said, the fact that all Bitcoin transactions are publically available and that every Bitcoin has a unique transaction history that cannot be altered may ultimately limit its use in the black market/underworld.

Bitcoin's role as a store of value can compromise its viability as a medium of exchange. Its high volatility, a result of speculative activities, is hindering its general acceptance as a means of payments for on-line commerce.

Is Bitcoin a bubble? Assuming Bitcoin becomes (1) a major player in both e-commerce and money transfer and (2) a significant store of value with a reputation close to silver, our fair value analysis implies a maximum market capitalization of Bitcoin of $15bn (1BTC = 1300 USD). This suggests that the 100 fold increase in Bitcoin prices this year is at risk of running ahead of its fundamentals.

Appendix

Bitcoin is based on **public-key cryptography** where each transaction is referenced by two keys: the public key that encrypts incoming payments and the private key that decrypts them. These keys are represented by long numbers to make encryption secure against brute-force guessing. Although it is possible to use the same account (public key) for all incoming and outgoing transactions, people who desire anonymity would generate unique public keys for each transaction. They would give out a unique address to receive and store one-time payments from other senders, rather than using a static single address as we do with bank accounts. Otherwise, the public can deduce how much money there is in each address and how the owners spend it by looking at the public history. To make large payments, the user may combine several sources of funds e.g. 10 public keys with 0.7 Bitcoins each to make a payment of 5 Bitcoins and simultaneously return 2 Bitcoins as change to a newly created address.

A **miner** acts like a historian logging and verifying new transactions in the public ledger. As an incentive to update the ledger, the miner receives a predetermined amount of Bitcoin when his block is linked to the Blockchain. Each block is an independent challenge: the first miner to compute the proof gets paid while the rest get nothing and have to start over on a new block. Each miner's problem is distinct because it depends on the previous block, outstanding transactions and the unique payment to themselves. Thus, a faster computer does not guarantee victory, but does increase the probability of winning. In practice, miners join guilds to spread profits based on individual contributions to reduce the volatility of large and significant payoffs from acting alone.

The main **block chain** contains the longest series of connected and verified blocks and establishes the definitive consensus on the public history of transactions. A block is considered verified when it contains a "proof of work," which is special piece of code the "miner" has calculated. A miner summarizes

the new transactions using what is known as a cryptographic hash function[7], which gives a compact description of new transaction entries that form the new block. Miners keep calculating new hashes until they're lucky and “hit bull’s eye” when they find a small hash that summarizes the new block and the transactions it contains. The blocks are connected because each new block references the previous block in the longest chain. The purpose of finding this small hash is to prove the miner did billions of calculations[8] and deserves the block. The computational requirement to verify each block makes it impractical to rewrite history by an attacker.

An **arms race** results from competition for easy mining profit where miners compete to outspend each other on the ever-improving mining equipment. Unlike real-life mining, the resource output does not increase with network size because of the difficulty adjustment applied to the verification of each block. The difficulty measures how small the target hash has to be and changes every 2016 blocks (every 2 weeks). As computing power goes up, thus the difficulty increases exponentially and ensures a new block is added every 10 minutes on average. In practice, occasional individual blocks can be 5 or 15 minutes apart. Every 210,000 blocks (4 years) the payments halve so that blocks in 2139 will only earn 1 Satoshi/each and none after 2140. Instead, the system allows for senders of transactions to propose a small transaction fee to go to the winning miner as a form of compensation. The miners then prioritize transactions with larger payments to get included into blocks faster.

Hobby miners have been recently displaced by capitalized industrial miners using specialized mining computer chips as the number of computations to yield $1 has been growing at 157%/year (Chart 4).

[7] A hash function is a one-way encryption that garbles input of any length into output of a fixed length, such as "The quick brown fox jumps over the lazy dog" hashes to 37f332f68db77bd9d7edd4969571ad671cf9dd3b. While “The quick brown fox jumps over the lazy cog" gives 132072df690933835eb8b6ad0b77e7b6f14acad7.

[8] A billion hashes is denoted as a Giga Hash and is used as a standard measurement of network speed.

Link to Definitions

Macro

Click here for definitions of commonly used terms.

Important Disclosures

BofA Merrill Lynch Research personnel (including the analyst(s) responsible for this report) receive compensation based upon, among other factors, the overall profitability of Bank of America Corporation, including profits derived from investment banking revenues.

BofA Merrill Lynch Global Credit Research analysts regularly interact with sales and trading desk personnel in connection with their research, including to ascertain pricing and liquidity in the fixed income markets.

Other Important Disclosures

Rule 144A securities may be offered or sold only to persons in the U.S. who are Qualified Institutional Buyers within the meaning of Rule 144A under the Securities Act of 1933, as amended.

SECURITIES DISCUSSED HEREIN MAY BE RATED BELOW INVESTMENT GRADE AND SHOULD THEREFORE ONLY BE CONSIDERED FOR INCLUSION IN ACCOUNTS QUALIFIED FOR SPECULATIVE INVESTMENT.

Recipients who are not institutional investors or market professionals should seek the advice of their independent financial advisor before considering information in this report in connection with any investment decision, or for a necessary explanation of its contents.

The securities discussed in this report may be traded over-the-counter. Retail sales and/or distribution of this report may be made only in states where these securities are exempt from registration or have been qualified for sale.

Officers of MLPF&S or one or more of its affiliates (other than research analysts) may have a financial interest in securities of the issuer(s) or in related investments.

This report, and the securities discussed herein, may not be eligible for distribution or sale in all countries or to certain categories of investors.

BofA Merrill Lynch Global Research policies relating to conflicts of interest are described at http://www.ml.com/media/43347.pdf.

"BofA Merrill Lynch" includes Merrill Lynch, Pierce, Fenner & Smith Incorporated ("MLPF&S") and its affiliates. Investors should contact their BofA Merrill Lynch representative or Merrill Lynch Global Wealth Management financial advisor if they have questions concerning this report.
"BofA Merrill Lynch" and "Merrill Lynch" are each global brands for BofA Merrill Lynch Global Research.

Information relating to Non-US affiliates of BofA Merrill Lynch and Distribution of Affiliate Research Reports:

MLPF&S distributes, or may in the future distribute, research reports of the following non-US affiliates in the US (short name: legal name): Merrill Lynch (France): Merrill Lynch Capital Markets (France) SAS; Merrill Lynch (Frankfurt): Merrill Lynch International Bank Ltd., Frankfurt Branch; Merrill Lynch (South Africa): Merrill Lynch South Africa (Pty) Ltd.; Merrill Lynch (Milan): Merrill Lynch International Bank Limited; MLI (UK): Merrill Lynch International; Merrill Lynch (Australia): Merrill Lynch Equities (Australia) Limited; Merrill Lynch (Hong Kong): Merrill Lynch (Asia Pacific) Limited; Merrill Lynch (Singapore): Merrill Lynch (Singapore) Pte Ltd.; Merrill Lynch (Canada): Merrill Lynch Canada Inc; Merrill Lynch (Mexico): Merrill Lynch Mexico, SA de CV, Casa de Bolsa; Merrill Lynch (Argentina): Merrill Lynch Argentina SA; Merrill Lynch (Japan): Merrill Lynch Japan Securities Co., Ltd.; Merrill Lynch (Seoul): Merrill Lynch International Incorporated (Seoul Branch); Merrill Lynch (Taiwan): Merrill Lynch Securities (Taiwan) Ltd.; DSP Merrill Lynch (India): DSP Merrill Lynch Limited; PT Merrill Lynch (Indonesia): PT Merrill Lynch Indonesia; Merrill Lynch (Israel): Merrill Lynch Israel Limited; Merrill Lynch (Russia): OOO Merrill Lynch Securities, Moscow; Merrill Lynch (Turkey I.B.): Merrill Lynch Yatirim Bank A.S.; Merrill Lynch (Turkey Broker): Merrill Lynch Menkul Değerler A.Ş.; Merrill Lynch (Dubai): Merrill Lynch International, Dubai Branch; MLPF&S (Zurich rep. office): MLPF&S Incorporated Zurich representative office; Merrill Lynch (Spain): Merrill Lynch Capital Markets Espana, S.A.S.V.; Merrill Lynch (Brazil): Bank of America Merrill Lynch Banco Multiplo S.A.; Merrill Lynch KSA Company, Merrill Lynch Kingdom of Saudi Arabia Company.

This research report has been approved for publication and is distributed in the United Kingdom to professional clients and eligible counterparties (as each is defined in the rules of the Financial Conduct Authority and the Prudential Regulation Authority) by Merrill Lynch International and Banc of America Securities Limited (BASL), which are authorized by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority, and is distributed in the United Kingdom to retail clients (as defined in the rules of the Financial Conduct Authority and the Prudential Regulation Authority) by Merrill Lynch International Bank Limited, London Branch, which is authorised by the Central Bank of Ireland and subject to limited regulation by the Financial Conduct Authority and Prudential Regulation Authority - details about the extent of our regulation by the Financial Conduct Authority and Prudential Regulation Authority are available from us on request; has been considered and distributed in Japan by Merrill Lynch Japan Securities Co., Ltd., a registered securities dealer under the Financial Instruments and Exchange Act in Japan; is distributed in Hong Kong by Merrill Lynch (Asia Pacific) Limited, which is regulated by the Hong Kong SFC and the Hong Kong Monetary Authority; is issued and distributed in Taiwan by Merrill Lynch Securities (Taiwan) Ltd.; is issued and distributed in India by DSP Merrill Lynch Limited; and is issued and distributed in Singapore by Merrill Lynch International Bank Limited (Merchant Bank) and Merrill Lynch (Singapore) Pte Ltd. (Company Registration No.'s F 06872E and 198602883D respectively) and Bank of America Singapore Limited (Merchant Bank). Merrill Lynch International Bank Limited (Merchant Bank) and Merrill Lynch (Singapore) Pte Ltd. are regulated by the Monetary Authority of Singapore. Bank of America N.A., Australian Branch (ARBN 064 874 531), AFS License 412901 (BANA Australia) and Merrill Lynch Equities (Australia) Limited (ABN 65 006 276 795), AFS License 235132 (MLEA) distributes this report in Australia only to 'Wholesale' clients as defined by s.761G of the Corporations Act 2001. With the exception of BANA Australia, neither MLEA nor any of its affiliates involved in preparing this research report is an Authorised Deposit-Taking Institution under the Banking Act 1959 nor regulated by the Australian Prudential Regulation Authority. No approval is required for publication or distribution of this report in Brazil and its local distribution is made by Bank of America Merrill Lynch Banco Múltiplo S.A. in accordance with applicable regulations. Merrill Lynch (Dubai) is authorized and regulated by the Dubai Financial Services Authority (DFSA). Research reports prepared and issued by Merrill Lynch (Dubai) are prepared and issued in accordance with the requirements of the DFSA conduct of business rules.

Merrill Lynch (Frankfurt) distributes this report in Germany. Merrill Lynch (Frankfurt) is regulated by BaFin.

This research report has been prepared and issued by MLPF&S and/or one or more of its non-US affiliates. MLPF&S is the distributor of this research report in the US and accepts full responsibility for research reports of its non-US affiliates distributed to MLPF&S clients in the US. Any US person receiving this research report and wishing to effect any transaction in any security discussed in the report should do so through MLPF&S and not such foreign affiliates.

General Investment Related Disclosures:

Taiwan Readers: Neither the information nor any opinion expressed herein constitutes an offer or a solicitation of an offer to transact in any securities or other financial instrument. No part of this report may be used or reproduced or quoted in any manner whatsoever in Taiwan by the press or any other person without the express written consent of BofA Merrill Lynch.

This research report provides general information only. Neither the information nor any opinion expressed constitutes an offer or an invitation to make an offer, to buy or sell any securities or other financial instrument or any derivative related to such securities or instruments (e.g., options, futures, warrants, and contracts for differences). This report is not intended to provide personal investment advice and it does not take into account the specific investment objectives, financial situation and the particular needs of any specific person. Investors should seek financial advice regarding the appropriateness of investing in financial instruments and implementing investment strategies discussed or recommended in this report and should understand that statements regarding future prospects may not be realized. Any decision to purchase or subscribe for securities in any offering must be based solely on existing public information on such security or the information in the prospectus or other offering document issued in connection with such offering, and not on this report.

Securities and other financial instruments discussed in this report, or recommended, offered or sold by Merrill Lynch, are not insured by the Federal Deposit Insurance Corporation and are not deposits or other obligations of any insured depository institution (including, Bank of America, N.A.). Investments in general and, derivatives, in particular, involve numerous risks, including, among others, market risk, counterparty default risk and liquidity risk. No security, financial instrument or derivative is suitable for all investors. In some cases, securities and other financial instruments may be difficult to value or sell and reliable information about the value or risks related to the security or financial instrument may be difficult to obtain. Investors should note that income from such securities and other financial instruments, if any, may fluctuate and that price or value of such securities and instruments may rise or fall and, in some cases, investors may lose their entire principal investment. Past performance is not necessarily a guide to future performance. Levels and basis for taxation may change.

Futures and options are not appropriate for all investors. Such financial instruments may expire worthless. Before investing in futures or options, clients must receive the appropriate risk disclosure documents. Investment strategies explained in this report may not be appropriate at all times. Costs of such strategies do not include commission or margin expenses.

BofA Merrill Lynch is aware that the implementation of the ideas expressed in this report may depend upon an investor's ability to "short" securities or other financial instruments and that such action may be limited by regulations prohibiting or restricting "shortselling" in many jurisdictions. Investors are urged to seek advice regarding the applicability of such regulations prior to executing any short idea contained in this report.

Foreign currency rates of exchange may adversely affect the value, price or income of any security or financial instrument mentioned in this report. Investors in such securities and instruments effectively assume currency risk.

UK Readers: The protections provided by the U.K. regulatory regime, including the Financial Services Scheme, do not apply in general to business coordinated by BofA Merrill Lynch entities located outside of the United Kingdom. BofA Merrill Lynch Global Research policies relating to conflicts of interest are described at http://www.ml.com/media/43347.pdf.

MLPF&S or one of its affiliates is a regular issuer of traded financial instruments linked to securities that may have been recommended in this report. MLPF&S or one of its affiliates may, at any time, hold a trading position (long or short) in the securities and financial instruments discussed in this report.

BofA Merrill Lynch, through business units other than BofA Merrill Lynch Global Research, may have issued and may in the future issue trading ideas or recommendations that are inconsistent with, and reach different conclusions from, the information presented in this report. Such ideas or recommendations reflect the different time frames, assumptions, views and analytical methods of the persons who prepared them, and BofA Merrill Lynch is under no obligation to ensure that such other trading ideas or recommendations are brought to the attention of any recipient of this report.

In the event that the recipient received this report pursuant to a contract between the recipient and MLPF&S for the provision of research services for a separate fee, and in connection therewith MLPF&S may be deemed to be acting as an investment adviser, such status relates, if at all, solely to the person with whom MLPF&S has contracted directly and does not extend beyond the delivery of this report (unless otherwise agreed specifically in writing by MLPF&S). MLPF&S is and continues to act solely as a broker-dealer in connection with the execution of any transactions, including transactions in any securities mentioned in this report.

Copyright and General Information regarding Research Reports:

Materials prepared by BofA Merrill Lynch Global Research personnel are based on public information. Facts and views presented in this material have not been reviewed by, and may not reflect information known to, professionals in other business areas of BofA Merrill Lynch, including investment banking personnel. BofA Merrill Lynch has established information barriers between BofA Merrill Lynch Global Research and certain business groups. As a result, BofA Merrill Lynch does not disclose certain client relationships with, or compensation received from, such companies in research reports. To the extent this report discusses any legal proceeding or issues, it has not been prepared as nor is it intended to express any legal conclusion, opinion or advice. Investors should consult their own legal advisers as to issues of law relating to the subject matter of this report. BofA Merrill Lynch Global Research personnel's knowledge of legal proceedings in which any BofA Merrill Lynch entity and/or its directors, officers and employees may be plaintiffs, defendants, co-defendants or co-plaintiffs with or involving companies mentioned in this report is based on public information. Facts and views presented in this material that relate to any such proceedings have not been reviewed by, discussed with, and may not reflect information known to, professionals in other business areas of BofA Merrill Lynch in connection with the legal proceedings or matters relevant to such proceedings.

This report has been prepared independently of any issuer of securities mentioned herein and not in connection with any proposed offering of securities or as agent of any issuer of any securities. None of MLPF&S, any of its affiliates or their research analysts has any authority whatsoever to make any representation or warranty on behalf of the issuer(s). BofA Merrill Lynch Global Research policy prohibits research personnel from disclosing a recommendation, investment rating, or investment thesis for review by an issuer prior to the publication of a research report containing such rating, recommendation or investment thesis.

Any information relating to the tax status of financial instruments discussed herein is not intended to provide tax advice or to be used by anyone to provide tax advice. Investors are urged to seek tax advice based on their particular circumstances from an independent tax professional.

The information herein (other than disclosure information relating to BofA Merrill Lynch and its affiliates) was obtained from various sources and we do not guarantee its accuracy. This report may contain links to third-party websites. BofA Merrill Lynch is not responsible for the content of any third-party website or any linked content contained in a third-party website. Content contained on such third-party websites is not part of this report and is not incorporated by reference into this report. The inclusion of a link in this report does not imply any endorsement by or any affiliation with BofA Merrill Lynch. Access to any third-party website is at your own risk, and you should always review the terms and privacy policies at third-party websites before submitting any personal information to them. BofA Merrill Lynch is not responsible for such terms and privacy policies and expressly disclaims any liability for them.

All opinions, projections and estimates constitute the judgment of the author as of the date of the report and are subject to change without notice. Prices also are subject to change without notice. BofA Merrill Lynch is under no obligation to update this report and BofA Merrill Lynch's ability to publish research on the subject company(ies) in the future is subject to applicable quiet periods. You should therefore assume that BofA Merrill Lynch will not update any fact, circumstance or opinion contained in this report.

Certain outstanding reports may contain discussions and/or investment opinions relating to securities, financial instruments and/or issuers that are no longer current. Always refer to the most recent research report relating to a company or issuer prior to making an investment decision.

In some cases, a company or issuer may be classified as Restricted or may be Under Review or Extended Review. In each case, investors should consider any investment opinion relating to such company or issuer (or its security and/or financial instruments) to be suspended or withdrawn and should not rely on the analyses and investment opinion(s) pertaining to such issuer (or its securities and/or financial instruments) nor should the analyses or opinion(s) be considered a solicitation of any kind. Sales persons and financial advisors affiliated with MLPF&S or any of its affiliates may not solicit purchases of securities or financial instruments that are Restricted or Under Review and may only solicit securities under Extended Review in accordance with firm policies.

Neither BofA Merrill Lynch nor any officer or employee of BofA Merrill Lynch accepts any liability whatsoever for any direct, indirect or consequential damages or losses arising from any use of this report or its contents.