

MRA Bitcoin Primer

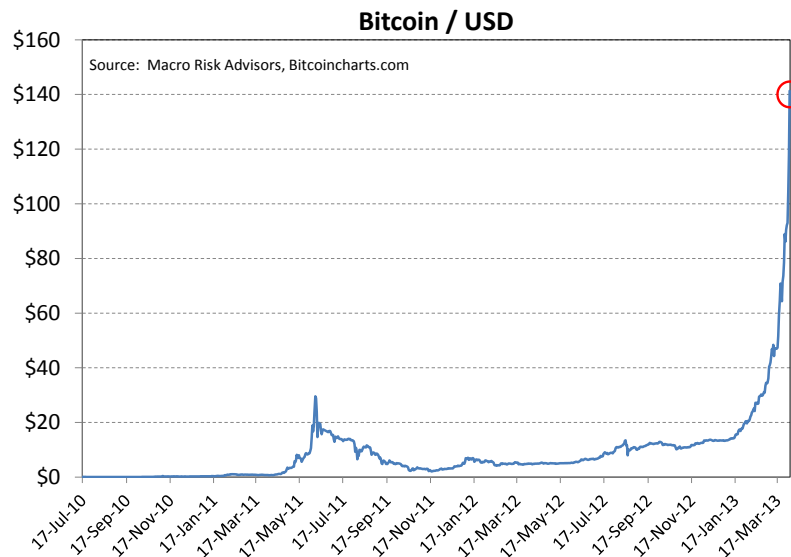
Phillip Rapoport
212-287-2687
prapoport@macroriskadvisors.com

What is Bitcoin?

Bitcoin is a digital currency that was created in 2009. As shorthand, it is often referred to as BTC, similar to how we use the abbreviations USD or EUR.

Bitcoin is not the first attempt at creating a digital currency, (you can find a [list of other attempts](#) on Wikipedia), but it is one of the most widely adopted ones today, with a monetary base in circulation that is well in excess of \$1 billion. ~\$80mm-\$100mm per day gets exchanged for fiat USD on bitcoin FX exchanges.

As interest in the alternative currency has soared, the BTC/USD exchange rate has also skyrocketed. 1 Bitcoin is now worth ~\$140 USD. That's +1060% since the start of 2013 and +409% since the beginning of March. A chart of the BTC/USD exchange rate is below.



Bitcoin has probably been more successful than other attempts at alternative currency systems because of its useful and well-designed features. It is easily transferable, fungible, durable, relatively anonymous, and – critically – it is believed to be secure.

It is also decentralized. This is an important and defining feature of Bitcoin. There is no central bank or central governing body controlling transactions. This very much appeals to the gold bugs and QE haters out there, and the 2009 creation of the currency is probably not coincidental timing.... Here's an excerpt from a piece written by Bitcoin's creator, Satoshi Nakamoto:

The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts.

Bitcoin aims to be a currency backed by our trust in math. There's no central server or trusted parties, because everything is based on cryptographic proof, instead of trust.

Instead of using a centralized model, Bitcoin is a peer-to-peer system: individual computers participating in the network serve to both announce and ratify transactions while providing security. We will discuss how this works in more detail later.

Bitcoins have value because they are useful – i.e. they can be exchanged for goods and services – and because they are scarce. They are not backed by any promise of convertibility. And there is certainly no guarantee that they will have any value in the future. But right now, you can use Bitcoin to purchase a [growing list](#) of things, including (but not limited to) [guitars](#), [socks](#), [gold bars](#), [web hosting](#), or even a [house in Canada](#). Its early uses were primarily among privacy wonks – you can donate to wikileaks anonymously using bitcoin, for example.

While many traditionalists may be quick to dismiss the idea of a digital currency that isn't backed by a major government, there are many common examples of private digital currencies that have been in use for years. Look at credit card points or airline miles as one example. These days, you can redeem credit card points on amazon.com, which means you can buy almost anything with an alternative currency.

Of course, Bitcoin's decentralized quality makes it preferable to airline points. You don't have to trust the airline (or any governing body) not to devalue the currency.

Below, we'll go into some detail on how Bitcoin actually works, as well as thinking through some of the investment implications and potential money making opportunities related to Bitcoin.

Who Created Bitcoin? Who Owns Bitcoin?

Bitcoin was created on Jan 3, 2009 by Satoshi Nakamoto. It turns out that Nakamoto is a pseudonym – so we don't really know who the creator is. It could be one person; it could be a group of people. There's an interesting [New Yorker article](#) from 2011 that details a search to reveal his identity. (It was unsuccessful).

The code is open source. Which means it's in the public domain; no one owns it. We can all see it and test it. We at MRA aren't knowledgeable enough to have an opinion on how secure it is, but some of the most respected cryptologists and hackers have tried their best to find loopholes or defeat the system, and it's generally considered to be extremely secure. That's not to say there isn't a flaw... but if there is, no one has publicly discovered it yet.

Here's Satoshi Nakamoto's original [white paper](#) explaining the currency. It's only 9 pages, but it's a bit technical. Here's a quote from Dan Kaminsky, a highly regarded security researcher:

“When I first looked into the code, I was sure I was going to be able to break it ... The way the whole thing was formatted was insane. Only the most paranoid, painstaking coder in the world could avoid making mistakes. ... I came up with beautiful bugs, but every time I went after the code, there was a line that addressed the problem. I've never seen anything like it. ... He's a world class programmer ... Either there's a team of people who worked on this, or this guy is a genius.”

The Double Spend Problem

A fundamental problem with digital currencies is solving the “double spend problem”. Unlike with physical money, digital items can be easily duplicated. (It's easy to make several copies of an mp3 or a file.) That's a big issue when we're talking about currency, since it creates theoretically unlimited supply.

The common solution for the double-spend problem is to use a trusted intermediary. The market is willing to trust Paypal or Citibank to make sure users don't spend the same dollars twice, because the intermediary deducts money from one user's account before the funds get added to the recipient's account.

This, however, is a centralized approach – one that Bitcoin is trying by design to avoid. Bitcoin is *decentralized*. It doesn't rely on an intermediary to govern the transaction process.

The concept underlying Bitcoin is that we can use encrypted digital signatures so anyone in the network can verify transaction records, without the need to trust any central authority. You only need to rely on your own calculations. It's a pretty libertarian idea. (Credit to [ArsTechnica](#) for some of the language used here).

A Master Ledger – “The Blockchain”

Think of the bitcoin network as a big master ledger. It's a giant log, recording every single bitcoin transaction that has ever happened, in chronological order. And a copy of the log is stored on every bitcoin client's computer. This log is called the “Blockchain”, but to avoid adding confusing jargon, We'll just keep referring to it as a log or ledger.

One interesting takeaway here is that all transaction data is public. We can see detailed information about every transaction that occurs... but the identities of the counterparties can remain anonymous.

Bitcoin Mining

If you've read some articles about bitcoin, you've probably heard the term bitcoin mining. “Bitcoin mining” and “bitcoin transaction verification” are more or less synonyms. Verifying transactions and adding them to the master ledger is very computationally intensive (by design). So to incentivize people to contribute their processing power, the system rewards bitcoin miners by awarding them with freshly minted bitcoin! In effect, you get paid for helping to process payments.

Bitcoin miners are racing to find solutions to what is called a “proof of work” problem. Finding a solution allows them to make a new entry on the master ledger. What does “proof of work” problem mean? It basically amounts to guessing the right input to generate a given output. Here's an example:

Input 1: “Test”

Output 1: 532eaabd9574880dbf76b9b8cc00832c20a6ec113d682299550d7a6e0f345e2

Input 2: “test” (lowercase t)

Output 2: 9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08

Note that the only difference in the input was changing the uppercase T to a lowercase t, and it generated a dramatically different output value.

Now imagine being given an output value, and trying to guess the correct input.

This is an oversimplification, but this is essentially what bitcoin miners are doing. It can take a lot of guesses. It's an elegant process, because it is very computationally intensive to guess until you find a solution. But once you propose a correct answer, everyone else in the network can very quickly and easily verify that your solution ‘works’. When a bitcoin miner finds a correct solution, he is awarded 25 BTC for his efforts. That new 25 BTC gets created out of thin air – the monetary base grows. And the miner is allowed to make a new entry in the ledger.

Other participants confirm the new entry, they copy the new version of the ledger, and then they move on to guessing the next input/output solution. Bitcoin mining is a mix of luck and computing power. You can now buy special [bitcoin mining computers](#), specifically designed to do this effectively.

Now here's the coolest part:

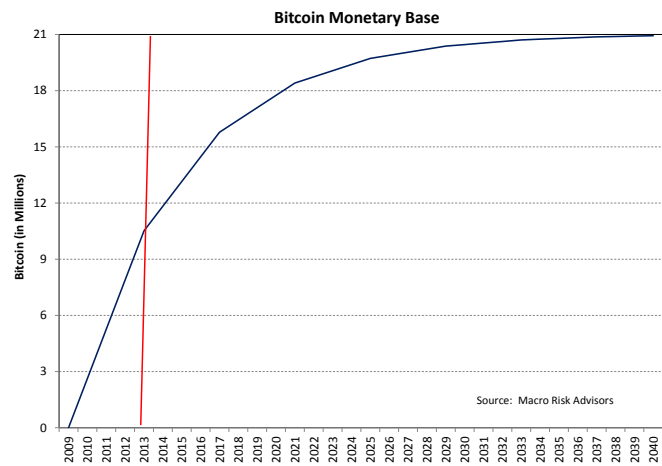
The system is designed so that a miner correctly guesses a solution every 10 minutes on average. But as more people dedicate computing power to the network, solutions will obviously be discovered more quickly. *So the system adjusts the difficulty of the problem accordingly, making it tougher to guess a solution.* It gets harder to find solutions as more people participate. Which is another way of saying the network becomes more secure as it scales.

Conceptually, if a hacker wanted to re-write the ledger, starting 10 transactions prior, he would have to have significantly more computing power than the network overall. And even if someone were to have access to that kind of computing power, the conventional thinking is that his financial incentive to act as a miner would exceed his incentive to hack maliciously...

Growth in the Bitcoin Monetary Base

As mentioned above, new bitcoin is created every 10 minutes and awarded to bitcoin miners. There are currently ~11mm BTC in circulation. The entire BTC supply has originated from mining. (Satoshi Nakamoto mined the first 50 BTC himself.)

Currently, 25 BTC is created and awarded to miners every 10 minutes as compensation for processing transactions. This reward for mining will gradually decline, halving every 4 years. So in 2017, the reward for mining will drop to 12.5 every 10 minutes from 25.0 every 10 minutes. This process continues until the total number of BTC in circulation reaches 21mm. At that point, there will be a fixed supply. See chart below. It is expected that we will hit the ceiling sometime around 2040+.



The red line is our current position

Coins can be divided down to 8 decimal places, in the event that their value grows. The smallest unit, 0.00000001, is called “1 satoshi”, after the founder’s pen name.

Some people criticize the system for overly rewarding early adopters. The reward for mining has already halved once – from 50 to 25 BTC every 10 minutes – in 2013. Mining was easiest in 2009/2010 when fewer participants were competing, and the rate of new creation was highest.

How Do I Buy Bitcoin?

You can trade BTC against most major currencies on any of several exchanges. A few popular sites: [MtGox](#) (by far the largest one with around 70% of exchange volume), [WirWoX](#), [Bitcoin-24](#), and [TradeHill](#) (a newcomer marketing itself to institutional investors).

Some data on bid/offer: At time of writing, the exchange market is currently 40bps wide for \$5k and 70bps wide for \$20k. Bitcoin.clarkmoody.com is a good site to see depth of market on MtGox without creating an account.

Overall exchange liquidity seems better than the bid/offer suggests: \$80-100mm/day has been trading on the major exchanges, up from ~\$20mm/day before the recent price surge. (See chart pack addendum).

This document has been prepared by Macro Risk Advisors’ (“MRA”) Sales and Trading Group for informational purposes only. MRA does not publish research reports as defined under FINRA Rule 2711. MRA does not trade proprietarily, and is not acting as an advisor or fiduciary. MRA does not guarantee the accuracy or completeness of information which is contained in this document and accepts no liability for any consequential losses arising from the use of this information. Any data on past performance, modeling or back-testing contained herein is no indication as to future performance. All opinions and estimates are given as of the date hereof and are subject to change. The options risk disclosure document can be accessed at the following web address: <http://optionsclearing.com/publications/risks/riskchap1.jsp> Please ensure that you have read and understood it before entering into any options transactions.

You can also buy directly from a service like Coinbase, by linking your bank account. Or if you want anonymity, you can pay cash (similar to sending a MoneyGram) at a retail location via Bitinstant.

There is also a Bitcoin ATM supposedly launching shortly in Cyprus, with another planned for LA.

Bitcoin is still very young and only now flirting with mass adoption. The infrastructure still has a long way to go. But if the current bitcoin mania holds, you can expect to see more mass market solutions soon. Many VC firms are actively investing in bitcoin infrastructure now.

Of course, the most 'organic' way to acquire bitcoin is through mining. Though this is now becoming the realm of experts -- special hardware and low electricity costs are required to be effective (or tremendous luck).



Ways to Trade/Invest in the Theme

- Inter-Exchange Arbitrage: Exchange prices are still *very* inefficient. Combining the order books from all exchanges, you can frequently find markets inverted by as much as \$5 (i.e. 4.3% on a \$115 BTC price). There may be 0.5-2% transaction fees in many cases, but there is still a lot of edge. Many exchanges offer trading APIs, and some plan to even offer FIX connectivity.

Of course, there are other implementation risks you need to worry about: Slow transaction confirmation, fading bids/offers, and exchange hacking issues, to name a few.

- Invest in Bitcoin infrastructure. There's no public equity that we're aware of. But there are many exchanges and other startups looking for seed capital. The ecosystem is catching up with the BTC price move.

Looking at the bitcoin exchange business, our rough estimates suggest MtGox transaction fees produced ~\$775k in revenue in Mar'13. That's +300% MoM vs. Feb'13 and +1433% YoY vs. Mar'12.

- Buy and Hold Bitcoin. And beware of the volatility.

Where Does the Government Stand on All This?

Regulation is certainly one of the biggest risks to bitcoin, particularly for US based investors. The decentralized nature of the system makes it tough for the government to "turn it off". (Think about how impossible it was to control p2p music piracy). But it can probably be regulated back into the shadows, which could cause the price to plummet. More regulation is likely coming, but we can point you to some recent guidance:

- The Financial Crimes Enforcement Network ("FinCEN") issued some guidance for virtual currencies on March 18, 2013. You can read the full [statement here](#). The language seems like a clear nod to bitcoin:

"... a de-centralized convertible virtual currency that has no central repository and no single administrator, and that persons may obtain by their own computing or manufacturing effort."

FinCEN says that if you are in the business of exchanging virtual currency for "real" currency (i.e. USD), you must register as a Money Center Bank ("MSB"). This means you must register, and follow know your customer and AML regulations.

This document has been prepared by Macro Risk Advisors' ("MRA") Sales and Trading Group for informational purposes only. MRA does not publish research reports as defined under FINRA Rule 2711. MRA does not trade proprietarily, and is not acting as an advisor or fiduciary. MRA does not guarantee the accuracy or completeness of information which is contained in this document and accepts no liability for any consequential losses arising from the use of this information. Any data on past performance, modeling or back-testing contained herein is no indication as to future performance. All opinions and estimates are given as of the date hereof and are subject to change. The options risk disclosure document can be accessed at the following web address: <http://optionsclearing.com/publications/risks/riskchap1.jsp> Please ensure that you have read and understood it before entering into any options transactions.

While regulation is probably one of the biggest risks to long term bitcoin adoption, the FinCEN statement actually seems pretty positive, as it implicitly seems to condone the actions of bitcoin users.

- Some [tax bloggers have suggested](#) that Bitcoin accounts in excess of \$10k may require people to file Foreign Bank Account Report ("FBAR").
- Here are some [thoughts on Bitcoin taxation](#). Is it a currency? A store of value? Or, in the case of bitcoin miners, ordinary income?

Some Closing Thoughts

Bitcoin could potentially be world changing. Or it could be the new tulip mania. As with most young, emerging technologies, the odds strongly favor the latter outcome.

Dust off your copy of "Extraordinary Popular Delusions", because there is already a mania underway -- the past 3 daily moves have been +12%, +13%, +20%. And with this asset, similar to gold, there is no valuation metric that anchors BTC price to reality. As long as demand exceeds supply, who's to say what 'overvalued' means?

There's also no good way to short it.

And the irreversible and anonymous characteristics can make the mechanics of borrowing BTC to short pretty messy (unless you want to involve a trusted intermediary... something the underlying premise of bitcoin tries to avoid).

One interesting aspect of the meteoric price rise is that it makes BTC extremely deflationary. Why would anyone spend bitcoin on goods, when the price seems likely to rise again tomorrow? Ironically, the deflationary aspect may prevent the currency in the short term from being adopted as a transactional tool rather than just a trading vehicle.

We'd describe bitcoin currently as a good medium of exchange but a poor store of value.

But it's not hard to imagine broader adoption. You don't have to believe that it will replace the USD -- it almost certainly won't. But a small amount of adoption could have a price big impact, given the limited supply by design. It does have strong appeal to several communities: libertarians, privacy advocates, black market economy participants, the zero hedge audience, and gold bugs to name a few.

Do you think a decentralized, digital currency can ever become mainstream? If so, then Bitcoin seems to have a reasonably good shot at being the one. Maybe a 10% or 15% chance?

The current bitcoin market cap is a bit above \$1B. It doesn't seem inconceivable that it could garner a market cap similar to SLV Equity. SLV is a product that's thought to be predominantly retail, has no real industrial use for its holders (no one is exchanging SLV for physical), where investment has been in large part motivated by fiat currency fears. SLV's market cap is currently \$9.4B, but it has gotten as high as \$17.2B as SLV made a run at \$50.

One hurdle to watch for is bitcoin acceptance on mainstream retail sites. Reddit.com is accepting bitcoin, but its accountants are [reportedly](#) spending more to manage the transactions than they are receiving in payments currently. A mainstream retail site accepting payment in bitcoin will go a long way towards legitimizing it as a currency.

Unfortunately, the rapid price rise impedes BTC from becoming a true medium of exchange. The parabolic move attracts hoarders and increases the crash probability. A gradual rise in which merchants could keep up with the rise in value would be preferable towards achieving a goal of a true digital currency. You need merchant transaction to increase over time. Right now, the market is mostly speculators flipping BTC rather than using it for real transactions, which creates a volatile feedback loop, making it less desirable for merchants.

If you invest in Bitcoin, we'd advise thinking about it as an option. It seems highly likely to lose most/all of its value at some point. Or at the minimum, have a vicious mean reversion. But it's not hard to envision broader adoption (and/or bitcoin mania) leading to a further 1000%+ price increase.

For what it's worth: the last crazy rally like this one – from 0.8 to 32.0 in summer 2011 – ended with a 90% drop in value as one of the major trading exchanges dealt with a [security breach](#). (Customer funds were stolen). And because many people used the same login/password credentials on several exchanges, the hack resulted in several exchanges experiencing a security breach. Though the bitcoin system itself is believed to be secure, the infrastructure surrounding it may not be.

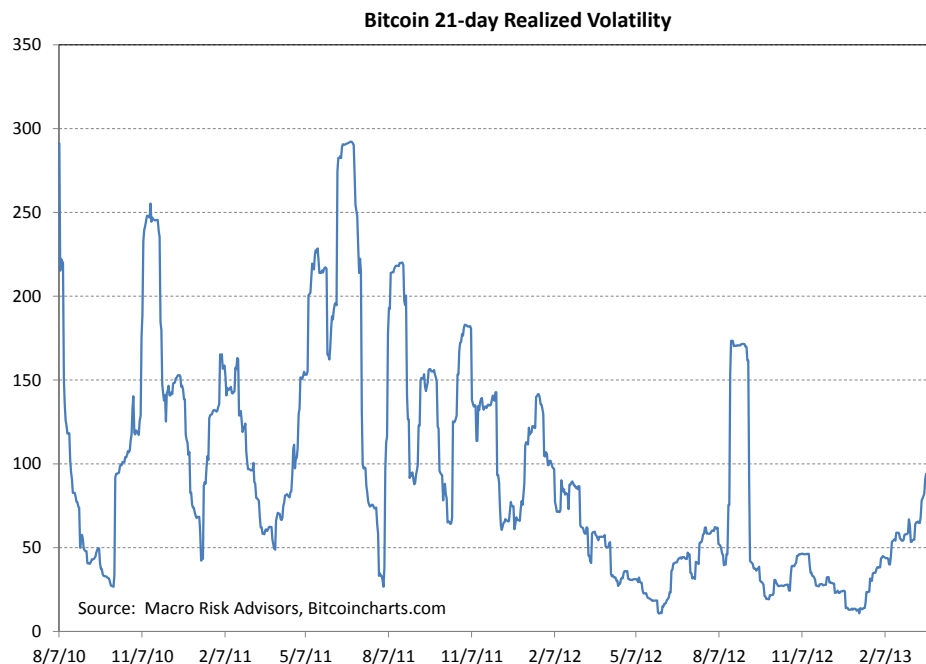
Full disclosure: The author is long bitcoins.

Bitcoin Options!

We'd be remiss if we didn't devote a few sentences to the possibility of options on bitcoin. There have been a few (very crude) attempts at creating an options market. But we haven't seen anything liquid or even really usable. Conceptually, replicating call options wouldn't be very difficult – you would buy the underlying to replicate, and buy more as it rallies.

But put options, given the lack of short selling ability, are more complicated. Hypothetically, if someone was long bitcoin inventory, they could offer puts to the market, and get less-long to delta hedge the position.

Below is a chart of 21-day realized volatility of BTC/USD. That's some serious realized volatility to hedge around.



Addendum: Bitcoin Chart Pack

Bitcoin Price in USD

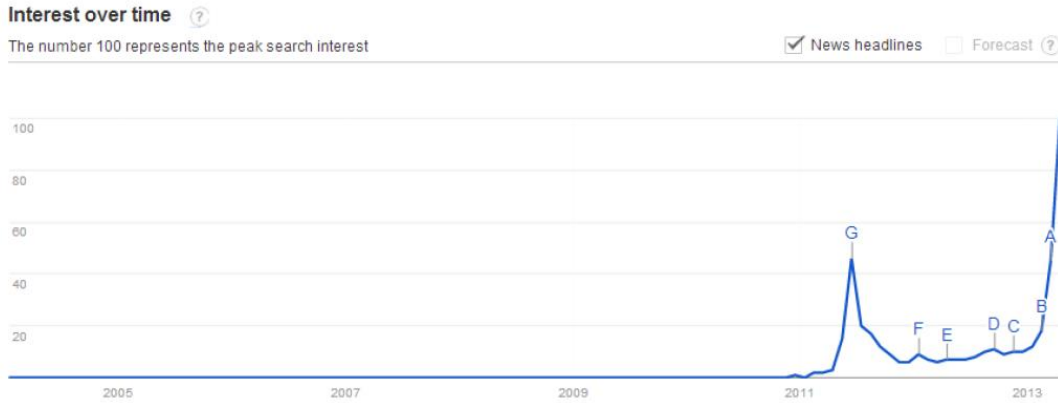


Bitcoin Market Cap in USD

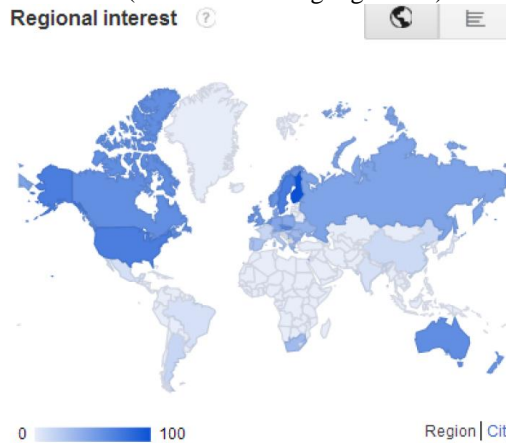


This document has been prepared by Macro Risk Advisors' ("MRA") Sales and Trading Group for informational purposes only. MRA does not publish research reports as defined under FINRA Rule 2711. MRA does not trade proprietary, and is not acting as an advisor or fiduciary. MRA does not guarantee the accuracy or completeness of information which is contained in this document and accepts no liability for any consequential losses arising from the use of this information. Any data on past performance, modeling or back-testing contained herein is no indication as to future performance. All opinions and estimates are given as of the date hereof and are subject to change. The options risk disclosure document can be accessed at the following web address: <http://optionsclearing.com/publications/risks/riskchap1.jsp> Please ensure that you have read and understood it before entering into any options transactions.

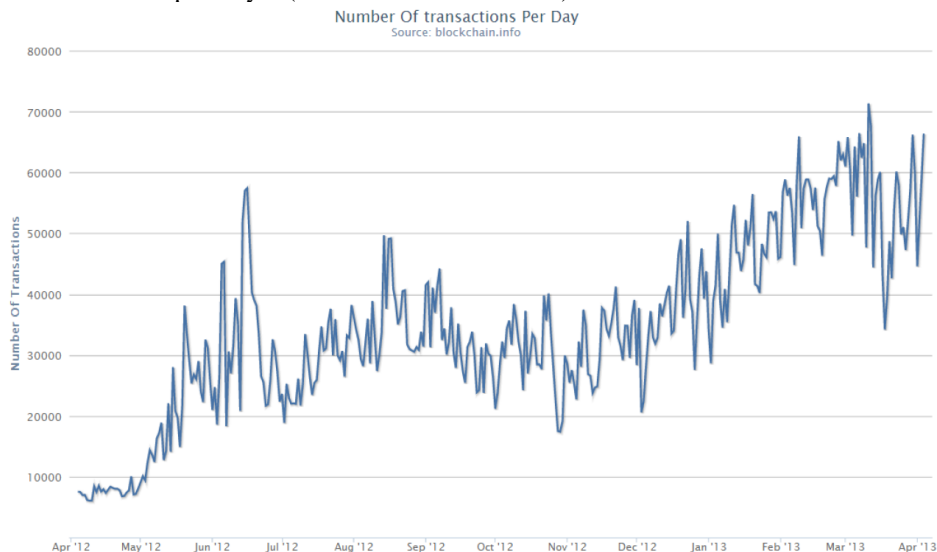
Google Trends Search Interest: Search interest recently broke through the previous peak set during the 2011 exchange security breach. (Source: Trends.google.com)



Regional Search Interest, trailing 12 months: (Source: Trends.google.com)



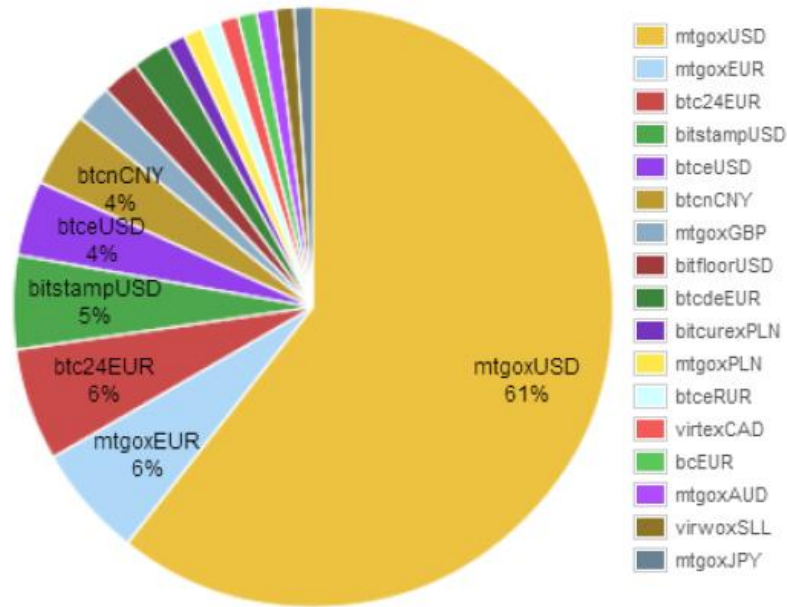
Number of Bitcoin Transactions per Day: (Source: Blockchain.info)



This document has been prepared by Macro Risk Advisors' ("MRA") Sales and Trading Group for informational purposes only. MRA does not publish research reports as defined under FINRA Rule 2711. MRA does not trade proprietarily, and is not acting as an advisor or fiduciary. MRA does not guarantee the accuracy or completeness of information which is contained in this document and accepts no liability for any consequential losses arising from the use of this information. Any data on past performance, modeling or back-testing contained herein is no indication as to future performance. All opinions and estimates are given as of the date hereof and are subject to change. The options risk disclosure document can be accessed at the following web address: <http://optionsclearing.com/publications/risks/riskchap1.jsp> Please ensure that you have read and understood it before entering into any options transactions.

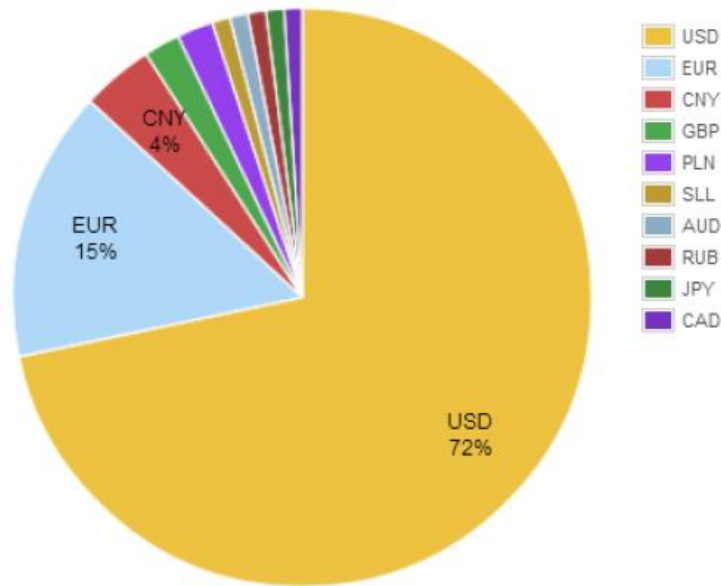
Exchange Volume Distribution (Source: Bitcoincharts.com):

by market



Exchange Volume Distribution (Source: Bitcoincharts.com):

by currency



This document has been prepared by Macro Risk Advisors' ("MRA") Sales and Trading Group for informational purposes only. MRA does not publish research reports as defined under FINRA Rule 2711. MRA does not trade proprietary, and is not acting as an advisor or fiduciary. MRA does not guarantee the accuracy or completeness of information which is contained in this document and accepts no liability for any consequential losses arising from the use of this information. Any data on past performance, modeling or back-testing contained herein is no indication as to future performance. All opinions and estimates are given as of the date hereof and are subject to change. The options risk disclosure document can be accessed at the following web address: <http://optionsclearing.com/publications/risks/riskchap1.jsp> Please ensure that you have read and understood it before entering into any options transactions.

USD Exchange Traded Volume: (Source: Blockchain.info)



Bitcoin Miners Aggregate Daily Revenue: (Source: Blockchain.info)



This document has been prepared by Macro Risk Advisors' ("MRA") Sales and Trading Group for informational purposes only. MRA does not publish research reports as defined under FINRA Rule 2711. MRA does not trade proprietary, and is not acting as an advisor or fiduciary. MRA does not guarantee the accuracy or completeness of information which is contained in this document and accepts no liability for any consequential losses arising from the use of this information. Any data on past performance, modeling or back-testing contained herein is no indication as to future performance. All opinions and estimates are given as of the date hereof and are subject to change. The options risk disclosure document can be accessed at the following web address: <http://optionsclearing.com/publications/risks/riskchap1.jsp> Please ensure that you have read and understood it before entering into any options transactions.

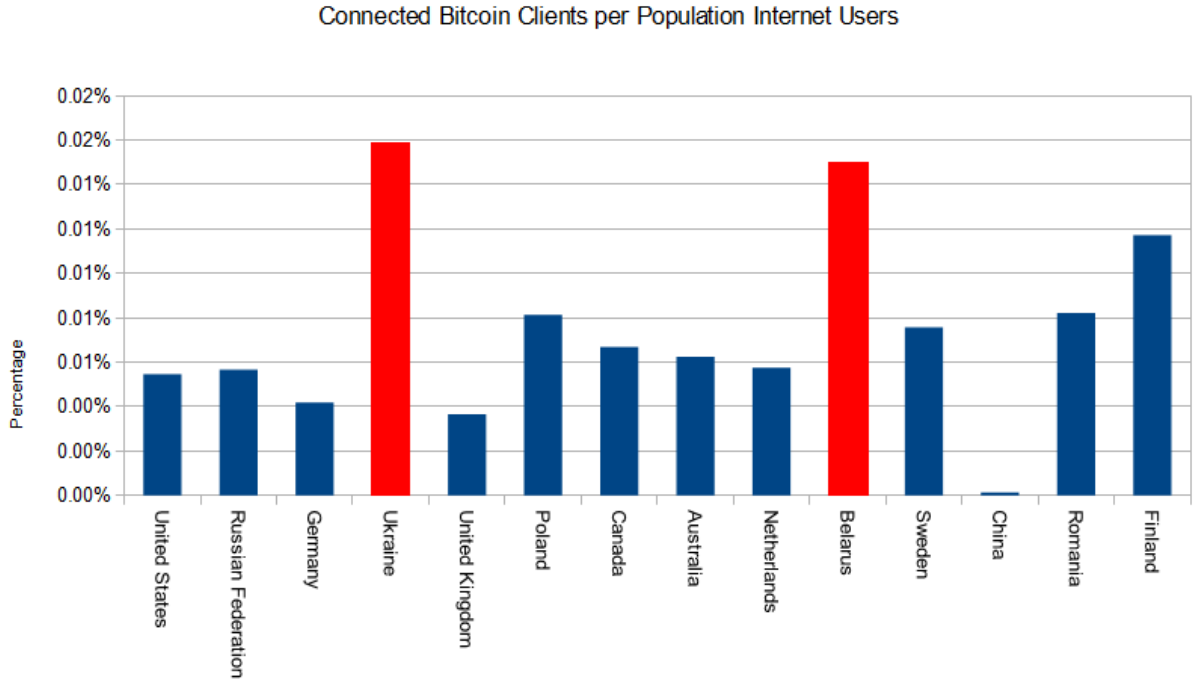
Some Bitcoin Mining Statistics, encompassing a 24 hour Period:

Bitcoin Mining Statistics: 24 hour period ended 3:30pm on 4/2/2013	
Blocks Mined	176
Time Between Blocks	8.18 (minutes)
Bitcoins Mined	4,400 BTC
Total Transaction Fees	59.13222421 BTC
No. of Transactions	61637
Estimated Transaction Volume	445,730.27168981 BTC
Estimated Transaction Volume (USD)	46,901,112.04 USD
Market Summary	
Market Price	\$105.22 USD (weighted)
Trade Volume	\$8,405,734.89 USD
Trade Volume	79,884.90 BTC
Mining Economics	
Total Miners Revenue	\$469,189.71
Electricity Consumption *	913.88 megawatt hours
Electricity Cost	\$137,081.49
Operating Profit	\$332,108.22
Operating Margin	70.78%
* Consumption based on 650W per gigahash; Cost based on 15c per KWh	
Source: Macro Risk Advisors, Blockchain.info	

Bitcoin Miner Operating Margins, based on assumptions above: (Source: Blockchain.info)



Bitcoin Clients as Percentage of Internet Users: (Source: thebitcointrader.com)



Bitcoin Exchange Arbitrage: This chart from cointhink.com shows how inverted the markets are between 3 exchanges (mtgox, btce, and bitstamp) this morning.

