

2013 Bitcoin Mid-Year Review and Outlook

Greg Schvey
Managing Editor

Jeff Schvey
Technical Director

Phillip Archer
Research Analyst

Jonathan Stacke
Research Analyst

www.TheGenesisBlock.com
contact@thegenesisblock.com

In This Report

Macro Trends	1
Trading Update	4
Bitcoin Exchanges	9
Entrepreneurs and Venture Capital	11
Protocol Developments	14
Mining Update	16
Regulatory Environment	21
Global Adoption	24
Notable Events	27

Macro Trends

To understand bitcoin's role in the first half of 2013, one must understand the macro trends driving its recent adoption. All of the below topics have existed for years, but have recently re-emerged to the forefront of global attention.

Capital Controls

The monetary freedom offered by bitcoin is becoming increasingly valuable.

Freely transacting with one's money is an ability many take for granted until it is stripped from them. As governments and banks around the world face economic desperation, global citizens are increasingly subject to restrictions on transfers and withdrawals from traditional banking institutions.

The fear of such actions has driven many to adopt bitcoin over the past six months for its unique ability to be sent anywhere in the world for little or no cost, without an intermediary party able to restrict those capital flows. Highlighting this phenomenon are a number of specific instances this year.

Cyprus

Global instability in recent years has led to a reduction in trust of many financial institutions.

As condition for receiving a much needed €10B bailout from the EU and IMF, a number of Cypriot banks were required to shave large sums from customer deposits and convert them into financial instruments to support the banks. To enforce this, the banks heavily restricted customer withdrawals and transfers. Depositors in other EU nations and around the globe saw this model as a potential template for future events, creating one of the most important macro events in bitcoin's history.

FIGURE 1 - EVENTS IN CYPRUS DRIVE WIDE-SCALE BITCOIN ADOPTION
(VIA MARKETS.THEGENESISBLOCK.COM)



Argentina

Uncontrollable inflation is driving global citizens to seek alternatives.

With the Peso seeing inflation rates as high as 20% and the Argentine government restricting cross-border capital flows, bitcoin has become an increasingly popular alternative. A recent meetup in Buenos Aires saw nearly 200 attendees interested in learning more about virtual currencies. Bitcoin now trades at a reported premium of 30% in Argentina, relative to global exchange rates.

Currency Wars

Bitcoin is immune to political manipulation of currency.

Allegations between governments of currency manipulation for trade advantages are nothing new to global economic and political discourse. America has levied such accusations against China for years, while Germany has been similarly targeted as the EU's industrial powerhouse benefiting from the currency of a monetary union that is likely far weaker than an independent Deutsche Mark.

For the first time, the possibility of a currency not issued by a central authority or subject to manipulation for trade advantages has come to the limelight. Many nations, most notably China, have repeatedly called for the USD's reign to come to an end and bitcoin, if it reaches the scale many believe is possible, may be a means to that end. For a more in depth discussion on this topic, we recommend the following articles published earlier this year:

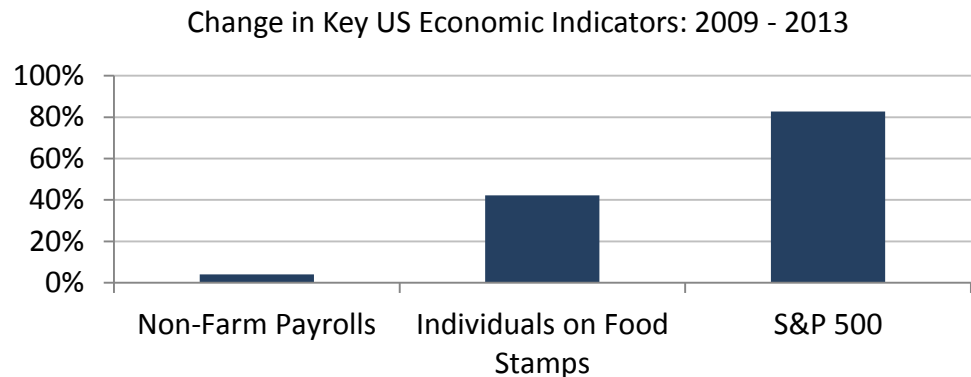
- [Bitcoin: The Newest Tool In China's Currency War Chest](#)
- [The Time For A Stateless Global Reserve Currency Approaching](#)

Monetary Easing

Debasement of fiat by central banks has led to fear of inflation.

The continued mass monetization of government debt across the globe has led many to fear widespread inflation in coming years. As central banks buy their own government's debt, interest rates have been pushed to near or below inflation with the intention of pushing wealth into risk assets to bolster the economy. While equity markets have risen to new highs, savers have been punished as the currency in their accounts is debased, with increasing concerns of even greater inflation as financial markets continue to decouple from underlying fundamentals.

FIGURE 2 - EFFECTS OF MONETARY EASING



Bitcoin's known issuance schedule is proving to be a welcomed alternative to government fiat.

For many, bitcoin's planned and publicly-known issuance schedule has become a welcomed alternative to politically-driven government fiat. This has proven true as the market reacts to central bank announcements, meaning that in addition to a leap forward in payment technology, bitcoin may be developing into a much-needed thermometer of global discontent with central banks.

Privacy Invasions

Recent events have led many to reconsider their rights to privacy.

Recent months have been filled with discussions about citizens' right to privacy from their governments. The leaked documents by Ed Snowden about the NSA's PRISM program has been the centerpiece of the discourse, though the conversation extends much further. In particular, similar discussions around financial privacy have been a long-time driver of bitcoin adoption.

Used largely for online narcotics purchases in its early days due to its ability to be transferred anonymously, bitcoin has since served as a means of financial freedom for those desiring transactions free of regulatory oversight for any reason. The use cases for this reach far beyond illicit purchases as anti-money laundering regulations have led to account freezes and transactional hurdles at countless banks and payment processors.

Bitcoin has also become a way for global citizens to express their voice without fear of prosecution. Donations to Wikileaks, US whistleblowers and a host of other entities fighting against governmental offenses have all been made possible by bitcoin.

Trading Update

Bitcoin rose 722% in the first six months of 2013.

Bitcoin trading opened 2013 with a foreshadow of what was to come, breaking the 21-month old high of \$31.91/BTC on February 28. Over the next 41 days, that record was broken another 20 times before peaking at \$266.00 on April 10. Though BTC fell from that peak to close the first half of 2013 at \$97.51, that figure still represents a remarkable 722% gain in just six months.

This is not the first bitcoin bubble.

While the price gain was impressive and the subsequent drop surely devastating for some, this is not the first time bitcoin has experienced this bubble-esque phenomenon. 2011 saw a similar scenario, with bitcoin reaching a peak of \$32 before eventually leveling off over a series of months. More importantly, there has been a consistent trend building on a logarithmic scale that shows a consistent upwards price movement as infrastructure around bitcoin continues to develop.

FIGURE 3 - COMPARISON OF 2011 AND 2013 BITCOIN BUBBLES

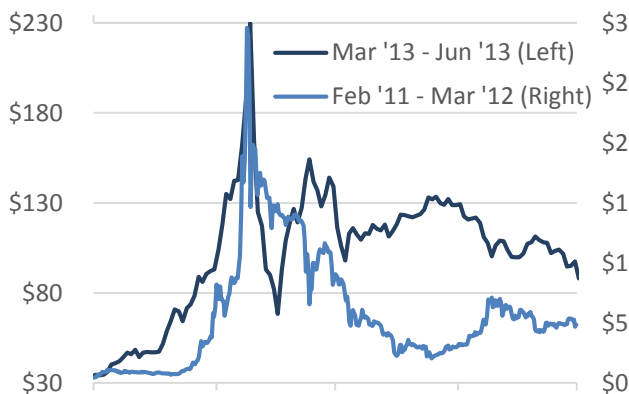


FIGURE 4 - LOGARITHMIC VIEW OF BITCOIN EXCHANGE RATE



Volume

USD-equivalent trading volume is 10x higher than it was in January.

Trading volume peaked in mid-April, reaching a high of \$72 million USD-equivalent and 848,000 BTC on April 12, across global exchanges. Since then, exchange volumes have subsided significantly, to approximately 50,000 BTC, or \$5 million per day. Interestingly, while daily BTC volume is less than double what it was on January 1, the USD-equivalent figure is approximately 10 times higher, meaning a significant amount of money has entered and remains in the market. As a result, global trading volume as a percentage of total market cap ended the first half of the 2013 at approximately the same level it started the year, despite the significant price gains.

FIGURE 5 - USD-EQUIVALENT VOLUME AT 10x JANUARY LEVEL

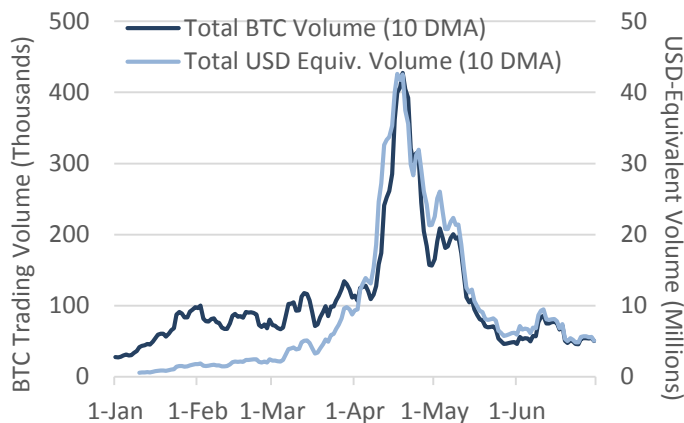


FIGURE 6 - DAILY TRADING VOLUME AS A PERCENTAGE OF MARKET CAP

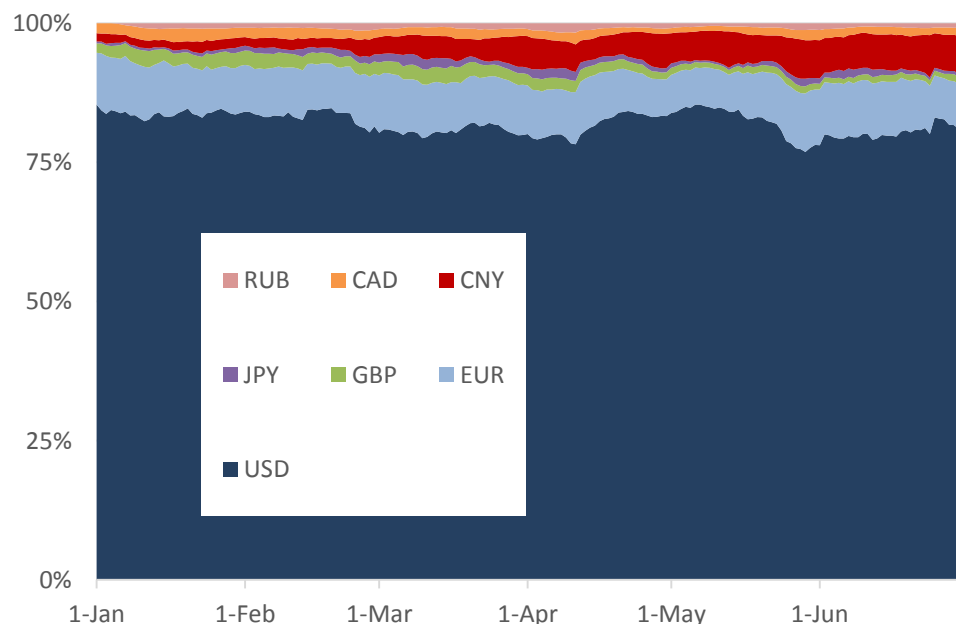


CNY's share of global trading volume has increased 600% this year.

The distribution of global trading volume across currencies has remained mostly consistent this year, with USD maintaining a dominant 80% share of the market and EUR trading at a distant second with roughly 8%. The one outlier in the global bitcoin trading story so far in 2013 has been CNY, with a meteoric rise from near obscurity at 1% in January to more than 6% of global volume at the end of June. This was largely attributable to a brief documentary about bitcoin aired on state-run CCTV. For more detailed overview of China's growth in the bitcoin market, we recommend the following:

- [China Climbs To Top Spot In Monthly Bitcoin Downloads](#)

FIGURE 7 - CURRENCIES AS A PERCENTAGE OF GLOBAL BTC TRADING

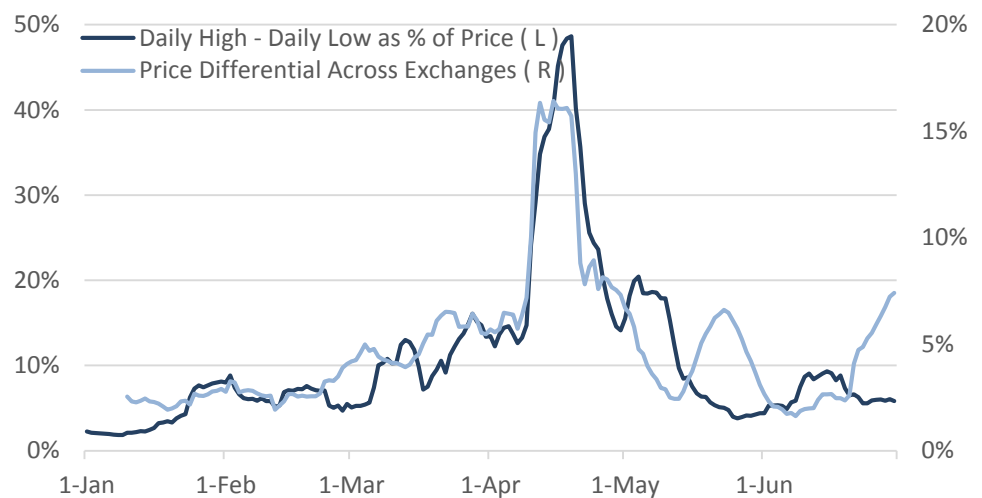


Daily volatility has doubled since the beginning of 2013.

Volatility

The drastic swings in bitcoin exchange rates remain elevated relative to traditional currencies. In fact, at a recent average of 5%, intraday volatility has roughly doubled since the beginning of the year. Though the price of bitcoin has continued to rise, it's day-to-day and intraday swings remain a significant barrier to its proliferation as a transactional currency unless merchants are prepared to swap it quickly to traditional fiat to avoid overwhelming rate exposure. While there are a number of vendors who provide that exact service for merchants, current bitcoin trading volumes prevent this from occurring on a mass scale.

FIGURE 8 - DAILY USD/BTC VOLATILITY VS. PRICE DISCREPANCY ACROSS USD EXCHANGES



Price discrepancies across exchanges create significant arbitrage opportunities for traders... if they're properly poised to take advantage.

While it may be detrimental for bitcoin's growth as a medium of exchange, the volatility has presented a number of exceptional arbitrage opportunities for traders. As macro events and news from different exchanges create unique trading dynamics, the price differential across exchanges can become quite significant. These differentials tend to trace volatility, with some exceptions for exchange-related events. For better or for worse, the difficulty and cost of setting up and funding accounts at multiple exchanges creates both a differential floor and a prohibitively expensive hurdle for smaller players. Accordingly, such differentials are likely to persist into the foreseeable future. For more info on such events, we recommend the following:

- [Turbulence at Mt. Gox Creates Arbitrage Opportunities](#)

As An Asset Class

Bitcoin has a long road ahead towards finding its place in the global macro environment. Yet, despite the fact that it remains a relatively immature asset class still subject to volatility, bubbles, and occasional manipulation, some correlations with other major financial assets are beginning to take shape.

Bitcoin's correlation with USD has directly inverted since June 19 when Ben Bernanke began to discuss tapering asset purchases.

As the first potentially viable, non-centrally issued currency, we were surprised to see a [remarkably high](#) correlation between BTC and the USD in June. As we noted at the time, bitcoin seemed to spend most of 2Q13 making gains during risk-off periods, serving as an alternative for those averse to the USD's susceptibility to inflationary central policy, despite its significant volatility.

That correlation flipped a full 180 degrees immediately after Ben Bernanke signaled that the Fed may begin to taper its \$85 billion per month asset purchases on June 20. From May 1 until that date, BTC and USD shared a 0.76 correlation. That correlation has since shifted to become almost completely inverse at -0.88 through mid-July. As a small market, bitcoin is still heavily influenced by individual micro events, but traders are clearly paying attention to major macro headlines as well.

FIGURE 9 - USD / BTC CORRELATION INVERTS FOLLOWING BERNANKE'S JUNE 19 TAPER MESSAGING

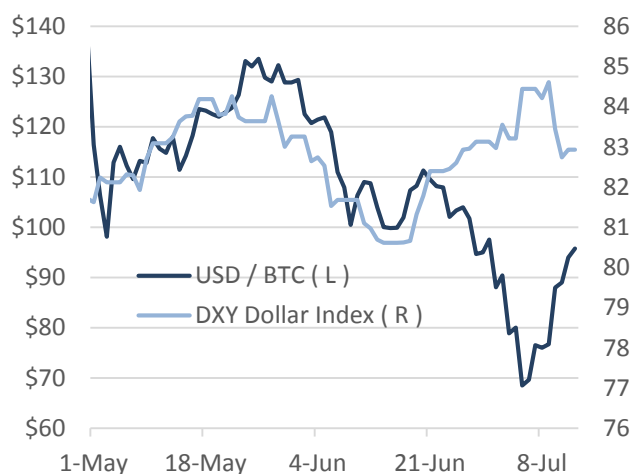
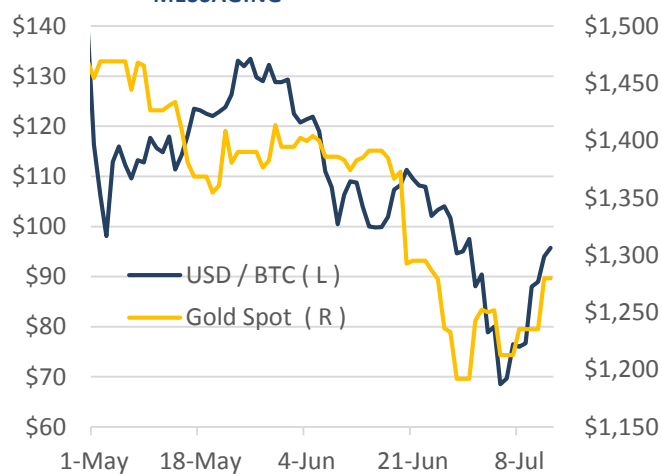


FIGURE 10 - GOLD AND BTC FIND CLOSE CORRELATION FOLLOWING BERNANKE'S JUNE 19 TAPER MESSAGING



Looking Forward

Micro news will continue to outweigh macro news until the bitcoin market achieves greater stability.

We expect micro news, particularly at exchanges, to continue to weigh heavily on market prices. With the tremendous infrastructure set to roll out during the remainder of the year (see the Entrepreneurs and Venture Capital section on page 12 of this report for more info), that trend will likely shift towards bitcoin maturing into a more defined role in the global financial environment, as we've seen start to develop over the past few weeks.

In particular, the trend of moving inversely with USD is likely to continue. Further discussions of Fed tapering, for example, should continue to put downward pressure on bitcoin prices. That inverse correlation remains subject to breaking on bitcoin-related macro news. One such scenario would be another Cyprus-like event where financial markets panic and rush to the safe-haven USD, while adoption for bitcoin as a means of subverting capital controls drives up BTC/USD rates simultaneously.

Cyprus-like events are becoming increasingly likely.

In particular, we are watching Greece, who has been consistently unable to meet debt reduction targets and remains at the whim of the ECB for continued solvency. We are also watching Italy, who was recently downgraded by S&P to BBB as their unemployment rate climbs above 12%. Similarly, Portugal's debt-to-GDP ratio has climbed from 108% to 124% already in 2013. The stipulations around a bailout for any of these countries may lead to a jump in bitcoin adoption amid financial unrest of the citizenry.

Bitcoin Exchanges

A focal point of regulatory, trading and investment news, bitcoin exchanges remain the center of the bitcoin universe. Exchanges serve as an entry point for many entering the bitcoin space, as well as the primary source of liquidity for those looking to adjust their positions.

Mt. Gox's mismanagement and susceptibility to attacks has reduced market stability.

The world of exchanges remains dominated by a small amount of legacy players, the most notable of which is Mt. Gox. Over the years, Mt. Gox has served an unquestionably vital role in the bitcoin ecosystem, but of late has been called into question for their ability to keep up with the massive increase in bitcoin's market size. Their technical infrastructure in the first half of 2013 made them susceptible to repeated denial of service (DDoS) attacks - a known tool for market manipulation. They've also faced a number of business and financial management setbacks, including the seizure of one of their US-based bank accounts by the Department of Homeland Security and a more recent freeze on all USD customer withdrawals. For more information on these topics, we recommend the following articles from earlier this year:

- [Have We Reached A Turning Point For Bitcoin Exchange DDoS?](#)
- [DHS Stops Dwolla From Servicing Mt. Gox Accounts](#)
- [Mt. Gox Withdrawal Freeze Driving Significant Liquidity Concerns](#)

A number of significant developments have occurred elsewhere in the bitcoin exchange market over the past six months. Regulatory issues (discussed further in the Regulatory Environment section beginning on page 21) have proven both a barrier to entry, as well as a potential increase in perceived legitimacy.

Exchanges Shutter

Numerous exchanges have closed in 2013 as a result of regulatory compliance issues.

Those concerns, as well as a series of others, have caused a handful of exchange closures since the beginning of the year. Bitcoin-24, one of the largest EUR/BTC exchanges halted operations in April after their accounts were closed by German authorities. Customers have since begun to receive funds from accounts held there. Similarly, New York-based Bitfloor had their account involuntarily closed, presumably due to regulatory matters, with many customers still awaiting the return of their funds.

European exchange Bitcoin Central halted operations in April after it was hacked and lost hundreds of BTC held in its accounts. It is expected to reopen soon. LibertyBit, Canada's second largest exchange before its closure, halted operations in April after their bank closed their account.

Stronger Entrants Emerge

The next wave of exchanges will be technologically superior and regulation-compliant.

Fortunately, a number of old and new entrants have stepped up to fill the gap from those closures with improved technology and compliance. Tradehill re-emerged in March after closing operations a year earlier. The revamped exchange will focus on larger players with accounts of \$10,000 or more and has dedicated significant resources to security and legal compliance.

Heavy venture funding will support upcoming exchanges.

We are also aware of three VC-backed exchanges currently in development. While we cannot disclose details this time, all three have expressed significant focus on technical security, capacity for high trade volume, and dedication to complete regulatory compliance. At least two of them are expected to be available for public use in the second half of 2013.

There are also a number of projects that will allow new entrants to more easily set up the technical aspects of an exchange. Buttercoin, an open source, high-volume trading engine, is available for anyone to build an exchange on top of. Similarly, bex.io is offering an out-of-the-box technical solution with a focus on security and performance.

Market Share Fluctuates

Mt. Gox's share of USD trading has fallen from 85% to 65% in 2013.

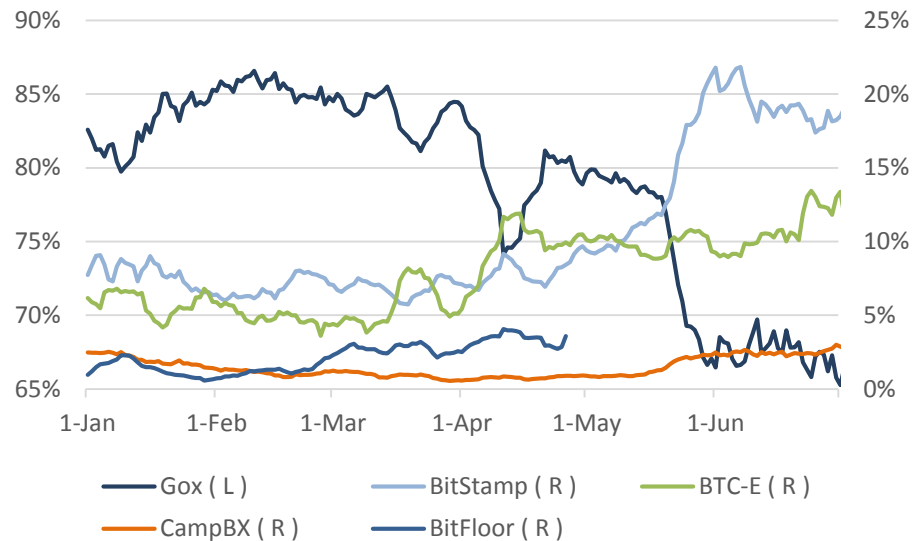
2013 has been a major step forward for the decentralization of USD trading volume across bitcoin exchanges, despite the loss of a number of companies. Mt. Gox's share of USD trading volume has fallen dramatically - from mid-80% in January to approximately 65% at June 30. Most of that has been picked up by BitStamp and BTC-E, which have roughly tripled and doubled their market share in 2013, respectively.

Mt. Gox's share of EUR trading has doubled in 2013 as a result of Bitcoin-24 halting operations.

EUR trading has seen quite the opposite so far this year. With Bitcoin-24 leaving the scene in April, Mt. Gox was able to nearly double its take of the market, rising to 80% in May. Since then, their share has dwindled somewhat as BTC-DE regained the 30% share it had at the beginning of 2013.

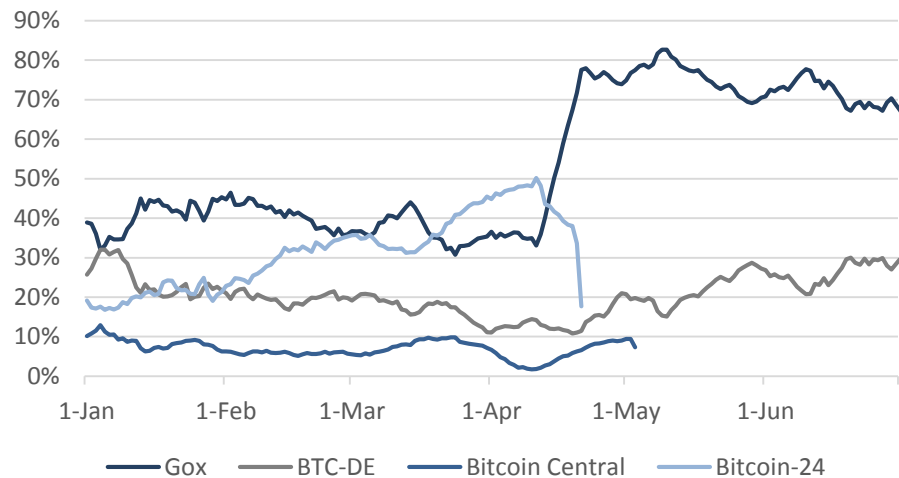
Mt. Gox continues to lose footing in the USD market.

FIGURE 11 - USD / BTC EXCHANGE MARKET SHARE BY VOLUME



After a series of key players leaving the market, Mt. Gox and BTC-DE absorbed their share of trading volume.

FIGURE 12 - EUR / BTC EXCHANGE MARKET SHARE BY VOLUME



Entrepreneurs and Venture Capital

VCs are new to bitcoin but enthusiastic about prospects.

Arguably the most exciting aspect of the bitcoin universe so far in 2013 has been the increase in new companies and products, as well as the venture capital backing them. The speed of growth in VC enthusiasm for bitcoin has been remarkable, summed up appropriately by Ribbit Capital's Nick Shalek when he stated, "we consider ourselves early investors in the space and our first investment was in March."

Bitcoin companies primed for next growth phase

Established companies have been the leaders in 2013 fundraising.

BitPay, a leading merchant processor for bitcoin payments, raised a \$510,000 seed round in January. The company quickly grew to 4,500 merchant customers with a transaction volume of \$5.2 million in April before closing a \$2 million round led by Founders Fund in May.

Y-Combinator backed Coinbase, a bitcoin consumer wallet and merchant processor, boasts more than 180,000 users and has grown from \$1 million of transactions in February to more than \$15 million in May, according to the company's blog. They recently raised \$6 million from top VCs including Union Square Ventures, Ribbit Capital, SV Angel, and Red Swan. In early July they began offering [instant bitcoin purchases](#) with a verified account.

BitInstant, a company that facilitates the funding of bitcoin exchange accounts is now processing \$7-10 million in transactions per month, according to CEO Charlie Shrem at a recent speaking engagement. BitInstant raised \$1.5 million in May in a seed round led by Winklevoss Capital.

In April, SecondMarket founder Barry Silbert and Tribeca Venture Partners combined for a \$500,000 seed investment in Coinsetter, a bitcoin trading platform offering margin trading, the ability to short bitcoin, and an exchange aggregator. Coinsetter is expected to launch in Summer 2013, according to CEO Jaron Lukasiewicz.

New entrepreneurs enter the space

Significant dry powder remains on the sidelines waiting to be allocated in bitcoin startups.

While the companies listed above are some of the most notable, it is not an exhaustive list. There are a number of stealth startups who have raised funding and are preparing to enter the scene over the coming months. There is also significant capital on the sidelines looking for the right bitcoin investments.

Liberty City Ventures, for example, launched a \$15 million digital currency fund and has yet to announce any allocations. Boost.vc, a startup accelerator in Silicon Valley, also recently announced that half of their next class is expected to be comprised of bitcoin companies.

Not to be overlooked is the recently formed BitAngels, a network of more than 100 angel investors across the globe with a specific focus on digital currency startups. They made at least one allocation to a proposed accelerator program in May, with an estimated \$18 million still waiting to be invested.

The Bitcoin Foundation continues to support bitcoin development through its new community grant program.

The Bitcoin Foundation has also allocated capital to two projects so far this year. Their grants generally go towards endeavors that are important to bitcoin's development, but may not be commercially viable. The first grant was for a new Testnet that allows for connected nodes to run an alternate blockchain on which new versions of Bitcoin can be tested. The second grant was given for a project that supported use of the first – a DNS seed that made it easier for Testnet nodes to connect to the network. Applications for 2Q13 grants were closed in mid-June, with winners expected to be announced soon.

Protocol Developments

Bitcoin blocks are 10 minute sets of transactions that serve as checkpoints in the block chain, bitcoin's transaction ledger. Bitcoin relies on all software versions reading the same version of this ledger in order to properly allocate bitcoins to addresses.

The v0.8 upgrade caused a forked block chain, resulting in bitcoin's first and only double-spend.

On February 19th the v0.8 upgrade to bitcoin-qt, the standard bitcoin client, was released. This resulted in miners using v0.8 building on a separate block chain from pre-v0.8 miners, effectively making two parallel ledgers.

There are significant consequences to a hard fork like the one described. It is possible that transactions would not match identically between the chains, causing discrepancies depending on which chain was being viewed. In the case of v0.8, 60% of the network mining power was using the v0.8 software, making it the dominant chain.

Users of the v0.8 software would see this longer chain, while users of pre-0.8 software would reject it and see the separate shorter chain as the dominant one. If the pre-0.8 chain were longer, both versions of the software would observe the same dominant chain. Therefore, anyone using pre-0.8 software would potentially see different transactions than users of 0.8.

The bitcoin community acted quickly and cohesively to reverse the effects of the error.

When the issue was identified, an emergency alert was sent to suspend all transactions until the fork could be resolved. The operators of BTCGuild and Slush, two of the largest bitcoin mining pools, downgraded to v0.7, allowing that fork to gain a majority of the mining power. Both of these pools gave up all blocks they had discovered before the switch in order to maintain the integrity of the network at their own expense.

Gavin Andresen, lead developer for bitcoin, commented at a meetup in DC that he was impressed with the selflessness of these pools, which bodes well for similar crises in the future. Additionally, infrastructure and an alert system are being put in place that would automatically identify when a side fork is gaining significant length - a strong indicator of an accidental hard fork.

This event also created the first intentional double-spend in bitcoin history. A user was able to use a modified version of the protocol to double spend the equivalent of \$10,000 worth of bitcoins going to payment processor OKPay. This attack can only be performed in the rare

event of a hard fork like the one that occurred in March, and should not be considered a general vulnerability in the protocol.

Additionally, it appears the double spend occurred more as an experiment than a malicious attack. This risk can be mitigated through automated systems that detect hard forks and stop accepting transactions until they can be resolved.

While this hard fork did highlight the ability of a decentralized system to act quickly and in a coordinated manner, it also underscored concerns over the consolidated control of the network's mining power. It became clear that a few pool operators have control over a majority of the network's power. These operators have not done anything that would draw question to their integrity, however it does create a degree of security risk going forward. We recommend the following article for further reading on hard forks:

- [The 51% Attack – What We Can Learn From Alt-coin Experiments](#)
- [Go Fork Yourself – Life After a Bitcoin Hard Fork](#)

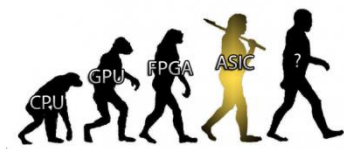
Looking Forward

V0.9 will bring significant merchant-friendly features to the bitcoin protocol.

In the coming months, v0.9 of the protocol will be released and a new feature should significantly increase merchant and customer usability. The key improvement is using payment messages between via http/https specifying the amount to be paid and a description of the transaction.

This will significantly improve the ease of merchant initiated transactions, allow for recurring payments with proper software, create signed receipts which can be used for dispute resolution, and enable immediate-feedback transactions that can reduce the overhead use of blocks for transaction messages. We recommend the following article for a detailed analysis of the forthcoming updates:

- [Significant Merchant Improvements Planned for Bitcoin v0.9](#)



Mining Update

Rise of the ASIC

The inevitable has happened. When bitcoin first launched in January 2009 central processing units (CPUs) were used to mine blocks, and after some refinement were able to get 20-40 MH/s (megahashes per second). Hashes are the basic computational component in bitcoin mining that is used to determine whether a miner has discovered a block.

Mining speed is measured in hashes per second, with 1 MH/s corresponding to 1 million hashes per second and 1 TH/s corresponding to 1 trillion hashes per second. The more hashes a miner is able to create, the more likely they are to find a block and be rewarded with newly issued bitcoins.

ASIC hardware has made all previous equipment obsolete in a matter of months.

By the end of 2010, software enabling graphics processing units (GPUs) to mine blocks was beginning to gain traction. In mid-2011, graphics cards were able to get 300-400 MH/s, and made mining bitcoins by CPU obsolete. It was clear that ASICs (application specific integrated circuits - customized hardware that can only serve one purpose such as mining blocks) was going to be the end game and eventually dominate mining. They are significantly more efficient than hardware which is repurposed for mining such as CPUs and GPUs. We recommend the following article for further reading:

- [The Evolution of Mining](#)

Throughout 2012, several companies began developing ASIC chips for bitcoin mining, and by early 2013 they began shipping to customers. Just as GPUs made CPUs irrelevant, it appears it will not be long before GPUs suffer the same fate from ASICs. Three companies started shipping ASIC products to customers this year: ASICMiner, Butterfly Labs (BFL), and Avalon.

ASICMiner

ASICMiner is a publicly traded company based in China. Of the 400,000 shares available, 163,962 are publicly traded while the rest are held in reserve by the issuer, Bitfountain. Shareholders are entitled to 100% of profits, minus withholdings for reinvestment in products. Share ownership is directly tied to bitcoin addresses, and weekly dividends from mining and hardware sales are paid directly to the owner's address.

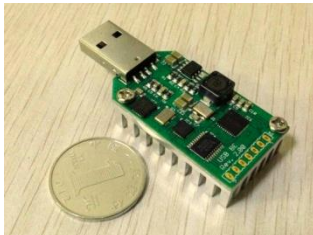
10 GH/s ASICMINER BLADE



ASICMiner's goal is to maintain 20% of the bitcoin network's speed, while selling any extra hardware on the open market. They have been the only ASIC manufacturer to have products available to ship immediately upon payment. This is starkly contrasted with their competitors BFL and Avalon who have opted to pre-sell all orders before shipping, causing customers to wait 3-12 months before receiving products.

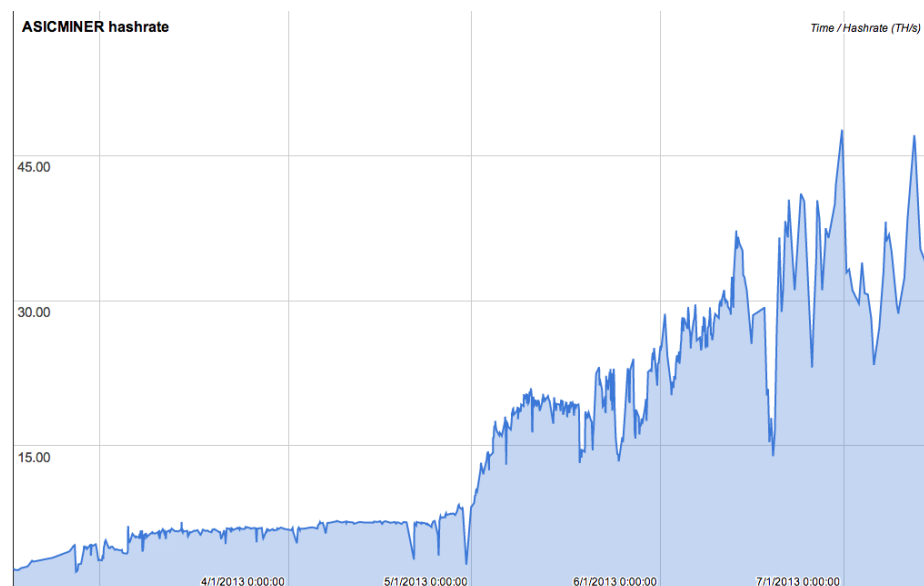
ASICMiner sells two versions of their miners, both of which use the same ASIC chips. The ASIC blades run at 10 GH/s, and were initially auctioned in lots before being sold for a flat rate of 50 BTC. The blades were recently discontinued while a new version is developed. Additionally, ASICMiner sells USB devices that mine at 330 MH/s for 0.89 BTC each.

330 MH/s USB MINER



Friedcat, CEO of ASICMiner, reported that the first miners began hashing on February 14th, 2013 at an initial speed of 2TH/s. Since then, ASICMiner has continued to add capacity up to the currently estimated 40 TH/s. Despite the network's large increase in speed over the last few months, ASICMiner has continued to maintain their targeted 20% of the network, which has contributed approximately 0.013 BTC/share to their weekly dividend. Total dividend distributions since February 28th have been 0.386 BTC per share.

FIGURE 13 - ASICMINER HASH RATE SINCE FEB 2012 (VIA ASICMINERCHARTS.COM)



\$5K invested in the ASICMiner IPO would be worth \$2M today – less than a year later.

The initial ASICMiner IPO was in August 2012 and sold in lots of 5,000 shares for 0.1 BTC each, raising over \$100,000 for initial ASIC production. As of this writing, shares are trading at 4.25 BTC each, providing initial shareholders a 4,250% return in 8 months and netting IPO investors millions of dollars in gains.

There are currently three methods of exchanging shares: the bitcointalk.org forums, BitFunder, and BTC Trading Corp (BTCTC). Share value tracks similarly across exchanges, however they differ on the methods of trading. Bitcointalk.org users trade shares person to person and require Friedcat to manually transfer the shares to a new address. BitFunder and BTCT Co hold shares and allow users to virtually trade them instantly through their websites. ASICMiner was added to BitFunder in February and to BTCTC in March.

Butterfly Labs

Butterfly continues to suffer significant delays, but began shipping their 2012 pre-orders in June 2013

BFL, based out of Leawood, Kansas, began taking pre-orders for ASIC miners on June 23, 2012. They decided to use a 65nm design, compared with ASICMiner and Avalon's 110nm design. This will ultimately provide a more powerful chip, however it adds significant complexity to design and manufacturing costs.

BFL suffered 10 months of production delays, continuously telling customers they were two weeks away from production. By early June 2013 they began shipping small quantities of product and completed shipping 5 GH/s units from June 2012 pre-orders by June 5, 2013 – nearly a full year after the initial orders were placed.

BFL PRODUCT LINE OVERVIEW

Product	Price
5 GH/s Miner	\$274
25 GH/s Miner	\$1,249
50 GH/s Miner	\$2,499
500 GH/s Miner	\$22,484

BFL offers 4 lines of product in varying ranges of speed. Product speeds and prices have been revised several times since initial pre-orders were announced. Current product offerings are shown in the table on the left.

Additionally, Butterfly labs offers bulk chip sales, allowing distributors to purchase large quantities in order to redistribute to customers. In order to use these chips, custom printed circuit boards (PCBs) must be designed and manufactured, and then the chips must be set. This option was introduced about 1 month after Avalon announced the same product line. The 4 GH/s chips are sold for \$75 each, and in minimum quantities of 100.

AVALON'S 60 GH/s BITCOIN MINER



Avalon

Avalon initially entered the market to prevent Butterfly Labs from being the sole supplier of ASIC chips. In September 2012, Avalon announced an initial test batch of 60 GH/s miners, with a production quantity of 10 units. These first publicly available ASICs were shipped in February 2013 to much excitement.

Pre-orders for large-scale production began on September 23, 2012 for \$1299 with an initial batch size of 300 units. Shipments of these began arriving on March 3rd, 2013 and returned their value back after only a few days of mining. Resale of these miners sold for 10-20x their initial costs, and Avalon priced later batches to better capture fair value.

Two later batches of 600 units have been pre-sold for 75 BTC each, however, despite shipping estimates of April and May, neither has been shipped to customers yet. To better capture the value of the units, pricing was placed at an estimated 30 days' worth of mining. Due to significant increases in network difficulty in recent months, the break-even period on these units will likely be dramatically longer by the time they reach customers.

Avalon also offers bulk sales of ASIC chips. The 282 MH/s chips are sold in lots of 10,000 units for 0.78 BTC each. Pre-orders for these chips began in mid-April, and with the projected 9-10 week lead time they should start arriving at distributors within the next few weeks. These require designing and manufacturing boards before they can be used. We recommend the following article for further reading:

- [10,000s of Avalon ASICs Set to Rival ASICMiner in July](#)

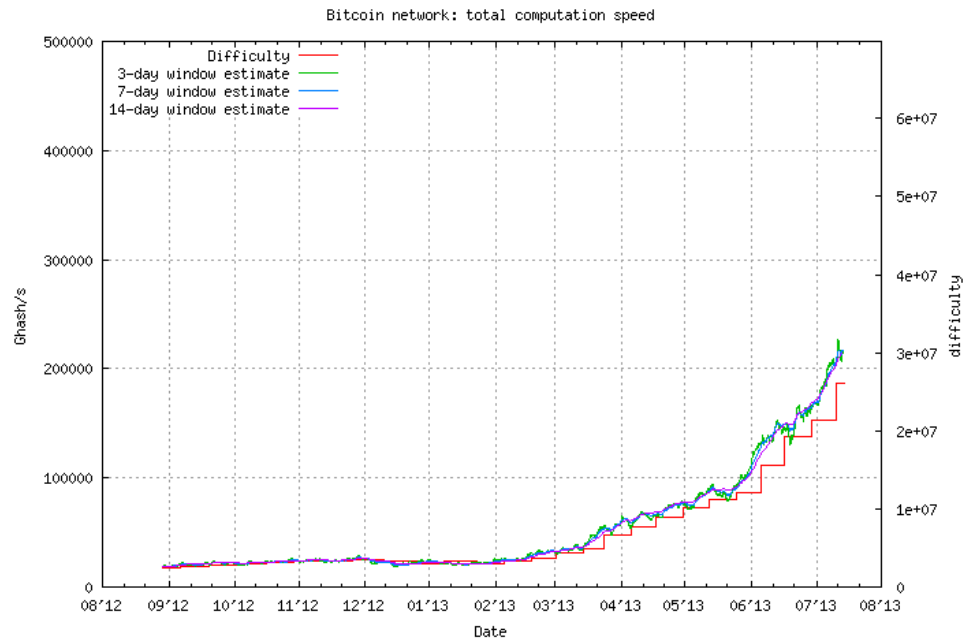
Network Speed and Hash Rate Distribution

The bitcoin network is growing at record speeds – a trend that is expected to continue.

The period from March to June 2013 saw the most rapid network speed increase in bitcoin history, breaking 100 Terrahashes/second (TH/s) in May, making it more powerful than the [top 500 supercomputers combined](#).

Bitcoin mining network speed plateaued for several months going into 2013, with relatively static speed between November 2012 and February 2013. This changed dramatically at the end of February when ASICMiner and Avalon began bringing their ASIC hardware online. Since mid-February, the network hashrate increased 900% from 25 TH/s to over 225 TH/s, leading many GPU miners to seek better returns with other digital currencies.

FIGURE 14 - NETWORK SPEED AND DIFFICULTY SINCE SEPTEMBER 2012
(VIA BITCOIN.SIPA.BE)



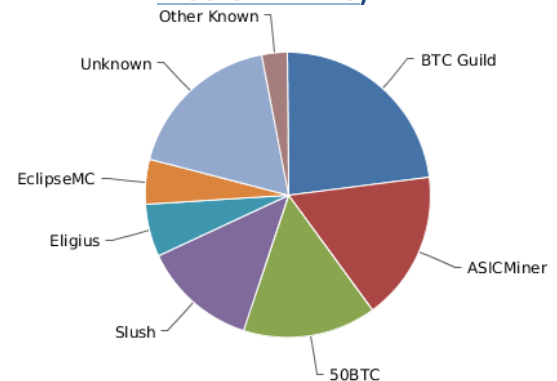
Despite near-majority computational power, mining pools continued to act in the interest of the network.

Centralization of mining power is a continuous concern within the bitcoin community because of the increased risk of a 51% attack, allowing for double-spends and other security compromises. There were several scares as BTC Guild, the largest mining pool, approached 50% of the network speed in March and April. It would be self-destructive to perform a double spend, since the security and value of the currency would be compromised, so it is not surprising to see that no attacks were made.

ASICMiner began solo to help distribute mining power.

A vast majority of BTC Guild's speed was due to ASICMiner using their pool. After the 50% scare ASICMiner began distributing some of their power to BitMinter to reduce centralization. Towards the end of May ASICMiner began solo-mining, which has resulted in the most decentralized mining network in several years, as shown on the chart on the right.

FIGURE 15 - MINING POOL NETWORK SHARE (VIA BLOCKCHAIN.INFO)



Regulatory Environment

Arguably the most important question surrounding bitcoin is the way it will be addressed by governmental regulators. Its use for illicit online transactions and its unregulated trading environment have led many to question the future hurdles faced by bitcoin companies. For better or for worse, the first six months of 2013 saw a number of important developments that clarified answers to these questions.

US Offers Guidance, Prosecutes Violations

FinCEN issues guidance – bitcoin exchanges are money transmitters.

In March, the Financial Crimes Enforcement Network (FinCEN - a division of the US Department of the Treasury) issued [guidance](#) clarifying that bitcoin exchanges are considered Money Transmitters and are required to obtain all proper licenses to conduct business in the US. That process is comprised of registration as a Money Service Business (MSB) not only at the federal level, but with each state in which a company wishes to conduct business as well - a process costing millions of dollars and generally taking more than a year to complete.

Many companies have not wasted time earning compliance, despite the significant cost.

A number of companies have already begun to successfully navigate these regulations. BitInstant has licenses in nearly 40 states and Tradehill partnered with MiiCard, an online identity service that aids in anti-money laundering (AML) and know your customer (KYC) data collection - core components of regulatory compliance.

In May, Mt. Gox lost a key payment processing partner when the Department of Homeland Security seized their account for improper registration as an MSB. While the fate of the account and the funds it contains remain unknown, the company has since filed for registration with FinCEN.

Regulators have actively prosecuted virtual currency operators who violate of anti-money laundering policies.

Also in May was an indictment of the founders of Liberty Reserve by US regulators, issuers of a centralized virtual currency allegedly responsible for laundering \$6 billion. While not directly related to bitcoin, and fundamentally quite different from a technical standpoint, it led to a number of concerns about bitcoin's future relationship with the US government. This was mitigated somewhat during the related press conference when regulators reminded the public that virtual currencies may play a vital role in payment innovation and that those following the rules have nothing to worry about.

While there has been widespread concern that bitcoin miners may be considered money transmitters per the guidance offered by FinCEN, it is the opinion of this firm that miners do not currently constitute money

transmitters. The cause for this concern is the clarification by FinCEN that creators of decentralized virtual currencies would fall under the money transmitter definition. While not an uncommon confusion, bitcoin miners do not actually create new bitcoins, but are merely the initial recipients of primary issuance.

In June, California's Department of Financial Institutions ordered a cease and desist notice to the Bitcoin Foundation to prevent them from continuing any activity as an unlicensed money transmitter. The Bitcoin Foundation is a non-profit organization dedicated to the standardization, protection and promotion of bitcoin. You can read their response to the order [here](#).

Non-US Governments More Accommodating

Canada and Europe show signs of greater accommodation, relative to the U.S.

The US has unquestionably been the least accommodating with regards to virtual currency regulations. Throughout the rest of the globe, government responses have ranged from deferment to outright encouragement so far this year.

FINTRAC, the Canadian equivalent of the US' FinCEN, sent a letter to a number of Canadian exchanges in May stating that they were not engaged as a money service business and are not currently required to register. The UK's HMRC sent a similar letter to an exchange in June, stating that they do not currently have to register, but that may change in the future. Germany has also seen greater accommodation, with capital gains taxes on bitcoins held for more than twelve months eliminated and Fidor Bank AG partnering with a German bitcoin exchange.

Looking Forward

The second half of 2013 should provide further clarification on bitcoin's place within regulatory frameworks. Most notably, the IRS and CFTC may take more concrete action than they have to date.

In May, the US Government Accountability Office encouraged the IRS to post official guidance on tax compliance related to virtual currencies. The time and cost of investigating what is still a small market may delay action from the IRS, but as bitcoin continues to grow it is likely specific tax rules will be outlined.

Expect further intervention from regulators if bitcoin continues to grow, particularly with regard to taxes and derivatives trading.

Similarly, bitcoin remains free of notable trading regulations within the US. While the global foreign exchange market remains largely unregulated, FX derivatives in the US generally fall under the watch of the Commodities Futures Trading Commission. One of the CFTC commissioners acknowledged virtual currency trading in May - we would not be surprised to see CFTC intervention if heavy bitcoin derivatives trading evolves, though that is unlikely before the end of the year.

The SEC saw its first official exposure to bitcoin with the recent S-1 filed by the Winklevoss twins for a bitcoin ETF. The proposed instrument has been the subject of much discussion, but its fate remains in the hands of the regulators reviewing the registration documents. For more info about the ETF, we recommend the following:

- [A Bitcoin ETF Is A Vital Step Towards Market Maturity](#)

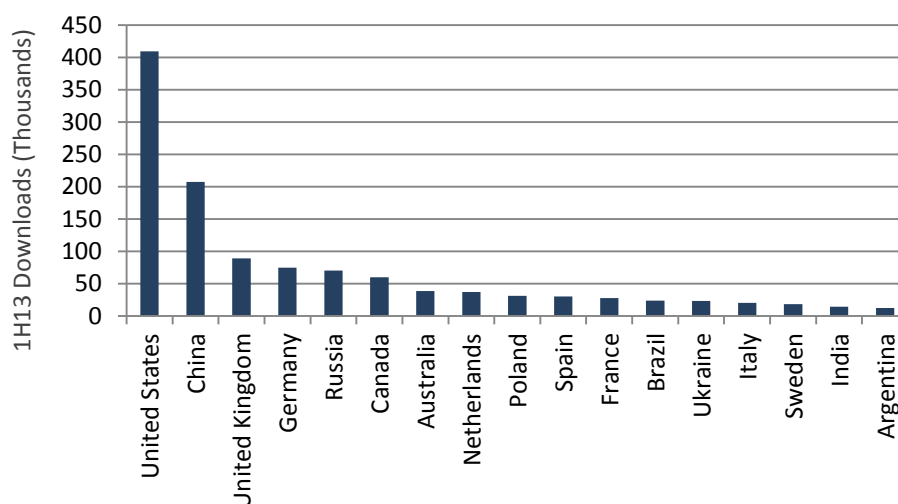
Global Adoption

The US remains the #1 downloader of the bitcoin client, with China rising to #2 from #5 so far in 2013.

One of bitcoin's greatest appeals is its ability to financially connect anyone in the world with an internet connection available. As bitcoin has exploded in popularity over the past six months, a number of telling patterns are beginning to emerge.

The bitcoin client was downloaded more than 1.5 million times between January and June, representing 48% of the 3.4 million total downloads over bitcoin's four and half year existence. The US remains the standout leader in downloads, crossing the 1 million mark in June, though China has been closing that gap, particularly in the second quarter of this year.

FIGURE 16 - TOP BITCOIN CLIENT DOWNLOADS IN 1H13



Chinese presence increases

Of the 50 countries with the most downloads going into 2013, China saw the largest increase at 207%.

At the beginning of the year, China claimed just over 5% of all-time downloads, but has since climbed to more than 9% after peaking in May at 29% of global downloads for the month. The new superpower fell to 10% of global downloads in June, but CNY trading volume remains at elevated levels, as illustrated on page 5 of this report.

While China sits at the top of the list for greatest increase in bitcoin downloads in 2013 with a 207% increase driven by implicit promotion from the state, bitcoin has also seen adoption elsewhere for its ability to circumvent government.

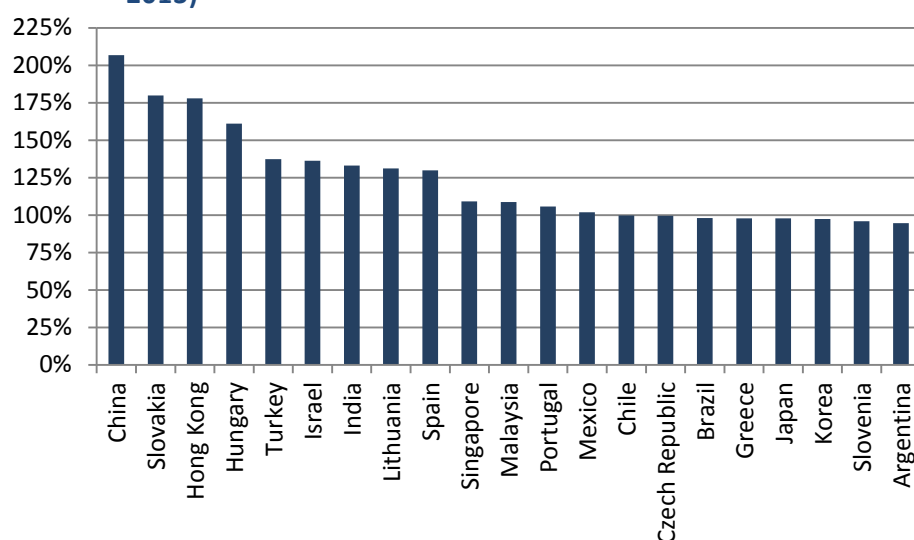
Spain, Portugal, and Argentina are among the top increases in bitcoin adoption amid fears of capital controls.

Capital controls drive interest

Also near the top of the list for greatest increase in downloads are Portugal and Spain, with gains of 106% and 130%, respectively - likely a result of the capital controls instituted in Cyprus earlier this year.

A similar situation is currently developing in Argentina, where significant inflation and restrictions on capital flows are forcing citizens to look for financial freedom through alternative currencies. In January, 0.5% of global bitcoin client downloads were in Argentina. By June, that number more than doubled to 1.1% and that adoption rate has already more than doubled again, with Argentina responsible for 2.6% of global downloads in the first two weeks of July.

FIGURE 17 - TOP INCREASE IN DOWNLOADS IN 1H13 RELATIVE TO PREVIOUS ALL-TIME DOWNLOADS (OF COUNTRIES IN TOP 50 ALL-TIME DOWNLOADS BEFORE 2013)



Emerging markets seek alternatives

Africa and other emerging markets may lead need-driven adoption of bitcoin.

Not to be overlooked are the recent developments in Africa. Earlier this year we explained why Kenya was [primed for wide-scale bitcoin adoption](#), noting the country's high mobile penetration, government corruption, inflationary concerns, remittance costs and widespread use of mobile payment system M-PESA. In the last week, an immense amount of coverage has been given to Kipochi, a bitcoin wallet that allows users to purchase bitcoin with M-PESA and transact with negligible fees.

Looking Forward

Cyprus may have been a template not just for bail-ins, but for bitcoin adoption as well.

Over the next six months we expect the United States to continue hold the top spot in bitcoin adoption. The overwhelming investor interest and entrepreneurial vigor is likely to continue to trump the regulatory hurdles. Moreover, the recent controversy surrounding the NSA's invasive programs is leading US citizens to seek options to protect their privacy. While that is becoming increasingly difficult with bitcoin as a result of FinCEN regulations, it is certainly still possible.

Bitcoin will also serve where it is needed most, helping global citizens circumvent capital controls, uncontrollable fiat inflation, and overwhelming counterparty risk presented by banking institutions. In particular, such events are likely to continue in Argentina, with an increasing probability of Cyprus-like events occurring in Greece, Italy and Portugal for the reasons listed in the Trading Update on page 8 of this report.

An SEC registered product offering exposure to bitcoin is unlikely to be available for the foreseeable future.

From the investment side, we do not foresee bitcoin being widely adopted by institutional players on a large scale over the coming months. Total market capitalization remains well below a level of interest for a major bank or most hedge funds to invest the resources required to understand digital currencies, a necessary step before allocating capital. That said, we expect more and larger retail players to enter the space, helping the value of the market continue to grow steadily. An SEC-registered bitcoin ETF like the one proposed by the Winklevoss twins may help in that regard, but the probability of such a tool being ready for use before the end of the year is extremely low.

Notable Events

The bitcoin community witnessed and participated in a number of important events in 2013. With multiple conferences, lawsuits and community developments, bitcoin news has been filled with important updates.

Bitcoin steps offline

Passionate enthusiasts continue to drive discussion at real world events.

In May, more than 1,000 bitcoin enthusiasts gathered in San Jose, California for Bitcoin 2013. The event featured presentation from bitcoin's core developers, major investors and leading entrepreneurs, as well as a host of panels on regulatory and technical topics. The event also featured a hackathon won by BitWall - a paywall for online content that capitalizes on bitcoin's low fee structures to facilitate seamless micropayments. For more information about the event, we recommend [our overview](#) as well as YouTube, where all of the speeches and panels are available for viewing.

In early July, Bitcoin London gathered together an impressive collection of investors and entrepreneurs for discussions on the economy, regulatory concerns, venture capital and merchant opportunities. The event was held in the legendary Canary Wharf - the heart of London's financial community. Video of the event will be posted online soon. You can also read our coverage of key panels for more info:

- [Bitcoin London - Regulatory Panel Review](#)
- [Bitcoin London - Venture Capital Panel Review](#)

All is not well in the state of bitcoin

In May, Coinlab filed a \$75 million lawsuit against Mt. Gox for failure to uphold an agreement signed in 2012. The agreement gave Coinlab exclusive rights to handle Mt. Gox's North American clients. According to the lawsuit, Mt. Gox never turned over the necessary materials required to facilitate the transition, such as access to client account information. Litigation in this case is ongoing.

A new leader emerges

The Bitcoin Foundation has a new Executive Director and seats open for nominations.

Peter Vessenes announced he was stepping down as Executive Director of the Bitcoin Foundation. Days later, Jon Matonis - a writer for Forbes who is well known in the bitcoin community - has since taken his place to help guide the bitcoin community in this important, albeit unofficial role.

This document has been prepared in good faith on the basis of information available at the date of publication without any independent verification. The Genesis Block (TGB) does not guarantee or warrant the accuracy, reliability, completeness or currency of the information in this publication nor its usefulness in achieving any purpose. Readers are responsible for assessing the relevance and accuracy of the content of this publication. TGB will not be liable for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on information in this publication.