Bitcoins and Banks

Problematic currency, interesting payment system

Equities

Global
Banks

Derek De Vries, CFA
Analyst
derek.devries@ubs.com
+1-212-713 4290

John-Paul Crutchley
Analyst
john-paul.crutchley@ubs.com
+44-20-7568 5037

Jack Hwang
Associate Analyst
jack.hwang@ubs.com
+1-212-713 0000

Ivan Jevremovic
Associate Analyst
ivan.jevremovic@ubs.com
+44-20-756 76171

Bitcoin: The first widespread implementation of a digital currency

Bitcoin, a decentralized digital currency created in 2009, is the first such currency to gain relatively widespread adoption. Unlike traditional currencies, which rely on central banks, Bitcoin relies on a decentralized computer network to validate transactions and grow money supply. Each Bitcoin is effectively a (divisible) unit which is transferred between pseudonymous addresses through this network.

Bitcoin faces economic, technical and regulatory challenges as a true currency

Bitcoin's speculation-driven volatility prevents it from being a stable store of value or unit of account, and its semi-fixed supply exacerbates volatility and deflationary pressure. As a means of exchange, it already consumes vast computing resources for relatively few transactions and faces scaling difficulties. Bitcoin also exists in something of a regulatory vacuum, or in some jurisdictions it is restricted or outright banned (e.g. in China, Russia) – which can be damaging to trust and sentiment.

Bitcoin poses limited threats to banks

The two main threats that Bitcoin poses to banks are disintermediation and competition over transaction fees. For disintermediation, widespread bank insolvency and/or deposit taxes and levies could drive customers to use Bitcoin in lieu of traditional bank deposits. In the case of transaction fees, if Bitcoin transaction fees are consistently lower than existing fees, banks may see increased competition in this space. We do not regard either of these threats as real, given Bitcoin's limited viability as a currency.

Banks could repurpose the underlying technology to improve payment systems

Setting aside its political agenda, we see Bitcoin as having some potential as a new transaction technology, where a bitcoin-like technology could provide a basis for a new shared payments and transfer system using existing currencies and securities. Such a system could reduce systemic costs, and provide faster, secure, transfers – particularly in the international arena. However, given the status quo and the lack of any clear incentive for developing such a network, we do not see banks developing this any time soon.

Contents

Derek De Vries, CFA
Analyst
derek.devries@ubs.com
+1-212-713 4290

John-Paul Crutchley
Analyst
john-paul.crutchley@ubs.com
+44-20-7568 5037

Jack Hwang
Associate Analyst
jack.hwang@ubs.com
+1-212-713 0000

Ivan Jevremovic
Associate Analyst
ivan.jevremovic@ubs.com
+44-20-756 76171

Executive summary

Every successful product fills a need in the marketplace. In our view, Bitcoin, while innovative, fails to fulfil most banking needs better than the current alternatives. As we see it, Bitcoin's only realistic prospect in the long term is as a money transfer system.

What is Bitcoin?

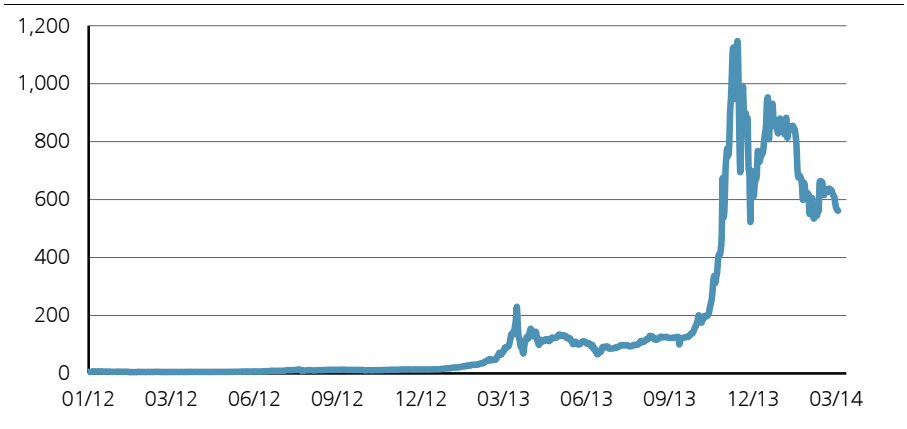
A novel form of electronic money that is based on a decentralised network of participating computers

Bitcoin is a novel form of electronic money that is based on a decentralised network of participating computers. It has no physical counterpart; it is merely arbitrary (divisible) units that exist on this network. There is no central bank; the system has a pre-programmed money supply that grows at a decreasing rate until reaching a fixed limit. There are no interest rates. Each user of Bitcoin merely has an address (like an email address) through which to make and receive transactions, making Bitcoin pseudonymous.

The crucial aspect that makes Bitcoin work is that it solves the double-spending problem without relying on a central authority. In other words, it is possible to send a Bitcoin securely, without then being able to spend that Bitcoin again, without someone else being able to forge a transaction, and also without your being able to claim that Bitcoin back (i.e. a chargeback).

These transactions get recorded in a decentralised ledger (known as the blockchain), which is maintained by a network of computers (called 'miners'). Miners maintain consensus in the blockchain through solving difficult mathematical problems (known as hashes), and are rewarded with Bitcoins and optional (voluntary) transaction fees. These rewards are the mechanism that increases the Bitcoin money supply. We give a more detailed description in a dedicated section later.

Figure 1: Coindesk Bitcoin Price Index (USD)



Source: Coindesk.com

The past and future trials and tribulations of Bitcoin

Excessive volatility – more like a virtual commodity than a currency

Our strategy team has already highlighted the bubble-like nature of Bitcoin and some of the issues it faces (*Weight Watcher: Where are the asset bubbles?*, 20 February 2014). We examine some of the problems facing Bitcoin in detail in the in-depth section later. Bitcoin has seen a rapid price rise and subsequently suffered excessive volatility, which we see as being driven by sentiment and speculative demand on a semi-fixed supply – more like a virtual commodity than a currency.

However, Bitcoin lacks many of the features of a commodity, not least of which is an independent physical presence. The oft-mentioned 'network effect' only really amounts to speculation unless Bitcoin actually functions well as an alternative currency.

Bitcoin struggles as a stable store of value and unit of account…

In principle, Bitcoin works very well as a sort of secure digital token system – 'cowrie shells in the sky'. However, as a stable store of value and unit of account, Bitcoin clearly struggles, and there is no obvious remedy given the impossibility of regulating the money supply to stabilise Bitcoin-denominated prices. As well as breeding volatility, even in an optimistic scenario this provokes deflationary pressure. This problem is compounded by the lack of a real 'Bitcoin economy'.

…and faces technical and practical problems

Bitcoin also faces several technical and practical problems. Amongst these are scaling difficulties – Bitcoin already consumes vast quantities of computing power to run a network that handles less than one transaction per second (vs thousands per second for Visa, for example). Despite the theoretically decentralised nature of mining, miners can group together in pools, and if one pool controls over 51% of the computing power it can destroy Bitcoin. The 10-minute transaction confirmation window can also impede small transactions, and creates scope for double-spending fraud. Some of these are merely technological issues that can be fixed by alternative digital currencies or systems – which in itself is a threat to Bitcoin.

The IRS has announced its decision to treat Bitcoin as a capital asset…

Finally, while Bitcoin and other virtual currencies operated in a relatively unregulated environment, various regulators have begun taking positions. Most recently, following the footsteps of Japan, the Internal Revenue Service announced its position of treating Bitcoin as a capital asset instead of currency. This treatment results in a reporting and compliance burdens that will likely deter users from typical retail transactions, thus further damaging Bitcoin's potential as a currency. It is notable that the IRS announcement only addresses the U.S. government's position from a tax revenue perspective and does not represent an endorsement or critique of the underlying products.[1]

… but consumer protection regulations remains to be seen after some users experienced substantial losses.

Regarding substantive regulation of Bitcoin, it remains to be seen what position financial regulators will take on Bitcoin. Recent events where users experienced significant losses could incentivize regulators to move quickly on it in the interests of consumer protection. One clear example of such loss is the recent bankruptcy of Mt Gox, one of Bitcoin's oldest and largest exchanges (for exchanging Bitcoins and fiat currency). Mt Gox had been experiencing problems for months, so its bankruptcy was not a total surprise – and crucially, Mt Gox's failure does not impact the rest of the Bitcoin system, in that the network is unaffected and Bitcoin transactions can proceed as normal. However, Mt Gox users who have lost their Bitcoins and fiat money have so far been left out in the cold. This harms sentiment and impedes Bitcoin's ability to take off as a currency (given that most users acquire their Bitcoins through purchase with fiat currency, and would prefer to store them on a third-party wallet for convenience). However, it does not represent a systemic failure in Bitcoin's technology (as evidenced by the continued operation of other large exchanges).

[1] Put differently, just as the IRS taxes income from illicit drug dealings, the substantive regulation falls under the authority of a separate agency.

Bitcoin is unlikely to pose a serious threat to banks

No reason to believe that banks will face increased competition for savings…

From the perspective of a banks analyst, the primary threat of a new currency would lie in its potential to cause disintermediation from banks. However, since Bitcoin's value is far less stable than traditional bank deposits, and given that the current Bitcoin structure fails to compensate savers with any interest, there is no reason to believe that banks will face increased competition for savings. In principle, consumers could adopt Bitcoin in greater numbers if the existing financial system comes under stress (and e.g. deposit taxes are levied), but in that case banks would be in trouble by definition anyway. Bitcoin also currently lacks developed financial products in a meaningful way (e.g. credit, derivatives etc). Given its limited market cap (c.$13bn at peak) and the operational risk involved, this seems to pose few opportunities or threats to banks.

…or transaction fees (unless Bitcoin's value stabilises in the longer term)

A secondary threat would lie in Bitcoin's ability to compete for credit card and transaction fees. In the short to medium term, we see no serious threat in this space, as Bitcoin's value has proven too volatile. Bitcoin customers would effectively be taking on massive currency risk with little to no compensation for this risk. In terms of the actual fee levied on transactions, Bitcoin remains marginally competitive for now. However, when taking into account mining revenue which will have to be replaced with transaction fees, together with the costs of compliance with eventual regulation, the cost of transacting with Bitcoin becomes comparable to existing solutions.

Bitcoin's technology could be repurposed

As anyone who has ever had to transfer money internationally knows, the process is both time-consuming and expensive. Bitcoin has already demonstrated the potential to transfer large sums securely. While there are issues relating to Bitcoin's volatility, the underlying technology clearly works, and could provide the basis for faster transfers that are settled throughout the day at comparable, if not lower costs, than current alternatives. In this sense we see Bitcoin as a flawed first take on such a technology, which could be used to move existing currencies and securities. Banks seem well placed to develop this given their existing customers and systems. However, given that this would likely require an industry initiative, and the lack of incentive to cannibalise existing fee income, this is only a long-term potential project for banks and is likely to remain the domain of fringe third parties.

Opportunities and threats for banks

Bitcoin's long-term prospects of success depend on its ability to fulfill a market need, or do a better job than the current options. In the context of banking, Bitcoin must provide traditional banking services such as deposits at a lower cost, as the space is already dominated by many large players. This section analyses these potential disruptive effects of Bitcoin on the banking industry, and the potential opportunities for the banking industry in the Bitcoin framework.

Mixed views, but no major bank is backing Bitcoin

Statements from the banking industry on Bitcoin have ranged from restrained optimism to the strongly negative.

Jamie Dimon and the US Treasury share "incredulity" about Bitcoin

Dimon predicts Bitcoin's demise; US Treasury's main concern is that it not be used to fund illegal activities

Asked whether JP Morgan would ever "participate in people who facilitate Bitcoin", CEO Jamie Dimon predicted Bitcoin's demise. Specifically, Dimon predicted that "as a payment system [Bitcoin must eventually] follow the same standards as other payment systems [such as know-your-customer regulations], and that will probably be the end of them." In a similar vein, Jacob "Jack" Lew, Secretary of the US Treasury, shared a "certain incredulity" with Dimon. However, Lew limited himself to stating that the government's primary concern with Bitcoin was that it "does not become an avenue to funding illegal activities".

As a side note, during the latest JP Morgan Investor Day, Gordon Smith of JP Morgan's Consumer & Community Bank detailed the bank's own proprietary payment network, ChaseNet. While based on a completely different technological infrastructure from Bitcoin's, ChaseNet purports to offer a more secure form of payment processing while cutting the time spent by customers on purchases (seeking to shorten online checkout times from an average of two minutes to an average of 30 seconds). Based on the information provided, it appears that ChaseNet is geared towards the online/mobile checkout market – differentiating it from Bitcoin, which seeks to be usable in bricks-and-mortar settings as well.

Wells Fargo takes middle ground, calls for "rules of engagement"

Wells Fargo has taken a more cautious approach

In contrast to Dimon's clearly negative take on Bitcoin, Wells Fargo has taken a more cautious approach by convening banking industry executives, virtual currency experts and government officials to develop "rules of engagement" regarding Bitcoin – specifically with respect to money laundering concerns. While it has not endorsed Bitcoin outright, Wells Fargo is one of few major financial institutions that has expressed any interest in the potential financial innovation that Bitcoin brings to the table.

Interestingly, Wells Fargo has already had some interaction with Bitcoin: US authorities seized the Wells Fargo account of Mark Karpeles, founder of Mt Gox, in connection with his alleged failure to register Mt Gox as a money transmitting business. This experience, it appears to have primarily spurred Wells Fargo to further investigate as opposed to outright shun Bitcoin related businesses.

Sberbank CEO asks Kremlin to avert possible restrictions – didn't work

In what is perhaps the most positive endorsement to date, Herman Gref, CEO of OAO Sberbank, believes Bitcoin to be "a very interesting global experiment that breaks the paradigm of currency issuance", and that a ban would be a "colossal

step backward".[2] In fact, Gref has gone so far as to send letters to the Kremlin, Central Bank of Russia (CBR) and Finance Ministry to "avert possible restrictions" on Bitcoin, thus allowing this "experiment" to run its natural course. Notably, these efforts did not work, as Russia has since banned the use of Bitcoin outright.[3]

Importantly, even Gref – with his generally positive view of digital currencies – does not necessarily believe that Bitcoin itself will survive. When asked about major Russian search engine Yandex's attempt to develop an e-commerce payment system, Gref said that "these experiments must end in one or two crashes." Thus, while Bitcoin supporters have found an ally in Sberbank, the bank's support only appears to go as far as trying to prevent Russian governmental interference, and not actual involvement in Bitcoin operations.

Nordics refuse to get involved – pending regulation

SEB, the largest Nordic FX trading bank, has also commented on Bitcoin. Joan Andersson, chief risk officer, said: "Given the rules we have established for ourselves and rules that authorities have set up to prevent money laundering, we have currently made the decision that we cannot offer transactions, accounts or currency exchange in Bitcoin." While not as negative as Dimon, nor as positive as Gref, SEB's stated position is that it "need[s] to understand the business, there needs to be a sustainable business plan, and routines for following money laundering rules" prior to its involvement.

Threats to banks

Given the general distaste, or at least extreme caution, displayed by most financial institutions, this section will analyse what external threats Bitcoin may pose to the banking system, given that banks are largely not involved.

Disintermediation threatens banking *if* digital currencies take off

Bitcoin poses a disintermediation threat to banks in times of stress

Bitcoin currently stands politically opposed to, and is largely outside of, the existing financial system – some would argue its very purpose is to threaten banks. Currently, Bitcoin's market cap, the largest of all the digital currencies, stands at approximately $7bn. This is a relative drop in the ocean compared to most large banks' balance sheets. However, in the context of emerging markets, widespread usage could lead to disintermediation for smaller, local banks – particularly in countries experiencing economic turmoil, high inflation, or general mistrust of the banking industry. Even then, these factors would already pose a significant threat without Bitcoin.

Furthermore, while this issue would more likely occur in emerging markets, advanced economies that have entertained or engaged in 'deposit taxes' and asset seizures, such as in the cases of Cyprus and Greece, could expose their local banks to disintermediation risk.

Even in a 'Bitcoin village', citizens need banking services

Without these stress factors, we see little threat from Bitcoin. As a thought experiment, we could consider that some small community adopts widespread usage of Bitcoin. This could initially pose a threat to a local bank which may only be capable of dealing with fiat currency. Nevertheless, these citizens would still

[2] http://www.bloomberg.com/news/2014-01-24/bitcoin-gains-support-from-sberbank-s-gref-as-russia-plans-curbs.html
[3] http://rbth.ru/business/2014/02/05/russia_becomes_the_second_country_to_ban_bitcoin_33871.html

presumably require some banking services in the form of deposits and lending. Here, either Bitcoin fails, or the local bank (and regulation) catches up, or a Bitcoin bank emerges.

In practical terms, we find it unlikely that Bitcoin (or something similar) could pose a threat on a systemic scale – not least because existing authorities would have to get involved, but also because of Bitcoin's various failures as a currency (discussed above). In sum, disintermediation would require an alternate, price-stable store of value, and Bitcoin – and digital currencies in general – have failed in this regard, thus largely mitigating this risk.

Credit card fees and money wire fees could face pressure

Bitcoin-like technology could provide secure and convenient payments

Thinking forward and more broadly – not just regarding Bitcoin with a capital B – there is a potential threat of a third party setting up a bitcoin-like payment system.

Firstly, the reality is that cross-border transfers can take days, where a system with a blockchain and public/private key infrastructure like Bitcoin can take minutes. Secondly, even on a national level, a bitcoin-like system could enhance security and reduce fraud on an everyday level. In the US in particular, credit cards are regularly used for everyday transactions for convenience – but this leaves both the merchant and the banks open to risks of chargebacks. In principle, this is less of a problem with debit cards. However, even then a bitcoin-like system could provide enhanced security and lower costs, by giving users direct control of their funds and the 'private key' which is used to ensure security through encryption.

A bitcoin-like payments system could threaten existing banks and systems

In principle, this kind of payment system could be developed and put into use by a third party – even a (possibly online-only) challenger bank that could appropriately handle deposits – which could potentially be a threat to existing banks. Banks currently collect billions of dollars of revenue from fees and commissions, many of which are related to cards and payments. To this end, a bitcoin-like system could potentially undercut the banks in this arena and threaten this source of revenue.

Mobile payments are already taking off

There have already been moves to disintermediate and simplify payment systems, especially from the point of view of the consumer making mobile payments. Near-field communication technology has already been employed in mobile phones by Samsung and in cards by Visa to facilitate contactless payments. In the UK, Zapp, a mobile payments app, is being launched as a joint-venture between various banks including HSBC and Santander. In the US, there have been rumblings that Apple will leverage its existing customer base to create a mobile payments system[4], the idea being that users could securely deploy their card details from iTunes in other apps and in the physical world.

Double-edged: a disruptive threat can be an opportunity for banks

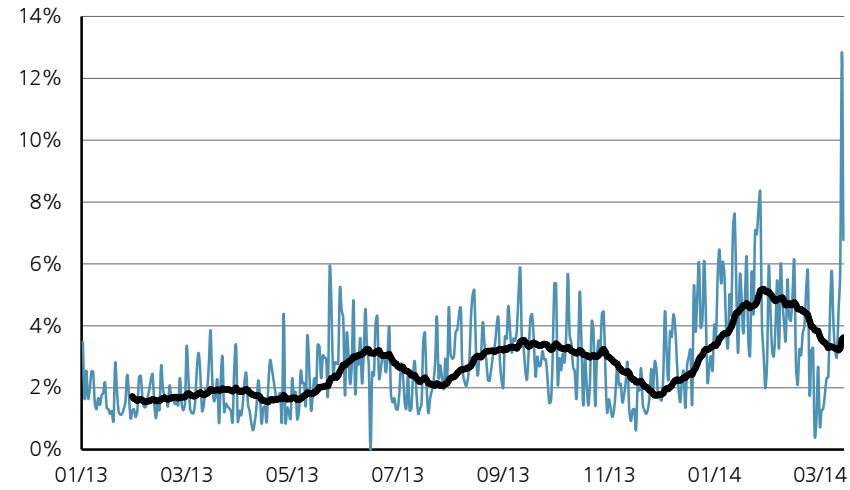
These developments display a trend towards new and simpler payment systems, and crucially the possibility of disintermediation – even leaving banks completely out of the loop. On the other hand, and especially with regard to bitcoin-like systems, we believe this kind of technology could be developed by existing banks, as an industry initiative even, turning it from a threat to an opportunity, as discussed below.

[4] "Apple pushes deeper into mobile payments", Wall Street Journal, 24-Jan-2014

Are Bitcoin transactions really cheaper for merchants?

In evaluating Bitcoin's disruptive potential with regard to credit card fees, the driving factor of success or failure is its overall cost. As seen in Figure 2, the daily miner compensation[5] as a percentage of daily transaction volume has fluctuated significantly over the past 15 months. Over this period, the average rate was c2.7%, with a 30-day moving average rate of 4.0%. While these figures are more or less in line with credit card fees (which range from 1% to 3%), since the beginning of 2014, the rate has trended upwards and been significantly more volatile – peaking at 8.3% at the beginning of February. In its current form, for Bitcoin to present any serious disruptive potential, both the average rate and the daily volatility would have to come down to predictable levels (not to mention the FX risk currently associated with holding Bitcoin for even a few hours).

Figure 2: Daily miner transaction fees as % of transaction volume (w. 30d M.A.)



Source: blockchain.info

Furthermore, unlike with credit cards, where funds are typically deposited in a merchant's bank account, to use Bitcoins, merchants need to take the additional step of converting Bitcoin to an existing fiat currency. Based on a review of several exchange prices, the lowest-cost option that we identified was 1% of volume.[6] This leads to an upward parallel shift of Figure 2 by 1 percentage point, making the overall Bitcoin value proposition far less appealing.

Bitcoin exposure would likely increase operational risks for banks

Lastly, Bitcoins could pose an internal threat if banks adopted it for any given purpose (e.g. banking services for Bitcoin exchanges, Bitcoin-related products, etc). Such exposure could increase reputational, legal and regulatory risks. While these risks are distinct in nature, they could occur in tandem should any of them come to pass. As detailed further below, Bitcoin's initial rise to fame was partially attributable to its association with black markets for illicit drugs and other illegal activities. This association led to a FBI investigation that ultimately resulted in the

[5] Daily miner compensation is calculated as Daily Transaction Fee plus Daily Bitcoins mined. As the number of Bitcoins mined decreases, we expect a shift in composition of miner income, not a decrease in overall compensation, as this is independent of miner costs.
[6] Coinbase which provides this 1% fee, provides an incentive of free transactions for the first $1,000,000 in sales. They also provide an instant exchange service, eliminating FX risk for merchants, by adding a $0.15 fee on top of the 1% for each transaction.

shutdown of an online marketplace and criminal prosecution of the marketplace operator.

In that specific instance, banks were not implicated in the fallout. However, if banks were to actively seek Bitcoin exposure, they would likely expose themselves to the same risks of increased regulatory scrutiny and criminal prosecutions, both of which would obviously damage the reputation of the bank.

Opportunities for banks

Banks could make Bitcoin ETFs...

As an asset class, Bitcoin and similar digital currencies offer an opportunity for banks to offer investment services to their clients by way of ETFs, similar to the offering currently proposed by the Winklevoss brothers. In this way, banks do not have to expose themselves to money-laundering risk or market risk – they can simply offer an investment vehicle and collect the fees.

...or Bitcoin derivatives

Taking this sort of ordinary financial servicing one step further, banks could also start offering elementary hedging products to businesses which deal in Bitcoin or another digital currency – contingent on being allowed to do so by regulation. This would be particularly helpful for businesses in the context of Bitcoin's volatility, which currently forces a lot of businesses to convert to fiat currency at the end of every day. These products would be a marginal source of fee revenue, but could equally turn into a threat if banks find themselves unable to create such a swaps market (e.g. due to regulation). If (and this is a big if) businesses were to start dealing with digital currencies in significant volumes, a third party or new entrant could offer the required hedging services. Ultimately, however, at those volumes a business would require fairly sophisticated hedging and financing services, which a bank would be best placed to provide and the regulator would have to get involved in any case.

A bitcoin-like technology with units of fiat currency could simplify existing systems

On a structural level, we think Bitcoin as a technology offers innovative new features that could be adopted by banks as an industry. A distributed blockchain offers a robust and secure way of storing customer funds. Transactions made by way to create public/private key cryptography and a consensus-building method offers a fast, low-cost and secure way of transferring funds – in principle anywhere in the world. The computational intensity currently required by Bitcoin is not a necessary feature; it is merely a quirk of this first implementation. The unit of account used does not have to be a new currency (like Bitcoin), but can simply account using existing fiat currencies. Such a system also offers a radical opportunity to drastically reduce duplication in the existing system, where each bank has to run its own proprietary system for managing funds and transactions. However, a significant difference in such a system from the current Bitcoin system would be the inclusion of 'know your customer' safeguards, removing the anonymity associated with Bitcoin transactions.

Banks can bring trust and regulation into the equation

Banks also arguably offer the advantage that they are fundamentally trustworthy institutions. Admittedly, banks' reputations have been tarnished since the financial crisis, but the majority of people still use bank accounts and debit/credit cards, and they receive salaries and pay bills by way of banks. Rather than trying to develop a completely new financial system as Bitcoin is trying to do, it makes more sense that banks, as existing money managers, absorb the benefits of the technological innovation. Banks already have systems to deal with regulation (money-laundering and other), they already have customers, and already have a franchise. For example, most people happily use debit and credit cards without understanding in detail how the underlying systems work. From this perspective, banks are better

placed to introduce a new technology that customers could more readily take up and trust.

However, as a cautionary note, any potential upside associated with Bitcoin will likely be limited given its relatively low market capitalization. At its peak, Bitcoin's market capitalization was just over $13bn. While this may be impressive in its own right, in the grand scheme debt and equity markets, it represents no more than a drop in the bucket. Thus, despite generating press coverage and general interest far in excess of what its relatively low market capitalization would suggest to be reasonable, we believe this low market capitalization will likely cap fee incomes at a relatively low level.

A hypothetical implementation of Bitcoin-like technology

As an example, such a technology could work as follows. Banks across the world maintain a distributed blockchain-like ledger through some consensus-building system, keeping track of public addresses (anonymously outside the relevant bank) and the balances associated with them. Customers have control of their private keys, possibly with the option of authorizing their banks to handle their keys for them as well, while keeping the customer front-end broadly similar (i.e. with bank account numbers, etc). Either using their private key, or existing identification methods, customers can make secure payments and transactions with no double-spending risk. In principle, there is still a confirmation time, but banks could guarantee the payment to bridge this gap. Moreover, they could keep track of which customers are associated with which public address, for tax and money-laundering purposes, among others. This way they can also chase up customers who might try to double spend. In the meantime, transfers anywhere in the world take minutes as per existing digital currencies, and if there is an FX transfer involved the relevant banks should be able to provide near-instant FX exchange.

This is very much a hypothetical example and a blue-sky idea; such a system has the potential to cannibalize existing high-fee businesses. Given this, banks would probably be hesitant to support the development of such a system. A possible incentive for banks to develop such a system would be increased money transfer volumes sufficient to offset decreased fees, or if costs are lowered enough to still boost profits, but any such projection would be highly speculative at this stage.

The likelihood of this aside, the general example serves to illustrate the potential that a bitcoin-like technology could bring for both consumers and banks. Rather than dealing with individual proprietary systems, and having some transfers take days (especially internationally), this is an opportunity for banks to offer some of the advantages presented by Bitcoin, such as fast, low-cost, secure transfers with reduced risk of fraud and chargebacks.

In-depth: What is Bitcoin?

Conceptual overview

In developing a framework to evaluate and think of Bitcoin, it is important to initially draw a distinction between Bitcoin as a network and Bitcoin as the unit of 'currency'.

In the case of the Bitcoin network, we have a decentralized network supported by numerous computers nodes, or miners, operating independently of one another.

Need to distinguish between the underlying Bitcoin network and Bitcoin as a unit of currency

On the other hand, we have Bitcoin as a unit of currency. At its most basic level, a Bitcoin is a digital signature (i.e. a unique sequence of numbers) that is meant to represent a unit of value in the same way a dollar or pound sterling would. However, as explained below, we adopt an alternative view by treating each Bitcoin as a series of transactions. Put differently, it is our view that Bitcoin is analogous to cheques with standardized value that have a running tab of endorsements, where each endorsement is (almost) immediately recorded in a decentralized ledger. However, unlike normal cheques, which would eventually be presented to a bank for payment, the cheques in this analogy are never cashed and just continuously collect endorsements as they pass from person to person[7].

For the remainder of this note, we use the term Bitcoin interchangeably, depending on the context.

Bitcoin on the surface: day-to-day use

Before delving into the underlying mechanics of Bitcoin, we first provide a primer on how Bitcoins are used in typical transactions and the various storage options for Bitcoins. The main topics we will discuss here are:

1) Getting started with Bitcoin
2) Wallet options for managing Bitcoin
3) Example: a hypothetical transaction

To get started, users only need a computer/internet access

Bitcoin is widely accessible in developed and developing countries, given the low barriers to access

First off, all aspects of Bitcoin are based entirely online with no physical presence. As such, the only prerequisites for dealing in Bitcoins are a computer and an internet connection. Once this is satisfied, anyone can create a Bitcoin account for free. In order to set up such an account, users need to download one of several free Bitcoin clients / wallets (hereafter, "wallet"). This wallet serves two primary purposes: (1) generating a public / private key, and (2) providing a user interface for the sending / receiving of Bitcoins.

[7] Side note on cheques: notably, even though Bitcoin and cheques bear common features from a transaction perspective, a fundamental difference would be that cheques still have a derived value. Eventually, a bearer of a cheque could demand from the original counterparty, the amount of fiat currency provided for by the cheque. Bitcoin on the other hand, has no 'counterparty' against whom a Bitcoin could be legally compelled to exchange for anything. As fiat currencies have natural demand by virtue of being legal tender, creditworthiness issues aside, a cheque would always have some value whereas a Bitcoin has no safety net.

Public / private key – analogous to payee and signature, respectively

The basis of transactions on the Bitcoin network revolves around two serial numbers known as keys. In the case of the public key, it is generally referred to as a Bitcoin address. This public key is analogous to an email address and enables a user to receive Bitcoins at that address. Furthermore, just as in the case of emails, where no correspondence can be sent from a given address without the password, Bitcoins cannot be sent without the private key associated with a given public key.

Analogizing this feature to the cheque example, the other way to think about it would be to equate the public key with the "Pay to the Order of" line on a cheque and the private key with the signature. The primary difference in this case between Bitcoins and traditional cheques is that cheques would then pass through a third party for verification of the funds to be withdrawn, whereas Bitcoins rely on a decentralized network.

Wallets are the user interface – payments cannot be made 'physically'

In addition to the generation of the keys, a wallet facilitates transactions by providing a user interface with which to conduct transactions. As stated before, without a physical aspect, Bitcoins cannot be 'given' for payment in a physical sense and must be transmitted over the internet. As there are multiple wallet software providers, the interface may vary, but the basic layout would require that a user enter their private key, the public address on the receiving end, and the number of Bitcoins to be transmitted.

Importantly, just as in the case of cheques, where banks are able to deposit cheques from different banks, Bitcoin wallets can send and receive regardless of the counterparty's wallet.

For the purposes of this discussion, Bitcoin wallets can roughly be separated into two categories: software wallets and third-party wallets.

Given that the Bitcoin user experience revolves around the wallet, a discussion on the types of wallets is essential to understanding certain aspects of Bitcoin.

- **Software wallets**

Software wallets store Bitcoins locally and are open to hacking or can be impractical

In the case of software wallets, the wallet is largely as described above, whereby a user downloads a wallet and proceeds to generate keys and conduct transactions. In choosing a software wallet, a user would install the wallet on their personal computer. However, this exposes the user to accidental and intentional risks – ranging from fires and floods to hackers and malware. In the case of the former, the risk can be somewhat mitigated in the form of safely stored, regular backups of the wallet file containing the private keys.

Notably, backups are useless if hackers or malware gain access to the computer files, as they can irrevocably transfer all the Bitcoins out of the account. This is unlike cheques, where if someone gains wrongful access to a customer's bank account, the customer could still seek recourse from the bank for improper authorization or inadequate security. Given the lack of a responsible third party, for Bitcoins, all transfers are final and irrevocable.

For dealing with this latter threat, some users of software wallets employ a tactic known as cold storage. In cold storage, users keep the Bitcoin wallet files in either a physical medium (e.g. paper) or an offline electronic medium (i.e. saving it on a computer that is always kept offline). Assuming this offline, storage medium is

then stored in a physically safe location such as a bank vault, risk of loss is minimized. However, as Bitcoin only exists on the internet, this makes access to the bitcoins in cold storage extremely inconvenient if the wallet files are stored in a hard to access place – like a bank vault.

- **Third-party wallets**

Third-party wallets are convenient but open to abuse

Given the risks and possible inconveniences associated with holding one's own wallet, the alternative would be to outsource the function to a third party. These third-party wallet services (a.k.a. browser-based wallets) act as intermediaries and either set up and manage wallets for users or they maintain their own wallet and allow individuals to set up accounts (i.e. additional wallets are not created for new users and instead the service provider aggregates the Bitcoins in their own wallet). While there are numerous third-party wallet services, a common theme among them is that they have simple, easily understood user interfaces, require no downloads, and allow for Bitcoins to be accessed from multiple devices.

However, by using a third-party wallet, a user is still exposed to the risks detailed above if the third party experiences natural disasters. Furthermore, hacking / malware risks may be exacerbated if the third party is targeted, given the larger number of Bitcoins, or if the user is directly targeted by older tactics such as key logging and phishing to steal their relatively less secure account passwords as opposed to a more secure private key.

Lastly, users of third-party wallets must also rely on the good faith of the service provider. An unscrupulous third party could unilaterally transfer all the Bitcoins in their custodial care and cease operations. If the provider is outside of the legal jurisdiction of the victims, this leaves the victim with no legal recourse.

Example: A hypothetical transaction

Having provided a basic description on how to get started with Bitcoin and the various end-user aspects, this section now provides examples of where Bitcoins could be used and how one would go about using them in a real-life situation.

Internet transaction: Largely similar to buying with a credit card

For online transactions, Bitcoin transactions are as easy to execute as credit card transactions

Some merchants are warming to the idea of accepting Bitcoin, and a significant portion of these new entrants to the Bitcoin arena are internet-based, given the ease of transaction. Major retailers in this space include Overstock and Tigerdirect. Furthermore, gift card retailer, Gyft, allows Bitcoin users to greatly expand the selection of retailers to include a wider variety of retailers such as Amazon, Target, etc.

Regardless, a typical transaction would at first proceed in much the same way as would a normal transaction. Customers would browse the retailer's website and add items to their shopping cart. At checkout, in addition to the option to pay by credit / debit card, customers will see an option to pay by Bitcoin. Upon selecting this option, customers will be directed to a public address and / or a QR Code representing that address. At this point, the customer would use their wallet to send the specified number of Bitcoins (plus a miner's fee to expedite the process) to the address and "Confirm Payment" on the website. The length of time this step takes varies depending on the retailer. After payment is confirmed, the retailer typically provides a receipt and fills the order.

As a final point, for most of the online retailers we reviewed, the product prices were denominated in USD with a real-time Bitcoin-to-USD conversion rate being applied at the checkout phase. Given the volatility of Bitcoin, prices can vary from transaction to transaction even if entered seconds apart.

Bricks-and-mortar transaction: requires specialized point-of-sale hardware or that customers have smart phones

Bricks-and-mortar transactions essentially add the requirement of smartphones for ease of use

Adoption does not appear to be as widespread in the bricks-and-mortar category as in the case of internet retailers. Despite this, a number of small-business owners have begun accepting Bitcoin – ranging from high-end restaurants to coffee shops.

As before, customers would first proceed as normal in selecting the goods that they want to buy. The main difference would be at the point of checkout. There are two primary ways that a merchant could go about accepting Bitcoins in this context. The easier of the two is to simply post a public key in the form of a QR code next to the register and allow customers to scan and pay with their smartphones.

Alternatively, merchants can use specially designed point-of-sale terminals which can process payments. However, such terminals may require that the customer have an account with the designer of the POS system. Essentially, some of these services operate in a similar fashion to the third-party wallets described above, in that users have more easily accessible accounts, from which they can direct Bitcoins to be sent to a given address.

Bitcoin transactions are not immediately confirmed, so open to fraud

A primary difference between bricks and mortar versus internet transactions, however, is the risk that a merchant could be undertaking in accepting Bitcoins. Since Bitcoin transactions are not instantaneous, after submitting payment, a customer could leave before the transfer is confirmed. If the customer is dishonest and does not actually have sufficient Bitcoins, the merchant could be left shouldering the loss.

They are also undisputable and irreversible

In the same vein, since Bitcoin transactions are irreversible, if a customer is ultimately dissatisfied with their product or service, they would have less recourse against a merchant – whereas in the case of credit cards or even debit cards, customers can easily dispute the charge.

Lastly, as a purely practical matter of using Bitcoins in a bricks-and-mortar setting, as this example shows, smartphones greatly simplify the process. Even though point-of-sale servicers can somewhat alleviate this issue, this depends on both merchants adopting those servicers and customers having accounts. Put simply, without a smartphone, it will be much harder to pay with Bitcoins in a bricks-and-mortar setting.

Bitcoin under the hood: How Bitcoin works behind the scenes

Given the above primer, we now delve deeper into the underlying mechanics of Bitcoin and the role that the nodes play in supporting the network.

As provided in the introduction, the concept of electronic currencies is nothing new. Indeed, there have been multiple past attempts at creating something like Bitcoin. However, none of these past attempts succeeded given their inability to solve the double spending problem.

To elaborate, since a unit of electronic currency is nothing more than a string of numbers, letters, or symbols, a dishonest party could attempt to send the same unit to multiple parties thus defrauding recipients. While the classic solution to this problem would be a central routing system where a third party checks account balances and transaction timestamps, this offers virtually no improvement compared to credit cards and other methods of electronic payment. Enter Bitcoin which adopts a novel approach, relying on a decentralized network that timestamps and validates transactions. This decentralized network effectively incentivizes a decentralized group of participants to take on the duties that a central bank or third party would normally do, by allocating rewards based on computing power used.

As alluded to above, it is our view that Bitcoin shouldn't be viewed as a unit of currency, but should instead be viewed as a series of transactions. In explaining how we arrive at this conclusion, we will touch on three main topics:

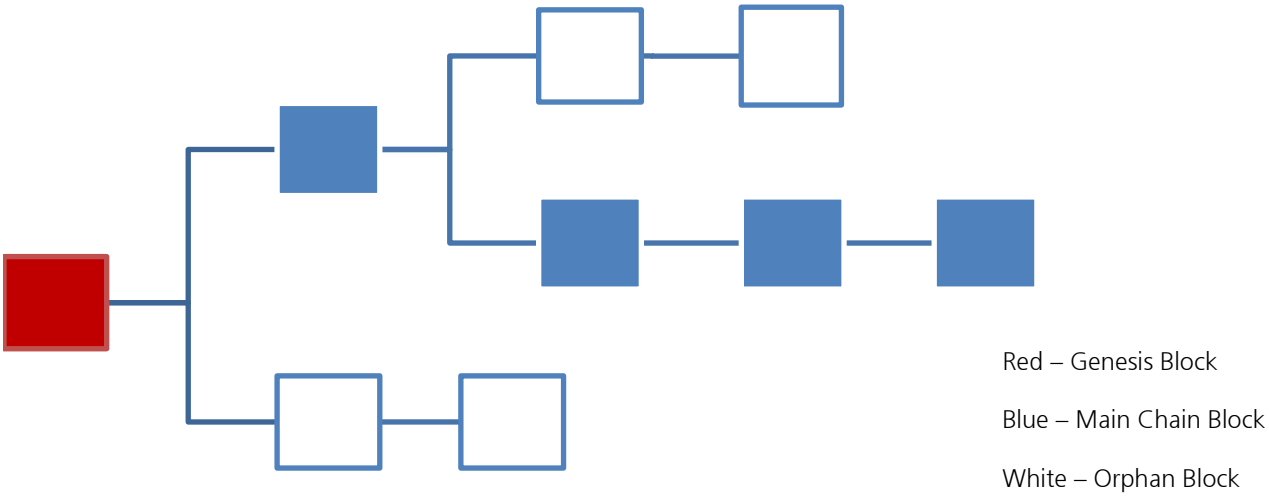
1) What is the blockchain?

2) How are blocks added to the chain?

3) Costs / benefits of being a node

What is the blockchain?

Figure 3: Visualization of the blockchain



Source: UBS Global Research

In order to understand how Bitcoin works on a technical level, we begin with the blockchain. Referencing the chequebook analogy from before, the entire blockchain is the ledger in the analogy that records all transactions on the Bitcoin network.

Within the blockchain, there are three distinct types of blocks: the Genesis block, main chain blocks, and orphan blocks. While each type of block has its own defining features, in all cases, a block is a compilation of unrecorded transactions. Thus, continuing with the chequebook ledger analogy, each block represents a page within the master ledger.

Genesis block – 'true north' for all other blocks

As its name suggests, the Genesis block is the first block in the blockchain. The Genesis block acts as the point of reference for all subsequent blocks added to the chain. Put differently, for any block (and by proxy, transaction) to be valid, one must be able to trace the movement of the Bitcoin back to the initial transaction, or the Genesis block. Given that there is no transaction prior to the Genesis block to trace it back to, the creator(s) of Bitcoin hardcoded the value as a point of reference for all subsequent transactions.

Main chain / orphan blocks – Miners may disagree leading to splits in the blockchain

In the case of the other two block types, they are identical in that they both reflect compilations of recently broadcasted transactions on the network. However, as the blockchain is a dynamic ledger that is updated every 10 minutes, every now and then, two miners may submit a new 'page' in the ledger at the exact same time. When this happens, a fork in the chain occurs. At this point, the respective miners that created the two blocks in question each broadcast their block to the network as though theirs was the true block. (For referential purposes, we'll refer to this divergence as B1 and B2.) Other miners at this point would receive either B1 or B2 and would begin compiling the next block to add to the chain. Assuming a miner working off of B1 finishes the next block in the chain before any miner working off of B2, it would broadcast its completed block to the network. At this point, any miner working off of B2 would automatically switch over to B1. Thus, only after having resolved the fork in the blockchain, can we label B1 as the main chain block and B2 as the orphan block. Also, after B2 is found to be an orphan, any transactions that were compiled in B2, but not B1, would then be re-queued for inclusion in a subsequent block. Lastly, for the inquiring reader who wonders what would happen if two miners submitted blocks at the exact same time again after B1 and B2 already diverged, the process proceeds as described until a miner eventually breaks the tie.

While this may not seem to be a particularly important distinction, orphan blocks reflect inefficiency and wasted mining efforts. As such, if there were many orphans being created, confirmation times would likely slow down and miner profitability (to be discussed in the following section) would drop, potentially leading to fewer miners willing to dedicate resources to supporting the Bitcoin network. However, as will be discussed now, the Bitcoin coding employs an innovative method to greatly reduce the chance of parallel chains from forming and from continuing if one is formed.

Blocks require validation prior to being added to the blockchain

Having explained what makes up the blockchain, this section discusses how a block is actually created and ultimately added to the chain.

The validation process acts as a bottleneck to increase user security

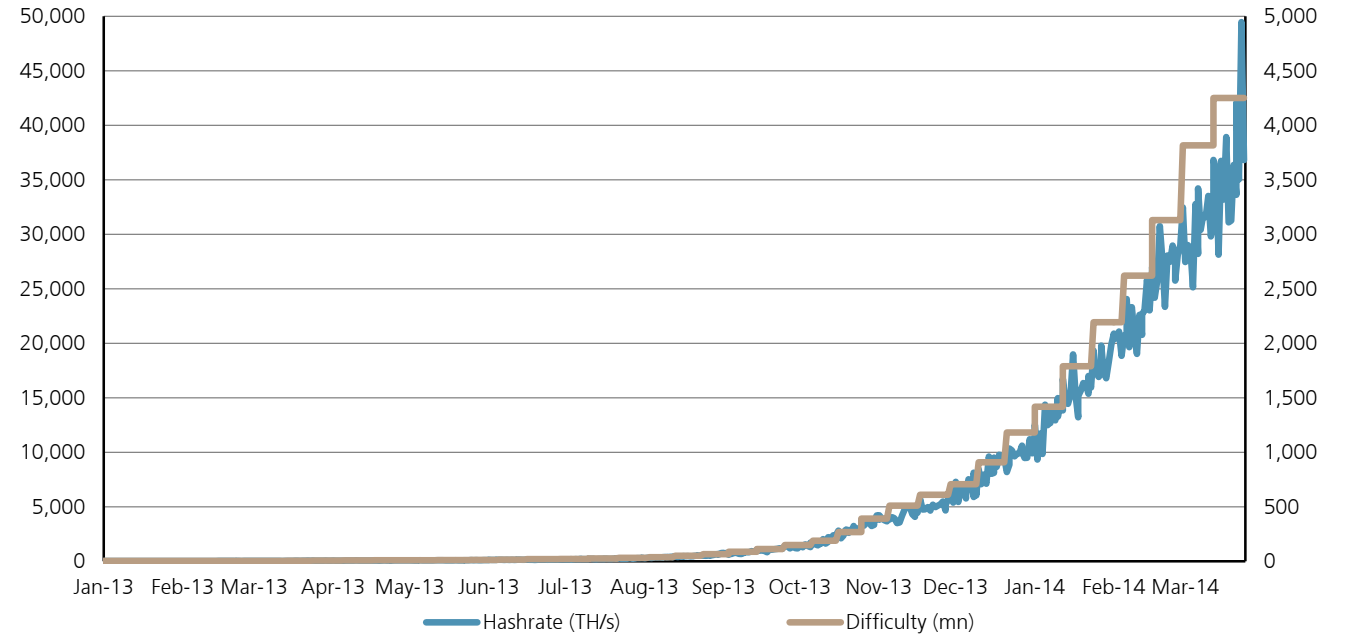
As described earlier, when a transaction occurs between two Bitcoin users, the software broadcasts the number of Bitcoins transferred, public addresses involved, and the time of the transaction. Miners pick up these broadcasts and compile them in real time to generate a block. However, without any limitations, thousands of blocks could be produced in an hour leading to multiple forks and orphans or nefarious individuals could attempt to submit multiple transactions with the same Bitcoin. To solve this, the software dramatically increases the difficulty of producing a block by requiring that miners also compute a cryptographic hash.

Simply defined, a cryptographic hash is a string of characters made of numbers and letters (e.g. 000001a2b3c4d5e6f – in practice, it would be a much longer string). From here, the Bitcoin software requires that miners combine the cryptographic hash value from the previous block with an unknown value in a hash function to produce a value with a certain number of zeros at the front of the string. The unknown value can only be solved by trial and error which amounts to no more than rapid, random guessing. Furthermore, the function is designed in such a way that miners can't work backwards from a given output to determine the unknown value.

However, with only the limitation of a hash function, an increase in miner computing power would still lead to blocks being produced too quickly. As such, the underlying Bitcoin software changes the difficulty setting every time 2,160 blocks is generated based on the average length of time used to create the last 2,160 blocks. Difficulty is increased or decreased to achieve a target block generation rate of 1 block per 600 seconds. Thus, if the total computing power of Bitcoin suddenly increased, the remaining blocks of the 2,160 limit would be solved faster than a 1 block / 600 second rate, but the underlying software would adjust the difficulty accordingly at the next reset time.

Costs / benefits of being a miner

Figure 4: Mining difficulty (rhs) and hashrate (lhs)



Source: blockexplorer.com

In the earlier days of Bitcoin when the difficulty was relatively low, desktop computers were capable of solving for the unknown value. However, as the value of Bitcoin rose, increasingly powerful and electricity efficient computers were dedicated to the mining process, culminating in the form of ASIC chips.[8] As compared with the average desktop CPU, a high-end ASIC chip can operate thousands of times faster while consuming less electricity per calculation. Given

[8] Application-specific integrated circuit – hardware designed for the sole purpose of running hash functions. These chips cannot be repurposed for any other use.

that the overwhelming majority of bitcoins are now mined with ASICs, computers using these chips are colloquially referred to as 'mining rigs'.

It should be noted, these mining rigs are not cheap, with a high end rig starting at roughly $10,000. Furthermore, in addition to this significant capital investment requirement, the variable cost of electricity can prove to be significant depending on the number of rigs being employed on the entire network (i.e. a larger number of rigs would increase the overall electricity required to produce a single block, but as stated, these blocks are roughly fixed at a 10 minute generation rate).

Increased competition has made casual Bitcoin mining an unprofitable activity

With such high costs, this begs the question of why anyone would want to engage in the costly process of acting as a network node. The answer to this is two-fold: (1) for now, miners can earn 25 new Bitcoins for each block added to the blockchain and (2) users can voluntarily attach transaction fees when sending Bitcoins, rewarding miners for processing their transactions.

New Bitcoins awarded to miners

The underlying code of Bitcoin allows Bitcoin to grow at a decreasing rate that levels off to 0 when 21mn Bitcoins have been generated. As the Bitcoin supply grows, the award of Bitcoins drop by 50% every time an additional 210,000 blocks is mined. Thus, even though new blocks originally awarded miners 50 Bitcoins per block, the current reward is 25 per block. Based on the average time of 1 block / 600 seconds, the last new Bitcoin is expected to be mined sometime around the year 2140.

While the incentive of new Bitcoins departs from how cheques normally work, essentially, every time a miner adds a page to the ledger, they are allowed to record an increase in their own balance.

Transaction fees provide alternate source of compensation

Given that new Bitcoins will be produced at an ever shrinking rate, the Bitcoin network also allows for individuals to attach transaction fees to their transactions. Since the bulk of miner incentive comes from new Bitcoins, transactions can still be sent with minimal transaction fees. However, even with transaction fees constituting such a small percentage of total miner compensation, failure to provide any fee can result in lengthy delays for a transaction to be included in the block chain and thus be confirmed. As Bitcoin continues to develop, this will be a key factor in the long term success as uncompetitive or unpredictable transaction fees would likely cause people to rely on traditional forms of payment such as credit cards.

In-depth: What do we see in Bitcoin?

Bitcoin is marketed by its developers and proponents as a currency. Traditionally, a currency has 3 functions as:

1) A store of value

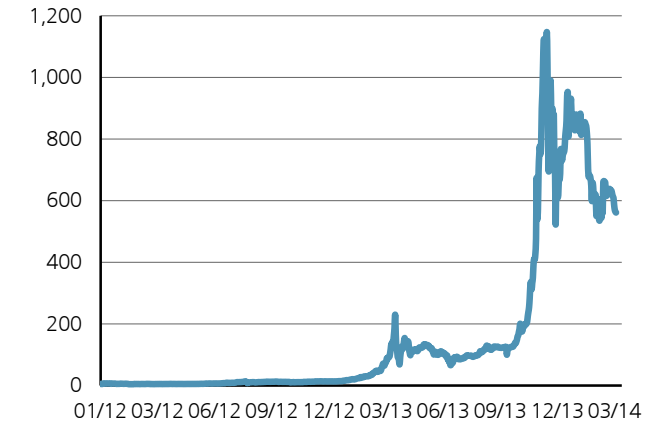
2) A means of exchange

3) A unit of account

We begin by investigating Bitcoin as a store of value, and thus more broadly as an investment, potentially like a commodity. Given Bitcoin's excessively volatile price we do not make a quantitative valuation, but instead examine potential sources of value for Bitcoin and how one could think of Bitcoin as an investment.

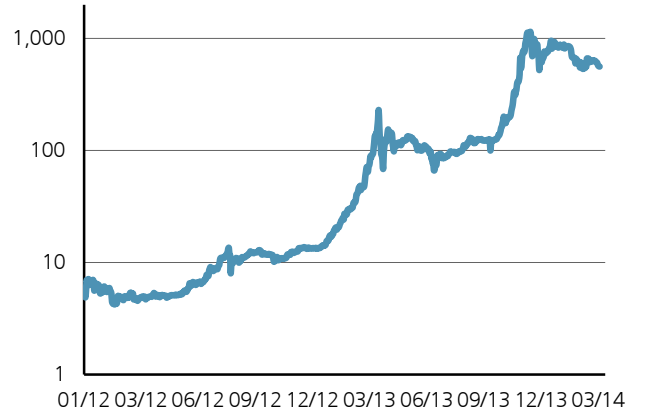
Bitcoin as a store of value

Figure 5: Coindesk Bitcoin Price Index (USD)



Source: Coindesk.com

Figure 6: Coindesk Bitcoin Price Index (USD, log scale)



Source: Coindesk.com

Bitcoin's recent meteoric price rise superficially has a simple reason, like for any other appreciating investment – there is high demand for a limited resource. As explained above, the supply of Bitcoin is predictable and effectively fixed, so the question purely becomes – what drives this demand? We discuss a few (and by no means all) factors below.

China loves alternative currencies

Tencent Q-coin in the early 2000s provides a precedent – was wildly popular and subsequently banned

A simple answer is that Bitcoin has increasingly entered the public sphere and generated media buzz bringing more investors in. For some, it is seen as a sort of 'digital gold', an alternative investment (currently) free from government control and in particular inflation. Chinese interest specifically has been a recent driver, as evidenced by the rapid increase in activity on Chinese exchanges in the second half of last year. From a Chinese perspective, the lack of government intervention and the possibility of circumventing capital controls have a particular attraction. Moreover, Chinese consumers are not new to the concept of digital currencies. In the first half of the 2000s, Tencent (an internet and media conglomerate) introduced Q-coin as a virtual currency scheme for purchase of goods and services from Tencent, fixed against the renminbi. This quickly evolved into effectively an illegal money scheme with annual flows of billions of yuan, demonstrating the Chinese demand for an alternative currency. Ultimately, the authorities banned the

use of Q-coin for trading in real goods, and further provided regulation for all virtual currency schemes whereby they were only to be used for purchase of virtual goods and services provided by the issuer.

Bitcoin has been increasingly restricted in China to control capital flow

This demonstrates that there is demand in China for an alternative currency to get around capital controls, but also that the authorities take a dim view of this, thereby limiting the possibility of Bitcoin's use as a currency. It is thus clear that Bitcoin is very much serving as a speculative investment rather than a currency, especially given recent specific crackdowns. Banks have been forbidden from engaging in Bitcoin transactions[9] and Bitcoin exchanges have been prohibited from directly taking renminbi deposits[10]. At the time of writing, a voucher system had developed for transferring yuan into Bitcoin, and some exchanges have started accepting bank transfers directly into their company accounts, but nevertheless there is a clear aim towards restricting Bitcoin activity in China. This is further reflected in the fact that Alibaba, China's largest retailer, recently banned transactions in Bitcoins or other digital currencies.

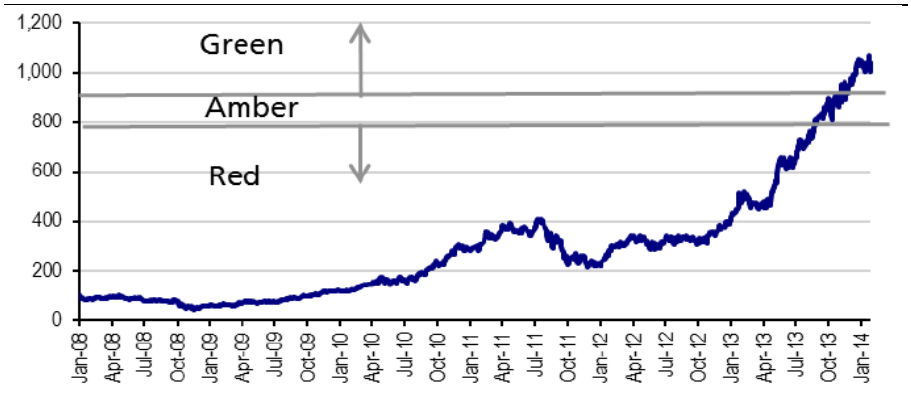
The most recent price dip came about due to a false report (since retracted) through micro-blogging site Sina Weibo that the PBOC would halt all Bitcoin transactions. Although untrue, the impact of this news flow demonstrates the significance that China still has to Bitcoin, and its general volatility otherwise

Media buzz and the tech bubble

Bitcoin has grown on the back of speculation and seemingly a growing tech bubble

Outside China, demand has been fuelled by the combination of a libertarian political agenda and increased media buzz. On the one hand, as mentioned, Bitcoin is ideologically attractive to some as a 'digital gold', free from government intervention – an international currency for the Internet age. On top of that, demand has been fuelled by increased media coverage and speculation, and varying positive/negative news flow (e.g. vaguely positive comments by Ben Bernanke[11], prohibitions in China as discussed above, the collapse of Mt Gox) has had significant impacts on the price. Bitcoin even seems to form part of a broader trend of the bubble in new, exciting tech 'stories' such as 3D printing and movie streaming where stocks trade at triple digit P/E; a symptom of excess liquidity and misallocation of capital as identified by our commodities strategy team (see the 4th Horseman from Commodities & Mining Q&A, 7 Jan 2014).

Figure 7: UBS Index of high momentum tech stocks



Source: UBS research, Bloomberg. Comprises Netflix, Netsuite, Tesla, Priceline, Stratysys & 3D systems corp.

[9] 'China bans banks from Bitcoin transactions', Financial Times, 5-Dec-2013
[10] 'China bans new Bitcoin deposits', Financial Times, 18-Dec-2013
[11] "Bitcoin hits $785 with a little help from Bernanke", Financial Times, 18-Nov-2013

Bitcoin as a commodity

In this vein, it is tempting to treat Bitcoin as a commodity – much like certain regulators of late e.g. in Finland[12] and Japan[13] – as its value is purely driven by supply and demand, and its supply is constrained. Indeed, unlike even commodities, Bitcoin's supply is completely predictable and effectively fixed – or rather, completely inelastic. Furthermore, there is nothing to underpin an intrinsic value for Bitcoin in the same way that is the case for tangible commodities like copper.

Gold is more unique and seems to have more intrinsic value than Bitcoin can

Gold is most often cited as a potentially comparable investment, but it has a millennia-long head start on Bitcoin as a store of value. Its physical properties as a relatively scarce and distinctive metal that doesn't corrode have developed it into a historical safe haven. These properties also make gold somewhat unique, whereas Bitcoin is functionally replaceable with another similar technology (e.g. Litecoin, see 'Alternatives').

The marginal cost of production is arguably irrelevant as a valuation metric for Bitcoin

Before considering the intrinsic value of Bitcoin more broadly, it is worth commenting on the cost of production as a measure of value. In commodities, the marginal cash cost of production provides support to price levels, so it is tempting to consider the same for Bitcoin. Rather than even attempting this estimate however, it is worth commenting on why this is not a good valuation approach. Firstly, the technology used is still highly varied, with a variety of computers in use of differing price and electricity consumption (in principle any computer can be used, but the probability of an ordinary PC mining a Bitcoin now is so low as to be unprofitable), with different electricity prices, all of which is exacerbated by the decentralised nature of Bitcoin mining. Combined with the volatility in Bitcoin prices, this means even miners' own estimates and investment decisions are ultimately unpredictable and irrational, so there is no widely estimable cost curve.

Secondly, Bitcoins are not a resource that is converted into or used as something else in the same way that (most) tangible commodities are, so the suppliers i.e. miners, have less bargaining power as existing Bitcoins can simply continue circulating. The market value of these existing Bitcoins can easily drop through the cost of production without users being significantly affected. On top of that, Bitcoin's apparent replaceability means that users can still relatively easily up sticks and leave miners in the lurch. Finally, the nature of the current Bitcoin network is such that even the very computers that miners have invested in are now largely specific to Bitcoin mining (aka Application Specific Integrated Circuits, ASICs), so the vast computing power that has been created cannot be used for anything else. Ultimately, the cost of the electricity and fixed asset investment that goes into mining Bitcoins doesn't (seem to) produce something of added or intrinsic value.

The network effect?

This brings us to the broader point that Bitcoin doesn't obviously offer up any intrinsic value to serve as a floor – each bitcoin is ultimately just a string of digits, and the whole system is just a distributed code. Having said that, software is also just code yet it can command very high prices and value. But as software, Bitcoin is just a secure way of transferring numbers publicly, securely and irreversibly, from one address to another, without a double spend problem. The software itself is

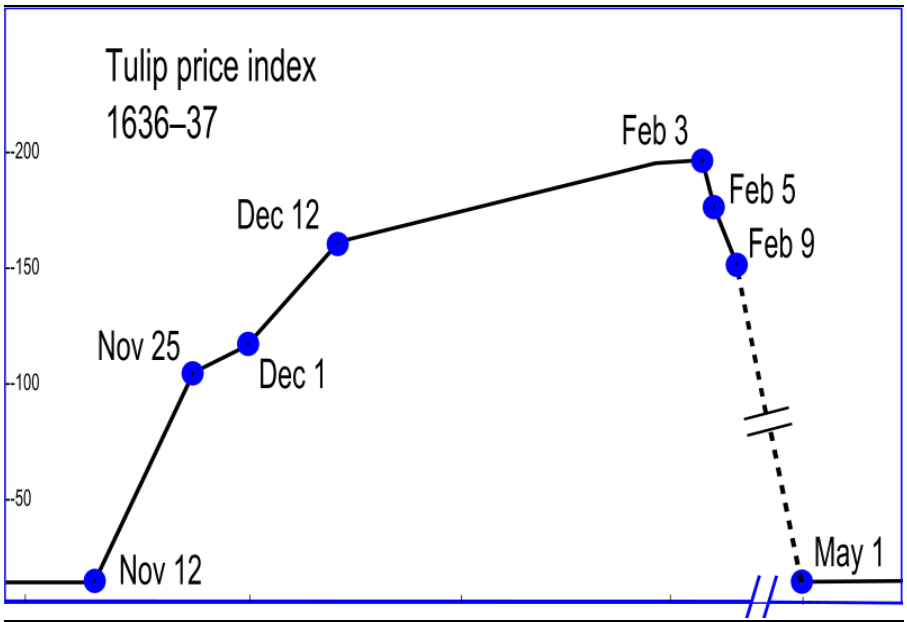
[12] "Bitcoin Judged Commodity in Finland After Failing Money Test", Bloomberg.com, 20-Jan-14
[13] 'Japan considers tax on Bitcoin transactions as part of crackdown', Financial Times, 5-Mar-14

freely available – the Bitcoins themselves do not need to command the significant prices that they do for the system to function, just like so much other open-source software.

Does Bitcoin's utility provide value through the network effect? Or is that just another name for speculative demand?

This may be overly pessimistic though, for there is the matter of the 'network effect' which is often espoused by Bitcoin evangelists. This is the argument that Bitcoin derives its value from its increasingly widespread usage. This is often compared to telephones, in that a telephone network derives value only for as long as it is widespread and thus useful. Where a telephone's fundamental utility is in facilitating voice conversations over a long distance, Bitcoin's utility lies in its function as a means of exchange, which we discuss in the following section. Moreover, unlike the telephone, Bitcoin's fundamental utility as a means of exchange is also inextricably linked back to its value (particularly its stability). Without it being a good means of exchange or having a guaranteed source of demand as legal tender (in particular being able to pay taxes with it), the 'network effect' just becomes another way of saying that its value is simply derived from speculative demand, as discussed above. With our usual currencies that also lack intrinsic value, there will always be guaranteed future demand in that one can always use them to settle future tax obligations and contracted debts. Given its lack of association with any kind of government and legal tender status, Bitcoin lacks this guarantee. Finally, telephony as a system seems to be less vulnerable to risk of replacement (although telephone companies may come and go), whereas Bitcoin seems more open to the threat of a competing digital currency (discussed in greater detail below).

Figure 8: Tulip bulb price in 17th century Holland



Source: Wikimedia Commons; Thompson, Earl (2007), "The tulipmania: Fact or artifact?", Public Choice 130(1–2): 99–114

In the meantime, its rapid price rise and subsequent volatility, driven by speculative demand which is apparently itself speculation on that self-same demand, makes Bitcoin strongly resemble a tulip bubble – fuelled only until investors find another alternative investment to misallocate capital into.

Bitcoin as a means of exchange

In principle and on a purely technical level, Bitcoins function well as tokens that can be sent between parties – in a sense they are like 'cowrie shells in the sky'. However, in our view there are a number of practical matters that get in the way of Bitcoin functioning as a true currency. Among them are the following difficulties, broken down into three groups:

- Economic issues:
  - Being a *stable* store of value
  - Functioning as a unit of account and the lack of a real Bitcoin economy
  - Avoiding a deflationary spiral (hoarding is already a problem)
- Technical issues:
  - The 10 minute confirmation window, in particular regarding double spending
  - Scaling difficulties
  - The '51% attack'
- Regulation (or lack thereof), anonymity and exchanges

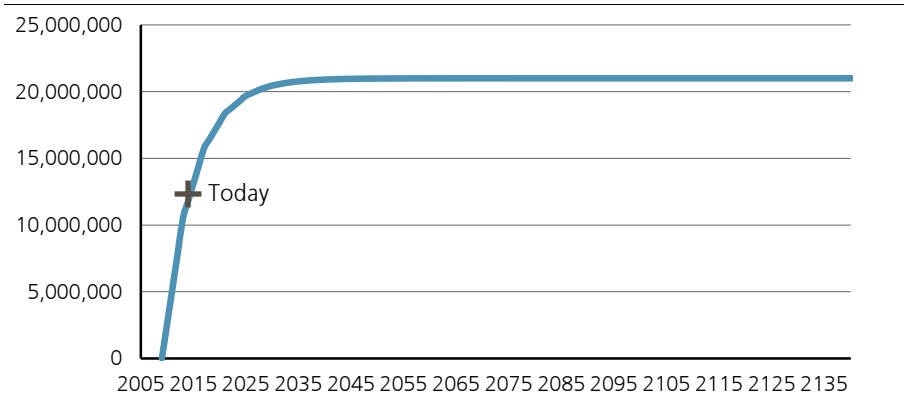
These points are key if Bitcoin is to function well as a true currency, and thus genuinely have some value that is beyond speculative. However, we do not believe that Bitcoin as it currently exists is adequately able to deal with these issues, and so in turn we are sceptical of the value Bitcoin can derive from its utility as a true currency.

Economic issues

Bitcoin suffers from significant volatility which also impedes its use as a unit of account

From the previous section, it is evident that Bitcoin suffers from significant price volatility. This is a serious problem for a currency, which needs to be a *stable* store of value – rather than just having some value – if people are to use it comfortably. To take an extreme example: if I have 1 Bitcoin in my pocket, and I can buy 1 laptop with it today, 2 tomorrow, but only half a laptop the day after that, the Bitcoin is no good as an effective value 'stopgap' over time, which is the ultimate point of using money to develop one step above a barter economy. This also prevents it from being a unit of account, which is another key feature of a currency – telling someone that something costs 2 Bitcoins means nothing if the value of a Bitcoin is unpredictable and volatile. Ultimately, this is why we have central banks to stabilise prices, but that is an antithesis of the Bitcoin philosophy.

Figure 9: Supply of bitcoin through time (# of bitcoins)



Source: http://en.bitcoin.it/wiki/Controlled_supply

Moreover, we do not see that it is possible for Bitcoin's value to sufficiently stabilise given its current form. Simply understood – assuming Bitcoin functions as a currency and not a speculative investment - the value of a Bitcoin should be the size of the Bitcoin economy (or 'bitcoinia') divided by the number of unit Bitcoin transactions (i.e. the velocity of money). The number of Bitcoins is completely known and predictable, and the blockchain allows exact measurement of transactions, but it is a question whether bitcoinia even really exists as a real economy. While a growing number of retailers (on- and off-line) accept Bitcoins, including a few larger players like Overstock, it effectively functions like a novelty payment system. These companies still need to pay their dues (to suppliers, employees etc.) in fiat currency. Given the volatility in the Bitcoin price and the lack of hedging products, these companies have to convert Bitcoins into fiat currency as soon as they can. Overstock has announced that they convert at the end of every day[14]. There is no economy that functions in terms of Bitcoin.

What should happen:

1BTC value = Bitcoin economy/ # of unit Bitcoin transactions

Assuming some form of bitcoinia exists, even if it is just companies using it as a payment system, the problems associated with the lack of a central monetary authority become apparent. There is no statistics agency to estimate the size of bitcoinia, leaving it to anyone's best guess. Even if there was, there is no way of altering the Bitcoin supply to track the growth of bitcoinia. This inelastic supply (often espoused as an advantage) poses a serious challenge. There is no denying that some form of bitcoinia is growing as more merchants accept Bitcoin, and either way we can take growth as an assumption to align ourselves with Bitcoin's proponents. It is clear that anything close to fast growth leads to rapid deflationary pressures. Thus, assuming demand for Bitcoin as a currency exceeds growth of the Bitcoin supply (only minimal demand growth is needed for this), the value of Bitcoin relative to goods and services will also increase. In such an environment, merchants would have to lower their prices – as denominated in Bitcoin – to remain competitive in bitcoinia. This brings with it the problem of hoarding, which is ultimately detrimental to any kind of Bitcoin economy. Some of Bitcoin's proponents defend this by reminding us that Bitcoins are divisible down to 0.00000001 BTC. This does solve the problem of 1 BTC being an unwieldy unit of account, but it does not preclude the fact that if I hold on to my 1 Bitcoin I might be able to buy more with it next week.

Given its semi-fixed supply, Bitcoin is fundamentally volatile and deflationary

[14] 'Big US online retailer to accept Bitcoin', Financial Times, 20-Dec-2013

Figure 10: Bitcoin holdings by wealthiest addresses

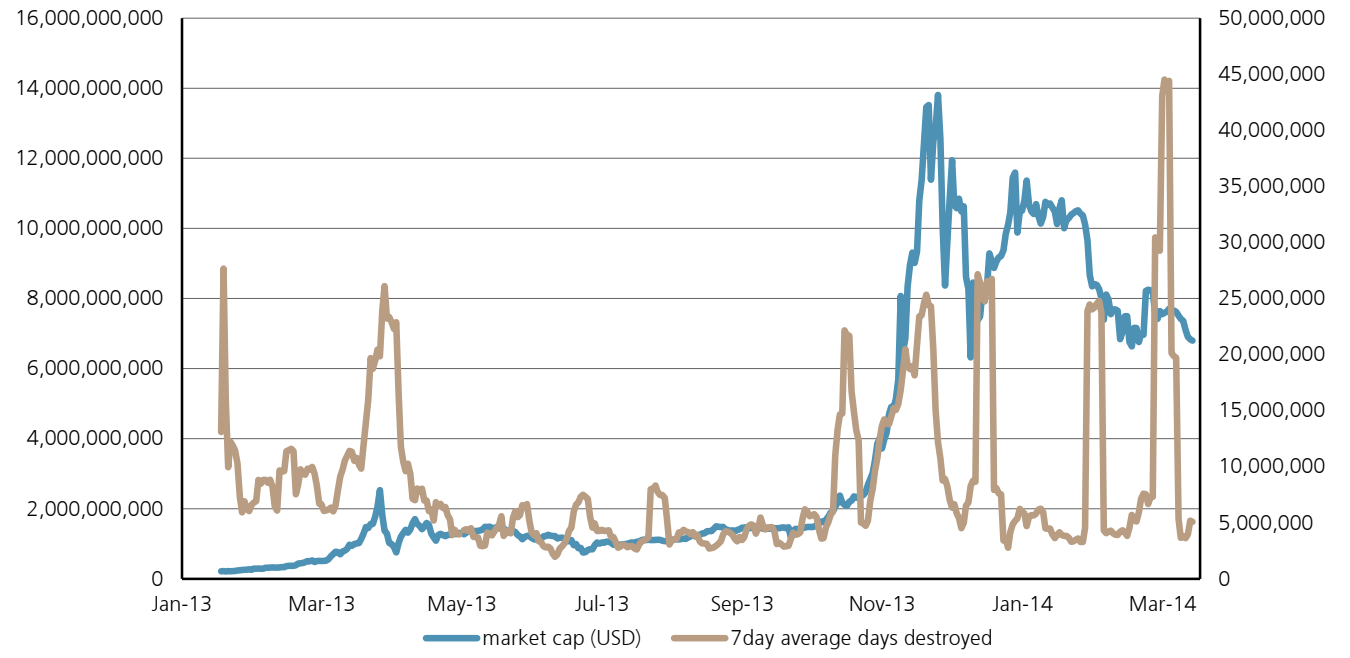
	Number of bitcoins	% of total
Total	12,553,750	
FBI holding	114,342	1%
Top 100 addresses	2,396,851	19%
Top 500 addresses	4,100,161	33%
---	---	
Unique addresses used per day (indicative)	*140,000*	

Source: bitcoinrichlist.com, retrieved 24-Mar-2014

Hoarding is already a serious problem for Bitcoin…

Finally, there is already evidence that hoarding is becoming a serious problem for Bitcoin. Figure 10 gives some known and estimated holdings of Bitcoins and Figure 9 shows Bitcoin days destroyed. Starting with the former, an analysis of the blockchain by bitcoinrichlist.com shows that the top 100 addresses own 19% of all Bitcoins, and the top 500 own 33%. As an order of magnitude comparison, approximately 140,000 unique addresses are used each day. The point has been made that some of these addresses probably belong to exchanges, which pool users' Bitcoins, but ultimately each address is still controlled by one person at most. At the same time the same individual or entity often has multiple addresses, so this statistic shows an extremely high concentration of wealth. If a wealthy exchange or other 'concentrator of wealth' were to get hacked, a rapid sell-off starting at that address could easily crash the Bitcoin market. We also see in Figure 10 that following the closure of the Silk Road (an online marketplace in illicit goods) and the seizure of its assets, the US government has ended up owning the single address with the most Bitcoins, amounting to 1% of all Bitcoins. This is an ironic twist of fate given Bitcoin's libertarian political agenda, as the US government has already amassed an influential stake.

Figure 11: Bitcoin market cap (USD, lhs), 7 Day moving average Bitcoin days destroyed (rhs).



Source: blockchain.info, UBS estimates

Bitcoin days destroyed is a measure that multiplies the number of Bitcoins spent in a transaction by the days they have lain dormant. This means 1 Bitcoin spent after 100 days of sitting dormant is worth the same as 100 Bitcoins spent after 1 day of sitting dormant, and is meant to be some indication of the real economic activity taking place in bitcoinia. Unsurprisingly, periods of high price volatility correlate to periods with lots of Bitcoin days destroyed, presumably as early adopters cash out. January saw very low Bitcoin days destroyed while the price stayed high, suggesting that Bitcoins were being hoarded. The latest sell-off was prompted by withdrawal problems at fiat currency exchanges starting with Mt Gox, culminating in its bankruptcy (while other exchanges have returned to normal operation). The subsequent spike relates to a movement of very old coins from Mt Gox. For now, days destroyed have quickly dropped back to lows, suggesting a return to the status quo of incremental hoarding.

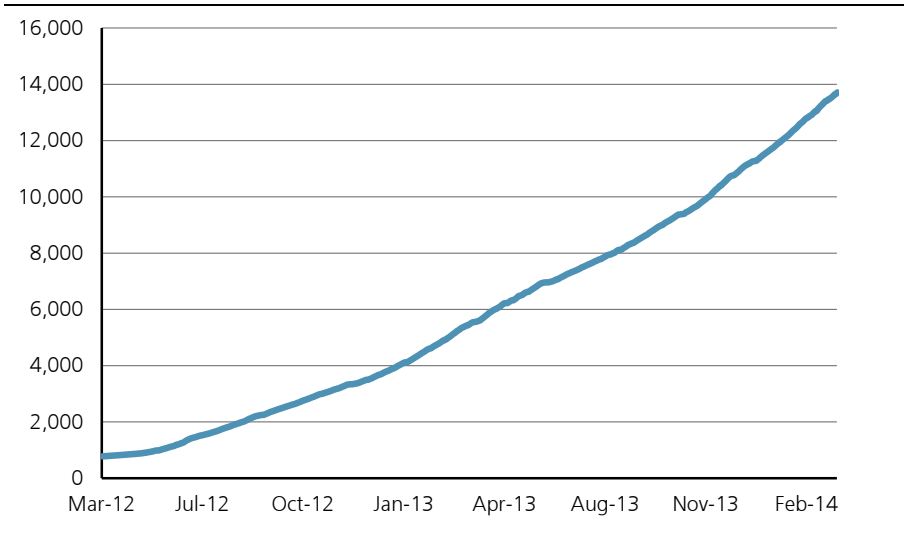
…and puts it at risk of sell-offs

Technical issues

The fundamental nature of the Bitcoin network is that it takes 10 minutes for an initial transaction confirmation, and it is even recommended that a user waits for several confirmations for full certainty. This is fine for large transactions e.g. buying a car, but impracticable for small transactions e.g. buying a coffee. As things stand, the only solution is zero-confirmation transactions – trusting the user to not double-spend during that 10 minute confirmation window. Nevertheless, there is nothing to stop a user from buying a coffee, walking into a neighbouring shop and buying another one within 10 minutes using the same Bitcoins. Ultimately, only one consensus will form and one coffee shop will be left short. Given the decentralised and anonymous (or pseudonymous) nature of Bitcoin, there is no way for the shop to chase the user for their debt. We see this as a significant problem for the widespread use of Bitcoin for everyday transactions, as the system currently stands.

The 10-minute confirmation window brings intractable double-spending risk

Figure 12: Size of the blockchain (MB)



Source: blockchain.info

The way Bitcoin mining works also brings technical obstacles. One is the difficulty of scaling the Bitcoin system to a mass scale. Bitcoin is currently limited to handling 7 transactions per second (tps), and in reality handles less than 1tps most of the time. This compares with Visa which handles thousands of transactions per second. Bitcoin's capacity could be lifted by increasing the allocated size of each block, but this still leaves other obstacles to scalability: an ever-increasing

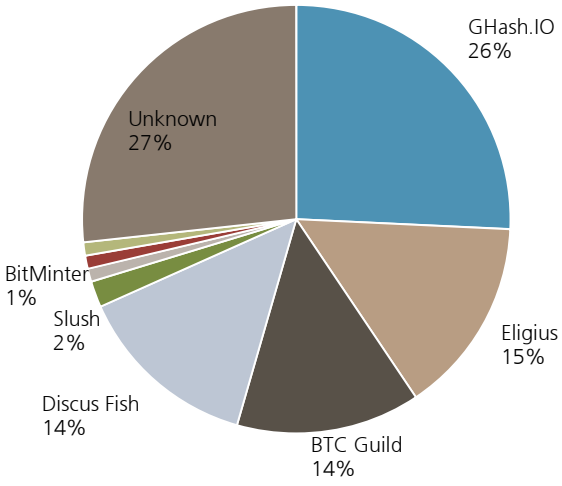
Bitcoin is currently limited to 7 transactions per second (and handles <1tps); Visa does thousands

blockchain, and the sheer amount of computing power required on top of that which is already employed.

Bitcoin is already very computer resource intensive - unnecessarily

The blockchain currently stands at about 14GB, which is approximately the size of a large computer game or a few Blu-ray films – not entirely unwieldy, but still inconvenient. However, should the network start handling even 10s of transactions per second, this would quickly escalate to hundreds of gigabytes, and at mass Visa-level scales this is thousands upon thousands of gigabytes, which would make running a full wallet completely impracticable for ordinary consumers. Moreover, an enormous amount of computing power is already being expended on maintaining the Bitcoin network, currently comparable to hundreds of thousands of petaflops[15] (a standard measure of computing power). By comparison, the top 500 supercomputers in the world have a combined computing power of about 250 petaflops[16]. If Bitcoin was really to scale up, it would consume an inordinate amount of computing power and electricity, which is seemingly unnecessary as less intensive consensus-building technologies are out there (as we briefly look at in the 'Alternatives' section).

Figure 13: 4-day average share of hash rate by mining pool



Source: blockchain.info, retrieved 24-Mar-2014

If a mining pool controls 51% of computing resources, it can destroy Bitcoin

Finally, a problem at the heart of the decentralised Bitcoin model is the '51% attack'. Due to the fact that individual miners might go a long time before seeing a Bitcoin pay-out, they have developed mining pools where the Bitcoins 'won' by the pool through mining are shared equally. Should a mining pool command 51% of the computing power, they would collectively be able to tamper with the blockchain and compromise the integrity of Bitcoin. This is already a real risk – the mining pool GHash.io recently controlled up to 45% of the network's computing power. The group has promised not to breach 51%, and regardless has argued it would not be in their interest to compromise Bitcoin if they did because then their rewards would be worthless. However, a non-financially motivated actor could still destroy the Bitcoin network, and even one with financial motivations could wish to do that in an effort to make people flock to an alternative digital currency where they stand to profit.

[15] http://www.bitcoinwatch.com/. On a technical note, Bitcoin ASIC miners do not actually perform floating point operations, so FLOPS are not a directly applicable unit here.
[16] http://www.top500.org/lists/2013/11/

Regulation (or lack thereof), anonymity and exchanges

Broadly speaking, Bitcoin remains largely unregulated[17]. There have been few outright bans (with the notable exception of heavy restrictions in China and a ban in Russia), but from the user's perspective there is also little promise of security such as deposit insurance.

Mt Gox shows the fallibility of fiat currency exchanges, but is not a systemic blow to Bitcoin

The most notable example of failure is the recent closure of Mt Gox, one of Bitcoin's oldest and previously largest exchanges. Mt Gox had been having problems for months, initially with withdrawals which were eventually suspended. Now the exchange has completely closed down, filed for bankruptcy and most of its users' Bitcoins have gone as well. The ultimate reasons behind the bankruptcy are unclear and possibly come down to simple theft. Crucially, this does not impact the rest of the Bitcoin system in that the network is unaffected and Bitcoin transactions are going through as normal. The key takeaway is that third parties which store users' Bitcoins and facilitate fiat currency conversions are fallible, and offer no protection to the consumer. This is bad for sentiment and impedes Bitcoin's ability to take off as a currency (given that most users acquire their Bitcoin's through purchase with fiat currency, and would prefer to store them on a third party wallet for convenience). However, it does not represent a systemic failure in Bitcoin's technology (as evidenced by the continued running of other large exchanges).

The Silk Road shutdown demonstrated Bitcoin's potential for anonymous transactions…

Another notable scandal involving Bitcoin was the Silk Road closure. Prior to widespread press coverage of Bitcoin, the online market, Silk Road, provided an anonymous marketplace whereby all transactions were conducted with Bitcoin.[18] While listings on Silk Road covered dozens of legitimate categories including books, apparel, and digital goods, it also provided a marketplace for illicit drugs and other illegal activities. Eventually, Silk Road attracted the attention of the FBI, which proceeded to arrest the owner and confiscate the Bitcoins held by Silk Road (c.144,000 BTC).

…but Bitcoin is not anonymous, it is pseudonymous

On the flip side, Bitcoin is not as anonymous as it is sometimes made out to be, given that all transactions are logged in the blockchain. Rather, it is pseudonymous – Bitcoin addresses are anonymous in principle, but their owners can be tracked, especially by governments and courts that have the power to subpoena organizations such as exchanges or online wallets to give up the identities of their clients. Even without these powers, blockchain analysis can compromise anonymity to a significant extent, as has been investigated by researchers from UCSD and George Mason University[19].

---

[17] http://www.coindesk.com/information/is-bitcoin-legal/ provides a good overview of individual jurisdictions and developments

[18] During this time period (February 2011 – July 2012), Bitcoins were relatively stable with an approx. exchange rate of $3 - $5 per Bitcoin. Silk Road provided a hedging service that would guarantee the value of Bitcoins, with Silk Road carrying the risk.

[19] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. 2013. A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference (IMC '13). ACM, New York, NY, USA, 127-140.

Bitcoin exchanges are not free from intervention

On that topic, while the Bitcoin network on its own is free from government intervention and smoothly functioning, the exchanges that facilitate exchange between Bitcoin and fiat currency are not necessarily so. They do come under government intervention, as we have seen in China in particular, but also when it comes to anti-money laundering rules in other countries[20]. Moreover, exchanges are subject to the problems and delays present in ordinary financial transactions (be it by bank transfer, credit card or otherwise) and the administration required for keeping track of their users. This significantly impacts Bitcoin's usability for ordinary users and is made apparent in the variety of prices that we see on exchanges as seen in Figure 14. Some Bitcoin traders do attempt to play this arbitrage, but the width of these gaps and their stubbornness are an obvious sign of the inefficiency present in Bitcoin exchanges.

Tax treatment as a capital asset is key to future developments

Finally, the tax treatment of Bitcoin recently clarified by the IRS will be a driving factor in Bitcoin's future development. Since the IRS intends to treat Bitcoin as a capital asset, this will create a significant compliance and reporting burden on users. Based on a preliminary reading of the IRS's position, every exchange of virtual currency for other property can result in a gain or loss for tax purposes if the fair market value of the good or service received exceeds the adjusted basis of the Bitcoins. This would result in the need to track adjusted basis for every Bitcoin and self-reporting on every transaction, significantly increasing the cost and difficulty of conducting small transactions. On the flip side, treatment as a capital asset also entitles Bitcoin to take advantage of the preferential long term capital gains rate assuming such Bitcoins are held for at least one year.

Other jurisdictions including Japan and Finland have classified Bitcoin as a commodity (i.e. a taxable asset), while the UK has scrapped VAT on Bitcoin transactions and mining – so an international consensus is still forming and this remains a key risk.

Figure 14: Snapshot of USD prices per 1BTC at various exchanges

Exchange	Latest price	Deviation from median
bitKonan	599	+7.0%
Camp BX	570	+1.8%
Crypto-Trade	569	+1.6%
Kraken	564	+0.8%
BTC-E	563	+0.6%
Justcoin	563	+0.6%
hitbtc	560	+0.0%
Ripple	559	-0.2%
Bitfinex	558	-0.4%
BitStamp	558	-0.4%
Asia Nexgen	557	-0.6%
The Rock Trading Company	551	-1.6%
LakeBTC.com	539	-3.7%

Source: bitcoincharts.com. Retrieved 24-Mar-2014

[20] The FinCEN in the USA has published explicit guidelines: http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

Bitcoin, banks and the future

Two separable sides to Bitcoin: political and technical

There are inherently two aspects to Bitcoin: the political and the technical. Politically, Bitcoin has stood for a broadly libertarian, internationalist agenda. Its key political features are supposed to be that it is free from government intervention or any kind of central authority at all, that it is a complete break from the existing financial system and that it provides anonymity to its users. This side of Bitcoin has driven initial interest and subsequently a substantial amount of media attention, especially in the wake of the financial crisis. However, these features are not integral to Bitcoin from a technical perspective.

Bitcoin is technically elegant and stands to benefit from regulation and development

Technically, Bitcoin provides an elegant solution to the double spend problem and is also (theoretically) a remarkably robust and secure network. The political agenda does not play an integral part here – as an extreme example, governments could require all citizens to register their Bitcoin addresses with the Ministry of Finance, which would have no impact on the technology of Bitcoin. More generally, we see that Bitcoin is currently in a slightly 'Wild West' phase, and it could potentially have much to benefit from what we call 'institutionalisation', whereby it is absorbed into certain existing regulatory and financial structures. Technologically, we see Bitcoin as a first iteration of a digital currency which could be improved on.

Do we really need a new currency?

Ultimately, an institutionalised, technologically different digital currency may no longer be Bitcoin with a capital 'B'. Indeed, we are sceptical on the need for a new true currency, but we see potential for Bitcoin as the foundations of a new payment system.

Institutionalising Bitcoin

Apart from in China and Russia which have played a more active role in regulation, the legal and regulatory framework for Bitcoin is still generally lacking. Users want security in the form of deposit insurance, and anti-money laundering and taxation is a concern for governments (and society at large). The US government has already shown that it can tackle illicit Bitcoin activity (e.g. "Bitcoin champion on laundering charge", Financial Times 27-Jan-14). Ultimately, without the possibility of this kind of anti-criminal control, governments would have to ban Bitcoin and similar digital currencies outright.

Taking this further, for Bitcoin to be a true currency, it would need a way of controlling its money supply to stabilise its value (like a central bank) – but outside of the libertarian agenda there seems to be no reason why a new currency as such is necessary.

Bitcoin is already used as a cheap international money transfer mechanism, and could be institutionalised as such

Instead, technologically, Bitcoin does provide a revolutionary new payment system. Bitcoin is already used as a cheap form of international money transfer – a market for which it arguably shows the most promise. In principle, financial institutions with existing anti-money laundering systems in place (like banks) could adopt a common Bitcoin-like technology to facilitate fast and secure international transfers between end-users, with fiat currencies as the unit of account (or possibly a digital currency serving purely as an intermediary), and minimal transaction costs. These institutions could also deal with bridging the confirmation time, by taking on the credit (and possibly FX) risk involved. By keeping track of users, they can also penalise or chase up those who attempt to defraud the system. This could be facilitated by new or existing entrants, although the question then becomes, given the costs associated with running a payments system, whether existing players like

Visa or MasterCard could be out-priced. We elaborate on this in the first section of the note.

Bitcoin is a first-generation tech product

With regard to technological issues, such as the 51% problem, the 10 minute transaction time, or the fact that Bitcoin is inordinately wasteful of electricity and computing resources – these are all first-generation problems that do have solutions. For instance, other mathematical processes can be used to discourage an arms race in mining, other consensus-building techniques exist to maintain decentralised transaction ledgers, and confirmation times can be reduced. Some of these are already being implemented in alternative digital currencies.

Alternatives

Over 90 other alternative digital currencies already exist [21], which already demonstrates the technological replaceability of Bitcoin. We isolate a few to comment on specific features in relation to Bitcoin.

Litecoin is one of the most prominent alternatives, often touted as the 'silver to Bitcoin's gold'. This only holds true in virtue of the fact that there are more Litecoins in circulation. One of the key features of Litecoin is that the mathematical problem involved in mining Litecoins is such that in principle no giant technological leap can be made to Litecoin-specific computers to be used as mining rigs. In theory, existing ordinary desktop computer processors are already as Litecoin-specific as a computer can get. Litecoin ASICs are still coming to market, but ought to have less of an impact than with Bitcoin. This means there is less of a computational arms-race and thus computer power and electricity aren't expended unnecessarily. Moreover, Litecoin has a reduced confirmation time of 2.5 minutes which makes it more practical without significantly reducing security, although it does run the risk of an excess of orphaned blocks. Nevertheless, Litecoin still suffers from the same problems of deflation and volatility related to an effectively fixed/predictable supply, and the vagaries of a ballooning blockchain.

Ripple is a system that is already moving down the payment system route, in that it allows transfers to be made in all currencies, as well as its own internal currency (also called the Ripple, or XRP). It uses a decentralised consensus-building system that is light on computation and based on a system of trusted links to nodes who you 'trust not to collude to defraud against you'. The security and integrity of this system is arguably still in question, but the principle of moving beyond simply a digital currency and towards a new payment infrastructure is promising. One of the potential issues is that Ripple is currently run by a private company called Opencoin, who control the software behind Ripple and also the money supply of XRP. This has the potential benefit of central bank-like management, but also the risk of abuse.

Auroracoin is a new digital currency founded in Iceland and based on Litecoin's technology, which aims to become an alternative currency for Icelanders in response to capital controls originating in the financial crisis. This is to be achieved by distributing half of Auroracoin's total supply to Icelanders in one go in a so-called 'Airdrop'. This has led it to rapidly rise in value, and it demonstrates the necessity of a functioning economy for an alternative currency to be viable. However, Auroracoin would still suffer from the same problems relating to an inelastic supply that Litecoin has. Moreover, there are still high risks to Auroracoin

[21] As identified on coinmarketcap.com

being able to take root in the Icelandic economy, not least because the Icelandic authorities would be obliged to react. **Aphroditecoin** is a similar concept, but with 75% of coins instead going to Cypriots.

Dogecoin is a novelty digital currency derived from Litecoin, just with some different parameters (such as the total number of Dogecoin and the rate they are produced at). Dogecoin was initially created as a joke based on an internet meme of a Shiba Inu dog called 'Doge', but currently commands the seventh highest market capitalization of all digital currencies. We believe this demonstrates two things: that Bitcoin is easily replaceable, and that the value of digital currencies is ultimately driven by speculative demand, sentiment and media attention, none of which bode well.

Figure 15: Top 7 digital currencies by market cap

Ranking		Market Cap (USD)	Price (USD)	Total Supply
1	Bitcoin	7,019,553,987	559.09	12,555,300 BTC
2	Ripple	1,244,439,206	0.012	99,999,996,204 XRP*
3	Litecoin	409,580,241	15.25	26,852,304 LTC
4	Auroracoin	153,408,498	14.43	10,630,551 AUR
5	Peercoin	63,780,922	3.00	21,254,587 PPC
6	Aphroditecoin	52,488,978	2.33	22,541,320 APH
7	Dogecoin	46,114,838	0.0073	63,351,792,537 DOGE

Source: coinmarketcap.com, retrieved 24-Mar-2014 *not mineable

Statement of Risk

Bitcoin and other digital currencies are a highly speculative, risky and experimental investment. We do not make any specific investment recommendations to buy or sell any of the digital currencies mentioned in this report or otherwise.

Required Disclosures

This report has been prepared by UBS Securities LLC, an affiliate of UBS AG. UBS AG, its subsidiaries, branches and affiliates are referred to herein as UBS.

For information on the ways in which UBS manages conflicts and maintains independence of its research product; historical performance information; and certain additional disclosures concerning UBS research recommendations, please visit www.ubs.com/disclosures. The figures contained in performance charts refer to the past; past performance is not a reliable indicator of future results. Additional information will be made available upon request. UBS Securities Co. Limited is licensed to conduct securities investment consultancy businesses by the China Securities Regulatory Commission.

Analyst Certification: Each research analyst primarily responsible for the content of this research report, in whole or in part, certifies that with respect to each security or issuer that the analyst covered in this report: (1) all of the views expressed accurately reflect his or her personal views about those securities or issuers and were prepared in an independent manner, including with respect to UBS, and (2) no part of his or her compensation was, is, or will be, directly or indirectly, related to the specific recommendations or views expressed by that research analyst in the research report.

UBS Investment Research: Global Equity Rating Definitions

UBS 12-Month Rating	**Definition**	**Coverage**[1]	**IB Services**[2]
Buy	FSR is > 6% above the MRA.	44%	36%
Neutral	FSR is between -6% and 6% of the MRA.	45%	35%
Sell	FSR is > 6% below the MRA.	11%	23%
UBS Short-Term Rating	**Definition**	**Coverage**[3]	**IB Services**[4]
Buy	Stock price expected to rise within three months from the time the rating was assigned because of a specific catalyst or event.	less than 1%	less than 1%
Sell	Stock price expected to fall within three months from the time the rating was assigned because of a specific catalyst or event.	less than 1%	less than 1%

Source: UBS. Rating allocations are as of 31 December 2013.
1:Percentage of companies under coverage globally within the 12-month rating category. 2:Percentage of companies within the 12-month rating category for which investment banking (IB) services were provided within the past 12 months.
3:Percentage of companies under coverage globally within the Short-Term rating category. 4:Percentage of companies within the Short-Term rating category for which investment banking (IB) services were provided within the past 12 months.

KEY DEFINITIONS: Forecast Stock Return (FSR) is defined as expected percentage price appreciation plus gross dividend yield over the next 12 months. **Market Return Assumption (MRA)** is defined as the one-year local market interest rate plus 5% (a proxy for, and not a forecast of, the equity risk premium). **Under Review (UR)** Stocks may be flagged as UR by the analyst, indicating that the stock's price target and/or rating are subject to possible change in the near term, usually in response to an event that may affect the investment case or valuation. **Short-Term Ratings** reflect the expected near-term (up to three months) performance of the stock and do not reflect any change in the fundamental view or investment case. **Equity Price Targets** have an investment horizon of 12 months.

EXCEPTIONS AND SPECIAL CASES: UK and European Investment Fund ratings and definitions are: Buy: Positive on factors such as structure, management, performance record, discount; **Neutral:** Neutral on factors such as structure, management, performance record, discount; **Sell:** Negative on factors such as structure, management, performance record, discount. **Core Banding Exceptions (CBE):** Exceptions to the standard +/-6% bands may be granted by the Investment Review Committee (IRC). Factors considered by the IRC include the stock's volatility and the credit spread of the respective company's debt. As a result, stocks deemed to be very high or low risk may be subject to higher or lower bands as they relate to the rating. When such exceptions apply, they will be identified in the Company Disclosures table in the relevant research piece.

Research analysts contributing to this report who are employed by any non-US affiliate of UBS Securities LLC are not registered/qualified as research analysts with the NASD and NYSE and therefore are not subject to the restrictions contained in the NASD and NYSE rules on communications with a subject company, public appearances, and trading securities held by a research analyst account. The name of each affiliate and analyst employed by that affiliate contributing to this report, if any, follows.

UBS Securities LLC: Derek De Vries, CFA; Jack Hwang. **UBS Limited:** John-Paul Crutchley; Ivan Jevremovic.

Unless otherwise indicated, please refer to the Valuation and Risk sections within the body of this report.

Global Disclaimer

This document has been prepared by UBS Securities LLC, an affiliate of UBS AG. UBS AG, its subsidiaries, branches and affiliates are referred to herein as UBS.

This document is for distribution only as may be permitted by law. It is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation or would subject UBS to any registration or licensing requirement within such jurisdiction. It is published solely for information purposes; it is not an advertisement nor is it a solicitation or an offer to buy or sell any financial instruments or to participate in any particular trading strategy. No representation or warranty, either express or implied, is provided in relation to the accuracy, completeness or reliability of the information contained in this document ('the Information'), except with respect to Information concerning UBS. The Information is not intended to be a complete statement or summary of the securities, markets or developments referred to in the document. UBS does not undertake to update or keep current the Information. Any opinions expressed in this document may change without notice and may differ or be contrary to opinions expressed by other business areas or groups of UBS. Any statements contained in this report attributed to a third party represent UBS's interpretation of the data, information and/or opinions provided by that third party either publicly or through a subscription service, and such use and interpretation have not been reviewed by the third party.

Nothing in this document constitutes a representation that any investment strategy or recommendation is suitable or appropriate to an investor's individual circumstances or otherwise constitutes a personal recommendation. Investments involve risks, and investors should exercise prudence and their own judgement in making their investment decisions. The financial instruments described in the document may not be eligible for sale in all jurisdictions or to certain categories of investors. Options, derivative products and futures are not suitable for all investors, and trading in these instruments is considered risky. Mortgage and asset-backed securities may involve a high degree of risk and may be highly volatile in response to fluctuations in interest rates or other market conditions. Foreign currency rates of exchange may adversely affect the value, price or income of any security or related instrument referred to in the document. For investment advice, trade execution or other enquiries, clients should contact their local sales representative.

The value of any investment or income may go down as well as up, and investors may not get back the full amount invested. Past performance is not necessarily a guide to future performance. Neither UBS nor any of its directors, employees or agents accepts any liability for any loss (including investment loss) or damage arising out of the use of all or any of the Information.

Any prices stated in this document are for information purposes only and do not represent valuations for individual securities or other financial instruments. There is no representation that any transaction can or could have been effected at those prices, and any prices do not necessarily reflect UBS's internal books and records or theoretical model-based valuations and may be based on certain assumptions. Different assumptions by UBS or any other source may yield substantially different results.

Research will initiate, update and cease coverage solely at the discretion of UBS Investment Bank Research Management. The analysis contained in this document is based on numerous assumptions. Different assumptions could result in materially different results. The analyst(s) responsible for the preparation of this document may interact with trading desk personnel, sales personnel and other parties for the purpose of gathering, applying and interpreting market information. UBS relies on information barriers to control the flow of information contained in one or more areas within UBS into other areas, units, groups or affiliates of UBS. The compensation of the analyst who prepared this document is determined exclusively by research management and senior management (not including investment banking). Analyst compensation is not based on investment banking revenues; however, compensation may relate to the revenues of UBS Investment Bank as a whole, of which investment banking, sales and trading are a part.

For financial instruments admitted to trading on an EU regulated market: UBS AG, its affiliates or subsidiaries (excluding UBS Securities LLC) acts as a market maker or liquidity provider (in accordance with the interpretation of these terms in the UK) in the financial instruments of the issuer save that where the activity of liquidity provider is carried out in accordance with the definition given to it by the laws and regulations of any other EU jurisdictions, such information is separately disclosed in this document. For financial instruments admitted to trading on a non-EU regulated market: UBS may act as a market maker save that where this activity is carried out in the US in accordance with the definition given to it by the relevant laws and regulations, such activity will be specifically disclosed in this document. UBS may have issued a warrant the value of which is based on one or more of the financial instruments referred to in the document. UBS and its affiliates and employees may have long or short positions, trade as principal and buy and sell in instruments or derivatives identified herein; such transactions or positions may be inconsistent with the opinions expressed in this document.

United Kingdom and the rest of Europe: Except as otherwise specified herein, this material is distributed by UBS Limited to persons who are eligible counterparties or professional clients. UBS Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. **France:** Prepared by UBS Limited and distributed by UBS Limited and UBS Securities France S.A. UBS Securities France S.A. is regulated by the ACP (Autorité de Contrôle Prudentiel) and the Autorité des Marchés Financiers (AMF). Where an analyst of UBS Securities France S.A. has contributed to this document, the document is also deemed to have been prepared by UBS Securities France S.A. **Germany:** Prepared by UBS Limited and distributed by UBS Limited and UBS Deutschland AG. UBS Deutschland AG is regulated by the Bundesanstalt fur Finanzdienstleistungsaufsicht (BaFin). **Spain:** Prepared by UBS Limited and distributed by UBS Limited and UBS Securities España SV, SA. UBS Securities España SV, SA is regulated by the Comisión Nacional del Mercado de Valores (CNMV). **Turkey:** Distributed by UBS Limited. No information in this document is provided for the purpose of offering, marketing and sale by any means of any capital market instruments and services in the Republic of Turkey. Therefore, this document may not be considered as an offer made or to be made to residents of the Republic of Turkey. UBS AG is not licensed by the Turkish Capital Market Board under the provisions of the Capital Market Law (Law No. 6362). Accordingly, neither this document nor any other offering material related to the instruments/services may be utilized in connection with providing any capital market services to persons within the Republic of Turkey without the prior approval of the Capital Market Board. However, according to article 15 (d) (ii) of the Decree No. 32, there is no restriction on the purchase or sale of the securities abroad by residents of the Republic of Turkey. **Poland:** Distributed by UBS Limited (spolka z ograniczona odpowiedzialnoscia) Oddzial w Polsce. **Russia:** Prepared and distributed by UBS Securities CJSC. **Switzerland:** Distributed by UBS AG to persons who are institutional investors only. **Italy:** Prepared by UBS Limited and distributed by UBS Limited and UBS Italia Sim S.p.A. UBS Italia Sim S.p.A. is regulated by the Bank of Italy and by the Commissione Nazionale per le Società e la Borsa (CONSOB). Where an analyst of UBS Italia Sim S.p.A. has contributed to this document, the document is also deemed to have been prepared by UBS Italia Sim S.p.A. **South Africa:** Distributed by UBS South Africa (Pty) Limited, an authorised user of the JSE and an authorised Financial Services Provider. **Israel:** This material is distributed by UBS Limited. UBS Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. UBS Securities Israel Ltd is a licensed Investment Marketer that is supervised by the Israel Securities Authority (ISA). UBS Limited and its affiliates incorporated outside Israel are not licensed under the Israeli Advisory Law. This Material is being issued only to and/or is directed only at persons who are Qualified Investors within the meaning of the Israeli Advisory Law, and this material must not be relied on or acted upon by any other persons. **Saudi Arabia:** This document has been issued by UBS AG (and/or any of its subsidiaries, branches or affiliates), a public company limited by shares, incorporated in Switzerland with its registered offices at Aeschenvorstadt 1, CH-4051 Basel and Bahnhofstrasse 45, CH-8001 Zurich. This publication has been approved by UBS Saudi Arabia (a subsidiary of UBS AG), a Saudi closed joint stock company incorporated in the Kingdom of Saudi Arabia under commercial register number 1010257812 having its registered office at Tatweer Towers, P.O. Box 75724, Riyadh 11588, Kingdom of Saudi Arabia. UBS Saudi Arabia is authorized and regulated by the Capital Market Authority to conduct securities business under license number 08113-37. **United States:** Distributed to US persons by either UBS Securities LLC or by UBS Financial Services Inc., subsidiaries of UBS AG; or by a group, subsidiary or affiliate of UBS AG that is not registered as a US broker-dealer (a **'non-US affiliate'**) to major US institutional investors only. UBS Securities LLC or UBS Financial Services Inc. accepts responsibility for the content of a document prepared by another non-US affiliate when distributed to US persons by UBS Securities LLC or UBS Financial Services Inc. All transactions by a US person in the securities mentioned in this document must be effected through UBS Securities LLC or UBS Financial Services Inc., and not through a non-US affiliate. **Canada:** Distributed by UBS Securities Canada Inc., a registered investment dealer in Canada and a Member-Canadian Investor Protection Fund, or by another affiliate of UBS AG that is registered to conduct business in Canada or is otherwise exempt from registration. **Brazil:** Except as otherwise specified herein, this material is prepared by UBS Brasil CCTVM S.A. to persons who are eligible investors residing in Brazil, which are considered to be: (i) financial institutions, (ii) insurance firms and investment capital companies, (iii) supplementary pension entities, (iv) entities that hold financial investments higher than R$300,000.00 and that confirm the status of qualified investors in written, (v) investment funds, (vi) securities portfolio managers and securities consultants duly authorized by Comissão de Valores Mobiliários (CVM), regarding their own investments, and (vii) social security systems created by the Federal Government, States, and Municipalities. **Hong Kong:** Distributed by UBS Securities Asia Limited. **Singapore:** Distributed by UBS Securities Pte. Ltd. [mica (p) 107/09/2013 and Co. Reg. No.: 198500648C] or UBS AG, Singapore Branch. Please contact UBS Securities Pte. Ltd., an exempt financial adviser under the Singapore Financial Advisers Act (Cap. 110); or UBS AG, Singapore Branch, an exempt financial adviser under the Singapore Financial Advisers Act (Cap. 110) and a wholesale bank licensed under the Singapore Banking Act (Cap. 19) regulated by the Monetary Authority of Singapore, in respect of any matters arising from, or in connection with, the analysis or document. The recipients of this document represent and warrant that they are accredited and institutional investors as defined in the Securities and Futures Act (Cap. 289). **Japan:** Distributed by UBS Securities Japan Co., Ltd. to institutional investors only. Where this document has been prepared by UBS Securities Japan Co., Ltd., UBS Securities Japan Co., Ltd. is the author, publisher and distributor of the document. Distributed by UBS AG, Tokyo Branch to Professional Investors (except as otherwise permitted) in relation to foreign exchange and other banking businesses when relevant. **Australia:** 1) Distributed by UBS AG (Holder of Australian Financial Services License No. 231087) and/or UBS Securities Australia Ltd (Holder of Australian Financial Services License No. 231098). The Information in this document has been prepared without taking into account any investor's objectives, financial situation or needs, and investors should, before acting on the Information, consider the appropriateness of the Information, having regard to their objectives, financial situation and needs. If the Information contained in this document relates to the acquisition, or potential acquisition of a particular financial product by a 'Retail' client as defined by section 761G of the Corporations Act 2001 where a Product Disclosure Statement would be required, the retail client should obtain and consider the Product Disclosure Statement relating to the product before making any decision about whether to acquire the product. 2) Clients of UBS Wealth Management Australia Ltd: This notice is distributed to clients of UBS Wealth Management Australia Ltd ABN 50 005 311 937 (Holder of Australian Financial Services Licence No. 231127), Chifley Tower, 2 Chifley Square, Sydney, New South Wales, NSW 2000, by UBS Wealth Management Australia Ltd. This Document contains general information and/or general advice only and does not constitute personal financial product advice. As such the content of the Document was prepared without taking into account the objectives, financial situation or needs of any specific recipient. Prior to making any investment decision, a recipient should obtain personal financial product advice from an independent adviser and consider any relevant offer documents (including any product disclosure statement) where the acquisition of financial products is being considered. UBS AG is authorised to provide financial product advice in relation to foreign exchange contracts in Australia, and as such UBS AG is responsible for all general advice on foreign exchange and currencies contained herein. **New Zealand:** Distributed by UBS New Zealand Ltd. The information and recommendations in this publication are provided for general information purposes only. To the extent that any such information or recommendations constitute financial advice, they do not take into account any person's particular financial situation or goals. We recommend that recipients seek advice specific to their circumstances from their financial advisor. **Dubai:** The research distributed by UBS AG Dubai Branch is intended for Professional Clients only and is not for further distribution within the United Arab Emirates. **Korea:** Distributed in Korea by UBS Securities Pte. Ltd., Seoul Branch. This document may have been edited or contributed to from time to time by affiliates of UBS Securities Pte. Ltd., Seoul Branch. **Malaysia:** This material is authorized to be distributed in Malaysia by UBS Securities Malaysia Sdn. Bhd (253825-x). **India:** Prepared by UBS Securities India Private Ltd. 2/F, 2 North Avenue, Maker Maxity, Bandra Kurla Complex, Bandra (East), Mumbai (India) 400051. Phone: +912261556000 SEBI Registration Numbers: NSE (Capital Market Segment): INB230951431, NSE (F&O Segment) INF230951431, BSE (Capital Market Segment) INB010951437.

The disclosures contained in research documents produced by UBS Limited shall be governed by and construed in accordance with English law.