Global Macro Research

Top of Mind

March 11, 2014

Issue 21

All About Bitcoin

From the editor: News about Bitcoin seems to be everywhere. So what is it? The short answer is that Bitcoin with a capital "B" is a peer-to-peer network that allows for the proof and transfer of ownership without the need for a trusted third party. The unit of that network is bitcoin with a little "b". But agreement on the topic seems to end there; indeed, there is a deep divide between true Bitcoin believers and serious skeptics. We look at the range of wildly diverging views. So where does that leave us? With the conclusion that bitcoin likely can't work as a currency, but some sense that the ledger-based technology that underlies it could hold promise.

Source: www.istockphoto.com

Inside

> "There is no question that the most vulnerable point of the entire Bitcoin network is the exchanges…the key challenges have not been [thefts and attacks] but governance issues… exchanges should be the focus of most regulations."
> **Dmitry Dain**

> "The core technological problem that [Bitcoin] has solved has never been solved before… the ability to prove and transfer ownership without the need for a trusted third party…payments is the first application of [this]…but there are more."
> **Fred Ehrsam**

> "[Bitcoin] would not be a good substitute [for fiat currency] because we actually do want the government to control the money supply…and advantages of using bitcoin over existing payment systems…are not as obvious as they might seem."
> **Eric Posner**

Editor: Allison Nathan | allison.nathan@gs.com | +1 (212) 357-7504 | Goldman, Sachs & Co.
Macro Executive Committee: Jeffrey Currie | Jan Hatzius | Kathy Matsui | Timothy Moe | Peter Oppenheimer | Dominic Wilson

Macro news and views

We provide a brief snapshot on the most important economies for the global markets

US

Latest GS proprietary datapoints/major changes in views

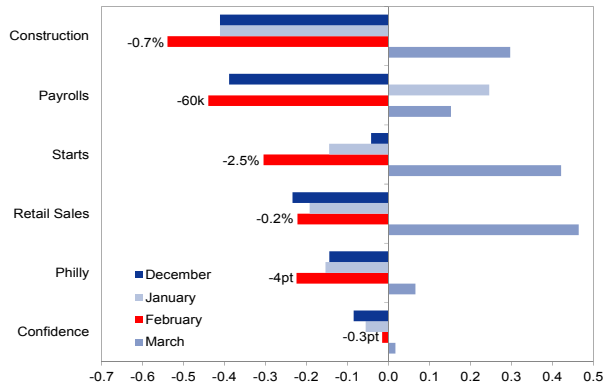
- Our Current Activity Indicator (CAI) averaged 1.8% over the three months ended in February, down from the roughly 2.75% rate of the preceding six months.

Datapoints/trends we're focused on

- Less-than-expected impact of poor weather on Feb payrolls.
- The extent to which recent economic weakness owes to adverse weather, accounting for a bit more than half of the decline in the CAI (0.5 pp), in our estimation. We expect a Spring bounce-back.
- The return to a fairly "normal" fiscal policy situation with the smooth increase in the debt ceiling.

Weather woes

Weather impact on key indicators



Source: Goldman Sachs Global Investment Research.

Japan

Latest GS proprietary datapoints/major changes in views

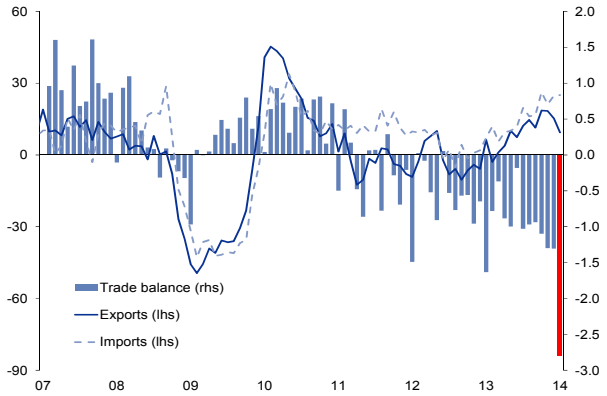
- Based on the weak Q4 GDP, we have revised down our FY2013-14 GDP growth forecasts to +2.2% (from +2.4%) and +0.5% (from +0.7%).

Datapoints/trends we're focused on

- Rush demand ahead of the April tax hike, production to meet the demand has likely neared or reached its peak.
- Much lower-than-expected October-December real GDP of 1.0% largely owing to weak net exports despite the weaker JPY.
- Largest trade deficit on record in January as imports rose sharply.

Largest trade deficit on record

yoy % chg (lhs), JPY tn (rhs)



Source: Japanese Ministry of Finance.

Euro Area (EA)

Latest GS proprietary datapoints/major changes in views

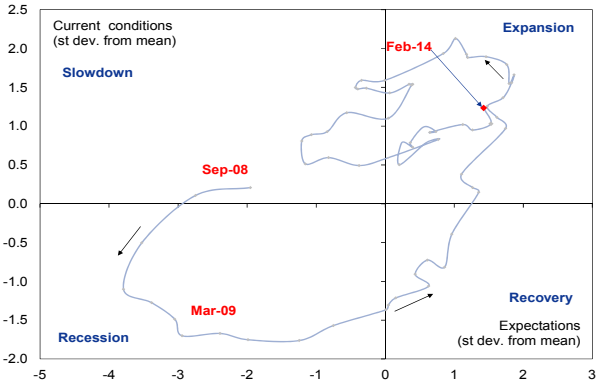
- We raised our 2014 EA GDP forecast by 0.1% to 1.2% factoring in Q4 GDP and recent indicators. We lowered our 2014 inflation forecast to 0.9%, and now expect it to trough at 0.4% in March.

Datapoints/trends we're focused on

- Continued weakness of broad money growth and bank credit creation despite improving growth.
- Further increases in Germany's IFO business survey.
- Prospects of the new Italian government led by Matteo Renzi.

Increasing IFO

German IFO "business expectations" subcomponent



Source: Ifo, Goldman Sachs Global Investment Research.

Emerging Markets (EM)

Latest GS proprietary datapoints/major changes in views

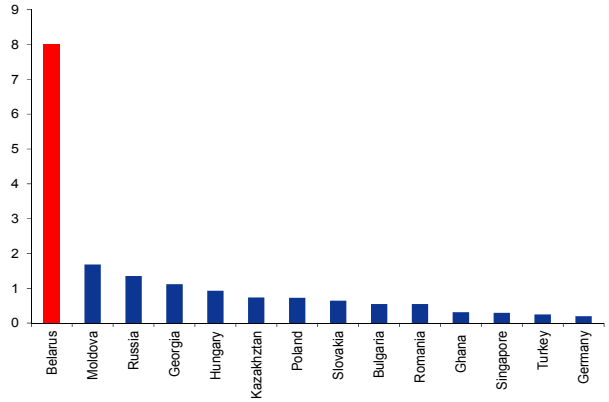
- We modestly lowered 1H2014 China GDP growth to reflect slowing domestic growth momentum, a relatively tight monetary policy stance in late 2013, and expectations of a slightly softer US recovery.

Datapoints/trends we're focused on

- Potential for Ukraine to trigger a fresh round of pressures in CEEMEA and broader EM assets.
- Tighter EM financial conditions increasing the risk of lower EM economic growth - despite the DM recovery.

Ukraine exposure

Exports to Ukraine as a share of GDP, %



Source: Haver Analytics, Goldman Sachs Global Investment Research.

All About Bitcoin

News about Bitcoin suddenly seems to be everywhere. The severe technological and security problems that have led to the outright collapse of Mt. Gox – the largest bitcoin exchange globally - on top of the stunning spike in bitcoin prices by more than five-fold late last year and spectacular collapse (then some rebound!) since, some high-profile arrests in the Bitcoin universe, and a swath of regulators and government officials beginning to weigh in on the subject have pushed Bitcoin and digital currencies to Top of Mind.

So what is Bitcoin? The short answer is that Bitcoin with a capital "B" is a peer-to-peer network that allows for the proof and transfer of ownership without the need for a trusted third party. The unit of that network is bitcoin with a little "b" (for a longer answer, see the box, and for even more details, see page 12). But while there seems to be broad consensus on this basic definition, agreement on the topic ends there; indeed, there seems to be a very deep divide between true Bitcoin believers and serious skeptics. In an effort to consider the range of wildly diverging views, we include many more external interviews than usual.

To start, some of the fiercest believers seem to grab on to the ideology of Bitcoin as providing an escape from centralized control, in particular viewing bitcoin as a new currency free from the grips of any government or central bank. On the other hand, some of the deepest skepticism surrounds the viability of bitcoin as a currency. **Eric Posner**, Professor of Law at the University of Chicago, believes that bitcoin would be a poor substitute for fiat currency, and would be unable to overcome likely government opposition as well as public distrust even if it weren't. **Dominic Wilson and Jose Ursua** of Goldman Sachs' markets research team also conclude that difficulties bitcoin faces as a store of value are likely to present a major roadblock to its adoption as a medium of exchange – the two key properties of a currency. And **Jeff Currie**, Head of Goldman Sachs commodities research, finds that bitcoin's attributes make it a commodity rather than a currency, but he also believes it is unlikely to replace gold as a commodity store of value.

Daniel Masters, Co-Principal of traditionally commodity-focused hedge fund, Global Advisors, also views Bitcoin opportunities within a commodities framework, and sees parallels between bitcoin and silver, which saw an explosive rise in price as new investors and users entered the market. However, it is precisely the fact that the vast majority of new entrants so far have been investors that has led some to conclude that this is nothing more than a speculative bubble, perhaps already in the midst of bursting.

While the above disagreements primarily revolve around the value of bitcoin – the unit - there is also some debate around the promises of Bitcoin – the technology. **Fred Ehrsam.** Co-Founder of one of the largest Bitcoin service providers globally, Coinbase, believes that the technology is revolutionary and, in a payments context (although there are many other potential applications – think asset registries, physical locks or programmable money) has several benefits. One of the largest benefits seems to be that it obviates the need for middlemen, which lowers the cost of making payments for merchants and people sending remittances abroad.

Specifically, because all bitcoin transactions are recorded in the "block chain" - a massive, transparent ledger of each and every bitcoin transaction since its inception, if Bob sends Alice $5, there is no risk that he sends the same $5 to someone else because his ownership of that $5 and its transfer to Alice can be verified by simply looking at the block chain. Of course, credit card companies and banks perform the same function today, but only at a cost.

Roman Leal, Goldman Sachs' IT Services equity analyst, estimates that based on *current* costs and volumes, the use of Bitcoin over traditional payment providers could theoretically save over 100 billion dollars per annum. But he quickly finds that comparisons of cost between Bitcoin and current payment systems can be misleading because of different costs that are (and may increasingly be) accrued at different points in the respective systems. And he questions whether promised Bitcoin cost advantages can last, given likely rising regulatory and operating costs for Bitcoin and potentially falling costs for the conventional players as they are forced to compete or co-opt. Whether Bitcoin is really a practical solution for the unbanked population currently reliant on money transfers is also a serious doubt.

What is Bitcoin?

Bitcoin is a decentralized, peer-to-peer network that allows for the proof and transfer of ownership without the need for a trusted third party. The unit of the network is bitcoin (with a little "b"), or BTC, which many consider a currency or internet cash. The Bitcoin network was conceived in 2008 and launched in 2009 by a programmer(s) who used the pseudonym Satoshi Nakamoto and whose identity remains uncertain. The network is based on a mathematical proof; people around the world called "miners" use software programs that follow a mathematical formula to produce bitcoins. The formula and software are freely available for anyone to use. There is a finite amount of bitcoins that can be produced and as more bitcoins are created, the mathematical computations required to create more become increasingly difficult. Bitcoin can be traded or used to buy goods and services. All bitcoin transactions are recorded in the "block chain" - a massive and transparent ledger of each and every bitcoin transaction maintained by the miners. There is no central authority that oversees Bitcoin.

Source: Goldman Sachs Global Investment Research.

Others are also unconvinced. **Posner** points out that enhancing the convenience and, importantly, security of using bitcoin will most likely raise the cost of its use. Indeed, while bitcoin is virtually impossible to counterfeit, it is very vulnerable to loss or theft if not properly secured. Cyber-security specialist **Dmitry Dain** explains the security vulnerabilities of Bitcoin, and how they might be overcome. But **Currie** suggests that the security of Bitcoin as well as the maintenance of the block chain is likely to become much more daunting as use rises, with the size of the block chain and the amount of computing power dedicated to mining and maintenance already growing exponentially in a short period – the block chain increased to nearly 15 GB from 10 GB in just six months.

And security concerns, along with some association of Bitcoin – which is not anonymous but is pseudonymous – with illicit activity, have increasingly attracted the scrutiny of regulators. **Dax Hansen and Jacob Farber**, Partner and Senior Counsel, respectively, at law firm Perkins Coie, note that regulators around the world have recently become less friendly to Bitcoin. While this has generally not been the case in the US, more US regulation is likely on the way, which will likely result in more costs. Finally, **Ken Hess**, information technology specialist and author, goes one step farther, questioning not only the ultimate cost of Bitcoin use, but also the point of Bitcoin altogether. He raises many grave doubts about the promised advantages of Bitcoin.

So where does that leave us? With the conclusion that bitcoin likely can't work as a currency, but some sense that the ledger-based technology that underlies it could hold promise.

Allison Nathan, Editor

Email: *Allison.Nathan@gs.com*
Tel: *212-357-7504*
Goldman, Sachs & Co.

Interview with Eric Posner

Eric Posner is the Kirkland & Ellis Distinguished Service Professor of Law at the University of Chicago. He has taught and written extensively about financial regulation including banking law, the legal infrastructure around currencies and the practical functioning of currencies in society. Below he explains why bitcoin could never replace fiat currency, but holds more promise as a technology, albeit most likely not one that will noticeably change the world.

The views stated herein are those of the interviewee and do not necessarily reflect those of Goldman Sachs.

Allison Nathan: How do digital currencies fit into the history of currency?

Eric Posner: There is a long history of unregulated currencies. Gold has been an unregulated currency at various times and in various places. In prison camps, cigarettes have served as currency. In the United States in the 19th Century, in some states, the currency was basically unregulated; people would set up banks that issued bank notes that circulated. Sometimes you get an unregulated currency simply because there is no government. Sometimes you get an unregulated currency because there is a government but it does not control the money supply very well or the government is corrupt and people do not trust the official currency. Bitcoin just seems to be another version of this. It is a lot like gold, in fact. The difference, of course, is that it is digital rather than a heavy, unwieldy object. That means that it could serve the same purposes as gold in terms of a currency, but much more efficiently because it does not have any mass and can be sent easily from place to place.

Allison Nathan: What is your response to those who claim that gold and bitcoin differ because gold has intrinsic value while digital currencies do not?

Eric Posner: I think that is the wrong way to think about it. It is true that gold has intrinsic value but it is not very much; a very small fraction of the price of gold reflects its intrinsic value and the rest of it reflects its virtues as a store of value or as a potential currency. Bitcoin has literally zero intrinsic value unless there are people out there who like the idea of having strings of numbers on their hard drives. But I do not think that matters in terms of its function as a currency. Lots of things have intrinsic value. The reason why gold has been a currency is not that it has intrinsic value, but because it has certain properties that you need in order for the currency to function. For example, it does not decay, it can be easily divided into smaller pieces, it is heavy but not so heavy that you cannot carry it around, at least for ordinary purchases, and you can detect impurities in it. Those are the things that make gold a useful store of value and, at times, a currency, and that has nothing to do with its intrinsic value.

Allison Nathan: Would bitcoin be a good substitute for fiat currency?

Eric Posner: No. Probably the most important reason why it would not be a good substitute is that we actually do want the government to control the money supply. One of the most appealing aspects of a decentralized currency for some people – and even perhaps a motivation for its creation - seems to be freedom from government or central bank control, as reflected in the libertarian mindset. But it is wrong to think that people would be better off if we lived in a world in which the government did not control the money supply. Control over the money supply is an extremely valuable attribute of government that allows it to navigate and minimize or avoid economic problems like recessions or, maybe, asset bubbles.

Like anything, monetary policy can be misused, in the same way that the government's power to tax and control the military can be misused – both of which I would view as far more dangerous than its control over the money supply. This all depends on one's view of the government – whether you think the government is basically benign and acts in the interest of the public or whether you believe it is incompetent or inherently out to harm people. My view is that right now central banks in most countries and certainly in developed countries generally act responsibly.

I would also note that Bitcoin is not completely autonomous. It actually has its own central bank in a way. The people who maintain the Bitcoin network can change the money supply through a majoritarian process. And that means that the supply of bitcoin is a function of what the majority of these people think at any given time. They are not economists or monetary experts, but technology and programming experts, and entrepreneurs. I find that unsettling and I think most people would feel the same way.

A single currency for the whole world, which is what the Bitcoin enthusiasts anticipate, is also not optimal. Different currencies in different countries or regions provide a tool for these economies to adjust to their own economic conditions. The current struggle of peripheral countries in the Euro area is a stark reminder of that.

Allison Nathan: Practically speaking, would it be possible for digital currencies to replace fiat currency, even if you believe they would be a poor substitute?

Eric Posner: Governments would likely resist it. They have driven out other types of currencies before, including gold, and they can do it now with Bitcoin. The main tool that the government has to effectively force people to use fiat currency is its ability to require payment of taxes in fiat currency. Governments could also outlaw the use of bitcoin in transactions. While that would not eliminate bitcoin completely, it would certainly prevent it from replacing a fiat currency.

Beyond that, bitcoin could replace the fiat currency only if nearly everybody preferred bitcoins to dollars. At this point, we do not know how secure bitcoins are even if the system itself – the so-called "block chain" - is secure and transparent. That is because people have to store their bitcoins somewhere and we all know that ordinary people do not take security precautions that they should. I think that people will feel less secure holding bitcoins than they do with fiat currency. That may change one day, but I do not think this change will happen quickly.

And even if bitcoin overcame all of these challenges, it would surely be a victim of its own success, as other virtual currencies flood the market. This is already happening. If these other currencies act as competitors, then we would be stuck with just as

much volatility and exchange rate risk at home as we currently have to deal with in transacting abroad. If they act as substitutes, then there really would be no way to control the money supply. If there is no limit to the supply, it would be very difficult for the currencies to maintain their value, and very little reason for people to hold them given that they could easily become worthless. I also disagree with those who believe that bitcoin will prevail as the first mover because of network effects. Network effects will not be strong because exchanges can handle multiple currencies.

Allison Nathan: Why would "benign" governments resist digital currencies?

Eric Posner: One reason would be to block criminal activity. It turns out that Bitcoin is not purely anonymous, only pseudonymous, so it is not really very good for criminals! Other crypto currencies might be more purely anonymous. But should these currencies make it harder for the government to stop terrorist financing and drug dealing, etc. that would be a clear and legitimate motivation for the government to shut them down. More likely, the government would require those who use digital currencies to maintain records and act through intermediaries. Another reason might be to maintain capital controls, which the use of these currencies currently evades. This is particularly relevant for places like China and other developing countries. Again, while these types of controls can be misused, there are oftentimes good reasons for governments to use them; economies can be badly hurt by sudden capital flight.

Allison Nathan: Do digital currencies really provide an escape from government?

Eric Posner: There is a real irony here in that history is repeating itself. Back in the 1990s everybody was talking about the internet as this great force for freedom. People thought that they would be able to communicate with each other without government control, that they would be able to criticize the government, and that they would be able to engage in transactions that the government could not stop. But as we have learned from Edward Snowden, the government controls the internet. It is a big piece of hardware that the government can tap into and use to learn things about people. Even when you use sophisticated cryptography, the NSA always seems to be one step ahead of you. So the internet empowered the government rather than citizens. Now, 20 years later, people are saying the same thing about Bitcoin that had been said about the internet. I am therefore skeptical about the idea that Bitcoin is liberating and allows people to evade government control.

Allison Nathan: What do you think drove the meteoric rise in the bitcoin price?

Eric Posner: My initial reaction was that it was a bubble driven by people who saw Bitcoin as a way to avoid government and central bank control over currencies and those institutions' inflationary temptations. I thus assumed that the price increase was driven by a false ideology, perhaps along with greater-fool style thinking. I have since changed my view. I now think that sophisticated investors believe that either bitcoin or the technology that underlies it could be valuable for improving payment systems or for other applications. This would explain why there has been a boom in all virtual currencies, not just bitcoin.

Allison Nathan: What's your view on the value of Bitcoin as a payments system?

Eric Posner: I think there could be some advantages of using Bitcoin over existing payment systems, but these advantages are not as obvious as they might seem. For example, probably the most compelling advantage is that Bitcoin transactions seem to be cheaper. Existing payment systems are often quite expensive either because somebody effectively has a monopoly, there are a lot of government regulations that are costly to comply with, or the companies that offer these services provide certain protections that people want and are willing to pay for.

In the case of Bitcoin as it stands now, these costs are largely avoided, at least to the extent that you can technically send bitcoins from one wallet to another wallet without incurring fees; no middlemen are required to do this. The problem is that most people will end up relying on intermediaries when they use bitcoin, not in least part due to security concerns around storing bitcoin on hard drives that can crash, be hacked, or, as in one famous case, thrown away. Most people will buy bitcoins from exchanges and use bitcoin service providers like Coinbase or Bitpay to store their bitcoins and transfer money to somebody in another part of the country or the world. Then that person will maintain their bitcoins with a service provider and/or will convert the bitcoins back into the money they use. And perhaps the same or other intermediaries will provide insurance or protection from exchange rate volatility. When you throw in all of these things, the effective price of using bitcoin is going to be greater than zero. Is it going to be as much as it costs right now to use your credit card or a bank wire? Maybe not, but it is too soon to tell.

"The internet empowered the government rather than citizens…I am therefore skeptical about the idea that bitcoin is liberating and allows people to evade government control."

Allison Nathan: Are you a Bitcoin skeptic?

Eric Posner: I am skeptical about the idea that bitcoin or any digital currency could replace fiat currencies. I am adopting a 'wait-and-see' attitude about the value of the technology for payment systems or other applications outside of currencies. There is clearly an interesting technological innovation that probably has valuable application, but my guess is that this technology will ultimately be domesticated by firms and governments. Twenty years from now, use of the Bitcoin - or other similar, perhaps improved networks– could very well be part of the process where you send money from one place to another, but an unobservable part of the process. In other words, firms that transfer money may find it in their interest to use this technology to transfer money but it is not going to look that different to ordinary consumers. I think that is the most likely way that this plays out.

You can call that skeptical or not skeptical. It is not skeptical in the sense that billions of dollars may be saved in costs, but this savings will not really be noticeable to people; everything will be just a tiny bit cheaper than it used to be. Or you could call it skeptical in the sense that we are not going to be living in an anarchist utopia. That being said, we are still in the early days of understanding the potential of this new technology, so the future is indeed very hard to predict.

Is bitcoin a currency? No.

Dominic Wilson and Jose Ursua of GS markets research conclude that Bitcoin has a much better shot at influencing payments technology than taking off as a currency

The question of whether bitcoin is a "real" currency has been fiercely debated (in 2012 an entire episode of the TV show "The Good Wife" revolved around the issue; and an actual legal battle led a Texas district judge to rule on it in 2013). At some level, this question is a semantic one since a watertight definition of a currency does not exist. So it is useful to look at the main ways in which bitcoin differs from standard "fiat" currencies.

The most commonly identified properties of a successful currency are that it is:

- Widely (if not universally) accepted as a medium of exchange
- A stable store of value

To achieve this, fiat currencies are generally protected by extensive regulation. They are usually recognized as legal tender; the government is generally obliged to accept them for tax payments; and the central bank is almost always the sole issuer. Most currencies are subject to banking system regulations, are routinely used for lending and saving and are often backed by deposit insurance. In the modern era at least, governments and central banks have aimed to use their control of the currency – not always successfully – to deliver a combination of low and stable inflation, to try to limit fluctuations in the business cycle and to stand as a lender of last resort during periods of turmoil.

Wide-spread use possible

Bitcoin currently shows more promise in terms of its payments technology than as a stable store of value. Although it is not yet "widely" accepted, the ability to pay for goods and services using bitcoin is growing. And the fundamental obstacles to bitcoin being used more broadly in the payments system are arguably not insurmountable, though connections with the conventional banking system are ultimately essential to its functioning. The absence of derivative markets makes it harder to manage and hedge risk around bitcoin's value, but it is possible to imagine how those could ultimately develop.

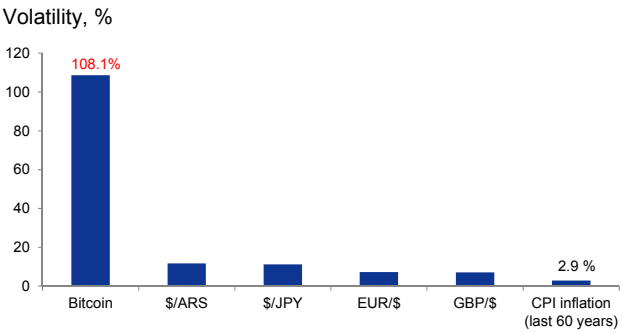
Stability more doubtful

The issue of whether bitcoin can be a stable store of value has proved a much tougher hurdle, even leaving aside the security concerns that have been in the spotlight. By limiting supply, bitcoin users may hope to protect themselves against the risks of inflation spikes that have damaged fiat currencies. But those episodes have become less common in major economies. And the more practical benefit that currency users seek is that currencies stay fairly stable in terms of the prices of goods and services they regularly buy. On that front, bitcoin currently has significant drawbacks versus conventional currencies.

The volatility of bitcoin prices so far has greatly exceeded the volatility of other currencies and gold. But for most users what matters is not the comparison with other currencies, but a comparison with the volatility of the currency that they hold (dollars in the US for instance) in terms of the things that they need to buy. The volatility of consumer prices (in dollars) has been even lower than FX rates, even if measured over a period including the 1970s. Put simply, if you hold cash today in most developed countries, you know within a few percentage points what you will be able to buy with it a day, a week or a year from now.

There is no obvious mechanism that ensures that bitcoin will achieve that stability. For fiat currencies, central banks are tasked specifically with preserving a relatively stable value (in the case of the Fed for instance, that the value of cash currency will depreciate in real terms by roughly 2% per year over the medium term). To do that, they are able to vary the supply of currency. But bitcoin has no equivalent authority prepared to act to guarantee the stability of its value. And because its supply is ultimately limited, prices will need to vary to accommodate shifts in demand, not the other way round. Unlike gold, bitcoin also has no fundamental value from alternative uses that could anchor its price.

Vicious vol



Source: Coindesk.com, Goldman Sachs Global Investment Research.

This does not mean that the value of bitcoin might not rise over time. If demand grows against a finite supply, it may. But without an issuer who could guide price changes, or an alternative valuable use, the notion that its value will be stable is harder to envisage. And the lack of these two anchors may make bitcoin's price more vulnerable to self-fulfilling price dynamics.

Unlike fiat currencies, bitcoin is also not a government monopoly. This has been part of its appeal for some investors, but it comes with costs. First, the barriers to other similar currencies entering circulation are relatively low. Only reputation and network effects are really a deterrent. Second, because it is not a government monopoly, governments themselves may choose to regulate it in ways that limit its use. So it remains vulnerable to policy decisions.

Most plausible impact on payments

We would argue that bitcoin, and other digital currencies, currently lie somewhere on the boundaries between currency, commodity and financial asset. Our best definition would be that it is currently a speculative financial asset that can be used as a medium of exchange. But the difficulties it faces as a store of value are likely to present a major roadblock to the breadth of bitcoin's adoption as a medium of exchange. If a ledger-based technology is to succeed, the cyber-currency would very likely have to have some type of fixed exchange rate in order to overcome this obstacle. On net, more than taking off as a widely-used alternative currency, it is much more plausible that bitcoin eventually has a significant impact in terms of its innovation on payments technology, by forcing existing players to adapt to it or coopt it.

Dominic Wilson, Chief Markets Economist

Email: *Dominic.wilson@gs.com* *Goldman, Sachs & Co.*
Tel: *212-902-5924*

Jose Ursua, Global Economist

Email: *Jose.ursua@gs.com* *Goldman, Sachs & Co.*
Tel: *212-357-2234*

Bullion bests bitcoin, not Bitcoin

Jeff Currie, head of GS commodities research, explains why bitcoin is a commodity, but won't best gold as a store of value

A commodity is any item that "accommodates" our physical wants and needs. And one of these physical wants is the need for a store of value. Throughout history humans have used different commodities as a store of value – even cocoa beans – but, more persistently, gold. In contrast, a security is any instrument that is "secured" against something else. As a currency is usually secured by a commodity or a government's ability to tax and defend, it is considered to be a security. By these definitions, bitcoin with a lower case "b," is a commodity, and not a currency, while Bitcoin with a capital "B" is the technology, or network, that bitcoin moves across. The analogy would be Shale technology versus shale oil.

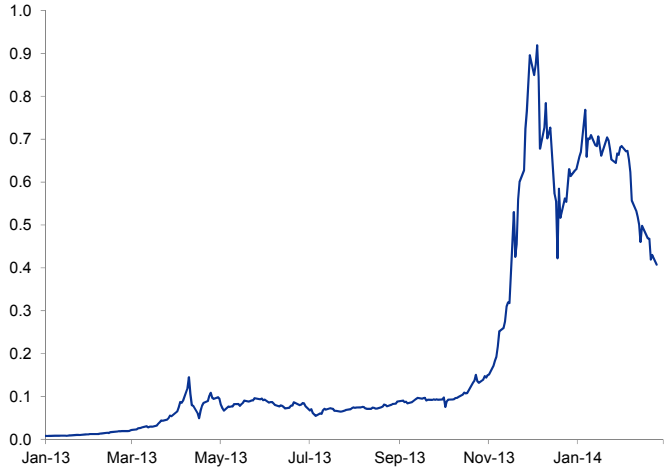
Coal solved an economic problem that bitcoin doesn't

Over the past three millenniums, society has learned which commodities are the most cost efficient at meeting its wants and needs. The replacement of an old commodity with a new commodity typically occurred precisely because the new commodity solved an economic problem that the old commodity could not. For example, coal replaced wood when fuel was needed for steam engines. So the question is: is there an economic problem with gold as a store of value that bitcoin solves?

The short answer is no. Gold is not failing as a store of value as wood failed as a source of energy in steam engines. Steam locomotives could go farther and faster on coal. But Bitcoin does not improve on gold. To understand this, we review the physical attributes of gold that make it a good store of value, ignoring scarcity, as bitcoin was designed to mimic gold's scarcity. We find that while bitcoin is unlikely to displace gold as a commodity store of value, focusing on the value of bitcoin as a commodity, which bitcoin with a lower case "b" clearly is, misses what Bitcoin with a capital "B" is – a technology, like the steam locomotive.

Bitcoin in toz

Gold toz/BTC



Source: Goldman Sachs Global Investment Research.

Stability and substitutability

It is almost universally accepted that any commodity that would make a good store of value should be stable over time (non-reactive). Though not as stable as gases, gold and other precious metals are the least reactive elements that are in solid form.

Bitcoin is "reactive" since software change has occurred in the past. There are thousands of bitcoin miners that maintain the Bitcoin network by using their computing power to verify transactions and place them in a block chain. If a majority of this computing power switched their software to adopt a change, then effectively that new software would become the standard and any verification using the old software would be rejected.

Gold also has nearly no competing substitutes that can erode its value. Silver is more reactive and plentiful than gold. Palladium is far less dense. While platinum can compete with gold on most physical attributes, it is too rare and has catalytic properties that bid it away from investment demand. Competition is likely bitcoin's weakest point, as its position was only secured by being the first mover. However, primary competitors – Litecoin and Ripple – are not yet a serious threat. Litecoin is bitcoin's silver and is less valuable and secure. Ripple is an exchange that supports multiple commodities including bitcoin, gold and silver.

Ease of storage

Gold is a good store of value not only because it is non-reactive, but also because it and platinum are the densest non-radioactive materials. Gold's density makes it extremely easy to store, allowing society to pack an enormous amount of value into a very small area. Nonetheless, the private keys that enable the spending of bitcoin today are far cheaper, easier and more efficient to store securely. Whether that will remain the case as Bitcoin use scales significantly higher is more debatable. And whether maintenance of the block chain by the mining community will remain a reasonable task is also in doubt given the rapidly increasing length of the block chain, which increased to nearly 15 GB from 10 GB in just six months, and the rising complexity of it as it splits.

Portability

While gold has low storage costs, it also has high transportation costs. This stands in sharp contrast to bitcoin for which transportation costs are far lower, which has made bitcoin useful for illegal activities in the same way as diamonds. But like gold or diamonds, should bitcoins be lost or stolen, the loss is irrevocable. And, again, the inevitable rising complexities of more meaningful adoption of Bitcoin also put this into question for the future.

Bullion bests "b"

Ultimately what really matters is the demand for these above physical attributes and the stability of that demand. Recent bitcoin price volatility owes largely to unstable demand. This volatility undermines the reasons to hold bitcoin. With millenniums of history behind it as a hedge against debasement, the key to gold's success is the stability and predictability of its demand.

On net, we find that bitcoin is easier to store and transport and is potentially more difficult to counterfeit, but it is not nearly as "stable" as gold and competitors still pose a greater risk.

Jeff Currie, Head of Global Commodities Research

Email: *Jeffrey.currie@gs.com* *Goldman, Sachs & Co.*
Tel: *212-357-6801*

Interview with Fred Ehrsam

Fred Ehrsam is the Co-founder of Coinbase, a bitcoin wallet and platform where merchants and consumers can transact with the new digital currency bitcoin. Below he shares his views on the power of the Bitcoin network and how Coinbase is helping unleash that power to the world.

The views stated herein are those of the interviewee and do not necessarily reflect those of Goldman Sachs.

Allison Nathan: What is Bitcoin?

Fred Ehrsam: Bitcoin with a capital B is a distributed network that allows for the proof and transfer of ownership without the need for a trusted third party. Bitcoin with a little B ("bitcoin", also abbreviated as "BTC") is a unit of that network which is by many considered to be a currency. Payments are the first major application of the Bitcoin network.

Allison Nathan: What is your response to those who say that Bitcoin is fake or just a bubble?

Fred Ehrsam: It is definitely not fake. The core technological problem that has been solved here has never been solved before, again, the ability to prove and transfer ownership without the need for a trusted third party. In terms of money, this was otherwise known as the "double-spending" problem. Previously, a third party such as PayPal was required in an electronic transaction because in the absence of such a trusted party that would record the transaction, there was nothing preventing someone from spending the same money more than once. Because the Bitcoin network maintains a giant, observable ledger – known as the "block chain" - of every transaction, this double-spending problem has been solved. That is very real, and there are many potential implications of that. Whether bitcoin is a bubble and whether or not it will prove to be a store of value over time is more debatable.

Allison Nathan: What is Coinbase?

Fred Ehrsam: Bitcoin fundamentally is a very powerful technology and protocol. One could view it in the same way that one viewed SMTP, which is the protocol for e-mail, or HTTP, the internet protocol. But, in order for it to be unleashed and used for the good of the masses, you have to build a user-friendly interface on top. That is what the first Web browsers did for the internet and what I see Coinbase doing for Bitcoin. Coinbase makes bitcoin easy to use for the average consumer and merchant. One of our key products is an easy-to-use bitcoin wallet – which you need to send, receive and store bitcoin - accessible on a user-friendly Web page. We keep your bitcoin safe and let you buy or sell bitcoin by hooking up any US bank account in the same way that PayPal does. We also offer merchant tools. If you would like to accept bitcoin as a business, you can put these tools up on your site, and we will take care of all the bitcoin details for you. One such tool allows merchants to instantly lock in the exchange rate of each payment they receive to their local currency such that they do not take any bitcoin volatility risk. We also allow other developers to build additional applications onto our platform, which will ultimately enhance the services we can offer.

Allison Nathan: How has your user base grown?

Fred Ehrsam: We are currently the largest wallet service in the United States, with about 970,000 consumer wallets. There is no real way of knowing the number of users globally, but I would estimate that represents about 20% of global users. On the merchant side, there are more than 24,000 merchants on the platform, including everything from "Donate" buttons for blogs to full-blown billion dollar-plus retailers like Overstock.com. It is all growing at about 30% month-over-month, so more than an order of magnitude a year.

Allison Nathan: What percentage of your individual users are speculators versus people making real payments?

Fred Ehrsam: The majority is speculators, but that is shifting. A year ago, 95% of activity was speculation versus 5% real payments. Now, I think it is closer to 80% speculation and 20% real payments, and that shift is ongoing. The other interesting trend is that six months ago, 93% of our users were male. As of a month ago, that percentage declined to about 86%; the number of females on the service doubled.

Allison Nathan: If an individual or a fund wanted to start using bitcoin tomorrow, how do they get started?

Fred Ehrsam: It depends on their objective. If they just want to get their feet wet, I think we have the easiest experience for that. They would go to Coinbase.com, sign up for an account with a given e-mail address, link their bank account and verify it, and then they can start buying bitcoin. But we are not a bona fide exchange; we are more of an easy-to-use platform and broker. If people are regularly doing seven-figure trades, there are other exchanges of varying levels of credibility around the world as well as over-the-counter markets. It becomes a bit more dispersed and a little scarier.

Allison Nathan: How does Coinbase make money?

Fred Ehrsam: We make 1% when you convert into or out of bitcoin. There are many consumer products one could imagine if this truly starts to replace financial piping, as well as lending, so a fee-based model is not necessarily the end plan, but it works well for now.

Allison Nathan: Why is Bitcoin as a payment network better than existing networks like credit cards or PayPal?

Fred Ehrsam: You have seen issues lately with Target and other retailers, where there have been massive credit card leaks. There is a fundamental difference between those networks and Bitcoin. Normally, when you pay somebody using a credit card, you are forced to give over your credit card number, your CVV, and all the other relevant payment details and those are the details which in turn can be used to make subsequent payments. You are putting all of the vulnerable information out there. The same thing does not happen in Bitcoin. When you send somebody money, it is publicly verifiable that those funds have been sent and that you are the one that sent them, and that they have arrived into the recipient's account. But, you need not give over your payment credentials, which then allow subsequent payments, in order to do all of that.

Payments on a Bitcoin network are also next to free, which is obviously not true for other networks. Even in a case where one is cashing out their bitcoin for local currency, exchanges such as Coinbase only charge 1% - substantially cheaper than the roughly 2-3% that credit card companies charge – and will likely charge less over time as competition dictates. Transactions are also almost

instantaneous whereas many forms of bank transfer can take days to settle. Other payment methods also oftentimes have base fees, which explain why when you go to your local corner store, there is a credit card minimum. This is important because it opens up new opportunities for business models that rely on micro-transactions. The open network also allows people to build on top of it, which I believe will ultimately improve the efficiency of the system, as opposed to one company owning infrastructure that they profit from but is proprietary. From a merchant perspective, there is also the benefit that there are no charge-backs. Once a payment is made, it is not reversible. Merchants today pay about 30 basis points of their total flow away due to fraud, which would be avoided.

Allison Nathan: Which are safer from theft or loss – bitcoin stored in a virtual wallet or cash stored in a bank account?

Fred Ehrsam: A Bitcoin wallet breaks down to public and private "keys". The public key is equivalent to the bank account number; it is the public address on the network that one would send bitcoins to if they wanted to send you money. The private key can be thought of as the password to spend those funds, and the public and private keys have a mathematical relationship between them. So, bitcoin storage and security all comes down to keeping that private key or password safe. In the early days of Bitcoin, there were numerous instances where this was a problem; private keys were stolen or lost due to data breaches or hard drive crashes, etc. And once that happens, your money is gone forever. But there are now technological solutions to this, and if they are utilized there is reason to believe that Bitcoin is actually safer than storage of fiat currency; it is just easier to hack into somebody's online banking account or steal their credit card number than it is to get at this private key if it is stored properly.

At Coinbase, we store upwards of 96% of our bitcoin deposits in what is called cold storage - also known as offline storage. The private keys are encrypted, and then they are split up into pieces that overlap a little bit, and then those pieces are put on USB drives and distributed geographically. The net effect resembles a nuclear launch key, where there is some amount of keys that exist in the world, and you need some subset of those to combine in order to be able to spend the funds again. We feel very confident that those keys are safe. The idea is that the other 4% of our deposits, which are still safeguarded but reside online and are easily accessible, are typically sufficient to meet the needs of our customers, while our deposits in cold storage are rarely required, and therefore stored away for safe keeping. In the few instances where we needed to access our cold storage, it took about 30 minutes to do so - not instantaneous but certainly not disruptive to customer activity.

Allison Nathan: Where do you see the future of Bitcoin?

Fred Ehrsam: The payment network is already taking off and I see that continuing. More and more sizable businesses are accepting bitcoin every day, such as Overstock.com, which is now using our merchant tools to accept bitcoin. There are other applications of the Bitcoin network. For example, one day it would not surprise me if physical locks did not exist; you should be able to walk through a door because you send a very small fraction of a bitcoin out from your address to another address, and you can prove that you own that address by signing that transaction with your private key, which authorizes you to enter the door. In my mind, bitcoin as a currency will be the last stage of this and will depend on how all of these applications blossom. I am not going to pretend that I can see the end game. I honestly do not know, for example, where the price of a bitcoin will end up.

Allison Nathan: Does the fact that there is a finite number of bitcoins – 21 million – limit its success as a currency?

Fred Ehrsam: It is true that there is a limit on the number of bitcoin but it is not as if we will ever run out. That's a myth. Bitcoin are divisible down to 8 decimal places, which means that a very, very large number of units could be created – more than enough for bitcoin as a currency to work. And even if you needed to create more, you could. That would require 51% of the computing power of the network to switch their software to adopt the change. Changes to the software have occurred a couple of times in the past. There are developer forums where such types of changes are typically discussed and a consensus is ultimately reached across the mining community that maintains the network.

Allison Nathan: What are other myths about Bitcoin?

Fred Ehrsam: The first myth is that activity on the Bitcoin network is primarily associated with illegal activity. I am not going to say that illicit activity does not exist, but as a percentage of overall activity, it is very low. It was found that volume on Silk Road – the black market exchange that was shut down by the FBI in October 2013 – represented less than 1% of all activity, and that was by far the largest operation of its kind. The other major myth is that Bitcoin is anonymous. In some ways, it is the most transparent payment network that has ever been created. You can look at the history of all payments from all addresses on the network for all of time. The only unknown piece is who owns that address. But I think of it as a big jigsaw puzzle. Once some pieces are known, it is relatively easy to figure out the rest. Law enforcement thought email was crazy in its early days because you could easily send a message from one person to another for criminal activity. Now e-mail is one of law enforcement's best friends because it leaves a trail.

Allison Nathan: How concerned are you about China's recent ban on Bitcoin-related activities for financial institutions?

Fred Ehrsam: It was really no surprise given China's stringent capital controls. But the move was interesting in the context of China's recent history. QQ Messenger, the most popular messaging application in China with currently 800 million users, at one time embedded its own virtual currency – QQ coin. In 2009, the PBOC issued guidance that said it was illegal to trade QQ coin for fear that it was getting out of control. Conversely, the PBOC issued guidance that Bitcoin is okay to trade, but traditional financial institutions and third-party payment processors should not be touching it. That is still not great, but it is a step forward.

Allison Nathan: Who loses because of the Bitcoin network?

Fred Ehrsam: Traditional money transmitters are potentially in big trouble. Bitcoin takes what was their business model, reduces the need for centralized infrastructure and distributes it in a way where remittance becomes almost an order of magnitude cheaper. Credit card networks are also vulnerable. There is still some need for a credit option to consumers, which Bitcoin does not replicate at the moment. But using credit cards as a payment network just does not make sense economically anymore. It is a legacy system that has been around for 40 years and is now technologically outdated. Lots of fees are higher than they need to be. So it is hard to see a good outcome for these companies.

Interview with Ken Hess

Ken Hess is an Information Technology specialist, author, freelance technology writer and consultant. He is a regular contributor to ZDnet.com and a serious Bitcoin skeptic. Below he explains why he just does not buy into Bitcoin.

The views stated herein are those of the interviewee and do not necessarily reflect those of Goldman Sachs.

Allison Nathan: You have called Bitcoin "the silliest of ideas." Why?

Ken Hess: Purchasing another currency to buy things that you could buy with regular currency just seems pointless and silly to me. If you're going to buy a cup of coffee or a camera or any item why do you need a separate currency for that?

Allison Nathan: Do you see any advantage to using Bitcoin as a payments platform?

Ken Hess: I think that Bitcoin could be a decent payments platform. Why not? But I don't see any real advantages to what we currently have. There are a zillion different ways to pay for something today; I can pay with cash, money order, cashier's check, wire transfer, credit card, debit card, PayPal, and the list goes on. Why is this method so much better? Electronically, I have used PayPal many times. I've used direct wire transfer. I've used debit cards online. I pay my credit card bills online and I've used bitcoin. I just don't see any real difference between them. If Bitcoin offered something really outside of what we already have, I might buy into it a little more, but I just don't find that it does.

For example, Bitcoin enthusiasts seem to suggest that its anonymity is an advantage. But, first, it is really not anonymous. Second, even if it were, so is cash. And third, if I am making a legitimate purchase, why does it need to be anonymous anyway? Something just feels underhanded about that. Basically, I feel like I am doing something wrong if I feel like I have to pay with bitcoin. And, by the way, I basically am because at this point bitcoin transactions generally fall under the IRS's radar. I am not a person that delights in paying taxes, but you really can't run an economy without them; somebody's got to pay for something. Beyond this somewhat criminal side of things, I just don't see anything special about Bitcoin as a payments platform.

> "I think that Bitcoin could be a decent payments platform. Why not? But I don't see any real advantages to what we currently have. "

Allison Nathan: What about the notion that Bitcoin allows for cheaper payments?

Ken Hess: I just don't believe that is ultimately the case. As a consumer using bitcoin to make purchases online, I was surprised to find transaction fees popping up when I went to pay with bitcoin. So there can be charges associated with using it. The cost might be less than other payment methods and, then again, it might not be. I find it subjective depending on the merchant.

And on the merchant side there is also a cost to accepting bitcoin. It might be less than credit card companies charge for now. But at some point, these costs are likely to rise because doing business in bitcoin is not seamless and it is not without risk. The volatility risk in particular is daunting. If a merchant accepts $500 worth of bitcoin for a laptop at noon on any given day, who knows what that bitcoin will be worth by 5pm?

The volatility is sufficiently daunting to the degree that bitcoin service providers are enticing retailers to sign up with them by agreeing to convert any payments received in bitcoin immediately back to fiat currency so that the merchants face virtually no bitcoin exchange risk. That may be a way to extend the merchants' customer base to Bitcoin enthusiasts (although, is it really? because, let's face it, bitcoin users are still very small in number and I doubt you can find a bitcoin user that can't also pay with fiat currency), but it is certainly not the endorsement of Bitcoin that Bitcoin enthusiasts claim it to be. There is just something fundamentally bizarre about that process. I guess it is cute to be able to accept bitcoin but that is just an odd and inefficient way of doing things. I mean, why don't they just accept dollars and call it a day?

> "[Bitcoin] is a pie-in-the-sky ideology - more something people want to believe in than something that is actually real. So I don't think people should get heavily involved in Bitcoin. "

Allison Nathan: How do you explain the enthusiasm around Bitcoin?

Ken Hess: The enthusiasm around Bitcoin basically comes from the excitement of putting one over on the government by escaping its clutches in your business and avoiding some of its taxes. There is the whole libertarian anarchy feeling about it. It is a pie-in-the-sky ideology - more something people want to believe in than something that is actually real. So I don't think people should get heavily involved in Bitcoin.

Allison Nathan: Do you see any advantage to being a distributive system?

Ken Hess: Being distributed means that no one entity or person controls the system. I don't really see any practical or logical advantage to that. If you think about it, banks are also somewhat distributed. If you blow up my branch bank, you don't blow up all the money in the bank because the money has been distributed and transferred around. I just don't get what the big deal is about the distributive nature of this.

Allison Nathan: Are there any advantages at all to Bitcoin?

Ken Hess: I think Bitcoin is an interesting experiment on crypto-currencies that we can learn a lot from, but beyond that I am not

sure it has any real advantages. This experiment is useful for the future because I do think at some point a well thought-out crypto currency could work. But you can't just mine some bitcoins and say, hey, we're going to assign some arbitrary value to this protocol or this fake currency and think that it will succeed over the longer term.

Allison Nathan: Are there any disadvantages of Bitcoin?

Ken Hess: Several. First, transactions are not reversible. While this could be good for merchants who can rid themselves of charge-back fraud, the consumer just has to trust that they are going to receive what they paid for. But there is no guarantee and no way to get your money back if that ends up not being the case.

Second, if you lose your wallet by accident, your bitcoins are gone forever. You can read story after story on the Internet about people losing their wallets and all of their bitcoin. It is not like losing your physical wallet. If I lose my physical wallet that contains $20, my driver's license and credit cards, it is inconvenient. I will have to replace everything. But I only lose $20, not my whole bank account! Holding bitcoin should not be akin to gambling; if you own bitcoin you should be able to recover those kinds of losses.

Third, it is just too volatile to be useful as a medium of exchange. Fourth, it is nowhere near being adopted widely enough for it to be useful; if my corporation paid me in bitcoin I would be at an extreme disadvantage because very few places accept it so I would have to exchange it for actual money at a cost so that I could spend it.

> "If I lose my physical wallet that contains $20, my driver's license and credit cards, it is inconvenient. I will have to replace everything. But I only lose $20, not my whole bank account! Holding bitcoin should not be akin to gambling. "

Fifth, I suppose there might ultimately be ways around this, but once bitcoins are lost to obscurity because somebody accidentally crashes a hard drive, etc., they will never come back. And you cannot mine more beyond the arbitrary 21 million maximum unless there is a broad consensus of the mining community to do so. So while everybody seems to be operating under the assumption that 21 million bitcoins will exist in the world, the number will actually be significantly lower. That makes bitcoin more and more inaccessible.

There is also no credit in the Bitcoin world. You have to have bitcoin to spend it, which ultimately might be a good thing, but that is not how the world works today. It seems like our economy is based on credit. And you are actually considered a deadbeat if you don't use credit. I might be missing some, but those are some of the glaring disadvantages.

Allison Nathan: Allison Nathan: Do you see any value in the innovation of the ledger-based protocol?

Ken Hess: Yes, the public ledger-based protocol is interesting. And I think that if bitcoins were recoverable, if they were guaranteed somehow, if the whole thing was less volatile then this protocol might be a good method of tracking different types of transactions. But given all of these flaws the ledger alone does not validate Bitcoin in its current form in any sort of way or help the whole Bitcoin argument in my mind.

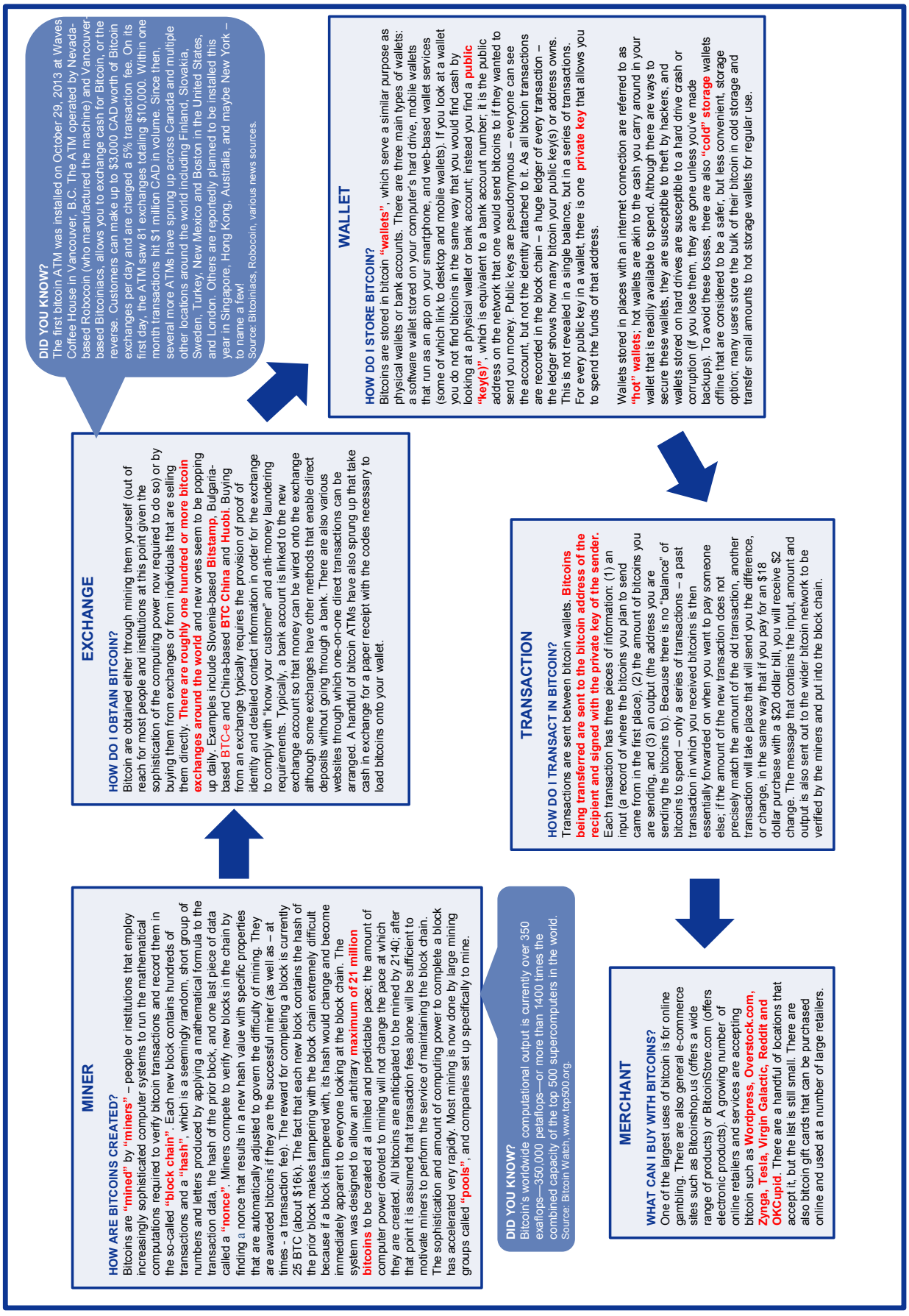
> "The ledger alone does not validate Bitcoin in its current form in any sort of way or help the whole Bitcoin argument in my mind. "

Allison Nathan: Do you see a future for Bitcoin?

Ken Hess: I am not totally anti-Bitcoin or crypto-currencies. I just think that Bitcoin is a bad implementation of a crypto-currency. So I think that there is a future for crypto-currencies. I just don't think it will be in Bitcoin. The possibility for a government-backed crypto-currency is high. I think it will happen because there are some advantages to the public ledger. But in order for it to work you are going to need better security. You're going to need reversible transactions. You're going to need more stability. You're going to need a way to put lost and stolen money back into circulation and a way to track the money.

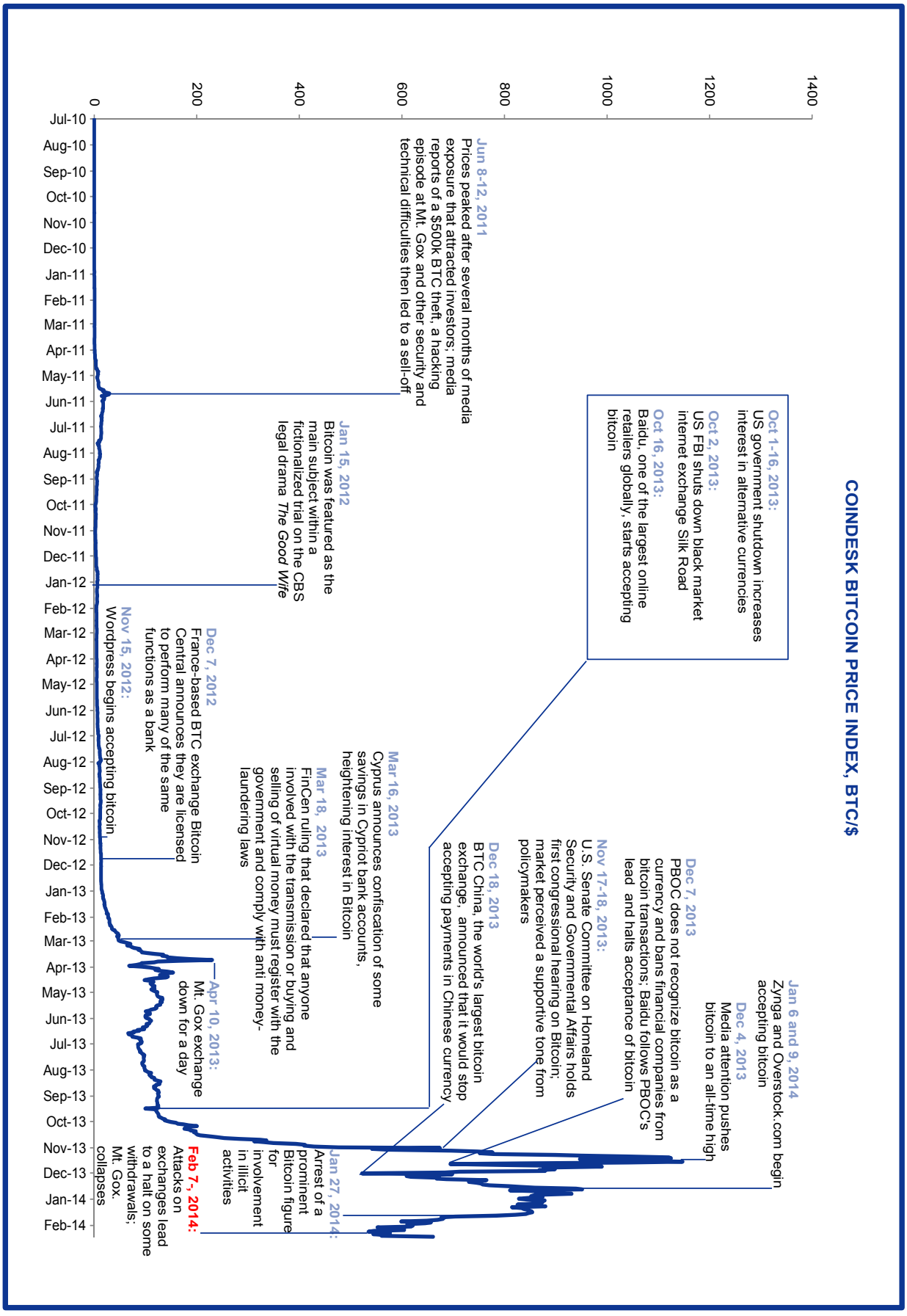
I realize that most of these changes go against the ideology of Bitcoin and will likely further raise the cost of using crypto-currency. But I think that is what will be required to create something useful beyond ideology. And my concern is that while Bitcoin has been an interesting and, yes, even somewhat successful experiment thus far, its ultimate, inevitable failure might set back crypto-currencies several years.

Bitcoin basics



Source: Coindesk.com, Jerry Brito and Andrea Castillo of the Mercatus Center, various news sources, Goldman Sachs Global Investment Research.

Bitcoin bumps



Source: Coindesk.com, Goldman Sachs Global Investment Research.

Interview with Dmitry Dain

Dmitry Dain is the CTO and Founder at Betalabs LLC, a startup focusing on payment solutions based on crypto-currencies. Prior to founding Betalabs, Dmitry was the CTO at Cipher Systems LLC where he ran a software development team focusing on cyber security products and big data analytics. Below he outlines the ease of Bitcoin theft, but also of safeguarding against it.

The views stated herein are those of the interviewee and do not necessarily reflect those of Goldman Sachs.

Allison Nathan: How easy is it to steal Bitcoin?

Dmitry Dain: It can be very easy if no or few precautions are taken, but extremely difficult if relatively straightforward precautions are put into place. Bitcoins are secured using Public Key Infrastructure (PKI), which simply means that some encryption code – a "private key" or password - is established for every public Bitcoin address, and that private key must be used to decrypt your Bitcoins and spend them. Practically speaking, the private key is really nothing more than a text file with gibberish inside. Theft occurs when somebody else gets a hold of that text file, which enables them to spend your bitcoin. And, for that matter, loss occurs if you lose that text file and have made no backups. Theft is by far the biggest security vulnerability. And loss is also a concern; there have been many instances of individuals accidentally losing the private keys that allow them to spend their bitcoins.

Allison Nathan: What methods are used to steal bitcoins?

The most common way that bitcoins are stolen is through the use of "malware", malicious software that gets into your computer through perhaps a seemingly innocuous email attachment. Malware looks for a Bitcoin application installation, and tries to locate the text file that contains your private key. Once the malware finds it, hackers simply download it onto their computer and, voila! They can transact your bitcoins out of your public address and into their own. Basically, as long as somebody is able to read a file on your computer remotely, they can potentially steal your bitcoins. This type of malware has exploded over the last year and can effectively steal very large values of bitcoin in a very short amount of time. Specifically, a single private key can control a very large number of bitcoins. From the perspective of the network, whether a key controls 10 bitcoins or 100,000 bitcoins really doesn't matter. Every transaction – regardless of size – is fully settled in about ten minutes or less. The ability to transfer very large amounts of money in that short amount of time is very powerful and potentially a very positive advantage of Bitcoin, but can also be very damaging in terms of theft.

Allison Nathan: Wouldn't such thefts be traceable?

Dmitry Dain: Yes, you would be able to see the public address that your bitcoins were sent to, but you would not know the identity associated with that address. If somebody is sophisticated enough to be able to steal your private key, generally they are sophisticated enough to cover their tracks in a way that makes it very difficult, if not impossible, for you to discover their identity.

Allison Nathan: Is it easier to steal a private key or hack into an online bank account/steal credit card information?

Dmitry Dain: It is hard to compare them as it depends on the security precautions taken by the various individuals. But one of the biggest differences for any user is that when somebody hacks into your online bank account or steals your credit card information, potential losses on your part are generally considered reversible. With Bitcoins, they are not reversible. Once the block chain is written it cannot be unwritten. That is what makes the private key more valuable, and thereby a focus of attack.

Allison Nathan: How do you protect against theft?

Dmitry Dain: Following relatively simple steps can prevent the theft of your bitcoins. Encrypting your text file that contains your private key with a strong password is generally sufficient. For even more security, you can store your keys offline entirely in what is called "cold storage". These computers are not actually online and in many cases are not even powered on. Your computer does not need to be on in order to receive bitcoins, which makes cold storage a very powerful security tool. You can also simply print a hard copy of the text file and store it in a safe deposit box, or between several safety deposit boxes; a key will only take up about one third of a printed page so this is very easy to do. People have also etched their private keys onto metal to accomplish the same thing, but also protect against fading, etc. Making backups in all of these ways also provides protection against outright loss in addition to theft.

Allison Nathan: So it is possible to safely store a private key?

Dmitry Dain: In my view, yes. It is much easier to store a bitcoin than other monetary instruments; these methods are very simple and very powerful. And once your key is stored properly, you and only you are in full control of your bitcoins.

Allison Nathan: How expensive is properly storing bitcoin?

Dmitry Dain: There is a cost. But is it a stratospheric cost? In banking terms, no. It is a tiny cost. It is definitely less expensive than securing most other monetary instruments. Securing physical gold, for example, is significantly harder and more expensive than securing pages of text. If you were to generate 10 private keys for every citizen of the United States, which would produce a little over 3 billion pages, it would be roughly equivalent to what is being printed every day in the United States. And storing bitcoins in a digital wallet, either third-party or on your own, is quite reasonable in terms of cost.

Allison Nathan: Is it possible to counterfeit bitcoin?

Dmitry Dain: Your Bitcoin wallet does not contain "bitcoin" but rather public and private keys; the private key is necessary to access the funds that are assigned to your public key or address on the block chain. So when you transfer bitcoins you do not send any physical bitcoins but rather submit a transaction to the network. There is no risk of Bitcoin counterfeiting for the reason that there are technically no physical or even digital "bitcoins" to counterfeit. The network makes sure that your public address is valid and has the proper value, and that value is then sent to the public address of the receiver. It is theoretically possible to double-spend bitcoin, which would be the closest thing to counterfeiting. The network prevents double-spending by verifying each transaction, but if someone had sufficient computing power, for example, controlled

more than 51% of the computing power of the network, they could cheat and include invalid transactions before validating a block of transactions. The amount of computing power required to pull this off gets more and more daunting as the system grows and is very unlikely to happen even today.

Allison Nathan: It seems that "malleability issues" may have played a role in Mt. Gox's downfall. What are they and do they pose a larger threat to Bitcoin?

Dmitry Dain: Malleability refers to the following fraud perpetrated by an exchange client: an exchange sends money to a client, but the client says that they never received it; when the exchange tries to find the transaction using the Bitcoin hash, which is the record in the block chain that allows you to identify the transaction, the exchange cannot find it because it has been changed by the client. Since the exchange cannot find it, they assume there was an error with their system and send the money again. So clients are able to double and triple dip withdrawing their money.

But the vulnerability of the Bitcoin protocol that allowed for this type of fraud has been very well known by the Bitcoin Foundation for a long time, and fixes to the protocol have been made that essentially prevent it from occurring for any exchange or customer that runs their system properly. Apparently, Mt. Gox had operated their own version of the protocol that may not have adequately addressed the malleability issue. Whether that issue was at least one of the reasons for the collapse of Mt. Gox is not known at this time. There were clearly also customer service issues and broader governance issues. But, generally, malleability is no longer considered an exploitable problem. A lot of people were quite surprised that Mt. Gox claimed to have an issue with this; no other exchanges have confirmed similar problems.

> "There is no question that the most vulnerable point of the entire Bitcoin Network is the exchanges."

Allison Nathan: What are DDoS attacks?

Dmitry Dain: Distributed Denial of Service Attacks occur when someone sends more information or more requests to your network than your network can process. The goal of the attack is to disrupt the system; there is no obvious monetary or other gain for the perpetrator. These attacks have been and will continue to be one of the largest cyber-security problems for firms operating on the Internet, and particularly for firms like banks where a concerted attack that freezes the system can be a major inconvenience and seriously impede business, at least for some period of time. Bitcoin is less vulnerable but more attractive to these types of attacks. It is less vulnerable because it is decentralized so it is more difficult to cripple Bitcoin by targeting just one point of attack. Of course, the most centralized points within the Bitcoin network are the larger exchanges, and we see exchanges getting absolutely hammered with denial of service attacks. But in the latest sophisticated DDoS attack against the exchanges, the only impact was a moderate slowdown in transaction speeds. The attraction of Bitcoin as a target of these attacks is that no one is going to investigate you; you are attacking lots of individuals, not a banking institution that may actually take action against you.

Allison Nathan: How pervasive are attacks on Bitcoin?

Dmitry Dain: Attacks are very pervasive and very persistent. Bitcoin has been under attack for a very long time now, which in a way gives us confidence that the system is overall robust.

Allison Nathan: What is the most vulnerable point on the Bitcoin system in terms of security?

Dmitry Dain: There is no question that the most vulnerable point of the entire Bitcoin Network is the exchanges. They are in fact the biggest targets of theft and attack and in years past have also borne the brunt of protocol vulnerabilities. But, in my view, the key challenges have not revolved around these factors but around governance issues associated with properly running an exchange. For this reason, I believe that exchanges should be the focus of most regulations.

Allison Nathan: Is it possible to have secure exchanges?

Dmitry Dain: It should be possible with competent management. But Mt. Gox was not really an outlier; there have been quite a few exchanges that have either seen their people arrested, could not make it in the market place or just simply disappeared. We do see very serious actors coming into the marketplace, and as legitimacy of Bitcoin grows, the assumption is that more investment will flow into the operation of the exchanges and that they will become more stable. But it is still a Wild West out there for the exchanges.

Allison Nathan: What other technical attacks might occur that destroy Bitcoin and how likely are they?

Dmitry Dain: One concern is what is referred to as a "51% attack" in which a malicious actor gains control of the majority of computing power and is therefore able to choose the transactions it validates and essentially implement any changes to the protocol it desires, including effectively wiping out the history of the block chain. From a technical perspective, such an attack is possible today. A mining group based primarily in Eastern Europe has had sufficient mining power for a long time to actually mount a 51% attack. But they have chosen not to for the main reason that it would not be in their financial interest to collapse the value of Bitcoins. And the more computing power devoted to mining Bitcoin, the lower the vulnerability to this type of attack. We have seen an explosion over the last 18 months in very sophisticated mining operations around the world, which has ostensibly made such an attack less likely. The feeling is that a state actor worried about losing control over its economy might be the perpetrator of such an attack, but at this time we do not have any evidence that there has been any involvement from state actors around the world. So my answer to whether this type of attack poses a long-term problem that could jeopardize the entire block chain is "No."

The other type of attack often mentioned is the "Goldfinger Attack" named after the 1964 James Bond movie in which the villain plots to render all of the gold in Fort Knox useless through radioactive contamination to make his own gold holdings more valuable and disrupt the global economy. Such an attack on Bitcoin would constitute buying up all of the bitcoins in the world and then forcefully losing them or freezing their private keys so that the bitcoins are effectively out of the system. It is fairly simple to see that the idea of such an attack is quite preposterous. It would only make the bitcoins of everybody who had not sold their bitcoins to this actor more valuable. There are also other crypto currencies based on Bitcoin that can be used to sidestep this attack. So it is basically not possible, although intriguing to imagine!

Interview with Perkins Coie

Dax Hansen is a Partner, and Jacob Farber is a Senior Counsel at Perkins Coie, LLP which has one of the leading decentralized virtual currencies law practices in the United States. Below they provide an update of the regulatory status, risks and future regulatory developments of bitcoin.

The views stated herein do not constitute legal advice.
The views stated herein are those of the interviewees and do not necessarily reflect those of Goldman Sachs.

Dax Hansen

Jacob Farber

Allison Nathan: Are virtual currencies legal?

Dax Hansen: The US Constitution and the Stamp Payments Act of 1862 give the Federal government the exclusive authority to create official coinage and currency of the United States. Printing a currency that is meant to compete with or confuse people about which is the legal tender is a crime. But the use of bartering, prepaid cards and other stores of value and virtual currencies is permitted as long as you comply with applicable laws.

Allison Nathan: Bitcoin is unregulated: true or false?

Dax Hansen: It is true and false. It is somewhat true in the sense that there are a limited number of regulations or laws in the United States that are specifically focused on virtual currencies. But it is false in the sense that current laws and regulations in many instances already regulate virtual currencies. There are a number of laws that one must look at if you are in the virtual currency business, including anti-money laundering laws, banking laws, money transmission laws and potentially commodity and securities laws. Because so many different regimes are potentially applicable, in some ways, bitcoin is one of the most heavily-regulated financial products. But not all aspects of bitcoin fit neatly into existing laws. And so the question is whether the laws need to be adjusted to fit this new paradigm of a decentralized virtual currency.

Allison Nathan: What is the regulatory status of bitcoin today? Is it a currency, commodity or something else?

Jacob Farber: The financial crimes enforcement network, FinCEN, which is the US Treasury department agency responsible for implementing the Bank Secrecy Act that includes US anti-money-laundering laws, has been the only US federal agency to date to make a definitive statement about the regulatory status of bitcoin, which they did on March 18, 2013. FinCEN found that bitcoin and similar virtual currencies have a lot of attributes of real currency, or legal tender, which means currency issued by a national government, although bitcoin itself is not issued by a government. The agency concluded that since it seems to operate in a similar way to a currency, it should be treated like currency or "monetary value" for the purposes of US anti-money-laundering laws, which means that certain types of bitcoin businesses involved with the transmission or buying and selling of bitcoin are subject to federal regulation as money transmitters. They must register with FinCEN and must comply with federal anti-money-laundering laws such as "know your customer" rules and reporting of suspicious transactions. Most states also regulate money transmission. The state regimes vary widely in how money transmission is defined. It appears that in some states bitcoin would fall within the statute, while in others it likely would not. But there has been relatively little guidance. At least in some states anyone transmitting bitcoin must be licensed with the state as a money transmitter.

Allison Nathan: What could new regulation around virtual currencies look like?

Jacob Farber: What is likely to be regulated is a particular use of bitcoin. If you use bitcoin like money, which has been its primary use so far, FinCEN has said that it will be treated in the same way as money for the purposes of anti-money-laundering laws. But in the future, virtual currencies may be used in different ways. For example, right now bitcoin may fit the definition of a commodity, but the Commodities Futures Trading Commission regulates only certain types of commodity trading. Commodities have to be traded on a futures or options basis as opposed to on a spot basis – which is how virtually all bitcoin exchanges settle transactions today - in order to be subject to the CFTC's jurisdiction. So if futures contracts on bitcoin begin to be traded, the CFTC is likely to regulate it. If you package bitcoin into securities as would be the case with a bitcoin-backed ETF, then the SEC is likely to regulate it. In fact, the SEC is currently reviewing an application for a bitcoin ETF. And if we ever reach the point of mass adoption, the consumer protection regulators are also likely to weigh in.

Allison Nathan: Are there likely to be new state regulations?

Jacob Farber: Yes. Benjamin Lawsky, the Superintendent of the New York Department of Financial Services, had hearings at the end of January on virtual currencies. New York has an existing statute governing money transmission, but it is unclear whether bitcoin falls under that statute. The thrust of the hearing was to explore whether in light of that, New York should adopt new rules or laws that would create an analog to a money transmitter's license for bitcoin and maybe other virtual currency companies called a "Bitlicense". After the hearing, Lawsky said that the goal is to have a new regime in place by the end of 2014.

Dax Hansen: Although New York has been perhaps the most public about its undertakings, I think that all state regulators are determining what they should do. What they decide will be a mixed bag because the states do not all have the same laws on the books today and they may have different levels of concern. Recently a conference of state bank supervisors formed a task force to look at bitcoin and other digital currencies. So it seems that all states are evaluating it now and we will see something either at a uniform level, a model law or recommendation, or state-specific solutions.

Allison Nathan: How is the IRS treating virtual currencies?

Jacob Farber: There has been no direct guidance from the IRS. For now, people are making their own judgments about how to handle it, and maybe coming to different conclusions. In some instances bitcoin may be considered an asset and therefore may be subject to capital gains. In other instances it may look like foreign currency, in which case the IRS could treat it as ordinary

income. And so there has been a big question mark, not just about how you characterize virtual currencies for tax purposes but also about when you have a taxable event in different kinds of transactions. But we may be getting answers soon. In May 2013, the General Accounting Office asked the IRS to provide some guidance on the tax treatment of virtual currencies. It was reported about six weeks ago that an IRS ruling should be out soon.

Allison Nathan: Has Congress weighed in on the topic?

Jacob Farber: There were Senate hearings in November 2013, which remain the high-water mark of congressional activity in the area. Two important themes came out of those hearings that have set the tone for how the Federal government is thinking about virtual currencies at a very broad level. The first theme was that there are risks around virtual currencies; they are something new and can be used for illicit purposes. So there is a perceived need to make sure that we develop the tools and techniques to be vigilant and to be able to track those illicit uses of bitcoin. The other major theme, which I think was one of the positive pivot points for virtual currency over the last year, was that there is tremendous potential both as a financial transaction system and beyond; there is an incredible amount of innovation and development happening and there are a lot of positives that are going to flow out of it.

Allison Nathan: What are the biggest regulatory risks that bitcoin-related companies face?

Dax Hansen: It depends on the company and where it fits into the Bitcoin ecosystem. But a key risk or concern that many of these bitcoin companies have revolves around whether or not they are involved in some form of money transmission. If they are, they may need a license at the state level, which is a costly and a time-consuming exercise. We are talking months, if not years, to get licenses on a state-to-state basis. And this technology is moving in dog years, which makes these types of delays very painful. But if they do not comply, the stakes are high. Engaging in non-bank financial services like money transmission without a license is punishable by fines and even prison time. They are also concerned about anti-money-laundering. They spend a lot of time developing their anti-money-laundering policies and trying to figure out what data they need to be collecting, what know-your-customer procedures they need to be implementing, and what reports they need to be filing. They need to make sure that these controls are actually applied and built into the technology platforms. It is not a regulatory issue per se, but many bitcoin companies are also spending time thinking about their banking relationships. Largely because of the sensational press around this issue and perhaps conflicting signals from Federal regulators, banks seem to be concerned about dealing with companies in the bitcoin space. And so the banks are being cautious and banking relationships for bitcoin-related businesses are hard to come by. This is a key concern because the difficulty in getting banking relationships is a gating issue for the development of a robust Bitcoin ecosystem here in the US.

Allison Nathan: How likely is it that regulation shuts down virtual currency businesses?

Dax Hansen: It is highly unlikely that we will see in the US an outright ban on virtual currencies or new laws or regulations that shutter entire categories of virtual currency businesses. Some US law enforcement officials, regulators and law makers have publicly acknowledged that virtual currencies offer potentially significant innovation and have legitimate uses. There seems to be a growing consensus that virtual currencies are here to stay because the related technology is so powerful.

Allison Nathan: Are investors protected if a service provider or exchange is shut down by regulators or just fails?

Jacob Farber: We have to distinguish between two scenarios. Bitcoin "wallets" have two parts: a public address and a private key. You can hold bitcoin in a wallet that you have complete control over. It is all about safeguarding your private keys. If you have your private keys, and you do not let them out of your control, then your only risk is being hacked if you are storing them online or losing them outright if, for example, you stored them on your hard drive with no back-ups and it crashed. There is generally no legal recourse or protection in these cases – your bitcoins are gone. But an investor can address these risks by using best practices for the storage of bitcoins that are pretty well-established at this point. The second scenario is if you have an account with an exchange or service provider where they store and control your private keys.

Dax Hansen: In this second scenario, user protection varies. One of the reasons that money transmission is regulated at the state level is to protect consumers. Licensed money transmitters are required to have certain net worth, permissible investments, and surety bonds that protect against consumer losses. So one feature to look for is whether the company is a licensed money transmitter. But investor due diligence should certainly not end there. Some businesses may be structured so that money transmission licenses are not required. Those companies might offer other protections. Maybe they are more reputable, more sophisticated or offer some sort of insurance. Maybe they are a bank or broker-dealer that would have other protections available. There are a host of different regimes that afford certain protections to investors, and so it is worth looking under the hood at your options to see what sort of qualifications, credentials and safeguards they provide. It is important to do your homework because if businesses are not licensed money transmitters that might be set up in international jurisdictions and/or have fewer protections and the entity failed or was engaged in some sort of misconduct, the user could be out of luck.

Allison Nathan: How is the US stacking up against other parts of the world in terms of its bitcoin regulation?

Jacob Farber: I think that the US has one of the clearer pictures so far. We know it is not illegal because FinCEN is giving us rules for it, and the states are looking at adopting rules. And the FinCEN guidance framework gives bitcoin businesses some degree of certainty. Globally, it is a real hodgepodge. Some countries have said that it is not legal. Some have said that it is not illegal, but that they are worried about it. The crackdown in China is one example of a country that has taken a pretty negative approach, although there is speculation that China's controls will loosen back up.

Dax Hansen: Over the last few weeks, the international responses have become more unfriendly to virtual currencies. But most international jurisdictions have generally taken a very hands-off approach to bitcoin. For instance, in the EU, bitcoin transactions are generally not regulated. You do not have to have the equivalent of a money transfer license and you do not even have to have an anti-money-laundering policy. So my view is that US regulations are more intense and complicated to navigate than those that exist internationally, especially given the state patchwork governing virtual currencies in the US. It is just too hard to set up a technology company focused on bitcoin here in the United States, and it is easier to do it someplace overseas.

Is Bitcoin the future of payments?

GS IT Services analyst Roman Leal envisages "co-opetition" between bitcoin service providers and traditional payment providers

The Bitcoin network uses the internet to bypass some of the money transfer hurdles from traditional banking systems and national boundaries. As a result, the network could theoretically solve some of the pain points involved in the current payments and money transfer ecosystems, potentially driving some savings for merchants and consumers. For example, Bitcoin – or other digital currencies might enable:

- Individuals to transfer money as seamlessly as sending an email, while reducing money transfer and currency conversion fees.
- Businesses to accept non-cash payments for the same percentage fee regardless of purchase amount ($5mn or $0.05).
- Travelers to buy goods abroad without paying cross-border fees typically charged by banks and/or networks.

However, it is important to note that the future could look different as likely rising regulatory and operating costs for Bitcoin and potentially falling costs for the conventional players as they are forced to compete or coopt narrows the cost gap between the two. Just as a flurry of new entrants – such as Square, Groupon, and PayPal - encouraged payment networks and payment processors to develop a mobile payments strategy, we expect traditional payment players to develop digital currency strategies.

Bitcoin – hypothetical savings – but can they last?

Potential annual net savings with Bitcoin based on 2013 volumes

2013 Market Size ($bn)	Retail	E-commerce	Remittances
Dollar volume by market	10,383	609	549
Prevailing average pricing	2.5%	2.9%	8.9%
Bitcoin pricing	1.0%	1.0%	1.0%
Prevailing transaction fees	259.6	17.8	48.9
Bitcoin transaction fees	103.8	6.1	5.5
Potential savings with Bitcoin ($ bn)	155.7	11.8	43.4

Source: Goldman Sachs Global Investment Research.

Potential savings for merchants?

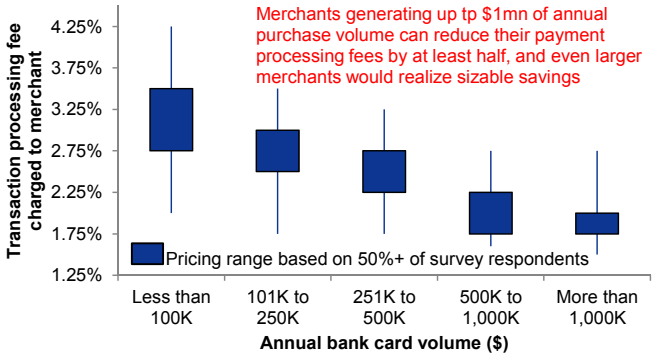
Currently, retailers pay a percentage of purchase volume called the merchant discount rate (MDR) in order to accept electronic forms of payments. In the United States, the average MDR is about 2.5% for offline retail payments and 3.0% for online retail payments (though these fees vary widely by merchant size and type). Today, the use of virtual currencies could theoretically eliminate these fees as they do not rely on traditional banking/payment networks. That said, Bitcoin gateway service providers such as BitPay and Coinbase, which enable merchants to accept Bitcoin payments, typically charge a fee of about 1%. At face value, the annual net savings if all electronic payments were conducted in Bitcoin could potentially add up to over $150 bn in retail point of sale and $12 bn in e-commerce fees per annum based on global 2013 purchase volume. Using this math, merchants generating $1 million in annual purchase volume would save at least half in payment processing fees by accepting bitcoin, with small merchants even better off.

But comparisons of cost between Bitcoin and current payment systems can be misleading because of different costs that are (and may increasingly be) accrued at different points in the respective systems. And Bitcoin savings may very well end up less than this math suggests as likely rising regulatory and other operating costs are potentially passed on to merchants. It should also be noted that many merchants that accept Bitcoin today typically choose to avoid any bitcoin exchange rate risk by automatically converting any bitcoin received into fiat currency, with each transaction incurring the 1% conversion cost.

Beyond the potential for rising costs, Bitcoin, like all nascent payment networks, faces a "chicken-and-the egg" problem: merchants are not incented to accept bitcoins unless they see a critical mass of consumers wanting to pay with the digital currency, and consumers are not incented to pay with bitcoins if they can't use the currency at enough merchants.

Big savings for small merchants…for now

Proprietary survey



Source: Goldman Sachs Global Investment Research.

Potential savings for consumers?

Currently, consumers pay a money transfer fee as a percentage of the total amount transferred; roughly 10% on average. Money transfer networks, such as Western Union, charge these fees for accessing their network, as well as to cover agent commissions and FX conversion fees. Today, Bitcoin could theoretically reduce these fees to 1% by bypassing traditional money transfer systems and instead enabling transfers directly between two Bitcoin wallets. As a result, annual net savings for consumers could theoretically amount to over $43 bn based on the World Bank's estimate of global money transfers. But again, this is likely to end up lower as costs of dealing in Bitcoin rise. And the Achilles heel of realizing any savings in this context is that at least one if not both parties typically involved in money transfers are unbanked, which would make converting bitcoin into local currency very difficult. The reality is that if individuals do not have access to a bank, the challenges of accessing Bitcoin would likely be just as daunting.

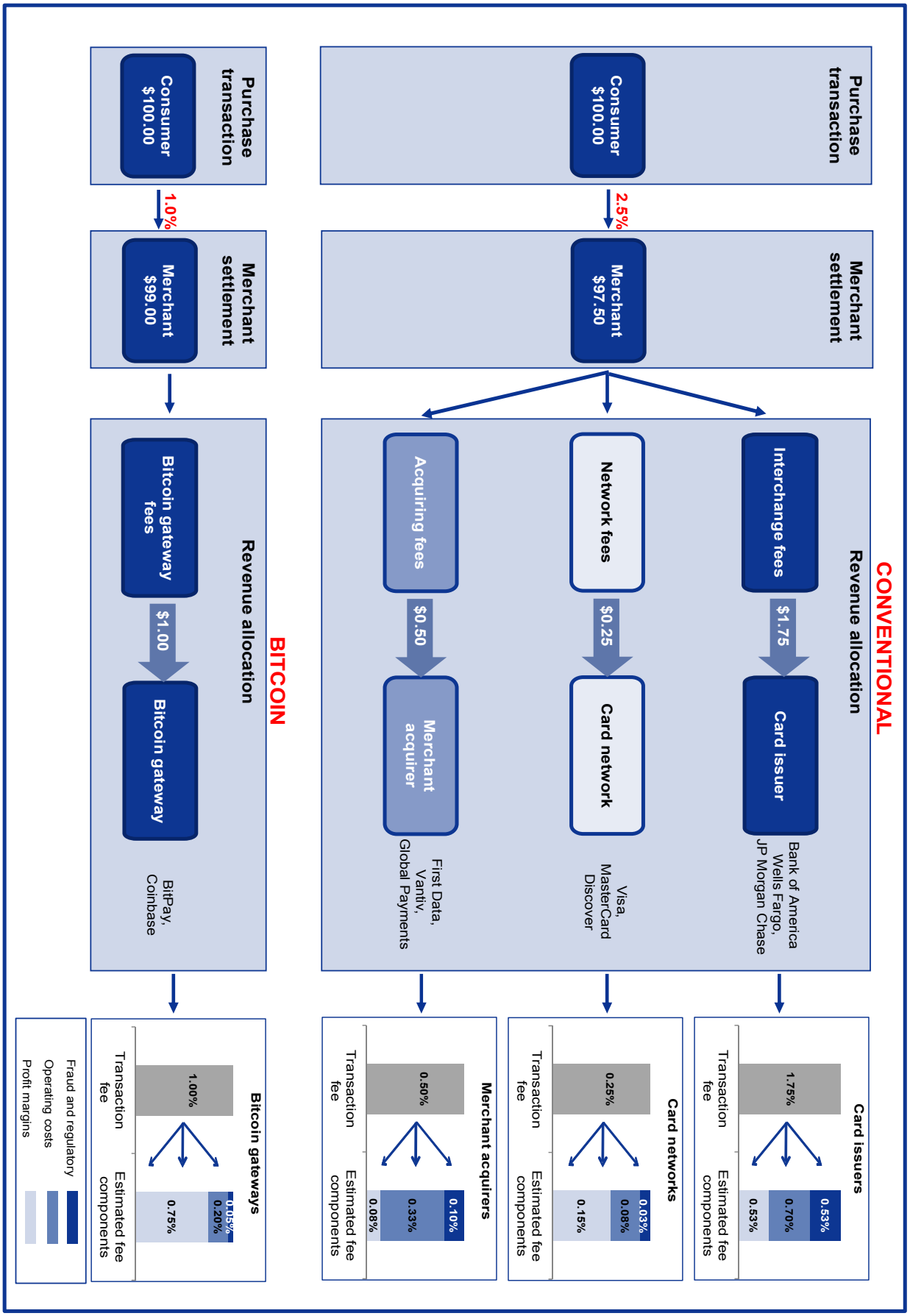
The big hurdle

The biggest hurdle for Bitcoin will be whether the current Bitcoin cost advantage will remain. Increasing regulation is very likely to increase the cost of dealing in Bitcoin, and Bitcoin providers may be forced to pass on this cost to its customers via higher fees. Operating costs more broadly are also likely to rise as operations are scaled up. At the same time, traditional payment providers are likely to respond to the competition by reducing their profit margins and potentially coopting the technology and/or making other structural changes to remain competitive. Indeed, "co-opetition" is already a prevalent feature of the current payments system. PayPal, for example, both competes and cooperates with the current payments ecosystem. While it is too early to tell how banks and payment processors will react to the threat of Bitcoin, we believe that it is only a matter of time before major incumbents develop a digital currency strategy.

Roman Leal

Email: *Roman.leal@gs.com* *Goldman, Sachs & Co.*
Tel: *415-249-7468*

Payments compared



Source: Goldman Sachs Global Investment Research.

Interview with Daniel Masters

Daniel Masters is a founding Co-Principal and Portfolio Manager of Global Advisors, historically a commodities trading house based in the Channel Islands. Below he addresses Bitcoin from a commodity perspective, finding that Bitcoin is an exciting, yet risky, new "commodity."

The views stated herein are those of the interviewee and do not necessarily reflect those of Goldman Sachs.

Allison Nathan: What is your exposure to Bitcoin today?

Daniel Masters: My company, Global Advisors, is based in the Channel Islands, and we are historically a commodities trading house. But one of the most exciting things we are now involved in is Bitcoin, which sits quite nicely on the boundary of our traditional experience. We are trading bitcoin directly on a proprietary basis. We have also started a collective investment fund for investment in bitcoin and the Bitcoin ecosystem. We also have a new Bitcoin storage business because when you start to look at the investment side or the fund side of Bitcoin, you immediately run up against this issue of safe custody. On the periphery, we are also contemplating creating a bitcoin tracker product, applying some of the systematic technology we use in commodities to bitcoin, and we have even toyed with the idea of deploying bitcoin ATM machines.

Allison Nathan: How convinced are you that Bitcoin succeeds?

Daniel Masters: I am optimistic about its prospects for success, but I am not unrealistic. I have a personal and professional investment in Bitcoin, so clearly I am talking my own position. But I have invested precisely what I am prepared to lose 100% of. That is how risky I think it is. I do not normally go around making investments thinking I might lose 100%. I only do so when I think I have a chance of making many multiples of that.

Allison Nathan: How difficult is it to trade bitcoin today?

Daniel Masters: If you are considering things like market access, volatility, bid to offer, market hours and so on I would say this is like trading probably something like zinc on the London Metal Exchange. By that I mean it is not the most liquid market in the world. On occasion, it can be stable. On occasion, it can be very volatile. It is not always a continuous market. So it is not a market that anybody can just trade in. But, every day that goes past it is getting more liquid, transparent and easier to access.

Allison Nathan: Where do you see value in Bitcoin?

Daniel Masters: I think of Bitcoin within the commodity framework and believe that commodity investments fall into three broad categories. The first category is short-term investment for a short-term move that is usually associated with a temporary event. An example would be positioning for a spike in North American natural gas prices due to a cold weather spell. These trades can return hundreds of percent annualized, but the condition usually only persists for a relatively short period. Looking at bitcoin from this perspective, there have clearly been some aggressive short-term moves basically driven by the interplay between rapid adoption of bitcoin and the pushback by regulators. So there are opportunities there, but they are hard to predict.

The second category is short-term investment for a long-term trade, whereby an observable and ongoing change in paradigm generates short-term trading opportunities. An example would be the silver market from 2005 to 2011, when a new class of buyer entered the market through the rise of physical silver-backed exchange-traded funds (ETFs). In the early stages of this paradigm shift, the new ETF buyer represented about 4% of the entire above-ground silver supply. But the reality was that much of that supply was not readily available since it was tied up in industrial uses or jewelry and silverware, etc. So this new demand actually represented about 65% of readily available supply – an enormous shock to the supply/demand balance – and prices had to climb high enough to make more supply available. The end result was a 900% rally in silver prices, and many opportunities along the way to take advantage of this.

> "In my view there is a voracious demand for new bitcoin and, similar to silver, prices will have to rise dramatically to meet it. "

In terms of Bitcoin, I believe this is where the meat of the whole story resides. Similar to the silver ETF, for bitcoin there are increasingly new constituents as more individuals and businesses adopt its usage. This is where the numbers get really scary, and one runs the risk of sounding like an old-time rabid gold-bug or bitcoin zealot - I'll try to avoid that! But in my view there is voracious demand for new bitcoin and, similar to silver, prices will have to rise dramatically to meet it. Specifically, I think the call on bitcoin could very reasonably be $150 billion, which places it, ironically, in the same ballpark as the valuation of Amazon and of Greece's M1 money supply. Essentially, if the average person carries around $100 in their wallet - which is a reasonable amount of walk-around money if you want to buy a coffee and a train ticket and a bunch of flowers to take home - and all of the 1.5 billion Facebook users acquire a virtual currency wallet of that size because they realize that the use of virtual currency is more convenient than using cash or credits cards, then that alone would get you there. But, again like silver, that $150 billion worth of bitcoin is not necessarily readily available. Assuming that 50% of bitcoin is put away in cold storage (stored offline so less readily accessible) or tucked away in an investment fund, then you are potentially looking at much more appreciation, and so on.

The third category is a long-term investment for a long-term move, which has not yet happened but that you expect to happen. An example would be the forward oil curve from the early 2000s to date when the expectations of rising oil demand from emerging market economies and falling oil supplies given natural decline rates in oil producing fields suggested the need for the oil forward curve – which had remained stable around $20/bbl for much of the history of forward pricing - to reprice to a higher level. Forward oil prices ultimately peaked at above $100/bbl and have largely maintained these higher levels to this day.

In the context of Bitcoin, this type of opportunity lies in the outlook for different forms of adoption. I think that there is a meaningful probability that credit cards will go the same way as typewriters and that wire transfer systems will be replaced in the same way that email replaced the postal service – that is the power of Bitcoin.

Bitcoin in pics

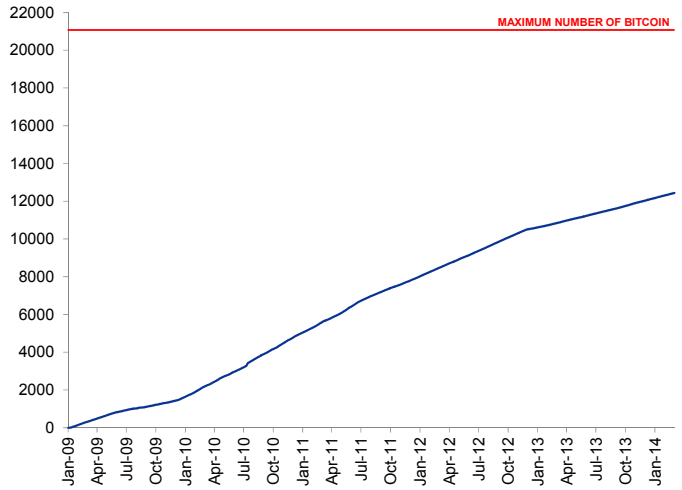
Volatile price; volatile interest

USD/BTC, lhs; Google trend interest, rhs.

Source: Blockchain.info, Google trends. Special thanks to Aaron Woodside.

Half way there

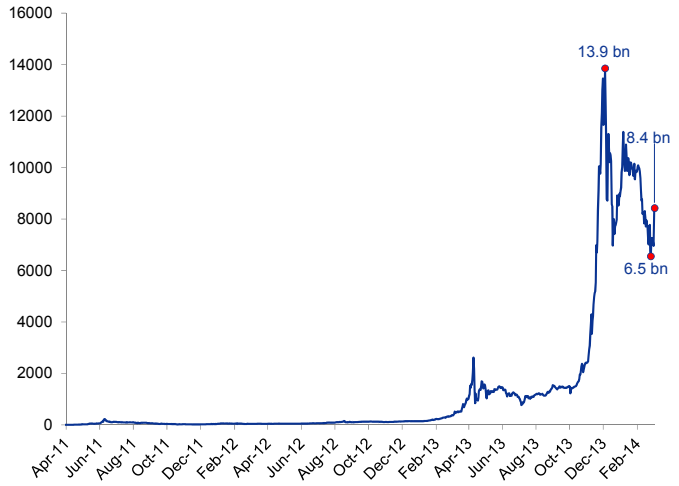
Total bitcoin in circulation



Source: Blockchain.info.

Moving market cap

Bitcoin market capitalization



Source: Blockchain.info.

Max market cap

USD/BTC

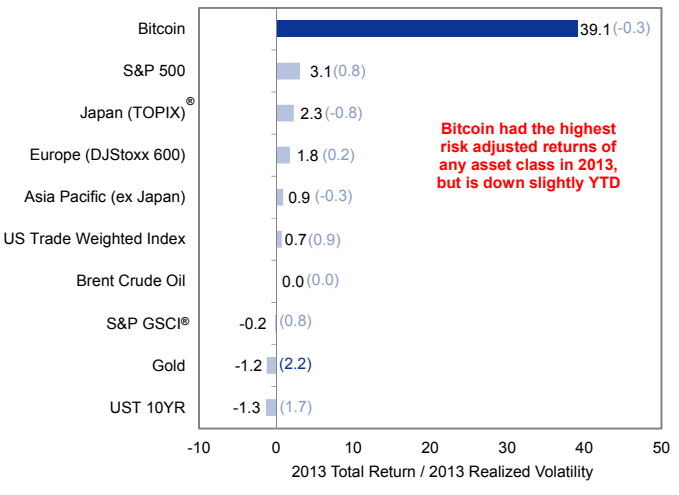
Price per BTC	Total Market Cap given 21 mn max BTC in circulation	Comparable
$100	$2,100,000,000	Tiny
$1,000	$21,000,000,000	A little less than a third of current gold ETF holdings
$10,000	$210,000,000,000	Google market cap
$100,000	$2,100,000,000,000	Roughly Brazil GDP
$1,000,000	$21,000,000,000,000	Roughly US GDP

* Assumes gold price of $1270/toz

Source: Goldman Sachs Global Investment Research.

Bitcoin besting

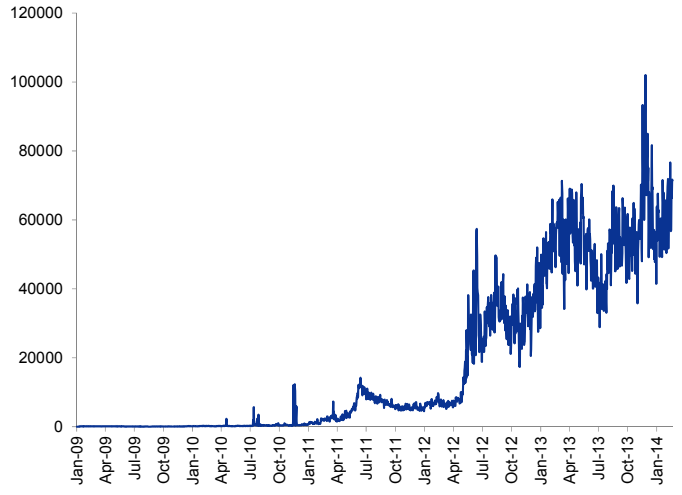
2013 risk-adjusted returns; values in parentheses are 2014 YTD returns



Source: Coindesk.com, Goldman Sachs Global Investment Research. Special thanks to Aaron Woodside.

Budding bitcoin?

Number of average daily bitcoin transactions



Source: Blockchain.info.

Snapshot of our key forecasts

	GDP Growth (% yoy)				FX				Equity				Rates (% eop)				Revision Notes
	2013		2014		3-mth		12-mth		3-mth		12-mth		Policy		10-yr		
	GS	Cons	GS	Cons	GS	Cons	GS	Cons	GS	Cons	GS	Cons	2013	2014	2013	2014	
Global	2.9	2.7	3.6	3.4	-	-	-	-	-	-	-	-	-	-	-	-	
					EUR/$		EUR/$		SP500		SP500						
US	1.9	1.7	3.0	2.9	1.38	1.33	1.40	1.28	1800	-	1900	-	0.09	0.13	2.75	3.25	
					EUR/$		EUR/$		Eurostoxx 50		Eurostoxx 50						
EURO AREA	-0.4	-0.4	1.2	1.0	1.38	1.33	1.40	1.28	3200	-	3500	-	0.25	0.10	-	-	On February 20, we raised our 2014 EA GDP forecast by 0.1% to 1.2% factoring in Q4 GDP and recent indicators.
					EUR/$		EUR/$		DAX		DAX						
GERMANY	0.5	0.5	2.0	1.8	1.38	1.33	1.40	1.28	-	-	-	-	-	-	1.90	2.25	
					$/CNY		$/CNY		HSCEI		HSCEI						
CHINA	7.7	7.7	7.6	7.5	6.10	6.04	6.05	5.95	-	-	12000	-	5.34	4.25	-	-	On February 7, We modestly lowered 1H2014 GDP growth to reflect slowing domestic growth momentum amid the strengthening of measures to combat corruption and pollution, a relatively tight monetary policy stance in late 2013, and expectations of a slightly softer US recovery. We also lowered our HSCEI target.
					$/BRL		$/BRL		BOVESPA		BOVESPA						
BRAZIL	2.3	-	2.4	2.0	2.40	2.44	2.55	2.51	-	-	-	-	10.00	11.00	-	-	On February 13, we revised our BRL forecasts weaker given weaker domestic fundamentals and overall global EM FX pressures that have continued to put pressure on the currency despite intervention; On February 26, we raised our 2014 policy target to 11%.
					$/JPY		$/JPY		TOPIX		TOPIX						
JAPAN	1.6	1.8	1.0	1.6	103	104	110	109	1350	-	1450	-	0.10	0.10	0.80	1.00	On February 24, we revised down our FY2013-14 GDP grpwth forecast to +2.2% (from +2.4%) and +0.5% (from +0.7%) based on weak growth in Q4 2013.

Commodities	Brent crude oil ($/bbl)				Copper ($/mt)				Gold ($/toz)				Corn ($/bu)				Revision Notes
	3-mth		12-mth		3-mth		12-mth		3-mth		12-mth		3-mth		12-mth		
	GS	Cons	GS	Cons	GS	Cons	GS	Cons	GS	Cons	GS	Cons	GS	Cons	GS	Cons	
	108	103	100	104	7000	-	6200	7069	1215	-	1050	1231	4.25	-	4.00	-	

Note: Recent revisions marked in red; GDP consensus is Consensus Economics, all other consensus is Reuters, commodity 12-mo consensus is Reuters for 2014 average.

Source: Goldman Sachs Global Investment Research.

Glossary of GS proprietary indices

Current Activity Indicator (CAI)

Measures the growth signal in the major high-frequency activity indicators for the economy. Gross Domestic Product (GDP) is a useful but imperfect guide to current activity. In most countries, GDP is only available quarterly, is released with a substantial delay, and initial estimates are often heavily revised. GDP also ignores important measures of real activity, such as employment and the purchasing managers' indexes (PMIs). All of these problems reduce the effectiveness of GDP for investment and policy decisions. Our CAIs are alternative summary measures of economic activity that attempt to overcome some of these drawbacks. We currently calculate CAIs for the following countries: USA, Euro area, UK, Norway, Sweden, China, Japan, Hong Kong, India, Indonesia, Malaysia, Philippines, Singapore, South Korea, Taiwan, Thailand, Australia and New Zealand.

Financial Conditions Index (FCI)

Financial conditions are important because shifts in monetary policy do not tell the whole story. Our FCIs attempt to measure the direct and indirect effects of monetary policy on economic activity. We feel they provide a better gauge of the overall financial climate because they include variables that directly affect spending on domestically produced goods and services. The index includes four variables: real 3-month interest rates, real long-term interest rates, real trade-weighted value of the exchange rate and equity market capitalization to GDP.

Global Leading Indicator (GLI)

Our GLIs provide a more timely reading on the state of the global industrial cycle than the existing alternatives, and in a way that is largely independent of market variables. Global cyclical swings are important to a huge range of asset classes; as a result, we have come to rely on this consistent leading measure of the global cycle. Over the past few years, our GLI has provided early signals on turning points in the global cycle on a number of occasions and has helped confirm or deny the direction in which markets were heading. Our GLI currently includes the following components: Consumer Confidence aggregate, Japan IP inventory/sales ratio, Korea exports, S&P GS Industrial Metals Index, US Initial jobless claims, Belgian and Netherlands manufacturing surveys, Global PMI, GS Australian and Canadian dollar trade weighted index aggregate, Global new orders less inventories, Baltic Dry Index.

Goldman Sachs Analyst Index (GSAI)

Our US GSAI is based on a monthly survey of Goldman Sachs equity analysts to obtain their assessments of business conditions in the industries they follow. The results provide timely "bottom-up" information about US economic activity to supplement and cross-check our analysis of "top-down" data. Based on their responses, we create a diffusion index for economic activity comparable to the ISM's indexes for activity in the manufacturing and nonmanufacturing sectors.

Macro-data Assessment Platform (MAP)

Our MAP scores facilitate rapid interpretation of new data releases. In essence, MAP combines into one simple measure the importance of a specific data release (i.e., its historical correlation with GDP) and the degree of surprise relative to the consensus forecast. We put a sign on the degree of surprise, so that an underperformance will be characterized with a negative number and an outperformance with a positive number. We rank each of these two components on a scale from 0 to 5, and the MAP score will be the product of the two, i.e., from –25 to +25. The idea is that when data are released, the assessment we make will include a MAP score of, for example, +20 (5;+4)—which would indicate that the data has a very high correlation to GDP (the '5') and that it came out well above consensus expectations (the '+4')—for a total MAP value of '+20.' We currently employ MAP for US, EMEA and Asia data releases.

Top of Mind Archive

Issue 1: Euro Area Sovereign Crisis
Euro Area – What's Next?
July 12, 2012

Issue 2: Fiscal Cliff
Staring Down the Fiscal Cliff
August 8, 2012

Issue 3: Oil: Iran, Shale and Regulation
Oil on the Boil – Again?
September 6, 2012

Issue 4: (Unconventional) Monetary Easing
The Big Ease
October 3, 2012

Issue 5: US Election
US Election Inspection
October 24, 2012

Issue 6: China Leadership Handover
Demystifying the China Handover
November 5, 2012

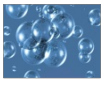
Issue 7: Natural Disasters and Climate Change
Catastrophes and Climate
December 11, 2012

Special Issue: 2012 Update, and Peek at 2013
December 20, 2012

Issue 8: Japan
On the Edge of Catharsis, or Crisis?
January 17, 2013

Issue 9: US Housing
US Housing in the Hot Seat
February 13, 2013

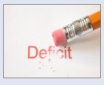
Issue 10: Currency Wars
Currency Wars on the Front Line
March 26, 2013



Issue 11: Sustainability of Low Bond Yields
Bond Bubble Breakdown
April 22, 2013

Issue 12: Future of the EU/EMU
Ins and Outs of the EU/EMU
May 16, 2013

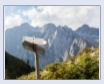
Issue 13: Search for Yield
Leading to Growth or Disaster?
June 20, 2013



Issue 14: US Fiscal Issues
Are US Fiscal Worries Really Over?
July 11, 2013

Issue 15: China Credit Build-up
China Credit Concerns
August 5, 2013

Issue 16: German Election
German Election Reflection
September 11, 2013



Issue 17: Emerging Markets
EM at an Inflection
October 9, 2013

Issue 18: Central Bank Forward Guidance
A Guide to Guidance
October 31, 2013

Issue 19: China Reform
Changing China
December 5, 2013

Special Issue: 2013 Update, and a Peek at 2014
December 18, 2013

Issue 20: Deflation
Deflation Dangers
January 22, 2014

Source of photos: www.istockphoto.com, NOAA-NASA GOES Project.

Disclosure Appendix

Reg AC

We, Allison Nathan, Jeffrey Currie, Jose Ursua, and Dominic Wilson, hereby certify that all of the views expressed in this report accurately reflect our personal views, which have not been influenced by considerations of the firm's business or client relationships.

I, Roman Leal, CFA, hereby certify that all of the views expressed in this report accurately reflect my personal views about the subject company or companies and its or their securities. I also certify that no part of my compensation was, is or will be, directly or indirectly, related to the specific recommendations or views expressed in this report.

Global product; distributing entities

The Global Investment Research Division of Goldman Sachs produces and distributes research products for clients of Goldman Sachs on a global basis. Analysts based in Goldman Sachs offices around the world produce equity research on industries and companies, and research on macroeconomics, currencies, commodities and portfolio strategy. This research is disseminated in Australia by Goldman Sachs Australia Pty Ltd (ABN 21 006 797 897); in Brazil by Goldman Sachs do Brasil Corretora de Títulos e Valores Mobiliários S.A.; in Canada by Goldman, Sachs & Co. regarding Canadian equities and by Goldman, Sachs & Co. (all other research); in Hong Kong by Goldman Sachs (Asia) L.L.C.; in India by Goldman Sachs (India) Securities Private Ltd.; in Japan by Goldman Sachs Japan Co., Ltd.; in the Republic of Korea by Goldman Sachs (Asia) L.L.C., Seoul Branch; in New Zealand by Goldman Sachs New Zealand Limited; in Russia by OOO Goldman Sachs; in Singapore by Goldman Sachs (Singapore) Pte. (Company Number: 198602165W); and in the United States of America by Goldman, Sachs & Co. Goldman Sachs International has approved this research in connection with its distribution in the United Kingdom and European Union.

European Union: Goldman Sachs International, authorized by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority, has approved this research in connection with its distribution in the European Union and United Kingdom; Goldman Sachs AG and Goldman Sachs International Zweignierderlassung Frankfurt, regulated by the Bundesanstalt für Finanzdienstleistungsaufsicht, may also distribute research in Germany.

General disclosures

This research is for our clients only. Other than disclosures relating to Goldman Sachs, this research is based on current public information that we consider reliable, but we do not represent it is accurate or complete, and it should not be relied on as such. We seek to update our research as appropriate, but various regulations may prevent us from doing so. Other than certain industry reports published on a periodic basis, the large majority of reports are published at irregular intervals as appropriate in the analyst's judgment.

Goldman Sachs conducts a global full-service, integrated investment banking, investment management, and brokerage business. We have investment banking and other business relationships with a substantial percentage of the companies covered by our Global Investment Research Division. Goldman Sachs & Co., the United States broker dealer, is a member of SIPC (http://www.sipc.org).

Our salespeople, traders, and other professionals may provide oral or written market commentary or trading strategies to our clients and our proprietary trading desks that reflect opinions that are contrary to the opinions expressed in this research. Our asset management area, our proprietary trading desks and investing businesses may make investment decisions that are inconsistent with the recommendations or views expressed in this research.

The analysts named in this report may have from time to time discussed with our clients, including Goldman Sachs salespersons and traders, or may discuss in this report, trading strategies that reference catalysts or events that may have a near-term impact on the market price of the equity securities discussed in this report, which impact may be directionally counter to the analysts' published price target expectations for such stocks. Any such trading strategies are distinct from and do not affect the analysts' fundamental equity rating for such stocks, which rating reflects a stock's return potential relative to its coverage group as described herein.

We and our affiliates, officers, directors, and employees, excluding equity and credit analysts, will from time to time have long or short positions in, act as principal in, and buy or sell, the securities or derivatives, if any, referred to in this research.

This research is not an offer to sell or the solicitation of an offer to buy any security in any jurisdiction where such an offer or solicitation would be illegal. It does not constitute a personal recommendation or take into account the particular investment objectives, financial situations, or needs of individual clients. Clients should consider whether any advice or recommendation in this research is suitable for their particular circumstances and, if appropriate, seek professional advice, including tax advice. The price and value of investments referred to in this research and the income from them may fluctuate. Past performance is not a guide to future performance, future returns are not guaranteed, and a loss of original capital may occur. Fluctuations in exchange rates could have adverse effects on the value or price of, or income derived from, certain investments.

Certain transactions, including those involving futures, options, and other derivatives, give rise to substantial risk and are not suitable for all investors. Investors should review current options disclosure documents which are available from Goldman Sachs sales representatives or at http://www.theocc.com/about/publications/character-risks.jsp. Transaction costs may be significant in option strategies calling for multiple purchase and sales of options such as spreads. Supporting documentation will be supplied upon request.

In producing research reports, members of the Global Investment Research Division of Goldman Sachs Australia may attend site visits and other meetings hosted by the issuers the subject of its research reports. In some instances the costs of such site visits or meetings may be met in part or in whole by the issuers concerned if Goldman Sachs Australia considers it is appropriate and reasonable in the specific circumstances relating to the site visit or meeting.

All research reports are disseminated and available to all clients simultaneously through electronic publication to our internal client websites. Not all research content is redistributed to our clients or available to third-party aggregators, nor is Goldman Sachs responsible for the redistribution of our research by third party aggregators. For research or data available on a particular security, please contact your sales representative or go to http://360.gs.com.

Disclosure information is also available at http://www.gs.com/research/hedge.html or from Research Compliance, 200 West Street, New York, NY 10282.