

TOP *of* MIND

IS BITCOIN A (BURSTING) BUBBLE?



Following the spectacular rise and fall of bitcoin prices, it goes without saying that cryptocurrencies are Top of Mind. While we maintain that the underlying blockchain technology holds promise, here we dig into the key question facing investors today: What is the value of cryptocurrencies themselves? According to Pantera Capital’s Dan Morehead, they are transformative enough to take market share from banks, credit card companies, currencies, and gold—implying a fair value much higher than recent peaks. We are more skeptical, as cryptocurrencies appear to solve economic problems only in a limited set of cases (e.g., in the absence of a well-functioning banking system). We also highlight the bubble-like characteristics of recent crypto price action and the hurdles to institutional investment. Finally, we question whether evolving technology could make today’s generation of cryptocurrencies obsolete, even if blockchain eventually plays a larger role in the economy.

“

Cryptocurrencies are clearly very volatile. And anything that can go up 10 times in six months can easily go down 50% in a week.... But it’s very difficult for me to believe that we are in the midst of a bubble.

- Dan Morehead, Founder and CEO, Pantera Capital

Whether any of today’s cryptocurrencies will survive over the long run seems unlikely to me, although parts of them may evolve and survive.... To my eye, they still seem too primitive to be the long-term answer.

- Steve Strongin, Head of Global Investment Research, Goldman Sachs

”

WHAT’S INSIDE

INTERVIEWS WITH:

Dan Morehead, Founder and CEO, Pantera Capital

Steve Strongin, Head of Global Investment Research, Goldman Sachs

CRYPTOCOMMODITIES, NOT CURRENCIES

Jeff Currie, Michael Hinds & Huan Wei, GS Commodities Research

IRRATIONAL (DIGITAL) EXUBERANCE

Charlie Himmelberg & James Weldon, GS Global Markets Research

BITCOIN AS MONEY

Zach Pandl & Charlie Himmelberg, GS Global Markets Research

BTC FOR INSTITUTIONS: MORE HURDLES TO CLEAR

Alex Blostein & Sheriq Sumar, GS Capital Markets Research

BEYOND BTC: A TAXONOMY OF OTHER CRYPTOS

James Schneider, GS Payments and IT Services Research

COULD BLOCKCHAIN BE TRANSFORMATIVE? YES.

James Schneider, GS Payments and IT Services Research

...AND MORE

Allison Nathan | allison.nathan@gs.com

Marina Grushin | marina.grushin@gs.com

David Groman | david.groman@gs.com

Investors should consider this report as only a single factor in making their investment decision. For Reg AC certification and other important disclosures, see the Disclosure Appendix, or go to www.gs.com/research/hedge.html.

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

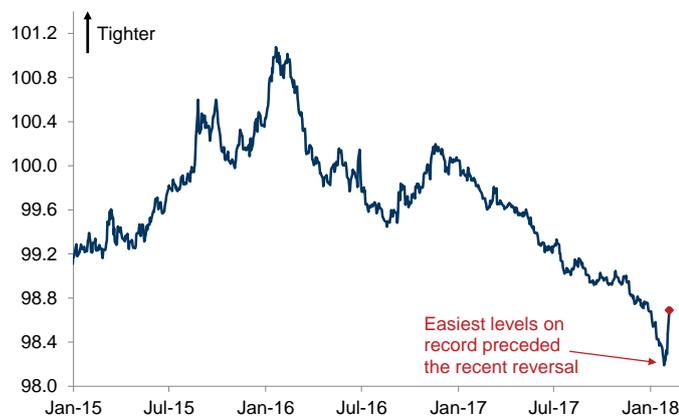
- We raised our 2018 GDP forecast by 0.2pp to 2.8% (on a Q4/Q4 basis), reflecting firm growth signals.
- We raised our odds of a March rate hike to 95% from 90%.

Datapoints/trends we're focused on

- The recent equity-driven tightening of our financial conditions index (FCI), albeit from historically easy levels.
- Signs of a potential reacceleration in wages, including the rise in average hourly earnings growth to 2.9% in January.
- A widening federal deficit—unusual this late in the cycle.

FCI reversal

GS US Financial Conditions Index (FCI)



Source: Goldman Sachs Global Investment Research.

Europe

Latest GS proprietary datapoints/major changes in views

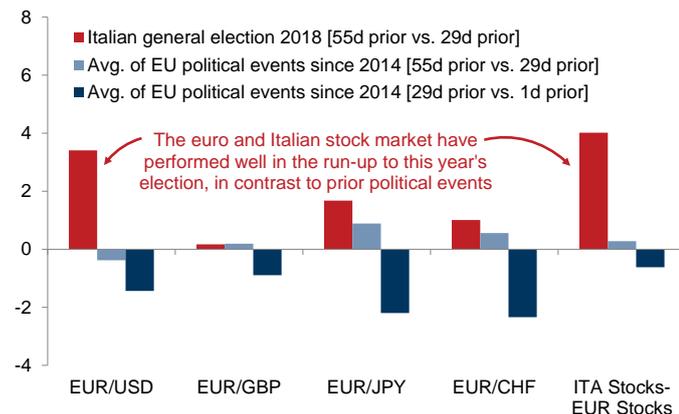
- We raised our Q1 Euro area GDP forecast by 0.2pp to 0.8% qoq on the back of strong real activity data.

Datapoints/trends we're focused on

- A new 11-year high in the Euro area composite PMI.
- ECB focus on the effects of EUR strength on inflation; we forecast muted inflation and a 3-month extension of the APP.
- Progress on German coalition talks, though differences on key issues must still be resolved before a government is formed.
- Signs of market complacency ahead of Italian elections.

Calm before the vote

Cumulative asset price change before European political events, %



Source: Bloomberg, Goldman Sachs Global Investment Research.

Japan

Latest GS proprietary datapoints/major changes in views

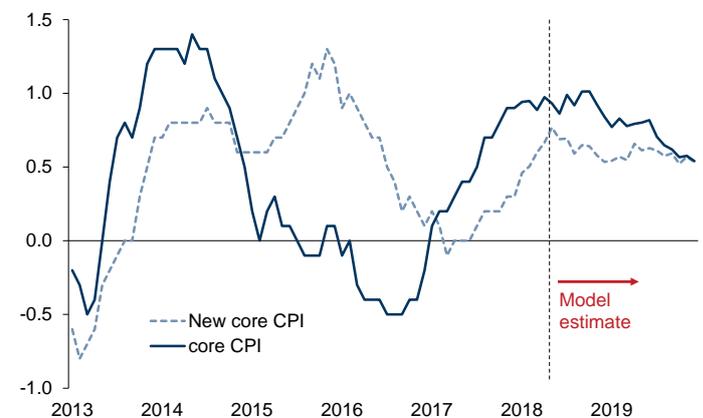
- We raised our Q2 GDP forecast by 0.2pp to 1.7% qoq ann. on private capex/consumption; we also lifted 3Q-4Q18 figures.

Datapoints/trends we're focused on

- The BOJ's recent reiteration of its commitment to continued easing until inflation reaches the 2% target—likely intended to dampen market expectations for an early rate hike.
- A boost to CPI from higher oil prices, which should reach 1% in 1H18; however, overall inflation trends remain weak.
- Post-crisis highs in the Reuters Tankan survey of manufacturers.

Rising, but still subdued

Japan core CPI and new core CPI (excl. fresh food/energy), %yoy



Source: MIC, Goldman Sachs Global Investment Research.

Emerging Markets (EM)

Latest GS proprietary datapoints/major changes in views

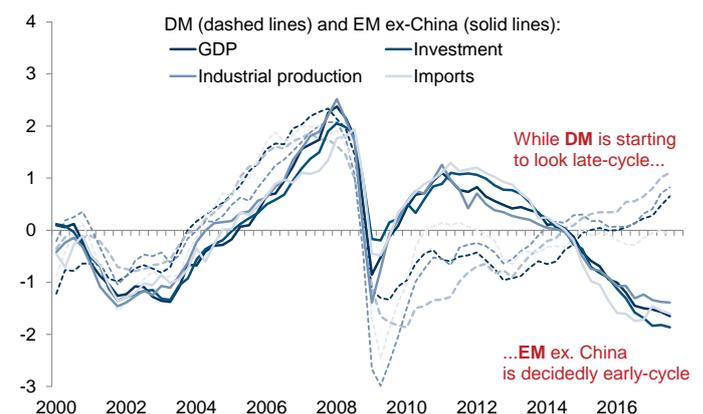
- No major changes in views.

Datapoints/trends we're focused on

- Room for sustained economic growth in the long run across EMs, which remain early-cycle (ex-China), unlike many DMs.
- Converging EM inflation rates driven by more credible monetary policy and a secular improvement in balance sheets.
- US investigations into Chinese trade practices; new trade barriers imposed by the US could elicit retaliatory sanctions.
- Prospects for lower inflation and rate cuts in South Africa.

EM is still early-cycle

Deviation of EM and DM indicators from 2000-17 trend, std. dev.



Source: Haver Analytics, Goldman Sachs Global Investment Research.

Is bitcoin a (bursting) bubble?

Do we even have to state that cryptocurrencies are Top of Mind? The spectacular rise in the price of bitcoin and other cryptocurrencies late last year, only to be followed by a more-than-60% drop from the peak in December, has ignited nothing short of a crypto mania on Main Street and Wall Street alike. The launch of the first bitcoin futures contracts in December, along with increased attention from regulators worldwide, has only added fuel to the fire.

We first wrote about bitcoin in [March 2014](#), exploring its perceived advantages and disadvantages from many angles. Our conclusion then was that bitcoin faced challenges to widespread adoption, but that the distributed ledger technology underpinning it and other cryptocurrencies (i.e., the blockchain), was a promising innovation—a view we maintain today.

Here, we dig deeper into the key question for investors currently contemplating the space: What is the value of cryptocurrencies themselves? The answer should help determine whether cryptocurrencies are a speculative bubble in the midst of bursting, or an innovation so transformative that its value is not yet reflected in the market price.

We begin by sitting down with Dan Morehead, founder and CEO of Pantera Capital, an investment firm focused exclusively on cryptocurrencies and one of the largest institutional investors in crypto to date. Not surprisingly, Morehead is a diehard crypto aficionado who believes that cryptocurrencies have enormous disruptive potential across financial services and money transmission. He sees cryptos as competitors to correspondent banks, credit card companies, conventional stores of wealth like gold, and fiat currencies. Assuming bitcoin captures some market share from each of these incumbents, he estimates its fair value could be roughly \$500,000 (no, we did not mistakenly add zeros).

In Morehead's view, it is therefore difficult to call recent cryptocurrency price action a bubble. And the potential for new market entrants in the form of institutional investors—which are essentially non-existent in the space today—gives him confidence that the price of cryptos will be substantially higher a year from now. What could quash his enthusiasm? Adverse regulatory action.

In a nutshell, we are more skeptical on the fair value of bitcoin and its peers. For one, Charlie Himmelberg and James Weldon of the GS Global Markets Research team argue that cryptocurrency price action and investor behavior fit the classic definition of a speculative bubble. In contrast to Morehead, they see the contagious enthusiasm for crypto among mainly retail investors as a telltale warning sign—the equivalent of daytraders buying anything ending in “.com” in 1999.

And while some observers have argued that the recent launch of bitcoin futures marks an important step in legitimizing cryptocurrency investing, GS Capital Markets Analysts Alex Blostein and Sheriq Sumar point out that futures alone cannot address some of the key market structure barriers facing crypto investors, particularly at the institutional level. Establishing reputable custody services, ensuring central clearing in the spot

markets, and addressing connectivity risks—among other issues—will take time.

Steve Strongin, Head of GS Global Investment Research, thinks institutional investors should be worried about more than just bubble risks or market structure. In his view, the more important question is whether today's cryptocurrencies will exist five or ten years from now. His answer? It's possible but not probable, for the same reason that almost all of the first internet search engines are now defunct: Something better replaced them. That doesn't mean blockchain technology—or some successor to it—won't eventually play a larger role in the economy; in fact, we see potential applications for blockchain across industries (see pgs. 18-19). But in Strongin's view, it does suggest that the cryptocurrencies that don't survive are likely to trade to zero—a risk that seems broadly underappreciated in the market today.

But even if that ends up the case, is there any way of knowing which cryptocurrencies—current or future—will have more staying power than their peers? GS Payments and IT Services Analyst James Schneider argues that different crypto use cases could provide some insight. For example, it is almost certain that only a very small number of coins could succeed as media of exchange, given that success depends on widespread acceptance. On the other hand, special-purpose tokens being developed for various distributed applications could probably co-exist in greater numbers.

All that said, the above begs the basic but crucial question of whether any cryptocurrency could actually derive value from acting as a currency or a commodity—the key to understanding its ultimate potential. In our view, this depends on what economic problem cryptocurrencies solve. As a currency, GS co-Head of Global FX and EM Strategy Zach Pandl and co-Chief Markets Economist Charlie Himmelberg argue that in most places where well-functioning fiat currencies and banking systems exist, there seems to be no obvious problem to solve and thus limited use for cryptocurrencies. But they do conclude that in corners of the world where this is not the case, cryptos may be a viable alternative.

As a commodity, GS Head of Global Commodities Research Jeff Currie and team also find some instances where cryptos solve an economic problem—if that problem is efficiently storing wealth outside of the established banking system. But that use case is likely to be most valued, again, in places with unreliable banking systems, as well as in dark markets. When it comes to acting as a store of value in regulated markets, gold remains superior to bitcoin and its peers, in their view. And a long list of hurdles remains for that to change.

P.S. For those of you just getting your feet wet in the world of cryptocurrencies, see our backgrounders on pgs. 15, 20, and 21 as well as an annotated history of bitcoin prices on pg. 8.

Allison Nathan, Editor

Email: allison.nathan@gs.com
Tel: 212-357-7504
Goldman Sachs and Co. LLC



Interview with Steve Strongin

Steve Strongin is the head of Goldman Sachs Global Investment Research. Below, he argues that that the current generation of cryptocurrencies is unlikely to survive even if blockchain technology endures.



Allison Nathan: Do cryptocurrencies have intrinsic value?

Steve Strongin: Like all fiat currencies, cryptocurrencies really don't have intrinsic value. But that doesn't mean that people won't treat them as if they do, and sometimes for sustained periods of time. In fact, people have throughout history

accepted things that have no value in exchange for things that do. Examples of non-government-issued currencies being used for periods of time include playing cards in the French colonies in the 18th century and limestone discs on the island of Yap centuries ago. What this means in practice is that even if a currency doesn't have intrinsic value, it could still be used for some period of time.

Allison Nathan: Will cryptocurrencies survive?

Steve Strongin: Whether any of today's cryptocurrencies will survive over the long run seems unlikely to me, although parts of them may evolve and survive. They really are the first "modern" experiments in blockchain technology and in cryptocurrencies. To my eye, they still seem too primitive to be the long-term answer. Aside from the fact that many cryptocurrencies have slow transaction times today, there are also challenges in safely storing the associated data, and maintenance requirements can be significant. Given the innovation that would be required to address these problems, it would be surprising—though not impossible—to see existing cryptocurrencies have real staying power in their current form. Ultimately, I think new cryptocurrencies will emerge but of course time will tell. As it relates to the underlying technology—blockchain or some successor to it—there is a great deal of hope that it will prove useful in a variety of ways. That may be true, but if the technology does survive, it may eventually look quite different than it does today.

“Whether any of today's cryptocurrencies will survive over the long run seems unlikely to me, although parts of them may evolve and survive.”

Allison Nathan: What about the argument that first mover advantage makes the earliest cryptocurrencies—like bitcoin—more likely to survive?

Steve Strongin: The idea of a "first mover advantage" in any industry seems a bit archaic today. In fact, examples of modern day first mover advantages are actually hard to find. The very first web browser and search engine, for example, are no longer in existence. So if being the first mover is an advantage at all today, it doesn't seem to be a deep or sustainable one. In the case of cryptocurrencies, the strong price movements in

dozens of them—not just the first one—suggest that even the broader market hasn't chosen a clear "winner."

Allison Nathan: Is the market accurately pricing the likelihood that several—if not most—of the current cryptocurrencies will ultimately fail?

Steve Strongin: I don't believe it is. People seem to be trading cryptocurrencies as though they're all going to survive, or at least maintain their value. The high correlation between the different cryptocurrencies worries me. Contrary to what one would expect in a rational market, new currencies don't seem to reduce the value of old currencies; they all seem to move as a single asset class. But if you believe this is a "few-winners-take-most" situation, then the potential for retirement depreciation should be taken into account. And because of the lack of intrinsic value, the currencies that don't survive will most likely trade to zero. This is actually an important distinction between cryptocurrencies and fiat currencies; if a government decides to phase out a currency, it will typically determine a residual value for that currency and exchange that currency for a replacement one. But here the ability to merge older cryptocurrencies with newer, better ones—and the incentives for the eventual winners to offer a residual value for the retiring currencies—appears very limited. The market does not seem to be taking this risk into account.

“The high correlation between the different cryptocurrencies worries me... if you believe this is a 'few-winners-take-most' situation, then the potential for retirement depreciation should be taken into account.”

Allison Nathan: But hasn't the launch of bitcoin futures contracts been a key development in helping legitimize cryptocurrencies and their use in regulated markets?

Steve Strongin: If 20 years from now bitcoin still exists, then the establishment of futures contracts will clearly be one of the benchmark events in its history. But there are numerous examples of failed futures contracts. So if bitcoin doesn't survive, it will be just another example in that long list of failed contracts. In the end, currencies are about buying stuff. So in my mind, the critical innovation would be one that enables cryptocurrency holders to buy large ticket goods and services efficiently.

Allison Nathan: Has recent price action in cryptocurrencies been indicative of a bubble?

Steve Strongin: I think so. At least at the moment, cryptocurrencies are not tied to the creation of economic value in the way that equities, for example, are tied to earnings growth over time. Rather, the way cryptocurrencies seem to be valued today is based on what people might pay for them tomorrow, which is almost the definition of a bubble. Even if

someone were to believe that blockchain technology will one day change the world, they would be hard-pressed to come up with a fundamental reason to explain why the price of cryptocurrencies increased many times over and then halved in a very short period of time; this volatility is indicative of speculative behavior.

In hindsight, this period will probably end up looking like the internet bubble of the late 1990s. Very few companies that existed then went on to become even more valuable. Amazon did—but in a completely different form. Google—a big winner today—had only just been formed at the time. And numerous other search companies existed but they were unable to create value and ended up disappearing. So, are any of today's cryptocurrencies going to be an Amazon or a Google, or will they end up like many of the now-defunct search engines? Just because we are in a speculative bubble does not mean current prices can't increase for a handful of survivors. At the same time, it probably does mean that most, if not all, will never see their recent peaks again.

“ Just because we are in a speculative bubble does not mean current prices can't increase for a handful of survivors. At the same time, it probably does mean that most, if not all, will never see their recent peaks again.”

Allison Nathan: Setting aside the recent price action, is there a useful role for cryptocurrencies in financial markets today?

Steve Strongin: As it relates to the underlying technology, there is clearly a role for improving the ledgers that underlie financial transactions. Substantial investment is being made in leveraging blockchain technology to more efficiently and quickly settle contracts, confirmations, and related transactions. But the current technology does not yet offer the speed that will be required for market transactions.

Now, if the question is whether there is a fundamental need for a currency that is not tied to a central bank, the answer in my opinion is “no” in most cases, at least within the regulated markets. Even if transaction times improved, the notion that people would prefer cryptocurrencies for everyday transactions seems like a stretch. There is perhaps a slightly more compelling case for their use as a store of a value. Cryptocurrencies are well-suited in particular for the many documented use cases in dark markets. They are cheap to store, easy to conceal and hard to trace. So it is plausible that cryptocurrencies may have a long-term role to play in these markets, but even that is not assured. And the possibility of cryptocurrencies catching on in the dark markets has little to no implication for their applications elsewhere; it is very difficult to turn an asset that was optimized for dark markets into one suitable for lit markets. Is it possible? Yes. But in my view, it is unlikely.

Cryptocommodities, not currencies

Jeff Currie and team argue that cryptocurrencies possess some superior attributes relative to other commodities, but with limited applications (i.e., in dark markets)

Despite being called cryptocurrencies, bitcoin and other digital assets are better described as “cryptocommodities.” A financial security—currencies included—has a claim or liability attached to it, as it is “secured” to an underlying real asset. Just as equity is secured to the future earnings of a real company, a dollar bill is secured to the US government and its tax revenue. In contrast, commodities have no obligation or liability to any government, company, or other entity. Given that bitcoin has no liability to any entity, it is a good like any other commodity. Bitcoin just happens to be the first digital commodity—in contrast to financial assets and money, which have long been digitized.

However, bitcoin is neither gold, nor oil or copper. Its value is derived from its own unique physical, financial, and economic properties. Physically, bitcoin and other cryptocurrencies have the highest value density (\$/cm³) of all assets, meaning users can store more money in less space and enjoy greater ease of transport than with any other commodity. Transactions in bitcoin at the protocol level also remain completely secure, with a verification process that beats assayed gold inside a vault. Financially, bitcoin futures yield a positive cash and carry; however, market fragmentation and high margin requirements make this carry difficult to arbitrage. Economically, the supply of new bitcoins must follow a pre-determined trajectory, in contrast to other commodities; this prevents supply from responding to changes in demand (although not all cryptocurrencies share this characteristic).

In most economies, a standard digital bank account provides ease of storage, secure transactions, and a positive carry. However, it is still a claim on a bank, and the funds cannot be concealed and transported without alerting regional authorities. To the extent that this is a problem, bitcoin solves it better than any other commodity (although other cryptocurrencies are starting to offer superior privacy and anonymity). This suggests that black markets and less developed regions without a reliable banking system would be the obvious sources of demand for cryptocurrencies (see also pgs. 12-13).

The physical: more value on a floppy disk than in Fort Knox

Unlike other storage commodities like oil, gold, platinum, diamonds, and even cash, there is no need to hold much physical material to own bitcoin; even a technology as obsolete as the 3½ inch floppy disk can hold almost 30,000 private keys. There is no theoretical upper limit to the value of bitcoins in a wallet, but if we assume each wallet secured by this disk contains as much as the largest wallet today (180,000 BTC), this single disk could “hold” all bitcoins in existence and remain less than 0.5% full. Assuming a bitcoin market cap of roughly \$190bn (as of late January), this disk would be the equivalent to either: 95% of the 4,583 tons of gold in Fort Knox, or 1,344 Very Large Crude Carrier supertankers of oil.

That said, long-term storage and security are extremely challenging for bitcoin. The primary risk is hacking, but physical degradation (“bit rot”) can also occur. Offline storage, hardware wallets, and paper backups can help to partially mitigate these risks, but these steps require deeper-than-average technical knowledge and are often skipped by users. And bitcoin custodial services are still extremely uncommon. In contrast, gold has the best properties for storage among all the chemical elements known to man (being solid, dense, non-reactive, non-explosive, non-radioactive, and non-toxic) and hence has an extensive global network of storage facilities. If the financial markets for bitcoin are to succeed, cryptocurrencies need to develop an equally extensive network of storage facilities with custodial services. Until then, gold will remain the dominant commodity used as store of value with institutional investors.

Storing \$190bn in bitcoin...

Value density, \$/3.5 inch floppy disk (27.8cm³)



Source: CME, Blockchain.com, Wikipedia, company data, Goldman Sachs Global Investment Research.

...vs. more than \$205mn in cash

Cash confiscated by US authorities in a 2007 drug/money laundering case



Source: US Department of Justice / Wikimedia Commons / Public Domain.

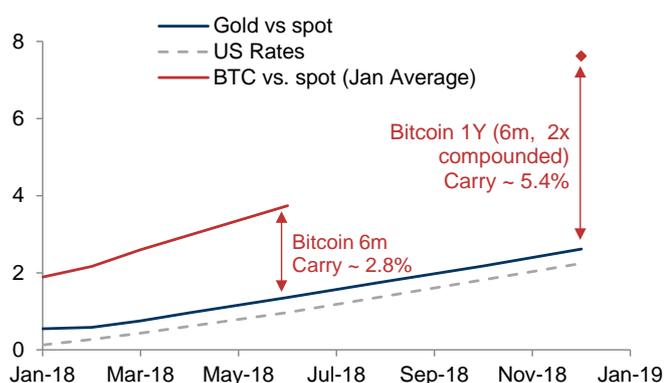
The financial: be wary of bitcoin's 5.4% yield

For the majority of bitcoin futures trading since their launch in December, the futures curves have been in steep contango, meaning that near-dated prices are below longer-dated prices. Gold, which is a non-yielding asset, shows similar contango behavior. For gold, in theory and in practice the “carry” embedded in this contango is just enough to cover the cost of borrowing money to buy the gold to deliver in the future. If that weren't the case, market participants could make risk-free profits, and would continue to buy spot gold and sell gold futures—ultimately bidding up the price for the former and bidding down the price for the latter—until the carry opportunity declined again to zero.

However, in the past few weeks before the first CME bitcoin contract expired, the “carry” in the bitcoin futures curve far exceeded the equilibrium in gold, implying a carry trade that could yield 5.4% annualized. Why would such an arbitrage opportunity exist? In our view the answer is the structure and early stage of the market.

Positive carry: not free money

US rates, gold futures vs. spot, and bitcoin futures vs. spot, %



Note: 5.4% carry calculated as of January 25, 2018.

Source: Bloomberg, CME, Goldman Sachs Global Investment Research.

Bitcoin spot trading still takes place among a highly segmented investor base and on many different spot exchanges. With no large institutions operating across exchanges, there is likely an insufficient scale of arbitrage to drive spreads out of the market. Bitcoin futures are also USD settled, not BTC deliverable (see more on pg. 14). In our view, this largely reflects the difficulty that many institutions currently face in handling bitcoin, including compliance risks (anti-money laundering, know your customer, and counter-terrorist financing); risks and costs associated with warehousing bitcoins, both physically, including risks of hacking, as well as balance sheet risk for a still highly volatile asset class; a slow ramp-up in IT and other systems; inability to leverage¹; uncertainty surrounding the true spot exchange rate²; and a lack of basic comfort over the underlying technology and economics. Combined, these issues are keeping spreads between exchanges, as well as between spot and futures prices, wide and volatile.

The economic: a real-world carbon footprint and real supply constraints

Mining both bitcoin and minerals requires substantial upfront expenditure with an uncertain future payoff. In bitcoin mining, this problem is exacerbated by the fact that prices fluctuate wildly and new hardware vastly out-competes old hardware, hyper-charging cycles of investment and obsolescence. The rate of technological improvement has been phenomenal; data on bitcoin mining hardware suggest that ASIC miners have achieved a 6x improvement in efficiencies from early 2014. In

contrast, the most impressive R&D success story of the last decades—shale oil—has managed only a 4x improvement in production per rig since January 2010, and only in the most productive basin.

Like most commodity production, bitcoin mining has low labor intensity versus extremely high capital intensity. Bitcoin may even be the least labor-intensive commodity. For example, the largest Chinese mine reportedly accounts for close to 4% of total network hash rate—corresponding to gross revenues of around \$400mn per year (657,000 BTC)—but employs only 50 people. In the oil market, the equivalent would be Canada, which accounts for 5% of global production, has gross production revenues of around \$100bn per year, and employs a total of 57,000 people in the sector. This example suggests that the ratio of USD output per employee is about 4x higher in bitcoin mining than in oil production. On the other hand, bitcoin mining requires relatively more energy than mining minerals and hydrocarbons, which is one reason why the carbon footprint of bitcoin has received much greater focus.

As with other commodities, bitcoin’s equilibrium price equals the cost of the last miner to join in producing. But in other commodities markets, producers can decide to add more capital when prices are high in order to produce more supply; when commodities prices rise, the quantity supplied also tends to rise. In contrast, the price of bitcoin cannot impact the supply of new coins, which follows a trajectory built into the bitcoin source code. So high prices can attract new miners but will not affect the number of new bitcoins created or bitcoin prices. Bitcoin aficionados view this characteristic positively, but the flip-side is that miners cannot adjust supply to accommodate shifts in demand, which leaves bitcoin structurally more volatile than other commodities, and even other cryptocurrencies that don’t share this fixed-supply characteristic.

Cryptocommodities no kryptonite for conventional commodity stores of wealth

On net, cryptocurrencies have superior physical attributes relative to other commodities for concealing and transporting large amounts of wealth, which could be valuable in dark markets and some areas that lack reliable banking systems. But a long list of hurdles remains for cryptocurrencies to reach the equivalence of precious metals in financial markets, and these will be difficult to overcome anytime soon. In the meantime, we believe gold still offers the best store of wealth given how institutionalized it has become over 3,000 years of active trading versus five years for bitcoin.

Jeff Currie, Head of Global Commodities Research

Email: jeffrey.currie@gs.com
Tel: 212-357-6801

Goldman Sachs and Co. LLC

Michael Hinds, Senior Commodities Strategist

Email: michael.hinds@gs.com
Tel: 917-343-3218

Goldman Sachs and Co. LLC

Huan Wei, Commodities Strategist

Email: huan.wei@gs.com
Tel: 212-357-2353

Goldman Sachs and Co. LLC

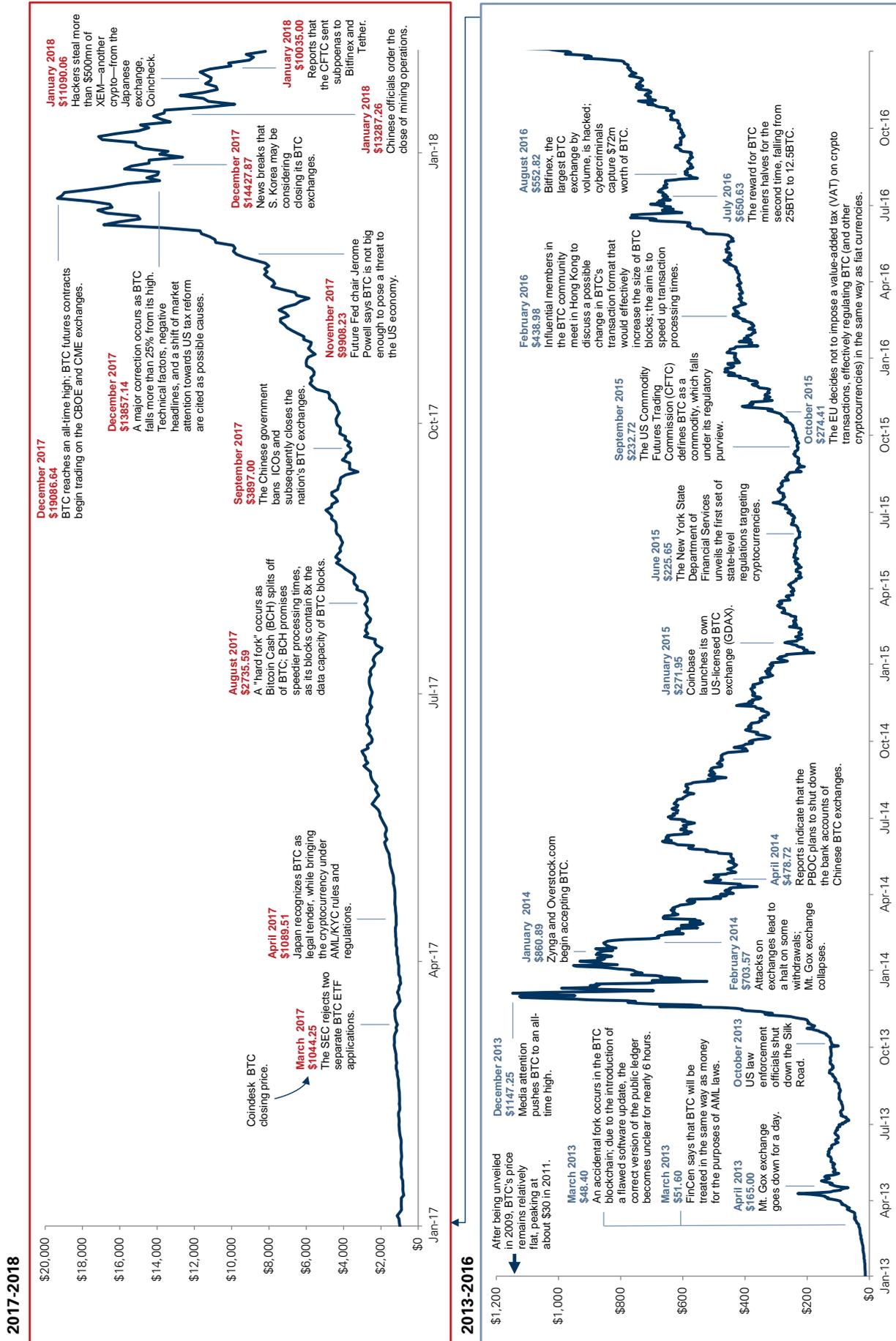
All figures as of January 25, 2018.

¹ For CME, the Maintenance Margin for the BTC future is 43%, where the Initial Margin for Hedger is 100% of the maintenance margin and the initial Margin for Speculator is 110% of that number. Additionally, FCMs may require a margin level beyond CME Clearing’s minimum requirement.

² In the spot market, there are over 20 exchanges intermediating BTC/USD. Premia as high as 40% have been observed on South Korean exchanges. The futures markets only use a subset of these exchanges (Gemini for CBOE futures, an average of Bitstamp, GDAX, iBit and Kraken for CME futures). Bitfinex, the largest exchange, is not included in either futures contract reference rate.

Tracking bitcoin's rise (and fall?)

For the exclusive use of ANTON_FILATOV@SBERBANK-CIB.RU



Sources: Coindesk, 99bitcoins, Goldman Sachs Global Investment Research, various news sources.

Irrational (digital) exuberance

Charlie Himmelberg and James Weldon argue that the recent boom in cryptocurrencies fits the classic definition of a bubble

In his book “Irrational Exuberance,” Robert Shiller offers a working definition of a bubble: “A situation in which news of price increases spurs investor enthusiasm which spreads by psychological contagion from person to person, in the process amplifying stories that might justify the price increase and bring in a larger and larger class of investors, who, despite doubts about the real value of the investment, are drawn to it partly through envy of others’ successes and partly through a gambler’s excitement.”

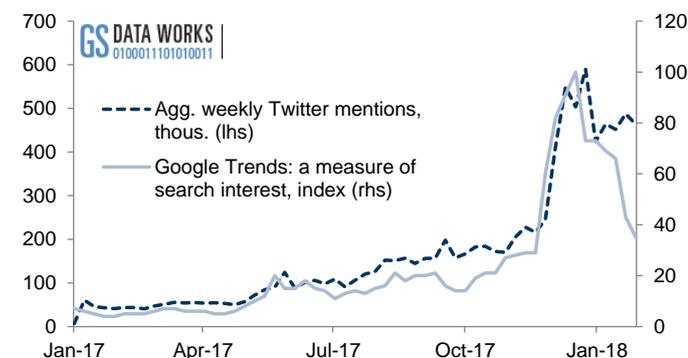
While there is no definitive taxonomy for bubbles, Shiller’s definition is probably as good as any. And if one is looking for recent examples of price action and investor behavior that fit this profile, it is hard to imagine a better match than bitcoin and the broader universe of “altcoins.” Price action that spurs investor enthusiasm? Check. Psychological contagion? Check. Doubts about fundamental value? Check. Envy of others’ successes and a gambler’s excitement? Check, check.

Crypto contagion

The elements of “social contagion” in the bitcoin boom are both intuitive and recognizable. As bitcoin prices rose by leaps and bounds last year, so did the likelihood that bitcoin investors wanted to tell their story. Their story is a good one, which prompted many listeners to get off the sidelines (as the economist and bubble historian Charles Kindleberger once quipped: “There is nothing as disturbing to one’s well-being and judgment as to see a friend get rich”). As the size of the “infected population” grew, so did the number of people who know somebody who knows somebody who made millions in bitcoin. The story naturally attracted media coverage, adding to the contagion with headlines like The New York Times’ “Everyone Is Getting Hilariously Rich and You’re Not.”

Symptoms of “social contagion”

Agg. weekly Twitter mentions (lhs) and Google search volume (rhs)



Based on search terms: bitcoin, BTC, coinbase, cryptocurrency, ethereum, ripple. Source: Google Trends, Crimson Hexagon, Goldman Sachs Global Investment Research; special thanks to Dan Duggan (GS Data Works) and Donnie Millar.

In addition to the exponential rise of prices and trading volumes, telltale signs of the social contagion were visible in last fall’s sharp increases in Google searches and Twitter mentions. They were also visible in stock prices that have doubled or tripled simply because companies have changed their name to include keywords like “blockchain” or “crypto.”

A similar lack of market scrutiny was visible during the 1990s tech bubble when the keyword du jour was “.com.”

Envisioning value vs. capturing it

Of course, the fact that crypto coins check the boxes on Shiller’s list does not invalidate the underlying technology. After all, internet commerce circa 1999 really was destined for greatness, as it turns out, even if most of the dotcom companies that populated the bubble are no longer around. Investor enthusiasm for new technologies sometimes fuels a bubble. This doesn’t mean the technologies can’t have value, but it does highlight what is often a very wide gap between the value of an idea and investors’ ability to capture that value.

Crypto enthusiasts differ on the source of value for crypto currencies. Some take the view that cryptocurrencies are literally that—currencies that will eventually take market share from established currencies like the US dollar or euro.

However, we are rather skeptical of this value proposition since two defining characteristics of successful currencies—stable value and ease of transactions—are features that for most cryptos have proven elusive, to put it gently (see also pgs. 12-13).

For this reason, we think it is probably more accurate (if still optimistic) to describe these crypto coins as crypto *assets*, that is, claims on the value of inputs to future payment systems which have yet to be developed, but which will eventually justify their scarcity value. In this respect, crypto coins may be analogous to land, and the recent mania for cryptos analogous to a land rush: The undeveloped land may not generate cash flows today, but investors can still speculate that future real estate developments will increase land values in the future.

Reasons for caution

The land metaphor requires two key conditions. First, like land, the supply of bitcoin must be effectively fixed (or the supply curve must at least be very steep). And second, again like land, there must be no close substitutes to bitcoin as an input to the future development of commercial applications (like decentralized payment systems). These conditions deepen our skepticism over the prospects for discovering fundamental value in crypto assets. While the first condition is arguably true—core functions in the bitcoin consensus algorithm are built to ensure this—it is hard for us to see what prevents new (and improved) “altcoins” from entering the market (at effectively zero cost) and thus increasing the supply of crypto “inputs” effectively without limit (indeed, the robust pace at which new “altcoins” are coming to market via ICOs already underscores this point). Nor is it clear what “barriers to entry” prevent incumbent firms (in, say, payment services) from developing and incorporating their own (low-cost) adaptations of blockchain technologies. The stock answer for seasoned tech analysts might be “network externalities,” but this presumes something that doesn’t yet exist—namely, a large base of existing users subject to significant switching costs.

Charlie Himmelberg, Co-Chief Markets Economist

Email: charles.himmelberg@gs.com
Tel: 917-343-3218

Goldman Sachs and Co. LLC

James Weldon, Global Markets Analyst

Email: james.weldon@gs.com
Tel: 212-357-6538

Goldman Sachs and Co. LLC

Interview with Dan Morehead

Dan Morehead is the founder and CEO of Pantera Capital, an investment firm that focuses exclusively on bitcoin, digital currencies, and companies utilizing blockchain technology. Prior to that, he was head of macro trading and CFO at Tiger Management and a CMO trader at Goldman Sachs. Below, he argues that potential returns on cryptocurrencies justify the risks, and that prices will be ultimately higher as existing markets are disrupted and institutional investors enter the space.

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



Allison Nathan: Bitcoin skeptics sometimes make the point that cryptocurrencies have no intrinsic value. What's your response?

Dan Morehead: There really isn't much intrinsic value in most stores of wealth or mediums of exchange, including the dollar. One could argue that the government has imparted

some value to the dollar by requiring that it be used to satisfy tax obligations. But if you actually tried accessing the true intrinsic value of US currency by, for example, melting pennies to capture the value of its mineralogical components, that's actually a felony. And there are enormously important stores of wealth with very little intrinsic value, such as Jackson Pollock paintings. The actual value of the paint and canvas in a Pollock painting is probably \$40. But they trade for \$100mn because people believe that in the future, they will sell for at least that or maybe much more. And that's the case with bitcoin; people can store their wealth in it with the expectation that it will be worth at least as much if not much more in the future. Citizens of countries with unreliable banking systems have been very quick to realize these benefits; some large importers of gold, like China and India, are now massive importers of bitcoin because of its superiority as a store of wealth.

Allison Nathan: But where do cryptocurrencies derive their value? Is the real value in the underlying blockchain technology?

Dan Morehead: Cryptocurrencies are the final piece of the protocol puzzle that is the internet. Our lives have been radically transformed by protocols like TCP/IP and SMTP that move all kinds of information around online. The one area where the internet has not had as big of an impact yet is in finance or money. That is where bitcoin and other current cryptocurrencies come in: they give people the ability to essentially email money. And with the invention of Ethereum, you can also use the blockchain's security and payments mechanisms for projects and contracts. The more people that want to use these features, the more value the networks—and the units that trade on them, like bitcoin—will have. To your second question—it's popular to say, "I love blockchain tech, but I hate bitcoin." I don't really know what that means. If you want to use blockchain technology to send \$300 from here to the Philippines, you have to buy bitcoins to use the blockchain.

Allison Nathan: What is the fair value of bitcoin?

Dan Morehead: It's difficult to put a precise number on it, but I believe it is much higher than today's price, with the risk-reward substantially skewed to the upside. If I had to take a

really big-picture view of the terminal value of bitcoin, I think it's roughly a half a million dollars per bitcoin. How do I calculate that? By taking into account some of the markets that bitcoin will disrupt. For example, bitcoin disintermediates the transfer of money across borders, so you could take the value of correspondent banking and the value of remittances. Bitcoin could also be a very strong competitor to the credit card companies, so you could take some fraction of their market capitalization. Bitcoin is, again, a very good store of wealth, so you could take some share of the roughly \$8tn market cap of gold and other stores of wealth. And lastly, bitcoin is similar to a currency, so it could take some market share from fiat currencies, which amount to around \$100tn of global money supply.

On top of those known use cases, there are others that we don't even know about yet. When you have a new technology like TCP/IP or bitcoin, you might not appreciate the incredible disruption that could follow. In the early '90s, I could understand selling books on the internet, but I had no idea that Uber or Snapchat would exist.

“ If I had to take a really big-picture view of the terminal value of bitcoin, I think it's roughly a half a million dollars per bitcoin. How do I calculate that? By taking into account some of the markets that bitcoin will disrupt.”

Allison Nathan: But even if you see a multitude of use cases, isn't the current blockchain technology falling short of its main objectives? For example, haven't transaction speeds slowed and fees risen substantially as volume on the bitcoin network has grown?

Dan Morehead: It's true that bitcoin has been so successful, and transactions are increasing so rapidly, that the blockchain is actually bumping up against a very artificial constraint. The creator of bitcoin set the maximum memory size for each block at one megabyte, the size of a 1980s floppy disk. This didn't matter for many years. Now that it does, it's created a governance crisis in bitcoin where some people want to stay true to the original one megabyte constraint, whereas almost all businesses would like to scale that up. Theoretically, it would be very easy to change; it would mean rewriting a few sentences of code. They just need to get past this governance issue. Either that will happen and bitcoin will return to being essentially free and real-time, or transactions will migrate to other blockchains, like Ripple, which have those characteristics.

Allison Nathan: Given the possibility of migration, and the likelihood that the technology and use cases evolve, isn't it possible that today's cryptocurrencies no longer exist 20 years from now?

Dan Morehead: My passionate belief is that most of the largest blockchains today will survive. That doesn't mean that 90% of the altcoins and ICOs being issued right now won't go to zero; I believe they will. But blockchains like bitcoin and Ethereum and Ripple will almost certainly still be very important in 10 or 20 years.

It's common for people to say that bitcoin is just the first instance of this and that bitcoin 2.0 is going to be even better. But it's really important to remind everyone that we've been trying to create cryptocurrencies for four or five decades. This is not a new idea. Satoshi Nakamoto got it right, and that's why it's so disruptive. In fact, some of the key competitors to bitcoin, like Bitcoin Cash and Litecoin, are essentially copies of bitcoin with different governance structures. So my belief is that either the bitcoin blockchain survives and wins, or a very similar blockchain will prevail.

I would add that many investors have spent way too much energy trying to figure out which one is the winner. But that's not the way you build a stock portfolio, right? You don't put 100% of your net worth in one stock. You buy 30 and some go up, some go down. That's the way I would suggest investors approach investing in cryptocurrency—by holding a diversified portfolio of coins.

“It's really important to remind everyone that we've been trying to create cryptocurrencies for four or five decades... Satoshi Nakamoto got it right, and that's why it's so disruptive.”

Allison Nathan: So it doesn't concern you that the vast majority of even a well-diversified cryptocurrency portfolio will likely go to zero?

Dan Morehead: I wouldn't think of it that way. I had a fun debate on CNN recently with Vivek Wadhwa of Carnegie Mellon University, who once wrote a paper titled, “RIP, Bitcoin. It's Time to Move On.” And he argued that bitcoin is the Pets.com of this era. But a portfolio of investments in early internet companies could have included much more than ventures like Pets.com; it could have included an Amazon.com. Even if 90% of cryptocurrencies are going to zero, I think you can craft a portfolio that will have some losing assets, but also a couple of truly transformative winners.

Allison Nathan: Even if all of that is the case over the long term, do you think it is reasonable to expect another major

correction in the cryptocurrency space? Many would argue it is a bubble that has started to burst.

Dan Morehead: I do not believe this is a bubble. Cryptocurrencies are clearly very volatile. And anything that can go up 10 times in six months can easily go down 50% in a week. So I have no idea where it's going to be in the short run. But it's very difficult for me to believe that we are in the midst of a bubble given that almost all institutional investors have zero exposure to it. That said, I do expect a substantial wave of institutional investor flows into the space over the next 18 months.

“Even if 90% of cryptocurrencies are going to zero, I think you can craft a portfolio that will have some losing assets, but also a couple of truly transformative winners.”

Allison Nathan: The absence of regulated custodians seems to be a substantial hurdle for institutional investors to get comfortable with the space. How have you dealt with this?

Dan Morehead: The fact of the matter is that there isn't yet an SEC-regulated custodian of crypto assets, which carries risk. But at the end of the day, we have gotten comfortable that the reward of being active in this space compensates for that risk. Some firms have announced an intention to offer custodial services, and I believe that more will do so over time. But there is a saying on Wall Street: buy the rumor and sell the fact. If you wait until there is an SEC-regulated custodian, the price may be an order of magnitude higher because investors will price that development in advance. We saw this with bitcoin futures; bitcoin prices increased substantially between the time the contracts were announced and their actual launch. I don't want to diminish the custodial risk, but at least for us, this has been a case of looking at risk versus reward.

Allison Nathan: So what does worry you about the future of cryptocurrencies?

Dan Morehead: I think the main risk is that regulatory bodies around the world issue rulings that are excessively harsh in their treatment of cryptocurrencies. This risk is particularly high for ICOs, which are very speculative—like early-stage venture capital—but are also a very important way to fund new projects. That said, overall, US regulatory bodies have been reasonable in allowing the cryptocurrency market to develop while coming down on bad actors like the Silk Road. And it has been a long time now since I've worried about the long-term future of blockchain. I think that has to do with the general population really embracing this new technology, learning how it works, and getting used to it. I have no doubt that blockchain will be important 20 years from now.

Bitcoin as money

Zach Pandl and Charlie Himmelberg argue that cryptocurrencies could potentially succeed in some corners of the globe—but face significant practical hurdles to wider adoption

To a modern US observer, cryptocurrencies can seem like a solution in search of a problem. Money derives its value from being useful in two ways—facilitating transactions and diversifying portfolios—and the US dollar serves both purposes relatively well. However, other types of money sometimes fall short of these criteria. This suggests that cryptocurrencies may be useful alternatives in some circumstances, although they face significant practical hurdles to wider adoption.

Dollar doing its job

In recent decades the US dollar has done its job relatively well. It has been a fairly stable store of value: Consumer price inflation has averaged 2.1% over the last 30 years, and the real trade-weighted exchange rate is about 3% above its average of the same period. It is true that the US financial system wobbled during the financial crisis, but the underlying problem was not the currency per se: The dollar actually appreciated 16% between June 2008 and March 2009. The dollar's reliability has made it useful around the world: It accounts for about 65% of global foreign exchange reserves and is the denominate currency in global trade, with about 30% of global trade flows excluding the US invoiced in USD. In other words, transaction and portfolio demand for the dollar are very high.

When money malfunctions

The same cannot be said for many other types of money. In certain parts of the world, and at points throughout history, multiple currencies have circulated in the same economic area—a phenomenon known today as “dollarization.” Many countries with a history of currency instability and/or underdeveloped financial markets use the US dollar for the traditional functions of money—as a medium of exchange, unit of account, and store of value. In sub-Saharan Africa, for example, many currencies have been debased by high inflation and the mismanagement of money supply. As a result, dollarization is widespread: foreign currencies account for more than 90% of deposits and loans in the DR Congo, and Zimbabwe demonetized its own currency in 2015 (a variety of foreign currencies now circulate). The US dollar is the official currency of Ecuador and a variety of smaller nations, where no separate legal tender circulates. The Peruvian economy remains significantly dollarized today despite stable inflation over the last decade—a legacy of its experience with hyperinflation in the late 1980s. In these circumstances, it is natural to see how alternative—possibly digital—anchor currencies could be useful as well.

Moreover, governments often restrict the use of domestic and foreign currencies within their borders. For example, countries can limit the amount of foreign exchange that can be held in bank deposits (e.g., Mexico) or by certain types of investors (e.g., pension funds in Poland). They can also tax foreign exchange transactions or maintain multiple official exchange rates, and capital controls may limit the degree to which

residents can convert domestic money into foreign exchange. Prominent recent examples include: (i) the prohibition on purchases of foreign assets by Greek banks, (ii) limits on currency conversion in Cyprus, and (iii) the use of various quotas for overseas investment by China. In these circumstances, it is natural to see how alternative—possibly digital—forms of money could be useful.

What drives money demand?

Demand for money comes from two sources: *transaction demand* and *portfolio demand*.

Transaction (or liquidity) demand for money boils down to the fact that we cannot easily exchange (non-monetary) financial assets (“assets”) for goods and services, so we tend to hold some amount of monetary assets (“money”) to facilitate consumption. Transaction demand for money declines with expected returns on assets (the opportunity cost of holding money), increases with transaction costs (like brokerage fees), and increases with income (because more transactions require more money).

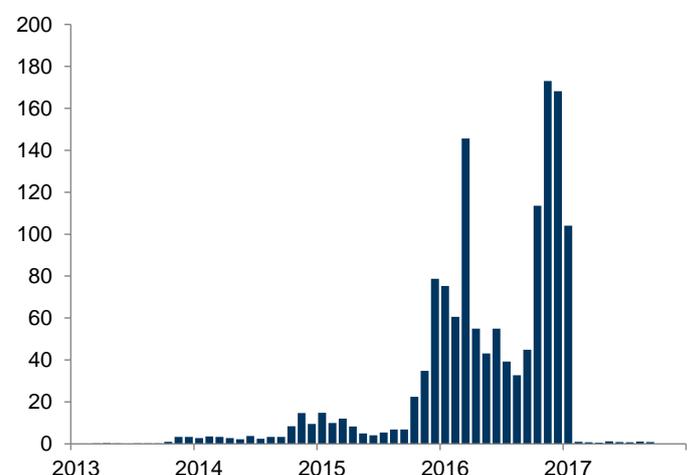
Portfolio demand for money also declines with expected returns on assets, and one could argue this is why some precious metals (such as gold) are more like money than other assets. Portfolio demand for money also increases with uncertainty about asset returns and increases with wealth (because more wealth means larger money balances).

Digging into demand

Indeed, we find some evidence that the demand for cryptocurrencies has come from regions with currency instability and/or capital controls. For instance, a Google Trends search shows that the highest search intensity for “bitcoin” over the last five years (scaled to overall search volumes in the country) came from Nigeria, South Africa and Ghana, all countries with currency instability and/or restrictions on the use of foreign exchange. In addition, bitcoin exchange volumes in China rose sharply following the tightening of capital controls in 2016. They subsequently collapsed when cryptocurrencies were more stringently regulated last year.

Evading capital controls?

CNY bitcoin exchange monthly volume, BTC mn

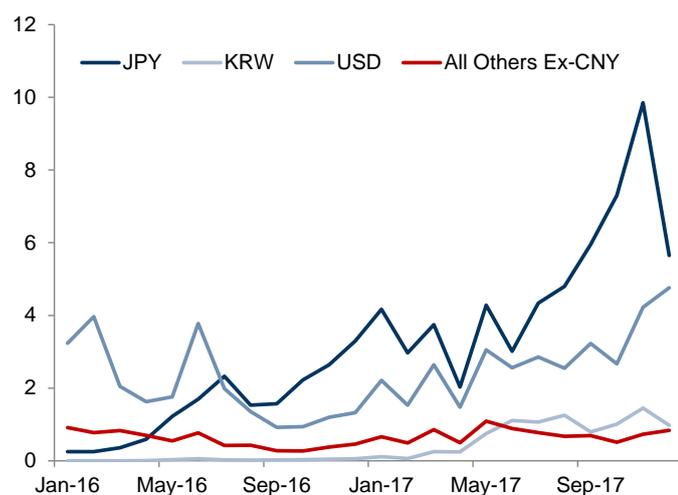


Source: Bitcoinity.org, CryptoCompare.com, Goldman Sachs Global Investment Research.

But other data look more consistent with a classic speculative bubble. First, bitcoin exchange volumes are now dominated by investors in Korea and Japan—countries with no recent history of monetary instability and/or unmet portfolio diversification needs. Second, cryptocurrency prices are correlated with Google search volumes. This may point to significant retail investor participation in these markets. Third, until the launch of bitcoin futures, it was generally not possible to short the market—a common feature of speculative bubbles.

More than just EM demand

Bitcoin exchange monthly volume, BTC mn



Source: Bitcoin.org, CryptoCompare.com, Goldman Sachs Global Investment Research.

A high bar for wider adoption

In practice, bitcoin and other digital currencies face significant practical hurdles to their adoption as outside forms of money. First, many purported benefits of cryptocurrencies come with significant drawbacks. For example, the fact that cryptocurrencies function without central banks may make them valuable as inflation hedges or stores of value, but it also makes them vulnerable to price volatility, since their supply cannot respond to fluctuations in demand. Such volatility makes them poorly suited as a substitute for money generally—which is why most nations eventually abandoned the gold standard in favor of fiat currencies. Volatility would likely need to decline dramatically (either naturally or through the widespread adoption of cryptocurrencies designed to better stabilize purchasing power via supply adjustments) before we see broader adoption.

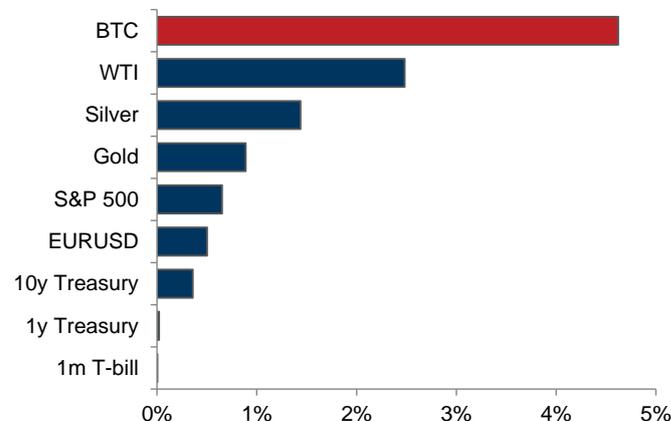
Second, some features of cryptocurrencies that might make them competitive with other forms of money appear unlikely to persist. For instance, once-low transaction costs on the bitcoin network—considered an important advantage over conventional forms of payment—have increased as transaction volume has grown. Similarly, the fact that many cryptocurrencies provide a useful medium of exchange for criminal activities is likely to eventually attract greater regulation and law enforcement by government.

Third, for any given cryptocurrency to succeed, it may need to reach a “critical mass” of acceptance—much in the way that a fiat currency like the US dollar derives some additional value from being widely accepted. This may be challenging given the large number of cryptocurrencies available today (around 1500).

And finally, while the recent returns from bitcoin and many cryptocurrencies have far surpassed that of conventional money, they are unlikely to last. Our working assumption is that long-run cryptocurrency returns should be equal to (or slightly below) growth in global real output—a number in the low single digits. Thus, digital currencies should be thought of as low/zero return or hedge-like assets, akin to gold or certain other metals. This could still mean that prices increase at a faster rate as the technology is adopted—an analogy might be the value of a biotech company that invents a drug, which eventually becomes a generic—but there is an inherent contradiction between cryptocurrencies as high-return assets on the one hand, and stores of value relative to goods and services on the other.

Not a stable store of value

Daily volatility, %



Source: Bloomberg, Goldman Sachs Global Investment Research.

Could bitcoin succeed as a form of money?

In theory, yes, if it proves to be more useful than the alternatives—in terms of facilitating transactions at a lower cost and/or providing better risk-adjusted returns for portfolios. After all, while cryptocurrencies may employ innovative technologies, there is nothing particularly unusual about new types of money (consider, for example, the introduction of the euro in 1999).

In practice, however, the gains from adopting cryptocurrencies look small, at least in developed market economies. Transaction costs there are already relatively low, exchange rates and price inflation are broadly stable, precious metals can be used for portfolio diversification, and governments place few restrictions on holding foreign currency or foreign assets. That said, the widespread use of the dollar outside the US—and full dollarization in some countries—suggests there is already demand for an internationally accepted medium of exchange and store of value. In those countries and corners of the financial system where the traditional services of money are inadequately supplied, bitcoin (and cryptocurrencies more generally) may offer viable alternatives.

Zach Pandl, Co-Head of Global FX and EM Strategy

Email: zach.pandl@gs.com
Tel: 212-902-5699

Goldman Sachs and Co. LLC

Charlie Himmelberg, Co-Chief Markets Economist

Email: charles.himmelberg@gs.com
Tel: 917-343-3218

Goldman Sachs and Co. LLC

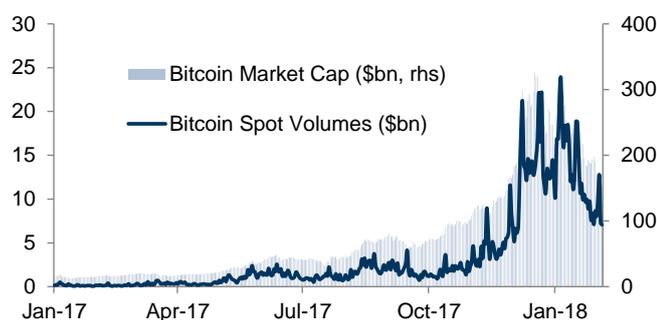
BTC for institutions: more hurdles to clear

Alex Blostein and Sheriq Sumar discuss the barriers to institutional investment in crypto

Trading volumes in bitcoin spot markets have risen rapidly. In 4Q17 alone, global volume in bitcoin spot markets reached \$6.5bn in daily average notional—up 7x vs. 1Q-3Q17. This trading momentum has carried forward into 2018, with \$12.5bn in daily average notional year-to-date. That said, institutional activity in bitcoin and other cryptocurrency markets remains nascent, with several material market structure barriers to wider adoption for both the end users and market makers.

Surge in spot

Bitcoin global spot trading volumes, \$bn; bitcoin market cap, \$bn (rhs)



Source: CoinMarketCap.com.

The three Cs

Counterparty, custody, and connectivity risks are among the most commonly cited challenges in institutional bitcoin trading. Specifically, today's cryptocurrency market structure is very fragmented, with customers taking counterparty risk against the trading venue (e.g., Coinbase, Gemini). This arrangement is unlikely to satisfy the risk parameters of most large institutions. While some of these platforms offer custody services, we believe institutional investors that are governed by the 1940 Investment Company Act would need the involvement of a more established provider to ensure safekeeping of assets. Some established market participants are contemplating entering the crypto custody space—State Street has recently discussed this in the press—but these initiatives will likely take time to gain traction.

Lastly, operational connectivity issues and a lack of interoperability between trading venues pose challenges for market makers, as these characteristics inherently could create more volatility and limit liquidity.

Looking for more than a good wrapper

Despite these challenges, increased institutional interest in cryptocurrencies has spurred efforts to establish new vehicles to facilitate crypto investment. Both the CME and the CBOE launched bitcoin futures in December 2017. Unlike spot markets, bitcoin futures provide exposure to bitcoin through a well-established product wrapper that trades on a regulated exchange (under CFTC jurisdiction) and is centrally cleared (at either the CME for CME futures or at the Options Clearing Corporation for CBOE futures), eliminating counterparty risk. However, given the volatility of the underlying, margin requirements are substantially higher than in more established products. In our view, a futures market alone is unlikely to materially rein in this volatility, which will likely require the establishment of more credible institutional trading backstop—a process that will take time.

On the back of the futures launch, several ETF providers including ProShares, First Trust, REX, Direxion, and GraniteShares, among others, filed to launch ETF products that would invest in futures and give investors access to the product in a "cash equity wrapper." However, regulatory approval remains a challenge, driving many ETF providers to withdraw their application either voluntarily or by the SEC's order. The SEC has highlighted several concerns that need to be addressed before the launch of any funds: valuations, liquidity in underlying cryptocurrency, custody requirements for a fund, arbitrage mechanisms in the cryptocurrency market, and potential risks from fraud and manipulation. Put differently, new product wrappers (so far) fall short of addressing the key challenges for institutional investment in cryptocurrencies.

Alexander Blostein, CFA, Senior Capital Markets Analyst

Email: alexander.blostein@gs.com
Tel: 212-357-9976

Goldman Sachs and Co. LLC

Sheriq Sumar, CFA, Capital Markets Analyst

Email: sheriq.sumar@gs.com
Tel: 212-902-3299

Goldman Sachs and Co. LLC

Contracts comparison

Details of CME and CBOE bitcoin futures contracts

	CME	CBOE
Launch Date	18-Dec-17	10-Dec-17
Product Code	BTC	XBT
Contract Unit	5 BTC	1 BTC
Underlying	CME CF Bitcoin Reference Rate (BRR), which aggregates trading activity across major BTC spot exchanges	Gemini auction price for bitcoin
Avg. Daily Volume	1,350 contracts (in notional terms: \$85mn)	6,100 contracts (in notional terms: \$77mn)
Price Limits	Special price fluctuation limits of 7%, 13%, and 20% above or below the previous settlement price. Trading not permitted outside the 20% band.	Not subject to price limits. If the best bid/offer in the contract closest to expiration is 10/20% or more above the daily settlement price of that contract on the prior business day, trading is halted for 2/5 minutes.
Margin Requirements	Maintenance margin: 43%; initial margin for hedger: 100% of the maintenance margin (43%); initial margin for speculator: 110% of maintenance margin (47%)	Maintenance margin: 40%; initial margin for hedger: 40%; initial margin for speculator: 44%
Settlement	Cash-settled	Cash-settled

All figures as of February 5, 2018.

Source: CME, CBOE.

Bitcoin basics

1. What is bitcoin? Bitcoin is a cryptocurrency—a digital unit of exchange operating on a decentralized, peer-to-peer network—that was launched in 2009 by a computer programmer using the pseudonym Satoshi Nakamoto. Participants on the network transmit data that allow the proof and transfer of ownership without the need for a trusted third party. Instead of owning coins, bitcoin users possess two unique strings of characters or “keys”: a public key, much like a bank account number for sending/receiving bitcoins, and a private key, comparable to a PIN that allows the owner to spend his/her coins.

2. How does it work? Every bitcoin transaction gets recorded in a string of data containing details including the keys of the sender/receiver and the value being transferred. These details get transmitted on the network for inclusion in a public ledger known as the blockchain. Network participants called “miners” then use computing power and cryptography to repackage data from verified transactions into a “block” of fixed size that is uniquely identifiable to everyone else on the network and linked to the prior block in the chain. The first miner to complete this process generates new bitcoins as a reward (they may also earn fees). Once transactions become part of the ledger, it is very difficult for them to be modified or reversed. For more, see pgs. 20-21.

3. What are the main arguments in favor of and against bitcoin? For bitcoin proponents, the cryptocurrency’s appeal lies primarily in its decentralization (i.e., the fact that no central bank, government, or other single authority controls it) and in its privacy. Proponents tout the blockchain’s power to eliminate middlemen, reduce transaction costs, and potentially find important applications in other areas (see pgs. 18-19).

Bitcoin skeptics argue that the technology facilitates illicit activity, and that bringing bitcoin in line with the legal, regulatory, and consumer protection standards used for other payment methods could increase transaction costs. They contend that the power to control supply and influence market structure has simply shifted from traditional institutions—such as central banks—to technologists. Skeptics also point out that bitcoin transaction costs have already risen as the network has grown (users now often pay higher fees to prioritize their transactions). For more views on bitcoin, see pgs. 4-5 and 10-11, as well as [Top of Mind Issue #21](#).

4. Is bitcoin anonymous? Bitcoin is frequently associated with privacy, given that transactions take place without the involvement of a third party such as a bank. However, the technology is pseudonymous rather than anonymous. In a bitcoin transaction, a public “address” associated with one’s public key is visible to other network participants. While the ownership of the address is unknown, it is potentially traceable. That said, network participants may take steps to protect their identity.

5. How secure is bitcoin? Unlike other payment methods such as credit cards, which require the purchaser to provide the merchant details that can then be used to make subsequent purchases, the information that enables bitcoin owners to spend their coins—the private key—is never revealed when making a transaction. To ensure the security of one’s bitcoin holdings, private keys must remain safe. But these keys are vulnerable to loss and theft. Bitcoin exchanges and digital wallet apps, which store keys, have been subject to security breaches, and hackers have employed various forms of malware to obtain keys from individual computers. Since bitcoin transactions are irreversible, recovering stolen coins is very difficult. Private keys can be stored offline either physically (e.g., printed and locked in a safe) or digitally (e.g., encrypted and saved on a USB drive). The costs and effectiveness of these storage solutions vary. And if the “hard” copy of a private key is damaged or lost, the coins are lost forever.

6. How susceptible is bitcoin to fraud? Bitcoin transactions are extremely difficult to counterfeit. Only a miner with control over the majority of the network’s computing power—51% or more—would be able to manipulate the blockchain. Such a “51% attack” could allow the miner to prevent transactions from being validated and/or enable coins to be spent more than once. However, the computing power required to gain control of the network is immense and growing every day. Experts also note that a 51% attack would almost surely lead to a drop in the value of bitcoin, which would not be in the miner’s interest.

7. How is bitcoin regulated?¹ In the US, bitcoin falls under the jurisdiction of different regulatory bodies depending on its use. In the context of money transmission, the Financial Crimes Enforcement Network (FinCEN), a branch of the US Treasury, considers bitcoin a “convertible virtual currency” subject to money transmission regulation. US businesses involved with the sale of bitcoin must register with FinCEN and comply with federal anti-money-laundering laws. US states are also beginning to clarify how cryptocurrencies fit under existing state money transmission statutes.

In the context of investing, the Commodity Futures Trading Commission (CFTC) has ruled that bitcoin is a commodity. While the CFTC generally does not regulate spot transactions (i.e., the majority of bitcoin transactions), it does regulate bitcoin futures. The CFTC could also be responsible for addressing trading irregularities as it typically functions as the financial regulator of last resort.

The Securities and Exchange Commission (SEC) does not consider bitcoin a security, but has expressly stated that any digital asset with the characteristics and applications of a security could fall under its jurisdiction. This could include tokens issued through initial coin offerings (ICOs)—a method for companies/projects to raise funds by selling digital tokens that are used to power their blockchain applications. Where the ICO occurs before the application is available, there is a strong likelihood that it will be viewed as a security offering. And, increasingly, non-blockchain companies are offering ICOs of tokens that offer a revenue share or are otherwise explicitly intended to be securities. Those offerings are subject to securities regulation.

8. How is bitcoin treated by the IRS?² For tax purposes, the IRS treats cryptocurrencies as property, meaning those purchasing bitcoin as an investment are subject to capital gains and losses. While some observers have argued that crypto-to-crypto trades are a “like-kind exchange” (meaning that gains are tax-deferred), recently passed tax legislation has directed the IRS to narrow such rules to functionally exclude cryptocurrencies.

^{1,2} Source: Jacob Farber, Partner and General Counsel at Alchemist, and former Senior Counsel at Perkins Coie, LLP as part of its blockchain and digital currency group. Other sources: Internal Revenue Service, Goldman Sachs Global Investment Research.

Beyond BTC: a taxonomy of other cryptos

Nearly 1500 cryptocurrencies other than bitcoin account for roughly two-thirds of the \$360bn of total crypto market capitalization. Many of them attempt to improve on bitcoin by enhancing its properties as a store of value or medium of exchange. Others are designed to support software platforms that exploit blockchain's distributed data and security features. We believe the relative utility of cryptocurrencies will determine their success: only those that deliver incremental functionality relative to incumbents are likely to survive. As the technology evolves from its nascent stages, we expect new cryptocurrencies to emerge which build on the market's experience, while many of today's cryptocurrencies may ease to exist. Below, we identify three main use categories of cryptocurrencies: store of value/speculative coins, currency/transactional coins, and application/utility tokens. While the number of coins necessary for storing value, speculation, and currency uses is likely to be limited, we believe application/utility tokens have potential to co-exist in greater numbers.

Store of value / speculative asset coins

A number of coins seek to improve upon the technical properties that made bitcoin appealing as a store of value and a speculative asset while addressing bitcoin's perceived shortcomings. Specifically, bitcoin does not require an intermediary to execute transactions, making it difficult for governments to enforce capital controls. And, in the absence of a code fork (a change in the blockchain's software code), bitcoin's supply is fixed, which shields it from inflation. However, bitcoin mining requires large amounts of computing power and energy. In addition, the anonymity valued by some bitcoin users has been undermined by new ways of tracking transactions. Bitcoin Gold (BTG) attempts to replicate bitcoin while avoiding concentration of mining capacity by changing the algorithm miners use to build the transaction ledger. Other coins—including Monero (XMR) and ZCash (ZEC) — enhance the anonymity of asset transfers. *There is likely to be a limited number of coins that demonstrate sufficient advantages over alternatives to become common stores of value.*

Currency / transactional coins

In the world of payments, international transactions with fiat currencies have been an historical pain point. Sending remittances with networks like SWIFT can take days, sometimes without confirmation of funds received. And multinational corporate operations often require pools of local reserves in illiquid currencies, resulting in working capital inefficiencies. However, bitcoin has proven to be a poor medium of exchange as transaction times and costs have risen dramatically in real terms. As a result, a set of cryptocurrencies has emerged to optimize blockchain for transaction processing. For example, Ripple (XRP) is designed for FX applications, cannot be mined, and is subject to centralized controls, which some institutional users find appealing. Bitcoin Cash (BCH) adapts the core bitcoin code, using larger blocks to enable faster transaction times. *However, the need for a currency to achieve broad acceptance suggests that only a small number of coins could become attractive media of exchange.*

Application / utility tokens

Many tokens have been developed for non-monetary applications. For example, [Ethereum](#) is a platform that allows for the creation of "smart contracts" whereby an algorithm executes actions based on steps taken by third parties or inputs from external data sources. Using these features, Ethereum enables developers to program code that can be turned into distributed applications used for file storage, social messaging, and trading. Distributed applications run on Ether (ETH), the unit of value on the network. Developers typically pre-fund their idea by issuing special-purpose tokens through an Initial Coin Offering (ICO), creating a "white paper" outlining the application's intended function and market. For example, Filecoin is designed to be a distributed file storage service similar to Dropbox, but without dependence on a single service provider. EOS is working on a tool for developers to optimize applications given resource constraints imposed by the ecosystem. *Many tokens can likely co-exist, but each application will need to prove its worth by establishing a user base that sees value in a distributed application that is functionally superior to its centralized equivalent—because users place a premium on censorship resistance, anonymity, or another feature of that token.*

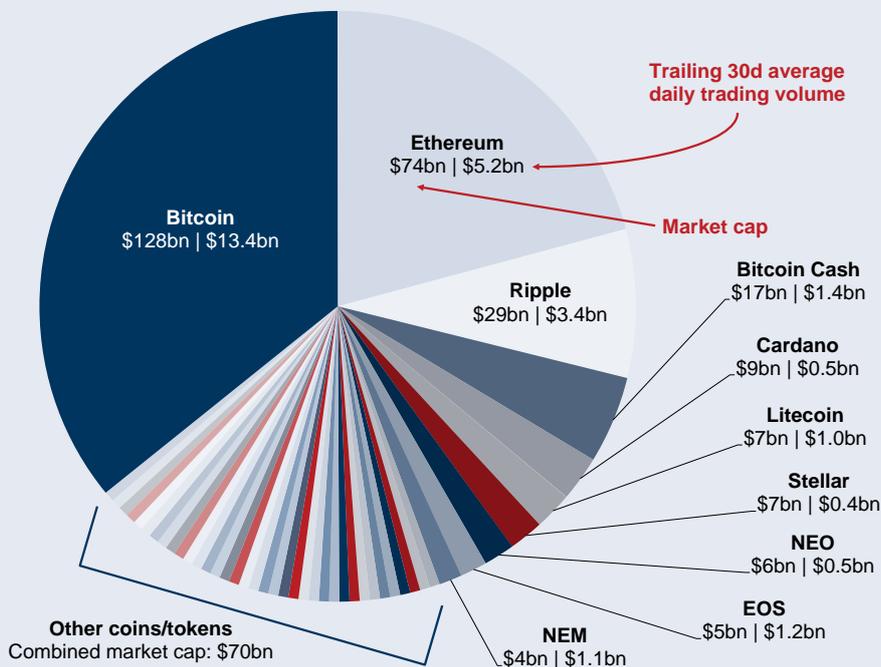
James Schneider, PhD, Payments and IT Services Analyst

Email: james.schneider@gs.com
Tel: 917-343-3149

Goldman Sachs and Co. LLC

BTC, ETH, and XRP: the lion's share of the crypto market

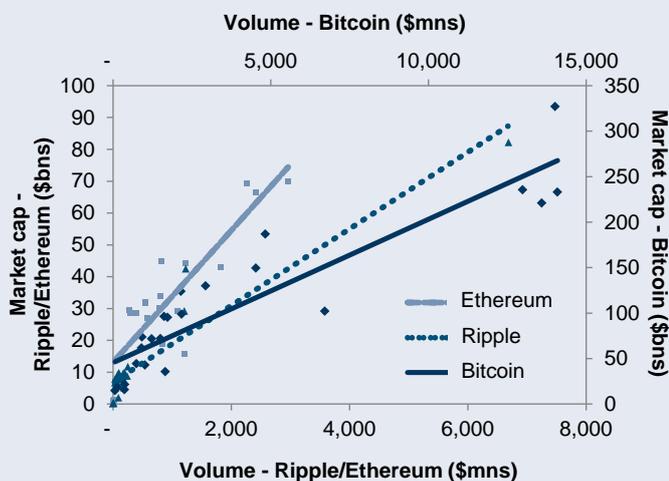
Market cap and trailing 30-day average daily trading volume as of Feb. 5, 2018, \$bn



Source: CoinMarketCap.com; Goldman Sachs Global Investment Research.

A key relationship

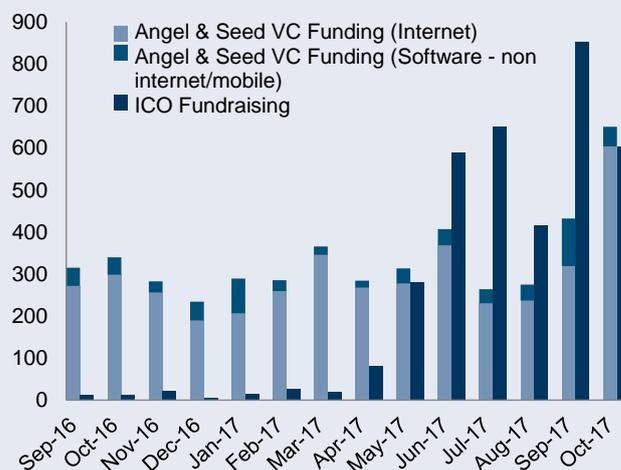
Crypto market cap (y axis, \$bn) and volume (x axis, \$mns)



Source: CoinMarketCap.com; Goldman Sachs Global Investment Research.

ICOs outpacing venture capital

ICO fundraising and VC investment, \$mn



Note: Angel and seed funding excludes crowdfunding.
Source: CoinSchedule, CB Insights, Goldman Sachs Global Investment Research.

For the exclusive use of ANTON_FILATOV@SBERBANK-CIB.RU

Could blockchain be transformative? Yes.

Blockchain technology has the potential to have a transformative impact across industries—by creating new markets, redistributing others with “creative destruction,” and making existing markets more efficient.

Why is blockchain transformative?

In its purest form, blockchain is a shared digital ledger of transactions recorded and verified across a network of participants in a tamper-proof chain that is visible to all. Permissioned or private variations add a layer of privileging to determine who can participate in the chain. This represents a break from the centralized data repositories that organizations historically used to support transaction processing and computation. Control of the database rested with its owner, who managed access and updates, limiting transparency and scalability. A distributed database—one that is maintained and synchronized across organizations—was technologically impossible. But advances in software, communications, and encryption now allow for such a system.

What is blockchain good for?

Blockchain’s transparency, security, and efficiency make it a good choice for reshaping businesses that are bogged down by inefficiencies, and for enabling new business models based on distributed marketplaces and technology:

- Facilitating secure, de-centralized transactions among many parties: Blockchain is particularly effective at handling distributed transactions among a very large number of parties—and delivers a high level of security for each transaction.
- Reducing fraud and increasing trust with increased security: In many parts of the world, corruption can lead to counterfeiting or alteration of official records. With blockchain, each transaction is uniquely encoded via cryptography and validated by other parties on the blockchain—so any attempt to alter or remove transaction information would be detected by others and corrected by other nodes (see also pgs. 20-21).
- Increasing transparency and efficiency in multi-party transactions: In any transaction involving two or more parties, the same transaction is typically entered separately by each party into that organization’s own independent systems. By using blockchain, organizations can streamline the clearing and settlement process, shorten settlement windows, and avoid substantial capital and operating expenses.

Which industries could see the biggest benefits?

While potential applications abound, some particularly promising areas where blockchain could be transformative include:

- Building trust between counterparties in the “Sharing Economy”: Peer-to-peer (P2P) lodging sites like Airbnb have already begun to transform the lodging industry by making a public market in private housing. However, concerns about safety (guests) and property damage (hosts) remain. By enabling a secure, tamper-proof system for managing digital credentials and reputation, blockchain could help accelerate the adoption of P2P lodging and generate incremental revenue opportunities.
- Transforming the US electricity industry by enabling distributed markets: Today, consumers rely on power generated centrally by utilities. With the advent of rooftop solar and high-capacity battery technology, individuals can potentially act as distributed power providers. Blockchain could be used to facilitate secure transactions of power between individuals on a distributed network who do not have an existing relationship.
- Streamlining clearing and settlement of securities: Despite the relatively low transaction costs for securities such as equities, up to 10% of trades are subject to errors, leading to manual intervention. By applying blockchain to the clearing and settlement of cash securities—equities, FX, commodities, OTC derivatives, repo—the industry could drive tens of billions in global cost savings by moving to a shorter settlement window.

When will blockchain really start to matter?

Early-stage technical prototypes have already emerged, and limited market adoption is likely in the next one to three years, with broader acceptance in the next five to 10 years. Specifically, consumer-focused “Sharing Economy” and social media companies could begin to implement blockchain-based identity and reputation management systems in relatively short order. In capital markets, a series of early prototypes should materialize over the next two years with limited numbers of participants. Broader market acceptance, however, is likely to take as much as 10 years given the regulatory oversight required and large number of market participants in large-scale markets such as cash equities in the US.

For more, see [Profiles in Innovation: Blockchain: Putting Theory into Practice](#), 24 May 2016.

James Schneider, PhD, Payments and IT Services Analyst

Email: james.schneider@gs.com
Tel: 917-343-3149

Goldman Sachs and Co. LLC

Five blockchain use cases

The Sharing Economy: Lodging

 **\$3-9bn** increase in US booking fees through 2020

What blockchain can do

Ease identity and reputation management. Blockchain can securely store and integrate users' online transaction and review history with identification and payment credentials—making it easier to establish trust between parties. This information can be used to streamline transactions and enhance review quality.

Select enablers

Airbnb, HomeAway, FlipKey, OneFineStay

Incumbents at risk

Hotel industry

Smart Grid

 **\$2.5-7bn** new US market for distributed power

What blockchain can do

Enable transactions in a decentralized power market. Blockchain can connect local power generators (think: neighbors with solar panels) to consumers in their area, enabling distributed, real-time power markets. A blockchain-enabled market could also increase grid security and spur adoption of smart grid technologies.

Select enablers

TransActive Grid; Grid Singularity

Incumbents at risk

Utility companies

Real estate title insurance

 **\$2-4bn** annual US cost savings

What blockchain can do

Improve efficiency and reduce risk. By recording property records in a blockchain, title insurers would have easier access to the information they need to clear a title. The fact that the ledger is tamper-proof could help lower real estate fraud in emerging markets.

Select enablers

Ubiquity, BitFury, Factom / Epigraph

Incumbents at risk

Title insurers

Cash securities (equities, repo, leveraged loans)

 **\$11-12bn** annual global cost savings

What blockchain can do

Cut settlement times and reconciliation costs. Using a blockchain-based system can significantly shorten trade settlement time, in some cases from days to just hours. It also helps lower capital requirements, OpEx and custody fees in the process. Additional savings could also be achieved if blockchain is applied in other capital markets such as FX, OTC derivatives and commodities.

Select enablers

ConsenSys, Digital Asset Holdings, R3CEV, Chain.com, Australian Securities Exchange, itBit, Axoni, Ripple

Incumbents at risk

Custody banks and clearing houses

Anti-money laundering compliance

 **\$3-5bn** annual global cost savings

What blockchain can do

Increase transparency and efficiency. Storing account and payment information with blockchain could improve data quality and reduce the number of falsely identified "suspicious" transactions.

Select enablers

SWIFT and others

Incumbents at risk

Specialty compliance software vendors

Source: *Profiles in Innovation: Blockchain: Putting Theory into Practice*, 24 May 2016.

Bitcoin: beyond the basics

Step 1: Joining the Network and Buying Bitcoin

- Bitcoin is a peer-to-peer payment system used to transfer value between digital **wallets**. Establishing a wallet to transact in bitcoin is analogous to signing up for e-mail before being able to send and receive messages.
- Wallets are composed of two major parts: **public keys** and a **private keys**. The public key is an account number, much like an e-mail address. Most bitcoin users will not actually share their public key. Instead, they will use a shortened version, called an **address**. This provides users an extra layer of security and privacy. The private key is like a password, allowing users to unlock certain funds.
- A wallet does not contain physical coins. Instead, it derives a user's total available balance from a record of transactions involving the associated public key(s). Think of the wallet as containing multiple gift cards loaded with funds from prior transactions; the values will add up to the owner's total balance.
- Wallets connected to the internet are called **hot wallets**. They offer users immediate access to funds but are prone to theft (if hackers can obtain the user's private key). However, private keys can also be kept offline in **cold storage** (e.g., saved on external hard drives or even hand-written). Cold storage is considered safer but less convenient. Many users store the bulk of their coins in cold storage and transfer small amounts to their hot wallets for regular use.
- Bitcoin can be obtained on an exchange or, less commonly, directly from other participants on the network. Most buyers on an exchange will face a prevailing market exchange rate plus a spread. Oftentimes, there is also a fee associated with a bitcoin purchase (e.g., 1.5%). Most customers will be required to provide detailed proof of identity per "know your customer" (KYC) and anti-money laundering (AML) requirements.

What do public and private keys actually look like?

Cryptographic keys—which underpin BTC wallets—are simply strings of numbers and letters.*



Public key: Account number, much like an e-mail address.

0450863aD64A87ae8A2fE83c1aF1a8403cB53f53e486D8511
DaD8A04887e5B23522cD470243453a299fa9E77237716103A
bc11A1dF38855eD6F2eE187E9c581bA6



Address: Shortened version of the public key, typically for single use and unique to each transaction.

1FfGkGsfN3DoDzwJTDmi zXVVBQKbVSwuo



Private key: Password granting access to a certain amount of a wallet's funds.

Kx3uWwctbQRj3dDhMynqamfLAPv6w1X7JUY7cgN1YQgi jhRY7PQe

What does a typical wallet look like?

Wallets contain digital records of past transactions, which are used to calculate a total balance.

Example: Web/Mobile Wallet	
.00643991BTC \$150	
Send BTC	Request BTC
Transaction History	
Received Bitcoin (1/3/2018)	0.003219955BTC (+\$50)
Sent Bitcoin (1/2/2018)	-0.00643991BTC (-\$100)
Bought Bitcoin (1/1/2018)	0.01287982BTC (+\$200)

Step 2: Transacting in Bitcoin

- Bitcoin can be transferred between wallets in exchange for local currency or goods/services. Transactions are announced to the bitcoin network in a string of data that includes the address of the recipient. The transaction is also "signed" with the sender's private key. As part of the **digital signature**, the private key is transformed in such a way as to remain secret.
- The bitcoin network's public ledger, the **blockchain**, records only bitcoin transactions, not user balances. Therefore, when transacting in bitcoin, the **input** (i.e., the amount sent) must correspond to a past transaction rather than the actual value being transferred (i.e., the **output**). If the amount sent is greater than the intended value of the transaction, the software will generate change back to the sender.
- For example, assume User A has a total balance of 5BTC received through two previous transactions of 3BTC and 2BTC. User A wants to send 1BTC to User B. To do so, User A must send 2BTC to User B and send the balance back to him/herself, officially recording the "change" of the transaction. User A may also pay a transaction fee, reducing his/her change to less than 1BTC. Such fees are typically based on digital size (bytes) rather than dollar value. Fees are intended to incentivize faster transaction processing by miners (see Steps 3 and 4).
- The transaction does not process immediately; instead, it enters a pool of pending transactions. Once the transaction is verified, it is added to the blockchain and the parties' wallet balances are updated accordingly.

How are bitcoin transactions actually recorded?

Example: User A Sends 1BTC to User B

Sender	Address	Input (BTC)
User A	14Q7x8pWz	2.0
Receiver	Address	Output (BTC)
User B	12rgbuMEv	1.0
User A	1EmDcxbnu	0.9
Receiver	Address	Fee (BTC)
Miner	-	0.1

Value sent must have been received in a past transaction—think of it like using a gift card with 2BTC.

The transaction's "change" goes back to User A; the address is different, but the funds will likely return to the same wallet.

A fee is directed to miners. The specific address will be determined later.

Transaction data is packaged and transformed mathematically to create a transaction ID. Users can search for this number online to view the transaction's status.

Example ID: 0818d8a2f694077370cedf571c246d9cb3c4bd490bec66960df684fae618c68

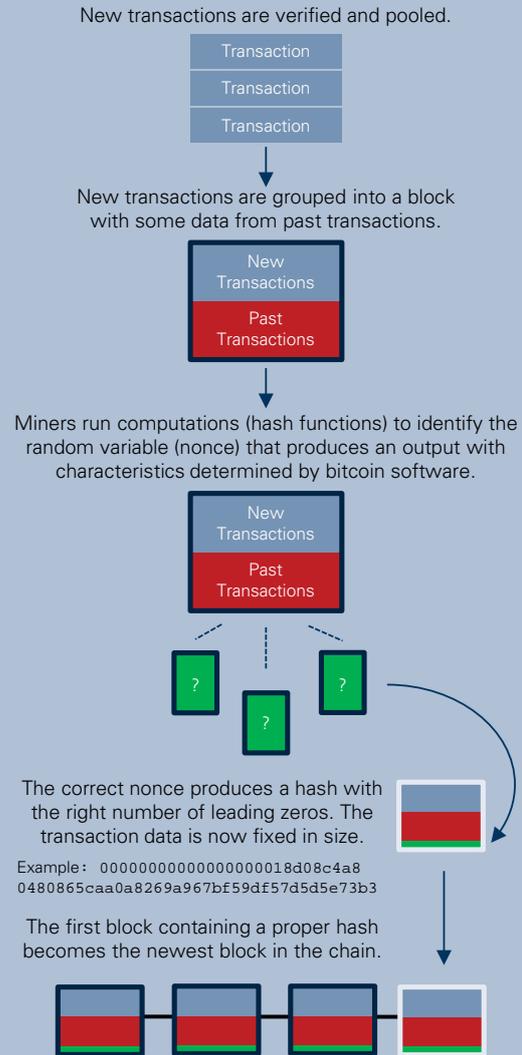
*Keys and addresses are examples only.

Source: Princeton University, Cambridge University, Satoshi Nakamoto, "The Bitcoin Whitepaper," Goldman Sachs Global Investment Research, various news sources.

Step 3: Verifying Bitcoin Transactions

- In order for transactions to be recorded in the blockchain, they must be processed and verified by **miners**. Miners, which may be individuals or groups called “pools,” can be thought of as competitive bookkeepers reviewing bitcoin transactions in exchange for compensation (in bitcoin).
- First, miners identify valid transactions—those in which the senders have both the proper authority and necessary funds—that have been announced to the network. Miners package data from a number of valid transactions into a **block** with a maximum size of 1MB.
- Miners then compete against one another to be the first to add their block of data to the blockchain by attempting to solve a cryptographic puzzle. This involves applying a **hash function** to the transaction data—a process that takes any amount of data and transforms it into an seemingly random output of fixed length (called the **hash**). Importantly, the same input will always give the same output, but it is impossible to guess the input by looking at the hash.
- The hash must begin with a specific number of zeros designated by the bitcoin software. This target, which changes automatically about every two weeks, determines the difficulty of mining at any given point in time. The difficulty can be increased or decreased such that a puzzle is solved about every 10 minutes regardless of the number of miners or available computing power.
- To produce a hash with the right parameters, miners use computing power to determine the correct input. In addition to entering the data for new transactions and some data from prior transactions, they must include a random variable called a **nonce**. Miners effectively participate in an elaborate guessing game, running through billions of numbers until they find the nonce that transforms their data into the correct hash. Once a miner produces the correct hash, they add the block of data to the blockchain.
- Importantly, the hashing process puts a timestamp on all transactions contained within each block. It also links the data from new transactions to information from past blocks. Any attempt to tamper with prior transactions will therefore be visible to other members of the bitcoin network, providing protection against fraud (see pg. 15 for more on this).

How do miners add to the blockchain?



Step 4: Creating New Bitcoins

- Miners’ primary incentive to verify transactions and maintain the blockchain is a reward in the form of new bitcoin (which goes to the first miner to solve the cryptographic puzzle). The reward for mining halves every four years. Initially, successful miners received 50BTC, then 25BTC, and now 12.5BTC.
- Miners also receive transaction fees. These are payments by wallet users to ensure that their transactions go through quickly given the limited throughput of the bitcoin network (approx. 3 transactions per second). Therefore, increases in transaction volume have led to an increase in transaction fees paid to miners.
- Bitcoin’s founder set an arbitrary limit of 21mn bitcoin. 16.8BTC have entered into circulation so far, although some coins have likely been lost. Given the halving reward for miners, the maximum number of bitcoin should be in circulation by 2140.
- Once the 21mn limit is reached, increased transaction costs will presumably need to be high enough to incentivize miners to continue maintaining the blockchain.

What’s keeping the network running?



*Transaction volume is calculated by Coinmetrics as the sum of all transaction outputs belonging to the blocks mined on the given day.
Source: Coinmetrics, Goldman Sachs Global Investment Research.

Source: Princeton University, Cambridge University, Satoshi Nakamoto, “The Bitcoin Whitepaper,” Goldman Sachs Global Investment Research, various news sources.

Summary of our key forecasts

For the exclusive use of ANTON_FILATOV@SBERBANK-CIB.RU

	GDP Growth (% yoy)						FX						Equity						Rates (% eop)						Revision Notes
	2018		2019		2019		3-mth		12-mth		EUR/\$		EUR/\$		SP500		SP500		Policy*		10-yr				
	GS	Cons	GS	Cons	GS	Cons	GS	Cons	GS	Cons	GS	Cons	GS	Cons	GS	Cons	GS	Cons	2018	2019	2018	2019			
GLOBAL	4.1	3.7	4.0	3.6	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		
US	2.8	2.6	2.2	2.2	1.26	1.18	1.30	1.21	1.21	1.21	1.21	1.21	1.21	2700	-	2850	-	2.25 to 2.50	3.25 to 3.50	3.00	3.50	3.00	3.50		
EURO AREA	2.2	2.2	1.8	1.8	1.26	1.18	1.30	1.21	1.21	1.21	1.21	1.21	1.21	3650	-	3950	-	0.00	0.00	-	-	-	-		
GERMANY	2.5	2.3	2.0	1.9	1.26	1.18	1.30	1.21	1.21	1.21	1.21	1.21	1.21	-	-	-	-	-	-	0.80	1.30	0.80	1.30		
JAPAN	1.7	1.3	1.3	1.0	1.10	1.14	1.15	1.15	1.15	1.15	1.15	1.15	1.15	1750	-	2000	-	-0.10	-0.10	0.10	0.40	0.10	0.40		
CHINA	6.5	6.5	6.1	6.3	6.35	6.60	6.45	6.60	6.60	6.60	6.60	6.60	6.60	-	-	102	-	3.00	2.75	-	-	-	-		
BRAZIL	2.7	2.5	3.1	2.8	3.00	3.30	3.10	3.30	3.10	3.35	3.10	3.35	3.10	78100	-	90450	-	6.75	8.00	-	-	-	-		
	Brent crude oil (\$/bbl)						Copper (\$/mt)						Gold (\$/toz)						Corn (cent/bu)						
	3-mth		12-mth		3-mth		12-mth		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	GS	Cons	GS	Cons	GS	Cons			
	75	64	75	62	7300	6860	8000	6780	1225	1305	1225	1315	1225	1305	1225	1315	350	-	350	-	350	-			

Note: Recent revisions marked in red; GDP consensus is Bloomberg; all other consensus is Reuters; commodity 12-mo consensus is Reuters for 2018 average.

* CNY daily fix

Source: Bloomberg, Thomson Reuters, Goldman Sachs Global Investment Research.

Glossary of GS proprietary indices

Current Activity Indicator (CAI)

Our CAI measures the growth signal in a broad range of weekly and monthly indicators, offering an alternative to Gross Domestic Product (GDP). GDP is a useful but imperfect guide to current activity. In most countries, it is only available quarterly and is released with a substantial delay, and its 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 aim to address GDP's shortcomings and provide a more timely read on the pace of growth. We currently calculate CAIs for the US, Euro area, Japan, UK, and 29 other countries. For more, see *Global Economics Analyst: Trackin' All Over the World – Our New Global CAI*, 25 February 2017.

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. Each FCI is calculated as a weighted average of a policy rate, a long-term riskless bond yield, a corporate credit spread, an equity price variable, and a trade-weighted exchange rate; in the Euro area we also include a sovereign credit spread. The weights mirror the effects of the financial variables on real GDP growth in our models over a one-year horizon.

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.

Real-Time Inflation and Activity Framework (RETINA)

RETINA provides a comprehensive econometric methodology able to filter incoming information from the most up-to-date high frequency variables in order to track real GDP growth in the Euro area. Along with a GDP tracker, RETINA also captures the interrelated mechanisms of the area-wide pricing chain, providing a short-term view on inflation dynamics.

Top of Mind archive: click to access



Special Issue
2017 Update, and a Peek at 2018
December 14, 2017



Issue 48
Breaking Down "Brexit Means Brexit"
June 23, 2016



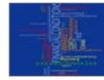
Issue 63
Late-Cycle for Longer?
November 9, 2017



Issue 47
Political Uncertainty
June 23, 2016



Issue 62
China's Big Reshuffle
October 12, 2017



Issue 46
Factoring in Financial Conditions
May 26, 2016



Issue 61
Fiscal Agenda in Focus
October 5, 2017



Issue 45
Brazil at a Crossroads
April 27, 2016



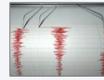
Issue 60
The Rundown on Runoff
September 11, 2017



Issue 44
Policy Stimulus: Running on Empty?
March 23, 2016



Issue 59
Regulatory Rollback
July 26, 2017



Issue 43
Credit Tremors
March 2, 2016



Issue 58
The Fed's Dual Dilemma
June 21, 2017



Issue 42
China Ripple Effects
February 9, 2016



Issue 57
Geopolitical Risks
May 16, 2017



Special Issue
2015 Update, and a Peek at 2016
December 23, 2015



Issue 56
Animal Spirits, Growth, and Markets
April 17, 2017



Issue 41
Liftoff
December 10, 2015



Issue 55
European Elections: More Surprises Ahead?
March 14, 2017



Issue 40
Reserve Reversal Rundown
November 3, 2015



Issue 54
Trade Wars
February 6, 2017



Issue 39
Picking Apart the Productivity Paradox
October 5, 2015



Special Issue
2016 Update, and a Peek at 2017
December 19, 2016



Issue 38
What's Going on in China?
September 24, 2015



Issue 53
The Return of Reflation
December 7, 2016



Issue 37
A Look at Liquidity
August 2, 2015



Issue 52
OPEC and Oil Opportunities
November 22, 2016



Issue 36
Greece, China and Grey Swans
July 9, 2015



Issue 51
US Presidential Prospects
October 18, 2016



Issue 35
Valuations—Dangerous Territory?
May 29, 2015



Issue 50
Central Bank Choices and Challenges
October 6, 2016



Issue 34
Politics, Parties, Populism
April 21, 2015



Issue 49
Trade Trends
September 29, 2016



Issue 33
Wage Worries
March 26, 2015

Source of photos: www.istockphoto.com, www.shutterstock.com, US Department of State/Wikimedia Commons/Public Domain.

Disclosure Appendix

Reg AC

We, Allison Nathan, Marina Grushin, David Groman, Jeff Currie, Michael Hinds, Zach Pandl, Steve Strongin, Huan Wei, James Weldon 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.

We, Alex Blostein, Charlie Himmelberg, James Schneider, Sheriq Sumar, hereby certify that all of the views expressed in this report accurately reflect our personal views about the subject company or companies and its or their securities. We 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.

Unless otherwise stated, the individuals listed on the cover page of this report are analysts in Goldman Sachs' Global Investment Research division.

Disclosures

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.; Ombudsman Goldman Sachs Brasil: 0800 727 5764 and / or ouvidoriagoldmansachs@gs.com. Available Weekdays (except holidays), from 9am to 6pm. Ouvidoria Goldman Sachs Brasil: 0800 727 5764 e/ou ouvidoriagoldmansachs@gs.com. Horário de funcionamento: segunda-feira à sexta-feira (exceto feriados), das 9h às 18h; in Canada by either Goldman Sachs Canada Inc. or Goldman Sachs & Co. LLC; 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. LLC. Goldman Sachs International has approved this research in connection with its distribution in the United Kingdom and European Union.

European Union: Goldman Sachs International authorised 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 Zweigniederlassung 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. The information, opinions, estimates and forecasts contained herein are as of the date hereof and are subject to change without prior notification. 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. LLC, 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 principal trading desks that reflect opinions that are contrary to the opinions expressed in this research. Our asset management area, principal 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 analyst's published price target expectations for such stocks. Any such trading strategies are distinct from and do not affect the analyst's 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.

The views attributed to third party presenters at Goldman Sachs arranged conferences, including individuals from other parts of Goldman Sachs, do not necessarily reflect those of Global Investment Research and are not an official view of Goldman Sachs.

Any third party referenced herein, including any salespeople, traders and other professionals or members of their household, may have positions in the products mentioned that are inconsistent with the views expressed by analysts named in this report.

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.

Differing Levels of Service provided by Global Investment Research: The level and types of services provided to you by the Global Investment Research division of GS may vary as compared to that provided to internal and other external clients of GS, depending on various factors including your individual preferences as to the frequency and manner of receiving communication, your risk profile and investment focus and perspective (e.g., marketwide, sector specific, long term, short term), the size and scope of your overall client relationship with GS, and legal and regulatory constraints. As an example, certain clients may request to receive notifications when research on specific securities is published, and certain clients may request that specific data underlying analysts' fundamental analysis available on our internal client websites be delivered to them electronically through data feeds or otherwise. No change to an analyst's fundamental research views (e.g., ratings, price targets, or material changes to earnings estimates for equity securities), will be communicated to any client prior to inclusion of such information in a research report broadly disseminated through electronic publication to our internal client websites or through other means, as necessary, to all clients who are entitled to receive such reports.

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, models or other data related to one or more securities, markets or asset classes (including related services) that may be available to you, please contact your GS 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.

© 2018 Goldman Sachs.

No part of this material may be (i) copied, photocopied or duplicated in any form by any means or (ii) redistributed without the prior written consent of The Goldman Sachs Group, Inc.