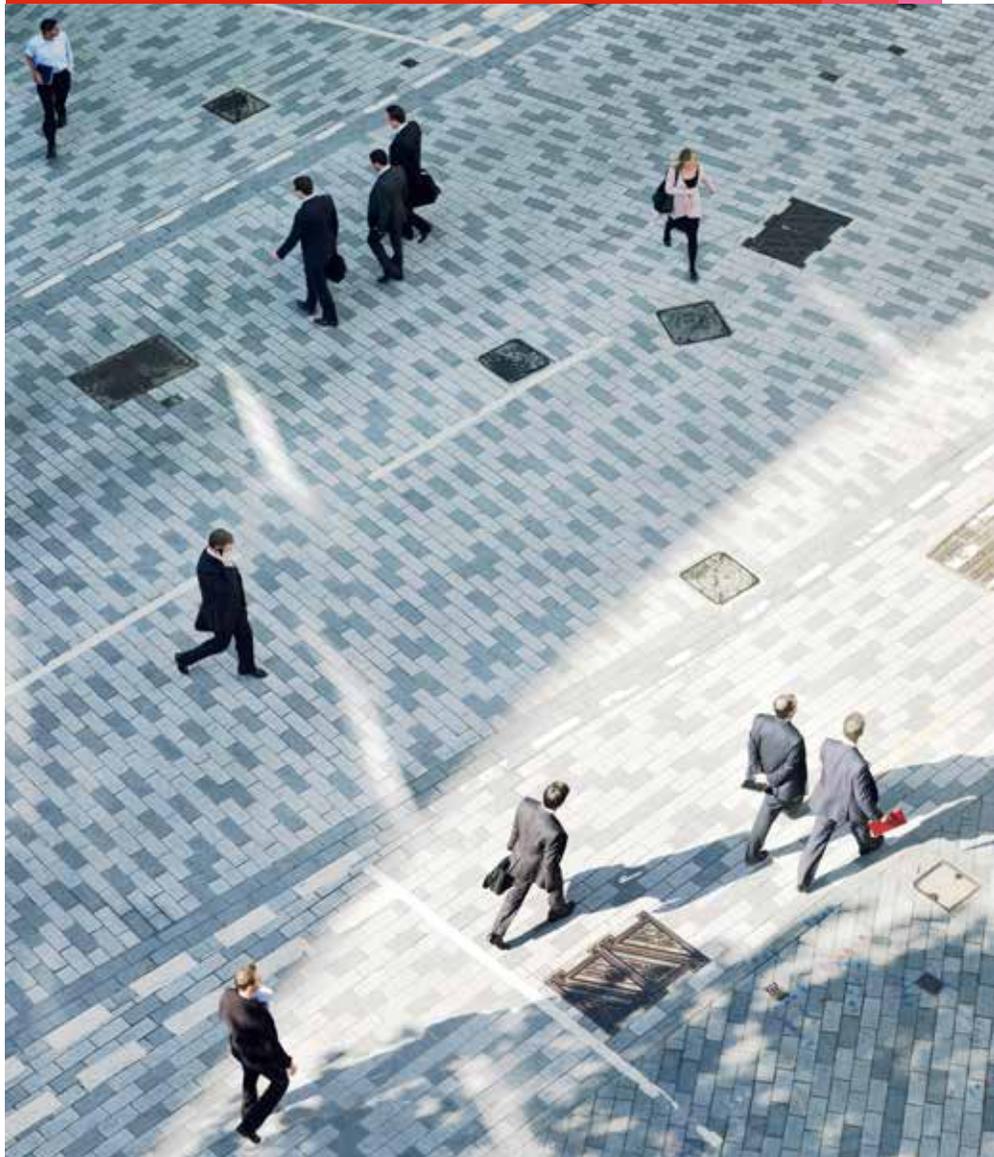


Virtual currencies: Out of the deep web, into the light

*Issues, risks, and
opportunities around the
digitization of money*

March 2014



Initially dismissed as a media- and speculator-driven bubble, Bitcoin's stunning emergence and accelerating mainstream acceptance suggests that the virtualization of currency is more than a mere fad. What began as the dream of a small group of technologists has become a very real phenomenon...one that demands the attention of any organization that deals in the transfer of funds.



Issues, risks, and opportunities around the digitization of money

Depending on whom you talk to, virtual currencies like Bitcoin constitute either a payment scheme for deep-web criminals or the future of money, the shared fixation of a relatively small tribe of technologists or an evolution of the global payments system, a nebulous string of computer code with no inherent worth or a new gold standard for the digital age. With a total value now topping \$8 billion and between 60,000 and 80,000 transactions occurring daily¹, Bitcoin—the most prominent, but by no means the only virtual currency in circulation—is undeniably gaining momentum. But the question remains: What exactly *is* it, and what opportunities and risks do it and other crypto-currencies (such as Ripple, Litecoin, and others) hold for the traditional banking system?²

or nonexistent processing fees, and the possibility of independence from the traditional financial system. No central authority issues, controls, and values bitcoins, which—like dollars, euros, and any other fiat currency—have value solely due to the promise of their acceptance by individuals and companies, and also because of their relative scarcity. By design, the total supply of bitcoins has been capped at 21 million. This self-limitation puts Bitcoin on a virtual par with gold-standard currency: an abstract instrument representing a scarce element (in this case, an elegant cryptographic system) to which a value has been attached by users. Like the gold standard, too, the limitation of total currency serves as an anti-inflationary measure.

In just four years, Bitcoin has seen enormous growth, both in value and public perception. Its skyrocketing market price—which rose from \$1 in mid-2011 to a high of \$1,242 in late November of 2013³—has drawn the eye of investors and sparked excitement as to its potential. In its earliest days, the system's potential for near-total anonymity and its challenge to traditional governmental and financial structures made it a darling of off-the-grid individualists, cryptographers, and others seeking enhanced digital privacy (for licit or illicit reasons). But like many underground, countercultural phenomena that suddenly find themselves awash in cash, Bitcoin has reached the point of broad influence, with the



Like many underground, countercultural phenomena that suddenly find themselves awash in cash, Bitcoin and other virtual currencies have reached the point of broad influence, with the potential to gain mainstream acceptance.

Short story: Bitcoin is both a digital currency and payment system built on a distributed peer-to-peer network architecture. It lives entirely online, created, stored, and traded within a decentralized computer network governed by complex cryptographic algorithms and designed to provide users with privacy, easy and rapid transfer, low

¹ <http://blockchain.info/charts>

² While this whitepaper focuses primarily on Bitcoin as (currently) the best-known virtual currency, the issues, risks, and opportunities it discusses are for the most part applicable to the virtual currency industry in general.

³ <http://blogs.marketwatch.com/thetell/2013/11/29/bitcoin-hits-record-1242-as-it-nears-value-of-ounce-of-gold/>



It is highly unlikely that virtual currencies will ever fully displace established payments systems. But they will surely play a role in the adaptation of those systems to a more digitized, globally-connected economy.

potential to tip over into full mainstream acceptance. This process will inevitably chip away some of Bitcoin's cachet but could simultaneously make it and/or other potential or existing cryptocurrencies an agent of technological, social, and business transformation.

What does the future hold for Bitcoin if it survives the wild market fluctuations of its youth and the serious (and in some cases fatal) challenges that have bedeviled its more prominent exchanges?⁴ From being a glorified barter system or black market scrip, Bitcoin could grow into the Skype of money, circumventing established, monolithic systems by providing an easier, cheaper, more usable, and more contemporary alternative. It could allow developing countries to leapfrog traditional banking systems the way cell phones helped some to move overnight from a deficient landline infrastructure to widely distributed mobile adoption. Its near-nonexistent transaction charges could help it find a niche in micropayments and other charge-sensitive markets—or, at the opposite end of the scale, it could become a game-changer for cross-border payments, replacing today's well-established systems with one that's nearly instantaneous, practically free, and do-it-yourself. Bitcoin could provide a ready mechanism for repatriating corporate earnings from highly-regulated economies, or give the wealthy citizens of countries with strict capital controls a way to move funds outside the country.

Bitcoin may not be the future of money, but then again, it may be. At the very least, it anticipates the tectonic shifts that may lie ahead, as individuals and businesses seek a payments solution that's more in tune with today's borderless, online economy. The time to pay attention is now.

Intersections, issues, and challenges

Bitcoin is hardly the first virtual currency, its antecedents including such everyday instruments as airline miles and virtual gift cards. Most of these are closed-loop systems in which the instrument's value can only be exchanged for goods from a specific service provider or retailer. Exchanging these instruments for cash is generally a small-scale and clunky process, involving individual transactions via Craigslist, Ebay, or similar marketplaces.

Bitcoin, on the other hand, is an open-loop system, with the value of bitcoins freely exchangeable for real-world "tangible" currencies. This transferability alone defaults the system into the category of high-risk products. Add the fact that Bitcoin has no central controlling authority and is instantly exchangeable directly from person to person, worldwide, with virtual anonymity, and you have a new class of monetary instrument whose associated risk will require a new type of non-face-to-face due diligence.

⁴ <http://dealbook.nytimes.com/2014/02/10/bitcoin-exchange-struggles>
<http://www.nytimes.com/2014/02/25/business/apparent-theft-at-mt-gox-shakes-bitcoin-world.html?ref=business>

Two principal security risks:

Bitcoins can be stolen by hackers gaining entry to users' Bitcoin "wallets."

Bitcoins are not guaranteed by any central authority, as traditional US bank deposits are by the FDIC and as certain investment losses due to broker-dealer failures are by the SIPC.

Financial institutions may need to reassess their monitoring and risk systems to encompass the inevitable expansion of these types of open-loop systems.

Key Bitcoin risks

As the Bitcoin economy grows and intersects with the analog economy, businesses that deal in Bitcoin will need to forge strong relationships with the traditional banking industry in order to accept wire transfers and cash deposits, bank their treasury in hard dollars rather than on vulnerable servers, and pay for goods and services that live outside the Bitcoin universe. For banks, relationships with these businesses present three potential central risks: volatility, security, and, most particularly, issues related to source of funds and the potential for money laundering, terrorist financing, and other illicit uses.

Source of funds. For traditional banks, the Bitcoin system's decentralization and anonymity make source of funds and the associated money-laundering potential the biggest risk. Bitcoin account addresses are simply alphanumeric identifiers composed of between 27 and 34 characters. Far from being personally identifiable (like, for instance, a Social Security number), they're temporary and ephemeral: Users are encouraged, for security reasons, to create a new address for every transaction they make. This anonymity raises the probability of illicit Bitcoin usage, and makes enhanced anti-money laundering (AML) protocols a necessity for any organization participating in the Bitcoin economy above the basic user or merchant level.

Recent guidance issued by the US Treasury's Financial Crimes Enforcement Network (FinCEN)⁵ and the intergovernmental Financial Action Task Force (FATF)⁶ have clarified this responsibility. FinCEN requires Bitcoin exchanges (which trade bitcoins for

traditional currencies) and most Bitcoin administrators (the "miners" that earn new bitcoins by growing the general public ledger of cryptographically signed transactions that form the chain of ownership for individual bitcoins) to conform to the regulations for money service businesses (MSBs). These regulations include requirements to implement a customer identification program (CIP), retain certain records, report all transactions of more than \$10,000, and file reports based on defined suspicious activities. Bitcoin users planning to do business with these organizations will thus be required to provide the same types of personally-identifying information, account information, and source-of-funding information that they would when buying, selling, trading, or converting traditional fiat currencies.

Still, the potential for money laundering persists. According to a 2012 FBI intelligence assessment⁷ that was leaked to the Internet, "malicious actors could increase their anonymity by laundering their bitcoins through third-party Bitcoin services registered outside the US," which allow currency exchange or money transfer without requiring verification of user identity or abiding by exchange limits. Some of these services act as exchangers or transmitters, converting bitcoins to traditional fiat currencies or other virtual currencies, or transferring bitcoins between members. Also of concern are Bitcoin "laundry" or "mixing" services, which accept Bitcoin payments and then return the same amount to the user in bitcoins that have no association with the original transaction. Such services, however, would require massive usage to be effective.

Security. Bitcoin carries two principal security risks: (1) bitcoins can be stolen by hackers gaining entry to users' Bitcoin "wallets," and (2) bitcoins are not

⁵ http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf (March 2013).

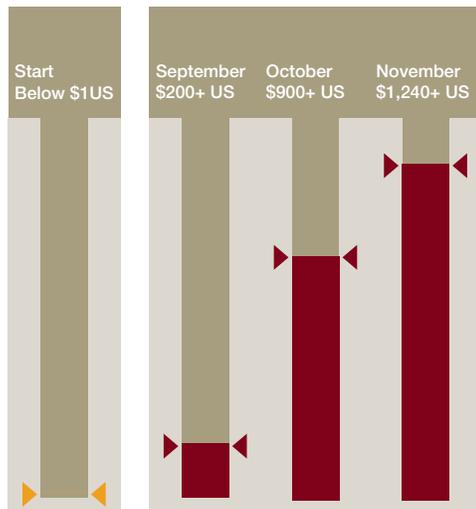
⁶ <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> (June 2013).

⁷ http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf (April 2012).

⁸ <http://www.wired.com/wiredenterprise/2013/11/inputs/>

Volatility

09 13



guaranteed by any central authority, as traditional US bank deposits are by the FDIC and as certain investment losses due to broker-dealer failures are by the SIPC.

With prices skyrocketing in recent months, thefts and scams have exploded, affecting Bitcoin users, administrators, exchanges, payments processors, mixing services, and “banks” (which offer supposedly secure bitcoin wallet storage and access).

In September 2013, New York-based exchange Bitfloor suffered a security breach that resulted in the loss of \$250,000 from their Bitcoin wallets. Late October then saw two major hacks: Australian Bitcoin bank inputs.io was robbed of 4,100 bitcoins (approximately \$1.2 million) in consecutive attacks⁸, and Chinese Bitcoin exchange GBL disappeared overnight, taking \$4.1 million in user accounts with it. GBL had been created only six months before, and had quickly grown into China’s fourth-largest Bitcoin exchange by trading volume. Details that emerged in the wake of the closure suggested the site had been a scam from the start.⁹ In November, the Czech exchange Bitcash.cz¹⁰ and the large, Denmark-based Bitcoin Internet Payment System (BIPS)¹¹ both suffered attacks, resulting in the loss of \$100,000 and \$1.5 million, respectively. That same month, the “Sheep Marketplace” site, an online black market for drugs and other illegal products and services, abruptly went dark after its administrators claimed a hacker had stolen 5,400 bitcoins worth some \$5.3 million.¹² It quickly became apparent that the losses were much more substantial, totaling some 96,000 bitcoins with a value of approximately \$100 million at the time.¹³ The perpetrators, whether external or internal, had gradually drained the accounts of the site’s vendors and buyers, while manipulating the system to make them appear untouched.

And, most recently (and spectacularly), March 2014 witnessed the bankruptcy filing of the Tokyo-based Mt. Gox exchange following the disappearance of hundreds of millions of dollars worth of bitcoins. Lacking FDIC deposit insurance or SIPC investment protection, Bitcoin users and investors have little recourse to retrieve stolen funds, adding credit risk to the investment and exchange risks of dealing in such a currently volatile commodity.

Volatility. To date, price volatility has been Bitcoin’s middle name. From its 2009 introduction until April 2011, the price of one bitcoin sat below US\$1. For the next two years it trended gradually upward before increased interest sent it soaring in the last quarter of 2013: past \$200 in late October, past \$900 in mid-November, and past \$1,240 in late November.

Bitcoin value also shows significant variances on a daily basis across the various exchanges. For instance, at one point in late November of 2013, the value of a single bitcoin varied from \$879 at vircorex.com to \$1,102 at Mt. Gox. Such differences in valuation represent the market’s attempt to react to a product that’s still young and surrounded by risk and uncertainty. As the system’s potential becomes known, its price volatility should stabilize, though whether it does so at, below, or above current valuations depends on the judgment of its users.

Regulatory uncertainty. Bitcoin’s borderless nature and its potential for black market use, tax evasion, money laundering, and terrorist financing make it a source of concern for regulators, who also recognize that the system holds great potential for the global payments system. The challenge for regulatory authorities is now to mitigate the currency’s risks without stifling its upside benefits.

⁹ <http://www.coindesk.com/bitcoin-scam-china-authorities/>

¹⁰ <http://bitcoinexaminer.org/hacker-steals-bitcoins-from-4000-wallets-hosted-exchange-bitcash-cz/>

¹¹ <http://www.coindesk.com/bitcoin-payment-processor-bips-attacked-1m-stolen/>

¹² <http://www.businessinsider.com/sheep-marketplace-goes-offline-and-up-to-44-million-in-bitcoins-disappears-2013-12>

¹³ <http://www.independent.co.uk/life-style/gadgets-and-tech/news/96000-bitcoins-stolen-from-the-users-of-shady-online-bazaar-sheep-marketplace-8981240.html>

In the US, the evolution of official policy on Bitcoin seems to be trending in the currency's favor, even as regulators act to move it under the umbrella of risk and reporting regulations applied to the traditional financial sector. In November 2013, the first congressional hearing devoted to virtual currencies saw representatives of US regulatory bodies offering positive assessments of the currency's potential. A written statement by Federal Reserve Chairman Ben Bernanke noted that virtual currencies "may hold long-term promise, particularly if the innovations promote a faster, more secure, and more efficient payment system."

Foreign regulators are taking varying approaches to the currency. In August 2013, Germany's Finance Ministry recognized Bitcoin as a "unit of account," meaning it can be used for purposes of tax and trade in the country.¹⁴ In China, however, a December 2013 directive from the People's Bank of China and four other ministries outlawed trading in Bitcoin by China's banks, citing a need to "protect the status of the renminbi as the statutory currency, prevent risks of money laundering and protect financial stability." While stating that members of the public remain free to participate in Bitcoin transactions on the Internet, the directive said Bitcoin "does not have the same legal status as a currency."¹⁵

The banking relationship: tentative at best, but vital

The uncertainties and potential risks that surround Bitcoin, along with the enhanced compliance and reporting obligations mandated by recent regulatory guidance, have together greatly strained the possibility of relationships between companies that deal in Bitcoin and the traditional banking sector.

On top of FinCEN's March 2013 guidance, which classified Bitcoin businesses as money service businesses, with all the requirements that designation entails, the US Office of the Comptroller of the Currency (OCC) issued new guidance in October 2013 requiring banks and other financial institutions to adopt risk-based processes for third-party relationships commensurate with the level of risk and complexity inherent in those relationships. With Bitcoin businesses considered high risk due to their potential for money laundering and other illicit uses, this guidance means banks will have to conduct enhanced due diligence on any company dealing in Bitcoin with which they are considering doing business.

Reportedly, the combination of high risk and high compliance costs has led many banks to effectively blacklist Bitcoin companies seeking to open a relationship.¹⁶ It's an understandable decision given the risks and Bitcoin's relatively small size vis-à-vis the wider economy, but it's also a strategy that avoids confronting a near-inevitable outcome. Eventually, banks and other financial firms will need to begin formulating real approaches to Bitcoin and other crypto-currencies that are bound to surface. In the meantime, the lack of engagement by the financial sector can be a major roadblock to Bitcoin-friendly businesses, and it has the potential to stymie US Bitcoin entrepreneurs and force innovation overseas.



In the US, the evolution of official policy seems to be trending in Bitcoin's favor, even as regulators act to move it under the umbrella of risk and reporting regulations applied to the traditional financial sector.

As the regulatory landscape around Bitcoin shifts, one thing is clear: With each new regulation and its attendant compliance and reporting responsibilities, the transaction costs of Bitcoin rise, detracting from one of the currency's greatest strengths.

¹⁴<http://www.cnn.com/id/100971898>

¹⁵<http://www.nytimes.com/2013/12/06/business/international/china-bars-banks-from-using-bitcoin.html?hpw&rref=business>

¹⁶<http://www.forbes.com/sites/kashmirhill/2013/11/15/bitcoin-companies-and-entrepreneurs-cant-get-bank-accounts/> (November 15, 2013).



But the view is not all bleak. On December 5, 2013, Bank of America Merrill Lynch released a major report on the currency, stating that Bitcoin “can become a major means of payment for e-commerce and may emerge as a serious competitor to traditional money transfer providers. As a medium of exchange, Bitcoin has clear potential for growth.”¹⁷

According to a major Bank of America Merrill Lynch report released in December of 2013, Bitcoin “can become a major means of payment for e-commerce and may emerge as a serious competitor to traditional money transfer providers. As a medium of exchange, Bitcoin has clear potential for growth.”

Dialing down Bitcoin AML risk exposures

In the Bitcoin money-transfer chain, risk resides first with Bitcoin users themselves, then with Bitcoin administrators and exchanges, then with banks and other large financial institutions where businesses dealing in Bitcoin seek to house and leverage their funds. Given the March 2013 FinCEN guidance, which imposed AML requirements on all businesses in this chain, and the new OCC guidance, which requires banks to scale their third-party risk management processes based on risk and complexity levels in the relationship, regulatory expectations are clear, at least in regard to AML. Businesses dealing in Bitcoin must develop effective customer identification and reporting protocols, and banks must extend to these businesses AML procedures and controls that meet the requirements of the Bank Secrecy Act/Patriot Act as well as applicable OCC guidance, keeping in mind the particular risks of the Bitcoin ecosystem.

As in any traditional AML program, two keys to the process are transaction monitoring and know-your-customer (KYC) protocols.

Transaction monitoring. Analyzing transaction information can help identify patterns in a Bitcoin user, exchange, or administrator’s behavior; predict future behavior; and assign a risk score. At a minimum, businesses dealing in Bitcoin should be assembling transaction records for all payments or funds transfers that include information identifying the parties to the transaction, all accounts involved, the amount transferred, and the date and nature of the transaction. Financial institutions doing business with these companies need a transparent view into their compliance procedures and documentation, commensurate with perceived risk and complexity. Oversight systems should include evaluating performance metrics, controls, and ongoing monitoring through standardized reporting. Financial institutions must also incorporate these third-party relationships into their current risk assessments and governance program, with proper oversight to ensure accountability.

Know-your-customer protocols. Given the premium the Bitcoin system places on anonymity, Bitcoin administrators and exchanges should consider enhanced customer due diligence that includes systems for the non-face-to-face verification of customer identity. Such a system would require the corroboration of information received from the customer with data from web searches, third-party databases, or other sources/methods—for example, tracing the customer’s IP address or capturing GPS coordinates from his or her mobile signal. Bitcoin-friendly companies can also consider requiring users with whom they do business to make their Bitcoin wallets public, essentially nailing up a sign that says “These bitcoins are mine.” While such a requirement would help clarify customer identifications, it would do little for verifying source of funds, as moneys could continue to flow into the user’s account anonymously.

¹⁷<https://s3.amazonaws.com/s3.documentcloud.org/documents/885843/banks-research-report-on-bitcoin.pdf>



At the bank level, KYC due diligence would seek to answer questions such as:

- Do the administrator/exchanges have a system of controls designed to comply with Bank Secrecy Act regulations?
- Has the company registered as a MSB with the Treasury, per the March 2013 FinCEN guidance?
- Has it implemented the required CIP program?
- Is the compliance program functioning effectively? Is it helmed by an experienced officer? Are its policies and procedures sufficiently robust and flexible to enable compliance with future regulatory changes?

Businesses dealing in virtual currencies must develop effective customer identification and reporting protocols. Banks, for their part, must extend to these businesses AML procedures and controls that meet the requirements of the Bank Secrecy Act/Patriot Act as well as applicable OCC guidance.

- If the company is, through the particular facts and circumstances of its operation, exempt from registration as a MSB, has it nevertheless voluntarily implemented a CIP initiative?
- Has the company completed end-to-end independent testing of its AML program? If so, how recently?
- Is the company registered with its home state as a money transfer business? If it believes it is exempt from this requirement, can it provide a solid legal opinion as support?

Functions throughout the organization must be involved. The front office is directly involved not only because of the risk currently inherent in Bitcoin, but because Bitcoin transactions are transmitted using high-risk products such as mobile apps and mobile payment networks. Compliance departments should oversee not only the internal operations of their third-party vendors,

but also their compliance and AML programs. Internal Audit should verify the controls the organization has established for third-party vendor relationships. Does the firm have acceptable controls in place to mitigate the risk of dealing with MSBs that exchange bitcoins, and are these controls being followed?

The Bitcoin crystal ball: cloudy with a chance of sunlight

Despite the attention (both positive and negative) showered on Bitcoin in recent months, the currency's future is still anything but clear. To a large extent—and appropriately, given its philosophical underpinnings—the system's future will be what its users make of it. But, it will also be what established power structures help it to become. If regulators fail to establish sound, consistent, and forward-thinking guidance, financial institutions may continue to shun doing business with companies that deal in Bitcoin, to the detriment of both domestic innovation and the overall respectability of the Bitcoin system. If, however, regulatory policies encourage practices that enhance security and transparency while maintaining the currency's core strengths of speed, ease, and low cost, Bitcoin could present financial institutions with a new world of opportunities—for example, in offering Bitcoin brokerage services, securities, loans, deposit accounts, and trusts. The OCC's new guidance on third-party vendors, while not specifically addressing Bitcoin or crypto-currencies in general, at least gives financial institutions a basis on which to make decisions regarding association with Bitcoin companies, based on MSB AML/KYC procedures.

Given the steadily increasing size and value of the system, and the sure expansion of virtual currencies in our ever more digital economy, the ability to properly assess the risks and opportunities of crypto-currencies should become part of the banking industry's skill set.



Contact us

To have a deeper conversation about the risks and opportunities related to virtual currencies, please contact:

John Sabatini

Advanced Risk & Compliance Analytics Leader
PricewaterhouseCoopers LLP
(646) 471 0335
john.a.sabatini@us.pwc.com

David Choi

Advanced Risk & Compliance Analytics Principal
PricewaterhouseCoopers LLP
+44 (0) (207) 212 1809
david.d.choi@us.pwc.com

Vikas Agarwal

Advanced Risk & Compliance Analytics Managing Director
PricewaterhouseCoopers LLP
(646) 471 7958
vikas.k.agarwal@us.pwc.com

Kevin Breitman

Advanced Risk & Compliance Analytics Director
PricewaterhouseCoopers LLP
(646) 313 3633
kevin.breitman@us.pwc.com

Edward Stoltenberg

Advanced Risk & Compliance Analytics Senior Associate
PricewaterhouseCoopers LLP
(646) 471 8554
edward.r.stoltenberg@us.pwc.com

