Fact Sheet

June 2014

www.crypto-currency-fund.com

The world's first crypto currency trading fund
2013 Return: 392%

Monthly Performance

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	YTD
2014	(prior	strategy)		-1.69%	39.46%	-1.77%							**34.71%**

Fund Information

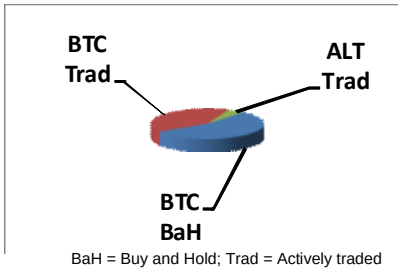
Strategy: The Crypto Currency Fund is the world's first crypto currency trading fund. It employs a variety of strategies in trading crypto currencies to maximize return and minimize risk, including event-driven, arbitrage (timing, exchange, inter-crypto currency, etc.), leverage, cyclic and volatility. While its major focus is on bitcoin, it also trades in "altcoins" (non-bitcoin crypto currencies) as they develop sufficient liquidity.

Implementation: Because crypto currency exchanges work 24/7, the Fund's traders have to monitor markets around the clock. To do so, Crypto Currency Fund has traders located in New York, Houston, Paris and Moscow.

Fund Information

Date Formed/Renamed	April 2005, strategy change and fund renamed April 2014
Investment Advisor	Enneking Asset Management
Fund Size	$6.6 M
Currency	US dollar
Current Price (NAV)	$331.96
Min. Investment	$10,000 (non-US); $100,000 (US)
Fees	2% management, 20% success
Subscription	Monthly
Redemption	Monthly, with 30-days notice
NAV	Monthly
Administrator	Maples Fund Services
Auditor	Altschuler, Melvoin & Glasser
Bank	Bank of New York
Legal Advisors	US: Finn Dixon; non-US: Harneys
FATCA Compliant?	Yes
Bloomberg ID	CRYPTOF KY, BBG006R08WH9
Lipper Tass/Thomson Reuters ID No.	96695
Eurekahedge ID No.	15532
CUSIP/ISIN	G3164M 100/KYG3164M1006
URL	www.crypto-currency-fund.com

Sector Allocation



BaH = Buy and Hold; Trad = Actively traded

CCF has now opened nine accounts with various exchanges and funded two of them. Three traders are currently active and doing well. One of them is trading altcoin, adding another dimension to CCF's portfolio.

Pricing

Bitcoin prices were again reasonably stable during June, at least by bitcoin standards. The opening price was $630, the high $670 and the low $580; overall, bitcoin fell slightly, as did CCF.

This new-found stability is important because the only remaining material criticism of bitcoin as a currency is its high volatility (whether that criticism is valid or not is another question). The recent stability, particularly after the chaos of the China/Mt. Gox sell-off, should go a considerable distance to assuaging that criticism.

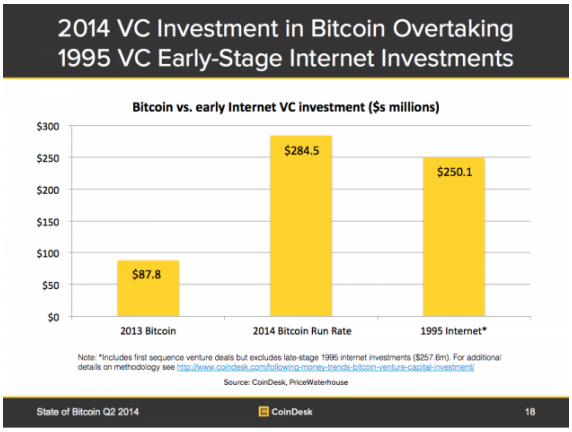
Performance (net of fees)

June's performance by CCF was in line with bitcoin. Trading took place during the entire month with the traders working in different "configurations" in terms of number of traders, accounts and locations. As in May, during the last week of which trading began, trading did not have a significant impact on performance because of the small size of the account (which will remain the case until the trading strategy has been proven). We were able to transfer more CCF assets from the Bitcoin Fund to CCF's actively traded accounts.

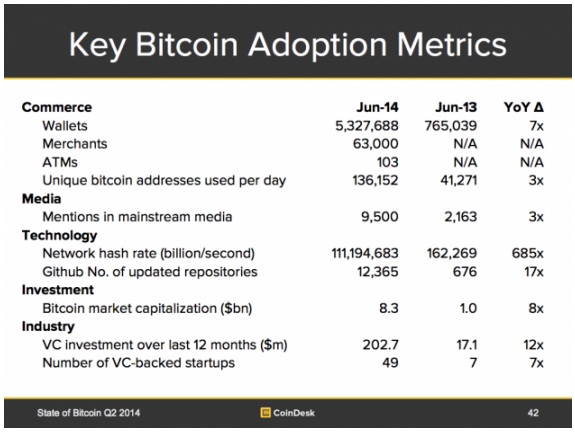
We are also happy to announce the Bloomberg ticker for the Crypto Currency Fund: **CRYPTOF KY**.

Market Developments

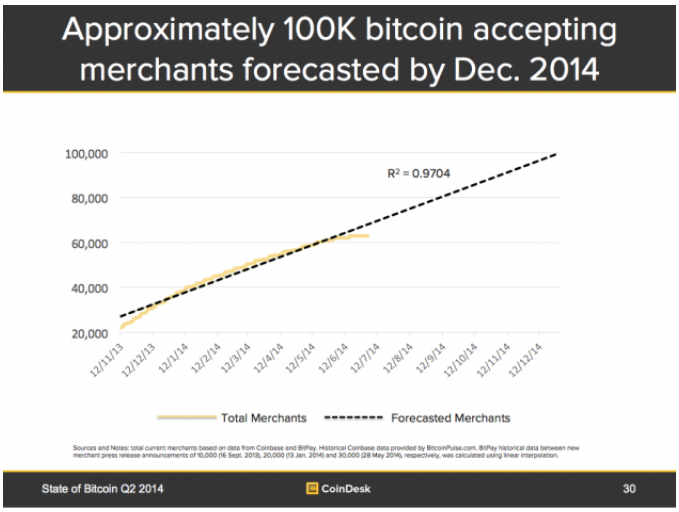
Constructive news on bitcoin just continued to roll out in June.



CoinDesk published its **State of Bitcoin Q2 2014** report which, among other things, compared the progress of bitcoin investment to that of the internet. The result is quite interesting (shown above).



The report also included important statistics on the major bitcoin adoption metrics, as summarized above.



Of particular importance are the number of merchants worldwide which accept bitcoin as shown above. (Entire report attached.)

Commercial Companies

- **MasterCard** filed a patent that would seek to incorporate bitcoin into its design for a planned global online shopping cart.
- Accounting software company **Intuit** has enabled its merchant network to accept bitcoin through its new **PayByBitcoin** service.
- **Cai-Capital** became the first UK firm to offer international investors the ability to buy UK properties with an extensive range of digital currencies, including bitcoin, litecoin, ripple, maxcoin and quark.
- South Korean payments gateway giant **Galaxia Communications** announced that its customers will be able to use bitcoin to pay on thousands of websites.
- **Newegg**, the online retailer of electronics and software deals and top rated services, now accepts bitcoin.
- **Bloomberg** published an explanatory video on crypto currencies. It's 2 minutes and 25 seconds long, but quite helpful and not at all technical. You can view it here: http://edition.cnn.com/2014/07/09/business/explainer-how-do-cryptocurrencies-work/index.html?c=business
- Digital gift card provider **Gyft** updated its **Apple** iOS app, adding a bitcoin payments option that was previously exclusive to its Android customers. Gyft supports retailers such as **Whole Foods**, **Starbucks**, **Groupon**, **GAP** and **Nike**.
- ***Il Giornale***, a conservative Italian newspaper serving the Milan area began accepting bitcoin for subscriptions to its premium PDF edition. The paper is owned by Paolo Berlusconi, Silvio's brother.
- Ukraine's **National Credit Bank** expanded its nationwide network of more than 4,900 payment terminals to allow customers to buy bitcoin for cash.
- John Bush and Catherine Bleish with their two children, began a four-week, 4,400-mile road trip across the US, from Texas to Washington, DC and back, during which they will only spend bitcoin. During the trip, they will shoot five episodes of their reality show "**Sovereign Living**". Recent announcements by **Gyft**, **eGifter** and **Expedia** allowed them to plan such a trip.
- **Western Union** CEO Hikmet Ersek has said his company is open to the idea of using bitcoin once the digital currency is regulated.
- **Overstock** CEO Patrick Byrne announced at a recent conference that his company is "going to start giving sort of special deals to the vendors who want to be paid in bitcoin."
- A new report by **Deloitte University Press** says bitcoin has great potential to disrupt payments and other industries, but that the media may be "distracting" governments and businesses from the technology's advantages. (Full report attached.)
- **Expedia** announced that it would begin accepting bitcoin for payments on June 11 and has already confirmed that its first foray into the ecosystem has proven a success, with bitcoin payments exceeding expectations.
- Peter H **Diamandis**, the founder and Chairman of the **XPRIZE Foundation**, announced that he feels that bitcoin is globally important and disruptive technology and that he is exchanging his personal holdings of gold for bitcoin.
- US online retailer **Overstock** has pledged to donate 3% of profits generated through bitcoin sales to advocacy organizations that promote digital currencies.
- **TOPOS Design Studio**, an award-winning architecture and interior design firm in Singapore, announced that it is the first such firm to accept bitcoin payments from clients. Furthermore, the company stated that it will retain bitcoin payments to pay its future business costs.
- **1-800-Flowers.com** has announced that it now accepts bitcoin.
- Jason Oxman, CEO of the **Electronic Transactions Association (ETA)**, the membership of which includes MasterCard, Paypal and Amazon stated that he believes that bitcoin offers unique advantages for the payments industry.
- Daily financial services newspaper ***American Banker*** announced that it will hold a one-day conference in July to bring the traditional financial services industry up to speed on developments in the bitcoin and digital currency ecosystem.

Governmental and Regulator Developments

- The **Organisation for Economic Co-operation and Development (OECD)** published a very informative working paper on bitcoin that draws generally positive conclusions about the technology behind the digital currency. (Full paper is attached.)
- **Governor Jerry Brown of California** has signed **Assembly Bill 129** which grants bitcoin and other digital currencies "legal money" status into law just weeks after the approval earlier in June by both the California Assembly and Senate**.**
- **Switzerland's Federal Council**, the nation's executive branch, issued a 25-page report on digital currencies which broadly defined how it believes specific bitcoin businesses should be regulated under existing law. It was greeted very favorably by bitcoin enthusiasts as an excellent regulatory precedent.
- The **Parliament of Canada** passed a bill that amends Canada's Proceeds of Crime (Money Laundering) and Terrorist Financing Act of 2000 to extend to both foreign and domestic businesses working in the bitcoin and digital currency sectors in Canada.
- **Temasek Holdings**, a $172bn, AAA rated investment company owned by the government of Singapore launched its first office in New York City, and stated that it has been "experimenting" with bitcoin, conducting a company-wide "bitcoin experiment", with all staff at the company – from drivers to board members – participating. The Chairman said he intended to seriously review investing in the bitcoin space.
- **US Republican Senator Branden Petersen** from Minnesota is leading the latest effort to bring bitcoin and its benefits to the global public through his position as Executive Director and founder of **yesbitcoin**, a new bitcoin-focused non-profit.
- **Geoff Bascand**, **Deputy Governor and Head of Operations at the Reserve Bank of New Zealand (RBNZ)** stated that digital currencies could one day evolve to "supplant cash as we know it".
- The **Central Bank of Sweden** published commentary on bitcoin which was quite favorable, saying among other things that bitcoin will help meeting "new payment needs and making payments cheaper and more secure."
- **Poland's Deputy Finance Minister Wojciech Kowalczyk** released a document confirming that under Poland's existing financial regulations, bitcoin is considered a financial instrument.
- **Gareth Murphy**, Director of Markets for the **Central Bank of Ireland**, became the first government-backed bank representative to speak at a digital currency conference.

- The **US Consumer Financial Protection Bureau** (CFPB), an independent federal agency tasked with policing financial products, is preparing to oversee bitcoin following a request from the **US Government Accounting Office (GAO)**.
- **Italian Senate** Vice President of the Treasury and Finance Committee Francesco Molinari, MP Stefano Quintarelli and representatives from Italy's academic and banking sectors met with Italian bitcoin enthusiasts on June 11. Another meeting was held on June 26 at which bitcoin transactions were demonstrated "live" for Italian lawmakers.
- On June 25, the **US Marshals Service** auctioned off approx. 30,000 bitcoins seized from Silk Road to a single bidder. Notwithstanding that there were nine blocks of 3,000 bitcoin and one block of approx. 2,656 bitcoin auctioned, legendary venture capitalist **Tim Draper** outbid the 40+ other bidders and bought them all. The USMS still holds approximate 140,000 bitcoin that it will also auction off.
- **FINMA**, the Swiss Financial Market Supervisory Authority, gave permission for bitcoin ATM operator **SBEX** to launch a network of bitcoin ATMs in Switzerland.
- Japan has formed the **Japan Authority of Digital Asset (JADA)**, an advocacy group for bitcoin businesses which has the explicit backing of the Japanese government. JADA will be a bitcoin business-only group intended to establish standards and codes of conduct for its members.
- The **European Commission** signaled it will try to impose rules on virtual currencies such as Bitcoin after the bloc's banking regulator ordered lenders to shun them.
- The **US Financial Action Task Force (FATF)** has published a paper looking into the money laundering and terrorism financing risks involved with digital currencies. (Full paper attached.)
- **Kuwait Financial Centre** published a new report entitled **"Disruptive Technology: Bitcoins, Currency Reinvented?"** on bitcoin in which it called the digital currency a disruptive technology that could help ignite the region's e-commerce industry.
- The **Russian Financial Action Task Force (FATF)**, an intergovernmental body set up to combat money laundering and terrorist financing, announced that it will clarify its stance on bitcoin in a forthcoming paper. In the meantime the **Bank of Russia** stated that bitcoin should not be rejected.
- **Guy Debelle**, the assistant governor of the **Reserve Bank of Australia (RBA)**, believes **Scotland** could become a testbed for cryptocurrencies if it gains independence from the UK.

Crypto Currency Companies

- With its second Series A-1 funding round of $20m, online wallet provider **Xapo** has raised its funding total to $40m, leapfrogging **BitPay** to become the best-funded bitcoin startup.
- Identity verification service **BlockScore** raised $2m in a seed funding round from a range of high-profile investors include **Battery Ventures**, **Lightspeed Venture Partners** and **Boost VC**.
- Global cash transaction network **ZipZap** has formally reinstated its bitcoin buying service, which was temporarily halted in March of this year, at more than 20,000 partner retail locations in the UK.
- **The Bitcoin Foundation** has hired Washington, DC-based firm **Thorsen French Advocacy** to lobby the US government.
- UK-based bitcoin exchange **Coinfloor** appointed Adam Knight, a former managing director from both **Goldman Sachs** and **Credit Suisse**, as its executive chairman.
- Open-source bitcoin ATM manufacturer **Skyhook**, which manufactures low-cost, portable bitcoin ATMs, announced that it has shipped 150 units since its May launch, 70 units were shipped to customers since the beginning of June alone, and expects to ship 1,000 units in 2014.
- Following a recent initiative aiming to transform the Indonesian island of **Bali** into a "**Bitcoin Paradise**", an advocacy group in the **British Crown dependency of Jersey** has announced similar plans to develop a "**Bitcoin Isle**".
- **BitBox** installed the first bitcoin ATM, made by **Robocoin**, in Israel.
- Bitcoin exchange **itBit** announced that it would relocate its headquarters from Singapore to New York City because of the pending regulatory changes there.
- **Rebit.ph**, a Philippines start-up, is targeting the remittance conversion problem as efficiently as possible in a country where over 12 million, or 10% of the entire population, live and work overseas; they sent $23 billion back home in 2013.
- **OpenBazaar** announced that it has created a "decentralized eBay" to allow any two parties to engage in a transaction without having to rely on the security and integrity of a questionable centralized network.
- The **Island of Jersey** has approved the launch of a bitcoin investment fund, **Global Advisors Bitcoin Investment Fund (GAB)**, which the government claims will be the first such fund to be regulated and set to launch on August 1. Unlike **CCF**, however, it will be another index fund and will not trade on its investors' behalf.
- Bitcoin ATM operator **QwikBit** announced that it had accepted delivery of its first batch of Lamassu bitcoin ATMs in the **Isle of Man**.
- **Expresscoin** now offers customers the ability to buy bitcoin, litecoin, dogecoin and blackcoin with debit cards
- Bitcoin payment processor **Coinbase**, which has raised $31.7m in funding, has enabled merchants to display the cost of goods and services in smaller denominations of bitcoins: "bits". Currently, a single bitcoin is divided into eight decimal places, with each unit known as a "**Satoshi**". One bit (or µBTC) is worth 100 Satoshis, so something worth $1 can be priced at 1,700 bits rather than 0.0017 BTC.
- **CoinCorner** launched the first digital currency exchange on the Isle of Man.

Fund Awards (prior to renaming)

Most Innovative Funds of Funds (for innovation and performance)

Most Innovative Funds of Funds (for innovation and performance)

No. 1 ranked fund of funds in the world, 2013

No. 2 ranked fund of funds in the world for 2010

No 8 ranked fund of funds in the world for 2009

No 1 ranked fund of funds in the world for 2005

Fund Information

Enneking Asset Management Mr. Timothy Enneking +7 910 439 1486 te@crypto-currency-fund.com	Maples Fund Services Ltd Mr. Mark Wellon Tel.: +1 514 228 2227 mark.wellon@maplesfs.com

Deloitte University Press

Bitcoin

Fact. Fiction. Future.

About the authors

Tiffany Wan is a former GovLab fellow and Strategy & Operations senior consultant with Deloitte Consulting LLP. Her area of expertise focuses on the intersection of strategy, finance, and public policy. Wan's interests include financial inclusion, economics, immigration, and emerging financial technology. Wan has a Master of Public Administration from Columbia University and a BA from Yale University in political science and international studies. You can reach her on Twitter at @tiffany_wan and by email at twan@deloitte.com.

Max Hoblitzell is a former GovLab Fellow and Strategy & Operations consultant with Deloitte Consulting LLP's Federal practice. His areas of interest include emerging financial technology, health care, and data analytics. His previous GovLab research focuses on how government can improve the use of challenge prizes to solve big problems. You can reach him on Twitter at @maxhoblitzell and by email at ahoblitzell@deloitte.com.

Acknowledgements

We are grateful to the many individuals who shared their time and expertise throughout the writing of this report. **Carmen Medina** served as the research sponsor for this project, providing us with insight, inspiration, and general "Yoda-ing." This GovLab project and paper would not have been possible without her mentorship. Special thanks go to **Shrupti Shah**, GovLab director, and **Bill Eggers**, director of Deloitte Global public sector research, for advice throughout the writing process.

Several Deloitte colleagues provided invaluable feedback at all phases of our research. We would like to thank **Brien Lorenze**, Financial Advisory Services principal, who early on in the research process saw promise and potential in this project. Thank you to **Val Srinivas**, head of research for Deloitte's Center for Financial Services, and to his staff, **Ryan Zagone** and **Dennis Dillon**, for collaborating on this emerging topic. We greatly appreciate the advice and support of Deloitte's Cryptocurrency Community of Practice, in particular **Pierre Rochard**. Thanks to **Tiffany Fishman**, Deloitte Services LP; **Mark White**, Global Consulting CTO; and **Devon Halley**, GovLab manager, for their wisdom and guidance. Hats off to **Vetan Kapoor**, former GovLab fellow, for his contributions to the project.

We would like to thank the individuals whose interviews informed our research, including **Barry Silbert**, CEO of SecondMarket; **Miles Kimball**, professor of economics and survey research at University of Michigan; **Nick Tomaino** and the team at **Coinbase**; **John Collins**, senior staff at the Senate Committee on Homeland Security and Government Affairs; **Rodolfo Gonzalez**, associate at Foundation Capital; and the **Ethereum** team. We also want to extend a special thank you to **Walter Frick**, associate editor at *Harvard Business Review*, for providing the opportunity to contribute to *Harvard Business Review*'s blog and for speaking opportunities at Harvard University.

Lastly, we would like to thank our **GovLab** colleagues for creating a culture of innovation—a place that supported and pushed us to take an exciting ride with Bitcoin.

Contents

Introduction

DESPITE an explosion in media coverage, virtual currencies such as Bitcoin are misunderstood. Every day, news articles describe exchange meltdowns, price volatility, and government crackdowns. This focus on Bitcoin as a volatile and even renegade currency may be distracting governments and businesses from *its potential long-term significance as a disruptive new money technology*.

Bitcoin is more than just a new way to make purchases. It is a protocol for exchanging value over the Internet without an intermediary. Much has been written about the payment applications of Bitcoin, including remittances, micropayments, and donations. However, Bitcoin could soon disrupt other systems that rely on intermediaries, including transfer of property, execution of contracts, and identity management.

As the Bitcoin ecosystem evolves and use cases emerge, the public and private sectors will face new challenges, opportunities, and responsibilities. Government may discover new methods for executing its mission as a regulator and law enforcer, while corporations may build upon Bitcoin technology to create innovative products and services. In the future, Bitcoin may even revolutionize the way we conduct business and think about work. The sooner the public and private sectors understand the potential of this new technology, the better prepared they will be to mitigate its challenges and realize the benefits of Bitcoin and other similar virtual currencies.

This report explains the technology underlying Bitcoin and other virtual currencies, identifies new applications, and explores the impact of potential future scenarios. If Bitcoin's short history is an indicator, the future of this technology will be an exciting ride.

Bitcoin overview

BITCOIN is best thought of as a natural next step in the evolution of money. Throughout history, many items have been used as a store of value and medium of exchange, such as cowrie shells, clay tablets, coins, and now paper money. Starting in the 18th century, nation-states increasingly used precious metals such as gold and silver to back their paper money, creating a monetary system called the gold standard. The gold standard required governments to hold enough precious metal reserves to support their currency. As the global economy became more complex in the second half of the 20th century, most nations eventually moved away from the gold standard, creating fiat currencies built on laws and trust in government.

As our understanding of money as a store of value, medium of exchange, and unit of account has matured, so have the methods and modes for exchanging it. In this sense, the exchange of money has always been a function of the technology available. We moved from precious metal coins to paper money before inventing checks, then credit cards. Yet credit cards weren't created for the Internet era. They've simply been adapted to meet the needs of consumers operating in a networked and digital world. With the consumer-accessible Internet now 20 years old, the question is not why a currency specifically designed for the Internet has emerged, but what took it so long.

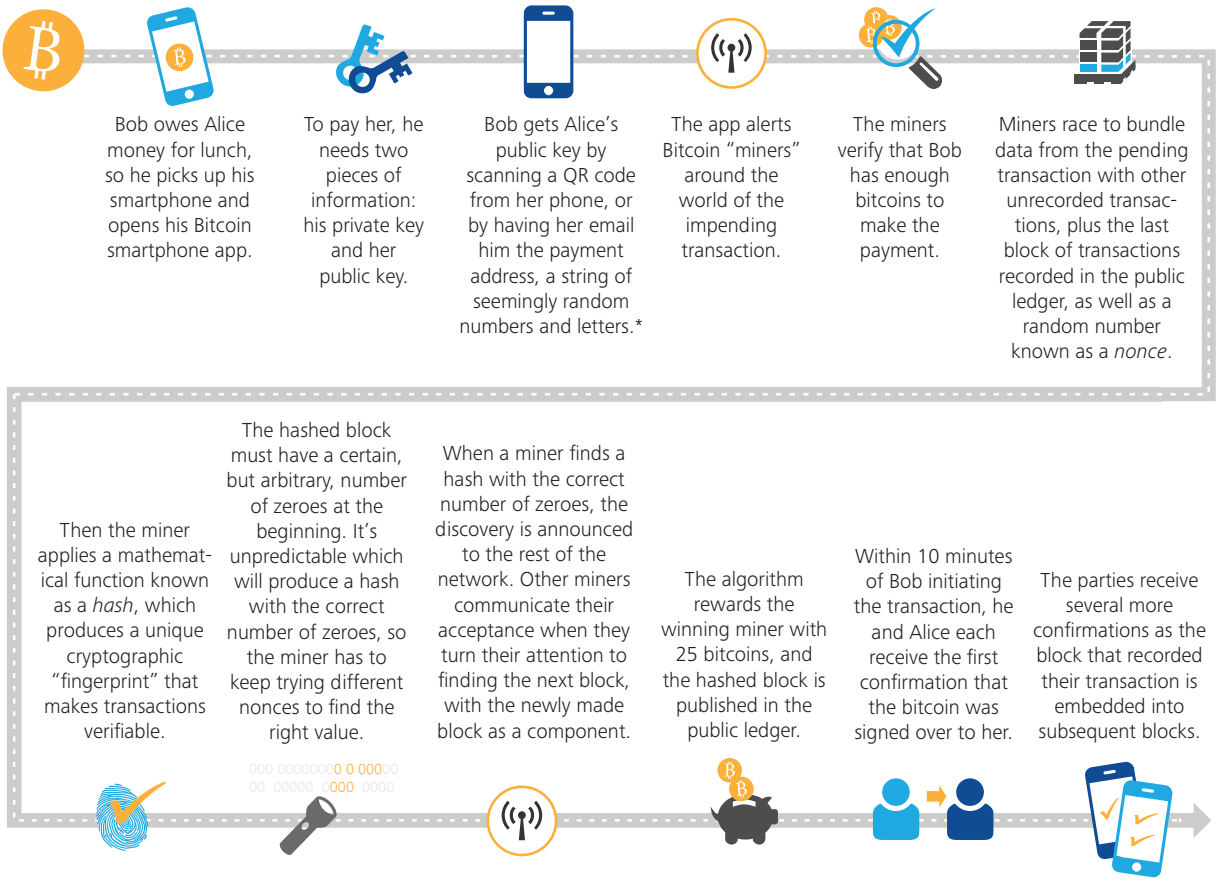
Bitcoin is one of the first currencies born on the Internet to be used in the real economy. It can be used to make purchases of goods like smartphones, hotel stays, pizza, and coffee. Other virtual currencies have since been created from the same open source code as Bitcoin, including Litecoin and Dogecoin, the virtual currency based on the Doge meme.[1] More are popping up every day. Some of these currencies aim to improve upon Bitcoin's technical or operational difficulties, such as transaction speed and security. However, Bitcoin so far has sustained its first-mover advantage. It is the most popular and has the highest value in circulation. As of June 4, 2014, there are 12.85 million bitcoins in circulation with a total market capitalization of $8.3 billion.[2]

How does Bitcoin work?

Bitcoin is a protocol for exchanging value over the Internet without an intermediary (figure 1). It's based on a public ledger system, known as the block chain, that uses cryptography to validate transactions. Bitcoin users gain access to their balance through a password known as a private key. Transactions are validated by a network of users called miners, who donate their computer power in exchange for the chance to gain additional bitcoins. There is a fixed supply of 21 million bitcoins that will be gradually released over time at a publicly known rate. There is no monetary authority that creates bitcoins. The capped supply of 21 million is known to all, and the rate of supply diminishes over time in a predictable way. As a store of value, this means that bitcoins are inherently deflationary. It also means that there is no government or central entity to make discretionary decisions about how much currency to create or attempt to defend it through monetary policy actions.[3]

In order to process a bitcoin-denominated transaction, Bitcoin verifies two facts addressed by current payment systems like PayPal or

Figure 1. How Bitcoin works



** Anyone who has a public key can send money to a Bitcoin address, but only a signature generated by the private key can release money from it.*

Source: American Banker, http://cdn.americanbanker.com/media/ui/how-bit-works-big.jpg.

Graphic: Deloitte University Press | DUPress.com

Visa. The first is that when user A transfers a bitcoin to user B, user A has a bitcoin to spend (that is, prevention of counterfeiting). The second is that when user A transfers a bitcoin to user B, user A is not trying to transfer the same bitcoin to another user, user C, simultaneously (that is, prevention of double spending).

As Bitcoin matures, an ecosystem of companies is emerging to support consumers and retailers in storing, exchanging, and accepting bitcoins for goods and services:

- **Banks and wallets** store bitcoins for users either online or on storage devices not connected to the Internet, known as "cold storage."
- **Exchanges** provide access to the Bitcoin protocol by exchanging traditional currencies for bitcoins and vice versa.
- **Payment processers** support merchants in accepting bitcoins for goods and services.
- **Financial service providers** support Bitcoin through insurance or Bitcoin-inspired financial instruments.

What are the qualities of Bitcoin as a technology system?

Bitcoin has three qualities that differentiate it from other currencies and payment systems.

Miners are individuals that provide the computing power for Bitcoin's validation process in exchange for the opportunity to gain new bitcoins. Together, miners make up Bitcoin's distributed network. Miners use their computing power to validate transactions by solving a cryptographic problem, called a hash function. By using their computing power for this work, miners are rewarded with bitcoins. This is how new bitcoins enter the money supply. Because the money supply is capped and the rate of supply diminishes over time, the difficulty of creating a block increases and the actual amount rewarded for each new block created decreases.

Mining has been the subject of significant media coverage, as an arms race has grown around hardware designed to perform highly specialized computations to mine bitcoins. In the early days of Bitcoin, miners were mainly hobbyists using personal computers to solve relatively simple cryptographic problems. Now, miners are raising investor dollars to construct server farms optimized for bitcoin mining.

First, Bitcoin is peer to peer, transferring value directly over the Internet through a decentralized network without an intermediary. Current payment systems, like credit cards and PayPal, require an intermediary to validate transactions; Bitcoin does not. As a result, Bitcoin has been referred to as "Internet cash," as it can be exchanged from person to person much like paper currency today.

Second, Bitcoin is open, yet securely authenticated. Traditional payment systems rely on the privacy of transaction information to maintain security. For example, the compromise of a credit card transaction can result in the release of valuable information that can be used to conduct future transactions. In comparison, Bitcoin relies on cryptography. As every transaction is validated with cryptography by the network of miners, Bitcoin functions because of its openness, not despite it.

Third, Bitcoin is self-propelling. Bitcoin uses its own product, bitcoins, to reward or "pay" miners who are providing the computing power that serves as the engine of the transaction verification system. As a result, the system does not require the same type of overhead that traditional payment systems might require. In this sense, Bitcoin functions because of those participating in the system.

These three aspects are part of what drives Bitcoin's success, enabling a nearly frictionless global payment system. However, these same factors have also created challenges.

Bitcoin caveats: Speculation, regulation, and whatever

In order to achieve wider adoption as a currency, Bitcoin needs to address significant questions around volatility, regulatory uncertainty, exchange security, ease of use, and transaction volume.

Bitcoin speculators have driven significant price volatility, reducing Bitcoin's utility as a medium of exchange. People may be reluctant to use Bitcoin to make large future commitments of value, or even buy a cup of coffee, when the price can change by 30 percent overnight. Unless Bitcoin's volatility settles, it will be used less as a currency and more as a vehicle for speculation and "get rich quick" schemes, much like a penny stock.

The global regulatory environment around Bitcoin remains uncertain. Any news of new government scrutiny or rumors of a policy change can significantly affect Bitcoin prices, reducing its stability as a currency. At the same time, businesses are unwilling to engage in the Bitcoin economy, while governments treat it as a fringe movement that is the purview of black-market operators and drug dealers, such as Silk Road. As governments begin to issue consistent guidance on Bitcoin, businesses may become more willing to accept it as a form of payment.

Security problems, punctuated by highly publicized exchange meltdowns, may prevent

mainstream usage of bitcoins as a currency. Many exchanges that have suffered—including Mt. Gox, which experienced the most notorious exchange collapse—were built on unstable platforms with little security, due to their having been created when bitcoin trading was small and nascent. Mt. Gox was like a bank storing valuables in the lobby entrance. To mature, exchange security needs to be as strong as at traditional banks.

The requirements necessary to safely store bitcoins have created ease-of-use problems. Though digital wallets have worked to solve some of these problems, best practices for storing bitcoins include locking flash drives in a bank vault. Really? Mainstream consumers are unlikely to use Bitcoin until wallet services develop more user-friendly and secure storage techniques.

Validating transactions requires significant electricity, bandwidth, and data storage. The resources required to support Bitcoin's relatively small volume of transactions are already being pushed to their limits. Currently, Bitcoin averages about 60,000 transactions per day.[4] VisaNet, the electronic payment processing network used by Visa, handles more than 150 million transactions daily from 2.1 billion Visa cards and over 2 million ATMs.[5] It can do this because it charges fees for the resources required to operate its servers. In order to support mainstream transaction volumes, the Bitcoin system for validating transactions will likely have to change how it uses electricity, bandwidth, and data storage.

Despite these obstacles, mainstream merchants are beginning to explore Bitcoin. One of the first major online retailers to accept bitcoins, Overstock.com, made more than $124,000 in bitcoin sales on January 10, 2014, its first day of accepting the currency. By March 2014, Overstock.com had topped $1 million in bitcoin purchases. The company has revised its bitcoin revenue projection for 2014 from an initial $3–5 million to $20 million.[6] According to Overstock.com, Bitcoin's popularity and its low fee structure drove new consumers to its marketplace. More large-scale merchants and mainstream actors in the global economy are following suit. SecondMarket, an online marketplace for buying and selling illiquid assets such as venture-backed private-company stock, is opening a Bitcoin trading platform for institutional investors.

One of the first major online retailers to accept bitcoins, Overstock.com, made more than $124,000 in bitcoin sales on January 10, 2014, its first day of accepting the currency.

Bitcoin: Beyond money

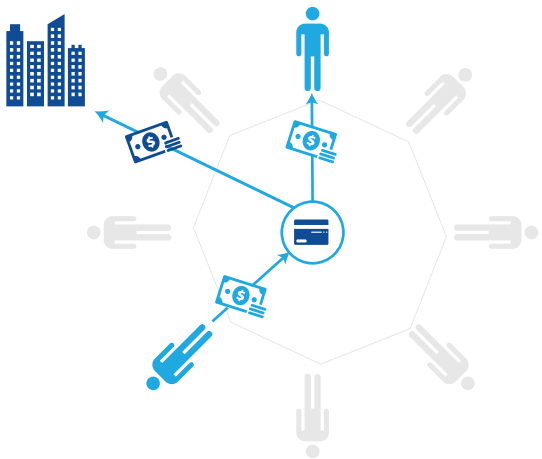
BITCOIN is more than a new currency. Bitcoin and other virtual currencies are creating a new architecture for exchanging information over the Internet that is peer to peer, open yet secure, and nearly frictionless. Imagine how other systems that rely on intermediaries, such as property transfer, contract execution, and identity management, could be disrupted by a similarly open peer-to-peer system.

System of payment

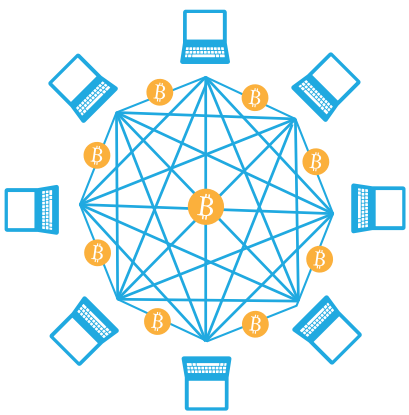
Bitcoin reduces friction in payments. Currently, when an individual transfers funds, he or she must work with a third party. This intermediary, such as a credit card or payments company, often exacts high fees. For example, for remittances, there is an average fee of 9 percent, with some banks charging an additional fee of up to 5 percent for turning the remittance into cash.[7]

Bitcoin allows for a direct payment to anyone, anywhere in the world, at any time (figure 2). With Bitcoin, an individual could transfer value to his or her cousin in India without paying a fee to a global money transmitter or a bank for the wire transfer. Though most uses of Bitcoin to make payments will rely on third parties, like Coinbase, Bitcoin may allow these companies to charge lower fees than they do today. This could disrupt the global remittance market, valued at $514 billion in 2012, by providing a less expensive method for direct transfers globally.[8] Current providers may be forced to lower fees or be replaced by entrants like BitPesa, a mobile payment application for Bitcoin in the developing world.

Figure 2. Payment process: Current versus Bitcoin



Current payment systems require third-party intermediaries that often charge high processing fees ...



... but machine-to-machine payment using the Bitcoin protocol could allow for direct payment between individuals, as well as support micropayments.

Graphic: Deloitte University Press | DUPress.co

ADDITIONAL USE CASES FOR BITCOIN IN THE PAYMENT SPACE INCLUDE:

- **Banking services in developing countries.** Developing countries with appropriate mobile phone infrastructure may be able to leapfrog the developed world in the maturation of mobile finance. As a form of electronic banking, Bitcoin could be an avenue for financial inclusion in emerging markets.
- **Micropayments.** A micropayment is a very small financial transaction that occurs online. Practical systems to allow for the transfer of $1 or less online with a credit card do not exist. Bitcoin could facilitate the direct payment to musicians for individual songs or the ability to "tip" individuals on Twitter, Reddit, or other social media platforms. It could also be used for newspapers and other content producers looking for new revenue models.

In the same way that Bitcoin lowers transaction costs for remittances, it could also lower transaction costs for everyday purchases of low-margin items. Today, if someone buys a donut with a credit card, the merchant pays an interchange fee to the credit card issuer. This interchange fee is usually a small flat amount (10–20 cents) plus a percentage of 1–3 percent.[9] For a low-margin good like a donut, a 10- to 20-cent flat fee can approach 100 percent of the cost of goods. This interchange fee is often passed on to the customer. Using Bitcoin, the transaction fee could be lowered to as little as 1 percent.[10] This could ultimately evolve into a new payment system for credit card companies and banks.

Transfer of property

The Bitcoin protocol could simplify complex asset transfers, revolutionizing the services that support this industry (figure 3). Currently, the transfer of large assets requires significant time and resources. For example, in order to purchase a car from an individual seller, one has to engage a third party to transfer the title. Additionally, one has to use services to learn about the car's accident and inspection history. And who doesn't like to spend a Saturday at the Department of Motor Vehicles updating a car registration?

The block chain, Bitcoin's public ledger, could change all of this. Bitcoins can be qualified in such a way that they represent real-world assets. Bitcoin entrepreneurs at companies like Colored Coin are already working on ways to use small portions of Bitcoin to denote physical property. A fraction of a Bitcoin would publicly identify who currently owns that property, and could include a record of both past ownership and other history about the property. When purchasing a car, one would be able to verify all accidents and inspections over the block chain and transfer the title on site. Similarly, real estate and financial instrument transactions could all be executed over Bitcoin or a similar protocol.

This could soon create efficiencies and reduce friction by allowing individuals to directly transfer property without the use of a broker, lawyer, or notary to sign off on the transfer.

Execution of contracts

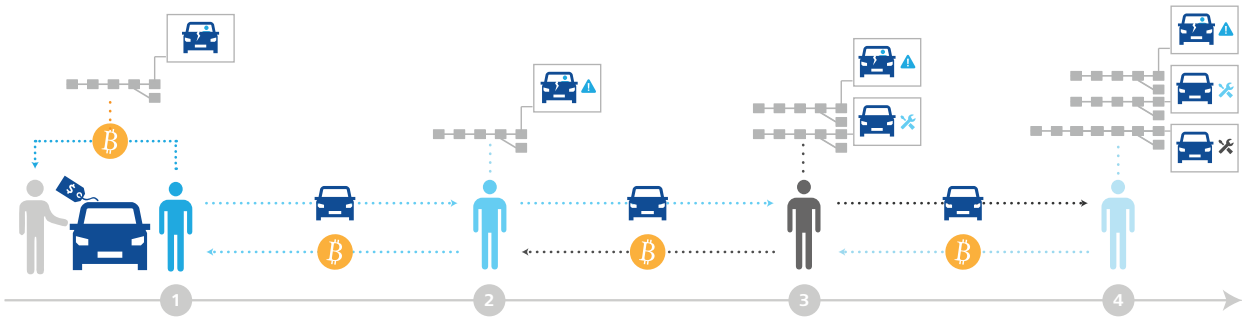
Bitcoin could similarly be used to structure contracts, bringing new efficiency and transparency to the process (figure 4). Contracts are typically developed by lawyers on a case-by-case basis, with significant time and resources devoted to negotiation, development, and enforcement. Additionally, markets based on contracts, including certain financial derivatives markets, lack transparency, which complicates regulation.

Traditional contracts could be replaced by code that self-executes when a triggering event occurs. In a simple example, a financial

instrument, like an option, could be developed and executed over the block chain. In addition to reducing legal fees, this could bring new transparency to financial markets, as regulators could use the public ledger to understand the market without forcing individual actors to reveal their specific positions. It is possible that new crypto-currencies will emerge to serve these niche purposes.

New ventures, like Ethereum, are creating these capabilities today. Ethereum is developing a network to serve as both the registry and

Figure 3. Individuals transfer property over the block chain, providing visibility into property ownership and history



Person A purchases a car from a dealer. That car is represented in the block chain by a bitcoin, allowing the purchaser to view the car's history in the public ledger.

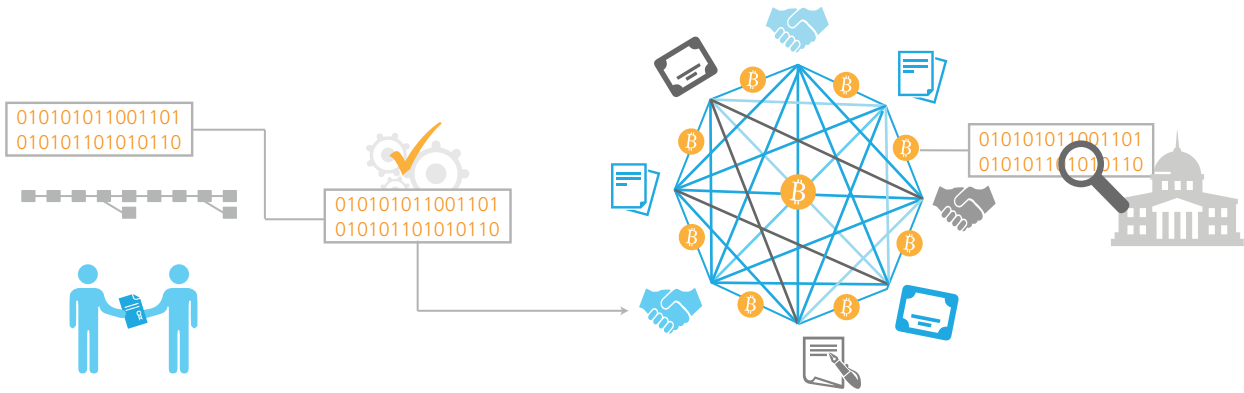
Person B purchases the car from Person A and learns the car was in an accident by reviewing the car's history in the block chain.

Person C purchases the car from Person B and learns the car was serviced regularly and there was an accident by reviewing the car's history in the block chain.

Person D purchases the car from Person C and reviews the car's history in the block chain to learn about the accident, service history, and recent work that was done on the car to pass an emissions test.

Graphic: Deloitte University Press | DUPress.com

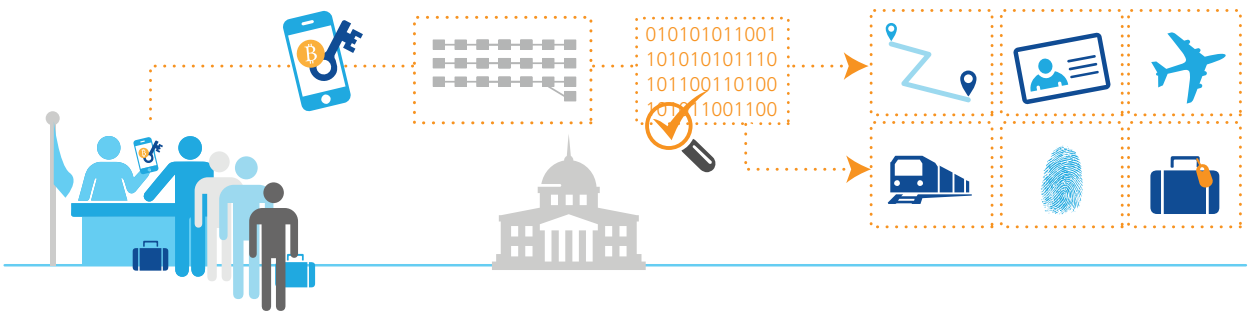
Figure 4. Using the block chain, Bitcoin-based contracts could enhance transparency while maintaining the anonymity of the individuals directly involved



1. An option contract between parties is written as code into the block chain. The individuals involved are anonymous, but the contract is in the public ledger.
2. A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.
3. Regulators can use the block chain to understand the activity in the market while maintaining the privacy of individual actors' positions.

Graphic: Deloitte University Press | DUPress.com

Figure 5. Regulators can be sure of the location of citizens abroad through cryptographically secure identity management on the block chain



Graphic: Deloitte University Press | DUPress.com

escrow to execute the conditions of a contract automatically through rules that can be checked by others.

Identity management

Bitcoin's cryptography and block chain could also transform identity management. Much of identity management, including passports, still operates on a paper-based system. These documents are frequently forged and stolen. Interpol's database currently lists 39 million stolen travel documents. But what if there was a way to create a unique, verifiable key that was impossible to forge?

A cryptographic network similar to but separate from Bitcoin could be used to verify individuals' identities and monitor movement across borders (figure 5). When a person travels through a checkpoint at a border crossing, instead of showing and scanning a paper passport, he or she could present his or her Bitcoin key. A network privately maintained by the government, a contractor, or other entity could verify the key and register the entry into the ledger. This system, based on cryptography instead of paper documents, would simultaneously increase mobility and security. If Bitcoin can be used for travel documents, it could also be used for other forms of identity management like social security numbers, tax identification numbers, or even driver's licenses.

Property, contracts, and identity management are only a few examples of how a peer-to-peer, open, and frictionless system could change business in the future. In order to achieve this wider adoption, Bitcoin will need to address significant questions around trust, ease of use, and operability. To date, the Bitcoin community has shown remarkable adaptability and it is already working to mitigate these problems. In the next decade, we can expect significant innovation around the Bitcoin network. Though much of that will revolve around payments, particularly early on, the evolution of Bitcoin could take several diverging paths.

Future of Bitcoin

MANY factors will influence Bitcoin's evolution, including regulation, technological innovation, and economic conditions. Predicting the future of Bitcoin today resembles what it must have been like to try to comprehend the significance of the Internet in the 1990s. Some experts, such as Ray Kurzweil in his book *The Age of Intelligent Machines*, first published in the late 1980s, got it spectacularly right. But others, like Paul Krugman, who in 1998 predicted that the Internet's impact on the economy would be no greater than the fax machine's, were dead wrong, though for understandable reasons.[11] Timelines for the adoption and extension of new technologies are inherently unpredictable, primarily because their ultimate impact will be a result of how humans interact with them.

Bitcoin's future can best be understood by considering four scenarios that represent a range of possible outcomes.

"Life on the fringe"

"Investors flee Bitcoin as another exchange collapse sends bitcoin prices plummeting"

Bitcoin, the currency, never solves its trust and security problems, reinforcing price volatility and skepticism. It remains an arena for illegal activity and speculation. As a result, companies in the Bitcoin ecosystem are unable to enter into mainstream commerce. Exchange collapses and sales of illicit goods and services continue to occur. The majority of bitcoins are held by speculators, crowding out users who want to use the protocol to make legitimate purchases. Bitcoin and its imitators resemble penny stocks instead of a payment system. In short, the focus on bitcoin's obstacles as a currency prevent the benefits of the technology from being fully realized.

How you can tell if this scenario is happening:

- Another exchange meltdown, security breach, or operational failure occurs
- Volatility continues to be 10 to 15 times higher than traditional assets such as gold[12]
- Bitcoin suffers a flash crash

Why this scenario might not happen:

- The Bitcoin community solves the trust and security problems related to bitcoin as currency
- Bitcoin as technology overwhelms the reservations about bitcoin as currency by creating new offerings and markets

What government's role could be:

- Issue guidance and regulations on Bitcoin as a currency and as a technology, signaling that both aspects can be taken seriously
- Focus on enforcement for illicit activity, like money laundering
- Create safeguards to protect mainstream consumers from being victimized by Bitcoin wallet and exchange scams

"CorporateCoin"

"Payment card companies compete to offer low-fee Bitcoin-based payment options"

Payment and technology companies incorporate the Bitcoin protocol into their payment systems. These companies build proprietary payment platforms using cryptography for security and the block chain for transaction validation. Bitcoin moves to the back office and becomes invisible to the consumer in the same way that different Internet protocols are invisible to most web users. As a result, payments occur across the Bitcoin protocol, but consumers are not required to hold bitcoins. This drives down fees for payment cards and eliminates exchange risk. In short, the Bitcoin protocol grows as a money technology, is adopted by mainstream institutions, and begins to serve as the backbone of many Internet transactions.

How you can tell if this scenario is happening:

- Services offered by traditional payment solutions, like credit and fraud protection, are provided around Bitcoin
- A new wallet technology is introduced in the form of a Bitcoin payment card

Why this scenario might not happen:

- Large payment companies lower fees to match Bitcoin without adopting its protocol
- Corporations continue to distrust open-source technology

What government's role could be:

- Enable companies to use Bitcoin as a payment mechanism through tax and financial crimes enforcement guidance
- Encourage payment companies to use the Bitcoin protocol to offer low-fee solutions for underbanked populations

"Satoshi for all"

"Regulators rescue Wall Street after block chain exposes new market risk"

Bitcoin becomes the protocol for all transfers of value, creating new visibility into financial markets and transforming the services around these functions. Exchanges of value and information, such as property transfer, contract execution, and identity management, are all performed on the block chain. As a result, the services that support these functions are revolutionized. Professionals like traders and lawyers focus on writing code and maintaining the block chain. The process of regulation is changed as well. Regulators download the ledger for a market, such as commodities, every day. Bitcoin's pseudonymity allows regulators to understand the risk of entire markets, while still maintaining the privacy of individual actors. The government creates the Block Chain Administration to oversee cryptographic exchanges and provide consumer protection. In short, all transfers of value are executed in a peer-to-peer and open, yet secure way, reducing fees and increasing transparency.

How you can tell if this scenario is happening:

- A piece of physical property is exchanged over the block chain
- Financial instruments, such as options, are created and traded over the block chain
- A Bitcoin-based central clearinghouse is launched

Why this scenario might not happen:

- Economic path dependence on current systems prevents such significant disruption
- Stakeholder interests challenge adoption
- A Bitcoin programming skills gap expands as the demand for programmers increases

What government's role could be:

- Provide consumer protection and education
- Regulate block chain-based transfers, providing standardization, security, and enforcement

"New networks"

"Number of individuals working 15 or more jobs reaches 10 percent of US population"

Two key attributes of Bitcoin enable a transition to a new model of work and employment. First, Bitcoin's utility in facilitating micropayments allows people to more easily receive compensation for the many tasks they perform as part of a digital network. Second, and perhaps even more important, is that Bitcoin is a self-propelling, decentralized, peer-to-peer network that allows its members to derive both income and utility from their participation. Today's technology services, like email and social media networks, provide utility to users free of charge and generate income for owners. But as the saying goes, if you're getting something for free, you aren't the customer, you're the product. In a Bitcoin world, users are both the customer and the product, because individuals participate in the Bitcoin network by both exchanging the currency and validating the transactions. Currently, at the average day job, a person may spend eight hours at her desk and be paid an income for that one role. In addition, he or she is tweeting, reading news articles, and checking out blogs, generating valuable data throughout the entire day. In the future, we could engage in these same activities and get paid for all of them as Bitcoin enables payment for the myriad activities individuals perform as part of a networked economy.

How you can tell if this scenario is happening:

- Mainstream online media sites reward commenters for input
- A public technology company accounts for user income on its 10-K

Why this scenario might not happen:

- This is a major departure from our current employment model
- Achieving this scenario requires technological savvy on a larger scale than exists today

What government's role could be:

- Adjust definition of employment to include this new type of work
- Refocus taxation and other policies to stimulate this new type of work
- Tap into the new labor pool created by this employment model

These scenarios lie within the realm of the possible. Though the first scenario is closest to the status quo, current trends may indicate that the second scenario is possible in the near term, which may lay the groundwork for the seemingly more distant scenarios. Certainly, some skeptics argue that Bitcoin will be the Esperanto of finance.[13] But, others are intrigued by Bitcoin's potentially more revolutionary impact. As Kevin Kelly, co-founder of *Wired*, writes in his latest book *New Rules for the New Economy*, "The great benefits reaped by the new economy in the coming decades will be due in large part to exploring and exploiting the power of decentralized and autonomous networks."[14] Bitcoin is an early example of this future.

Given the spectrum of possible scenarios, the range of actions available to governments and businesses is broad. Some foreign governments have tried to ban Bitcoin by making the exchange of cash for bitcoins illegal. Others have taken a "wait and see" approach, allowing the ecosystem around Bitcoin to develop while closely monitoring it. In the United States, government agencies have begun to

issue taxation and other guidance, paving the way for entrepreneurs to create a new wave of Bitcoin-related companies and large corporations to engage in the Bitcoin economy.

Bitcoin is yet another example of how new technologies and trends can pop up seemingly out of nowhere, creating problems and opportunities for government as it sorts out how to respond. Most governments chose a hands-off approach to the Internet when it emerged in the 1980s. But the lessons of the Internet should be fair warning that these new technologies can come out of nowhere and change everything. Bitcoin's direct relevance to traditional government domains, such as currency and taxes, merits specific consideration. Given its broad potential impact on activities from contracts to identity management, agencies tasked with diverse operations, from financial markets oversight to border patrol, need to monitor Bitcoin's evolution. Governments need to understand how Bitcoin will evolve in the short term. But even more importantly, they need to explore how the concepts underlying this new technology could intersect with their mission in the future.[15]

Endnotes

1. Doge is a slang term for "dog" that is primarily associated with pictures of Shiba Inus (nicknamed "Shibe") and internal monologue captions on Tumblr. These photos may be altered to change the dog's face or captioned with interior monologues in Comic Sans font.
2. Blockchain, "Bitcoin charts," https://blockchain.info/charts, accessed June 4, 2014.
3. Staci Warden, "Bitcoins: Currency of the future?," presented at The Impact Lab, Georgetown University Beeck Center, April 10, 2014.
4. Blockchain, "Number of transactions," http://blockchain.info/charts/n-transactions, accessed June 4, 2014.
5. Visa, Inc., *VisaNet: The technology behind Visa, 2013*, pp. 2-5, http://usa.visa.com/download/corporate/_media/visanet-technology/visa-net-booklet.pdf, accessed June 4, 2014.
6. John Southurst, "Overstock CEO Patrick Byrne to keynote Bitcoin 2014 conference," *CoinDesk*, March 25, 2014, http://www.coindesk.com/overstock-ceo-patrick-byrne-keynote-bitcoin-2014-conference/, accessed June 4, 2014.
7. Joshua Brustein, "Will migrant workers drive Bitcoin's mundane future?" *Bloomberg Businessweek*, October 8, 2013, http://www.businessweek.com/articles/2013-10-08/will-migrant-workers-drive-bitcoins-mundane-future, accessed June 4, 2014.
8. Saifur Rahman, "Global remittance flow grows 10.77% to $514 billion in 2012: World Bank," *Gulfnews.com*, April 20, 2013, http://gulfnews.com/business/economy/global-remittance-flow-grows-10-77-to-514-billion-in-2012-world-bank-1.1172693, accessed June 4, 2014.
9. Visa, Inc., "Visa U.S.A. interchange reimbursement fee," http://usa.visa.com/download/merchants/visa-usa-interchange-reimbursement-fees-april2013.pdf, last modified April 20, 2013.
10. Jason Del Rey, "Stripe merchants will soon be able to accept Bitcoin payments," *Re/Code*, March 27, 2014, http://recode.net/2014/03/27/stripe-merchants-will-soon-be-able-to-accept-bitcoin-payments/, accessed June 4, 2014.
11. Paul Krugman, "Why most economists' predictions are wrong," *Red Herring*, June 10, 1998, http://web.archive.org/web/19980610100009/www.redherring.com/mag/issue55/economics.html.
12. Eli Dourado, "The Bitcoin volatility index," http://btcvol.info/, last modified May 31, 2014.
13. Stephanie Baker, "Bitcoin bets feed Twitter dreams as regulators circle," *Bloomberg*, October 2, 2013, http://www.bloomberg.com/news/2013-10-02/bitcoin-bets-feed-twitter-dreams-as-regulators-circle.html, accessed June 4, 2014.
14. Kevin Kelly, "Maxims for the network economy," http://kk.org/newrules/selected_maxims.php, accessed June 4, 2014.
15. Selections of this paper previously appeared in a *Harvard Business Review* blog authored by Tiffany Wan and Max Hoblitzell, published on April 24, 2014. The blog post can be accessed here: http://blogs.hbr.org/2014/04/bitcoins-promise-goes-far-beyond-payments/.

About GovLab

GovLab is a think tank in the Federal practice of Deloitte Consulting LLP that focuses on innovation in the public sector. It works closely with senior government executives and thought leaders from across the globe. GovLab Fellows conduct research into key issues and emerging ideas shaping the public, private, and nonprofit sectors. Through exploration and analysis of government's most pressing challenges, GovLab seeks to develop innovative yet practical ways that governments can transform the way they deliver their services and prepare for the challenges ahead.

Contact

Carmen A. Medina
Specialist Leader
Deloitte Consulting LLP
+1 703 340 5119
camedina@deloitte.com

Tiffany A. Wan
Senior Consultant
Deloitte Consulting LLP
+1 202 999 8889
twan@deloitte.com

Max Hoblitzell
Consultant
Deloitte Consulting LLP
+1 202 997 8012
ahoblitzell@deloitte.com

 Follow @DU_Press

Sign up for Deloitte University Press updates at DUPress.com.

About Deloitte University Press

Deloitte University Press publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte University Press is an imprint of Deloitte Development LLC.

About this publication

About Deloitte

CoinDesk

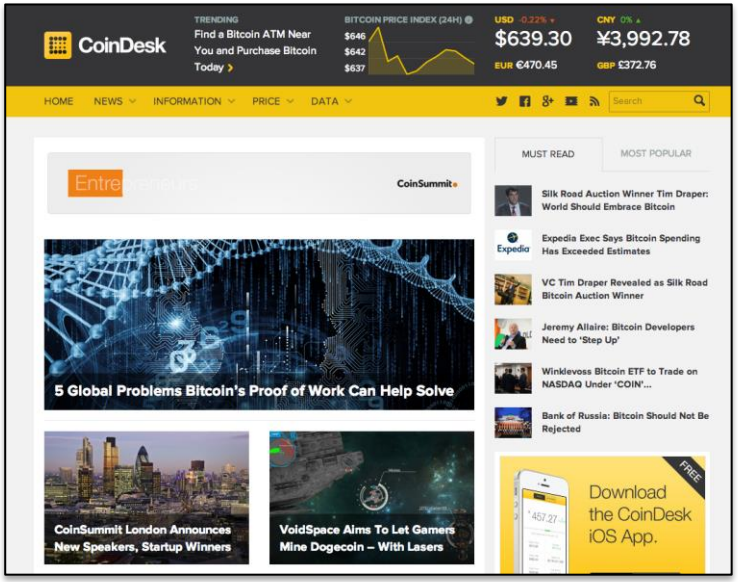
State of Bitcoin Q2 2014

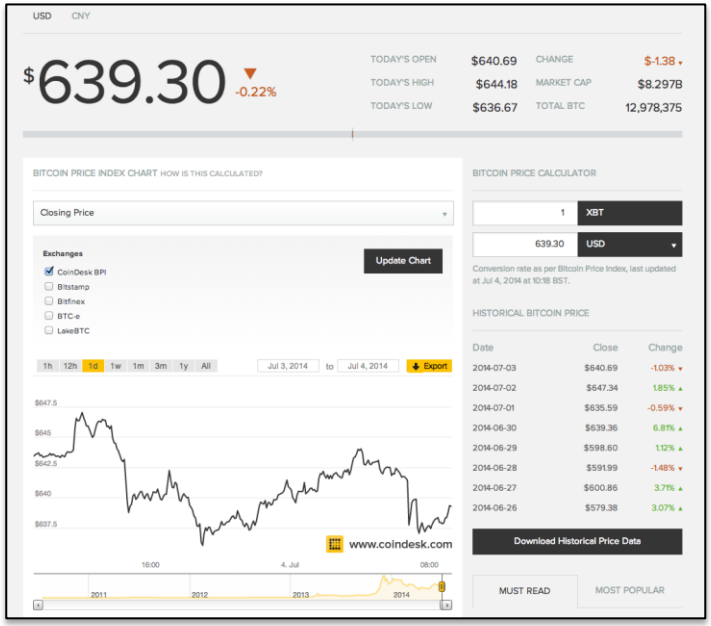
Presented 10th July 2014 at CoinSummit London

Contents

About CoinDesk

- World leader in digital currency news, prices and information
- Our Bitcoin Price Index serves as an industry reference point
- London-based and remote team with a global focus
- Our editors are based in London, Boston, San Francisco, and Tokyo





Q2 2014 Summary

Bitcoin's price has bounced back: up 39.4% from end of Q1 but still down 16% from start of year

Stories mentioning 'bitcoin' in the mainstream media rose 439% from 2012/13 to 2013/14

All-time bitcoin VC investment of $240m; 2014 run rate of $280m+

Approximately 63,000 business now accept bitcoin; 5.3m total wallets

Larger, more established consumer brands are adopting bitcoin (eg Dish, Expedia)

Regulatory environment continues to see positives (eg California) and setbacks (eg Bolivia)

Key Bitcoin Adoption Metrics

Commerce	**Jun-14**	**Jun-13**	**YoY Δ**
Wallets	5,327,688	765,039	7x
Merchants	63,000	N/A	N/A
ATMs	103	N/A	N/A
Unique bitcoin addresses used per day	136,152	41,271	3x
Media			
Mentions in mainstream media	9,500	2,163	3x
Technology			
Network hash rate (billion/second)	111,194,683	162,269	685x
Github No. of updated repositories	12,365	676	17x
Investment			
Bitcoin market capitalization ($bn)	8.3	1.0	8x
Industry			
VC investment over last 12 months ($m)	200.7	17.1	12x
Number of VC-backed startups	48	7	7x

Price and Valuation

Four of the Most Popular CoinDesk News Stories in Q2 2014 About Bitcoin's Price

Story	Date
1. CEO of Bitcoin Official Bans China [April Fools' article]	1st Apr
2. List of Possible Silk Road Bitcoin Bidders Leaked by US Marshalls	18th Jun
3. Why Bitcoin's Price Has Leapt 64% Since April	28th May
4. New Colorado Marijuana Vending Machines Will Accept Bitcoin	16th Apr
5. Renewed Optimism as Bitcoin Price Nears $500	20th May
6. Bitcoin Price Drops 10% as Chinese Exchanges Stop Bank Deposits	10th Apr
7. Mark T. Williams to Bitcoin Bulls: Time Will Vindicate My Prediction	31st May
8. 500 Million Dogecoins Mined by Unknown Hacker in Malware Attack	17th Jun
9. Bitcoin Price Falls Below $600 as Govt. Prepares for 30,000 BTC Selloff	13th Jun
10. Is it Too Late to Get Involved in Bitcoin?	26th Apr

CoinDesk Bitcoin Price Index – Q2 & YTD 2014 by the Numbers

Q2 Price Summary

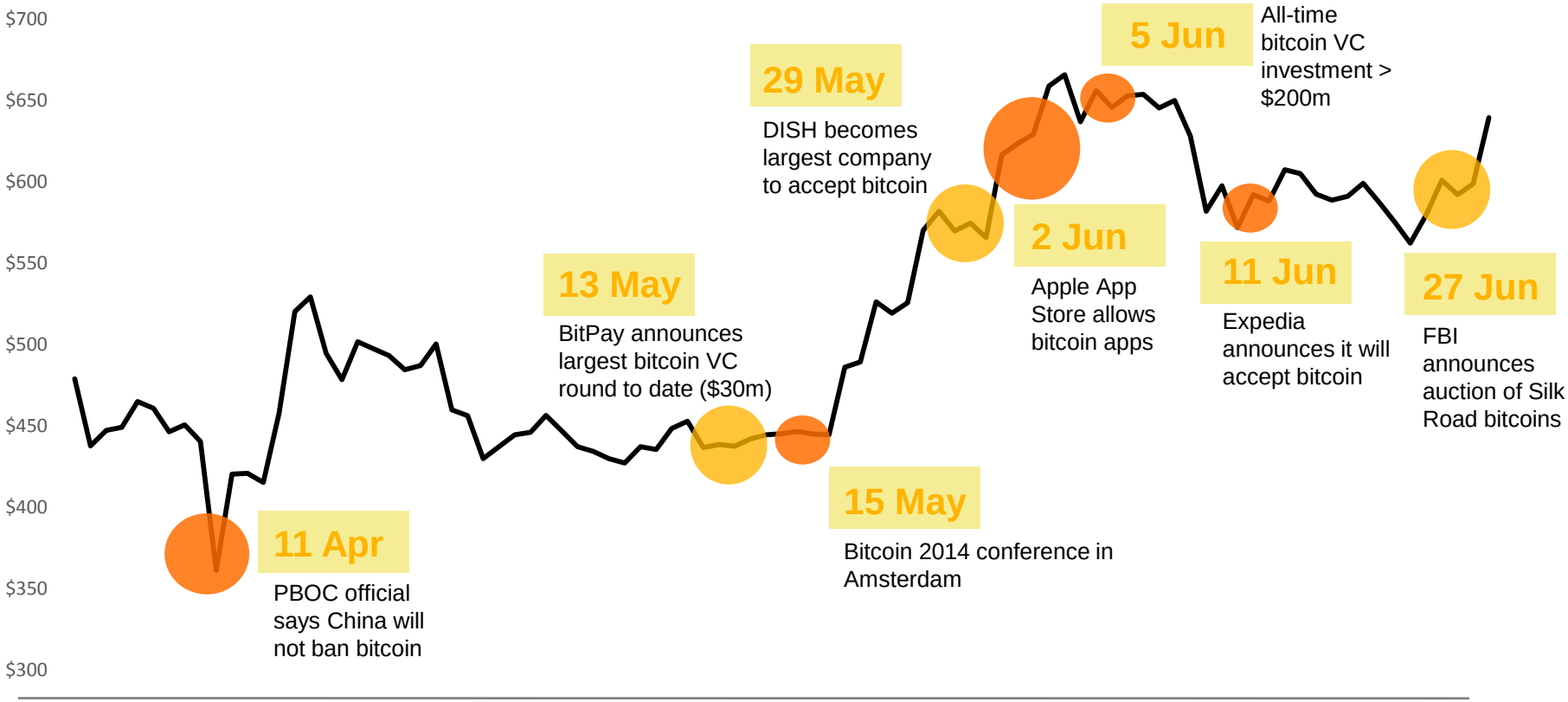
Q2 2014 Open	$458.50
30 June Price	$639.36
Q1/Q2 % Δ	+39.4%
30 June Market Cap	$8.3bn

YTD Price Summary

High (6th Jan)	$951.39
Low (10th April)	$360.84
YTD % Δ	-15.6%
Average	$611.31
Median	$591.99

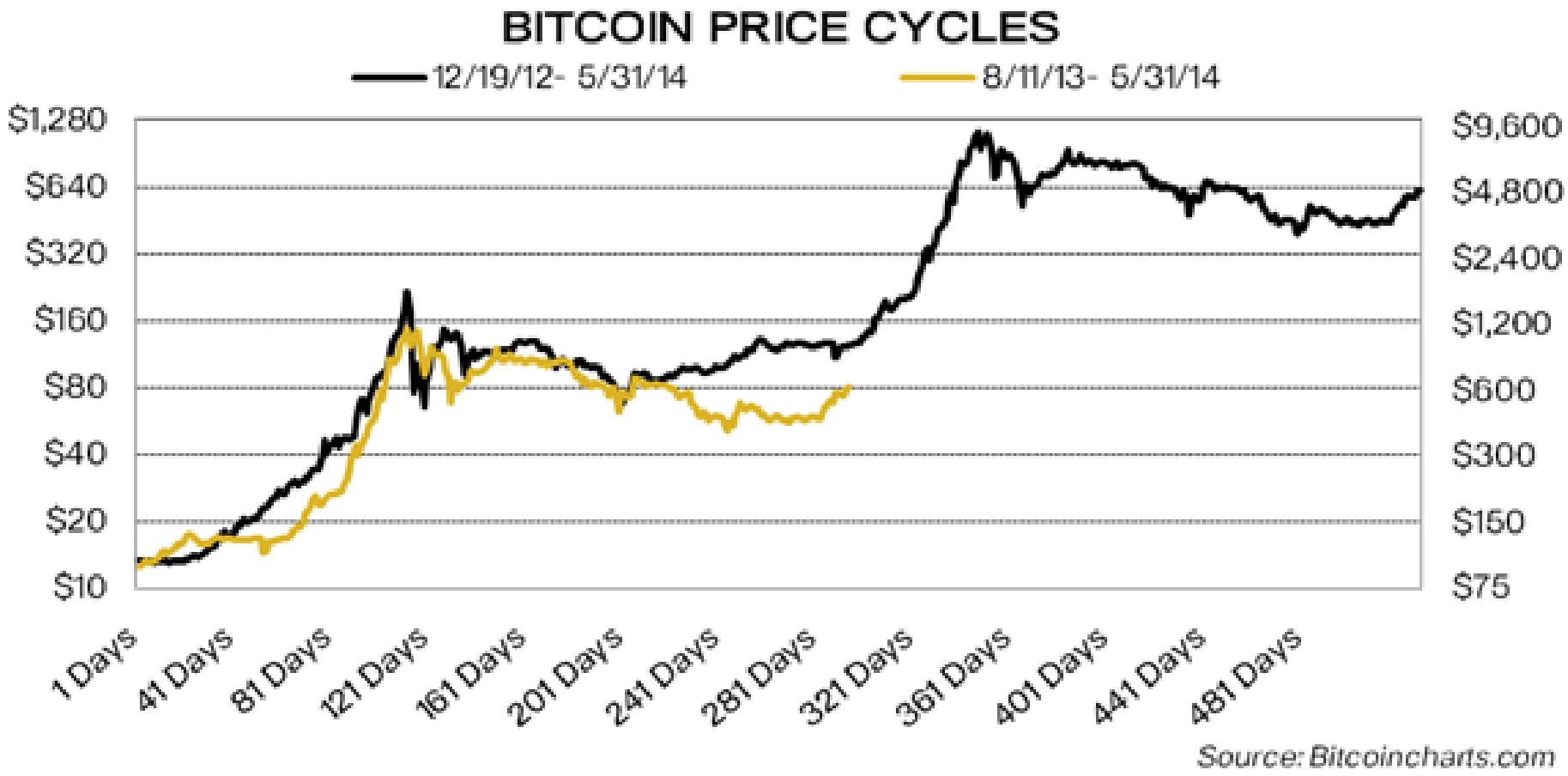
Source: CoinDesk Bitcoin Price Index, daily data collected at 00:00 UTC

Significant Bitcoin Events and Price Response – Q2 2014



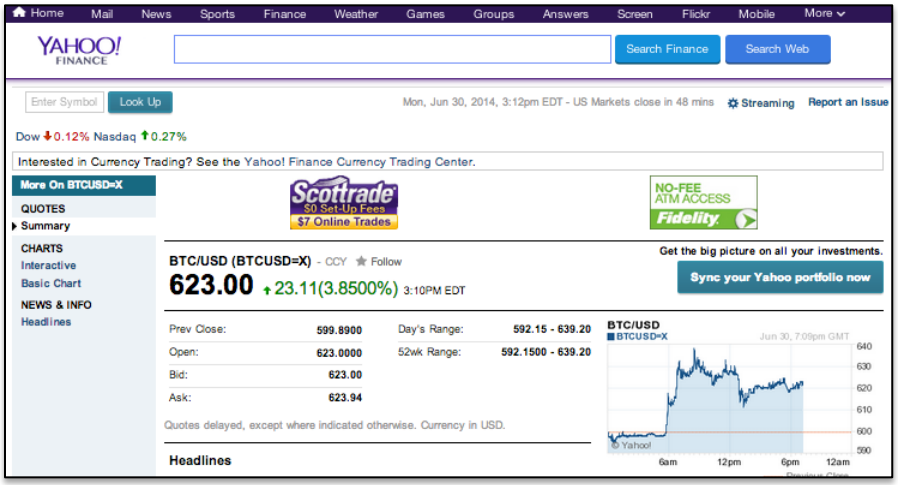
Source: CoinDesk Bitcoin Price Index daily closing price (taken at 00:00 UTC)

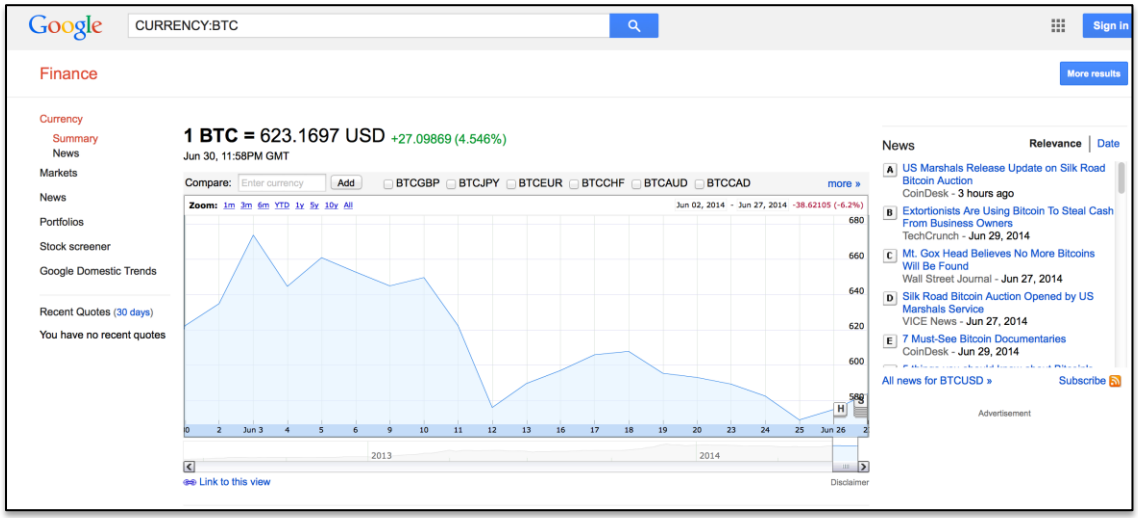
If Recent Bitcoin Price Trends Continue Following Historical Pattern, Then Further Upside is Anticipated



Source: Pantera Capital

Bitcoin's Price is Now on Yahoo Finance, Google Finance and Bloomberg





Bitcoin Now Represents 93.4% of Total Cryptocurrency Market Cap, +3.4% Change from 16th April

1	Bitcoin	$ 8,485,563,727	$ 654.31
2	Litecoin	$ 265,848,755	$ 8.92
3	Nxt	$ 61,415,955	$ 0.061416
4	Darkcoin	$ 39,333,058	$ 8.88
5	Ripple	$ 29,976,139	$ 0.003834
6	Peercoin	$ 29,827,098	$ 1.39
7	Dogecoin	$ 22,111,831	$ 0.000260
8	Namecoin	$ 15,696,694	$ 1.71

Bitcoin market cap 35x larger than litecoin, up from 18x two months ago

Market capitalizations:

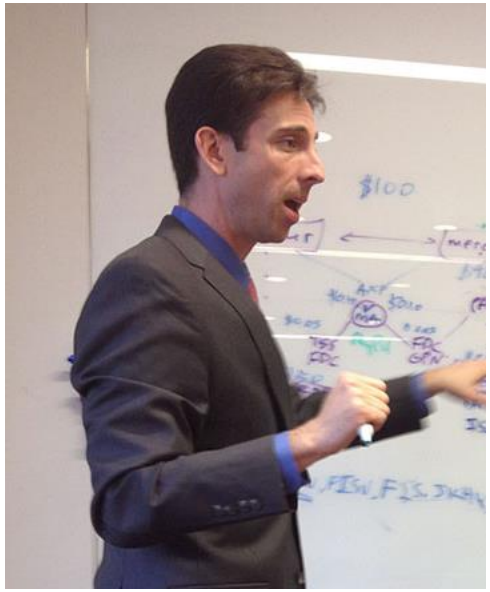
$8.5bn – bitcoin
(Δ of +31% from 16th April)

$9.1bn – all cryptocurrencies
(Δ of +28% from 16th April)

Source: CoinMarketCap.com 1 July 2014

The Timing and Scale of Bitcoin's Disruptive Potential

- "Bitcoin-related technologies will disrupt payments markets and other trust-based markets within the next few years and for decades to follow."
- "US bank fees generate $250 billion a year and global payments-related revenues exceed $300 billion a year."
- "We also see an emerging bitcoin opportunity within the Internet of Things."



Gil Luria
Wedbush Securities

Fees and Other Financial Services Costs That Could be Impacted by Bitcoin

- Payment processing
- Deposit
- Withdrawal/Overdraft
- Foreign exchange
- Float
- Transfer/Wire
- Title insurance
- Exchange trading
- Escrow
- Trust management
- Collections
- Notary

Source: Wedbush Securities, CoinDesk

$3.4 Trillion, or 21% of US GDP From Trust-Based Service Sectors Could be Impacted

Figure 2: Portion of US GDP from Trust-Based Industries

Value added (Millions of dollars)	2012	2012%
Gross domestic product	16,244,586	*100.0*
Agriculture, forestry, fishing, and hunting	201,138	*1.2*
Mining	429,656	*2.6*
Utilities	275,148	*1.7*
Construction	581,073	*3.6*
Manufacturing	2,034,333	*12.5*
Wholesale trade	962,694	*5.9*
Retail trade	927,849	*5.7*
Transportation and warehousing	471,637	*2.9*
Information	776,740	*4.8*
Finance, insurance, real estate, rental, and leasing	3,172,548	*19.5*
Finance and insurance	1,078,153	*6.6*
Federal Reserve banks, credit intermediation, and related activities	435,033	*2.7*
Securities, commodity contracts, and investments	184,592	*1.1*
Insurance carriers and related activities	413,066	*2.5*
Funds, trusts, and other financial vehicles	45,463	*0.3*
Real estate and rental and leasing	2,094,395	*12.9*
Real estate	1,917,249	*11.8*
Rental and leasing services and lessors of intangible assets	177,146	*1.1*
Professional and business services	1,937,240	*11.9*
Professional, scientific, and technical services	1,140,168	*7.0*
Legal services	225,249	*1.4*
Computer systems design and related services	229,792	*1.4*
Miscellaneous professional, scientific, and technical services	685,126	*4.2*
Educational services, health care, and social assistance	1,339,698	*8.2*
Arts, entertainment, recreation, accommodation, and food services	596,547	*3.7*
Other services, except government	352,014	*2.2*
Government	2,186,268	*13.5*

Sum of Trust-Based Service Sectors	$3,397,798
As a percentage of GDP	*21%*

Source: Bureau of Economic Analysis, Wedbush Securities, Inc.

Total Potential Market Cap Disrupted by Bitcoin of $546bn

Market Caps (millions) as of 1st July 2014

Processors	Market Cap
Visa Inc	$105,228
American Express Co	$100,430
MasterCard Inc	$82,558
Capital One Financial Corp	$47,213
Discover Financial Services	$28,900
Alliance Data Systems Corp	$15,246
Total System Services Inc	$5,928
Global Payments Inc	$5,232
Euronet Worldwide Inc	$2,458
Heartland Payment Systems Inc	$1,477
Green Dot Corp	$753
Total	**$395,422**

Money Transfer/ATM Outsourcing	Market Cap
Western Union Co	$9,345
Euronet Worldwide Inc	$2,458
Cardtronics Inc	$1,516
MoneyGram International Inc	$804
Xoom Corp	$1,001
Total	**$15,124**

Trust/Escrow	Market Cap
M&T Bank Corp	$16,311
Associated Banc-Corp	$2,883
PrivateBancorp Inc	$2,268
Total	**$21,462**

Payment Hardware	Market Cap
NCR Corp	$5,892
MICROS Systems Inc	$5,080
VeriFone Systems Inc	$4,106
Ingenico	$4,802
Diebold Inc	$2,595
Outerwall Inc	$1,210
Wincor Nixdorf AG	$1,895
Agilysys Inc	$316
On Track Innovations Ltd	$79
Total	**$25,975**

Bank Software	Market Cap
Fidelity National Information Services Inc	$15,754
Fiserv Inc	$15,033
Jack Henry & Associates Inc	$5,025
ACI Worldwide Inc	$2,117
Total	**$37,930**

Securities Exchanges	Market Cap
Intercontinental Exchange Inc	$21,753
CME Group Inc	$23,824
NASDAQ OMX Group Inc	$6,591
Total	**$52,169**

Source: Wedbush Securities, CoinDesk

Media

Selection of Q2's Biggest Bitcoin Stories

Apple's App Store allows return of bitcoin apps

Tim Draper successfully bids on 30,000 BTC at Silk Road bitcoin auction

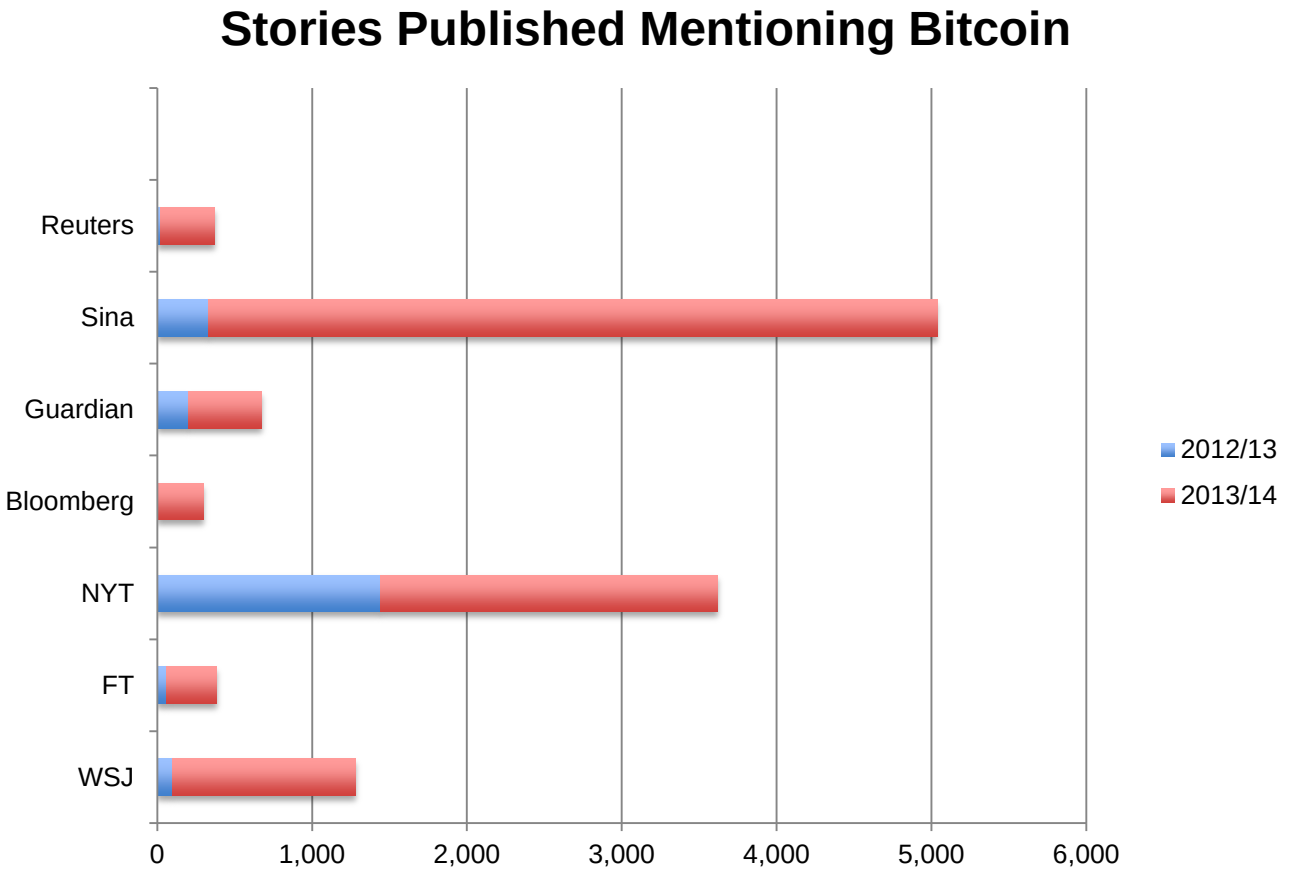
Scale of bitcoin VC investment tracking the early Internet

bitpay

BitFury

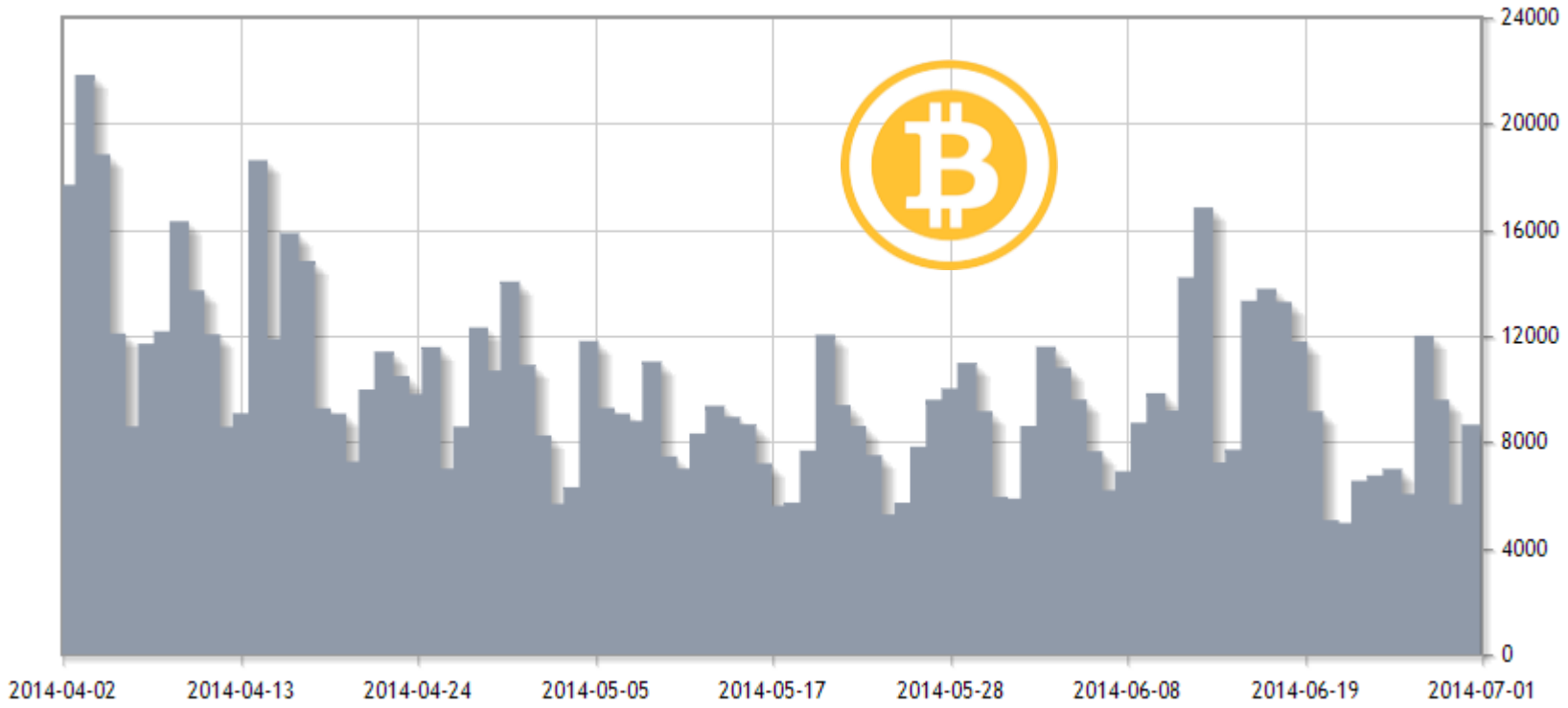
More seasoned entrepreneurs set their sights on bitcoin [Halsey Minor pictured]

Accelerating Mainstream Media Interest in Bitcoin



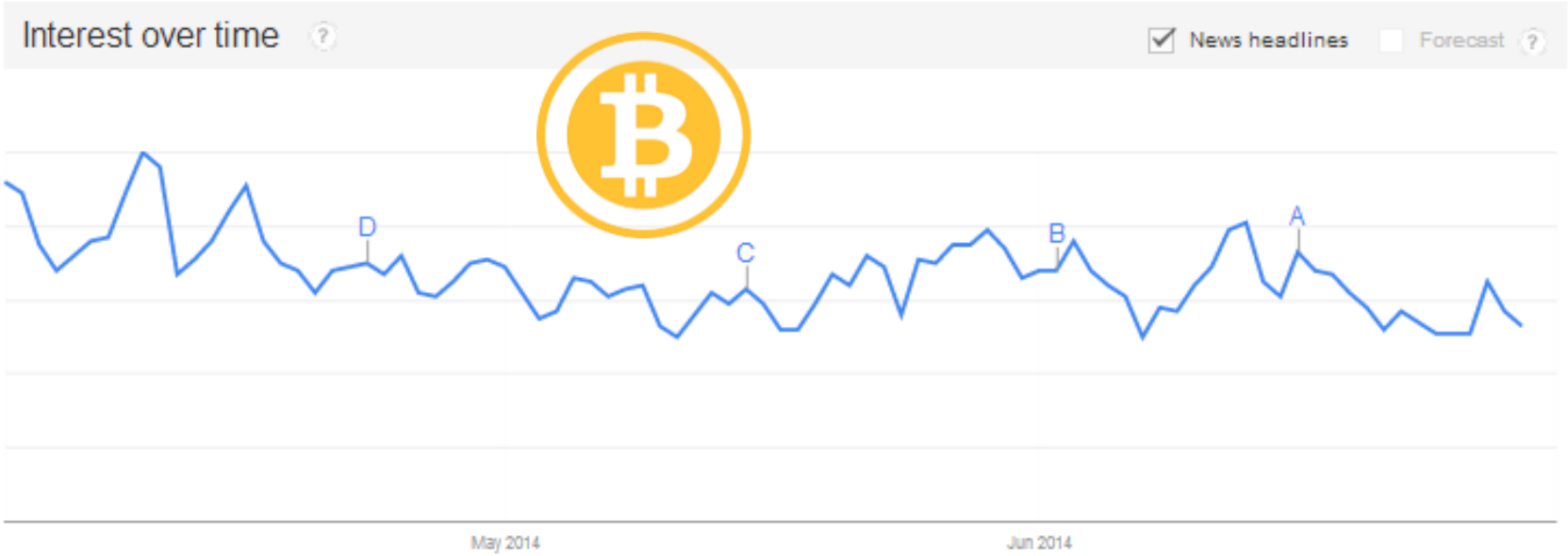
Source: Respective publishers' websites. Date range used is 1st June to 31st May.

“Bitcoin” is the 89th Most Heavily Trafficked Wikipedia Page, 889k Views in Last 90 Days



Source: Wikipedia 1st July 2014

Google Search Interest in “bitcoin” During Q2 Has Remained Relatively Constant



Source: Google Trends

Some Intellectuals Remain Skeptical, While Others Recognize Bitcoin's Potential

Ken Rogoff

"Not a currency; it isn't going to be a currency."

Larry Summers

"I think bitcoin has the potential to be a very, very important development."

Niall Ferguson

"It would be unwise to assume, as some do, that it poses no challenge at all."

Ecosystem and VC Investment

Two Biggest Bitcoin VC Deals in Q2

$30m

(Series A) May 2014

$20m

(Series A) May 2014

Source: CoinDesk (http://www.coindesk.com/bitcoin-venture-capital/)

BitPay's $30m Round was the Largest Bitcoin VC Deal to Date

- More than 30,000 total merchants
- As of January 2014, adding more than 1,000 merchants to its network each week
- Processing $1m in bitcoin payments every day
- Processed more than $100m in bitcoin payments in 2013
- Most recent VC round valued BitPay at $160m

Bitcoin Venture Capital Investment Accelerated in Q2, Up 28% QoQ

Q1 2014 bitcoin VC investment:

$57m

Q2 2014 bitcoin VC investment:

$73m

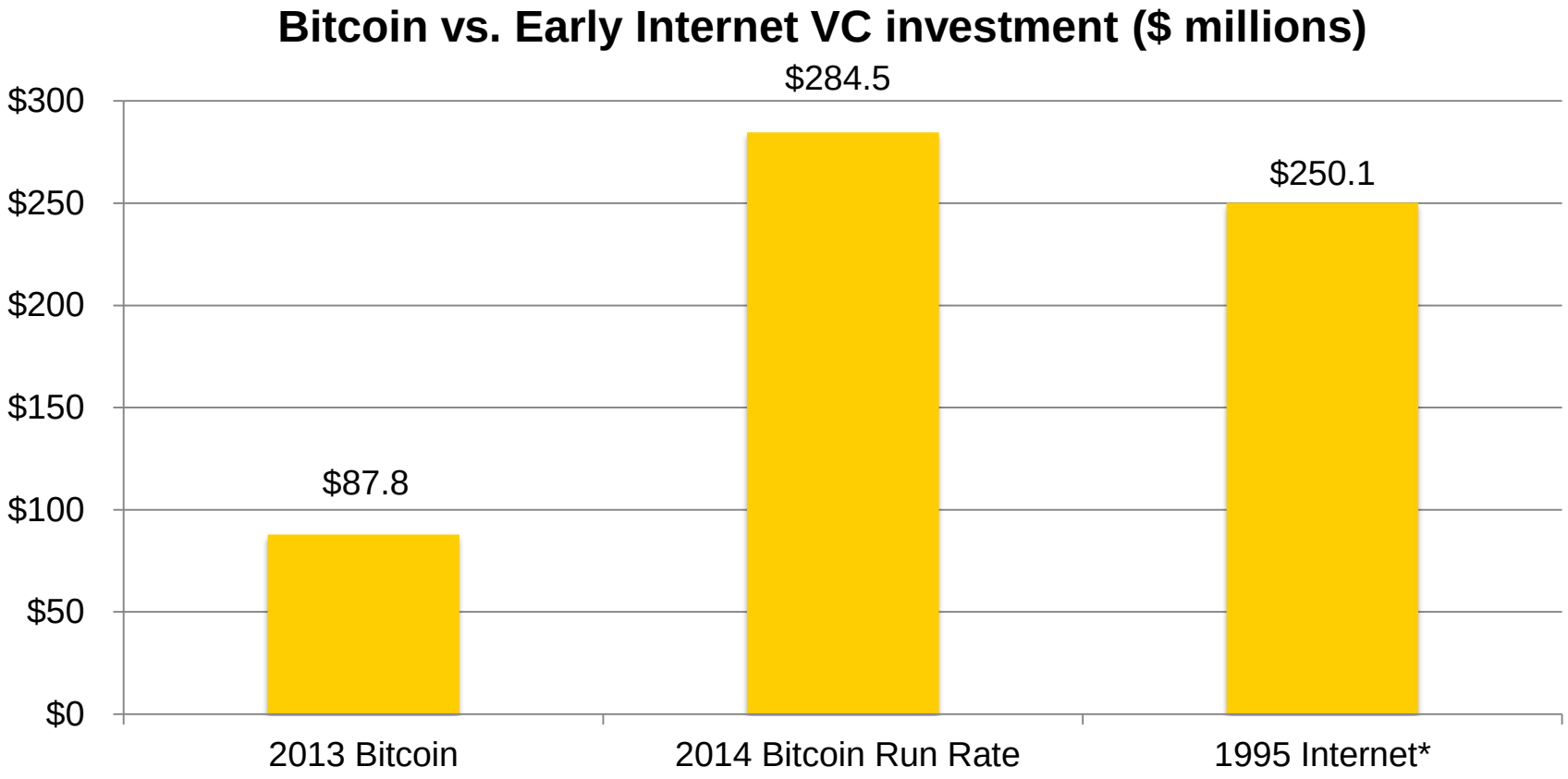
Total VC investment in cryptocurrency startups to date:

$240m

*Note: Q2 figure excludes recent July deals (eg Xapo $20 million) but all-time figure of $240m includes these deals.

Source: CoinDesk (http://www.coindesk.com/bitcoin-venture-capital/)

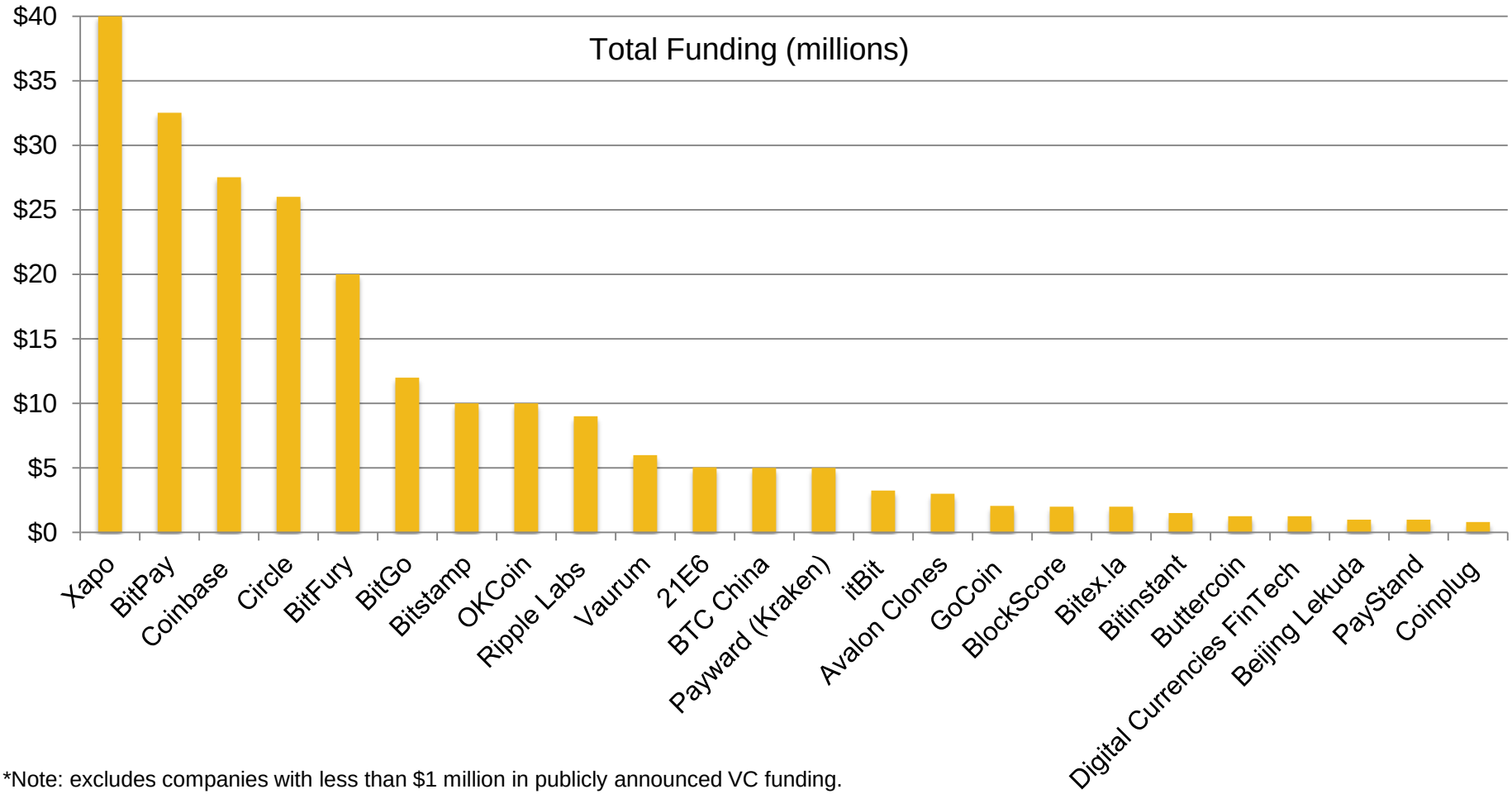
2014 VC Investment in Bitcoin Overtaking VC Early-Stage Internet Investments



Note: *Includes first sequence venture deals but excludes late-stage 1995 internet investments ($257.6m). For additional disclosure on methodology see http://www.coindesk.com/following-money-trends-bitcoin-venture-capital-investment/

Source: CoinDesk, PriceWaterhouse

8 Startups With ≥$10m VC Funding; 22 Startups ≥$1m



*Note: excludes companies with less than $1 million in publicly announced VC funding.

Source: CoinDesk (http://www.coindesk.com/bitcoin-venture-capital/)

2014 YTD Investment in Bitcoin Startups of $150m

Recently Announced Investment Rounds

Close Date	Company	Size ($m)	Round	Select Investors	Headquartered
Jul-14	TBC	0.25	Seed	Individual Investors	TBC
Jul-14	Xapo	20.00	First	Index Ventures, Greylock Partners, Emergence Capital Partners, Yuri Milner, Max Levchin, Jerry Yang	Palo Alto
Jun-14	BlockScore	2.00	Seed	Battery Ventures, Lightspeed Venture Partners, Boost VC, New Atlantic Ventures, Khosla Ventures, Y Combinator	Palo Alto
Jun-14	BitPagos	0.60	Seed	Pantera Capital, Boost Bitcoin Fund, 8capita, South Ventures, NXTP Labs, Tim Draper, Barry Silbert, Individual Investors	Palo Alto
Jun-14	BitGo	12.00	First	Redpoint Ventures, Bitcoin Opportunity Corporation, Radar Partners, Liberty City Ventures, Crypto Currency Partners, A-Grade Investments	San Francisco
Jun-14	HashPlex	0.40	Seed	Barry Silbert, Jason Prado, Individual Investors	Seattle

Source: CoinDesk (http://www.coindesk.com/bitcoin-venture-capital/)

2014 YTD Investment in Bitcoin Startups of $150m

Recently Announced Investment Rounds

Close Date	Company	Size ($m)	Round	Select Investors	Headquartered
May-14	BitFury	20.00	First	Binary Financial, Crypto Currency Partners, Georgian Co-Investment Fund, Queensbridge Venture Partners and ZAD Investment Company, Jonathan Teo, Bill Tai	Amsterdam
May-14	Bitex.la	2.00	First	Undisclosed UK-based investor	Buenos Aires
May-14	BitPay	30.00	First	Index Ventures, AME Cloud Ventures, Felicis Ventures, Founders Fund, Horizons Ventures, RRE Ventures, Sir Richard Branson, TTV Capital	Atlanta
May-14	Vaurum	4.00	Seed	Battery Ventures, Tim Draper, Steve Case	San Mateo

Source: CoinDesk (http://www.coindesk.com/bitcoin-venture-capital/)

2014 YTD Bitcoin VC Investments (contd.)

Close Date	Company	Size ($m)	Round	Select Investors	Headquartered
Apr-14	GogoCoin	0.10	Seed	500 Startups	Mountain View
Apr-14	Bonifide.io	0.10	Seed	500 Startups	Mountain View
Apr-14	Coinalytics	0.10	Seed	500 Startups	Mountain View
Apr-14	Neuroware	0.10	Seed	500 Startups	Mountain View
Apr-14	Monetsu	0.10	Seed	500 Startups	Mountain View
Apr-14	Coinplug	0.40	Seed	Tim Draper	Seoul
Apr-14	PayStand	1.00	Seed	Cervin Ventures, Serra Ventures, Central Coast Angels, TiE LaunchPad	Santa Cruz
Mar-14	Circle Internet Financial	17.00	Second	Breyer Capital, Accel Partners, General Catalyst Partners, Oak Investment Partners, Pantera Capital, Bitcoin Opportunity Fund	Boston
Mar-14	GoCoin	1.50	First	Bitcoin Shop, Owen Van Natta, Crypto Currency Partners	Singapore
Mar-14	Hive	0.19	Seed	Roger Ver, Seedcoin	Hong Kong

Source: CoinDesk (http://www.coindesk.com/bitcoin-venture-capital/)

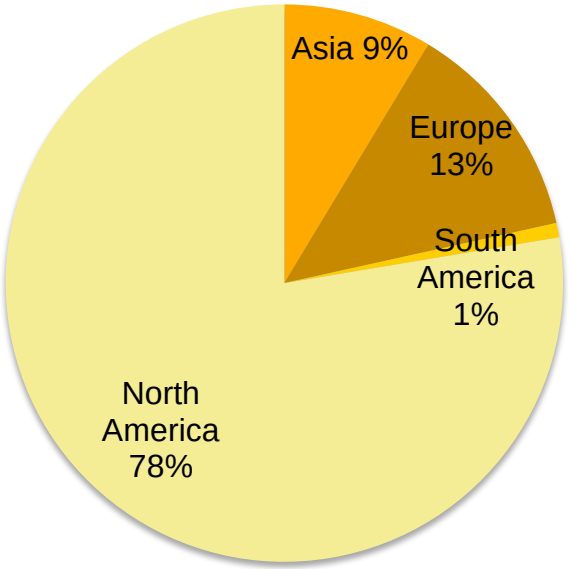
2014 YTD Bitcoin VC investments (contd.)

Close Date	Company	Size ($m)	Round	Select Investors	Headquartered
Mar-14	Payward, Inc. (Kraken)	5.00	First	Hummingbird Ventures	San Francisco
Mar-14	BTC.sx	0.30	Seed	Seedcoin, Joe Lee	Singapore
Mar-14	MexBT	0.34	Seed	Seedcoin, Individual Investors	Mexico City
Mar-14	OKCoin	10.00	First	Ceyuan Ventures, Mandra Capital, VenturesLab	Beijing
Mar-14	Xapo	20.00	First	Benchmark, Fortress Investment Group, Ribbit Capital	Palo Alto
Mar-14	Tembusu Terminals	0.20	Seed	Individual Investors	Singapore
Feb-14	Safello	0.60	Seed	Nicolas Cary, Roger Ver, Erik Voorhees, Ira Miller, Jan Rees, Anders Bruzelius, Victor & Victor	Stockholm
Feb-14	BitSim	0.50	Seed	Seedcoin, Individual Investors	Hong Kong
Feb-14	Cryptopay	0.08	Seed	Seedcoin	London
Jan-14	Tangible Cryptography (BitSimple)	0.60	Seed	Undisclosed Investor(s)	Wilmington
Jan-14	Korbit	0.40	Seed	Strong Ventures, Bitcoin Opportunity Fund, Tim Draper, David Lee, Naval Ravikant	Seoul

Source: CoinDesk (http://www.coindesk.com/bitcoin-venture-capital/)

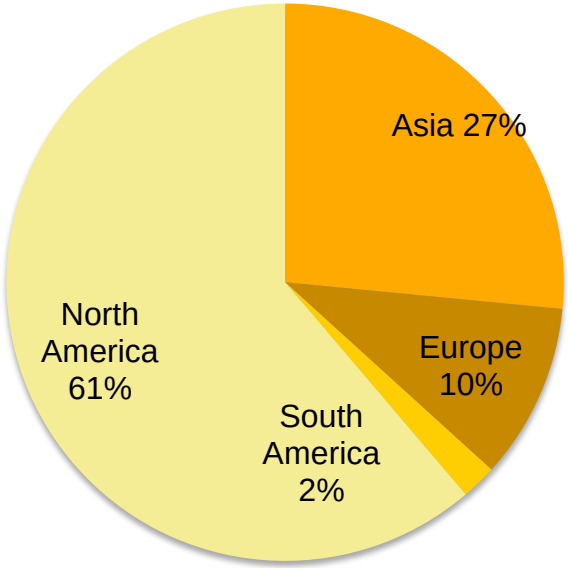
Europe Passed Asia in Total Bitcoin VC Investment in Q2, Both Still Lag North America

$ Invested



Regions	Value ($m)	No. of companies
Asia	20.8	13
Europe	30.9	5
S. America	2.0	1
N. America	186.3	30
Total	**$240.0**	**49**

No. of Companies

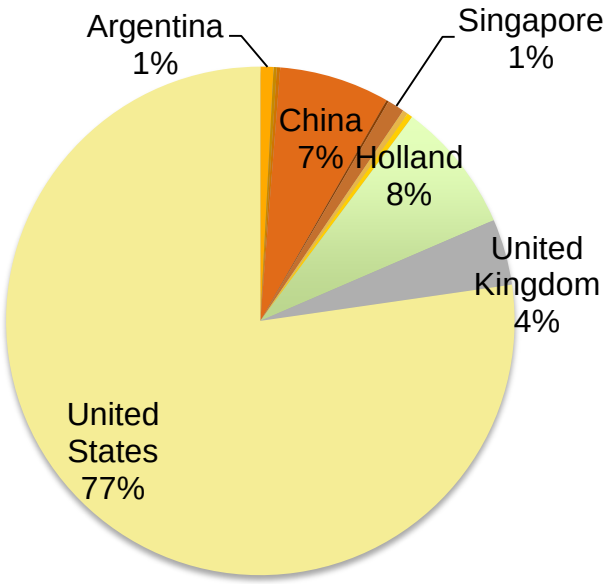


- Over a quarter of VC-backed bitcoin companies are based in Asia
- 78% of all bitcoin VC $s have been invested in North America to date, but only 61% of the companies are based there

Source: CoinDesk (http://www.coindesk.com/bitcoin-venture-capital/)

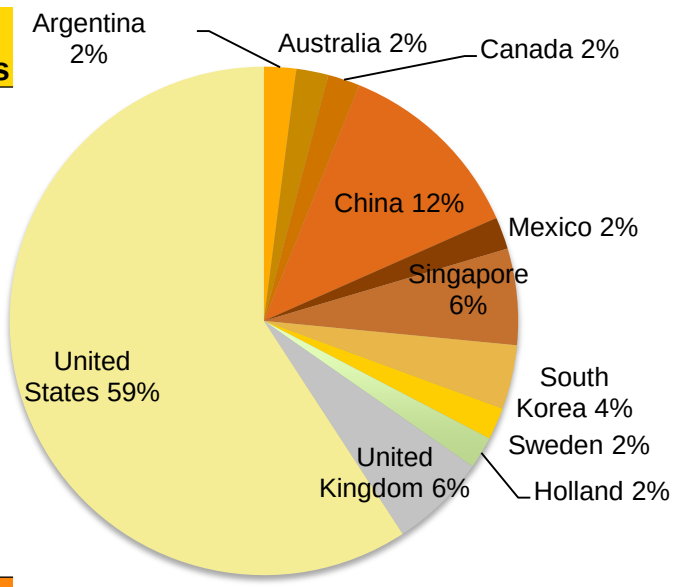
US Continues to Dominate Bitcoin VC Investment, Total Share Increased in Q2

$ Invested



Countries	Value ($m)	No. of companies
Argentina	2.0	1
Australia	0.5	1
Canada	0.5	1
China	16.9	6
Mexico	0.3	1
Singapore	2.6	3
South Korea	0.8	2
Sweden	0.9	1
Holland	20.0	1
United Kingdom	10.1	3
United States	185.5	29
Total	**$240.0**	**49**

No. of Companies

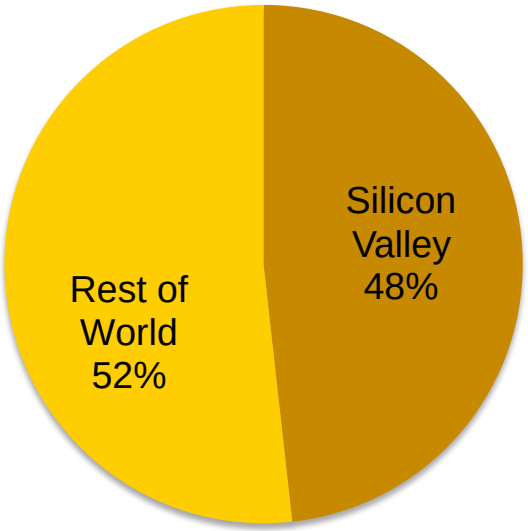


- Mexico, Holland and Argentina added their first VC-backed bitcoin startups in Q2
- Greatest number of VC-backed bitcoin companies are in the US and China

Source: CoinDesk (http://www.coindesk.com/bitcoin-venture-capital/)

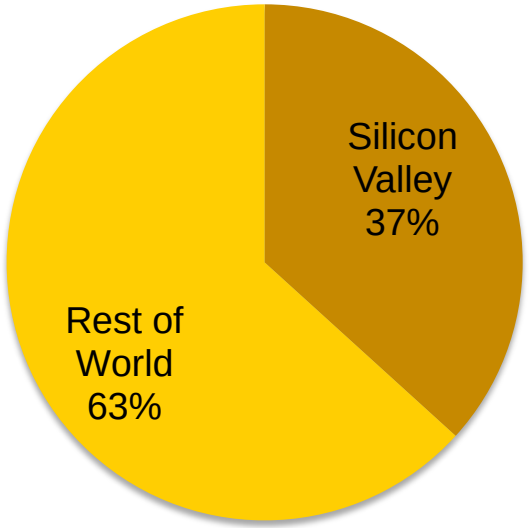
Silicon Valley's Share of Bitcoin VC Investment Climbed Slightly From 46% in Q1 to 48%

$ Invested



Tech hub concentration	Value ($m)	No. of companies
Silicon Valley	115.8	18
Rest of World	124.3	31
Total	**$240.0**	**49**

No. of Companies



- 63% of VC-backed bitcoin companies are based outside Silicon Valley, but have just over one-third of all bitcoin funding

Source: CoinDesk (http://www.coindesk.com/bitcoin-venture-capital/)

Investor Views on Bitcoin

"Just like the Internet disrupted the publishing industry, we're going to see bitcoin micropayments creating some very interesting opportunities for pay-as-you-go, pay-based-on-time online businesses, and, frankly, some risks as well to the traditional business model as to how things get sold online."

Barry Silbert
SecondMarket, Bitcoin Investment Trust

"On the question of whether bitcoin will replace money, a good analogy is the postal service and email. Email didn't replace traditional mail, and we still send the same amount of mail today as we did before. But today we have totally new ways of communicating – chat, text, Facebook – things we didn't imagine when the Internet first arrived."

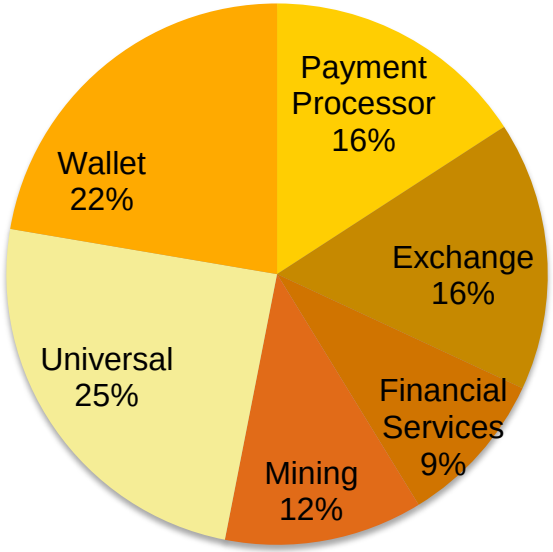
Dan Morehead
Pantera Capital Management

Source: CoinDesk, Absolute Return

The Bitcoin Startup Ecosystem: Six Different Bitcoin Company Classifcations

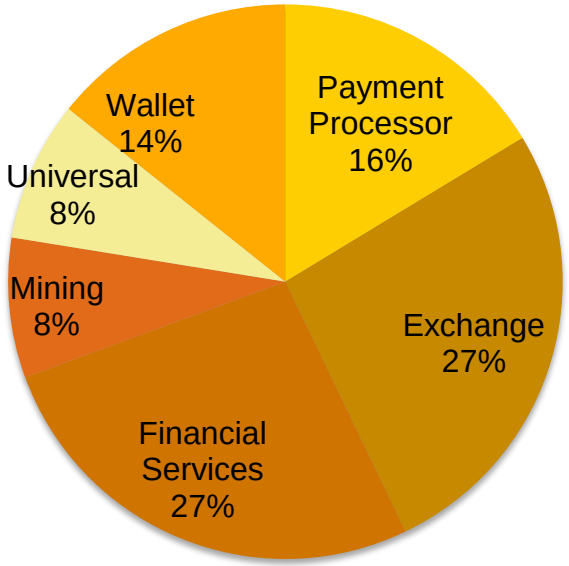
Universals Command the Most VC Investment

$ Invested



Sector	Value ($m)	No. of companies	Avg/co. ($m)
Universal	59.0	4	14.8
Wallet	53.6	7	7.7
Exchange	38.6	13	3.0
Payment Processor	38.0	8	4.8
Mining Hardware	28.5	4	7.1
Financial Services	22.3	13	1.7
Total	**$240.0**	**49**	**$4.9**

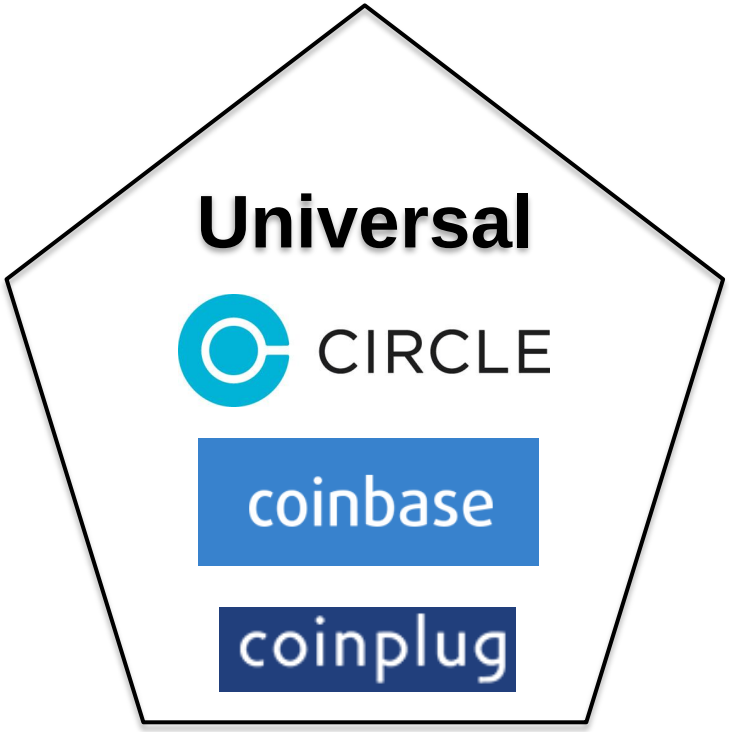
No. of Companies



- *Payment Processor (5.3x), Wallet (2.5x), Mining (2.2x) and Financial Services (1.5x) saw the largest Q1 over Q2 investment increase*

Source: CoinDesk, Dow Jones VentureSource, VentureScanner.com

The Emergence of the Universal Bitcoin Company



- Universals operate across more than one aspect of the bitcoin value chain (eg Coinplug offers payment processing, wallet, and ATM)
- Universal bitcoin companies leverage two key elements of financial services: efficiency and trust
- It's possible that more and more bitcoin startups will pursue the universal model, be absorbed by universals, or fade away

Commerce

New Applications and Services Announced in Q2 Are Making Bitcoin Easier to Use and Trust

CIRCLE

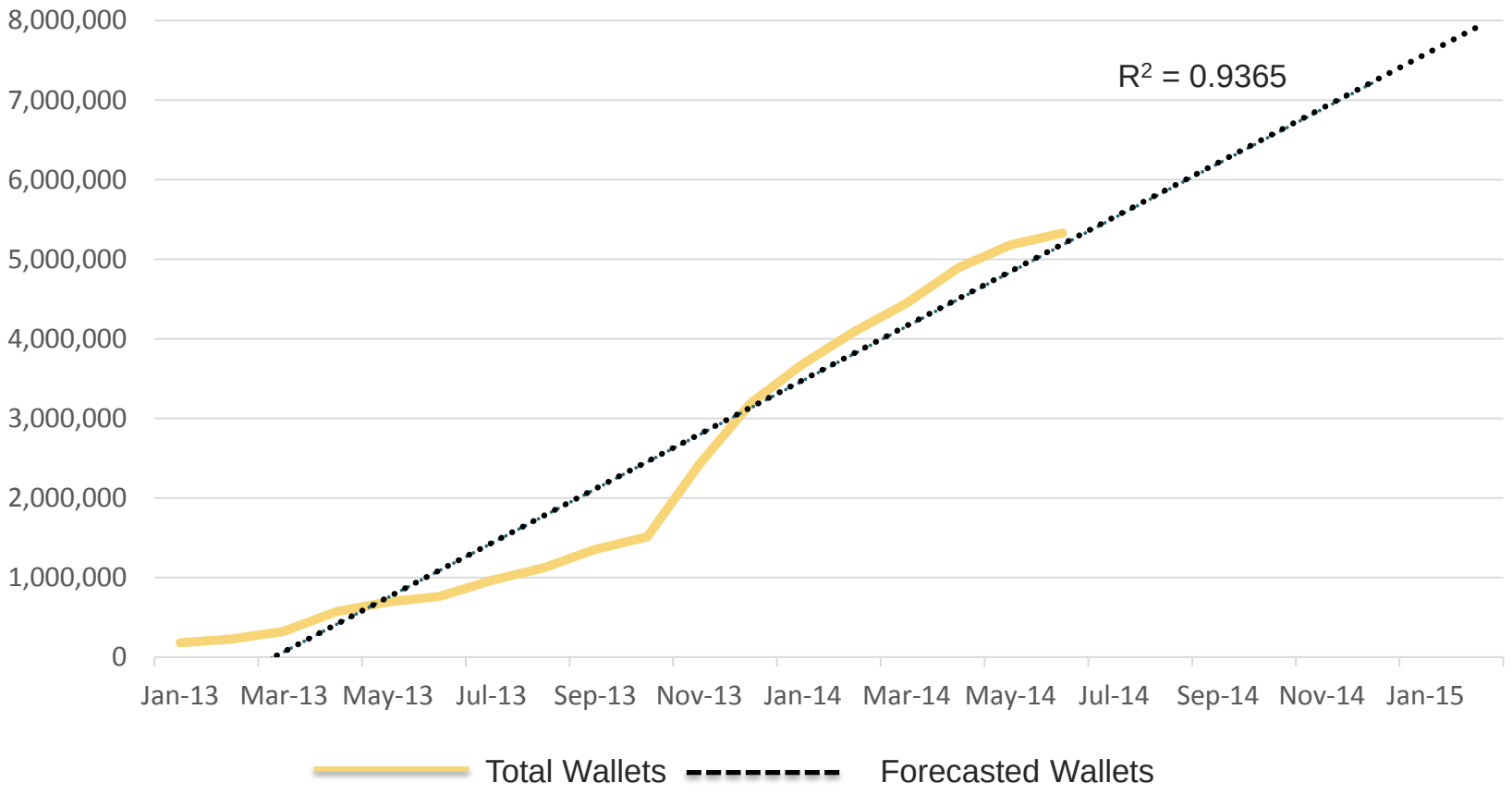
Insured bitcoin wallets

Bitcoin-linked debit cards

bitreserve

Transparent balance sheet

Approximately 8 Million Bitcoin Wallets Forecasted by Dec 2014



Sources and notes: total wallets based on data from Blockchain.info, MultiBit.org, Coinbase, Andreas Schildbach (Android Bitcoin Wallet developer). Historical Coinbase data provided by BitcoinPulse.com.

Approx. 63,000 Merchants Now Accept Bitcoin, Vast Majority Are Online Businesses

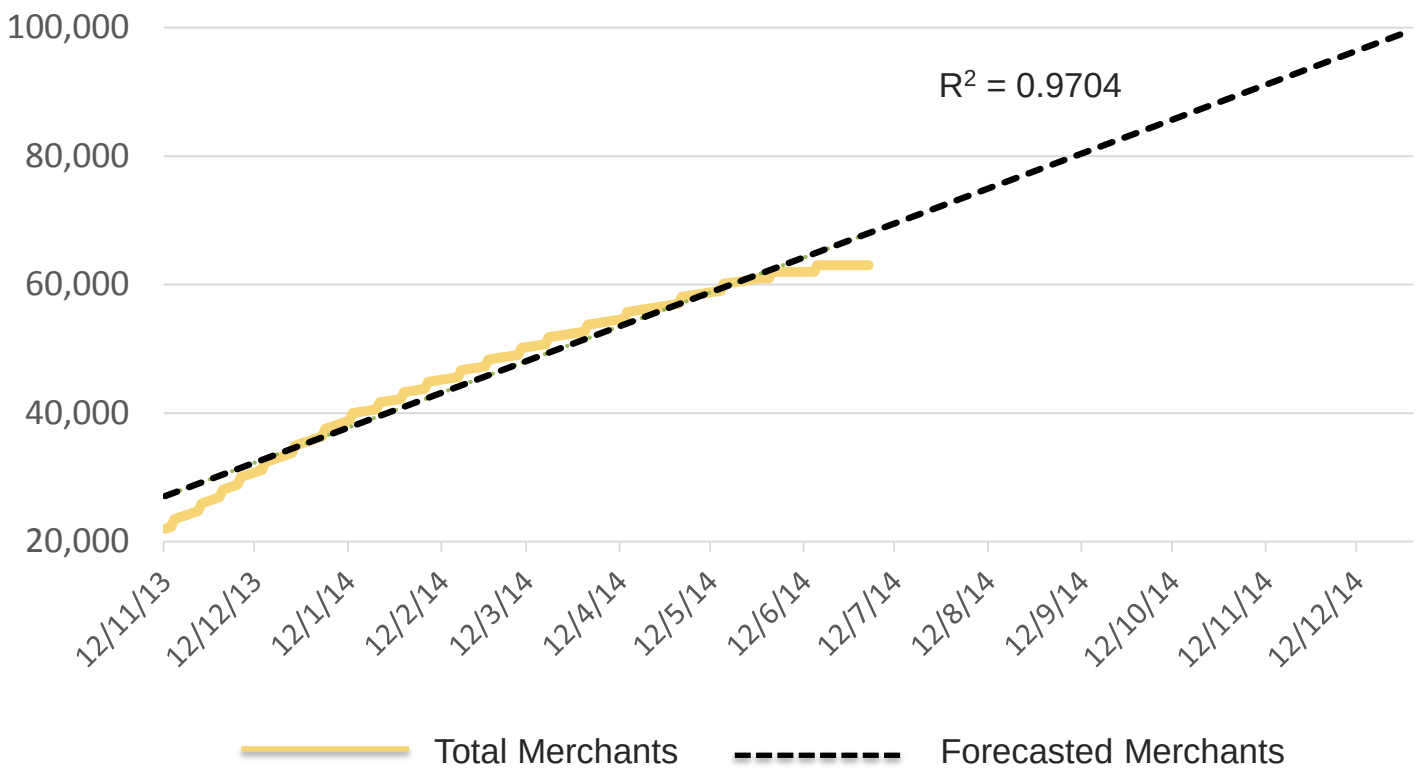
$13.9 billion annual revenue

$5 billion annual revenue

$2.8 billion annual revenue

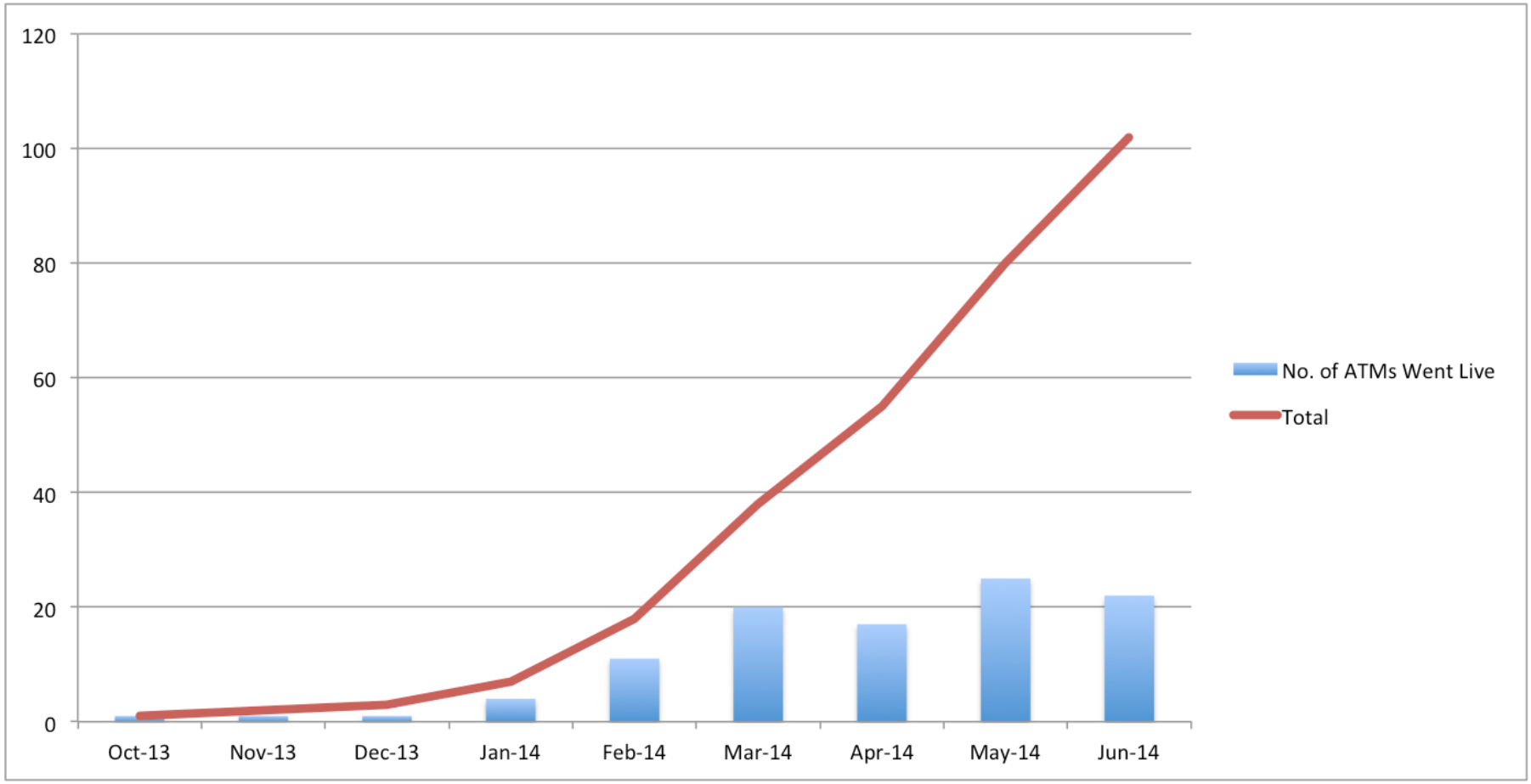
Source: Coinbase and BitPay

Approximately 100k Bitcoin-Accepting Merchants Forecasted by Dec 2014



Sources and notes: total current merchants based on data from Coinbase and BitPay. Historical Coinbase data provided by BitcoinPulse.com. BitPay historical data between new merchant press release announcements of 10,000 (16th Sept 2013), 20,000 (13th Jan 2014) and 30,000 (28th May 2014), respectively, calculated using linear interpolation.

Bitcoin ATM Deployments Gained Pace in Q2 2014 …



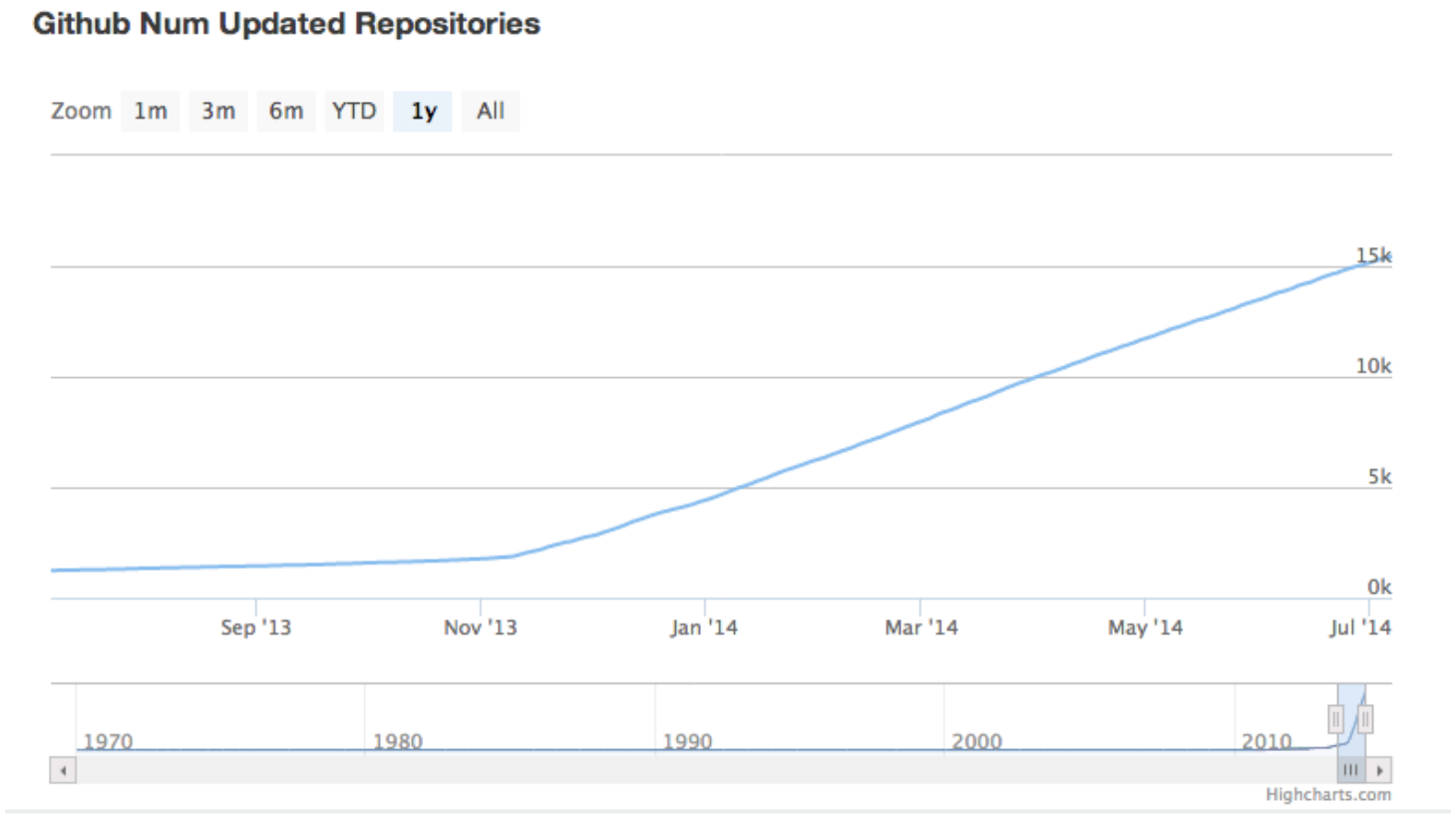
Source: CoinDesk

… Now Over 100 Bitcoin ATMs Around the World

Technology

Bitcoin Developer Ecosystem Grows

- Developers continue to remain highly engaged with bitcoin projects



Source: BitcoinPulse.com

There Are Now Approximately 340 Bitcoin iOS Apps …

… and 250 Bitcoin Apps on Android

Bitcoin is 4,000x Cheaper Than a Typical Remittance Transaction

Remittances:
Average global remittance fee of 8.14% per $200 ($16.28)

Bitcoin:
Median transaction fee is $0.004

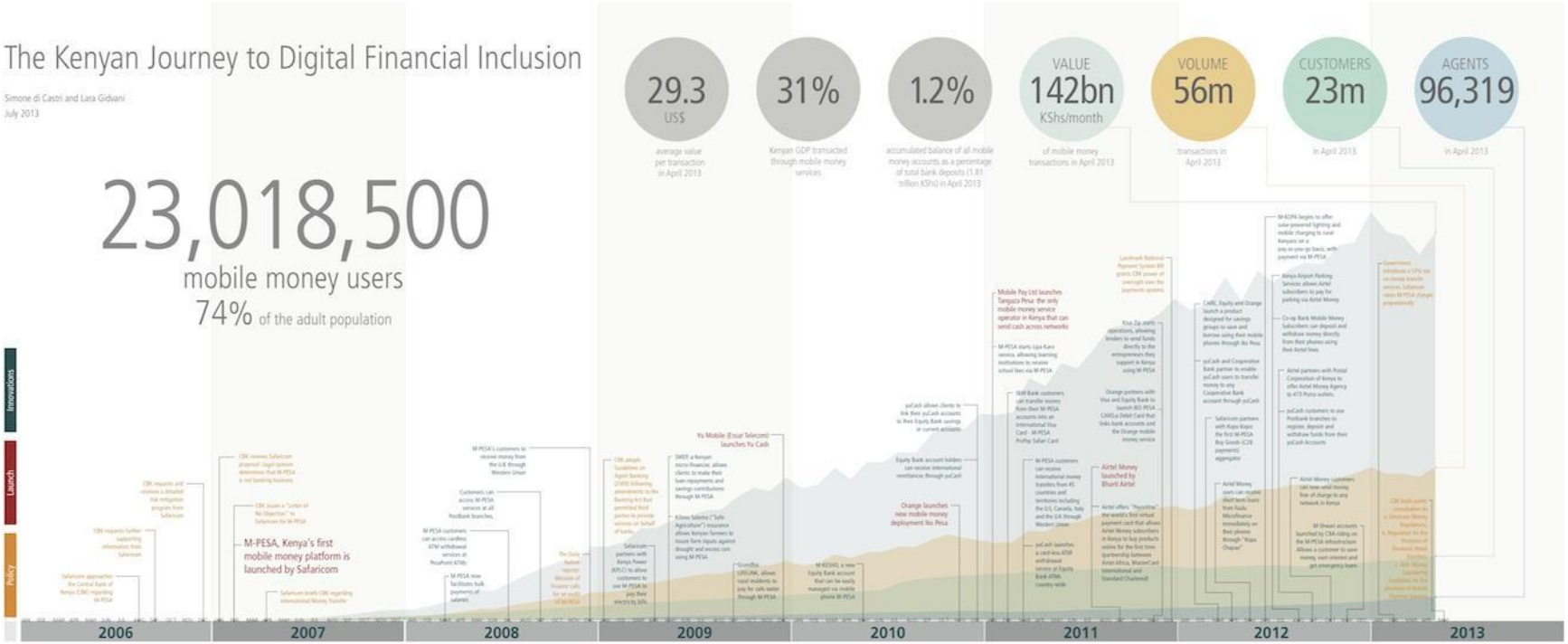
Remittances vs. bitcoin:
Bitcoin is 4,070 times cheaper on a $200 transaction

Source: World Bank Remittance Prices Worldwide; Blockchain.info

Emerging Markets and Macro

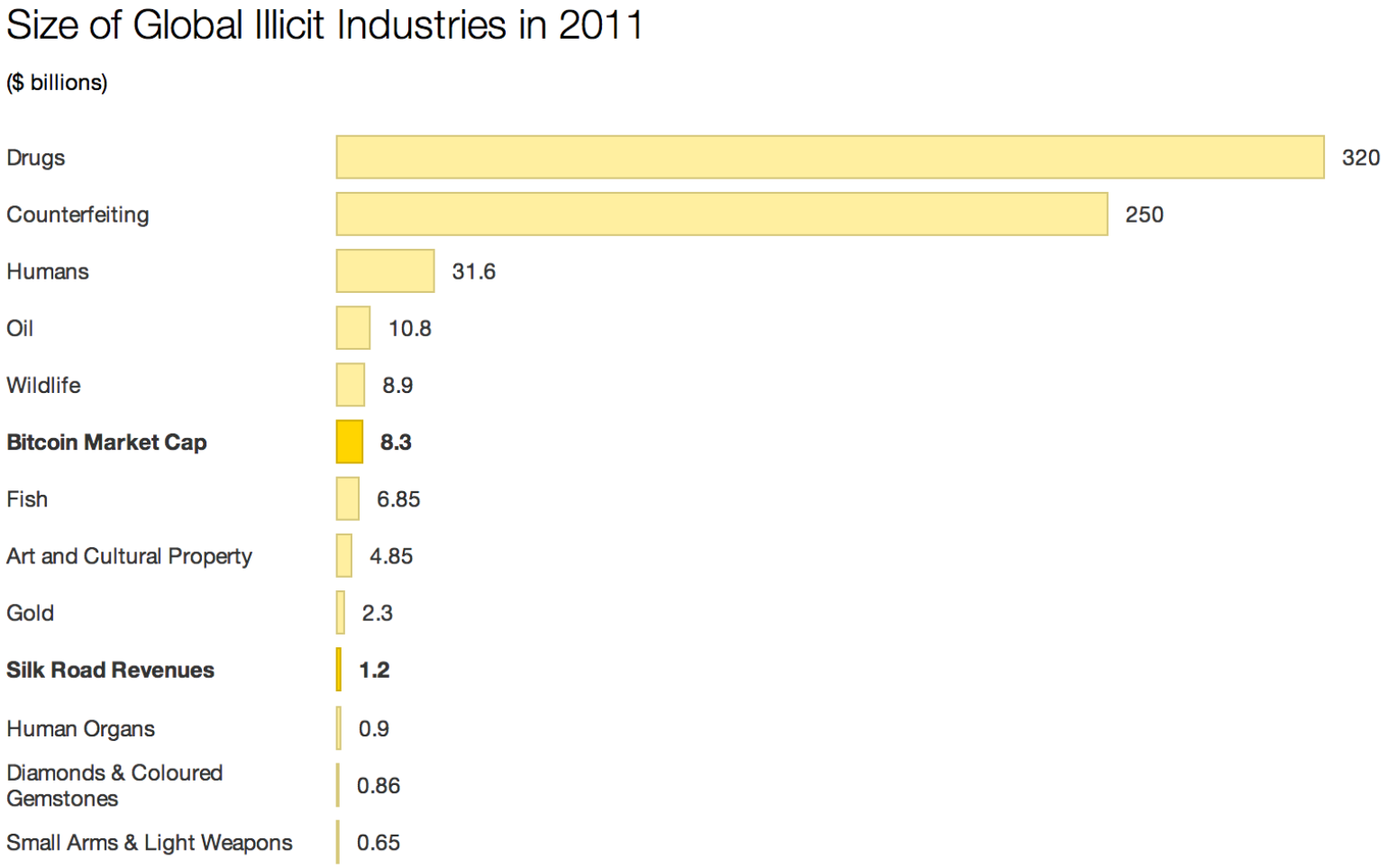
Emerging Markets Love Mobile Money

- 74% of Kenya's adult population uses M-Pesa and other mobile money services



Sources: GSM Association, Simone di Castri and Lara Gidvani

Bitcoin Dwarfed by Global Illicit Markets



Source: Global Financial Integrity, FBI. Full chart: http://cf.datawrapper.de/Gc83O/4/

Bitcoin's Regulatory Environment is Stabilizing and Trending Toward the Positive

- Recently released minutes from a Federal Reserve Advisory Council and Board of Governors meeting suggest that "banking could participate increasingly in bitcoin fund flows, especially as multicurrency accounts proliferate and reputational concerns subside".

- "The Advisory Committee can't dictate policy, but the minutes can shed light on what Fed policy might look like in the future." [CNN]

- "A task force of US state regulators is working on the first bitcoin rule book with the hope of protecting users of virtual currency from fraud without smothering the fledgling technology. Bitcoin users currently face a range of rules across the 50 states." [Reuters]

Bitcoin Continues to See Regulatory Gains and Setbacks, But Overall Regulation Has Slowed

California legalized bitcoin in June 2014

Bolivia made bitcoin and other cryptocurrencies illegal in May 2014

Keeping Mt. Gox in Perspective

J.P. Morgan to Pay More Than $2 Billion to U.S. in Penalties in Madoff Case

Email Print 44 Comments

By DAN FITZPATRICK And JEAN EAGLESHAM CONNECT

Updated Jan. 5, 2014 11:37 p.m. ET

Credit Suisse Pleads Guilty in Felony Case

By BEN PROTESS and JESSICA SILVER-GREENBERG MAY 19, 2014 4:50 PM 288 Comments

HSBC Judge Approves $1.9B Drug-Money Laundering Accord

By Christie Smythe | Jul 3, 2013 4:06 PM ET | 12 Comments Email Print

Former Chief of JPMorgan's China Unit Is Arrested

By NEIL GOUGH and MICHAEL FORSYTHE MAY 21, 2014 2:23 AM 27 Comments

UBS Admits Rigging Rates in 'Epic' Plot

Email Print 95 Comments

By DAVID ENRICH and JEAN EAGLESHAM

Updated Dec. 20, 2012 7:17 a.m. ET

Mexico Authorizes Arrests in Fraud at Citigroup Unit

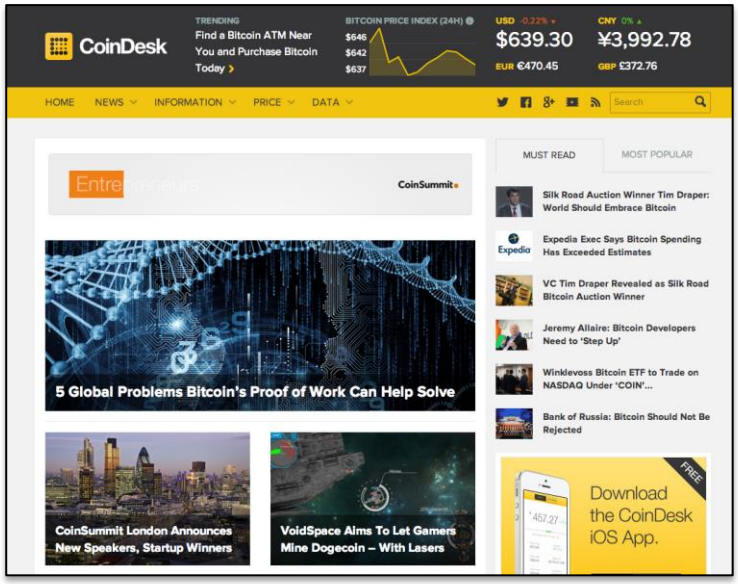
By ELISABETH MALKIN and MICHAEL CORKERY JUNE 1, 2014 12:05 PM 6 Comments

$8.9bn fine

Source: Baseline Scenario

Appendix - CoinDesk

- Find out more at www.coindesk.com
- Follow us on Twitter: [@coindesk](https://twitter.com/coindesk)
- Subscribe to our daily email newsletters for the latest digital currency news
- If you have data you think should be included in future State of Bitcoin reports, email stateofbitcoin@coindesk.com
- We also welcome any feedback you have on the report



Disclaimer

- CoinDesk makes every effort to ensure that the information in this presentation is accurate and up to date. We cannot, however, accept responsibility for any loss or inconvenience caused by reliance on the material contained here.

- This presentation does not constitute financial advice or an investment recommendation in any way whatsoever. It is recommended that you perform your own independent research and/or speak with a qualified investment professional before making any financial decisions.

OECD publishing

Please cite this paper as:

Blundell-Wignall, A. (2014), "The Bitcoin Question: Currency versus Trust-less Transfer Technology", *OECD Working Papers on Finance, Insurance and Private Pensions*, No. 37, OECD Publishing.
http://dx.doi.org/10.1787/5jz2pwjd9t20-en

OECD Working Papers on Finance, Insurance and Private Pensions No. 37

The Bitcoin Question

CURRENCY VERSUS TRUST-LESS TRANSFER TECHNOLOGY

Adrian Blundell-Wignall

JEL Classification: E5, F39, F65, G19, G2

OECD WORKING PAPERS ON FINANCE, INSURANCE AND PRIVATE PENSIONS

OECD Working Papers should not be reported as representing the official views of the OECD or of its member countries. The opinions expressed and arguments employed are those of the authors.

Working Papers describe preliminary results or research in progress by the author(s) and are published to stimulate discussion on a broad range of issues on which the OECD works. Comments on Working Papers are welcome and may be sent to the Directorate for Financial and Enterprise Affairs (daf.contact@oecd.org), OECD, 2 rue André-Pascal, 75775 Paris Cedex 16, France.

OECD Working Papers on Finance, Insurance and Private Pensions provide timely analysis and background on industry developments, structural issues, and public policy in the financial sector, including insurance and private pensions. Topics include risk management, governance, investments, benefit protection, and financial education.

The papers are generally available only in their original language, English or French, with a summary in the other if available.

OECD WORKING PAPERS ON FINANCE, INSURANCE AND PRIVATE PENSIONS
are published on www.oecd.org/daf/fin/wp

The Bitcoin Question:
Currency versus Trust-less Transfer Technology

by
Adrian Blundell-Wignall, OECD*

ABSTRACT

The financial crisis has led to a widespread loss of trust in financial intermediaries of all kinds, perhaps helping to open the way towards the general acceptance of alternative technologies. This paper briefly summarises the crypto-currency phenomenon, separating the '*currency*' issues from the potential technology benefits. With respect to crypto currencies, the paper argues that these can't undermine the ability of central banks to conduct monetary policy. They do, however, raise consumer protection and bank secrecy issues. The valuation of Bitcoins and price volatility issues are discussed, as well as electronic theft, contract failures, etc., all of which could result in large losses to users and hence ultimate costs to the taxpayer (e.g. the failure to provide adequate private pensions resulting in increased reliance on public pensions). The anonymity features of the crypto-currencies also facilitate tax evasion and money laundering, both of which are major public policy concerns. The technology associated with crypto-currencies, on the other hand, could ultimately shift the entire basis of trust involved in any financial transaction. It is an innovation that creates the ability to carry out transactions without the need for a trusted third party; i.e. a move towards trust-less transactions. This mechanism could work to eliminate the role of many intermediaries, thereby reducing transactions costs by introducing much needed competition to incumbent firms. The generic issues that policy makers need to examine are summarised.

Authorised for publication by Gabriela Ramos, OECD Chief of Staff and Sherpa to the G20.

JEL codes: E5, F39, F65, G19, G2

Keywords: Bitcoin, Gold standard, trust-less transaction, payment technology, intermediaries, legal tender, plenary powers, monetary policy

* Adrian Blundell-Wignall is the Special Advisor to the OECD Secretary-General on Financial Markets and Acting Director of the OECD Directorate of Financial and Enterprise Affairs (www.oecd.org/daf/abw). Paul Atkinson and colleagues in the OECD Secretariat provided comments on earlier drafts of this paper, though all errors and omissions remain those of the author.

Table of Contents

I. INTRODUCTION

"Money" has three broad characteristics: a store of value, a unit of account and a medium of exchange - though "money" doesn't have to be legal tender. On the face of it crypto-currencies could be thought of as meeting all of these "money" roles. They are (as are many things) a potential store of value, albeit a very unstable one. They could be used as a unit of account and, as the earliest known use of a Bitcoin retail transaction was to buy a pizza, they can be used as a medium of exchange for anyone willing to accept them. In this latter role they have significant advantages, as they can be divided digitally for any size of transaction and they avoid the high fees charged by credit card companies. But it is likely that the main reason crypto-currencies are 'taking off' in acceptability as a means of payment is due to the anonymity feature. The high degree of anonymity feature has great advantages for illegal activities such as money laundering, avoiding financial regulations, terrorist financing and evading taxes.

The financial crisis led to a loss of trust in many financial intermediaries, trading platforms and payment systems. The main innovation of crypto-currencies is the feature of trust-less transactions (the ability to avoid the need for a trusted third party). Barter is always possible – window cleaners could negotiate with shops, doctors' surgeries and farms to exchange hours or cleaning for goods and services. However, barter is a poor medium of exchange and cleaning cannot be meaningfully stored (and hence isn't a store of value). Casino chips, airline miles, Amazon credits, Disney money could also be used for some functions outside of their primary intended use, but not with the potential usability features of crypto-currencies in the digital age.[1]

Crypto-currencies can never become an alternative to legal tender, for the simple reason (as will be explained below) that people have to pay their taxes. This protects existing fiat currencies from being displaced, and the fear of loss of monetary control should not be used as an argument to prevent Bitcoins from circulating as parallel currencies. However, the technology of the digital payment protocols should not be confused with the parallel currency issue. With respect to the currency function, there are two potential policy issues: (a) consumer protection issues: e.g. electronic theft; a collapse in value of crypto coins say due to the emergence of substitutes; the use of government plenary powers to ban them, etc.; and (b) anonymity features permitting an expansion of socially unacceptable activities such as tax evasion and money laundering. The digital transfer technology, on the other hand, could play highly-socially useful roles. The basics of crypto-currencies are set out in section II using Bitcoin as the main example. How to think about their value is discussed in section III. Theft, substitutes and plenary powers are discussed in section IV. Contract law and the relevance of the need to pay taxes are set out in section V. The use of the governments' plenary powers is discussed in the context of the abandonment of the Gold Standard in section VI. The 'useful technology' issue is discussed in section VII. Finally, some concluding observations on policy issues are offered in section VIII.

[1] These parallel currencies have an exchange rate with the dollar, and this is also possible with Bitcoin by using a broker like *Coinbase* which provides easy to use Bitcoin wallets linked to bank accounts not unlike Paypal.

II. WHAT IS A CRYPTO-CURRENCY?

With respect to Bitcoin, the founders "seeded" the market by providing algorithms to early "miners" who accumulated the first stock of Bitcoins; and holders of such stock benefited from subsequent price increases. By using computers intensively and incurring high electricity costs, subsequent participants could mine for Bitcoins, of which a total of 21 million is the fixed supply. The supply function for the coins is reputedly spread out by reducing the size of blocks to be found and via an algorithm that makes finding them dynamically more difficult if they are found too quickly. It may take many years to mine them all. Bitcoins trade on an online market and anyone can buy them at the going exchange rate with the dollar on Bitcoin broker platforms (like *Coinbase),* though the price has proven to be very volatile to date. Part of the reason for this is that there is no clear intrinsic value or agreed valuation method, and certainly no Bitcoin central bank prepared to intervene to make the price more stable, which would violate the fixed supply element.

The digital transfer technology is very interesting. There is an open source key cryptology, one public and one private. Bitcoin transactions transfer ownership of a 'coin' from one public address to another, but a private key is required to de-crypt the Bitcoins and spend them. Public and private keys are alphanumeric strings based on sophisticated encryption: random numbers and letters are derived from public keys by the application of a "hash" function (a process that takes an arbitrary block of data and returns a fixed size bit string). Authentication is like *fingerprinting* - there can only be one generator of transfers with a given address (though of course storing private identification strings online opens the way for stealing and fraud as with anything where money and the internet is involved). Bitcoins in the form of public keys are stored in "wallets", on a computer's hard drive and can only be accessed with the private key. Safety against hacking is increased by the use of off-line "cold storage", and such services are provided by broker platform intermediaries. Wallets stored with an internet connection, or linked with a smartphone application are akin to cash, and Bitcoins can be moved from cold storage to mobile wallets as required.

Transactions are recorded in the "Block Chain" which is the key innovation in this technology – that is, a technology that removes the need for a trusted third party and the intermediary costs associated with such institutions (banks, credit card companies, payment companies, non-bank financial intermediaries). The Block Chain is a public database (giant ledger book), openly maintained by computers all over the world – it is a sequential record of all transactions and current ownership. This tracking and verification of transactions is supported by the decentralised computing power generated by the activity of 'mining', and this activity is rewarded in Bitcoin fees. The Block Chain allows participants to check whether transfers are coming from actual owners of coins and it avoids problems like "double spending" – you can't spend the same Bitcoin fraction more than once.[2]

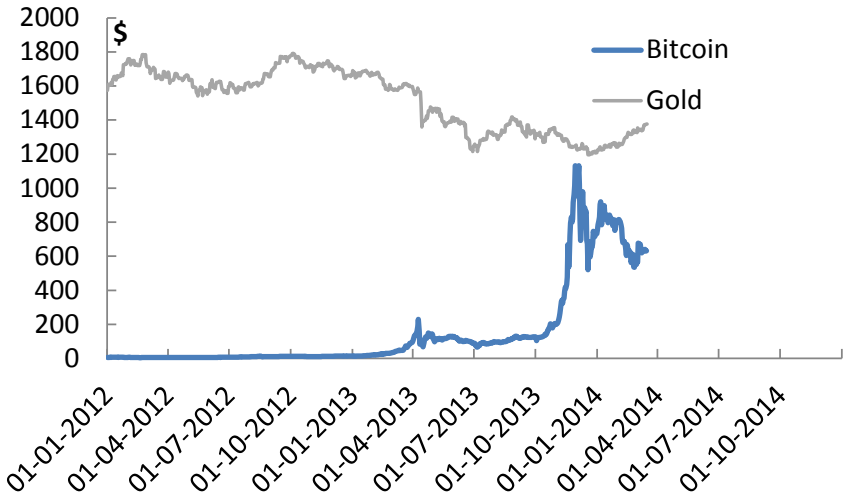
This Bitcoin technology has spawned a rapidly growing industry of crypto-currency innovations that use independent block chain methods (e.g. Bitcoin, Litecoin, Dogecoin, NXT, BitShares and Ethereum). Other protocols are built on top of the Bitcoin Block Chain to do new interesting things, like tokens being identified with specific assets for trading purposes (Coloured Coins, Mastercoin, and Counterparty). The Block Chain technology does have an important scalability problem, however, related to the computing power required to re-calculate the history of all transactions (discussed below), a problem which grows larger the more widespread the use of Bitcoins.

[2] Problems with this could arise if one miner controlled 51% of the computing power, which would attacks on the Block Chain.

III. VALUING BITCOINS

Figure 1 shows the Bitcoin price compared to the gold price. The price is single digit in 2012, around $100 for much of 2013 and then it moves up quickly to $1100 at the end of the year and collapses to the $500-$800 range for the early months of 2014.

Figure 1. **Bitcoin Prices versus Gold**



Source: Datastream, Bitcoincharts.com.

Such extreme high prices might be explained by strong inelastic demand and tight supply. Assuming that anonymity is important for some market participants to evade taxes or to launder money, the demand can well exceed mining supply. The supply side too may be a factor. For example, the difficulty of mining might suddenly accelerate, or miners might engage in cartel-like behaviour. Alternatively, speculative demand might enter the market, with each trader believing that buying at 10 or 20 times the mining cost doesn't matter, as long as someone else is willing to pay more than that – the '*greater fool'* theory. Judging by the sudden and extreme pick up in the volume of trading around the time of the price surge, the greater fool theory is probably the best contender for explaining the surge[3]. The recent price volatility certainly seems to have little to do with fair value – and part of the problem in valuing a crypto-currency is that it is a technology and not a business with a reported balance sheet or a currency backed by a commodity.

Attempts to value Bitcoins are highly unsatisfactory. Bank of America's David Woo tries to do so by using a potential market capitalisation approach, putting a value on each of the following components:

[3] Though several news headlines in late 2013 helped to legitimise Bitcoin to the man in the street: the purchase of a large quantity of Bitcoins by a well-known executive; the BTC market in becoming the largest exchange in China possibly resulted in speculation about the potential for Bitcoins in China; perception of support by politicians after the first Congressional hearings; etc. All of these may have encouraged investor interest.

medium of exchange (B2C); means of payment (C2C); and store of value.[4] The values are based on heroic assumptions that add up to about $15bn (2012 prices), and with the coins in circulation at the time a Bitcoin would be worth about $1300. For the medium of exchange component he uses macro assumptions for consumption and money, assuming that ultimately Bitcoins will be responsible for 10% of world transactions (he gets a $5bn number). But this set of arbitrary assumptions ignores the potential role of competitors: barriers to entry in starting up a new crypto-currency are relatively low, regulation and a number of other factors that could just as easily make the coins worthless. For a means-of-payment value, Bitcoin is given a market cap in line with the three big money transfer companies: Western Union, Moneygram, and Euronet (about $4.5bn). However Bitcoin is not a company with payment system spreads that generates revenues for shareholders. Indeed the main socially-beneficial feature of the Bitcoin is that it is a technology that has low transactions costs. As a store of value Woo uses silver as a guide (about $5bn). This seems highly unrealistic as silver has intrinsic value whereas Bitcoins do not – they are not backed by anything.

An alternative way of thinking about fair value is to focus only on the medium of exchange role of Bitcoins: recognising the potential value of the technology of trust-less exchange, but also incorporating some of the risks. Let M reflect the (constant) electricity, hardware time and human capital cost of mining a Bitcoin, and ε is a random add-on to that cost depending on the degree of difficulty of the algorithm at the time, random 'luck' and other one-off factors. This is the underlying value to which market prices should gravitate, with the mining supply of Bitcoins rising or falling in response to whether the market price sits above or below it – provided of course that the crypto-currency is always 'acceptable' with no risk of being worthless due to fraud; a better substitute coming along; technological scalability issues; or government policy banning them. However, since all of these risks are present, the fair value of the coin could be thought of as the present discounted value of the variable mining cost with a probability "p" of a fatal risk event in any period. Using (say) a 5-year horizon:

$$PV = (1-p_1)(M+\varepsilon_1)d_1 + p_1(1-p_2)(M+\varepsilon_2)d_2 + \cdots + p_1p_2p_2p_4(1-p_5)(M+\varepsilon_5)d_5$$

Where: $d_i = 1/(1+r)^i$, r is the riskless bond rate and i=1…5.

For example, if the mining cost of 1 Bitcoin happened to be $100 exactly in every period, the risk free rate for the discount factor is 4% and the probability of a risk event is 50% in each period, then the value would be $85. Since $100 per coin might be thought of as a high mining cost, it is difficult to understand how values of over $1000 can be achieved. If there is no earnings stream for a payment system role and no intrinsic value (such as for gold or silver), or the 'good faith and credit' of a government (as for a fiat currency)[5], then the price should gravitate to the discounted medium-of-exchange (only) value. If the probability of a fatal event were to rise to 90% each period, the price would fall to $26; for 100% the price would fall to zero.

Unlike gold, there is no intrinsic value for a Bitcoin. Gold is a rare substance with a long history of discovery and a high cost of production. Gold's main use historically has been as money, and the move towards fiat currencies began only from 1914. Gold also has a strong store-of-value role as a hedge against inflation and other risks as well as industrial and decorative uses. Bitcoins have a supply function and a demand curve derived from the advantages they convey. But if governments take away those advantages, the coins are stolen via fraud or an alternative better crypto-currency emerges, Bitcoin prices would fall to zero and the recovery value for the stock of 'coins' too would be zero.

[4] See Sharf (2013). B2C stands for business-to-consumer, and C2C for consumer-to-consumer.

[5] Even gamblers in a casino have the good faith and credit of the casino when they use its chips.

IV. CONSUMER PROTECTION AND RISK EVENTS FOR CRYPTO-CURRENCIES

Dabbling in crypto currencies with extreme volatility raises consumer protection issues that bear some scrutiny by the relevant authorities, since unsophisticated investors could become involved and provide the 'greater fools' to the market. Since major losses by a household could ultimately result in the state having to pay higher benefits (e.g. failure to provide for an adequate pension as a result of large Bitcoin losses) the state should provide clear guidelines on registration and *know-your-customer* issues. The structure of the Bitcoin and other networks is not well set up for this due to the decentralised and anonymous nature of the participants.

Market volatility and fairness

The potential for market volatility and contract litigation issues seems large. For example, a real estate sales company starts taking Bitcoins to pay for houses from persons unknown and of dubious origins. They fail to convert the Bitcoins into legal tender for the client just prior to a major dip in price, or an event that takes their value to zero. The coins are not backed by anything and the network has no capital or obligations. The client has signed a contract accepting the risks and takes a massive wealth loss, while the money launderer now owns a building. Who does the house seller litigate against? Presumably the real estate agent, as the buyer is unknown. The real estate entity fails, and it has other links with banks and the financial system, creating losses and instability elsewhere in the financial system.

Fraud

This requires little elaboration. The Mount Gox episode illustrates that it is certainly possible for the coins to be stolen in a digital attack, and an exchange shut down, with the likelihood of all ex-owners losing their "money". Such episodes will likely incentivise other exchanges for crypto-coins to improve their security practices.

Substitutes

Bitcoins already have their imitators and innovators: e.g. Litecoin, Worldcoin, Mastercoin, Coloured Coins, Dogecoin and others – barriers to entry do seem to be very low. There is no reason why good or better crypto-currencies won't drive out bad ones, including Bitcoin itself. An initial widespread use of Bitcoins could emerge as a parallel currency only to be replaced by a better one. It would not be the first time that second-mover advantages outweigh those of first-movers.

Regulation

Some governments have already moved in some jurisdictions to regulate Bitcoins. China has banned yuan to Bitcoin deposits into BTC China (its largest exchange) and banned the use of the QQ exchange which had been used to buy real goods and services. Germany, France, Korea and Thailand have also indicated a repudiation of Bitcoins as a currency. Other countries are yet to follow. However, while some form of regulation of crypto-currencies will be important due to the anonymity issue, it is not at all necessary to ban their use as a private currency on the grounds of loss of monetary control, for reasons that will be explained in the following section.

V. CONTRACT LAW, LEGAL TENDER AND PAYING YOUR TAXES

The government decides what can or cannot settle a legal monetary contract. In most civil societies that consists of legal tender or cheques and other transfers drawn on a bank that is regulated by the government and is a part of the payments system - in normal circumstances a bank deposit is transferable into legal tender (since the bank deposits are insured and/or the bank can obtain cash through the lender-of-last-resort function). The government enforces all legal contracts through the civil legal code.

Some might argue that a crypto-currency is also transferable into legal tender. Stocks and securities of all forms are all transferable into legal tender, but they cannot serve as legal tender.

The ultimate reason for this is a certain government monopoly within the payments system. Everyone has to pay their taxes, and hence anyone's bank has to be able to clear with the government's bank, most often the central bank. The government will only accept legal tender for this purpose, which is precisely the leverage over the financial system that ensures that the government can affect interest rates in the entire economy. The government's bank will not accept Bitcoins in the clearing process. As the central banks own liabilities are the (rare) legal tender, no bank can exchange legal tender for Bitcoins within the payments system. A non-bank Bitcoin seller can receive a cheque or cash from a non-bank buyer, and then deposit dollars in his or her bank within the normal clearing system, as is also the case with stocks and bonds. But it is not "money". No matter how acceptable Bitcoins are amongst its enthusiasts, it can in no way impact the ability of the government to conduct monetary policy because everyone at the end of the day has to pay their taxes and must obtain central bank liabilities to clear with the central bank.

In the case of the '*dollarization*' phenomenon (e.g. Zimbabwe) this conclusion is not changed. While good US dollars drive out de-based local currency, dollarization involves the government accepting US dollars in the payment of taxes fees and fines, and hence the dollar's acceptance into the payment system. At this point the government has effectively decided to import US monetary policy as an explicit decision. No government should accept Bitcoins into the payment system and thereby lose control of the money supply and interest rates.

Taxes and money laundering issues are more substantial

While paying taxes involves clearing with the central bank and that ensures in general that monetary policy cannot be undermined, the issue of how to treat capital gains and losses for tax purposes in the crypto currency world and the problem of using anonymity to evade taxes are legitimate policy issues.

There appears to be a move by some countries to treat Bitcoin as a 'commodity' in terms of taxation. In November, the Canada Revenue Agency issued a news release which stated that any gains or losses from trading a digital currency would be considered taxable income or capital for the taxpayer. This tax treatment is similar to a capital asset (stocks, bonds, commodities, etc.), which are traded in the open market. The United States, Internal Revenue Service has taken a similar position for tax purposes. In other words, the position is that Bitcoin is not a currency, but that it will be treated as a commodity which can be traded with resulting gains or losses and which can be used to pay for goods and services with valuations for tax purposes being whatever the value of the Bitcoin is on the date of the payment or receipt.

The use of Bitcoins for tax evasion is a potentially very significant policy issue. Bitcoins, like cash transfers, cannot be traced by third parties and are essentially invisible to tax authorities. Everyone can see the public key accounts and all transactions, but not the identity attached to it. This makes taxation at source and information exchange agreements largely irrelevant, and similar issues would apply for money laundering. The Financial Crimes Enforcement Network (FinCen) of the US Treasury determined in March 2013 the circumstances under which Bitcoins would come within the Bank Secrecy Act. They have guided that Bitcoins are *'convertible virtual currencies'* and should be treated like a currency for the purposes of US anti-money laundering laws in the cases where Bitcoin money service providers can be classified as "*money transmitters*" (where Federal and State registration, recording, reporting and '*know your customer'* rules come into play)[6]. This is not inconsistent with the above treatment of Bitcoins as a commodity for tax purposes – it is akin to a currency with an exchange rate to the dollar the gains and losses from which are taxable.

A paradox

If a *raison d'etre* for Bitcoins is to carry out illegal activities due to the 'anonymity factor' it is likely true that the means is easily found to convert them back into legal tender. But there is a paradox here. The more successful the crypto currencies become at fraud, money laundering and/or the undermining of the tax system, the greater will be the incentive for the government to use its plenary powers to abandon its hitherto 'light-touch' in dealing with the crypto-currency phenomenon. Exchanges dealing in illegal activities have already been closed down and in the limit the government may use its plenary powers simply to ensure that any form of legal contract involving Bitcoins is unenforceable. All contract clauses in Bitcoins could be abrogated and unenforceable by the action of lawmakers. History is replete with examples, but none better than with the abandonment of the gold standard.

[6] That is, a business of administration of Bitcoin activities with a central repository which is transmitting something of value from one location to another where third parties to an initial transaction are involved. See FinCen (2013). In January 2014 it was further clarified that individuals and companies obtaining Bitcoins for their own use, or as investments, does not constitute being a money transmitter under the Bank Secrecy Act.

VI. PLENARY POWERS AND THE ABANDONMENT OF THE GOLD STANDARD IN 1933

Prior to 1933 the Gold Standard was the basis of the world monetary system. In the UK a *gold specie standard* was in place from 1821 when the Royal Mint began producing gold sovereigns until the outbreak of World War I. At that time the specie standard was abandoned and was replaced by Treasury notes backed by gold specie (i.e. redeemable in gold specie) – but with the Bank of England using patriotic motivations to avert the need for actual redemptions in gold specie. This in itself caused no legal issues as gold clauses in contracts could still be binding. In 1925 Britain formally returned to a gold bullion standard – the law compelled the authorities to sell gold at a fixed price in terms of the pound sterling. Any form of cash outflow from a country would cause them to begin losing gold stocks, the money supply would contract, and policies to reduce demand would be implemented to restore external balance. This caused intolerable economic hardship in the 1930's, and Australia and New Zealand were the first to leave the gold standard. Britain followed in 1931.

When Franklin D. Roosevelt came to power in the midst of the Great Depression, he immediately closed the banks under the Emergency Banking Act. Executive order 6102 then required the surrender of all gold bullion, coins and gold certificates to the government by 1 May 1933, in exchange for dollars at the rate of $20.67 per troy ounce.[7] However, many legal contracts were written with gold clauses, based on the legal tender at the time they were written. So Congress passed a resolution cancelling all gold clauses in both private and public contracts. The sense of the resolution was that gold clauses interfered with the power of Congress to regulate the US currency.

This was challenged in the High Court in a number of cases (Norman versus The Baltimore and Ohio Railroad; The USA versus Bankers Trust Corporation, 1935; Nortz versus the United States; and the Unites States versus Perry, 1935). The court decided in a 5-4 majority in all of these cases that: "*the power to regulate money is a plenary power*". The abrogation of all gold clauses was considered to be within the powers of Congress when such clauses presented a threat to Congress' control of the monetary system. In short, contracts specifying payment in a fixed quantity of gold were not enforceable in law. If Bitcoins begin to undermine the financial and tax systems they will be shut down and all contracts between traders would be unenforceable.

[7] See Friedman and Schwartz (1963) and, for a short summary, Richardson, Komai and Gou (2013).

VII. THE TECHNOLOGY WITHOUT ANONYMITY

Crypto-currencies solve an important problem: the safe transfer of ownership without the need of a middleman or trusted third party. This technology has the potential to reduce transactions costs for retail spending with credit cards, E-commerce costs and money transfers. Goldman Sachs (2014) uses the Coinbase fee of 1% for providing these services with Bitcoin and compares this to the 2-3% fees on credit cards, the 2.9% average fee for E-commerce and the 8.9% average fee for money transfers. Future regulatory costs could of course push up the cost of this example. But such companies are intermediaries too, and it should not be forgotten that competition in the crypto-currency world is fierce, and new decentralised technology innovations may reduce costs dramatically.

The biggest problem for the Bitcoin approach is the need to re-calculate the full Block Chain history to verify the validity of all current transactions – which becomes increasingly computer intensive and costly – if full security is to be assured. While miners are rewarded in this verification activity, other approaches are looking to provide new alternatives to the Block Chain. This scalability problem is something Bitcoin will have to solve but it isn't yet clear how this can be done.

The *Ripple* protocol is interesting in this respect and solves the scalability problem of Bitcoin. It is a trust-less transfer technology based on a network of servers that enables trading in different currencies. While it does have its own currency (XRP), this is mainly for system protection reasons. XRP is not required to be the store of wealth, unit of account and medium of exchange, and at least one global bank has begun to use the technology in the payment system to cheapen costs and reduce exchange risk. The equivalent of the block chain is a public ledger shared by a *unique node list* (UNL) of members' servers. The ledger is a record of all Ripple accounts – the '*last closed ledger'* is the last validated set of Ripple accounts. A set of new transactions arrives as proposals to change the ledger and forms a *candidate set* which is distributed to all external servers – those not on the UNL list are discarded and a set of iterations begins to match the transactions in the current candidate set. Once voting of server nodes reaches a consensus of 80% (after reformulating the candidate set and discarding invalid transactions at each stage) validation is declared, a new last closed ledger forms and the process starts again. This takes minutes only, and the voting procedure removes the huge electricity cost of mining activities associated with recalculating the Block Chain in the Bitcoin world. There is a small transaction fee in XRP (all members must hold at least 20 XRP) so that the cost in XRP can respond to any flooding scams and essentially block it.[8] This approach doesn't require the huge private centralised servers used by credit card companies, and ultimately this type of technology should act to undermine their expensive systems in the long run if they do not adapt to use it themselves. One German online bank has already adopted the Ripple protocol, allowing it to do trust-less transfers with partners greatly reducing payment costs. The speed of transactions greatly reduces currency risk during the payment process.[9]

[8] Ripple is said to deduct only 0.00001 of one unit of its currency XRP as a transactions fee, and one XRP in early 2014 was in the 30 to 40 cents range – tiny.

[9] In the current banking world a transfer order is made, and a cumbersome process with correspondent banks begins. The client is informed later of the price at which the exchange took place. The Ripple protocol allows an almost instantaneous transfer at the current price.

Whether or not the Ripple protocol is the ultimate winner remains to be seen, but policymakers should welcome the exploration of the use of new technology to improve efficiency and provide competition to high-cost incumbent intermediaries in the financial system. Policymakers do need to focus on how to ensure that the new technologies operate in the most socially-useful way. That is, it should be possible to make use of a new technology to facilitate the medium-of-exchange transporter and ledger functions and increase competition in financial services, while eliminating the 'anonymity' problems. In the above description of Ripple, for example, the nodes are clearly money transmitters, and so full registration should be required for all nodes. Such a system can have members that use their own unit of account and store of wealth – such as gold for example. It is not difficult to imagine an entire network using the technology of trust-less transfer amongst all sorts of assets based on an exchange rate with gold, or some other commodity priced in real time or a fiat currency like the dollar – banks, payment system companies, fund managers, insurance companies etc. transacting directly between members without requiring trusted third party intermediaries.

The technology is not a currency, and even if networks do use gold, Bitcoins, XRP coloured coins and the like, this could not interfere with monetary policy and would help to provide much needed competition for credit cards and other payment system functions.

VIII. CONCLUDING COMMENTS

There are genuine policy issues with existing crypto-currencies, including consumer protection and socially unacceptable activities related to tax evasion and money laundering. The payment technology itself, however, could play and important useful role in the financial system.

The generic policy issues that need to be addressed are:

- A general ban on any form of use of crypto currencies in the clearing system between banks and the central bank – to ensure that the monetary system is not undermined.

- Recognition that a trust-less transfer and ledger technology is separable from the idea of a crypto-currency and is potentially very useful for future competition in the financial system.

- Some form of agreement for best practice registration that permits consumer protection, tax and anti-laundering authorities to verify the owner's identity.

- A level playing field for all players in the financial system is important, so balance sheet reporting and income statements for all networks and other appropriate regulations would be important.

- Some amount of capital should be held by exchanges on the balance sheet (perhaps in the form of legal tender) for fraud and technological failures.

- Some form of backing for crypto-currencies may be wise – such as gold.

- The use of government plenary powers to close down all non-complying networks.

The general aim of policy should be to encourage technologies that improve competition in the payments system, and to ensure that the use of crypto-currencies remove anonymity where money transmission is concerned (to avoid the darker aspects of Bitcoin use) and to meet minimum requirements for consumer protection.

REFERENCES

FinCen (2013), "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", 18 March.

Friedman, M. and A. Schwartz (1963). *A Monetary History of the United States, 1867-1960*. Princeton: Princeton University Press.

Goldman Sachs (2014), "All About Bitcoin", in *Top of Mind*, March 11.

Richardson, G., A. Komai and M. Gou (2013), "Roosevelt's Gold Program: Spring 1933", in: 100 Years of the Federal Reserve System, http://www.federalreservehistory.org/Events/DetailView/24.

Sharf, Samantha (2013) "Bitcoin Gets Valued: Bank of America Puts a Price Target on the Virtual Tender", Forbes Magazine, 12 May 2013.

WORKING PAPERS PUBLISHED TO DATE

The full series is listed below in chronological order. Prior to March 2010, the series was named *OECD Working Papers on Insurance and Private Pensions*. All working papers can be accessed online at: www.oecd.org/daf/fin/wp.

2013

WP 36 Institutional investors and infrastructure financing

WP 35 Institutional investors and green infrastructure investments: selected case studies

WP 34 Promoting Financial Inclusion through Financial Education

WP 33 Financial Education in Latin America and the Caribbean

WP 32 Pension Fund Investment in Infrastructure: A Comparison between Australia and Canada

WP 31 Policyholder Protection Schemes: Selected Considerations

2012

WP 30 The Effect of Solvency Regulations and Accounting Standards on Long-Term Investing

WP 29 Trends in Large Pension Fund Investment in Infrastructure

WP 28: Communicating Pension Risk to DC Plan Members: The Chilean Case of a Pension Risk Simulator

WP 27: The Role of Funded Pensions in Retirement Income Systems: Issues for the Russian Federation

WP 26: Infrastructure Investment in New Markets: Challenges and Opportunities for Pension Funds

WP 25: The Status of Financial Education in Africa

WP 24: Defining and Measuring Green Investments: Implications for Institutional Investors' Asset Allocations

WP23: The Role of Institutional Investors in Financing Clean Energy

WP22: Defining and Measuring Green Investments: Implications for Institutional Investors' Asset Allocations

WP21: Identification and Assessment of Publicly Available Data Sources to Calculate Indicators of Private Pensions

WP20: Coverage of Private Pensions Systems: Evidence and Policy Options

WP19: Annual DC Pension Statements and the Communications Challenge

WP18: Lessons from National Pensions Communication Campaigns

WP17: Review of the Swedish National Pension Funds

WP16: Current Status of National Strategies for Financial Education

WP15: Measuring Financial Literacy: Results of the OECD International Network on Financial Education (INFE) Pilot Study

WP14: Empowering Women through Financial Awareness and Education

WP13: Pension Fund Investment in Infrastructure: Policy Actions

WP12: Designing Optimal Risk Mitigation and Risk Transfer Mechanisms to Improve the Management of Earthquake Risk in Chile

2011

WP11: The Role of Guarantees in Defined Contribution Pensions

WP10: The Role of Pension Funds in Financing Green Growth Initiatives

WP9: Catastrophe Financing for Governments

WP8: Funding in Public Sector Pension Plans - International Evidence

WP7: Reform on Pension Fund Governance and Management: The 1998 Reform of Korea National Pension Fund

2010

WP6: Options to Improve the Governance and Investment of Japan's Government Pension Investment Fund

WP5: The New IAS 19 Exposure Draft

WP4: The EU Stress Test and Sovereign Debt Exposures

WP3: The Impact of the Financial Crisis on Defined Benefit Plans and the Need for Counter-Cyclica Funding Regulations

WP2: Assessing Default Investment Strategies in Defined Contribution Pension Plans

WP1: Framework for the Development of Financial Literacy Baseline Surveys: A First International Comparative Analysis

OECD Working Papers on Insurance and Private Pensions

2010

WP41: Policy Action in Private Occupational Pensions in Japan since the Economic Crisis of the 1990s

WP40: Pension Funds' Risk-management Framework: Regulation and Supervisory Oversight

WP38: Managing Investment Risk in Defined Benefit Pension Funds

2009

WP37: Investment Regulations and Defined Contribution Pensions

WP36: Private Pensions and Policy Responses to the Financial and Economic Crisis

WP35: Defined-contribution (DC) arrangements in Anglo-Saxon Countries

WP34: Evaluating the Design of Private Pension Plans

WP33: Licensing Regulation and the Supervisory Structure of Private Pensions

WP32: Pension Fund Investment in Infrastructure

WP31: Pension Coverage and Informal Sector Workers

WP30: Pensions in Africa

WP29: Ageing and the Payout Phase of Pensions, Annuities and Financial Markets

2008

WP27: Fees in Individual Account Pension Systems

WP26: Forms of Benefit Payment at Retirement

WP25: Policy Options for the Payout Phase

WP24: National Annuity Markets

WP23: Accounting for Defined Benefit Plans

WP22: Description of Private Pension Systems

WP21: Comparing Aggregate Investment Returns in Privately Managed Pension Funds

WP20: Pension Fund Performance

WP19: Coverage of Funded Pension Plans

WP18: Pension Fund Governance

WP17: Funding Regulations and Risk Sharing

WP16: Evaluating the Impact of Risk Based Funding Requirements on Pension Funds

WP15: Governance and Investment of Public Pension Reserve Funds in Selected OECD Countries

WP14: Sovereign Wealth and Pension Fund Issues

2007

WP13: Reforming the Valuation and Funding of Pension Promises

WP12: Pension Fund Investment in Hedge Funds

WP11: Implications of Behavioural Economics for Mandatory Individual Account Pension Systems

WP10: Portfolio Investment in an Intertemporal Setting

WP9: Collective Pension Funds

WP8: Pension Fund Regulation and Risk Management

WP7: Survey of Investment Choice by Pension Fund Members

WP6: Benefit Protection

WP5: Benefit Security Pension Fund Guarantee Schemes

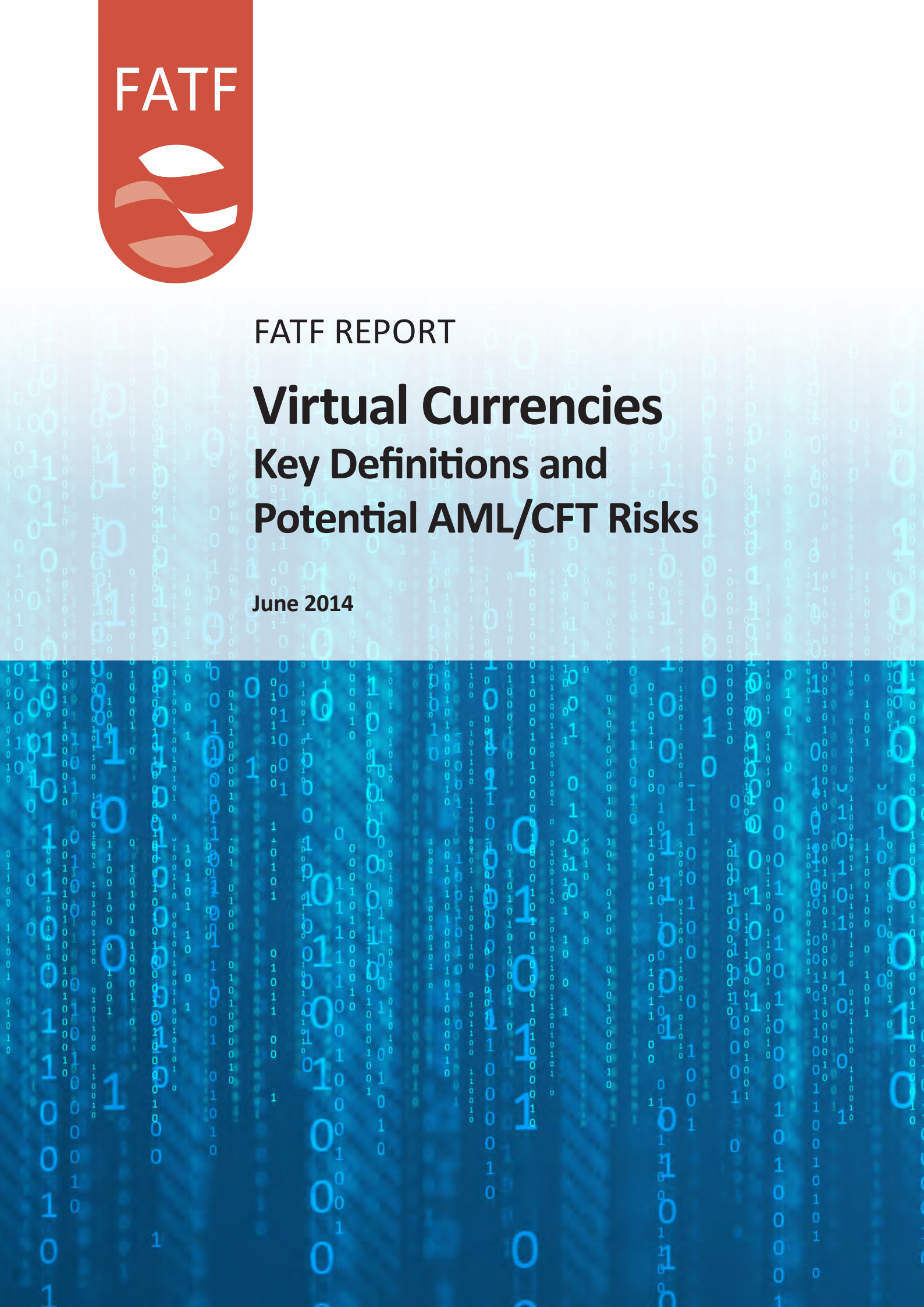
WP4: Governments and the Market for Longevity-Indexed Bonds

WP3: Longevity Risk and Private Pensions

WP2: Policy Issues for Developing Annuities Markets

2006

WP1: Funding Rules and Actuarial Methods



FATF REPORT

Virtual Currencies
Key Definitions and Potential AML/CFT Risks

June 2014

FINANCIAL ACTION TASK FORCE

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

www.fatf-gafi.org

CONTENTS

ACRONYMS

AML/CFT	Anti-money laundering / countering the financing of terrorism
ECB	European Central Bank
FATF	Financial Action Task Force
NPPS Guidance	Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services

VIRTUAL CURRENCIES - KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS[1]

INTRODUCTION

As decentralised, math-based virtual currencies—particularly Bitcoin[2]—have garnered increasing attention, two popular narratives have emerged: (1) virtual currencies are the wave of the future for payment systems; and (2) virtual currencies provide a powerful new tool for criminals, terrorist financiers and other sanctions evaders to move and store illicit funds, out of the reach of law enforcement and other authorities.[3] Against this backdrop, this paper builds on the 2013 New Payment Products and Services (NPPS) Guidance (FATF, 2013) by suggesting a conceptual framework for understanding and addressing the anti-money laundering / countering the financing of terrorism (AML/CFT) risks associated with one kind of internet-based payment system: virtual currencies. Specifically, the paper proposes a common definitional vocabulary that clarifies what virtual currency is and classifies the various types of virtual currency, based on their different business models and methods of operation,[4] and identifies the participants in typical virtual currency systems. It also applies risk factors set forth in Section IV (A) of the 2013 NPPS Guidance to specific types of virtual currencies to identify potential risks; describes some recent investigations and enforcement efforts involving virtual currency; and presents a sample of jurisdictions' current regulatory approaches to virtual currency.

While the 2013 NPPS Guidance broadly addressed internet-based payment services, it did not define "digital currency," "virtual currency," or "electronic money." Nor did it focus on virtual currencies, as distinct from internet-based payment systems that facilitate transactions denominated in real money (fiat or national currency) (e.g., Pay-Pal, Alipay, or Google Checkout). It also did not address decentralised convertible virtual currencies, such as Bitcoin. The 2013 Guidance also notes that, "[g]iven the developing nature of alternate online currencies, the FATF may consider further work in this area in the future" (2013 NPPS Guidance, p. 11, para. 29). A short-term typologies project on this basis was initiated with the following objectives:

- develop a risk-matrix for virtual currencies (or perhaps, more broadly, for both virtual currencies and e-money);
- promote fuller understanding of the parties involved in convertible virtual currency systems and the way virtual currency can be used to operate payment systems; and
- stimulate a discussion on implementing risk-based AML/CFT regulations in this area.

This typologies project may lead to policy work by the FATF, e.g. the issuance of supplemental guidance for applying a risk-based approach to virtual currencies that would incorporate the proposed vocabulary and risk-matrix developed by the typologies project and explain how specific FATF Recommendations apply in the context of virtual currency.

KEY DEFINITIONS:

A common set of terms reflecting how virtual currencies operate is a crucial first step to enable government officials, law enforcement, and private sector entities to analyse the potential AML/CFT

risks of virtual currency as a new payment method. As regulators and law enforcement officials around the world begin to grapple with the challenges presented by virtual currencies, it has become apparent that we lack a common vocabulary that accurately reflects the different forms virtual currency may take. The following set of terms is intended to aid discussion between FATF members. It is important to note that this vocabulary may change as virtual currency evolves and as regulators and law enforcement/government officials continue to consider the challenges virtual currencies present. Nevertheless, the proposed vocabulary aims to provide a common language for developing conceptual tools to help us better understand how virtual currencies operate and the risks and potential benefits they offer.

VIRTUAL CURRENCY

Virtual currency is a digital representation[5] of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment)[6] in any jurisdiction.[7] It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from **fiat currency** (a.k.a. **"real currency," "real money,"** or **"national currency"**), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e**-money**, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status.

Digital currency can mean a digital representation of either virtual currency (non-fiat) or e-money (fiat) and thus is often used interchangeably with the term "virtual currency". In this paper to avoid confusion, only the terms "virtual currency" or "e-money" are used.

CONVERTIBLE VERSUS NON-CONVERTIBLE VIRTUAL CURRENCY

This paper proposes dividing virtual currency into two basic types: convertible and non-convertible virtual currency.[8] Although the paper uses "non-convertible" and "closed", and "convertible" and "open" as synonyms, it should be emphasised that the notion of "convertible currency" does not in any way imply an ex officio convertibility (e.g. in the case of gold standard), but rather a de facto convertibility (e.g. because a market exists). Thus, a virtual currency is "convertible" only as long as some private participants make offers and others accept them, since the "convertibility" is not guaranteed at all by law.

Convertible (or open) virtual currency has an equivalent value in real currency and can be exchanged back-and-forth for real currency.[9] Examples include: Bitcoin; e-Gold (defunct); Liberty Reserve (defunct); Second Life Linden Dollars; and WebMoney.[10]

Non-convertible (or closed) virtual currency is intended to be specific to a particular virtual domain or world, such as a Massively Multiplayer Online Role-Playing Game (MMORPG) or Amazon.com, and under the rules governing its use, cannot be exchanged for fiat currency. Examples include**:** Project Entropia Dollars; Q Coins; and World of Warcraft Gold.

It should be noted that even where, under the terms set by the administrator, a non-convertible currency is officially transferrable only within a specific virtual environment and is not convertible, it is possible that an unofficial, secondary black market may arise that provides an opportunity to exchange the "non-convertible" virtual currency for fiat currency or another virtual currency. Generally, the administrator will apply sanctions (including termination of membership and/or forfeiture of remaining virtual currency) to those seeking to create or use a secondary market, contrary to the rules of the currency.[11] Development of a robust secondary black market in a particular "non-convertible" virtual currency may, as a practical matter, effectively transform it into a convertible virtual currency. A non-convertible characterisation is thus not necessarily static.

CENTRALISED VERSUS NON-CENTRALISED VIRTUAL CURRENCIES

All non-convertible virtual currencies are centralised: by definition, they are issued by a central authority that establishes rules making them non-convertible. In contrast, convertible virtual currencies may be either of two sub-types: centralised or decentralised.

Centralised Virtual Currencies have a single administrating authority (**administrator)**—i.e., a third party[12] that controls the system. An administrator issues the currency; establishes the rules for its use; maintains a central payment ledger; and has authority to redeem the currency (withdraw it from circulation). The exchange rate for a convertible virtual currency may be either **floating**—i.e., determined by market supply and demand for the virtual currency--or **pegged**—i.e., fixed by the administrator at a set value measured in fiat currency or another real-world store of value, such as gold or a basket of currencies. Currently, the vast majority of virtual currency payments transactions involve centralised virtual currencies. Examples: E-gold (defunct); Liberty Reserve dollars/euros (defunct); Second Life "Linden dollars"; PerfectMoney; WebMoney "WM units"; and World of Warcraft gold.

Decentralised Virtual Currencies (a.k.a. crypto-currencies) are distributed[13], open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight. Examples: Bitcoin; LiteCoin; and Ripple.[14]

Cryptocurrency refers to a math-based, decentralised convertible virtual currency that is protected by cryptography.—i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties (in Bitcoin, referred to as miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the "block reward" and in some cases, also transaction fees paid by users as a incentive for miners to include their transactions in the next block). Hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, which uses a proof-of-work system to validate transactions and maintain the block chain. While Bitcoin provided the first fully implemented cryptocurrency protocol, there is growing interest in developing alternative, potentially more efficient proof methods, such as systems based on proof-of-stake.

Bitcoin, launched in 2009, was the first decentralised convertible virtual currency, and the first cryptocurrency. Bitcoins are units of account composed of unique strings of numbers and letters

that constitute units of the currency and have value only because individual users are willing to pay for them. Bitcoins are digitally traded between users with a high degree of anonymity and can be exchanged (purchased or cashed out) into US dollars, Euros, and other fiat or virtual currencies. Anyone can download the free, open-source software from a website to send, receive, and store bitcoins and monitor Bitcoin transactions. Users can also obtain Bitcoin addresses, which function like accounts, at a Bitcoin exchanger or online wallet service. Transactions (fund flows) are publicly available in a shared transaction register and identified by the Bitcoin address, a string of letters and numbers that is not systematically linked to an individual.. Therefore, Bitcoin is said to be "pseudo-anonymous". Bitcoin is capped at 21 million bitcoins (but each unit could be divided in smaller parts), projected to be reached by 2140.[15] As of April 2, 2014, there were over 12-and-a-half million bitcoins, with total value of slightly more than USD 5.5 billion, based on the average exchange rate on that date.

Altcoin refers to math-based decentralised convertible virtual currency other than bitcoins, the original such currency. Current examples include Ripple; PeerCoin, Lite-coin; zerocoin; anoncoin and dogecoin. One popular exchanger, Cryptsy, would reportedly exchange over 100 different virtual currencies (as of 2 April 2014). (Popper, N., 2013)

Anonymiser (anonymising tool) refers to tools and services, such as darknets and mixers, designed to obscure the source of a Bitcoin transaction and facilitate anonymity. (Examples: Tor (darknet); Dark Wallet (darknet); Bitcoin Laundry (mixer)).

Mixer (laundry service, tumbler) is a type of anonymiser that obscures the chain of transactions on the blockchain by linking all transactions in the same bitcoin address and sending them together in a way that makes them look as if they were sent from another address. A mixer or tumbler sends transactions through a complex, semi-random series of dummy transactions that makes it extremely difficult to link specific virtual coins (addresses) with a particular transaction. Mixer services operate by receiving instructions from a user to send funds to a particular bitcoin address. The mixing service then "comingles" this transaction with other user transactions, such that it becomes unclear to whom the user intended the funds to be directed. (Examples: Bitmixer.io; SharedCoin; Blockchain.info; Bitcoin Laundry; Bitlaunder; Easycoin).

Tor (originally, The Onion Router) is an underground distributed network of computers on the Internet that conceals the true IP addresses, and therefore the identities of the network's users, by routing communications/transactions through multiple computers around the world and wrapping them in numerous layers of encryption. Tor makes it very difficult to physically locate computers hosting or accessing websites on the network. This difficulty can be exacerbated by use of additional tumblers or anonymisers on the Tor network. Tor is one of several underground distributed computer networks, often referred to as darknets, cypherspace, the Deep web, or anonymous networks, which individuals use to access content in a manner designed to obscure their identity and associated Internet activity.

Dark Wallet is a browser-based extension wallet, currently available on Chrome (and potentially on Firefox), that seeks to ensure the anonymity of Bitcoin transactions by incorporating the following features: auto-anonymiser (mixer); decentralised trading; uncensorable crowd funding platforms; stock platforms and information black markets; and decentralised market places similar to Silk Road.

Cold Storage refers to an offline Bitcoin wallet—i.e., a Bitcoin wallet that is not connected to the Internet. Cold storage is intended to help protect the stored virtual currency against hacking and theft.

Hot Storage refers to an online bitcoin wallet. Because it is connected to the Internet, hot storage is more vulnerable to hacking/theft than cold storage.

Local Exchange Trading System (LETS) is a locally organised economic organisation that allows members to exchange goods and services with others in the group. LETS use a locally created currency to denominate units of value that can be traded or bartered in exchange for goods or services. Theoretically, bitcoins could be adopted as the local currency used within a LETS. (Examples: Ithica Dollars; Mazacoin).

VIRTUAL CURRENCY SYSTEM PARTICIPANTS

An **exchanger (also sometimes called a virtual currency exchange)** is a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, non-affiliated, or a third party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts.

An **administrator** is a person or entity engaged as a business in **issuing** (putting into circulation) a centralised virtual currency, establishing the rules for its use; maintaining a central payment ledger; and who has the authority to **redeem** (withdraw from circulation) the virtual currency.

A **user** is a person/entity who obtains virtual currency and uses it to purchase real or virtual goods or services or send transfers in a personal capacity to another person (for personal use), or who holds the virtual currency as a (personal) investment. Users can obtain virtual currency in several ways. For example, they can (1) purchase virtual currency, using real money (from an exchanger or, for certain centralised virtual currencies, directly from the administrator/issuer); (2) engage in specific activities that earn virtual currency payments (e.g., respond to a promotion, complete an online survey, provide a real or virtual good or service); (3) with some decentralised virtual currencies (e.g., Bitcoin), self-generate units of the currency by "mining" them (see definition of miner, below),and receive them as gifts, rewards, or as part of a free initial distribution.

A **miner** is an individual or entity that participates in a decentralised virtual currency network by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system used to validate transactions in the virtual currency system. Miners may be users, if they self-generate a convertible virtual currency solely for their own purposes, e.g., to hold for investment or to use to pay an existing obligation or to purchase goods and services. Miners may also participate in a virtual currency system as exchangers, creating the virtual currency as a business in order to sell it for fiat currency or other virtual currency.

Virtual currency wallet is a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency.

A wallet provider is an entity that provides a virtual currency wallet (i.e., a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency). A wallet holds the user's private keys, which allow the user to spend virtual currency allocated to the virtual currency address in the block chain. A wallet provider facilitates participation in a virtual currency system by allowing users, exchangers, and merchants to more easily conduct the virtual currency transactions. The wallet provider maintains the customer's virtual currency balance and generally also provides storage and transaction security. For example, beyond providing bitcoin addresses, the wallet may offer encryption; multiple key (multi-key) signature protection, backup/cold storage; and mixers. All Bitcoin wallets can interoperate with each other. Wallets can be stored both online ("hot storage") or offline ("cold storage"). (Examples: Coinbase; Multibit; Bitcoin Wallet).

In addition, various **other entities** may participate in a virtual currency system and may be affiliated with or independent of exchangers and/or administrators. These include web **administration service providers (a.k.a. web administrators**); **third party payments senders** facilitating merchant acceptance; **software developers**; and **application providers** (some of the "other entities" listed in this paragraph may already fall into one of the categories above.). Applications and software development can be for legitimate purposes—e.g., to increase ease of merchant acceptance and customer payments or to respond to legitimate privacy concerns—or for illicit purposes—e.g., a mixer developer/operator can target illicit users with products designed to avoid regulatory and law enforcement scrutiny.

It must be emphasised that this list of participants is not exhaustive. Moreover, given the rapid development of virtual currency technologies and business models, additional participants could arise within virtual currency systems and pose potential AML/CFT risks.

Taxonomy of Virtual Currencies

	Centralised	**Decentralised**
Convertible	Administrator, exchangers, users; third-party ledger; can be exchanged for fiat currency. Example: WebMoney	Exchangers, users (no administrator); no Trusted Third-Party ledger; can be exchanged for fiat currency. Example: Bitcoin
Non-convertible	Administrator, exchangers, users; third-party ledger; cannot be exchanged for fiat currency. Example: World of Warcraft Gold	Does not exist

LEGITIMATE USES

Like other new payment methods, virtual currency has legitimate uses, with prominent venture capital firms investing in virtual currency start-ups. Virtual currency has the potential to improve

payment efficiency and reduce transaction costs for payments and fund transfers. For example, Bitcoin functions as a global currency that can avoid exchange fees, is currently processed with lower fees/charges than traditional credit and debit cards, and may potentially provide benefit to existing online payment systems, like Paypal.[16] Virtual currency may also facilitate micro-payments, allowing businesses to monetise very low-cost goods or services sold on the Internet, such as one-time game or music downloads. At present, as a practical matter, such items cannot be sold at an appropriately low per/unit cost because of the higher transaction costs associated with e.g., traditional credit and debit. Virtual currency may also facilitate international remittances and support financial inclusion in other ways, as new virtual currency-based products and services are developed that may potentially serve the under- and un-banked. Virtual currency - notably, Bitcoin- may also be held for investment. These potential benefits need to be carefully analysed, including whether claimed cost advantages will remain if virtual currency becomes subject to regulatory requirements similar to those that apply to other payments methods, and/or if exchange fees for cashing out into fiat currency are factored in, and whether volatility, consumer protection and other factors[17] limit their potential for financial inclusion.

POTENTIAL RISKS

Convertible virtual currencies that can be exchanged for real money or other virtual currencies are potentially vulnerable to money laundering and terrorist financing abuse for many of the reasons identified in the 2013 NPPS Guidance. First, they may allow greater anonymity than traditional non-cash payment methods. Virtual currency systems can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified.

Decentralised systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached, and the system has no central server or service provider. The Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity. There is no central oversight body, and no AML software currently available to monitor and identify suspicious transaction patterns. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger may collect). It thus offers a level of potential anonymity impossible with traditional credit and debit cards or older online payment systems, such as PayPal.

Virtual currency's global reach likewise increases its potential AML/CFT risks. Virtual currency systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers. In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more

difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of decentralised virtual currency technology and business models, including the changing number and types/roles of participants providing services in virtual currency payments systems. And importantly, components of a virtual currency system may be located in jurisdictions that do not have adequate AML/CFT controls. Centralised virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes. Decentralised convertible virtual currencies allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country.

LAW ENFORCEMENT ACTIONS INVOLVING VIRTUAL CURRENCY

Law enforcement is already seeing cases that involve the abuse of virtual currency for money laundering purposes. Examples include:

LIBERTY RESERVE

In what is to date the largest online money-laundering case in history, in May 2013, the US Department of Justice charged Liberty Reserve, a Costa Rica-based money transmitter, and seven of its principals and employees with operating an unregistered money transmitter business and money laundering for facilitating the movement of more than 6 billion USD in illicit proceeds. In a coordinated action, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the US financial system.

Established in 2006, Liberty Reserve was designed to avoid regulatory and law enforcement scrutiny and help criminals distribute, store, and launder the proceeds of credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography by enabling them to conduct anonymous and untraceable financial transactions. Operating on an enormous scale, it had more than a million users worldwide, including more than 200 000 in the United States, and handled approximately 55 million transactions, almost all of which were illegal. It had its own virtual currency, Liberty Dollars (LR), but at each end, transfers were denominated and stored in fiat currency (US dollars).

To use LR currency, a user opened an account through the Liberty Reserve website. While Liberty Reserve ostensibly required basic identifying information, it did not validate identities. Users routinely established accounts under false names, including blatantly criminal names ("Russia Hackers," "Hacker Account," "Joe Bogus") and blatantly false addresses ("123 Fake Main Street, Completely Made Up City, New York"). To add a further layer of anonymity, Liberty Reserve required users to make deposits and withdrawals through recommended third-party exchangers—generally, unlicensed money transmitting businesses operating in Russia, and in several countries without significant governmental money laundering oversight or regulation at that time, such as Malaysia, Nigeria, and Vietnam. By avoiding direct deposits and withdrawals from users, Liberty Reserve evaded collecting information about them through banking transactions or other activity that would create a central paper trail. Once an account was established, a user could conduct transactions with other Liberty Reserve users by transferring LR from his or her account to other

users, including front company "merchants" that accepted LR as payment. For an extra "privacy fee" (75 US cents per transaction), users could hide their Liberty Reserve account numbers when transferring funds, making the transfers completely untraceable. After learning it was being investigated by US law enforcement, Liberty Reserve pretended to shut down in Costa Rica but continued to operate through a set of shell companies, moving millions through their accounts in Australia, Cyprus, China, Hong Kong, Morocco, Russia, Spain and elsewhere.[18]

SILK ROAD

In September 2013, the US Department of Justice unsealed a criminal complaint charging the alleged owner and operator of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs, weapons, stolen identity information and other unlawful goods and services anonymously and beyond the reach of law enforcement, with narcotics trafficking, computer hacking, and money laundering conspiracies. The Justice Department also seized the website and approximately 173 991 bitcoins, worth more than USD 33.6 million at the time of the seizure, from seized computer hardware. The individual was arrested in San Francisco in October and indicted in February 2014; the investigation is ongoing.

Launched in January 2011, Silk Road operated as a global black-market cyber bazaar that brokered anonymous criminal transactions and was used by several thousand drug dealers and other unlawful vendors to distribute unlawful goods and services to over a hundred thousand buyers, a third of whom are believed to have been in the United States. It allegedly generated total sales revenue of approximately USD 1.2 billion (more than 9.5 million bitcoins) and approximately USD 80 million (more than 600 000 bitcoins) in commissions for Silk Road. Hundreds of millions of dollars were laundered from these illegal transactions (based on bitcoin value as of dates of seizure). Commissions ranged from 8 to 15 percent of total sales price.

Silk Road achieved anonymity by operating on the hidden Tor network and accepting only bitcoins for payment. Using bitcoins as the exclusive currency on Silk Road allowed purchasers and sellers to further conceal their identity, since senders and recipients of peer-to-peer (P2P) bitcoin transactions are identified only by the anonymous bitcoin address/account. Moreover, users can obtain an unlimited number of bitcoin addresses and use a different one for each transaction, further obscuring the trail of illicit proceeds. Users can also employ additional "anonymisers," beyond the tumbler service built into Silk Road transactions (see discussion below).

Silk Road's payment system functioned as an internal Bitcoin bank, where every Silk Road user had to hold an account in order to conduct transactions on the site. Every Silk Road user had at least one Silk Road Bitcoin address (and potentially thousands) associated with the user's Silk Road account, stored on wallets maintained on servers controlled by Silk Road. To make a purchase, a user obtained bitcoins (typically through a Bitcoin exchanger) and sent them to a Bitcoin address associated with his or her Silk Road account to fund the account. When a purchase was made, Silk Road transferred the user's bitcoins to an escrow account it maintained, pending completion of the transaction, and then transferred the user's / buyer's bitcoins from the escrow account to the vendor's Silk Road Bitcoin address. As a further step, Silk Road employed a "tumbler" for every purchase, which, as the site explained, "sen[t] all payments through a complex, semi-random series

of dummy transactions ... --making it nearly impossible to link your payment with any [bit]coins leaving the site."[19]

WESTERN EXPRESS INTERNATIONAL

An eight-year investigation of a multinational, Internet-based cybercrime group, the Western Express Cybercrime Group, resulted in convictions or guilty pleas of 16 of its members for their role in a global identity theft/cyberfraud scheme. Members of the cybercrime group interacted and communicated primarily through Internet "carding" web sites devoted to trafficking in stolen credit card and personal identifying information and used false identities, anonymous instant messenger accounts, anonymous email accounts, and anonymous virtual currency accounts to conceal the existence and purpose of the criminal enterprise; avoid detection by law enforcement and regulatory agencies; and maintain their anonymity.

The criminal enterprise was composed of vendors, buyers, cybercrime services providers, and money movers located in numerous countries, ranging from Ukraine and throughout Eastern Europe to the United States. The vendors sold nearly 100 000 stolen credit card numbers and other personal identification information through the Internet, taking payment mostly in e-Gold and WebMoney. The buyers used the stolen identities to forge credit cards and purchase expensive merchandise, which they fenced (including via reshipping schemes), committing additional crimes, such as larceny, criminal possession of stolen property, and fraud, and generating about USD 5 million in credit card fraud proceeds. The cybercrime services providers promoted, facilitated, and aided in the purchase, sale and fraudulent use of stolen credit card numbers and other personal identifying information by providing computer services to the vendors and the buyers. The money mover laundered the cybercrime group's illicit proceeds in a variety of high-tech ways, moving more than USD 35 million through various accounts.

The hub of the entire operation was Western Express International, Inc., a New York corporation based in Manhattan that operated as a virtual currency exchanger and unregistered money transmitter to coordinate and facilitate the Internet payment methods used by the criminal enterprise, and to launder the group's proceeds. One of the largest virtual currency exchangers in the United States, Western Express International exchanged a total of USD 15 million in WebMoney and USD 20 million in e-Gold for the cybercrime group and used banks and traditional money transmitters to move large sums of money. It also provided information and assistance through its websites (including Dengiforum.com and Paycard2000.com) on ways to move money anonymously and to insulate oneself from reporting requirements.

Western Express International and its owner/operator, a Ukrainian national, plead guilty in February 2013 in New York State to money laundering, fraud, and conspiracy offenses. (In February 2006, Western Express was also indicted for running an illegal check cashing/wire transfer service.) Three other defendants were convicted after trial in June 2013; several more plead guilty in August 2009. Two indicted defendants remain fugitives. The investigation was conducted jointly by the US Secret Service and the Manhattan (New York County) District Attorney's Office and was successfully prosecuted by the Manhattan District Attorney's Office.

NOTES

[1] The first draft of this paper was prepared jointly by Australia, Canada, Russia, the United Kingdom and the United States for the FATF meetings in February 2014. After that all delegations were invited to provide comments on the draft with a view to adopting a final paper at the next meeting. Comments were received from 10 delegations, and these have been taken into account in preparing this revision.

[2] "Bitcoin" (capitalised) refers to both the open source software used to create the virtual currency and the peer-to-peer (P2P) network formed as a result; "bitcoin" (lowercase) refers to the individual units of the virtual currency.

[3] It should also be noted that some observers, including former US Federal Reserve Chairman Alan Greenspan, Nout Wellink, a former President of the Dutch Central Bank, and Nobel Laureate economist Robert Shiller, maintain that virtual currency is a passing fad or bubble, akin to Tulipmania in 17th Century Netherlands.

[4] Virtual currency is a complex subject that implicates not only AML/CFT issues, but also other regulatory matters, including consumer protection, prudential safety, tax and soundness regulation, and network IT security standards. The proposed vocabulary is thus relevant across a number of complementary regulatory jurisdictions. Adoption of consistent terms and a common conceptual understanding of virtual currency by all relevant government entities is important to avoid duplicating efforts and/or working at unintended cross purposes, and facilitates the capacity of governmental authorities to leverage their various perspectives and areas of expertise in order to most effectively identify and address relating to virtual currencies.

[5] **Digital representation** is a representation of something in the form of digital data—i.e., computerised data that is represented using discrete (discontinuous) values to embody information, as contrasted with continuous, or analog signals that behave in a continuous manner or represent information using a continuous function. A physical object, such as a flash drive or a bitcoin, may contain a digital representation of virtual currency, but ultimately, the currency only functions as such if it is linked digitally, via the Internet, to the virtual currency system.

[6] Legal tender status does not necessarily require an entity or individual to accept payment in a particular type of legal tender. For example, in many jurisdictions, a private business, person, or organisation is free to develop internal policies on whether or not to accept the jurisdiction's physical currency or coins (cash) as payment for goods and/or services.

[7] This definition differs from that offered in 2012 by the European Central Bank (ECB), which defined virtual currency "as a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community" ECB, *Virtual Currency Schemes* (October 2012), p. 6. The ECB recognised on p.13 of its report that its "definition may need to be adapted in future if fundamental characteristics change." Its definition now appears too limited, since math-based, decentralised virtual currencies like Bitcoin are not issued and controlled by a central developer, and some jurisdictions (e.g., the United States, Sweden, and Thailand) now regulate virtual currencies.

[8] This categorisation differs from the ECB's three-part classification, which divides virtual currencies into three types: "Type 1 . . . refer[s] to closed virtual currency schemes . . . used in an online game. Type 2 . . . [refers to] schemes [that] have a unidirectional flow (usually an inflow), i.e. there is a conversion rate for purchasing the virtual currency, which can … be used to buy virtual goods and services . . . (and exceptionally also … real goods and services) . . . Type 3 [refers to] schemes . . .[with] bidirectional flows, i.e. the virtual currency . . . acts like any . . . convertible [real] currency, with . . . [buy and sell] exchange rates . . . [and] can . . . be used to buy [both] virtual . . . [and] real goods and services." ECB *Virtual Currency Schemes*, p. 6. This discussion paper adopts a simpler, bifurcated classification because at present, only (fully) convertible virtual currencies that can be used to move value into and out of the formal financial sector present significant AML/CFT risks. This is because money laundering requires: Conversion or transfer (of illicit funds); concealment or disguise of the source/origin (of illicit funds); or acquisition/possession/use (of illicit funds).

[9] Some convertible virtual currencies can be exchanged directly through the issuing administrator (directly exchanged); others must be exchanged through a virtual currency exchanger (third-party exchanged).

[10] For example, WebMoney is a virtual currency because "valuables" (assets) are transferred and stored in the form of a non-fiat currency, The units of measurement of the valuables' property rights stored by the guarantor are WebMoney Title Units (WM) of the corresponding type. http://wmtransfer.com/eng/about/

[11] For example, despite such deterrence measures, several exchanges allow blackmarket conversion of World of Warcraft Gold.

[12] A third-party is an individual or entity that is involved in a transaction but is not one of the principals and is not affiliated with the other two participants in the transaction—i.e., a third party functions as a neutral entity between the principals (e.g., sender and receiver, buyer and seller) in a business or financial transaction. The third party's involvement varies with the type of business or financial transaction. For example, an online payment portal, such as PayPal, acts as a third party in a retail transaction. A seller offers a good or service; a buyer uses a credit or debit card entered through the PayPal payment service; and the trusted third party completes the financial transfer. Similarly, in a real estate transaction, a third-party escrow company acts as a neutral agent between the buyer and seller, collecting the documents from the seller and money from the buyer that the two principals need to exchange to complete the transaction.

[13] Distributed is a term of art that refers to an essential feature of decentralised math-based virtual currencies: transactions are validated by a *distributed* proof-of-work system. Each transaction is *distributed* among a network of participants who run the algorithm to validate the transaction.

[14] Apart from the initial creation and issuance of ripple coins (RXP), Ripple operates as a decentralised virtual currency. Ripple's founders created all 100 billion ripple coins and retained 20 billion of them, with the remainder to be distributed by a separate entity, Ripple Labs. However, all transactions are verified by a decentralised computer network, using Ripple's open source protocol, and recorded in a shared ledger that is a constantly updated database of Ripple accounts and transactions.

[15] In 2140, the block award will cease to be available and miners will be rewarded only by transaction fees.

[16] For example, PayPal is actively looking at accepting and clearing bitcoins on the PayPal platform, and JP Morgan Chase has filed a US patent application for an online electronic payments system using a math-based virtual currency protocol that would enable users to make anonymous payments without providing an account number or name, with the virtual currency to be stored on JPMC computers and verified through a shared log, much like the 'block chain' in the bitcoin system.

[17] For instance, it remains to be seen whether virtual currency systems can provide a pathway to other financial services, like credit and insurance.

[18] The Liberty Reserve investigation and takedown involved law enforcement action in 18 countries and jurisdictions, including Costa Rica; the Netherlands; Spain; Morocco; Sweden; Switzerland; Cyprus; Australia; China; Hong Kong, China; Norway; Latvia; Luxembourg; the United Kingdom; Russia; Canada; and the United States to restrain criminal proceeds, forfeit domain names, and seize servers.

[19] The Silk Road investigation involved multiple US law enforcement agencies, led the Federal Bureau of Investigation's (FBI')s New York Special Operations and Cyber Division, and the Drug Enforcement Administration's (DEA's) New York Organized Crime Drug Enforcement Strike Force (comprised of agents and officers of DEA, the Internal Revenue Service (IRS), the New York City Police Department, US Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), the New York State Police, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the US Secret Service, the US Marshals Service, Office of Foreign Assets Control (OFAC), and NY Department of Taxation), with assistance and support of the ICE-HIS Chicago field office, the Department of Justice's Computer Crime and Intellectual Property and Asset Forfeiture and Money Laundering Sections, the United States Attorney's Office for the Southern District of New York, and foreign law enforcement partners, particularly the Reykjavik Metropolitan Police of the Republic of Iceland and the French Republic's Central Office for the Fight Against Crime Linked to Information Technology and Communication.

BIBLIOGRAPHY AND SOURCES

FATF (2013), FATF *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services,* FATF, Paris
www.fatf-gafi.org/topics/fatfrecommendations/documents/rba-npps-2013.html

Popper, N. (2013), "In Bitcoin's Orbit: Rival Virtual Currencies vie for Acceptance", in *New York Times, Dealb%k,* (Nov. 24, 2013) http://dealbook.nytimes.com/2013/11/24/in-bitcoins-orbit-rival-virtual-currencies-vie-for-acceptance/?_r=0, accessed June 2014.