History of Electronic and Virtual Currencies

Traditionally, currencies have been tied to physical tangible items, such as paper or gold, and have provided three functions: a medium of exchange, a unit of account, and a store of value. The earliest published research using cryptography as a basis for electronically transferring cash is from 1982[1] by David Chaum, a Ph.D. graduate in Computer Science from the University of California at Berkeley[2]. He founded a company in 1990 called DigiCash[3], which originally sold smart cards for use in closed systems, such as highway tolls. In 1994, the company sent the first electronic cash ("ecash") payment over public computer networks.[4] Although the history of DigiCash is controversial, most sources criticize two main decisions made by management: not forming the right business partnerships soon enough and designing centralized and closed source software.[5] Other companies, such as Dexit, InternetCash, Qpass, Flooz, Mondex, and NetCheque, performed similar online payments, but none of these companies have gained meaningful traction due to the complexities and expenses of navigating the technological, economic, legal, political, social, and cultural challenges in virtualizing currencies.[6][7]

The two most common types of virtual currencies are: currencies used inside video games or ecosystems, and cryptocurrencies. Some popular gaming and ecosystem virtual currencies are: Linden Dollars used in the game Second Life, Amazon Coins used on the Kindle Fire HD, Facebook Credits used on Facebook, Microsoft Points used on its Xbox and Zune products, and airline frequent flyer programs. These virtual currencies are all centralized, monitored, controlled, and use closed source software. The majority of these virtual currencies flow in one direction, from fiat to virtual, except for Linden Dollars, which flow both directions. A cryptocurrency is loosely defined as a digital or virtual currency that relies on cryptography for security.[8] In 2008, a paper was published by a person or group known as "Satoshi Nakamoto" that defined a cryptocurrency called Bitcoin.[9] A year later, Bitcoin was considered to be the first cryptocurrency to trade relying on the claims of an open, decentralized, distributed, and secure protocol.

Over the last few years, three main factors have contributed to a conducive environment for cryptocurrencies: an unstable economic period, expensive fees on money transfers, and a proliferation of computing devices. First, the severe recessions in many countries from 2008 to 2011 contributed to an increase in unemployment and a decrease in the U.S. consumer confidence level, which reached a historic low.[10][11] Second, money transfer fees abroad were high, with a global average of 9.8% for sending 200 U.S. dollars in 2008.[12] Third, there was a proliferation of computing devices in which more

[1] http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF
[2] http://www.chaum.com/
[3] http://archive.wired.com/wired/archive/2.12/emoney_pr.html
[4] https://w2.eff.org/Privacy/Digital_money/?f=digicash.announce.txt
[5] http://cryptome.org/jya/digicrash.htm
[6] http://felix.openflows.com/html/digicash.html
[7] http://cryptome.org/jya/digicrash.htm
[8] http://www.investopedia.com/terms/c/cryptocurrency.asp
[9] https://bitcoin.org/bitcoin.pdf
[10] http://online.wsj.com/news/articles/SB126073152465089651
[11] http://en.wikipedia.org/wiki/File:U.S._Consumer_Confidence_Index.png
[12] http://remittanceprices.worldbank.org/

than 80% of the households in the U.S. had some type of PC, and almost half had more than one by 2011.[13] In addition, as of 2013, 56% of U.S. adults had smartphones.[14]

Emerging Cryptocurrencies

Bitcoin was published first and many other cryptocurrencies followed. By market size in U.S. dollars, the top four cryptocurrencies as of May 2014 are: Bitcoin at $5.6B, Litecoin at $299M, Peercoin at $44M, and Dogecoin at $36M.[15] The majority of cryptocurrencies share the same core software, which comes from Bitcoin. Litecoin was released in 2011, Peercoin the next year, and Dogecoin the following year in 2013.

Attributes of Cryptocurrencies

Current cryptocurrencies all share some general attributes, such as being decentralized, maintaining public ledgers, and being based off Bitcoin's core open source software. Other attributes vary between cryptocurrencies, such as the size of the currency supply, rate of releasing new units of currency, amount of the transaction fees, and level of anonymity (Exhibit 1). The decentralized nature of cryptocurrencies prevents any single authority, such as a central bank or government, from ultimate control. By maintaining a public ledger, known as a blockchain, cryptocurrencies provide transparency, which is essential for building trust between untrusted parties. With the core software open sourced, anybody can view, submit bug fixes, or submit updates, which in turn helps improve the system.

Cryptocurrencies vary in the size of the coin supply with Bitcoin at a fixed 21M and other cryptocurrencies with flexible or no limits to the supply, in an effort to avoid being a deflationary currency. The rate at which the currency is released also varies among cryptocurrencies, with Bitcoin releasing 25 coins roughly every 10 minutes to Dogecoin releasing a random amount every minute. Transaction fees also differ. Bitcoin doesn't require transaction fees, but expedites transactions with fees[16]. In contrast, Dogecoin does require transaction fees. The majority of cryptocurrencies are generally not considered anonymous. The Bitcoin Foundation warns that "Bitcoin is not anonymous and cannot offer the same level of privacy as cash."[17] The lack of anonymity is attributed to the extensive public records maintained in the transaction ledger. Theoretically, by using sophisticated data mining techniques, it may be possible to trace the history of any transaction, identify users, or identify patterns in transactions and activities, even years after the fact. The Federal Bureau of Investigation has not released how, but they were able to locate and seize 144,000 Bitcoins (~$65M*) that they claim belonged to the operator of Silk Road, an online black market for drugs.[18] Zerocoin[19] was announced in 2013 as an extension to

---

[13] http://blogs.forrester.com/reineke_reitsma/11-04-29-the_data_digest_how_many_us_households_have_multiple_pcs
[14] http://marketingland.com/pew-61-percent-in-us-now-have-smartphones-46966
[15] http://coinmarketcap.com/
[16] https://bitcoin.org/en/faq#how-much-will-the-transaction-fee-be
[17] https://bitcoin.org/en/faq#is-bitcoin-anonymous
[18] http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/
[19] http://zerocoin.org/

make Bitcoin completely anonymous, but the Bitcoin Foundation has not expressed interest in incorporating Zerocoin.

Technology behind Cryptocurrencies

As Bitcoin was the original open source cryptocurrency, most others are built using the same core technologies, such as keys, wallets, miners, and decentralized peer-to-peer networks. Ownership of cryptocurrencies requires a pair of keys (one public and one private), each a unique string of numbers and letters. A public key functions as an "address", to which other users send units of the cryptocurrency. A private key is kept confidential and allows a user to claim ownership of the associated cryptocurrency units. Wallets store the cryptographic keys that are used to access a cryptocurrency. There are three main types of wallets (Exhibit 2): device-based, cloud-based, and paper-based. There are varying levels of security between the different wallets, with cloud-based considered weaker and paper-based considered stronger. The level of convenience varies inversely with the level of security. Miners serve two important functions, verifying and confirming transactions as well as introducing new units of currency. Mining software varies for each cryptocurrency but is usually based on popular and complex "proof-of-work" functions that commonly rely on either the industry standard SHA-256 cryptographic hash function, designed by the U.S. National Security Agency, or scrypt, published by the Internet Engineering Task Force (IETF). Proof-of-work functions consist of a computation that is extremely difficult to solve, but very easy to verify.[20] A peer-to-peer network is a distributed set of computers that act as both servers and clients, similar to Napster and Bittorrent. Each peer-to-peer node confirms and relays transactions throughout the network, creating a decentralized system. Bitcoin developers have kept the core software open to the public, allowing alternative cryptocurrencies to be easily created by cloning and modifying Bitcoin's software.

Risks to Cryptocurrencies

As with all currencies, cryptocurrencies come with risks. The more prominent risks come from theft, fraud, volatility, technical failures, lack of government support, regulatory uncertainty, competition from other currencies, and level of adoption. Many of these risks could result in one or more cryptocurrencies losing all value. For cryptocurrencies, theft most often occurs online from either an insider, an individual who works at or has physical access to the company, or an outside individual, who gains unauthorized access to the company's or individual's systems online through a hack. In both cases, control of the cryptocurrency is transferred away from the owner. There have been two main targets for theft: exchanges and users. Over the last five years, many cryptocurrency exchanges have been hacked resulting in theft and the loss of cryptocurrency. These types of online theft are not uncommon and are similar to the hack that impacted Target, where over 40 million credit card numbers were stolen in November 2013 and which is estimated to cost Target billions in damages.[21] In addition to targeting exchanges, hackers have also successfully targeted many users who store cryptocurrency on their desktops, laptops, or mobile phones. Fraud occurs in cryptocurrencies as well. The most famous case is that of Trendon Shavers, who the Securities And Exchange Commission (SEC) has charged

[20] https://en.bitcoin.it/wiki/Proof_of_work
[21] http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

with running a Ponzi scheme that Shavers called Bitcoin Savings and Trust.[22] The SEC alleges that Shavers promised up to 7% weekly interest on Bitcoin deposits, but instead paid old investors with the funds from new investors. Generally, currencies can be very volatile (quickly appreciate and depreciate) and central banks typically go through extensive efforts to minimize that volatility. As a currency appreciates, currency holders often delay spending and as a currency depreciates, currency holders often accelerate spending. As cryptocurrencies have no central monetary authority, there is no limit to their volatility. Over the last year, Bitcoin has been five times more volatile than the Ukrainian Hryvnia and 12 times more volatile than the Euro (Exhibit 3). The scope for technical failures is quite broad given the short history and combination of new technologies involved in cryptocurrencies. Technical issues can impact any system dealing with cryptocurrencies, including the software for wallets, mining, nodes, transactions, or exchanges. No cryptocurrency has government-provided insurance against loss or a central bank acting as a lender of last resort. Regulation and guidelines on cryptocurrencies differ by geographic region and in many countries there is a lot of legal ambiguity (Exhibit 4). In the U.S., there is no specific cryptocurrency law passed by Congress, but various federal agencies and state governments have issued interpretations. At the federal level, in March of 2013, FinCEN (Financial Crimes Enforcement Network) issued an interpretation of existing law claiming that decentralized virtual currencies, such as Bitcoin, are a form of currency.[23] A year later, the Internal Revenue Service released a public notice stating that Bitcoin is to be treated as property.[24] In addition, each of the 50 states in the U.S. has its own money transmitter laws that might or might not apply to cryptocurrencies. In China, some institutions handling Bitcoins have reported that their bank accounts were closed by the People's Bank of China (PBOC), while others have remained open.[25] Another risk comes from the competitive nature of currencies and cryptocurrencies, which could result in some or all cryptocurrencies collapsing. Finally, there is the possibility that not enough people will adopt a currency, limiting its utility.

The notorious case of Magic The Gathering Online eXchange's (Mt. Gox) bankruptcy has yet to be cleanly sorted. Prior to Mt. Gox filing for bankruptcy on February 28th, 2014 due to losses from "hackers"[26], there were two prior events where Mt. Gox lost Bitcoins and one prior event where Mt. Gox lost U.S. dollars. In June of 2011, Mt. Gox lost 2,000 BTC (~$900,000)* and leaked users' logins and passwords.[27] Four months later, in October of 2011, Mt. Gox improperly programmed a transaction which resulted in destroying 2,609 BTC (~$1.1M)*. The Department of Homeland Security, in May of 2013, claimed "that there's probable cause to believe Mt. Gox is engaging in 'money transmitting' without a license" and seized around $5M of Mt. Gox's funds.[28][29] In the bankruptcy filings Mt. Gox indicates that it lost 750,000 BTC (~$338M)* of customer funds and 100,000 BTC (~$45M)* of company funds. A few weeks later, Mt. Gox announced that it discovered 200,000 BTC ($90M)* in an old file.[30] In one of four class-action lawsuits against Mt. Gox, plaintiffs' lawyers say "Mt. Gox knew it was in trouble long

[22] http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539730583
[23] http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html
[24] http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance
[25] http://english.caixin.com/2014-03-27/100657518.html
[26] http://dealbook.nytimes.com/2014/03/05/plaintiffs-in-suit-seek-to-freeze-mt-goxs-u-s-assets/
[27] https://bitcointalk.org/index.php?topic=576337#post_toc_21
[28] http://arstechnica.com/tech-policy/2013/05/feds-reveal-the-search-warrant-that-seized-mt-gox-account/
[29] http://www.wired.com/2014/03/bitcoin-exchange/
[30] https://www.mtgox.com/img/pdf/20140320-btc-announce.pdf

before it went offline, and deliberately misled customers..."[31] In one of the other class-action lawsuits, the plaintiff's attorney, Jay Edelson said, "We believe that he's [Mt. Gox CEO] got a bunch of them [Bitcoins], and we believe that he's got a bunch more. Our belief is that the reason that they [Mt. Gox] supposedly found this [the 200,000 BTC] was because they understood that we and others had already found this amount and knew that they were holding it. So the idea that they found it and were going to come public is exactly the opposite of what we believe happened."[32] In addition, Jay Edelson said "The idea that they have no money is not credible. They were taking deposits up until the day before they shut down."[33] As the class-action lawsuits and bankruptcy cases in the U.S. and Japan unfold, more details will be made public.

Business and Institutional Adoption of Cryptocurrencies

There are over 4,300 various businesses and institutions that have started accepting cryptocurrency payments around the world (Exhibit 5). Two important segments of business are: financial institutions and commercial stores. Across the world there are over 30 exchanges facilitating the buying and selling of cryptocurrency and fiat currency. None of the exchanges are backed or operated by well-known financial institutions. JPMorgan Chase filed a patent application in December 2013 for an online system that facilitates anonymous electronic payments stored on the payee's computer with transactions being verified through a shared log, having strong similarities to the features of cryptocurrencies[34] At the same time, Bank of America released a research report stating a belief that "Bitcoin can become a major means of payment for e-commerce and may emerge as a serious competitor to traditional money transfer providers."[35] In March 2014, Wells Fargo Securities released a report titled, "Bitcoin 101: A Primer", concluding that "while we think Bitcoin clearly has some potential as an alternative payments system, it is probably too early to assess its long-term potential and sustainability."[36] Bloomberg started providing Bitcoin pricing data to its 320,000 financial services subscribers in April 2014.[37] There are payment processors that allow merchants to accept Bitcoins, but receive U.S. dollars, as the payment processor handles the exchange, removing all cryptocurrency risk from the merchant. Some common payment processors are BitPay, Coinbase, Square, and Stripe. There has been little to no adoption of cryptocurrencies in the way of traditional checking accounts, savings accounts, or loans by existing retail banks.

Commercial stores have shown some interest in accepting payments of cryptocurrencies, specifically Bitcoin, mainly due to the lower transaction fees and the removed risk of chargebacks when compared to other electronic methods. The largest commercial retailer to accept Bitcoin is Overstock.com, with company revenue of $1.3B in 2013. The largest electronics retailer to accept Bitcoin, is TigerDirect, a subsidiary of Systemax, which had revenue of $3.3B in 2013.

---

[31] http://dealbook.nytimes.com/2014/03/05/plaintiffs-in-suit-seek-to-freeze-mt-goxs-u-s-assets/
[32] http://dealbook.nytimes.com/2014/03/21/mt-gox-says-it-has-found-200000-bitcoins-worth-about-114-million/
[33] http://dealbook.nytimes.com/2014/03/05/plaintiffs-in-suit-seek-to-freeze-mt-goxs-u-s-assets/
[34] http://www.economist.com/blogs/schumpeter/2013/12/bitcoin
[35] http://www.forbes.com/sites/kashmirhill/2013/12/05/bank-of-america-analysts-say-bitcoins-value-is-1300/
[36] https://www08.wellsfargomedia.com/downloads/pdf/com/insights/economics/special-reports/Bitcoin_101_FINAL-20140306092235.pdf
[37] http://www.coindesk.com/bloomberg-list-bitcoin-prices-financial-terminals/

A variety of other venues, from professional sports teams to schools, have started accepting payment in Bitcoins. The first professional sports team to accept Bitcoin payments is the Sacramento Kings.[38] Yelp, an online urban guide, with a strong focus on local restaurants and retail stores, lists whether a business accepts Bitcoin payments.[39] The first accredited university to accept Bitcoin payments is the University of Nicosia in Cyprus.[40]

Future Alternative Uses of Cryptocurrencies[41]

The underlying protocol used by cryptocurrencies solves a fundamental problem by allowing two untrusted parties to securely exchange value over the internet without a trusted intermediary. The following are three use cases, which currently rely on intermediaries, that could be disrupted by cryptocurrencies: property transfer, contract execution, and identity management.

Transferring large assets requires time, resources, and at least one third party. An example could be the sale of a used car that involves performing a background check on the history of the car, engaging a third party to transfer the title, and working with the local DMV to update the car's registration. A car's accident, inspection, and repair history could all be stored in a fraction of a coin on a cryptocurrency's public ledger, and the blockchain would make it easily and publicly accessible. A company called Colored Coin is working to implement this system with Bitcoin. The process could be applied to other assets, such as land, houses, or financial instructions.

Contracts are typically created, negotiated, and enforced by lawyers, which requires time and resources. There are markets based on contracts, such as the financial derivatives markets, that can lack transparency and some have drawn increasing regulation. Contracts could be digitized with code, stored in the public ledger, and executed when a specific event occurs. An example could be a financial option contract that triggers an action when a specific price is reached. Ethereum is a new platform that integrates many features of Bitcoin in an attempt to develop a network that serves as a registry and escrow to execute contracts based on programmable rules.

Identity management at a government level consists mostly of paper documents, such as passports or driver licenses. These documents are frequently stolen or forged. Using the cryptography underlying cryptocurrencies, identities could be linked to a private Bitcoin key that is impossible to forge. Governments could verify the key when allowing specific actions, such as crossing a border. In addition, the same private key could also be used in place of a social security or tax identification number. OneName is providing individuals with a private Bitcoin key and publicly associating it with personal information, such as a name, email address, or website.

The Bitcoin Foundation outlines 12 broad categories of innovations that harness the underlying technology to go beyond its current use facilitating payments.[42] Some of the additional categories are: crowdfunding, dispute mediation, and multi-signature accounts.

---

[38] http://www.nba.com/kings/news/sacramento-kings-become-first-professional-sports-team-accept-virtual-currency-bitcoin

[39] http://officialblog.yelp.com/2014/04/now-on-yelp-businesses-that-accept-bitcoin.html

[40] http://www.unic.ac.cy/news-and-events/73/unic-to-be-the-first-university-in-the-world-to-accept-bitcoin/112831

[41] http://blogs.hbr.org/2014/04/bitcoins-promise-goes-far-beyond-payments/

[42] https://bitcoin.org/en/innovation

*All Bitcoin to USD prices as of May 2014

Exhibit 1: Comparison of cryptocurrency attributes

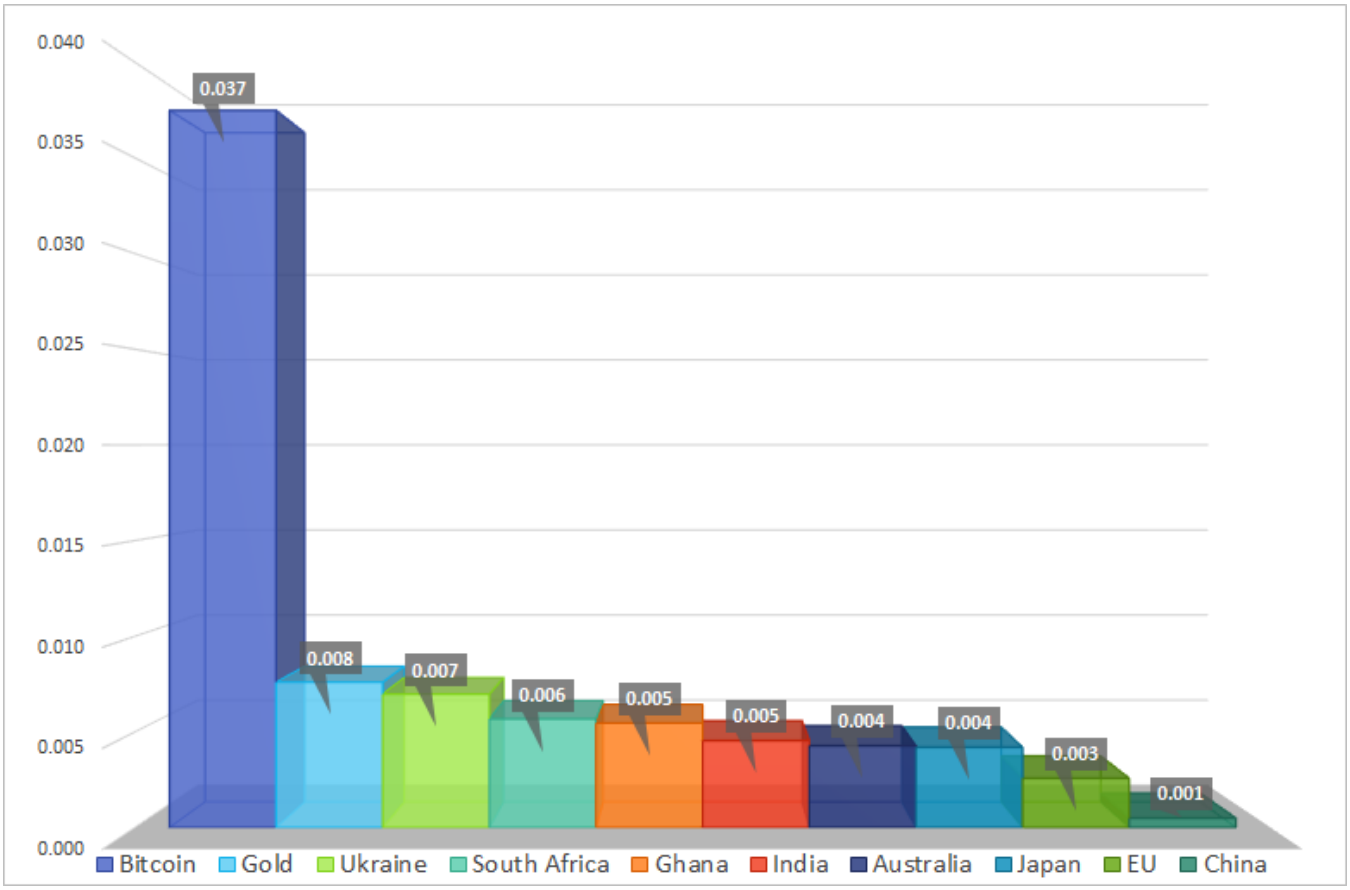
Name	First Mined	Market Cap[+]	Size of Supply	Rate of Coin Release	Transaction Fees
Bitcoin*	1/3/2009	$5,667,897,051	21 million	25 coins/10 minutes	Not required
Litecoin*	10/7/2011	$299,178,840	84 million	50 coins/2.5 minutes	Not required
Peercoin*	8/19/2012	$44,563,463	Unlimited	Inverse with level of activity/10 minutes	Required
Dogecoin*	12/6/2013	$36,570,591	99 billion, then 5 billion/year	Random/1 minute	Required

[+]Market Cap (Existing Supply in USD) = Number of existing coins * Exchange rate with USD - As of March 9th 2014
*Pseudo-anonymous
Sources: https://en.bitcoin.it/wiki/History, http://peercoinmyths.com/, https://en.bitcoin.it/wiki/List_of_alternative_cryptocurrencies, and http://coinmarketcap.com/

Exhibit 2: Common Bitcoin Wallet Software Programs

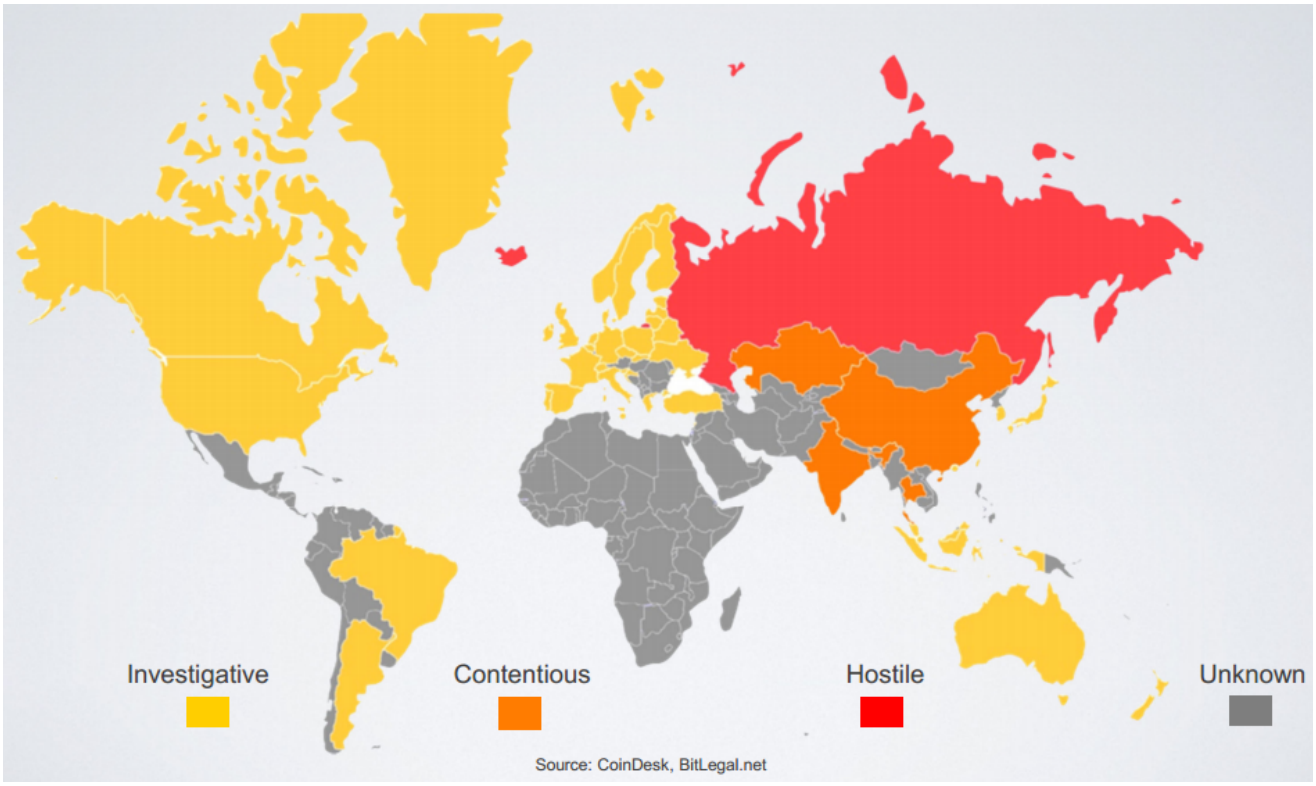
Source: http://media.coindesk.com/report/CoinDesk-State-of-Bitcoin-2014.pdf

Exhibit 3: Volatility Comparison (Against USD)



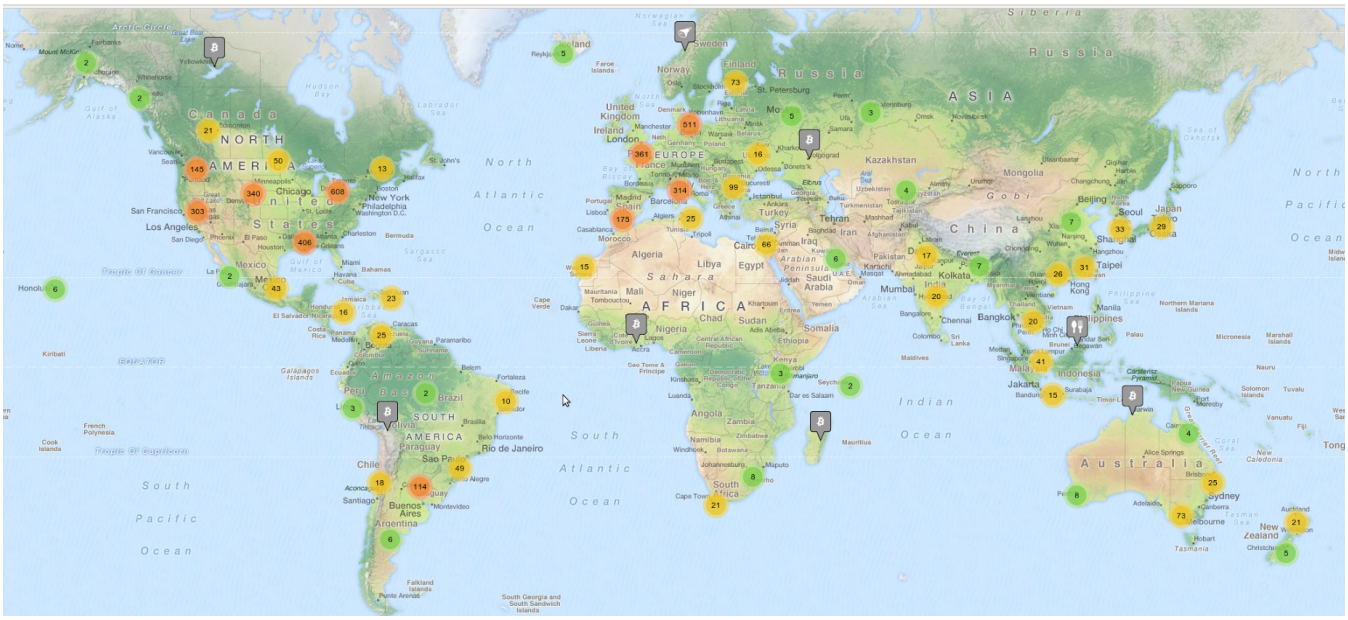
All time periods are one year, from May 2013 to 2014
Values are computed using the average daily absolute percent change in the exchange rate against USD

Exhibit 4: Global Regulatory Heat Map



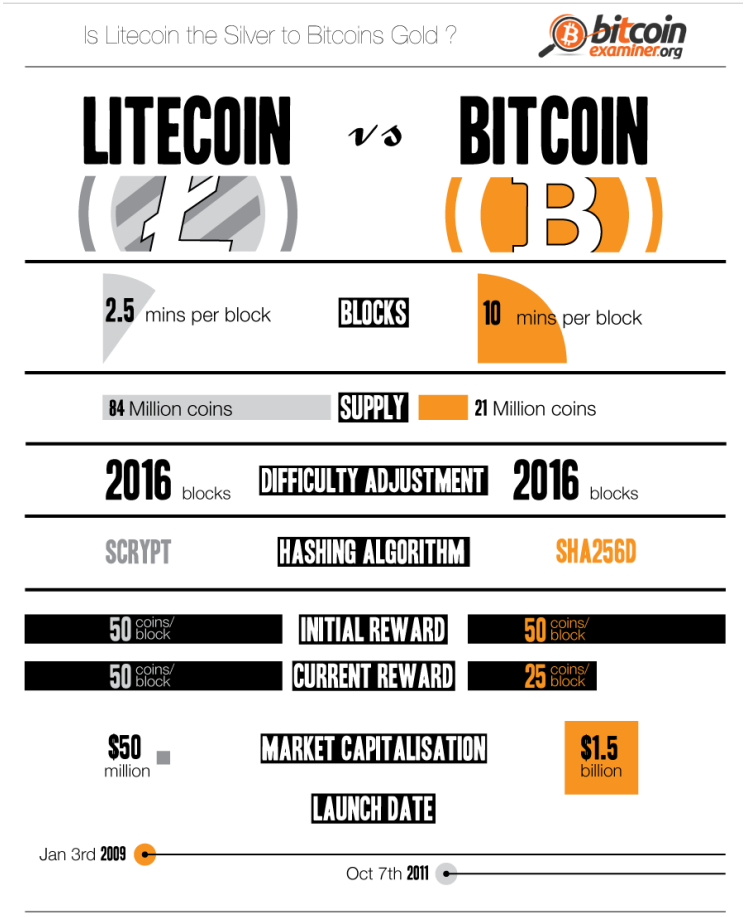
Source: http://media.coindesk.com/report/CoinDesk-State-of-Bitcoin-2014.pdf

Exhibit 5: Over 4,300 Retail Locations accept Bitcoin Worldwide



Source: http://www.coinmap.org from May 8th 2014

Exhibit 6: Comparison between Bitcoin and Litecoin



Source: http://bitcoinexaminer.org/litecoin-vs-bitcoin-who-wins-the-crypto-battle-infographic/