

Crypto-Assets Unencrypted* †

Seoyoung Kim
Santa Clara University

Atulya Sarin
Santa Clara University

Daljeet Viridi

[forthcoming in the *Journal of Investment Management*]

January 2018

JEL Classification: E42; G10, G11, G12.

Keywords: cryptocurrency; coins; digital assets; bitcoin; ethereum; fintech.

* We thank Sanjiv Das, Bhawarth Sangwan, and Natasha Sarin for helpful comments and discussion.

† The authors may be reached at srkim@scu.edu; asarin@scu.edu; daljeetv@gmail.com.

Crypto-Assets Unencrypted

[forthcoming in the *Journal of Investment Management*]

January 2018

Abstract. With the recent surge in crypto-activity, a natural question arises as to what exactly a “cryptocurrency” is and how to value and assess these digital assets. In this paper, we provide an overview of the history and technology underlying cryptocurrencies. We also present information on the volume, size, and volatility of this emerging asset class, which we compare to major fiat currencies and commodities. Finally, we provide a framework for valuing crypto-assets, discuss the still-evolving regulatory environment for this asset class, and discuss the mechanics of investing in cryptocurrencies.

JEL Classification: E42; G10; G11; G12.

Keywords: cryptocurrency; coins; digital assets; bitcoin; ethereum; fintech. A glossary of terms is provided in Appendix A.

1. Introduction

In 2009, an unknown author or authors identified by the pseudonym “Satoshi Nakamoto” introduced Bitcoin (“BTC”), the first viable and henceforth widely adopted cryptocurrency, with the vision to create “an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact with each other without the need for a trusted third party.”¹ Since then, crypto-activity has increased dramatically, with a notable surge in 2017. Motivated by the success of BTC and its successors, the rate of new initial coin offerings (“ICOs”) has rapidly increased and, by mid-2017, had surpassed angel and VC funding as a source of early-stage financing for tech projects and startups.² But much like the era of the dot-com bubble of the late 1990s, which experienced artificially increased valuations simply for appending “.com” to company names,³ there now appears to be a “coin bubble.”

History has shown that innovative asset classes are fraught with problems when first introduced, particularly when they are not yet well vetted or understood. Cryptocurrencies (also referred to as “coins” or “tokens”) are no different. Many cryptocurrency offerings operate with very little structure and language as to expected redemptions and repayment, and many ICOs and simple agreements for future tokens (“SAFTs”) seem largely to be an attempt to fund risky ventures while bypassing SEC scrutiny.⁴ Overall, this sudden surge in crypto-activity has also prompted many legal and regulatory challenges pertaining to theft by hacking, allegations of fraud, and attempts at regulatory arbitrage, and the global regulatory landscape has been mixed, often with polarized views toward this new asset class.

Given the sudden influx of cryptocurrencies, a natural question arises as to how to value and assess these digital assets as part of an investor’s opportunity set. At the infancy of this crypto-era, we do not yet understand all of the opportunities and use cases inherent in this new digital market. We therefore do not yet know how these technologies will continue to evolve and the extent to which they will be employed. The confusion and lack of understanding surrounding this emerging digital asset is a concern for many potential investors.

One source of confusion lies in the term “cryptocurrency” itself, which may be misleading given that, unlike Bitcoin, most cryptocurrencies do not function as actual currencies. In fact, cryptocurrencies as an emerging “asset class” actually embody several distinct asset

¹ Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed on <<https://bitcoin.org/bitcoin.pdf>>

² See Kharpal, Arjun. *Initial coin offerings have raised \$1.2 billion and now surpass early stage VC funding*. CNBC. August 9, 2017. Accessed on <<https://www.cnbc.com/2017/08/09/initial-coin-offerings-surpass-early-stage-venture-capital-funding.html>>

³ Cooper, M., et. al., 2001. “A Rose.com by Any Other Name.” *Journal of Finance*, 56(6), 2371-2388.

⁴ U.S. Security and Exchange Commission. “Statement on Cryptocurrencies and Initial Coin Offers.” Dec. 2017.

classes, and the single unifying theme across cryptocurrencies is the blockchain technology underlying these digital assets. Otherwise, simply identifying an asset as a “cryptocurrency” does not provide the true essence of what the asset represents. Depending on the intent of the issuer or creator, these digitized investments may represent a medium of exchange, a contractual right to transact on a future or existing protocol, or a de facto security providing cash flow claims.

Overall, a clearer understanding of the cryptocurrency landscape is necessary, and sorely lacking. A first step in shedding light on this underserved arena involves organizing information on the volume, size, and volatility of this emerging asset class and providing a valuation framework for assessing digital assets. Toward that end, this paper is organized as follows. Section 2 provides a discussion as to what a cryptocurrency actually represents, and the governance mechanisms ensuring that the underlying platforms are appropriately maintained. Section 3 describes our data sources and presents key summary statistics and empirical analyses. Section 4 compares and contrasts cryptocurrencies with actual fiat currencies and provides a valuation framework for assessing cryptocurrencies. Section 5 discusses the regulation of cryptocurrencies. Section 6 describes the mechanics of investing in cryptocurrencies, and Section 7 provides concluding remarks.

2. What Is a Cryptocurrency?

The concept of a cryptocurrency first emerged in the late 1990s, when Wei Dai published his b-money proposal outlining a proof-of-work protocol to establish a distributed, permission-less currency removed from governmental intermediation.^{5,6} Although not referenced in the seminal bitcoin whitepaper by Nakamoto,⁷ cryptographer Nicholas Szabo also released a cryptocurrency proposal for “bit gold,”⁸ which was also based on a distributed, proof-of-work system.⁹

However, only in 2009 did the first implementation of this concept, propelled by Nakamoto, come to fruition. Despite the rumors, and even conspiracy theories, surrounding the identity of its creator,¹⁰ Bitcoin has quickly risen to prominence and become a hot topic even among the least technically and financially inclined. Now, with a price in excess of \$11,000 USD

⁵ Dai, Wei. “b-money.” 1998. Accessed on <<http://www.weidai.com/bmoney.txt>>

⁶ Bitcoin. *Frequently Asked Questions*. Accessed on <<https://bitcoin.org/en/faq#who-created-bitcoin>>

⁷ Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed on <<https://bitcoin.org/bitcoin.pdf>>

⁸ As distinct from Canadian payments company, BitGold, accessed on <<http://www.bitgold.com>>

⁹ Szabo, Nick. *Bit gold*. Accessed on <<https://unenumerated.blogspot.com/2005/12/bit-gold.html>>

¹⁰ Bearman, Sophie. Bitcoin’s creator may be worth \$6 billion – but people still don’t know who it is. CNBC. October 27, 2017. Accessed on <<https://www.cnbc.com/2017/10/27/bitcoins-origin-story-remains-shrouded-in-mystery-heres-why-it-matters.html>>

and a market capitalization of approximately \$187 billion (as of December 3, 2017),¹¹ Bitcoin has inspired the creation of many more cryptocurrencies. Currently, more than 1,300 crypto-exchange coins are traded,¹² in addition to many other unlisted coins, pre-offering coins, and failed coins. After BTC, the five largest cryptocurrencies by market capitalization are Ether (minted in 2015) (“ETH”), Bitcoin Cash (minted in 2017) (“BCC”/”BCH”),¹³ Ripple (minted in 2013) (“XRP”), Dash (minted in 2014) (“DASH”), and Litecoin (minted in 2011) (“LTC”).¹⁴ In **Appendix B**, we provide a brief description of each of the ten largest cryptocurrencies by market capitalization.

The term cryptocurrency is somewhat of a misnomer, as most cryptocurrencies are currently far too volatile to serve as a meaningful store of value compared to actual fiat money of established governments. In addition, most cryptocurrencies are not widely accepted as a form of payment, and, likewise, do not constitute a natural metric to assess the cost of goods. For instance, we can instinctively and seamlessly determine that \$100 is a high price to pay for a carton of eggs. However, it is more difficult to instinctively assess whether 0.001 BTC or 0.05 ETH is reasonable, particularly because the market value of these cryptocurrencies has exhibited extreme fluctuations over a very brief period.¹⁵

To further confound matters, the term cryptocurrency is broad, with a wide range of legitimate uses, some of which fall within the scope of established asset classes with which we are already familiar. That is, depending on the intent of the issuer or creator, these digitized investments can function as (i) a medium of exchange, (ii) a contractual right to transact on a future or existing protocol, (iii) a de facto security providing cash flow claims, or even (iv) a symbolic gesture or statement with no explicit practical value attached.

Given the many different categories of cryptocurrencies, retail investors often conflate these digital assets with traditional asset classes, such as equity securities, with which they are more familiar. Many developers solely issue pure utility tokens for a protocol under development, which is essentially an advance sale of a product or service to compensate the developers and finance development. However, because many investors are unfamiliar with the concept of more-nebulous digital assets such as a utility token, they mistakenly believe the coin

¹¹ This meteoric rise represents gains in excess of 1,400 percent in just a one-year horizon. Gandal, Hamrick, Moore, and Oberman (2018) also observed a similar runup in 2013, with BTC prices jumping from approximately \$150 USD to more than \$1,000 USD in the final two months of the year.

¹² CoinMarketCap. *Cryptocurrency Market Capitalizations*. Accessed on <<https://coinmarketcap.com/all/views/all/>>

¹³ We note that Bitcoin Cash is associated with two different tickers, BCC and BCH, depending on the listing crypto-exchange. For instance, Coinbase lists it as BCH, whereas Bittrex and Binance list it as BCC.

¹⁴ Throughout this document, coin companies will be referred to by both their names and their tickers.

¹⁵ We provide a more detailed discussion of this topic later in Section 4.1.

is tied to an explicit stake in the profits accrued from some breakthrough idea or technology, such as the general notion of blockchain.

This misconception is further propelled by the fact that some crypto-firms exist as organized entities that generate free cash flows, but also issue cryptocurrencies that are pure utility tokens and separate from an equity stake in the firm. For instance, Ripple has issued a private equity stake in the firm itself. It has also separately issued XRP coins for use on an open-source transaction-protocol it built for exchanging currency. Similarly, Factom has issued a private equity stake in the firm itself, along with separately issued factoids (i.e., FCT coins) for future use on a Factom protocol that is currently in development. These XRP and FCT coins are purely utility tokens and do not provide an equity stake in the future cash flows of Ripple and Factom, respectively.

What, then, exactly is a cryptocurrency? The single unifying theme across cryptocurrencies is the distributed ledger technology on which the digital asset is secured and verified to allow peer-to-peer transactions while preventing the double spending that may occur without the careful eye of a trusted intermediary. Generally speaking, transactions on the protocol are grouped together into blocks. Once enough transactions have been recorded or a certain amount of time has passed, a new block is created. However, this new block is chained to the prior block via a cryptographic link, thereby forming a *blockchain*. The safety of the blockchain is predicated on this cryptographic link, which typically entails hashing the contents of the prior block and using the resulting hash code as the first element of the new block. If a malicious user attempts to alter a transaction from a prior block, the ensuing hash code will not conform with the hash codes already written into subsequent blocks. Thus, the network will reject the faulty transaction and will reach consensus via correct peer blocks, assuming the majority of users are not maliciously colluding. These platforms reward validators on the network with the native token for providing the computing power that maintains the integrity of this cryptographically linked blockchain of transactions.

In sum, the only apparent criterion for inclusion in this “asset class” is that a coin reside on this blockchain technology or some newer derivative forms of this technology.¹⁶ Thus, simply identifying an asset as a “cryptocurrency” does not provide the true essence of what the asset represents. That is, two different coins could represent very different types of assets. We now provide examples of the four basic cryptocurrency categories, which we broached above.

¹⁶ For instance, IOTA has introduced what they called the *tangle*, which is a directed acyclic graph designed to facilitate machine-to-machine transactions at greater speeds and improved scalability than the original bitcoin blockchain. See the IOTA whitepaper (Popov) for further details. Accessed on <https://iota.org/IOTA_Whitepaper.pdf>

- 1) *Cryptocurrencies designed to serve as a medium of exchange.*

Bitcoin is the quintessential example of coins that fall under this category, making it quite different from the many subsequent cryptocurrencies. What makes Bitcoin particularly unique is that it is a pure-play currency and was never designed to have any other use case. This original design is in contrast to utility tokens such as ETH, which was designed to allow the holder to transact on Ethereum, which is the platform underlying the Ether cryptocurrency. However, its early adoption and widespread popularity has extended the use of ETH from being purely a utility token used to fuel smart contracts on the Ethereum protocol to serving as an increasingly accepted medium of exchange.
- 2) *Cryptocurrencies designed to serve as a contractual right to transact on a future or existing protocol.*

This category encompasses most cryptocurrencies today. For instance, ETH is the native cryptocurrency token fueling transactions on Ethereum, which provides a convenient platform for developers to implement smart contracts on a trusted and tested protocol.¹⁷ With the popularity of Ethereum and skyrocketing price of ETH, similar platforms have followed. For instance, Cardano has been developing a platform to rival that of Ethereum, and users hoping to transact on this platform can purchase 1 ADA token for \$0.13 as opposed to \$467.68 for 1 ETH (as of December 3, 2017). However, ADA holders may ultimately have nowhere to spend their tokens if the project does not reach fruition. This scenario is analogous to a not-yet-built arcade that issues game tokens to fund its construction, whereby users will have nowhere to spend their tokens if the arcade does not materialize.
- 3) *Cryptocurrencies designed to serve as a de facto security providing cash flow claims.*

Blockchain Capital, a VC fund, chose to raise money via this format. That is, the fund issued coins via an ICO, which gave investors shares in the fund. Thus, these coins essentially operate as *tokenized securities*, but unlike traditional equity shares, they reside on a blockchain (as opposed to a centralized bookkeeping record), following the unifying theme of what it currently means to be called a “cryptocurrency.”
- 4) *Cryptocurrencies designed as a symbolic gesture or statement.*

Examples in this category include the FOMO (Fear of Missing Out) Coin and Jesus Coin,¹⁸ which have no intended use cases or practical value. In contrast, one coin in this category, Dogecoin, began as a joke currency, but has since become widely adopted as a peer-to-peer medium of exchange and internet reward mechanism with a market capitalization of more than \$2 billion dollars.

¹⁷ See **Appendix C** for examples of notable smart contracts built on the Ethereum platform and similar platforms designed to facilitate the development of smart contracts.

¹⁸ For more information, see FOMO Coin, accessed on <<http://fomocoin.org/>>; and Jesus Coin, accessed on <<https://jesuscoin.network/>>

2.1. How Are New Cryptocurrencies Introduced?

The most common method by which a new cryptocurrency comes into circulation is through an ICO. The ICO is often preceded by a pre-launch sales phase during which investors provide funds in exchange for the rights to a future distribution of tokens via a SAFT. Many of these ICOs have been implemented as a set of smart contracts built on the Ethereum blockchain. Notable examples include ICOs by The DAO (Decentralized Autonomous Organization) and Bancor, which issued DAO tokens and Bancor network tokens, respectively, in exchange for ETH via sales executed by smart contracts developed on the Ethereum platform. The DAO and Bancor each raised \$152 million and \$153 million in their respective ICOs. Other notable ICOs include those of: Filecoin, which raised \$257 million; Tezos, which raised \$232 million; and EOS, which raised \$185 million.

Another way in which a new cryptocurrency is “born” is through a *fork* on an existing protocol. Because cryptocurrencies reside on open-source distributed networks, developers can design updates to improve the existing protocol. A *hard fork* occurs when developers implement major changes in software that are not backward-compatible, causing a split in the blockchain and resulting in two separate blockchains (and, thus, two separate cryptocurrencies) going forward. In contrast, minor updates designed to be backward-compatible to maintain the original blockchain are known as *soft forks* and do not result in a new cryptocurrency. Bitcoin Cash is an example of a hard fork on the Bitcoin blockchain network. Another prominent example involves the Ethereum blockchain. Ethereum underwent a hard fork in 2016 due to disputes surrounding approximately \$50 million worth of ETH that was misappropriated in association with a project financed via smart contracts built on the Ethereum network. This hard fork resulted in two separate cryptocurrencies: ETH and Ethereum Classic.

2.2. Governance of Cryptocurrencies

Given the disintermediated leaderless nature of public blockchains, a natural question arises as to how proper governance is maintained in these systems. That is, a public firm is run by an executive team, with checks and balances instituted by the board of directors, which, in turn, is elected by shareholders of the firm. However, cryptocurrencies such as BTC and ETH, which are built on distributed, permission-less ledgers, have no designated leaders or elected boards to ensure the platform operates smoothly and remains up to date with ongoing trends. Instead, these public blockchains depend on a crowd-sourced, consensus-based network of validators who operate independently and without leadership.

For the avoidance of doubt, public blockchains are entirely open source and do not require permission to participate; that is, literally anyone can contribute to the network. In contrast, private blockchains require permission (that is, an invitation) to participate, and contributors to the network must be validated by the centralized “owner” or by a set of rules put in place by the network “owner.” Some public blockchains were created by an entity that also runs proprietary private blockchains. For instance, the protocol underlying the XRP cryptocurrency token was developed by Ripple, which is a private business entity that also develops and maintains other proprietary platforms that are not open source and distributed. Because private blockchains are maintained by a specific entity (or group of entities), their governance issues lie within the scope of standard corporate governance principles.

One way in which sound governance practices are instilled on public blockchain-based protocols is through the market value of the native cryptocurrency token. Thus, contributors have an incentive to continually develop up-to-date patches and soft forks to ensure the protocol remains a desirable place to transact (relative to other protocols) to maintain the value of their own native tokens. For instance, if technological improvements bring forth safer and faster ways to implement a blockchain-based currency exchange, then Ripple’s XRP platform will become obsolete unless its network of contributors works to provide timely updates. This token-based financial incentive is analogous to incentive-based contract design in executive compensation, which attempts to align executives’ interests with those of shareholders to ensure sound management practices without constant or explicit oversight.

A more drastic way is through a hard fork on the blockchain. That is, if fundamental differences within the network community cause disagreements as to the appropriate amendments to implement on the network protocol, the disgruntled participants can develop substantial changes to the underlying source code to create an offshoot from the original protocol going forward. In this manner, they create a separate blockchain (and cryptocurrency) that adheres to their principles. This split-based incentive is analogous to the threat of takeovers as a governance mechanism that keeps management in check.

2.3. Other Issues to Consider in Implementing a Public Blockchain

The original BTC blockchain is based on a Proof of Work (“PoW”) consensus protocol, wherein a computationally expensive problem must be solved (i.e., “mined”) to validate transactions on the network. However, the recent surge of users participating in these networks has highlighted issues in this method, namely in the increasing amounts of computational power required and the

inevitable network congestion that now plagues traditional blockchain networks. This issue, referred to as the *horizontal scalability* of a chosen consensus protocol, has been the focus of many of the newer blockchain networks.

Recent innovations to improve horizontal scalability have predominantly focused on implementing a protocol based on Proof of Stake (“PoS”) rather than on PoW. That is, developers have been grappling with various ideas as to how to implement a consensus protocol wherein a single user or subgroup of users is selected to validate the next block. This selection process can be based on a number of characteristics, such as tenure within the network or wealth as measured by the proportion of native tokens, and contains a stochastic component to mitigate the likelihood of bestowing centralized power to a single user or small subgroup of users.

Although PoS is far faster than PoW, the increased speed may come at the cost of other technical issues that concern the integrity of the validated blocks. Thus, ongoing development of consensus protocols based on PoS has predominantly concerned methods to thwart dishonest users. For instance, some developers suggest implementing a punitive PoS protocol by embedding sufficiently severe punishments to deter the validation of faulty blocks (e.g., a rule to confiscate native tokens from malicious users). In addition to efforts made to address vulnerabilities inherent in a PoS protocol, other potential solutions for horizontal scalability include: (i) replacing the linear blockchain with a directed, acyclic graph, which Iota developers refer to as “the tangle”;¹⁹ and (ii) implementing a “proof of correctness” consensus protocol based on reaching consensus via a Unique Node List (“UNL”), that can be randomly generated or individually selected by each user to serve as selected validators.²⁰

3. Data Sources and Key Summary Statistics

In this section, we describe our data sources and present key summary statistics and empirical findings with respect to liquidity trends and market size of this asset class over time.

3.1. Data Sources

Our sample period spans January 1, 2013, through December 3, 2017, and consists of 169 crypto-exchanges and the cryptocurrencies listed across these exchanges. For tractability, we focus on the 20 largest cryptocurrencies, based on market capitalization, for our more detailed analyses. We collect information on daily prices, volume, circulating supply, and market

¹⁹ See the Iota whitepaper (Popov), accessed on <https://iota.org/IOTA_Whitepaper.pdf>

²⁰ See the Ripple Consensus whitepaper (Schwartz et. al.), access on <https://ripple.com/files/ripple_consensus_whitepaper.pdf>

capitalization directly from the exchanges on which these cryptocurrencies are traded. In addition, we obtain exchange rates from the Federal Reserve Economic Data (“FRED”) to determine percentage price volatility (in USD) for various fiat currencies and inflation rates for each of these countries from inflation.eu.

3.2. Cryptocurrency Listings, Market Capitalization, and Liquidity over Time

We begin by exploring the total number of distinct listings across three major crypto-exchanges: (i) Poloniex, (ii) Bitfinex, and (iii) Bittrex. The results, which we present in **Figure 1**, show that each exchange had 99, 67, and 276 trading pairs (untabulated) (**Panel A**), respectively, listed and traded as of December 3, 2017.

A trading pair represents the paired combination of the cryptocurrency purchased and the baseline cryptocurrency used to pay for the purchase. For instance, BCH is listed as three different trading pairs on Bittrex, since it can be purchased with either BTC, ETH, or USDT (Tether) (**Figure 5, Step 5**). **Figure 1** also demonstrates a sudden influx of new listings in 2017. That is, of the 359 distinct trading pairs across the three exchanges, 183 were newly listed in 2017 (**Panel B**).

Table 1 provides a snapshot of basic summary statistics with respect to the 20 largest cryptocurrencies, based on market capitalization, as of December 3, 2017. From these statistics, we observe a roughly equal split between the *mineable* and *pre-mined* cryptocurrencies, the latter denoted with an asterisk (*) next to the crypto-ticker. A mineable currency compensates individuals who maintain the integrity of the system. For instance, the Bitcoin blockchain rewards miners with newly minted Bitcoins for providing proof of work for the underlying Bitcoin blockchain. In contrast, a pre-mined currency does not produce new coins into circulation. For instance, developers of Ripple generated the entire Ripple coin supply at the onset of the project.

Overall, the three largest cryptocurrencies are BTC, ETH, and BCH, with market capitalizations of approximately \$187 billion, \$45 billion, and \$26 billion, respectively. These three cryptocurrencies were also the most liquid according to their average daily dollar volume of approximately \$4.8 billion, \$0.8 billion, and \$0.8 billion, respectively, in 2017. The twentieth coin on our list, Zcash (ZEC), had a market capitalization of approximately \$910 million and an average daily dollar volume of approximately \$65 million.

To place these numbers in context, Microsoft common stock (MSFT) had an average daily dollar volume of approximately \$1.8 billion based on the three months of daily trading

activity leading up to December 15, 2017 (**Figure 2**). At that time, MSFT had a market capitalization of approximately \$670 billion. During the same time, BTC had more than twice the average daily dollar volume of MSFT, with a market capitalization equal to less than one third of MSFT's market capitalization.

On further examination of the two largest cryptocurrencies, BTC and ETH, over time (**Figure 3**), we observe a sudden surge in both prices (**Panel A**) and total market capitalization (**Panel B**) in 2017. We also observe a sudden surge in daily volume for both Bitcoin and Ether at this time (**Figure 4**). Similarly, in **Table 2**, we present numerically the market capitalization (**Panel A**) and average daily volume (**Panel B**) for each year from 2013 through 2017 for the ten largest cryptocurrencies by market capitalization as of December 3, 2017.

This marked increase in the value and trading activity of BTC and ETH coincides with the influx of new listings in 2017 (recall **Figure 1**), suggesting that the valuation spikes in Bitcoin and Ether are, at least in part, attributable to their concentrated positions as the gateway to accessing other cryptocurrencies. Specifically, investing in other cryptocurrencies requires that investors first convert an actual currency (for instance, USD) into a baseline cryptocurrency used to purchase other coins, with BTC and ETH as the most commonly used baseline cryptocurrencies for these transactions.

3.3. Top Crypto-Exchanges

In **Table 3**, we present the top 20 crypto-exchanges by average daily dollar volume in 2017. We observe a substantial amount of daily trading activity in the past year, with the three most liquid exchanges showing average daily dollar volumes of approximately \$3.5 billion (Bitfinex), \$2.4 billion (Bitmex), and \$2.2 billion (Bithumb). The exchanges vary widely in the number of listings offered. For instance, Gemini and bitFlyer each list only three cryptocurrency trading pairs. Conversely, HitBTC, Bittrex, and Binance currently feature 340, 274, and 180 listings, respectively.

We also observe numerous security breaches across the various crypto-exchanges on our list. Specifically, we note verified instances of hacking in six exchanges: Bitfinex,²¹ Bithumb,²² Poloniex,²³ HitBTC,²⁴ OKEEx,²⁵ and Bitstamp.²⁶ For instance, investors on HitBTC lost coins

²¹ See Higgins, Stan. *The Bitfinex Bitcoin Hack: What We Know (And Don't Know)*. Coindesk. August 3, 2016. Accessed on <<https://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know/>>

²² See Parker, Luke. *Fourth largest Bitcoin exchange. Bithumb, hacked for billions of Won*. Brave NewCoin. July 4, 2017. Accessed on <<https://bravenewcoin.com/news/fourth-largest-bitcoin-exchange-bithumb-hacked-for-billions-of-won>>

²³ See Rizzo, Pete. *Poloniex Loses 12.3% of its Bitcoins in Latest Bitcoin Exchange Hack*. Coindesk. March 5, 2014. Accessed on <https://www.coindesk.com/poloniex-loses-12-3-bitcoins-latest-bitcoin-exchange-hack/>>

valued in excess of \$300 million to hackers in 2015, and investors on Bitfinex lost coins valued at approximately \$72 million to hackers in 2016.

4. Valuation and Classification of Cryptocurrencies

We begin this section with a discussion of the key differences between fiat money and the most money-like cryptocurrencies. We then provide a basic valuation framework by which to assess these digital assets.

4.1. Asset or Currency?

Economists and central banks generally consider the following three functions that define what it means to be a currency.

- 1) *Store of Value*. If the cryptocurrency is held for a period of time, will it provide similar purchasing power as it does today?
- 2) *Unit of Account*. Can the cryptocurrency be easily adopted as a common metric to think of the cost of goods?
- 3) *Medium of Exchange*. Is the cryptocurrency a practical and widely accepted method of payment?

Currently, the vast majority of cryptocurrencies do not satisfy the *medium-of-exchange* criteria, as they cannot be readily used in transactions to obtain other goods or services. We therefore focus on BTC, ETH, LTC, and USDT, which currently serve as the predominant baseline currencies by which to gain access to other cryptocurrencies. As we will discuss in Section 6 (How to Invest in Cryptocurrencies), these baseline currencies are currently the only means by which to purchase other cryptocurrencies because they cannot be purchased using traditional fiat money. Of these, USDT is the farthest from serving as a widely accepted medium of exchange, because it is currently accepted only as a medium of exchange in purchasing other cryptocurrencies. However, as we discuss shortly, USDT is the closest to operating as a store of value and easy unit of account.

²⁴ See NewsBTC. *BTER Allegedly the First in a Long Line of Hackings and Attacks*. February 16, 2015. Accessed on <<http://www.newsbtc.com/2015/02/16/bter-allegedly-first-long-line-hackings-attacks/>>

²⁵ See Gao, Alex. *Chinese Bitcoin Exchange OKEx Hacked for \$3 Mln, Police Not Interested*. The Cointelegraph. October 2, 2017. Accessed on <<https://cointelegraph.com/news/chinese-bitcoin-exchange-okex-hacked-for-3-mln-police-not-interested>>

²⁶ See Whittaker, Zack. *Bitstamp exchange hacked, \$5M worth of bitcoin stolen*. ZDNet. January 5, 2015. Accessed on <<http://www.zdnet.com/article/bitstamp-bitcoin-exchange-suspended-amid-hack-concerns-heres-what-we-know/>>

In contrast, despite their volatility, BTC, ETH, and LTC have steadily been gaining traction as payment in various transactions. For instance, major online vendors such as Expedia, Overstock.com, Newegg.com, and Microsoft (online store) accept Bitcoin as a form of payment.²⁷ Online vendors have expanded this trend to include other large, liquid cryptocurrencies such as ETH and LTC. In addition, we observe vast and rapid improvements in the transaction speeds on the underlying platforms as technology has improved (see **Table 4**). For instance, the Bitcoin, Ethereum, and Litecoin networks currently process 7, 20, and 56 transactions per second, respectively, and the Ripple protocol is able to process 1,500 transactions per second. In comparison VISA and Paypal process 1,700 and 193 transactions per second, respectively. We also observe ongoing improvements in the transaction fees. Specifically, the average transaction fees on the Bitcoin, Ethereum, and Litecoin networks is \$28.75, \$2.56, and \$0.295 USD, respectively. In comparison, VISA charges between 1.43% and 2.4%, and Paypal charges \$0.30 in addition to 2.9% of the transaction amount.

Overall, the case for these particular cryptocurrencies as a medium of exchange is not yet convincing, although they are on an upward trajectory. We make the same stipulations with respect to the *unit-of-account* criterion, given that a unit of account is fundamentally tied to commonly accepted mediums of exchange. Thus, we turn to the *store-of-value* criterion. In **Table 5** we present the daily percentage price volatility of BTC, ETH, LTC, and USDT, which we compare to the daily percentage price volatilities of various physical commodities and major fiat currencies. We also present annualized inflation rates of the various countries issuing the currencies examined.

Although these cryptocurrencies are relatively new, their recent history suggests a highly volatile, and therefore uncertain, price path. For instance, BTC exhibited a daily percentage price volatility of 4.99% in 2017, with a notable spike to 8.76% in December 2017 (**Table 5, Panel A**). Similarly, ETH and LTC exhibited daily percentage price volatilities of 7.30% and 8.69%, respectively, in 2017 (**Table 5, Panel A**).

We note that Tether exhibits no price volatility based on a USD conversion rate, because it is designed to be pegged to the US dollar. Specifically, Tether Limited purports to hold one USD in reserve for each USDT issued on its platform,²⁸ and belongs to a growing class of

²⁷ See Nishanian, Mariam. *8 surprising places where you can pay with bitcoin*. Business Insider. October 11, 2017. Accessed on <<http://www.businessinsider.com/bitcoin-price-8-surprising-places-where-you-can-use-2017-10>>

²⁸ See Tether, accessed on <<https://tether.to/>>

cryptocurrencies known as “stablecoins”,²⁹ whose values are pegged to some other fiat money or asset with inherent value. Other examples of *stablecoins* include: the Dai coin (DAI),³⁰ which is a collateral-backed coin with price-stability mechanisms built into its protocol to correct deviations from a 1:1 exchange rate with the US dollar; and Basecoin,³¹ which is still in proof-of-concept stage.

In comparison to BTC, ETH, or LTC, none of the actual fiat currencies comes close in terms of their daily percentage price volatilities based on USD conversion rates (**Table 5, Panel C**). The physical commodities we examine are also far less volatile than the cryptocurrencies. For instance, silver and gold exhibited daily percentage price volatilities of 1.17% and 0.68%, respectively, in 2017 (**Table 5, Panel B**).

Furthermore, we observe that the daily percentage price volatilities of BTC, ETH, and LTC far exceed even the annualized inflation rates of advanced economies such as the United States (2.13%), Great Britain (0.55%), and Japan (1.57%) (**Table 5, Panel D**). That is, holding a U.S. Dollar or a British Pound will afford us roughly the same purchasing power in a month with a high degree of certainty. In contrast, the purchasing power of BTC, ETH, and LTC could fall by 27.33%, 39.98%, and 47.60%, respectively, in just one month.³² We also observe that the daily percentage price volatilities of BTC, ETH, and LTC are on par with or even exceed annualized inflation rates of Mexico (5.97%) and South Africa (5.26%) (**Table 5, Panel D**). That is, holding a Mexican Peso or a South African Rand provides far greater certainty in next month’s purchasing power than holding either BTC, ETH, or LTC.

Overall, BTC, ETH, and LTC are far too volatile to qualify as actual currencies, and the continued risk of theft by hacking further diminishes their validity as a safe store of value. Moreover, the very fact that these cryptocurrencies are created to serve as decentralized monies independent of government intermediation provides little guidance or hope that they will enjoy the same protection of government-sponsored deposit insurance afforded to actual fiat currencies. Thus, even after several years and hundreds of new cryptocurrencies later, we arrive at the same conclusion as Yermack, who questioned whether Bitcoin is “a real currency.”³³ That

²⁹ This class of cryptocurrencies is not to be confused with the coin, StableCoin (SBC), which is mine-able and is not pegged to any assets or fiat money.

³⁰ See Dai coin, accessed on <<https://makerdao.com>>

³¹ See Basecoin, accessed on <<https://www.getbasecoin.com>>

³² These figures are based on a one-standard deviation decline when applying the square-root-of-time rule to the daily percentage price volatility. For instance, $0.0499 \times \sqrt{30} \approx 0.2733$.

³³ Yermack, D., 2014. “Is Bitcoin a Real Currency? An Economic Appraisal”, *NBER and New York University Working Paper Series*.

is, these cryptocurrencies are more appropriately labeled “crypto-assets.” We now provide a basic valuation framework in pricing these crypto-assets.

4.2. A Basic Valuation Framework

As we discussed in section 2.1, there are three distinct types of crypto-assets. We value tokenized securities no differently than other securities. The same kinds of uncertainties exist regarding the cash flow of these securities as do in the early stages of any paradigm-shifting technology. Also, real options exist that must be accounted for, which can be complicated. The speed at which we have moved from being reluctant to share our credit card information on the Internet to e-commerce becoming a bona fide threat to shopping malls is not something we could have factored into projections of Amazon’s free cash flows in 1996. The problem is compounded when attempting to value a utility token or something like Bitcoin that has been issued as a pure-play digital currency.

At this stage of development, Blockchain is a transformational technology that will increase the speed, efficiency, cost, and transparency of many transactions. But how will this translate into value for the holders of crypto-assets? Many of the crypto-assets have been issued as utility tokens, to be used for conducting transactions. For instance, to develop smart contracts on the Ethereum network, users must pay in ETH tokens, and to exchange currency on the Ripple protocol, users must pay in XRP tokens. This is fundamentally different from a traditional, centralized platform company in which the investors are entitled to a fee for all of the transactions carried out on their platform.

Consider Uber, a traditional, centralized platform company. Every time it connects a rider to a driver, the investors are paid a portion of the fare for making that connection. A decentralized protocol version of Uber, say “UberB,” would directly connect the rider to the driver without the need for an intermediary, and consequently without any associated transaction costs.

Thus, a fair question for any potential investor is, given a decentralized, peer-to-peer transaction and no transaction fees, what possible monetary benefits could exist for the holders of UberB tokens? The answer lies in the role the UberB tokens (or more broadly, crypto-assets) will play in this decentralized, peer-to-peer platform. UberB tokens will be needed to hail rides and/or for drivers to register on the platform. As more people start using UberB and the number of tokens is limited, the value of the tokens will increase and the holders of tokens will benefit from capital appreciation.

Overall, the demand for a utility token is dictated by (i) the forecasted value or popularity of the underlying service or product to which the token grants access; (ii) the liquidity of the token (i.e., the ease with which a user on the platform can trade the token); (iii) the fungibility of the token (i.e., the alternative uses for the token outside of the main platform for which it was issued), whether intended at creation or not; (iv) the risk of obsolescence, and (v) the velocity of the usage of the token.

Naturally, all else equal, increased demand for the utility token increases its value. However, this valuation function is complicated further by feedback effects, whereby an increase in value requires fewer coins in circulation, thereby depressing demand.

Valuation of pure-play cryptocurrencies like BTC is even more complicated. Bitcoin may well play a very important role in this ecosystem by being the dominant asset that can be readily converted to different utility tokens. In our Uber example, there could be a mechanism whereby we would convert our BTC to UberB tokens to hail a ride and pay for it. Once paid, the driver would convert the UberB tokens to Bitcoin.

So, much like we carry dollars when we travel that can be readily converted to most local currencies, BTC could become the global currency of the Blockchain era that businesses and individuals have in their digital wallets and convert into utility tokens to procure goods and services.

Bitcoin has a first-mover advantage as the first viable Blockchain currency – a wide variety of fiat currencies can be readily converted to Bitcoin at many exchanges (or even at Bitcoin ATMs), it can be readily converted to other crypto-assets, companies can hold it without assuming price risk because they can hedge their positions in the futures market, it is secure (generally considered unhackable), and it has had perfect uptime since its launch on January 3, 2009. However, it could also be replaced by a superior future iteration of Bitcoin with lower transaction costs, or a stable coin whose value is tied to the value of a dollar or basket of currencies, or even a government-issued cryptocurrency.

Clearly, the range of possible outcomes is broad. One way is to think of crypto-assets is as a commodity in limited supply that currently has no (limited) use. Over time, when we develop a technology that requires the use of crypto-assets, its demand, and consequently its value, will increase. When we invest in crypto-assets, we are investing in whether the blockchain protocol has an economic advantage over the existing way of doing business, is scalable, and will meaningfully limit the supply of coins. If the usage of the protocol increases, the value of the coins needed to participate in it will also increase.

5. The Current Regulatory Landscape

The recent meteoric rise in crypto-asset valuations and the issuances of new coins via ICOs has been met with a wide range of reactions by governments across the world.³⁴ Some have enthusiastically welcomed the new technology, although possibly for nefarious reasons. For instance, North Korea has enthusiastically embraced Bitcoin, but by many accounts, its amassed wealth has been through a recent spate of hacks and cyberattacks rather than through mining or otherwise legitimately earning the crypto-assets.³⁵ In another example, Venezuela has announced its intent to launch its own sovereign cryptocurrency, largely in an attempt to circumvent financial sanctions.³⁶

On the other end of the spectrum, some economies have established an outright moratorium on certain crypto-activity. For instance, South Korea has banned ICOs³⁷ and has generally taken the stance that crypto-assets are excessively risky, with many new issuances lacking any intrinsic value.³⁸ South Korea has placed additional restrictions on gaining any exposure to crypto-activity, with reported plans to even ban trading in Bitcoin futures.³⁹ China has also banned ICOs⁴⁰ and, like South Korea, has banned financial institutions from using Bitcoin in any part of financial transactions, including as collateral.⁴¹

Overall, a more-balanced approach is necessary to allow innovation while shielding the most vulnerable would-be investors. While it would be a mistake for the regulatory community to ignore the nascent crypto-asset industry, it would be perhaps an even graver mistake to over-regulate and delay this innovation from reaching its full potential. Countries such as the U.S. and

³⁴ For a summary of the current regulatory climate by country, see McKenna, Francine. *Here's how the U.S. and the world regulate bitcoin and other cryptocurrencies*. MarketWatch. December 28, 2017. Accessed on <<https://www.marketwatch.com/story/heres-how-the-us-and-the-world-are-regulating-bitcoin-and-cryptocurrency-2017-12-18>>

³⁵ See Cuthbertson, Anthony. "North Korea Hacking War on Bitcoin Exchanges is Part of "Biggest Global Sting."" *Newsweek*. December 19, 2017. Accessed on <<http://www.newsweek.com/north-korea-hacking-war-bitcoin-exchanges-part-biggest-global-sting-752161>>

³⁶ See Ulmer, Alexandra; and Buitrago, Deisy. *Enter the 'petro': Venezuela to launch oil-backed cryptocurrency*. Reuters. December 3, 2017. Accessed on <<https://www.reuters.com/article/us-venezuela-economy/enter-the-petro-venezuela-to-launch-oil-backed-cryptocurrency-idUSKBN1DX0SQ>>

³⁷ See Nakamura, Yuji; and Kim, Sam. *Cryptocurrencies Drop as South Korea Bans ICOs, Margin Trading*. Bloomberg Technology. September 29, 2017. Accessed on <<https://www.bloomberg.com/news/articles/2017-09-29/cryptocurrencies-drop-as-south-korea-bans-icos-margin-trading>>

³⁸ See Ramirez, Elaine. "5 Times Cryptocurrencies Rocked South Korea In 2017." *Forbes*. December 19, 2017. Accessed on <<https://www.forbes.com/sites/elaineramirez/2017/12/19/5-times-cryptocurrencies-rocked-south-korea-in-2017/#251741fc74c9>>

³⁹ See Williams-Grut, Oscar. *South Korea has reportedly banned bitcoin futures*. Business Insider. December 11, 2017. Accessed on <<http://www.businessinsider.com/south-korea-bitcoin-futures-2017-12>>

⁴⁰ See Choudhury, Saheli Roy. *China bans companies from raising money through ICOs, asks local regulators to inspect 60 major platforms*. CNBC. September 4, 2017. Accessed on <<https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html>>

⁴¹ See Bloomberg News. *China Bans Financial Companies From Bitcoin Transactions*. December 5, 2013. Accessed on <<https://www.bloomberg.com/news/articles/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions>>

Canada have largely adopted this perspective. In **Table 6**, we present an overview of the regulatory stance taken by various nations across the globe, which demonstrates a wide array of responses to the potential adoption of cryptocurrencies.^{42,43}

Overall, regulators are grappling with many reasonable concerns today related to cryptocurrencies. One issue relates to how crypto-investments should be reported, taxed, and audited. A more serious concern is the potential for outright fraud, as some of the ICOs are conducted with no purpose other than to expropriate money from investors.⁴⁴ Uninformed investors may unwisely invest their life savings into digital assets that will one day become worthless.

Furthermore, security breaches in the crypto-exchanges have led to massive thefts of wealth from unwitting investors. Perhaps most disturbingly, there is a legitimate concern that criminals and terrorist groups are using the existence of anonymized exchanges to move capital for funding terrorist activities. Lawmakers are justified in wanting to protect their citizens (and their tax base), and the innovators in this space seek clarity from the regulatory community that will provide certainty and enable the institutional investors to comfortably deploy their capital to these investments.

Thus, legitimizing the industry will require a baseline regulatory framework as well as oversight. This framework should outline principles to be followed by market participants and should also begin to craft a strategy for tax treatment. However, we should avoid placing onerous filing or licensing burdens on the participants, thus allowing the market to evolve. Laws that entail large legal, compliance, and filing costs will only protect incumbents and may unwittingly drive innovation out of the state or even the country.

6. How to Invest in Cryptocurrencies

In this section, we describe the process of investing in cryptocurrencies, including procuring the digital asset and proper storage of the asset to mitigate the likelihood of loss or theft.

6.1. Purchasing Cryptocurrencies

Purchasing cryptocurrencies and subsequently liquidating these investments is more complex than and not as widely practiced and understood as investments in traditional asset classes, such

⁴² McKenna, Francine. *Here's how the U.S. and the world regulate bitcoin and other cryptocurrencies*. *Op. cit.*

⁴³ PerkinsCoie. *Digital Currencies: International Actions and Regulations*. December 2017. Accessed on <<https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html>>

⁴⁴ See, for instance, Kharpal, Arjun. *Cryptocurrency start-up Confido disappears with \$375,000 from an ICO, and nobody can find the founders*. CNBC. November 21, 2017. Accessed on <<https://www.cnbc.com/2017/11/21/confido-ico-exit-scam-founders-run-away-with-375k.html>>

as equity securities. The three ways in which a prospective investor can gain direct exposure⁴⁵ to cryptocurrencies are (i) mine the cryptocurrency, if applicable; (ii) purchase the cryptocurrency through an ICO or pre-launch token sale via a SAFT; or (iii) purchase the cryptocurrency via a secondary market transaction on a crypto-exchange. **Figure 5** provides a graphical depiction of the steps to investing in a cryptocurrency via secondary markets. We summarize these steps as follows.

- 1) Create a digital wallet designed to store cryptocurrencies (**Figure 5, Step 1**). Many online wallet services now exist, and we use coinbase for illustrative purposes.⁴⁶ A coinbase account comes with four different wallets: BTC wallet (for Bitcoin), ETH wallet (for Ethereum), LTC wallet (for Litecoin), and USD wallet (for U.S. dollars). Once a wallet is created, note the unique wallet address, which can be accessed via the “receive” button of the wallet (**Figure 5, Step 2**). This address is required to receive crypto-funds and comprises an alpha-numeric string of varying lengths, which may or may not be case-sensitive depending on the cryptocurrency in question.
- 2) Next, link a valid credit card or bank account to enable the USD wallet. Use the money in this USD wallet to purchase BTC, ETH, or LTC (**Figure 5, Step 3**), which are the main baseline cryptocurrencies used to purchase other cryptocurrencies. Depending on the crypto-exchange and desired cryptocurrency, additional accounts with other wallet service providers may be needed, given that cryptocurrencies are listed in pairs depending on the baseline cryptocurrency being used for purchase (much like how equity securities on NYSE are purchased with U.S. dollars and equity securities on TSE are purchased with yen). For instance, certain cryptocurrencies must be purchased using USDT (i.e., Tether), and coinbase does not offer a USDT/Tether wallet.
- 3) Once the crypto-wallet has been established, create a trading account on a crypto-exchange. As evidenced in the empirical data, there are now more than 150 crypto-exchanges on which these coins are traded. For illustrative purposes, we use Bittrex (**Figure 5, Step 4**).⁴⁷ Additional trading accounts on other crypto-exchanges may be required depending on the cryptocurrencies desired.
- 4) Deposit funds into the trading account in a baseline cryptocurrency, such as BTC or ETH. For instance, obtain the address for the BTC wallet in the Bittrex trading account, and use this address to send Bitcoins from the BTC wallet on coinbase to the BTC wallet on Bittrex.⁴⁸ Once this is complete, purchases of other cryptocurrencies can be made using BTC as the baseline cryptocurrency. Similarly, these steps must be performed for ETH or

⁴⁵ As of December 2017, investors can now gain indirect exposure to bitcoin via bitcoin futures contracts, which are settled in cash (USD). See CME Group. *Now Available: Bitcoin Futures*. Accessed on <<http://www.cmegroup.com/trading/bitcoin-futures.html>>

⁴⁶ See coinbase, accessed on <<https://www.coinbase.com>>

⁴⁷ See Bittrex, accessed on <<https://bittrex.com>>

⁴⁸ An attempt to send coins from, say, a BTC wallet to an ETH wallet will result in permanent loss of the digital asset.

USDT wallets to purchase cryptocurrencies using either ETH or USDT as the baseline currency. For instance, BCH is available for purchase using BTC, ETH, or USDT as the baseline cryptocurrency (**Figure 5, Step 5**). That is, BCH is listed on Bittrex as three different trading pairs.

In **Figure 6**, we provide a graphical depiction of the steps to convert a cryptocurrency investment back into USD. This conversion entails selling the cryptocurrency to convert it to a baseline cryptocurrency, such as BTC, then sending the coins in the BTC wallet in the investor's Bittrex account to the BTC wallet in the investor's coinbase account using the unique wallet address, as demonstrated in **Figure 5, Step 2**. Once the BTC has been transferred to the BTC wallet in the coinbase account, BTC can be converted back to USD.

6.2. Storing Cryptocurrencies

As discussed previously, other cryptocurrency investments are typically accessed via a baseline transactional cryptocurrency, such as BTC or ETH. When between crypto-investments, an investor will need a secure way to store BTC or ETH. There are three ways in which these baseline cryptocurrencies can be stored, each with its own relative advantages and disadvantages (see **Figure 7** for a summary of methods):

- 1) *Software wallets* are generally the most convenient, but also more vulnerable to hacking and theft than other storage methods. Software wallets include (i) desktop wallets, (ii) mobile wallets, and (iii) online wallets maintained by a third-party provider. Desktop wallets provide the greatest security but the least convenience. Examples of desktop-wallet software include Armory⁴⁹ and Electrum,⁵⁰ which are designed to safely store private keys on the computer and offline. Mobile and online wallets are the most convenient but offer the least security from potential hacking. Examples of mobile-wallet services include Bread⁵¹ and Mycelium,⁵² and examples of online-wallet services include coinbase⁵³ and the numerous online crypto-exchanges that each provide their own BTC, ETH, LTC, USDT, and other altcoin wallets.
- 2) *Hardware wallets* store an investor's private wallet keys on a portable hardware device, such as a USB flash drive. Examples include KeepKey,⁵⁴ Trezor,⁵⁵ and Ledger.⁵⁶ Hardware wallets are generally more secure than software wallets, given that the private

⁴⁹ See Armory, accessed on <<https://www.bitcoinarmory.com/>>

⁵⁰ See Electrum, accessed on <<https://electrum.org/>>

⁵¹ See bread, accessed on <<https://breadapp.com/>>

⁵² See Mycelium, accessed on <<https://wallet.mycelium.com/>>

⁵³ See coinbase, accessed on <<https://www.coinbase.com/>>

⁵⁴ See KeepKey, accessed on <<https://www.keepkey.com/>>

⁵⁵ See Trezor, accessed on <<https://trezor.io/>>

⁵⁶ See Ledger, accessed on <<https://www.ledgerwallet.com/>>

keys are stored offline. However, this method is still subject to physical loss by negligence, theft, or destruction (e.g., fire, water, etc.).

- 3) *Paper wallets* are sheets of paper imprinted with an investor's private wallet keys. Investors can use encryption software, such as [bitaddress.org](https://www.bitaddress.org)⁵⁷ or MyEtherWallet,⁵⁸ to generate and print keys onto a sheet of paper, which can then be stored in a safety deposit box for maximum security.

7. Concluding Remarks

Crypto-assets are a highly speculative asset class that belong as a small part of a well-diversified portfolio. While many of these will fail, some may reach lofty valuations if they become an integral part of the new blockchain economy. It is even possible that this entire asset class could be a “geek fad” that, like the beanie babies of yesteryear, will be forever relegated to our intellectual basements.

Regardless of how this plays out, the sudden surge in activity, extreme volatility, high failure rate, and high regulatory uncertainty of this new asset class suggest the need for a structured framework by which to assess and better understand the valuation and classification of these digital assets. Overall, a deeper understanding of the use cases of digital assets is critical, as is regulatory guidance that protects investors while providing a sandbox for innovation to continue without restraint.

⁵⁷ See [bitaddress.org](https://www.bitaddress.org), accessed on <<https://www.bitaddress.org>>

⁵⁸ See MyEtherWallet, accessed on <<https://www.myetherwallet.com/>>

References

- Armory, accessed on <<https://www.bitcoinarmory.com/>>
- Basecoin. Accessed on <<https://www.getbasecoin.com>>
- Bearman, Sophie. Bitcoin's creator may be worth \$6 billion – but people still don't know who it is. CNBC. October 27, 2017. Accessed on <<https://www.cnbc.com/2017/10/27/bitcoins-origin-story-remains-shrouded-in-mystery-heres-why-it-matters.html>>
- bitaddress.org, accessed on <<https://www.bitaddress.org>>
- Bitcoin. *Frequently Asked Questions*. Accessed on <<https://bitcoin.org/en/faq#who-created-bitcoin>>
- BitGold. Accessed on <<http://www.bitgold.com>>
- Bittrex, accessed on <<https://bittrex.com>>
- Bloomberg News. *China Bans Financial Companies From Bitcoin Transactions*. December 5, 2013. Accessed on <<https://www.bloomberg.com/news/articles/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions>>
- bread, accessed on <<https://breadapp.com/>>
- CME Group. *Now Available: Bitcoin Futures*. Accessed on <<http://www.cmegroup.com/trading/bitcoin-futures.html>>
- Choudhury, Saheli Roy. *China bans companies from raising money through ICOs, asks local regulators to inspect 60 major platforms*. CNBC. September 4, 2017. Accessed on <<https://www.cnbc.com/2017/09/04/chinese-icos-china-bans-fundraising-through-initial-coin-offerings-report-says.html>>
- coinbase. Accessed on <<https://www.coinbase.com>>
- CoinMarketCap. *Cryptocurrency Market Capitalizations*. Accessed on <<https://coinmarketcap.com/all/views/all/>>
- Cooper, M., O. Dimitrov, and R. Rau, 2001. "A Rose.com by Any Other Name", *Journal of Finance*, 56(6), p. 2371-2388.
- Cuthbertson, Anthony. "North Korea Hacking War on Bitcoin Exchanges is Part of "Biggest Global Sting."” *Newsweek*. December 19, 2017. Accessed on <<http://www.newsweek.com/north-korea-hacking-war-bitcoin-exchanges-part-biggest-global-sting-752161>>
- Dai, Wei. "b-money." 1998. Accessed on <<http://www.weidai.com/bmoney.txt>>
- Dai Coin. Accessed on <<https://makerdao.com>>

Electrum, accessed on <<https://electrum.org/>>

Federal Reserve Economic Data (FRED).

FOMO Coin, accessed on <<http://fomocoin.org/>>; and Jesus Coin, accessed on <<https://jesuscoin.network/>>

Gao, Alex. *Chinese Bitcoin Exchange OKEx Hacked for \$3 Mln, Police Not Interested*. The Cointelegraph. October 2, 2017. Accessed on <<https://cointelegraph.com/news/chinese-bitcoin-exchange-okex-hacked-for-3-mln-police-not-interested>>

Gandal, N., J. T. Hamrick, T. Moore, and T. Oberman, 2018. “Price Manipulation in the Bitcoin Ecosystem”, *Journal of Monetary Economics* (forthcoming).

Higgins, Stan. *The Bitfinex Bitcoin Hack: What We Know (And Don't Know)*. Coindesk. August 3, 2016. Accessed on <<https://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know/>>

inflation.eu.

Jesus Coin. Accessed on <<https://jesuscoin.network/>>

KeepKey, accessed on <<https://www.keepkey.com/>>

Kharpal, Arjun. *Initial coin offerings have raised \$1.2 billion and now surpass early stage VC funding*. CNBC. August 9, 2017. Accessed on <<https://www.cnbc.com/2017/08/09/initial-coin-offerings-surpass-early-stage-venture-capital-funding.html>>

Kharpal, Arjun. *Cryptocurrency start-up Confido disappears with \$375,000 from an ICO, and nobody can find the founders*. CNBC. November 21, 2017. Accessed on <<https://www.cnbc.com/2017/11/21/confido-ico-exit-scam-founders-run-away-with-375k.html>>

Ledger, accessed on <<https://www.ledgerwallet.com/>>

McKenna, Francine. *Here's how the U.S. and the world regulate bitcoin and other cryptocurrencies*. MarketWatch. December 28, 2017. Accessed on <<https://www.marketwatch.com/story/heres-how-the-us-and-the-world-are-regulating-bitcoin-and-cryptocurrency-2017-12-18>>

Mycelium, accessed on <<https://wallet.mycelium.com/>>

MyEtherWallet, accessed on <<https://www.myetherwallet.com/>>

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed on <<https://bitcoin.org/bitcoin.pdf>>

Nakamura, Yuji; and Kim, Sam. *Cryptocurrencies Drop as South Korea Bans ICOs, Margin Trading*. Bloomberg Technology. September 29, 2017. Accessed on

<<https://www.bloomberg.com/news/articles/2017-09-29/cryptocurrencies-drop-as-south-korea-bans-icos-margin-trading>>

NewsBTC. *BTER Allegedly the First in a Long Line of Hackings and Attacks*. February 16, 2015. Accessed on <<http://www.newsbtc.com/2015/02/16/bter-allegedly-first-long-line-hackings-attacks/>>

Nishanian, Mariam. 8 surprising places where you can pay with bitcoin. Business Insider. October 11, 2017. Accessed on <<http://www.businessinsider.com/bitcoin-price-8-surprising-places-where-you-can-use-2017-10>>

Parker, Luke. *Fourth largest Bitcoin exchange. Bithumb, hacked for billions of Won*. Brave NewCoin. July 4, 2017. Accessed on <<https://bravenewcoin.com/news/fourth-largest-bitcoin-exchange-bithumb-hacked-for-billions-of-won>>

PerkinsCoie. *Digital Currencies: International Actions and Regulations*. December 2017. Accessed on <<https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html>>

Popov, Serguei. *The Tangle*. October 1, 2017. Accessed on <https://iota.org/IOTA_Whitepaper.pdf>

Ramirez, Elaine. “5 Times Cryptocurrencies Rocked South Korea In 2017.” *Forbes*. December 19, 2017. Accessed on <<https://www.forbes.com/sites/elaineramirez/2017/12/19/5-times-cryptocurrencies-rocked-south-korea-in-2017/2/#251741fc74c9>>

Rizzo, Pete. *Poloniex Loses 12.3% of its Bitcoins in Latest Bitcoin Exchange Hack*. Coindesk. March 5, 2014. Accessed on <https://www.coindesk.com/poloniex-loses-12-3-bitcoins-latest-bitcoin-exchange-hack/>>

Sarin, Atulya. *Here’s how bitcoin can fit with your stocks and bonds*. MarketWatch. November 20, 2017. Accessed on <<https://www.marketwatch.com/story/heres-how-bitcoin-can-fit-with-your-stocks-and-bonds-2017-11-20>>

Sarin, Atulya. *This new way to trade bitcoin could kill its rally*. MarketWatch. December 7, 2017. Accessed on <<https://www.marketwatch.com/story/this-new-way-to-trade-bitcoin-could-be-what-kills-its-rally-2017-12-06>>

Sarin, Atulya. *The blockchain economy is coming, with or without bitcoin*. MarketWatch. January 3, 2018. Accessed on <<https://www.marketwatch.com/story/the-blockchain-economy-is-coming-with-or-without-bitcoin-2018-01-03>>

Sarin, Atulya. *Regulators should keep their hands off bitcoin and blockchain*. MarketWatch. January 16, 2018. Accessed on <<https://www.marketwatch.com/story/how-bitcoin-and-blockchain-can-truly-become-internet-20-2018-01-16>>

Schwartz, David; Youngs, Noah; and Britto, Arthur. *The Ripple Protocol Consensus Algorithm*. Accessed on <https://ripple.com/files/ripple_consensus_whitepaper.pdf>

Szabo, Nick. *Bit gold*. Accessed on <<https://unenumerated.blogspot.com/2005/12/bit-gold.html>>

Tether, accessed on <<https://tether.to/>>

Trezor, accessed on <<https://trezor.io/>>

U.S. Securities and Exchange Commission, December 11, 2017. “Statement on Cryptocurrencies and Initial Coin Offerings” (SEC Chairman Jay Clayton).

Ulmer, Alexandra; and Buitrago, Deisy. *Enter the ‘petro’: Venezuela to launch oil-backed cryptocurrency*. Reuters. December 3, 2017. Accessed on <<https://www.reuters.com/article/us-venezuela-economy/enter-the-petro-venezuela-to-launch-oil-backed-cryptocurrency-idUSKBN1DX0SQ>>

Whittaker, Zack. *Bitstamp exchange hacked, \$5M worth of bitcoin stolen*. ZDNet. January 5, 2015. Accessed on <<http://www.zdnet.com/article/bitstamp-bitcoin-exchange-suspended-amid-hack-concerns-heres-what-we-know/>>

Williams-Grut, Oscar. *South Korea has reportedly banned bitcoin futures*. Business Insider. December 11, 2017. Accessed on <<http://www.businessinsider.com/south-korea-bitcoin-futures-2017-12>>

Yermack, D., 2014. “Is Bitcoin a Real Currency? An Economic Appraisal”, *NBER and New York University Working Paper Series*.

Appendix A. Glossary

Presented below a list of commonly used acronyms and terms with corresponding definitions.

Coin-Related Terms:

Cryptocurrency A digital asset predicated on advanced encryption methods which are used to oversee coin supply and to verify settlement and transfer of funds

Mineable Refers to cryptocurrencies that compensate individuals who maintain the integrity of the system. Examples include Bitcoin (BTC) and Ether (ETH), where miners are rewarded with newly minted coins for providing proof of work for the underlying blockchain.

Pre-Mined Refers to cryptocurrencies for which developers have generated the entire coin supply at the onset of the project. Examples include Ripple (XRP) and Tether (USDT).

Exchange-Related Terms:

Daily Volume 24-hour trading volume, often expressed in USD.

Listings / Trading Pairs The manner in which an exchange-traded cryptocurrency is listed for purchase with an underlying cryptocurrency. On Bittrex, for instance, Bitcoin Cash (BCH) may be purchased using Bitcoin (BCH-BTC), Ether (BCH-ETH), or Tether (BCH-USDT), resulting in three separate listings / trading pairs for this cryptocurrency.

Common Acronyms:

ICO *Initial Coin Offering.* A primary market transaction in which funds are raised for the project/developers in question (loosely analogous to an IPO)

SAFT *Simple Agreement for Future Tokens.* Pre-launch token sales prior to the ICO.

Other Technical Terms:

| | |
|-----------------------|---|
| <i>Blockchain</i> | A continuously growing chain of transaction records, known as <i>blocks</i> , which provide the technical foundation on which cryptocurrencies are developed and maintained. A <i>public</i> blockchain is a decentralized, permission-less system maintained by the collective masses. In contrast, a <i>private</i> blockchain is maintained by a centralized group of users with permission to the system. |
| <i>Client Fork</i> | A software update designed to be backward compatible so as to maintain the original blockchain without a split. Also known as a <i>soft fork</i> . |
| <i>Hard Fork</i> | A major change in software that is not backward compatible, which causes a split in the blockchain and results in two separate cryptocurrencies. Examples include bitcoin cash (BCH) and bitcoin gold (BCG). Also known as a <i>coin split</i> . |
| <i>Smart Contract</i> | A program or protocol designed to verify and enforce a system of pre-determined rules. |

Appendix B. Use Cases and Design of Select Cryptocurrencies

Presented below is a brief description of each of the ten largest cryptocurrencies by market capitalization.

| | |
|--------------------|---|
| Bitcoin (BTC) | Bitcoin is the first cryptocurrency to use novel blockchain technology based on a proof-of-work system outlined in “Bitcoin: A Peer-to-Peer Electronic Cash System” by Satoshi Nakamoto in November 2008. To date, Bitcoin is the largest digital-currency and payments system based on a trustless, distributed-ledger protocol. |
| Ethereum (ETH) | Ethereum, which was first proposed by Vitalik Buterin in 2013, is a platform that allows users to implement smart contracts on the underlying blockchain. Many uses have been proposed for the Ethereum platform, including financial transactions, the internet-of-things, farm-to-table produce, electricity sourcing and pricing, and sports betting. As of 2017, Ethereum is the most widely used blockchain platform for the implementation of initial coin offerings. |
| Bitcoin Cash (BCH) | The Bitcoin scalability debate led to a hard fork to the Bitcoin blockchain on August 1, 2017, which was designed to increase the block size to eight megabytes in order to decrease computational complexity. This split resulted in a new cryptocurrency: Bitcoin Cash. |
| Ripple (XRP) | The Ripple protocol, which was released in 2012, provides a real-time currency exchange and settlement system, with payments settling in as little as four seconds. The system supports tokens representing fiat currency, cryptocurrency, commodity or any other unit of value such as frequent flier miles or mobile minutes. |
| Litecoin (LTC) | Litecoin is nearly identical to Bitcoin with respect to its intended use case and along many technical details. However, Litecoin facilitates much faster settlement, with the Litecoin network aiming to process blocks every 2.5 minutes (compared to Bitcoin’s 10-minute processing time). |
| Bitcoin Gold (BTG) | Bitcoin Gold, which came to fruition on October 24, 2017, is the result of another hard fork to the Bitcoin blockchain. The major change instilled on the underlying protocol was switching Bitcoin's SHA-256 proof-of-work algorithm to the Equihash ASIC-resistant algorithm. |

- IOTA (IOTA) IOTA, which was founded in 2012, seeks to provide an IoT (Internet of Things) protocol to secure machine-to-machine communications and payments. Transactions on IOTA are expected to be faster and more conducive to horizontal scalability than those on the Bitcoin Blockchain, largely based on the adoption of an innovation that replaced the blockchain implementation with a directed acyclic graph referred to as a “tangle”. The IOTA protocol is still under development.
- Cardano (ADA) Cardano, which began development in 2015, seeks to provide a faster more scalable rival to Ethereum. That is, Cardano also intends to provide a protocol on which to develop and execute smart contracts, but with a proof of stake, as opposed to proof of work, system, which is expected to make transactions much faster and less taxing. The Cardano protocol is still under development.
- Monero (XMR) Monero focuses on privacy by obscuring the information regarding the sender, recipient, and amount of each transaction. By providing a high level of privacy, Monero is fungible, meaning that every unit of the currency can be substituted by another unit, and addresses with coins previously associated with undesirable activity can be blacklisted by users.

Appendix C. Examples of Smart Contracts

ICOs are not the only implementations of smart contracts written on Ethereum and newer rival platforms designed to facilitate the creation of decentralized apps (dApps). Presented below are a few examples of notable non-ICO smart contracts and decentralized apps (dApps) built on the Ethereum blockchain.

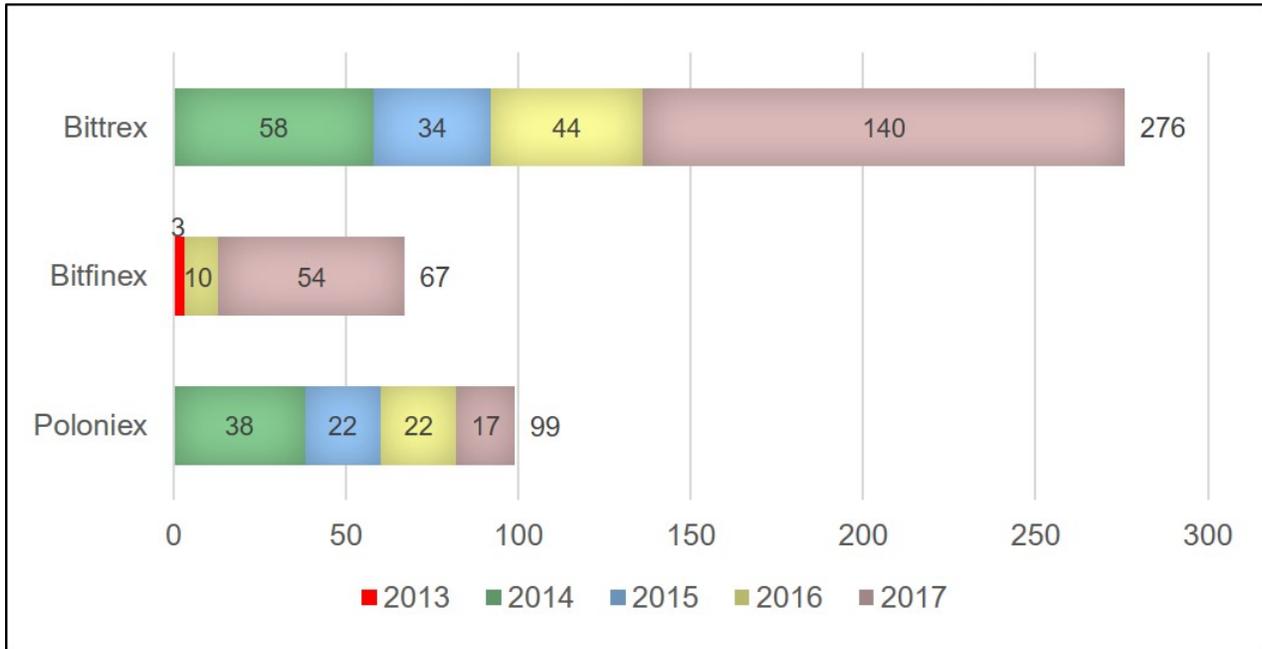
- CryptoKitties CryptoKitties is a frontrunner in blockchain-based games in which players can collect, trade, and breed virtual cats known as cryptokitties. Each cryptokitty is unique, and ownership is validated on the underlying blockchain. Although cryptokitties can be purchased and sold, they do not constitute a native token to the platform. That is, transactions in this virtual game require Ether, which fuels the smart contracts to track the cryptokitties on the Ethereum blockchain. Accessed on <<https://www.cryptokitties.co/>>
- Fishbank Motivated by the success of CryptoKitties, Fishbank is another blockchain-based game currently in development. Much like in CryptoKitties, players in Fishbank collect and trade virtual fish, and fishing in this game requires Ether. Players can expand their collections by purchasing virtual fish from other players at the virtual Fishbank Market. Accessed on <<https://fishbank.io>>
- World of Ether World of Ether is a decentralized virtual game currently in development. Interested players must purchase eggs (with Ether), which will hatch into various monsters once the game is deployed. Similar to CryptoKitties, players in the World of Ether can breed and trade monsters, with the added feature of also battling their monsters against those of other players. Accessed on <<https://worldofether.com>>
- EtherTweet EtherTweet is a decentralized microblogging platform, which is designed to provide a Twitter-like experience, but without a central owner controlling users or content. Accessed on <<https://github.com/yep/eth-tweet>>
- Weifund Weifund is crowdfunding platform developed on Ethereum. Users can either run a campaign or fund a campaign, with contributions made in Ether. As with all smart contracts written on the Ethereum platform, each transaction on Weifund also incurs a network fee to be paid in Ether. Accessed on <<http://weifund.readthedocs.io/en/latest>>

Figure 1. Total Number of Listed Cryptocurrencies

Total number of listings, as of December 3, 2017, across three major cryptocurrency exchanges: (i) Poloniex, (ii) Bitfinex, and (iii) Bittrex.

Panel A:

Total number of listings (i.e., trading pairs) per exchange, broken down by vintage (i.e., the year the coin was first listed).



Panel B:

Total number of distinct listings across the three exchanges

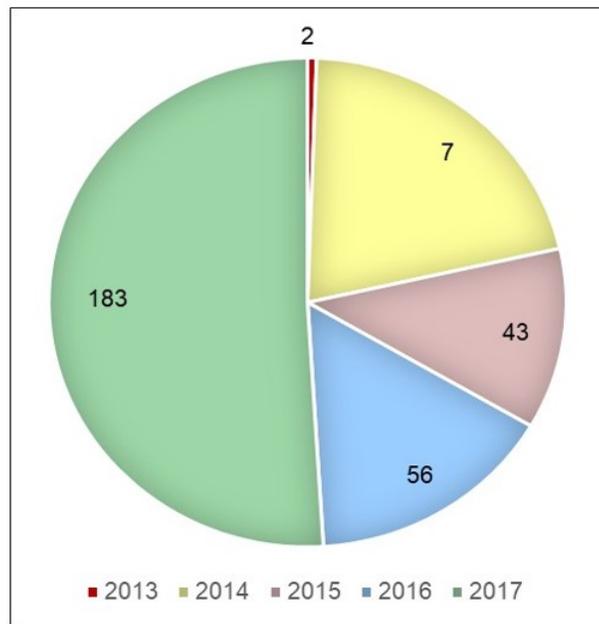
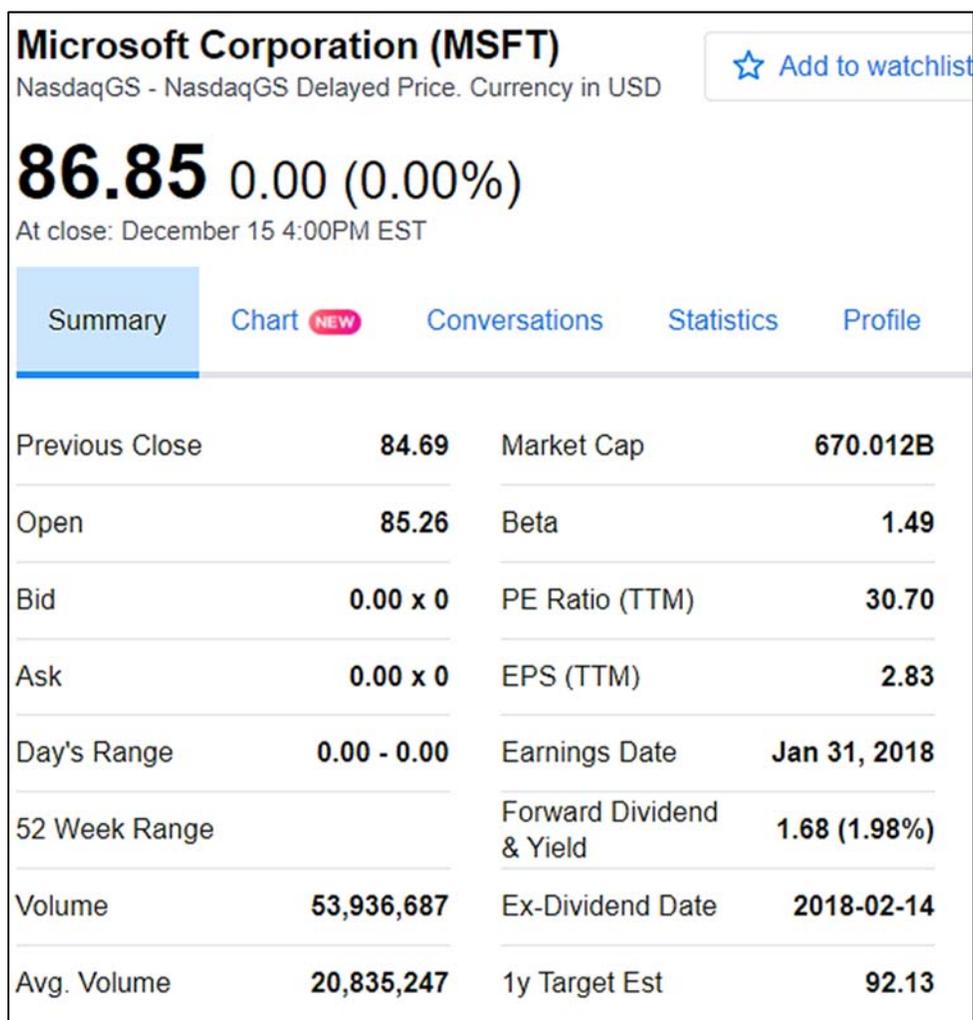


Figure 2. Comparison Snapshot of MSFT

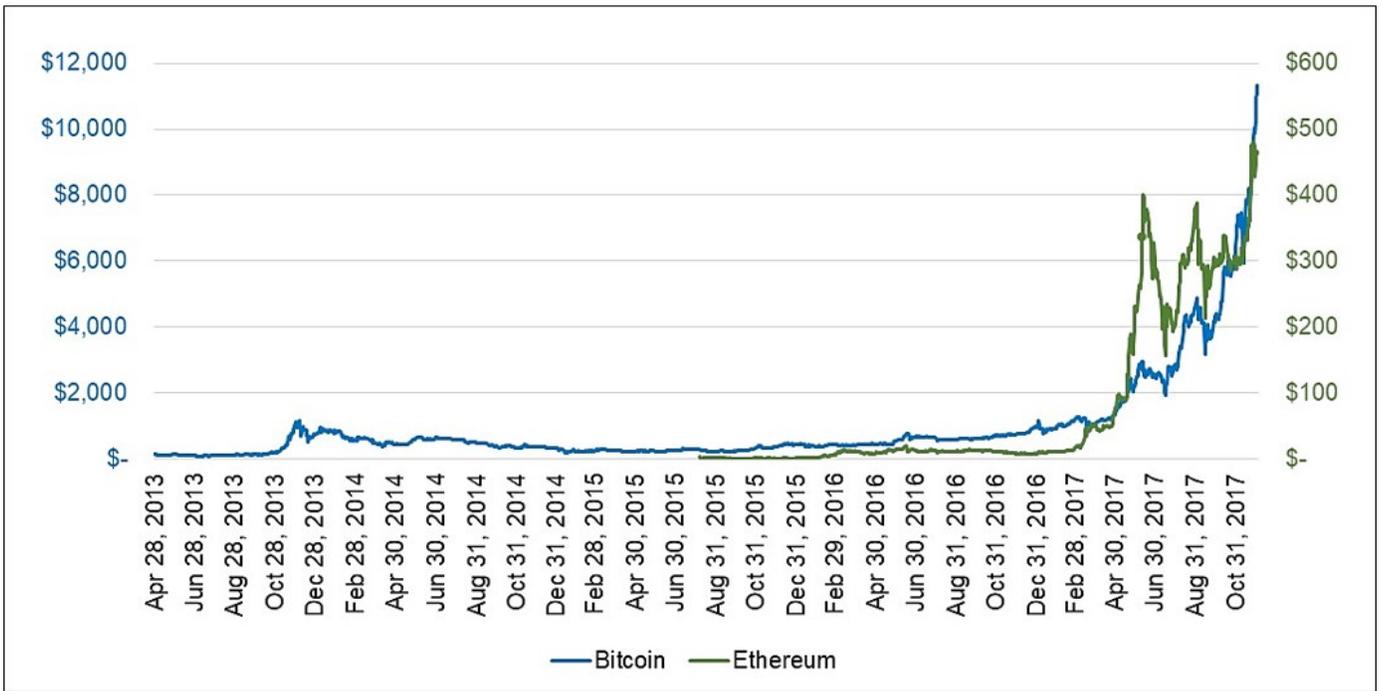


The numbers indicate that as of this date, MSFT had a market capitalization of approximately \$670 billion with a three-month trailing daily average trading volume of approximately \$1.8 billion.

In comparison, on this same date, bitcoin (BTC) had a market capitalization of approximately \$187 billion, with an average daily dollar volume of approximately \$4.8 billion (see **Table 1** for details).

Figure 3. Market Capitalization and Unit Prices for Bitcoin and Ether Over Time

Panel A:
Price per Unit Over Time



Panel B:
Market Capitalization Over Time (\$ billions)

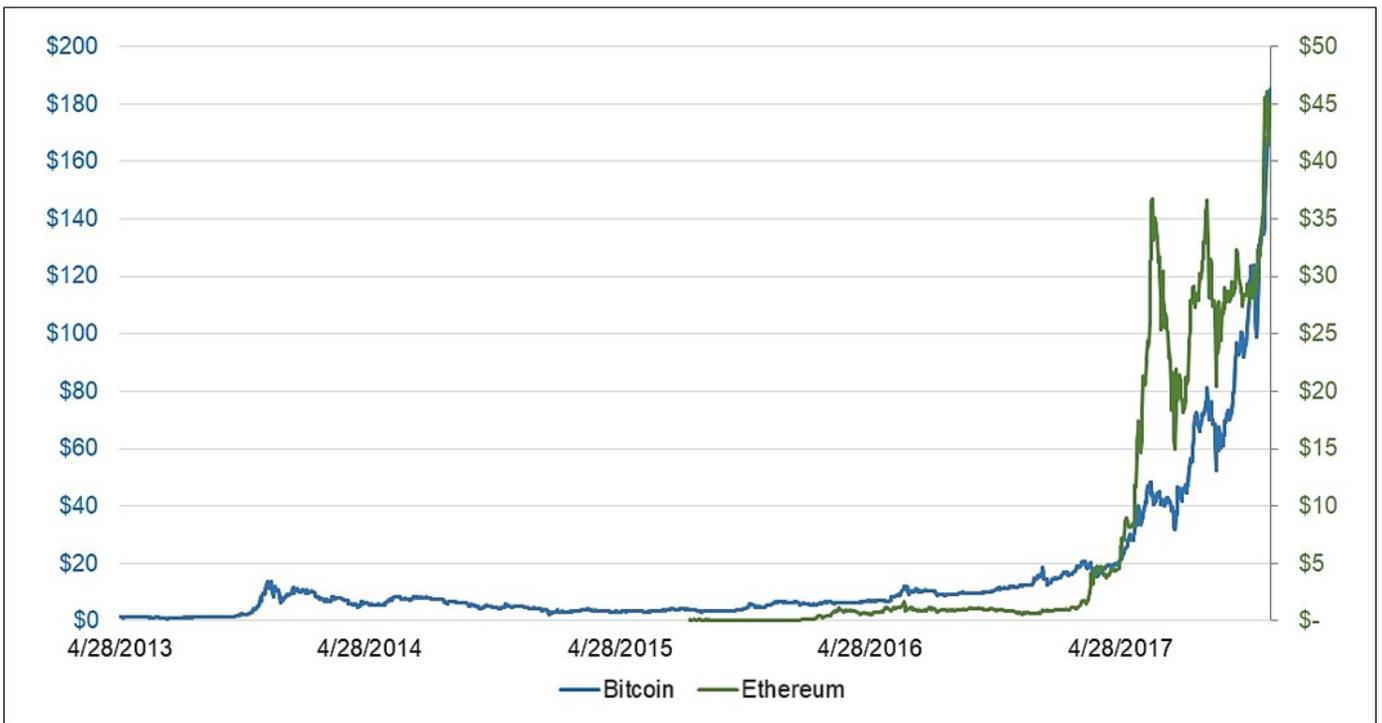


Figure 4. Dollar Volume for Bitcoin and Ether Over Time

Daily frequency from 4/28/2013 through 12/3/2017. Daily prices over time calculated as the volume-weighted daily average price across 169 exchanges at time 00:00:00.

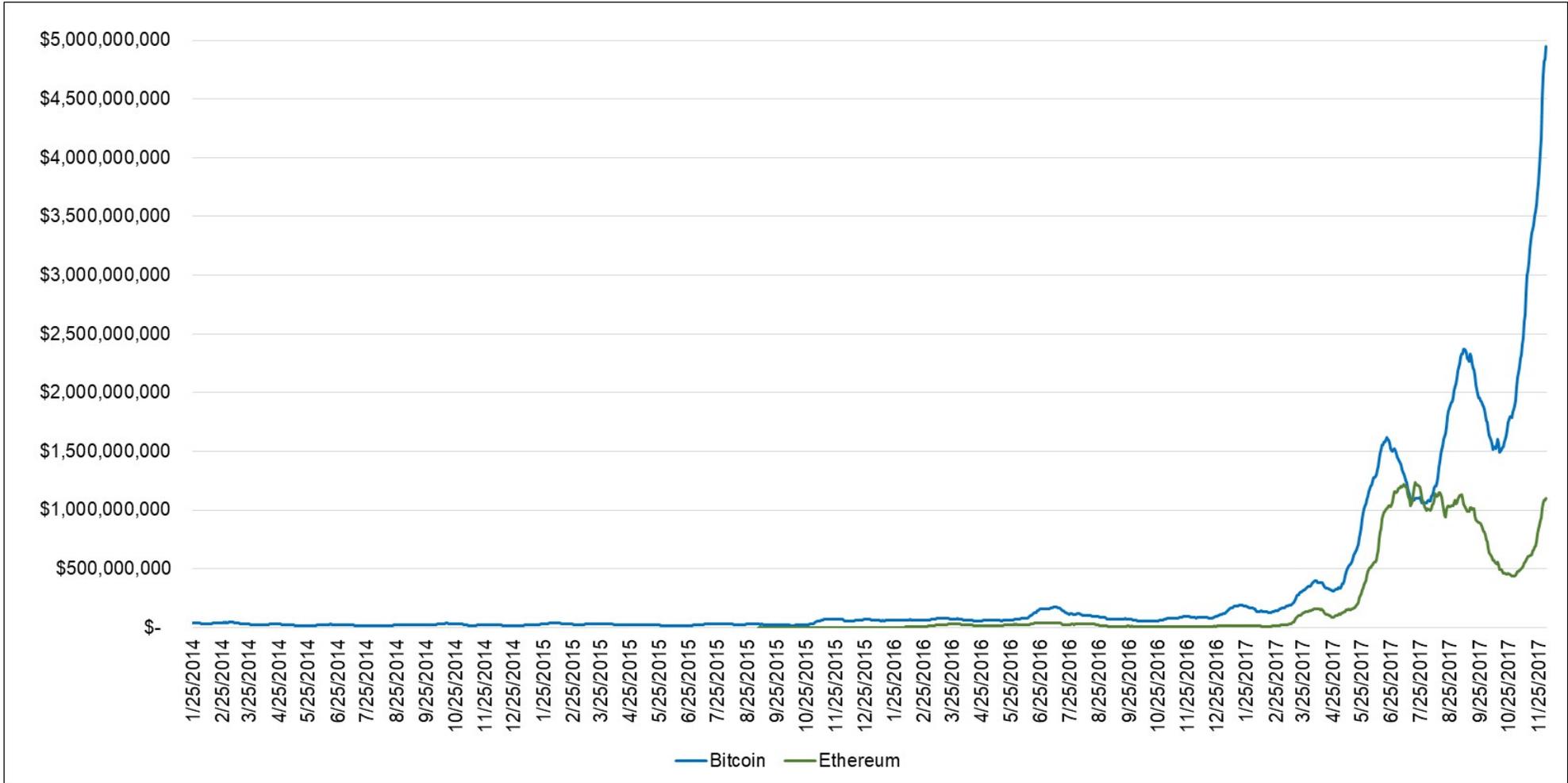
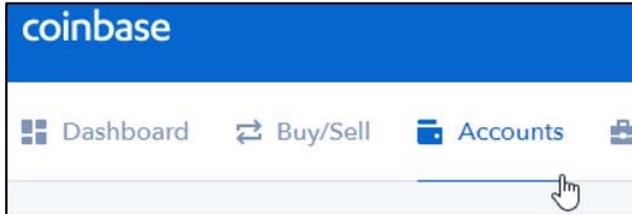


Figure 5. Steps to Investing in Cryptocurrencies

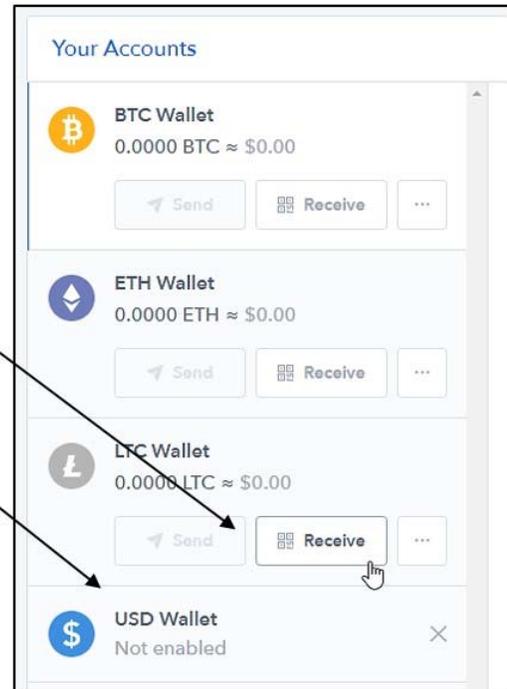
Step 1: Create an account on **coinbase**.



Step 2: Click on the Accounts tab to see your wallet". You will send and receive funds via a unique "address."

Step 3: Enable your USD wallet with a credit card or bank account. Then begin purchasing Bitcoin (BTC), Ethereum (ETH), or Litecoin (LTC).

Step 4: Create an account on **Bittrex**.



Step 5: Purchase another cryptocurrency, paying with either BTC (Bitcoin), ETH (Ethereum), or USDT (Tether).

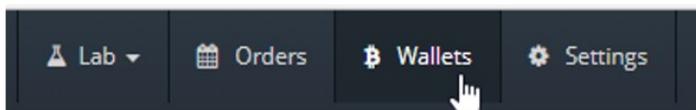
| BITCOIN MARKETS | | | | |
|-----------------|-------------|----------|----------|------------|
| MARKET | CURRENCY | VOLUME ↓ | % CHANGE | LAST PRICE |
| BTC-EMC2 | Einsteinium | 7570.959 | -10.9% ↓ | 0.00012000 |

| ETHEREUM MARKETS | | | | |
|------------------|----------|----------|----------|------------|
| MARKET | CURRENCY | VOLUME ↓ | % CHANGE | LAST PRICE |
| ETH-XLM | Lumen | 7141.186 | -7.2% ↓ | 0.00027367 |

| USDT MARKETS | | | | |
|--------------|------------------|---------------|----------|------------|
| MARKET | CURRENCY | VOLUME ↓ | % CHANGE | LAST PRICE |
| USDT-BTC | Bitcoin | 180377964.562 | 5.6% ↑ | 15285.95 |
| USDT-LTC | Litecoin | 12830232.732 | 2.6% ↑ | 149.00 |
| USDT-ETH | Ethereum | 9883973.933 | -3.1% ↓ | 443.00 |
| USDT-BCC | Bitcoin Cash | 7297611.157 | -4.4% ↓ | 1290.90 |
| USDT-ETC | Ethereum Classic | 4351781.588 | -4.3% ↓ | 25.90 |
| USDT-NEO | Neo | 4294888.117 | -4.4% ↓ | 33.60 |
| USDT-BTG | Bitcoin Gold | 3910070.678 | -9.6% ↓ | 210.00 |

Figure 6. Steps to Withdraw Cryptocurrency Investments

Step 1: Go to the Wallets tab in your **Bittrex** account.



Step 2: Click the “-” button of the cryptocurrency you wish to withdraw.

ACCOUNT BALANCES

Estimated Value: 0.00000000 BTC / 0.00 USD

Hide zero balances

| | | CURRENCY NAME | SYMBOL | AVAILABLE BALANCE |
|--|-----|---------------|--------|-------------------|
| | + - | Bitcoin | BTC | 0.00000000 |
| | + - | Litecoin | LTC | 0.00000000 |
| | + - | Dogecoin | DOGE | 0.00000000 |
| | + - | Vertcoin | VTC | 0.00000000 |

Step 3: Complete the fields. You will need your unique crypto-wallet address, obtained from your **coinbase** account (Figure 1, Step 2)

WITHDRAWAL DOGECOIN **CURRENTLY AVAILABLE: 0 DOGE**

| | | |
|------------|--|------|
| Address | <input type="text"/> | ADDR |
| Quantity | <input type="text" value="0"/> | DOGE |
| Tx Fee | <input type="text" value="2.00000000"/> | DOGE |
| Withdrawal | <input type="text" value="-2.00000000"/> | DOGE |

Please verify your withdrawal address. We cannot refund an incorrect withdrawal.

Do not withdrawal directly to a crowdfund or ICO. We will not credit your account with tokens from that sale.

[Withdrawal](#)

Figure 7. Storing Cryptocurrencies

Sample Providers of the Basic Methods for Storing Digital Assets

Software Wallets

| | |
|-----------------|--|
| Desktop wallets |   |
| Mobile wallets |   |
| Online wallets |  + exchange-specific wallets |

✓ Most convenient
✓ Least secure

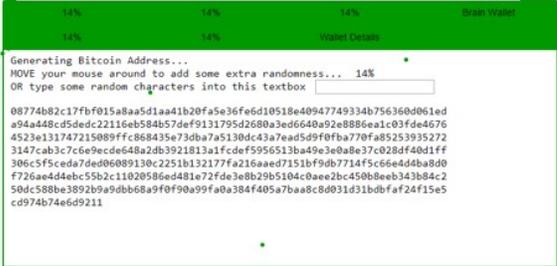
Hardware Wallets








Paper Wallets

*generate encrypted key to print on paper



✓ Least convenient
✓ Most secure (assuming paper is stored in safety deposit box)

Table 1. Cryptocurrency Summary Statistics

Basic statistics for the top 21 cryptocurrencies by market capitalization as of December 3, 2017

- *Market Cap* is the total value outstanding for the cryptocurrency aggregated across 169 exchanges.
- *Price (\$)* is the price per unit for the cryptocurrency, whereby the price is calculated as the volume-weighted average across 169 exchanges at time 00:00:00.
- *Volume (24h)* is the 24-hour dollar volume aggregated across the various trading pairs across 169 exchanges.
- *Circulating Supply* is the total number of coin units outstanding for the cryptocurrency.
- *Ticker* is the symbol under which the cryptocurrency trades, and an asterisk (*) next to the corresponding crypto-ticker denotes that the cryptocurrency has been pre-mined.

| | Market Cap (\$ millions) | Price | Volume (\$ millions) | Circulating Supply | Ticker |
|----------------------|-------------------------------------|--------------|---------------------------------|-------------------------------|---------------|
| 1. Bitcoin | 186,852 | 11,177.76 | 4,826 | 16,716,397 | BTC |
| 2. Ether | 44,944 | 467.68 | 823 | 96,101,457 | ETH |
| 3. Bitcoin Cash | 25,833 | 1,534.47 | 845 | 16,835,069 | BCH |
| 4. Ripple | 9,850 | 0.26 | 99 | 38,622,870,411 | XRP* |
| 5. Dash | 6,003 | 777.05 | 166 | 7,725,321 | DASH |
| 6. Litecoin | 5,443 | 100.61 | 329 | 54,101,549 | LTC |
| 7. Bitcoin Gold | 5,096 | 305.43 | 98 | 16,685,244 | BTG |
| 8. IOTA | 4,124 | 1.48 | 114 | 2,779,530,283 | IOTA* |
| 9. Cardano | 3,391 | 0.13 | 51 | 25,927,070,538 | ADA* |
| 10. Monero | 3,121 | 202.28 | 101 | 15,429,762 | XMR |
| 11. Ethereum Classic | 3,011 | 30.71 | 520 | 98,027,415 | ETC |
| 12. NEM | 2,447 | 0.27 | 34 | 8,999,999,999 | XEM* |
| 13. NEO | 2,333 | 35.89 | 47 | 65,000,000 | NEO* |
| 14. EOS | 2,029 | 3.94 | 172 | 514,717,161 | EOS* |
| 15. Stellar Lumens | 1,650 | 0.09 | 61 | 17,762,891,469 | XLM* |
| 16. BitConnect | 1,030 | 323.3 | 15 | 3,185,692 | BCH |
| 17. OmiseGO | 986 | 9.67 | 55 | 102,042,552 | OMG* |
| 18. Qtum | 959 | 13.02 | 98 | 73,696,328 | QTUM* |
| 19. Lisk | 918 | 7.94 | 20 | 115,533,469 | LSK* |
| 20. Zcash | 910 | 330.55 | 65 | 2,751,830 | ZEC |
| 21. Tether | 814 | 1 | 926 | 814,017,348 | USDT* |
| Total Sum | \$311,745 | | \$9,463 | | |

Table 2. Liquidity and Market Capitalization of Major Cryptocurrencies Over Time

Total market capitalization and average daily dollar volume on an annual basis for each of ten major cryptocurrencies from information aggregated across 169 exchanges

- Calculations for each year are made based on snapshots at 12/3/2017, 12/4/2016, 12/6/2015, 12/7/2014, and 12/1/2013, respectively.
- “N/A” denotes that the cryptocurrency in question was not yet traded in the particular year.
- Data on trading volume is unavailable prior to 2013.

| | | 2017 | 2016 | 2015 | 2014 | 2013 |
|--|--------------------|-------------|------------|-----------|-----------|------------|
| <i>Panel A. Market Capitalization (\$ 000)</i> | | | | | | |
| 1. | Bitcoin (BTC) | 186,851,800 | 12,346,015 | 5,894,778 | 5,089,269 | 13,063,516 |
| 2. | Ether (ETH) | 44,944,331 | 679,896 | 65,116 | N/A | N/A |
| 3. | Bitcoin Cash (BCH) | 25,832,964 | N/A | N/A | N/A | N/A |
| 4. | Ripple (XRP) | 9,850,343 | 236,220 | 175,753 | 447,130 | 367,703 |
| 5. | Dash (DASH) | 6,002,925 | 60,961 | 14,452 | 11,578 | N/A |
| 6. | Litecoin (LTC) | 5,443,078 | 191,152 | 153,070 | 127,275 | 934,939 |
| 7. | Bitcoin Gold (BTG) | 5,096,157 | N/A | N/A | N/A | N/A |
| 8. | IOTA (IOTA) | 4,123,970 | N/A | N/A | N/A | N/A |
| 9. | Cardano (ADA) | 3,391,457 | N/A | N/A | N/A | N/A |
| 10. | Monero (XMR) | 3,121,066 | N/A | N/A | N/A | N/A |
| <i>Panel B. Average Daily Volume (\$ 000)</i> | | | | | | |
| 1. | Bitcoin (BTC) | 4,826,067 | 56,120 | 77,589 | 5,850 | --- |
| 2. | Ether (ETH) | 822,953 | 9,545 | 350 | N/A | --- |
| 3. | Bitcoin Cash (BCH) | 845,126 | N/A | N/A | N/A | --- |
| 4. | Ripple (XRP) | 98,707 | 1,059 | 771 | 1,443 | --- |
| 5. | Dash (DASH) | 165,748 | 925 | 62 | 51 | --- |
| 6. | Litecoin (LTC) | 329,120 | 1,261 | 2,953 | 1,694 | --- |
| 7. | Bitcoin Gold (BTG) | 98,241 | N/A | N/A | N/A | --- |
| 8. | IOTA (IOTA) | 113,598 | N/A | N/A | N/A | --- |
| 9. | Cardano (ADA) | 51,419 | N/A | N/A | N/A | --- |
| 10. | Monero (XMR) | 100,557 | N/A | N/A | N/A | --- |

Table 3. Crypto-Exchange Summary Statistics

Basic statistics for the top 20 crypto-exchanges by average daily dollar volume in 2017

- *Inception* is the year in which trading commenced on the exchange in question.
- *No. of Listings* is the total number of distinct trading-pair listings on the exchange as of December 6, 2017.
- *Average Daily Vol.* is the average daily dollar volume, in both USD and BTC, of trades across all trading pairs of listed cryptocurrencies on the exchange throughout 2017.
- *Hacked* is a binary indicator denoting whether the exchange has been hacked.

| | Inception | Location | No. of Listings | Average Daily Vol. | Hacked? |
|--------------|------------------|-----------------|------------------------|--------------------------------------|----------------|
| 1. Bitfinex | 2012 | Taiwan | 67 | \$3,471,177,411 USD [254,009 BTC] | Yes |
| 2. Bitmex | 2014 | Hong Kong | 12 | \$2,404,460,000 USD [174,503] | |
| 3. Bithumb | ? | South Korea | 11 | \$2,182,701,300 USD [254,080 BTC] | Yes |
| 4. Bittrex | 2014 | USA | 274 | \$2,161,340,799 USD [158,204 BTC] | |
| 5. Binance | 2017 | Asia | 180 | \$1,320,927,439 USD [96,688 BTC] | |
| 6. GDAX | 2011 | USA | 9 | \$1,092,758,670 USD [79,705 BTC] | |
| 7. Poloniex | 2014 | USA | 99 | \$983,604,000 USD [71,763 BTC] | Yes |
| 8. Coincheck | 2014 | Tokyo | 1 | \$945,304,000 USD [68,605 BTC] | |
| 9. Coinone | 2015 | South Korea | 8 | \$719,858,540 USD [52,506 BTC] | |

Continued on next page

Table 3. Crypto-Exchange Summary Statistics, continued

| | Inception | Location | No. of Listings | Average Daily Vol. | Hacked? |
|--------------|------------------|-----------------|------------------------|-----------------------------------|----------------|
| 10. HitBTC | 2013 | London | 340 | \$638,235,739 USD [46,553 BTC] | Yes |
| 11. OKEx | 2013 | Belize | 40 | \$473,200,124 USD [34,515 BTC] | Yes |
| 12. Quoine | 2014 | Singapore | 30 | \$463,672,046 USD [33,651 BTC] | |
| 13. Bitstamp | 2011 | Luxembourg | 14 | \$473,200,124 USD [31,591] | Yes |
| 14. Kraken | 2011 | San Francisco | 45 | \$370,178,453 USD [27,001 BTC] | |
| 15. bitFlyer | 2014 | Japan | 3 | \$346,659,100 USD [25,285 BTC] | |
| 16. Korbit | 2013 | Seoul | 6 | \$285,953,974 USD [20,857 BTC] | |
| 17. Huobi | 2013 | Beijing | 47 | \$276,204,858 USD [20,055 BTC] | |
| 18. Gemini | 2015 | New York | 3 | \$267,969,800 USD [19,448 BTC] | |
| 19. BTCC | 2011 | Shanghai | 4 | \$213,351,560 USD 15,484 BTC | |
| 20. BTCBOX | 2014 | Tokyo | 4 | \$110,598,000 USD [8,027 BTC] | |

Table 4. Comparison of Transaction Speeds and Fees

- Average number transactions per second across various platforms
- Average transaction fees across platforms, expressed in USD

| | Average Transactions Per Second | Average Transaction Fee |
|----------|--|------------------------------------|
| Bitcoin | 7 | \$28.75 |
| Ethereum | 20 | \$2.56 |
| Litecoin | 56 | \$0.295 |
| Ripple | 1,500 | \$0.016 |
| Visa | 1,700 | 1.43% to 2.4% |
| Paypal | 193 | 2.9% plus \$0.30 |

Table 5. Volatility Comparison of Cryptocurrencies with Commodities/Currencies

- Daily percentage price volatility (based on USD conversions) on an annual basis
 - Major cryptocurrencies
 - Physical commodities
 - Fiat currencies
- Annualized inflation rates for each of countries issuing the actual fiat currencies
- “NA” denotes that the cryptocurrency was not yet traded at the year in question.

| | December | | | | | |
|--|-----------------|-------------|-------------|-------------|-------------|-------------|
| | 2017 | 2017 | 2016 | 2015 | 2014 | 2013 |
| <i>Panel A. Daily % Price Volatility (in USD) of Major Cryptocurrencies</i> | | | | | | |
| Bitcoin (BTC) | 0.0876 | 0.0499 | 0.0251 | 0.0360 | 0.0391 | 0.0685 |
| Ether (ETH) | 0.0770 | 0.0730 | 0.0692 | 0.1137 | N/A | N/A |
| Litecoin (LTC) | 0.1149 | 0.0869 | 0.0301 | 0.0630 | 0.0532 | 0.1347 |
| Tether (USDT) | --- | --- | --- | --- | N/A | N/A |
| <i>Panel B. Daily % Price Volatility (in USD) of Various Commodities</i> | | | | | | |
| Silver | 0.0094 | 0.0117 | 0.0179 | 0.0152 | 0.0137 | 0.0198 |
| Gold | 0.0063 | 0.0068 | 0.0097 | 0.0082 | 0.0080 | 0.0128 |
| Platinum | 0.0104 | 0.0098 | 0.0137 | 0.0123 | 0.0087 | 0.0118 |
| Paladium | 0.0112 | 0.0143 | 0.0177 | 0.0172 | 0.0119 | 0.0144 |
| <i>Panel C. Daily % Price Volatility (in USD) of Various Fiat Currencies</i> | | | | | | |
| US Dollar (USD) | --- | --- | --- | --- | --- | --- |
| Euro (EUR) | 0.0034 | 0.0045 | 0.0056 | 0.0076 | 0.0037 | 0.0049 |
| British Pound (GBP) | 0.0042 | 0.0051 | 0.0089 | 0.0052 | 0.0033 | 0.0047 |
| Swiss Franc (CHF) | 0.0039 | 0.0044 | 0.0053 | 0.0112 | 0.0041 | 0.0058 |
| Japanese Yen (JPY) | 0.0037 | 0.0056 | 0.008 | 0.0054 | 0.0049 | 0.0075 |
| Chinese Yuan (RMB) | 0.0019 | 0.0021 | 0.002 | 0.0018 | 0.0012 | 0.0007 |
| Indian Rupee (INR) | 0.0021 | 0.0026 | 0.0031 | 0.0036 | 0.0041 | 0.0081 |
| Mexican Peso (MXN) | 0.0050 | 0.0067 | 0.0105 | 0.0068 | 0.0043 | 0.0064 |
| South African Rand (ZAR) | 0.0129 | 0.0098 | 0.0132 | 0.0096 | 0.0065 | 0.0079 |

Continued on next page.

Table 5. Comparison of Cryptocurrencies with Physical Currencies, continued

| | 2017 | 2016 | 2015 | 2014 | 2013 |
|---|-------------|-------------|-------------|-------------|-------------|
| <i>Panel D. Annualized Inflation Rates of Various Countries</i> | | | | | |
| United States (USD) | 0.0213 | 0.0126 | 0.0012 | 0.0162 | 0.0147 |
| Euro-Zone (EUR) | 0.0155 | 0.0024 | 0.0003 | 0.0043 | 0.0135 |
| Great Britain (GBP) | 0.0051 | -0.0043 | -0.0114 | -0.0001 | -0.0022 |
| Switzerland (CHF) | 0.0041 | -0.0012 | 0.008 | 0.0276 | 0.0035 |
| Japan (JPY) | 0.0157 | 0.0200 | 0.0144 | 0.0192 | 0.0262 |
| China (RMB) | 0.0235 | 0.0497 | 0.0588 | 0.0637 | 0.1092 |
| India (INR) | 0.0267 | 0.0064 | 0.0005 | 0.0147 | 0.0253 |
| Mexico (MXN) | 0.0597 | 0.0282 | 0.0272 | 0.0402 | 0.0381 |
| South Africa (ZAR) | 0.0526 | 0.0659 | 0.0451 | 0.0612 | 0.0577 |

Table 6. Regulatory Landscape of Cryptocurrencies Across Countries

| Country | Government Advisory? | Is It Legal? (Y=yes, N=No, U=Undecided) | | | | Miscellaneous | |
|----------------|----------------------|--|-------------------------|--------------------------------|-------------|--------------------------|----------------------|
| | | Payments / Transactions | Retail Investor Trading | Institutional Investor Trading | ICO Listing | Consideration of Bitcoin | State coin to launch |
| United States | Y | Y | Y | | | Commodity / property | N |
| Abu Dhabi | Y | Y | Y | U | U | Commodity / property | N |
| Argentina | Y | Not legal tender | U | U | U | Undecided | N |
| Austria | Y | U | U | U | U | Undecided | N |
| Australia | Y | Y | U | Y | U | Commodity / property | N |
| Bangladesh | N | N | N | N | N | Illegal | N |
| Belgium | Y | Not legal tender | U | U | U | Undecided | N |
| Bermuda | N | No statement | No statement | U | U | No statement | N |
| Bolivia | Y | N | N | N | N | NO | N |
| Brazil | Y | U | U | U | U | Undecided | N |
| Bulgaria | N | U | U | U | U | Commodity / property | N |
| Canada | Y | Y | Y | Y | Y | Commodity / property | N |
| China | Y | Y | N | N | N | Commodity / property | N |
| Columbia | Y | N | N | N | N | NO | N |
| Croatia | Y | U | U | U | U | Undecided | N |
| Cyprus | Y | U | U | U | U | Undecided | N |
| Czech Republic | Y | Y | Y | Y | U | Undecided | N |
| Denmark | Y | U | U | U | U | Not taxable | N |
| Ecuador | Y | N | N | N | N | Illegal | Y |
| Estonia | Y | U | U | U | U | Commodity / property | Y |
| European Union | Y | U | U | U | U | Undecided | N |
| Finland | Y | U | U | U | U | Commodity / property | N |

Table 6. Regulatory Landscape of Cryptocurrencies Across Countries, continued

| Country | Government Advisory? | Is It Legal? (Y=yes, N=No, U=Undecided) | | | | Miscellaneous | |
|-------------|----------------------|--|-------------------------|--------------------------------|-------------|--------------------------|----------------------|
| | | Payments / Transactions | Retail Investor Trading | Institutional Investor Trading | ICO Listing | Consideration of Bitcoin | State coin to launch |
| France | Y | Y | Y | Y | U | Commodity / property | N |
| Germany | Y | U | Y | U | U | Private Money | N |
| Greece | Y | U | U | U | U | Undecided | N |
| Greenland | Y | U | U | U | U | Not taxable | N |
| Hong Kong | Y | U | U | U | U | Undecided | N |
| Hungary | Y | U | U | U | U | Undecided | N |
| Iceland | Y | N | U | N | N | Virtual currency | N |
| India | Y | U | N | U | U | Undecided | N |
| Indonesia | Y | N | N | N | N | No | N |
| Iran | Y | U | U | U | U | Undecided | N |
| Ireland | N | U | U | U | U | Undecided | N |
| Isle of Man | Y | Y | Y | Y | U | Cash | N |
| Israel | Y | U | U | U | U | Intangible asset | N |
| Italy | Y | Y | U | U | U | Undecided | N |
| Japan | Y | Y | Y | Y | U | Undecided | N |
| Jordan | Y | N | N | N | N | Illegal | N |
| Khazakstan | N | Y | Y | Y | Y | Commodity / property | N |
| Kyrgyzstan | Y | N | N | N | N | Illegal | N |
| Latvia | Y | U | U | U | U | Undecided | N |
| Lebanon | Y | N | N | N | N | e-money | N |
| Lithuania | Y | U | U | U | U | Undecided | N |
| Luxembourg | Y | U | U | U | U | Not legal tender | N |

Table 6. Regulatory Landscape of Cryptocurrencies Across Countries, continued

| Country | Government Advisory? | Is It Legal? (Y=yes, N=No, U=Undecided) | | | | Miscellaneous | |
|--------------|----------------------|--|-------------------------|--------------------------------|-------------|--------------------------|----------------------|
| | | Payments / Transactions | Retail Investor Trading | Institutional Investor Trading | ICO Listing | Consideration of Bitcoin | State coin to launch |
| Malaysia | Y | U | U | U | U | Not legal tender | N |
| Malta | Y | U | Y | Y | U | Undecided | N |
| Mexico | Y | U | U | U | U | Not legal tender | N |
| Morocco | Y | N | N | N | N | Illegal | N |
| Netherlands | Y | U | U | U | U | Undecided | Y |
| New Zealand | Y | U | U | U | U | Undecided | N |
| Norway | Y | U | U | U | U | Commodity / property | N |
| Philippines | Y | Y | Y | U | U | Commodity / property | N |
| Poland | Y | Y | Y | Y | U | Undecided | N |
| Portugal | Y | U | U | U | U | Commodity / property | N |
| Russia | Y | U | U | U | U | Undecided | Y |
| Saudi Arabia | N | U | U | U | U | Undecided | Y |
| Senegal | N | U | U | U | U | Undecided | Y |
| Serbia | Y | U | U | U | U | Not legal tender | N |
| Singapore | Y | Y | Y | Y | U | Undecided | N |
| Slovenia | Y | U | U | U | U | Not legal tender | N |
| South Africa | Y | U | U | U | U | Not legal tender | Y |
| South Korea | Y | U | U | U | N | Not legal tender | N |
| Spain | Y | U | U | U | U | Not legal tender | N |
| Sweden | Y | U | U | U | U | Commodity / property | Y |
| Switzerland | Y | Y | Y | Y | U | Virtual Currency | N |
| Taiwan | Y | U | U | U | U | Commodity / property | N |

Table 6. Regulatory Landscape of Cryptocurrencies Across Countries, continued

| Country | Government Advisory? | Is It Legal? (Y=yes, N=No, U=Undecided) | | | | Miscellaneous | |
|-------------------|----------------------|--|-------------------------|--------------------------------|-------------|--------------------------|----------------------|
| | | Payments / Transactions | Retail Investor Trading | Institutional Investor Trading | ICO Listing | Consideration of Bitcoin | State coin to launch |
| Thailand | Y | U | Y | Y | U | Undecided | N |
| Tunisia | N | U | U | U | U | Undecided | Y |
| Turkey | Y | U | U | U | U | Undecided | N |
| United Arab Emir. | Y | U | U | U | U | Undecided | N |
| United Kingdom | Y | Y | Y | Y | U | Commodity / property | N |
| Vietnam | Y | U | U | U | U | Not legal tender | N |