Cryptocurrency Trading and Investment
Assessing the Risks

Robert J. Frey, CEO – FQS Capital, LLC

Cryptocurrencies Are More Than Money

A cryptocurrency is an alternative digital currency that uses distributed decentralized ledger to manage the creation of new currency units and execute transactions securely and anonymously. The first and most popular cryptocurrency is Bitcoin whose ledger was initialized January 2009 by its "genesis block" (Figure 1) containing a comment on the financial instability caused by fractional reserve banking: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."

```
static CBlock CreateGenesisBlock(uint32_t nTime, …, const CAmount& genesisReward)
{
const char* pszTimestamp = "The Times 03/Jan/2009 Chancellor on brink of second
bailout for banks";

const CScript genesisOutputScript = CScript() << ParseHex("04678…11d5f") <<
OP_CHECKSIG;

return CreateGenesisBlock(pszTimestamp, …, genesisReward);
}
```

Figure 1 - Bitcoin Genesis Block

If you had purchased $1,000 worth of bitcoins at $13.40 on January 3, 2014, they would be worth $537,308 on July 20, 2018 when the closing price hit $7,333.93. On that day the total market value of all bitcoins was nearly $140 billion. Of course, that was down considerably from its highest close of $19,345.50 on December 16, 2017. Bitcoin in specific and cryptocurrencies in general have garnered increasing interest among governments, financial institutions, investors, and traders. According to industry website coinmarketcap.com, total market value of the over 1,300 cryptocurrencies now operating is over $300 billion, but that value varies greatly day-to-day.

In Figure 2 we have plotted the closing price of Bitcoin using all data using the API from the cryptocompare.com web site. The price swings have occurred over several orders of magnitude and so we have resorted to a logarithmic scale so that the data could be meaningfully represented. Much of the interest in cryptocurrencies comes from the fact that several of the early purchasers of Bitcoin have become billionaires.

As we will see, cryptocurrencies and the blockchain technology that supports them are in a position to disintermediate transactions across a wide range of applications, including currency management, securities trading, resource allocation, contract management, and just about any activity which now demands

the presence of a trusted third-party to execute. They offer the possibility to do so with greater speed, greater security, greater surety, greater confidentiality, and lower cost. However, this revolution is in its early stages. The details necessary to make its promise a reality are far from settled. If experience is a guide, then even if ultimately successful, we are in for a wild ride and dramatic industry shakeout along the way.

Figure 2 - Bitcoin Price History (Source: cryptocompare.com)

An Overview and History

We will survey this area and along the way develop a clearer view of the opportunities and risks involved with investing and trading in cryptocurrencies and in the underlying blockchain technology that enables them. We will then close with a statistical overview of the changes in value of four major cryptocurrencies: Bitcoin, Ethereum, Ripple, and Litecoin through July 2018.

Money is meant to serve as a medium of exchange and store of value. Most money we are familiar with is fiat currency, which is not backed by any hard asset but is created by central banks and further expanded by fractional reserve banking. Most of the money exists as entries in the ledgers of governments and financial institutions, not as physical bills and coins. Thus, “money” today is an abstract concept and has value because we all agree to give it value.

A cryptocurrency, whose units are generically called coins or tokens, is a digital asset that, like familiar fiat money, is not backed by hard assets and is intended to be used as a medium of exchange and store of value. Unlike the fiat currencies of nations, there is no trusted third-party to create them (a central bank) or transact or record them (a bank or other financial institution). Cryptocurrency exchanges maintain a distributed digital ledger in which currency units are created

and transactions are executed and recorded by consensus. Transactions in Bitcoin and most other cryptocurrencies are both public and anonymous.

The first practical cryptocurrency was Bitcoin, created in 2009 by a developer or group of developers operating under the pseudonym Satoshi Nakamoto. The new technology that enabled this was the blockchain, which is used to create a distributed public database or ledger of transactions. The records, or blocks, in the ledger are linked using a strong form of encryption. Each block contains a number of individual transactions. The blockchain's design makes it impractical to counterfeit currency units, to record false transactions (such as double spending the same currency unit), or to change a record retroactively. The blockchain works by consensus and will maintain its integrity even if a significant minority of exchanges attempts to subvert it.

New currency units are most frequently created using a proof-of-work scheme. Miners, the managers of the exchanges that constitute the distributed ledger, are rewarded for doing the cryptographic work required to record and coordinate transactions in the blockchain. The computations required are extensive, and major costs of operating a mining operation are the specialized hardware needed and electricity consumed. A proof-of-space scheme, where miners commit memory or storage space instead of CPU cycles, is the next most used method. There are several others, although all are based on the miners' commitment of resources of one form or another to the maintenance of the blockchain. Miners also receive compensation from transaction fees.

In order to prevent inflation from mining, there are limits placed on the creation of new currency units. The total number of coins that ultimately will be produced is fixed (21 million in the case of Bitcoin). As the supply grows, the cryptographic work required to mine coins also grows. Many therefore consider them to be deflationary. On the other hand, the code is open source. New cryptocurrencies are easily created, and there are over a thousand competing cryptocurrencies in operation. Also, a new currency can be "forked" off an existing cryptocurrency. Forks of Bitcoin so far have been: August 2017 creating BitcoinCash, October 2017 creating BitcoinGold, and February 2018 creating BitcoinPrivate.

Coins are controlled by their owners' wallets, cryptographic keys contained in a computer file or even printed on paper (Figure 3) that are used to spend or receive coins. Transactions can be in fractional coins. In Bitcoin the smallest of fractional unit is the eponymously named satochi, one millionth of a bitcoin. Despite the fact that transactions are public, wallets provide anonymity (or at least pseudonymity) through their keys.

Figure 2 - Bitcoin Paper Wallet (showing cryptographic keys)

Risk of Lost Wallets

If an owner loses a wallet, then there is normally no way to retrieve the coins it contains. In June of 2014 a Welshman inadvertently trashed a hard drive containing his wallet with 7,500 bitcoins that had been originally purchased for $1,000. At the time of the loss they were worth $1.5 million. It is unknown how many "orphan" bitcoins exist, but estimates run as high as a third of the total. The potential for stolen or lost wallets means that the anonymity of cryptocurrencies comes with its own risks. It is possible for digital wallets to be held by a third party to guard against such loses, but this compromises the inherent anonymity and security of the blockchain.

Risks of Regulation

Many economists, governments, and financial institutions have reacted with skepticism, if not outright hostility, towards cryptocurrencies. Early in 2018 economist Paul Krugman posted on Twitter, "Bitcoin is worthless…its price rise has been driven purely by speculation—by what Robert Shiller calls a natural Ponzi scheme in which entrants make money only because others buy in…". Jaime Dimon, CEO of JP Morgan Case, has called Bitcoin a "fraud".

Many with libertarian leanings find it attractive that cryptocurrencies operate in an anonymous manner outside the control of governments. Unfortunately, it is also attractive to those engaged in money laundering, theft, drug and arms sales, tax evasion, or other illegal activities. The most famous example is The Silk Road, an online marketplace for illegal drug sales that opened in 2011 and was closed by the FBI in 2013.

Governments and large influential financial firms do not take well to being disintermediated. The potential regulatory risks associated with cryptocurrencies remains high. Many have enacted regulations requiring that exchanges maintain personal information about their users. In 2014 the Chinese Central Bank banned the handling of cryptocurrencies by that country's financial institutions. The UK's Prime Minister Theresa May has said that cryptocurrencies like Bitcoin should be looked at "very seriously." In 2018 US Treasury Secretary Steve Mnuchin stated that there was no need for "crypto" alternatives to the US dollar and that the Treasury's

Financial Stability Oversight Council has established a working group to evaluate their risks and possible illegal uses.

An additional motivation for regulation is to preserve the US dollar's role as the world's reserve currency. The dollar is the primary currency of international exchange. Many countries buy and sell Treasuries to fix their exchange rate or to keep it within close bounds. This is done to stabilize their currency and facilitate trade. Estimates are that two thirds of world's foreign currency reserves are in dollars.

However concerns about both the level of indebtedness and the economic dominance of the US have caused cracks to appear. Russia and China have agreed to transact with one another in their respective national currencies and an increasing proportion of reserves are being held in euros. Cryptocurrencies represent a potential new threat and how that threat will be answered is not known.

While many of the larger governments and central banks have been suspicious, some of the smaller have jumped on the trend. In February of 2018 Venezuela, using its crude oil reserves as a backing, launched its own cryptocurrency, the Petro—whose purchase in the US was quickly banned. A month later the Marshall Islands, an equatorial Pacific nation of 60,000, launched the Sovereign or SOV as legal tender alongside the U.S. dollar. Predictably, the specter of stricter regulation in some countries has resulted in others setting themselves up as safe havens with minimal reporting and low taxes. Lithuania already has a mature and well regarded international banking and finance system and is an early entrant to become a leader in supporting cryptocurrencies.

Cryptocurrency Thefts and Frauds

In many forms of cryptography a single key is distributed to trusted parties and used to encode and decode messages. The risk of a security breach is high; it only takes one out many trusted parties to compromise the key. In contrast, cryptocurrencies depend on modern public key cryptography. A user publishes a public key, which is used to encode messages; messages can only be decoded, however, using a private key, which the user keeps secret. Hence, there is only one point of failure. While these schemes are for all practical purposes computationally unbreakable at our current level of knowledge and technology, there is always the prospect that either some new mathematical attack will prove successful or some new technology such as quantum computing will make breaking public key cryptography practical.

Nothing can guarantee absolute security, and there have been major cryptocurrency thefts. People manage the exchanges and wallets, and people can be careless or be tricked into bypassing their own security. In July 2018 the Wall Street Journal reported that according to Autonomous Research, a financial-services research firm, there have been at least 56 cyber-attacks at cryptocurrency exchanges with total loses topping $1.6 billion. Carbon Black, a cyber-security firm,

noted that much of the malware used to hack exchanges is cheap, readily available, and does not require much technical skill to use.

The most well known theft was in 2014 and involved $473 million in Bitcoin, causing the bankruptcy of one of the largest exchanges, Mt. Gox. In 2017 the Tether cryptocurrency was hacked resulting the loss of currency worth $31 million. There were several incidents in 2017. Among them, a software flaw in the Ethereum wallet application Parity resulted in the theft of $30 million. Later another Parity flaw led to $280 million in coins being frozen. That December thieves used a sophisticated social engineering attack that caused coin holders to compromise their passwords on a Slovenian-based Bitcoin miner, stealing $64 million.

Aside from security lapses, many initial coin offerings, ICOs, are outright scams. Investors anxious to participate in the price run–ups that often occur when a new cryptocurrency comes online are instead finding that they have been defrauded. Recent research jointly conducted by the Wall Street Journal and China's National Committee of Experts on Internet Financial Security concluded that about 20% of ICOs offered in the last twelve months and more than 400 of the existing cryptocurrencies are frauds.

Naturally, the "normal" financial system is not free of problems. "The Financial Cost of Fraud – 2015", a report jointly issued by PKF Littlejohn LLP and the University of Portsmouth, stated, "Fraud is the last great unreduced business cost…" The total cost of financial fraud over the years 2010 to 2013 was estimated to be over $4 trillion. Supporters of cryptocurrency claim that it is less prone to fraud and that security will continue to improve as it becomes widely used and as its users become more experienced.

Risks of Market Manipulation

Another danger is that there are disproportionately large holders among most cryptocurrencies who can manipulate the market to their advantage. In a pump-and-dump scheme prices are send downward by large orders only to be swept up by these same holders at lower prices, gaining both profits and greater control in the process. In April 2018 trading by a Bitcoin "whale" with $1.49 billion in holdings appeared to have caused a $200 drop in a single day. Similar moves appear in the records of the other major cryptocurrencies. These exchanges are not subject to the same level of regulatory restraint offered by, for example, the stock market, and their participants therefore have less protection against such manipulations. The DOJ and the Commodity Futures Trading Commission have, however, begun an investigation of Bitcoin, basing their authority on the fact that Bitcoin futures trade on the Cboe and CME.

Some Institutions Are Embracing Cryptocurrencies

Aside from genuine issues about fraud, illegal activities, and financial risk, many institutions are naturally concerned because cryptocurrencies support many

of the functions that are these organizations' *raisons d'etre*. However, as cryptocurrencies have flourished and customers have requested easier ways to invest in them, attitudes have begun to change as many have begun to worry about being left out.

Banks are floating plans to support cryptocurrencies and funds dealing in them. This may give these managers the opportunity to be recognized as SEC advisors, an option that was not open to them before. Coinbase, a digital exchange operating out of California, has developed relationships with several banks and investment managers, including Fidelity, USAA Bank, and Norwegian bank Skandiabanken. In 2017 Goldman Sachs began including comments on Bitcoin in its reports to clients. The Bitcoin Investment Trust is a passively managed trust backed by bitcoin that has daily liquidity. The commodity exchanges, the Cboe and CME, have begun to offer Bitcoin futures. Many more such programs are in development.

Reports are that some large corporations such as Microsoft, Dell, and Expedia have begun to accept bitcoins. This is not quite true. The usual arrangement is that the company will work through an intermediary such as Coinbase, which immediately coverts the bitcoins into dollars and transmits those to the payee.

Blockchains Have Other Applications

Some of the best opportunities may not come from cryptocurrencies *per* se but from the underlying blockchain technology. Blockchains have many potential uses aside from cryptocurrencies. Estonia and Dubai are testing using blockchains to store their citizens' healthcare records where they can be both publicly and anonymously shared. The ID2020 Project, a consortium that includes the United Nations, seeks to use blockchain and biometric data to serve the 1.1 billion people living without a recognized identity, providing them with access to government services and voting rights. Deutsche Bank sees significant international business opportunities in using blockchains to provide secure, fast, low cost, and "graft free" transactions involving digital tokens representing everything from traditional currencies, real estate, securities, and other assets. Many "cryptocurrency" exchanges have already expanded their business model to include such generalized tokens. And IBM has developed its own blockchain platform with applications in financial services, insurance, and supply chain management.

One remarkable application of blockchains is the smart contract. A smart contract is both a specification of the agreement between two or more parties and the mechanism to ensure that contract is honored when certain conditions are met by events occurring in the blockchain. A smart contract is not merely a program to implement a contract; it is the contract itself. The use of smart contracts is likely to increase. Yet, they are not a complete alternative to more traditional agreements, and there are many open practical and legal issues that remain open.

Some cryptocurrencies have already provided for smart contracts by supporting a standardized set. The primary difference, for example, between Bitcoin

and the next largest cryptocurrency Ethereum is that Bitcoin is intended to serve as an alternative currency and supports a limited set of contracts. Ethereum both functions as a cryptocurrency and is set up to handle generalized tokens representing all sorts of assets, tangible and intangible. And Ethereum also supports a full programming language that allows users to create smart contracts of arbitrary complexity.

A smart contract is a computer program. The more complex it becomes, the less certain one can be that it is bug free. Of course traditional contracts written by attorneys are not known to be error free and often involve Byzantine steps and involve third party intermediaries to minimize counter-party risks that do not exist with smart contracts.

A Statistical Risk Analysis of Cryptocurrency Daily Returns

We have analyzed the daily returns of four major cryptocurrencies: Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), and Litecoin (LTC). Our data were downloaded from the cryptocompare.com website, which provides history data for all major cryptocurrencies. For comparison we also used data for the S & P 500 index (S&P) downloaded from Yahoo!Finance.

The day-to-day variation in cryptocurrency returns was immense. So large, in fact, that attempting to characterize it using many of the usual approaches are no longer meaningful. The distributions that best fit the data are Log-Student *t* Distributions. These distributions fit the data extremely well and have estimated degrees of freedom between 1.5 and 3.4. They all have extremely heavy tails and the conventional approach of characterizing their volatility in terms of a standard deviation will not work. Instead we estimated the Value-at-Risk (VaR) and Conditional Value-at-Risk or expected shortfall (CVaR).

The VaR is based on two parameters, sampling frequency and confidence level. We used a daily VaR at a 99.9% confidence level. The VaR is that value such that the daily return is expected to be greater than it 99.9% of the time, or alternately, 0.01% of the time the daily return is expected to be worse than the VaR. A figure like 0.01%, or one out of a thousand, may not sound dangerous, but for daily returns this means one-day loses greater than the VaR will occur on average about once every four years. A related and more interesting statistic is the CVaR, the expected size of the loss given that the returns have broken the VaR threshold. For the S&P 500 the VaR is -5.6% and the CVaR is -8.2%.

For Bitcoin the numbers are quite different: 48.1% and 66.1%, respectively. The VaR and CVaR are illustrated below against part of the lower tail of the distribution of Bitcoin's daily returns (Figure 4). The 0.1% worst losses are represented by the shaded area; the VaR is the upper bound; the CVaR is the expected value.

The cryptocurrencies' expected shortfalls, the CVaRs, average *ten times* that of the S&P 500! When we consider that these "returns" are changes in the BTC/US$ exchange rate, they display a variability that is hardly in keeping with a currency representing "a stable store of value".

Unlike the S&P 500, the cryptocurrencies trade every day; hence, we slightly adjusted their VaRs' confidence level so that a comparable once-every-four-years frequency was achieved. We used data from 1950 on for the S&P 500; however, the cryptocurrency results are based on trading from July 1, 2015 to July 20, 2018. We used recent returns because earlier trading occurred in very thin markets. In latter half that variability steadied. The VaR-CVaR risk comparisons appear below (Figure 5).

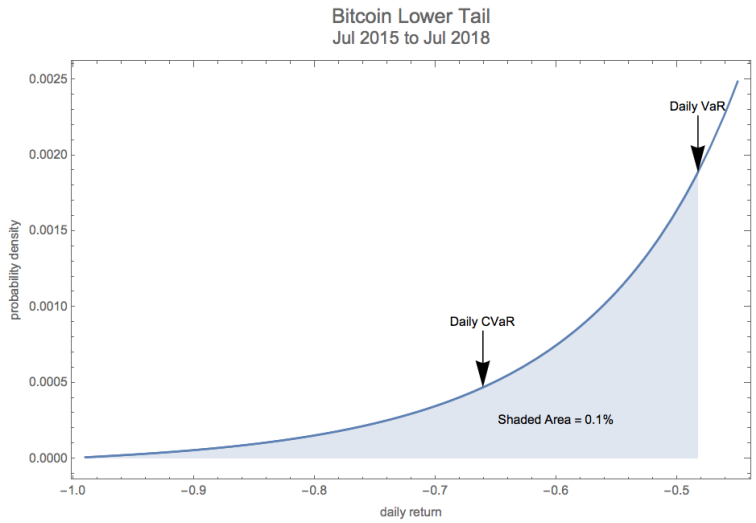

Figure 3 - Bitcoin Value-at-Risk and Expected Shortfall

There is a term "hold on for dear life", or HODL, that refers to individuals who are convinced that the cryptocurrency of their choice will ultimately be successful as an internationally accepted currency and, therefore, take a long-term buy and hold position. Many others, however, see a cryptocurrency more akin to a commodity such as gold or oil. Seeing the dramatic swings in value, they are interested in making gains by playing the cryptocurrency markets.

Comparative Risk Analysis From Jan 2015 To Jul 2018		
	VaR	CVaR
S&P	-5.6%	-8.2%
BTC	-48.3%	-66.1%
ETH	-58.2%	-72.8%
XRP	-75.0%	-87.6%
LTC	-79.3%	-91.4%

Figure 4 - Risk Analysis: S & P vs. Cryptocurrencies

Unfortunately, with the variation shown in their valuations, short positions (where the downside is unlimited) or leveraged ones (where gains and losses are magnified) is dangerous, exposing the holder to losses far in excess of committed capital. Even simple unleveraged long positions risk losses hitting so quickly and dramatically that it is unlikely that a stop loss provision could be exercised in a timely manner. Unlike other commodities, there are no options markets that can be used to place lower bounds on losses.

The Biggest Risk of Cryptocurrencies

We started this article with a brief look at the wide swings in value that Bitcoin has experienced over its short history. When we look at the other major cryptocurrencies, we see the same. This volatility means positions carry tremendous risk. Early in 2018 Warren Buffett in a CNBC interview said, "I can say almost certainly [cryptocurrencies] will come to a bad ending. When… or how I don't know… If I could buy a five-year put… I'd be glad to do it, but I would never short a dime's worth." Buffet's comment makes it clear that despite the fact he believes cryptocurrencies will eventually become worthless, he recognizes that they are so volatile that a short position could very well bankrupt you before that happens.

In the long-term cryptocurrencies' greatest risk is, of course, whether they will ever be accepted as money. As a medium of exchange cryptocurrencies do have the capability to support transactions—anonymously, more securely, more cheaply, more quickly, more simply, and with lower counter-party risk. An increasing number of businesses are willing to deal with some of the major cryptocurrencies, but adoption could not be called widespread.

Many find the possibility that cryptocurrencies will ever become recognized as a *bone fide* currency remote, arguing that there is no basis for people to assign any value to them. Much of the same argument, however, was leveled against fiat currencies when the world began abandoning the gold standard in the later part of the Twentieth Century. The counter argument that national fiat currencies are managed by central banks that maintain the necessary discipline to prevent unhealthy levels of inflation and deflation is easily met with countless examples

where countries have failed to exercise proper discipline. Cryptocurrencies have the incorruptible function of the blockchain to control them.

To say that valuations of cryptocurrencies have been extremely volatile is an understatement, and it is hard to see how any of them can function as a viable form of money unless that volatility is tamed. Our analyses clearly show, however, that until this volatility decreases even the most mature cryptocurrencies cannot function as workable stores of value.