LONG FINANCE

DISTRIBUTED FUTURES

Liquidity Or Leakage

Plumbing Problems With Cryptocurrencies

March 2018

CARDANO FOUNDATION

Yen

The Z/yen Group

Liquidity Or Leakage

Plumbing Problems With Cryptocurrencies

Rodney Greene
Quantitative Risk Professional
Advisor to Z/Yen Group

Bob McDowall
Advisor to Cardano Foundation

Foreword

Liquidity is the probability that an asset can be converted into an expected amount of value within an expected amount of time. Any token claiming to be 'money' should be very liquid.

Cryptocurrencies often exhibit high price volatility and wide spreads between their buy and sell prices into fiat currencies. In other markets, such high volatility and wide spreads might indicate low liquidity, i.e. it is difficult to turn an asset into cash. Normal price falls do not increase the number of sellers but should increase the number of buyers. A liquidity hole is where price falls do not bring out buyers, but rather generate even more sellers.

If cryptocurrencies fail to provide easy liquidity, then they fail as mediums of exchange, one of the principal roles of money. However, there are a number of ways of assembling a cryptocurrency and a number of parameters, such as the timing of trades, the money supply algorithm, and the assembling of blocks, that might be done in better ways to improve liquidity.

This research should help policy makers look critically at what's needed to provide good liquidity with these exciting systems.

Michael Parsons FCA
Chairman, Cardano Foundation,

Contents

Preface

This research report is trying to help the governance of cryptocurrencies, by more clearly tying their novel money supply algorithms to traditional economic and financial analysis. We should note that liquidity management issues recur throughout the centuries. Christopher Brown-Humes relates: "In the early 19th century, the Bank of England's main policy tool was a weather vane. When the wind blew from the East, ships sailed into London and the Bank supplied money so traders could buy the goods being unloaded at the docks. If a westerly wind blew, it would mop up any excess money to stop too much money chasing too few goods, thereby avoiding inflation". ["Room for Manoeuvre", Securities & Investment Review, Securities & Investment Institute, July 2007] The old gold standard was abandoned, in part, to give more ability to governments to manage broad money supply.

There is a lovely story about an analyst at the Bank of England realising that gilts went illiquid at 11:45am on most days. After much deeper analysis he realised that the illiquidity was due to Sweetings, the renowned fish restaurant. Sweetings doesn't book tables. If you're not in Sweetings by 12:00, you won't get a seat. So the gilt markets went illiquid at 11:45 because traders went for some fish and some liquid.

Traditional economic and financial analysis ranges widely among at least four types of liquidity - timing liquidity, value liquidity, market liquidity, and monetary liquidity. More often than it should be, 'liquidity' is discussed in a way that is simply synonymous with monetary policy, private equity lending, credit derivatives or the prevalent, popular 'carry trade'.

I would contend that the characteristics of liquid markets are resilience, depth and tightness. We can visualise the idea of "discovering the supply and demand curves" – they may not be smooth, nor continuous; they may have a wide band of uncertainty. In normal circumstances, liquidity risk = the odds of being surprised that the supply or demand curve isn't where you thought. We also know that black holes and white bubbles fundamentally change the nature of liquid markets – where sellers draw in more sellers, or buyers draw in more buyers, the price drops,

or rises, precipitously. Finally, we believe that liquidity risk might be reduced in markets that encourage diversity of participants and types of transactions.

But we will always struggle with the 'Alice in Wonderland' nature of defining liquidity. I'm afraid I can't resist concluding with a little ditty of my own, based on Jonathan Swift's construction around a flea:

> So, financiers observe, small pools
> suck larger pools' liquidity;
> yet tinier pools drain other drops,
> and so on to aridity.

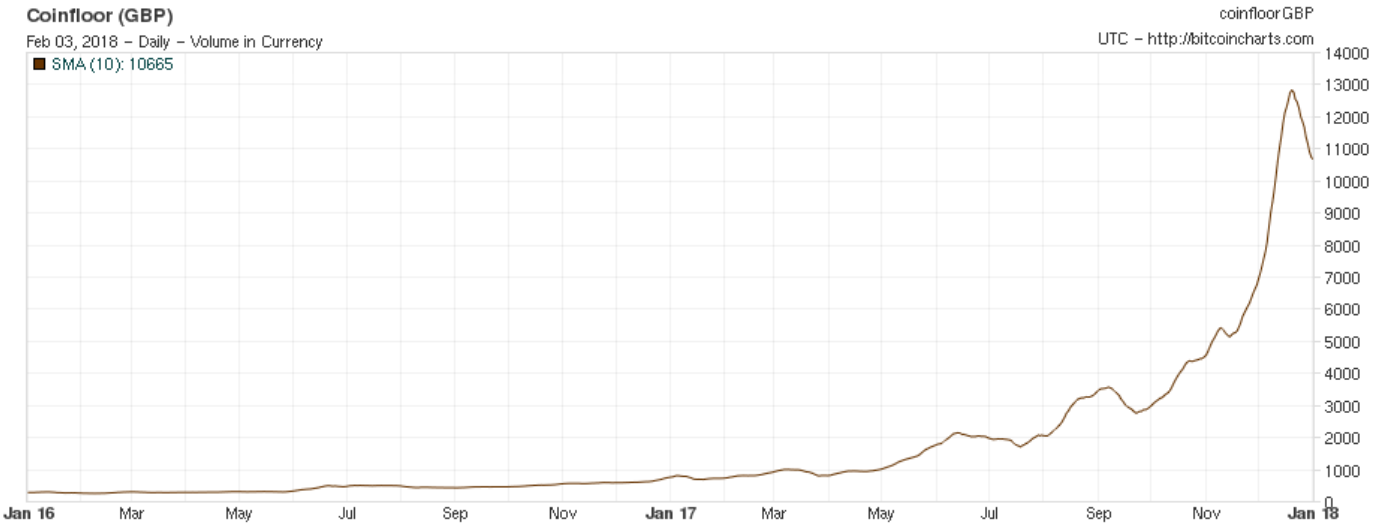
My sincere hope is that much of the analysis in this report helps improve the governance and regulation of cryptocurrencies by showing that traditional problems have not changed their spots that much in the wonderful new world of Smart Ledgers.

Professor Michael Mainelli FCCA FBCS FCSI
Executive Chairman, Z/Yen Group

Introduction

Liquidity, that is the ability to buy or sell a commodity or financial instrument and realise cash immediately, is an essential prerequisite for confidence in a market. Consumer interest in acquisition of cryptocurrencies has exponentially soared during Q4 2017. Figure 1 illustrates the exponential growth of the GBP/Bitcoin market's daily volume over the 2016-2017-time period.

Figure 1 Daily trade volume on the Coinfloor GBP/BTC exchange (units are GBP). Note that the daily volume increased from 1000 to over 12K in calendar year 2017.



Daily volume skyrocketed from less than a thousand to over 12,000 Bitcoins during this period. The scale and volume of speculation has expanded from a base of cognoscenti and aficionados of the cryptocurrency product to selective institutional investors and the general public on a global basis. Facilities that execute and settle transaction in cryptocurrencies have not been prepared or resourced for the volume and value of transactions. Conventional wisdom would suggest that increases in volume and value of transactions would increase liquidity in cryptocurrencies.

Liquidity has not increased. In fact, Bitcoin liquidity decreased by an order of magnitude from 2016 to 2017. Execution venues have suffered from inefficiency, inadequate customer servicing, and compliance and regulatory issues in processing transactions. Technical problems in establishing and operating secure storage of cryptocurrencies contributed to the to lack of liquidity. At the moment,

cryptocurrencies are suffering from the immaturity of the underlying mutual distributed ledger technology. The premise of this report is that this technology will quickly evolve, and so will financial applications of mutual distributed ledgers.

Address The Thirst For Cryptocurrency Liquidity With Technical And Operating Standards

The cryptocurrency market is enjoying a delightful roller coaster ride. Consider the following headlines just since December 2017:

- The Tokyo-based cryptocurrency exchange CoinCheck suffered the largest loss in mutual distributed ledger history – approximately $533 million worth of NEM crypto-tokens were hacked away in January 2018

- The Korean-based cryptocurrency exchange Youbit declared bankruptcy after hackers absconded with 17% of the exchange's assets

- Intel announced a potentially catastrophic security flaw in all computers – this flaw could dramatically slow adoption of the mutual distributed ledgers by corporate interests

- The US-Dollar/Bitcoin exchange rate peaked 19 December,2017 at $19,000/Bitcoin. The market cap reached $327 billion. The exchange rate has since fallen to $9,200/Bitcoin ($155 billion market cap) on 1 February, 2018.

Despite the outrageous investment returns, no publicly listed money-centre bank has made a material investment directly in cryptocurrencies – indeed Jamie Dimon, the CEO of the banking giant JP Morgan Chase, stated Bitcoin is "worse than tulip bulbs" a reference to the quick boom and bust that rocked the 17th century tulip market in Western Europe. He went further, stating "it's a fraud" that would eventually blow up. Chairman Dimon's comments beg the question, "is an asset with a market capitalisation in the hundreds of billions of dollars really a fraud that should be ignored or, perhaps, is there a hint of value under the crypto-tulip drama?"

In fact, there is great value that will soon be captured by these money-centre banks and other industries. The true long-term value of cryptocurrencies will be realised by wide-scale commercial adoption of the technology underlying cryptocurrencies, namely mutual distributed ledgers. The considerable operational, liquidity, and market risk factors of the crypto-markets and how mutual distributed ledger technologies can mitigate them are the topics covered in this paper.

This report also describes a key mutual distributed ledger technology, smart contracts or ledgers, and address their unique legal enforceability questions. The report concludes that changes must come to the Over the Counter (OTC) financial derivative market as a result of adoption of smart contracts.

The report is organised as follows.

- **Section 1**: An overview of mutual distributed ledgers and a description of their security vulnerabilities

- **Section 2**: Enumerates the economic risk factors of the cryptocurrency markets, with special attention on their illiquidity

- **Section 3**: Summarises the opinions of Doctor Anna Donovan, UCL Faculty of Laws, regarding the legal enforceability of smart contracts

- **Section 4:** Details the counterparty default risk reduction benefits of smart contracts in the financial derivatives domain

- **Conclusions**

Despite the hype, cryptocurrencies are here to stay. Mutual distributed ledger technology is immature, but the capital markets industry is driving forward to realise the true value and integrity in the underlying mutual distributed ledger smart contract business paradigm.

1. Cryptocurrency Mutual Distributed Ledgers - Introduction And Security Risks

- Despite the theoretical possibility of malicious mining, most MDL miners are rational and hence would prefer to collect the steady honest mining income

- The outsized crypto-returns make mutual distributed ledger infrastructure (especially crypto-wallets) very attractive hacking targets. Hence distributed ledgers should employ best practice software development and information security protocols.

- The impact of the recently announced Intel hardware vulnerabilities, Meltdown and Spectre, on mutual distributed ledgers and crypto-wallets may be quite severe

Mutual Distributed Ledger (MDL) Defined

A mutual distributed ledger (aka *blockchain*) is a computer data structure (an ordered chain of data blocks) with the following defining attributes:

- Mutual - shared across organizations and owned equally by all members of the network

- Distributed - copies of the data are spread across multiple locations. Each user on the network keeps her own copy, thus providing resilience and robustness

- Ledger - the structure is immutable. Once a transaction is written to the data structure it cannot be erased. This mean's the ledger's integrity can be easily proven.

Another way to think of mutual distributed ledgers is as permanent timestamping engines for computer records. Timestamps can be used to prove that data elements were entered at or before a certain time and have not been altered.

An MDL is a database that is consensually shared and synchronised across a computer network. The database is spread across multiple sites, institutions or geographies. Each user owns an identical copy. Any changes or additions to the ledger are reflected by nodes and copied to all participants in a matter of seconds or minutes.

MDLs can be *permissionless* or *permissioned*. Permissionless MDLs do not require registration with a central party. Users are anonymous. Permissioned MDLs require the identity of users to be whitelisted or blacklisted through some type of Know Your Customer (KYC) procedure.

Both permissioned and permissionless MDLs require a process by which the MDL is extended each time a new block of data is added.

This process must abide by the following rules:

- Data added to the MDL must maintain the integrity of the MDL structure
- Updates must be fluid, with new data broadcast quickly to all users of the MDL
- The process must be resilient to downtime and take account of individual users being unable to access the system
- Where a discrepancy occurs between versions of the MDL broadcast by different nodes (a 'fork'), there must be a process to ensure that the situation is resolved quickly, and the integrity of the MDL data is maintained

Un-permissioned MDLs assign the right to update the MDL either by a Proof of Work (PoW) or Proof of Stake (PoS) consensus mechanism. There is considerable debate amongst the crypto-currency community as to the best approach.

Proof of Work requires users to find a solution to a complex mathematical problem. The more computing power a user employs, the more likely the user is to achieve the solution before others and hold the right to update the MDL. In crypto-currencies such as Bitcoin, this is termed 'mining'. The first user to find a solution receives a prize of newly minted coins, which is the economic driver for

participation in the process. However, mining is time intensive and carries a heavy overhead in terms of energy and equipment.

Proof of Stake is an alternative approach, currently used by the Ripple MDL and explored by the Ethereum MDL. Proof of stake requires users to prove ownership of a certain amount of currency or to use some of their 'stake' in the currency to indemnify transactions against fraud, in order to participate in the next update of the MDL.

For the sake of completeness, it must be clear that there are additional blockchain consensus algorithms (e.g., Proof of Authority, Practical Byzantine Fault Tolerance, among others).

Permissioned MDLs have different technical and governance models for achieving consensus. The choice of mechanism will depend on the deployment of MDLs and the number of active users:

- Regulated environments demand a 'user of last resort'. This entity would maintain a current copy of the MDL and contracts so that it can be rebroadcast if necessary

- A single central party could have the right to validate and update the MDL, though it is more likely that governance would require some full participants based on selection of MDL technology in the first place

- A voting system can be established allowing users to decide on the correct version of the MDL. This requires either unanimity or a threshold number of participants.

Public MDLs are 'permissionless' ledgers. Crypto-currencies typically run on public MDLs. Public MDLs are designed to eliminate third parties in transactions by setting up peer-to-peer networks. Examples include Bitcoin, Ethereum, Monero, Dash, Litecoin, and Dogecoin.

Private MDLs are permissioned commercial MDL networks, established to serve the needs of businesses. Private MDLs are by definition 'permissioned'. The parties conducting the transactions involved must disclose their identity. MONAX, Multichain, the Hyperledger project from the Linux Foundation, R3CEV's Corda, and

the Gem Health network are examples of private blockchain projects under development.

MDLs typically employ some type of digital token that effects a value-exchange protocol, which uniquely compels offer and acceptance[1]. Token ownership is manifested by records of unspent tokens in a file called a *wallet*. As will be detailed in this paper, wallets are a key security vulnerability for mutual distributed ledger systems.

Mutual Distributed Ledger Security Vulnerabilities

- 51% Attack - a mining pool that controls 51% of an MDLs mining power can hard fork at will, potentially appending false transactions to the main chain of blocks

- Selfish Mining Attack – as described by [Eyal and Sirer, 2013], this attack requires just 33% of the total mining power

A quick look at the mining power of the major mining pools, Figure 2, suggests that two large pools could potentially collude to launch a successful selfish mining attack.

As there is no governance of the Bitcoin MDL, these malicious mining attacks appear to be quite possible and most likely make the Bitcoin consensus protocol unusable for an industrial application.

[1] It is important to note that a crypto-token is not necessary for an MDL. Indeed, the smart contract company Adjoint has implemented commercial-grade private mutual distributed ledger software (Uplink) that is without any underlying cryptocurrency and is absent miners. See interview with Somil Goyal, the COO, in Section 4 below.

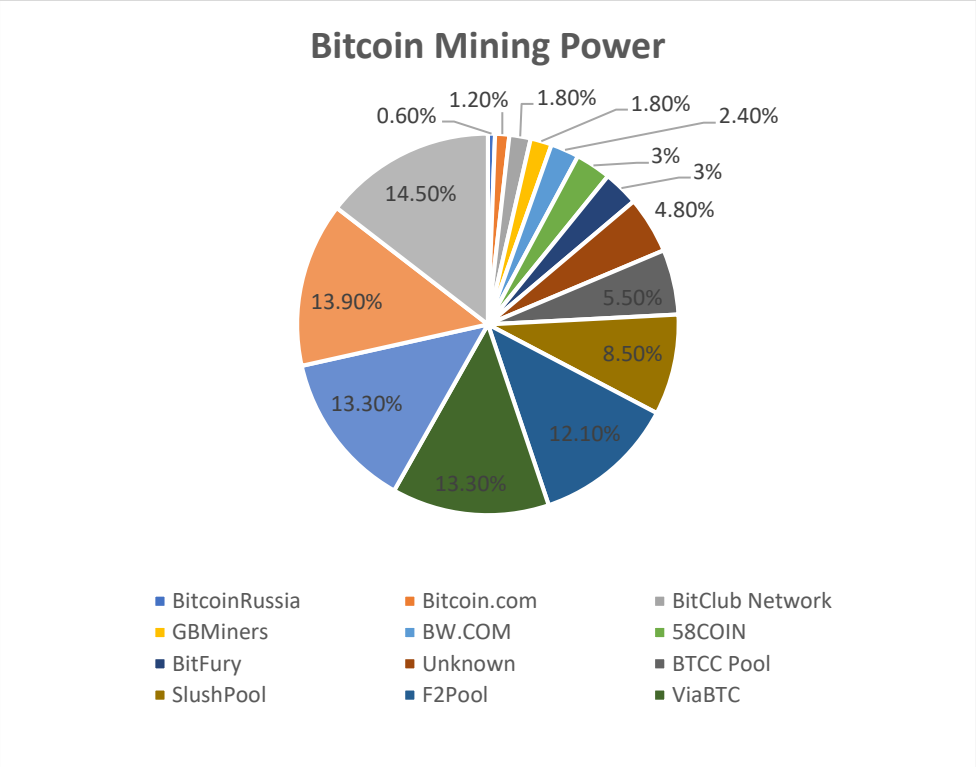


Figure 2 Bitcoin mining pool hashing power. It is apparent that the largest pools could potentially form partnerships that could accumulate sufficient mining power to selfish mine a MDL. (Taken from https://blockchain.info/pools?timespan=24hours , Dec 9)

Bitcoin is the transaction token (miners receive newly created Bitcoin upon appending a block) as well as the medium of value exchange between counterparties in a transaction. Subsequent to the release of the Bitcoin MDL, others have come into use (each with a token, a so-called cryptocurrency). Coinmarketcap.com reports there are now 1,424 cryptocurrencies. Each MDL may be employed for peer to peer payments (and token speculation) or for business process purposes. So-called *smart contracts* are software protocols that facilitate negotiation and performance of business contracts. Some MDLs are more suited for hosting smart contracts, whereas others are more appropriate for peer to peer payments (e.g., Bitcoin).

There is a vast body of ongoing academic research on the security vulnerabilities of the different MDL architectures[2].

[2] The catalog of possible attacks is much larger than the 51% and Selfish Mining attack strategies. See for example [Gervais, et. al., 2016], [Baliga 2017] , [Conti, et. al., 2017], [Eyal and Sirer, 2013], [Hacken 2017], [Yongxing 2014], and [Zheng, et. al., 2016].

Table 1- Recent Crpto-Blockchain Data Breaches, 2017-2018

Blockchain	Month of Breach	Description of Breach
Youbit	April	A hack of the South Korean cryptocurrency exchange stole 3,100 Bitcoin.
Parity (Ethereum client)	July	A hacker exploited a software bug in the Ethereum smart contract software code to irrevocably steal $31 million of ether crypto-tokens.
BTC-e	July	Principals were arrested for alleged money laundering. The U.S. Department of Justice shut down the exchange.
Parity (Ethereum client)	November	A security vulnerability due to a smart contract software bug froze $150 million of ether crypto-tokens.
NiceHash	December	Hackers took control of Bitcoin wallets at NiceHash mining marketplace to abscond $60 million in Bitcoin.
Youbit	December	A hack of the South Korean cryptocurrency exchange stole 17% of the exchanges assets, forcing it into bankruptcy.
CoinCheck	January 2018	A hack of the Tokyo-based exchange stole $533 million worth of NEM crypto-tokens.

What is the bottom line of these research endeavours? One takeaway is that it certainly is conceivable there are shadow alliances of mining pools that have the mining power to hard-fork and double-spend tokens at will. Despite this fact, there has been no documented instances of such activity. Indeed, the documented forks on the Bitcoin and Ethereum MDLs have mostly been planned and peer-reviewed by their respective open developer forums. The high-profile MDL related data breaches in the past year (see Table 1) show that they are not due to fundamental weaknesses in the MDL peer-to-peer consensus architecture – they are mostly due to traditional software hacking activities. Phishing MDL related websites (i.e., stealing credentials from careless employees and exploitation of vulnerabilities in poorly tested software) is the typical cause of the breaches in the table. It is worth

mentioning that each economic loss in Table 1 exceeds the $3.6 million average loss due to industrial data breaches, as reported by IBM Security ([IBM 2017]).

Hence, despite the academic focus on the security weaknesses of various MDLs, the data breaches that have been documented are the type of breaches that, also, befall other software that connected to the Internet.

The conclusion one may draw is that any commercial application of MDL technology must employ best practice software development and information security practices

The MDL Miner Conundrum

- Aggressively pursue honest mining and collect steady revenue stream from block appending rewards. Currently, upon appending a block, a miner receives 12.5 Bitcoin (equivalent to £100,000).

- A miner may also supplement her revenue with malicious mining pursuits to effect, for example, double spending. This supplemental income has lower expected return with a large uncertainty. See Ref. [Hacken 2017].

- A typical mining computer costs £3,500 - £11,000. After making such large investments in dedicated mining hardware (plus the ongoing electricity costs) most rational mining pool owners would choose to mine honestly to collect the steady income.

Very recently, Intel disclosed two hardware flaws (so-called Meltdown and Spectre) affecting all Intel, ARM and AMD processors[3]. The flaws allow external software processes to surreptitiously read data from an effected computer. Intel announced that it is working on a software patch that will result in a 30% performance reduction on patched CPU's. This flaw would allow a malicious actor to steal private keys from a MDL node or from a cryptocurrency exchange. As many exchanges employ Cloud services to store keys (*e.g.*, Amazon Web Services) and these services

[3] See [Peaster 2018], [Hertig, 2018], [Kovacs, 2018].

are hosted on servers with this hardware bug, potentially many crypto-exchanges are at risk. On the other hand, initial indications are that the flaw will have immaterial impact on MDL mining.

2. Cryptocurrency Liquidity And Market Risk Factors

- Cryptocurrency is an extremely illiquid asset class – it is two orders of magnitude more illiquid than equities. It is a classic example of a liquidity black hole.

- The illiquidity is caused by crypto-exchange failures, large-scale hoarding of crypto-tokens by a few large investors, and the immaturity of the crypto-exchange market

- Cryptocurrency will be shunned by money-centre banks due to excessive VaR-based economic capital requirements

- Until cryptocurrency volatility dramatically declines, it is doubtful cryptos will gain a large footprint in commerce

If an investor owned a share of the FTSE 100 Index ETF at the beginning of 2017, she might have sold it near the end of the year to capture a quite respectable 40% return. On the other hand, had she converted her single Bitcoin into pound sterling, she would have been the proud recipient of a 1,400% return. As a rational investor, her personal assessment of these investment returns must consider the relative risks involved. The previous section of this paper discussed some of the so-called operational risks of cryptocurrency speculation (e.g., malicious mining, fraud due to wallet hacking, etc.). By employing simple econometric metrics, this section describes the liquidity risks involved in cryptocurrency investing. The focus is on the Bitcoin market, as it has the largest market capitalisation. A description of cryptocurrency market risks will follow the liquidity risk discussion.

Figure 3 previews the liquidity conclusions. It shows the historical annual rates of returns of various asset types versus a subjective illiquidity measure. Along the horizontal axis, it is clear that government bonds, which can be easily purchased from one's online brokerage account, are much more liquid than highly privatised investments in venture capital funds. It is apparent from the figure that more illiquid assets historically realise higher returns. Given the outsized returns of the crypto-markets, this figure foretells the conclusion that cryptos are quite illiquid. It turns out that high market risk piggy-backs this crypto-illiquidity. These challenges

will limit large-scale adoption of cryptos by vendors for payments. Nevertheless, they are a compelling asset for speculation.

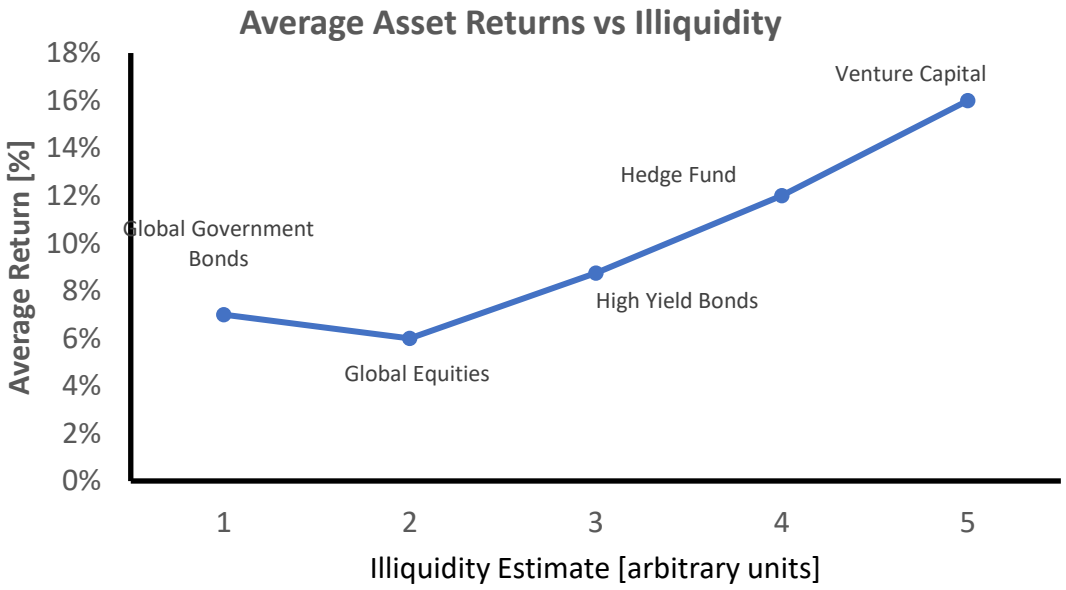


Figure 3 Measured average asset returns, 1990-2009, versus a subjective illiquidity estimate. The trend of increasing return with increasing illiquidity points to extreme illiquidity in the cryptocurrency markets. From [Schroders 2015].

A. The Crypto-Market's Liquidity Risk

What Is Asset Liquidity?

- An asset is said to be liquid if one may transact it without materially impacting its prevailing market price
- We expect the rate of return for illiquid assets to exceed the rate of return for liquid assets (recall Figure 3). The rationale is that an investor must be compensated for taking on liquidity (i.e., transaction) costs in an illiquid asset.
- Given the outlandishly high crypto-returns we expect to measure low levels of liquidity (conversely, high illiquidity) in this market

A business person making an assessment of cryptocurrency participation cares about liquidity because the liquidity level impacts the rate of return. One expects the rate of return for illiquid assets to exceed the rate of return for liquid assets (recall Figure 3). The rationale is that an investor must be compensated for taking on liquidity (i.e., transaction) costs in an illiquid asset. Given the Bitcoin market has experienced outlandishly high returns, one expects to measure low levels of liquidity in this market.

The Index Of Martin

The so-called *Index of Martin* is a convenient metric that allows for comparison of liquidity levels of different classes of assets. It is convenient because it is dependent on easily accessed market observables (namely, price and volume) and it provides a measure of market impact, which is the key to accessing liquidity. The Index of Martin measures price dispersion per unit of transaction. Hence, a higher Index of Martin value corresponds to a greater price impact, which is the hallmark of a lower liquidity asset[4]. Conversely, an asset with a small value of the Index of Martin is more liquid.

In order to study Bitcoin liquidity with the Index of Martin, this study calculates it for major (by daily volume) exchanges for the foreign exchange rate pairs $\frac{USD}{BTC}$, $\frac{GBP}{BTC}$ and $\frac{EUR}{BTC}$ for the calendar years 2015, 2016, and (most of) 2017. By graphically comparing the Bitcoin Indices of Martin to that of large-cap Sterling, Euro, and Dollar equity ETFs (which are assumed to be very liquid), it is possible to dramatically assess the crypto-liquidity level. The study leverages and extends the work of [Loi 2017], whose data sample stopped in 2015. The present sample spans

[4] Martin (1975) proposes a liquidity index (MLI) given an assumption that a stationary distribution of price changes hold through the entire transaction time. A high value of MLI indicates less liquidity of a stock. The higher value of the ratio means the larger price dispersion corresponding to the traded volume.

$$MLI_{date\ window} = \sum_{i=1}^{N_{window}} \frac{(P_i - p_{i-1})^2}{V_i}$$

where P_i is the date-t closing price and V_i is the 24-hour volume of the asset. Since Bitcoin exchanges operate 24/7, by convention the trading day runs 0GMT – 24GMT.

1 January 2015 – 20 December 2017, which allows examination of the period of hyper-volatility in the final quarter of 2017 in the Bitcoin market.

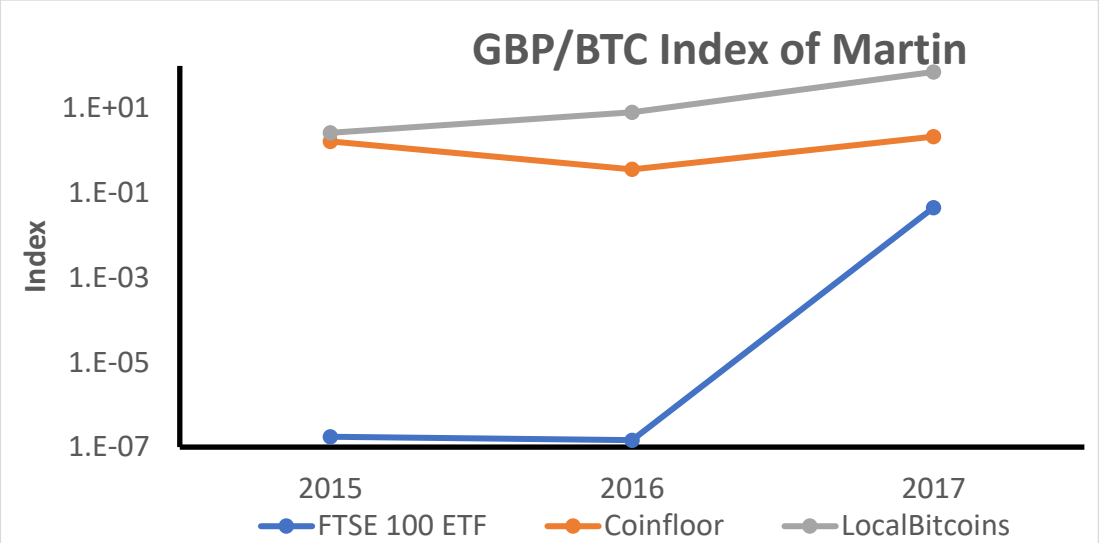


Figure 4 The Index of Martin plotted for the calendar years 2015 – 2017, with trend lines, for the GBP/BTC exchange rate as traded on the Coinfloor and LocalBitcoins exchanges. The plot compares these Bitcoin Martin Indices to that of a very liquid large-cap FTSE-100 equity index ETF (iShares Core FTSE100 ETF). A larger value of the Index of Martin represents illiquidity. It is apparent Bitcoin is 2 – 7 orders of magnitude more illiquid than the GBP equity market.

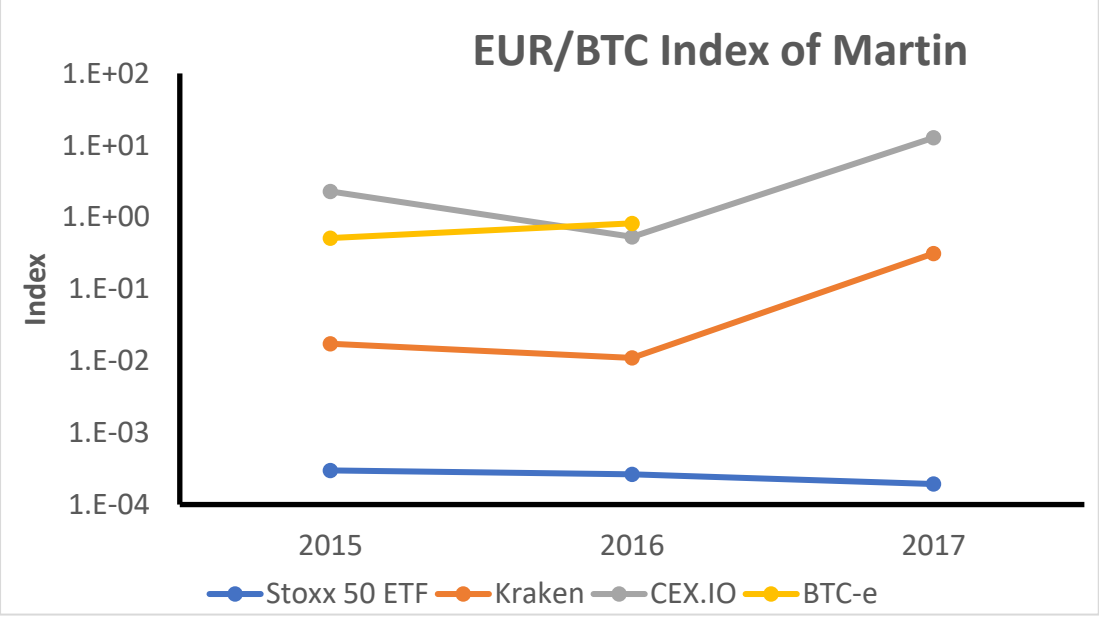


Figure 5 The Index of Martin plotted for the calendar years 2015 – 2017, with trend lines, for the EUR/BTC exchange rate as traded on the Kraken and CEX.IO exchanges. The plot compares these Bitcoin Martin Indices to that of a very liquid large-cap STOXX-50 equity index ETF (iShares Euro Stoxx 50 ETF). A larger value of the Index of Martin represents illiquidity. It is apparent Bitcoin is 2 – 3 orders of magnitude more illiquid than the Euro equity market. The failed BTC-e exchange is also shown to demonstrate how extreme selling pressure (due to absent AML/KYC policies) can make a lightly regulated exchange just as illiquid as the popular CEX.IO crypto-exchange.

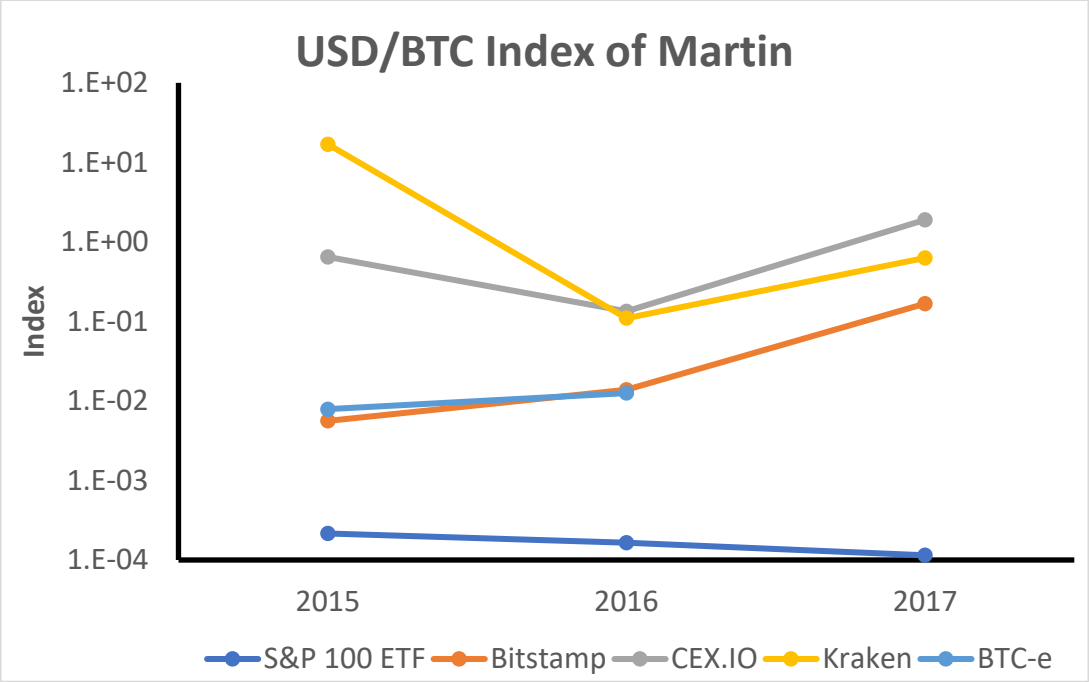


Figure 6 The Index of Martin plotted for the calendar years 2015 – 2017, with trend lines, for the USD/BTC exchange rate as traded on the Bitstamp, CEX.IO and Kraken exchanges. The plot compares these Bitcoin Martin Indices to that of a very liquid large-cap S&P100 equity index ETF (iShares S&P100 ETF). A larger value of the Index of Martin represents illiquidity. It is apparent Bitcoin is 2 – 3 orders of magnitude more illiquid than the Euro equity market. The failed BTC-e exchange is also shown to demonstrate how extreme selling pressure (due to absent AML/KYC policies) can make a lightly regulated exchange just as illiquid as the popular Bitstamp crypto-exchange.

The Indices of Martin for the GBP/BTC, EUR/BTC, and USD/BTC markets are plotted in Figures 4 to 6. Each plot shows the Index of Martin calculated for three calendar years for the Bitcoin exchange rate at different trading venues. An exchange with high daily volume and an exchange with moderate daily volume are shown. On each plot the benchmark liquidity Index of Martin is represented by that for a very liquid large-cap equity index ETF (exchange traded fund). The equity ETF represents a very liquid market that level-sets the Martin indices calculated for the Bitcoin markets. Recall that the smaller the Index of Martin, the more liquid the market.

The data sample includes major exchanges (Bitstamp, CEX.IO, Kraken, Coinfloor, LocalBitcoins), which are all domiciled in G10 countries and have some level of KYC/AML[5] compliance, as well as at least a modicum of transparency. The operational risk profile of these exchanges is relatively lower than that of most crypto-trading venues. These exchanges are compared to (for the USD/BTC and EUR/BTC markets, Figure 5 and Figure 6) the BTC-e exchange for the calendar years

[5] There is a robust body of regulation covering the principles of Know Your Customer (KYC) and Anti-Money Laundering (AML) in G10 countries.

2015 and 2016. In July 2017, BTC-e was shut down by the US Department of Justice and arrest warrants were issued for the exchange's principals – hence it is not possible to calculate a 2017 entire-year Index of Martin for BTC-e. This exchange had extremely light KYC/AML policies, as well as enhanced trader anonymity features. Hence, this exchange was potentially more attractive to users desiring to convert illicitly obtained cryptocurrency into fiat currency. One would expect that lower KYC/AML policies would result in a higher operational risk profile for the trading venue, and, therefore, lower liquidity. [Kroeger and Sarkar, 2017] measured this effect and found the enhanced anonymity actually created large selling pressure that kept the exchange rates systematically lower than what was traded on other exchanges.

What Does The Index Of Martin Tell Us (Figure 4 – Figure 6)?

- The Bitcoin markets are all at least two orders of magnitude more illiquid than the large-cap equity market ETFs. This would help explain the outsized returns (due to the illiquidity premium) observed in the Bitcoin markets.
- Bitcoin illiquidity increased at least an order of magnitude from 2016 to 2017. Again, this illiquidity uptick contributed to the massive Q4 2017 returns observed in the Bitcoin markets.
- There are material liquidity gaps between the different crypto-trading venues

B. So What's Creating Crypto Illiquidity?

- Crypto trading and its conversion to fiat currencies is promulgated on lightly regulated trading venues that have shallow capitalisation and, therefore, high default risk

- The high failure rate of crypto-exchanges (due to operational failures and software hacks) vastly increases their illiquidity relative to conventional assets

- The diversity of the transaction fee structures and anonymity rules create intra crypto-exchange liquidity gaps

- Diverse order matching search frictions create liquidity gaps between crypto-exchanges and between cryptos and liquid fiat-denominated assets

- Crypto-hoarding increases their illiquidity

- The homogeneous incentives of the large crypto-hoarders and miners creates liquidity black holes in the cryptocurrency economy

Given the very large liquidity differences between the equity and Bitcoin markets, it is apparent there are material systematic differences between the two markets that are driving these liquidity gaps. There are obvious differences: the exchange-traded equity markets are highly regulated and have centralised exchanges where only well-capitalised members (who each contribute to a mutualised default protection fund at the exchange) may participate. These members are linked to brokers, who in turn are linked to institutional and retail clients. Throughout this relationship chain there are AML/KYC[6] rules that enhance transparency. The Bitcoin market is without this infrastructure and regulatory framework – it is essentially broker-less, with trading effected on lightly regulated exchanges with shallow capitalisation.

The sizable intra-exchange liquidity differences (e.g., Coinfloor and LocalBitcoins in Figure 4, Kraken and CEX.IO in Figure 5, Bitstamp and CEX.IO in Figure 6), can produce material price differences between exchanges, thereby creating classical intra-exchange arbitrage opportunities. [Kroeger and Sarkar, 2017] performed a detailed empirical study of persistent price differences (which reflect intra-exchange liquidity differences) on USD/BTC exchanges and identified the following key components of intra-exchange liquidity gaps: bid/ask spread, order book

[6] Anti-Money Laundering (AML) and Know Your Counterparty (KYC) rules compel financial counterparties to undergo due-diligence checks on each other.

depth, exchange rate volatility (per the classical economic theories), diverse exchange fees for participants, heterogeneous exchange anonymity rules and the perceived probability of the failure of a trading venue (see Figure 7).

Also note that arbitrage between exchanges is not instantaneous - typically exchanges require at least three Bitcoin MDL confirmations (~30 minutes) to accept a transaction as final[7]. In addition, withdrawals in fiat currency may require 3 to 7 business days to settle. Similarly, deposits effected via wire transfers may require 5 to 10 business days to settle. Transactions are highly exposed to exchange rate volatility during these settlement periods, thereby creating an additional intra-exchange liquidity gap.

It is interesting that [Kroeger and Sarkar, 2017] report that BTC-e, an exchange whose domicile and ownership structure is publicly unknown and has enhanced anonymity relative to other exchanges, had USD/BTC exchange rates persistently 1%-2% lower than other exchanges[8]. The authors posit this exchange had higher sell pressure (and, therefore, lower exchange rates) due to elevated levels of conversions of illicitly gained Bitcoin into fiat currency. Finally, different search frictions on the various exchanges contribute short term intra-exchange liquidity differences[9].

Crypto Hoarding Also Contributes To Illiquidity

It has been observed there is significant hoarding among Bitcoin investors. The U.S. Securities and Exchange Commission (SEC) estimates that 98% of Bitcoin is hoarded or out of circulation, with over 50% controlled by just 1000 individuals [SEC 2016]. [Badev and Chen 2014] estimates less than 50% of all bitcoins in circulation are used in transactions. Recall that the crypto market is without brokers. Hence, market participants trade directly peer-to-peer. Foreign exchange transactions occur directly between a trader's crypto-wallet and an exchange.

[7] This 'wait and see' approach is common – the idea is the probability of a hard fork deserting a block diminishes as blocks are appended to the main blockchain. See [Gervais, et. al., 2016] and [Rosenfeld 2014] for quantitative analysis of this wait and see strategy.

[8] The maximum observed price difference was 41% between Bitstamp and BTC-e.

[9] Search friction refers to the exchange activity that identifies matching orders. These frictions delay trade execution.

To some extent, crypto-market participants are encouraged to hoard due to the tax treatment of cryptocurrency, as well as the fact that few vendors accept crypto-tokens for payments.

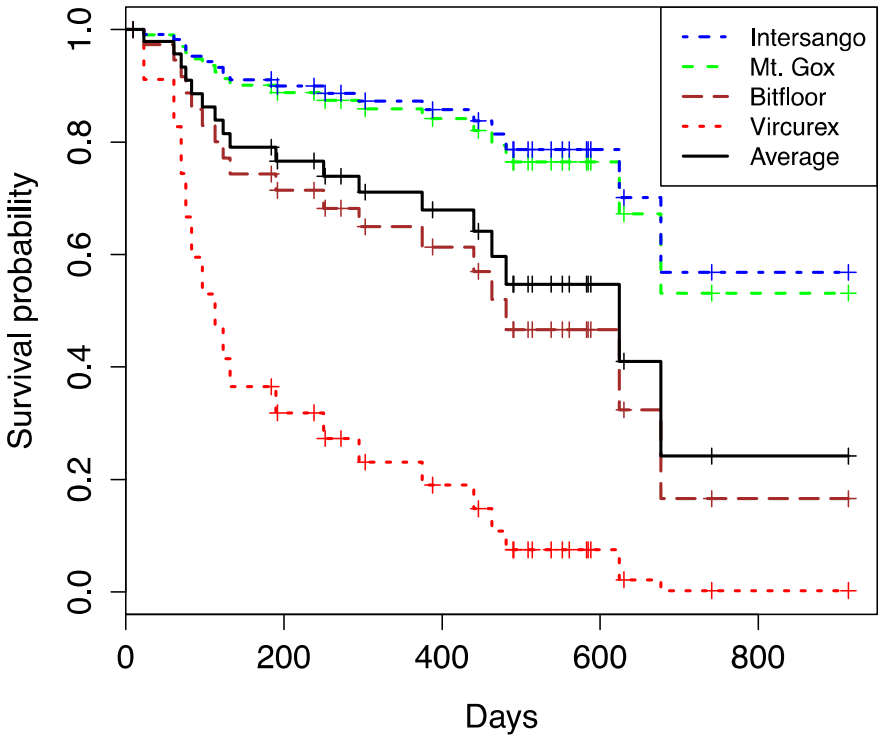


Figure 7 Empirically calculated survival probability functions for a sample of Bitcoin exchanges. It is apparent from the plot there is just a 25% probability, on average, that a Bitcoin exchange will last 700 days. This low survival probability contributes to crypto-illiquidity. From [Moore and Christin, 2013].

Another potential reason for hoarding is the material probability that a given cryptocurrency exchange will fail. There have been many documented crypto-exchange failures, including the largest, Mt. Gox, and the most recent, Youbit and CoinCheck. [Moore and Christin, 2013] empirically estimated the survival probability (i.e., the probability that an exchange does not fail) of a sample of Bitcoin exchanges and obtained measurable differences between the exchanges. Figure 7 is their result. Per their study, the average Bitcoin exchange will survive 700 days of existence less than 30% of the time. Per the figure, the different exchanges have materially different survival probabilities. [Kroeger and Sarkar, 2017] identified this intra-exchange failure probability as a component of the intra-exchange liquidity differences.

The statement about high levels of hoarding in the Bitcoin market aligns with a recent econometric study about the fundamental economic drivers of Bitcoin foreign exchange rates. [Dimpfl 2017] identifies adverse selection as a key driver. Adverse selection is private information that allows the owners of the information to control order flow and hence liquidity. The pseudo-anonymity of the Bitcoin ecosystem certainly allows for the easy flow of private information, perhaps between investors and mining pools.

The Crypto-Liquidity Black Hole

- Per [Mainelli 2007], to say that an asset market resides in a liquidity black hole that means there is a positive feedback between trading and asset price – an increase in price causes more purchases whereas price reductions cause more sales
- Homogeneity of the incentives of the few large crypto-market participants (hoarders and miners) breads this illiquidity

The above details the liquidity risk of the cryptocurrency market. Liquidity risk is characterised by the level of price impact in a market as well as the likelihood of a seller not finding a matched buyer. This study finds that compared to the overall equity market, the liquidity risk of the Bitcoin market is quite high. Traders are rewarded for assuming this risk with high (volatile) returns.

In light of the arid crypto-liquidity landscape, what can be said about its market risk profile?

C. Crypto Market Risk Factors

- The extreme Value at Risk levels of cryptocurrencies create economic capital barriers that diminish their value proposition for money-centre banks

- The hyper-volatility of cryptocurrencies coupled with the immature market in hedging instruments (i.e., crypto-options) will impede its adoption as a medium of exchange by vendors and its adoption as a value-adding asset class by professional asset managers

Investors also monitor an asset's market risk. Market risk is the sensitivity of the value of the asset to changes in the market, as evidenced by equity levels, interest rates, exchange rates, historical returns, etc. Standard measures of market risk (as adopted by trading desks and financial regulators) include volatility, Value at Risk[10] and Expected Shortfall[11]. [Osterrieder and Lorenz, 2016], [Chan, et. al. 2017] and [Stavroyiannis 2017] provide VaR estimates of major cryptocurrencies.

Table 2 Annualised volatility of BTC/USD and G10 exchange rates measured over the time period Sept 2013-Sept 2016. Bitcoin volatility outstrips the fiat volatility, indicating it's unlikely a regulated bank will have large crypto-holdings due to excessive economic capital requirements. From [Osterrieder and Lorenz, 2016].

Exchange rate	Annualized Volatility
Bitcoin/USD	77%
AUD/USD	11%
CAD/USD	8%
CHF/USD	14%
EUR/USD	9%
GBP/USD	10%
JPY/USD	10%
NOK/USD	12%
NZD/USD	11%
SEK/USD	10%

Table 2 shows the annualised volatility reported in [Osterrieder and Lorenz, 2016] for the BTC/USD and nine other G10 fiat currency exchange rates. The Bitcoin volatility is 6-7 times that of the fiat exchange rates. High Bitcoin volatility leads to high Bitcoin VaR - [Osterrieder and Lorenz, 2016] observed it is five times that measured for the G10 currencies.

[Osterrieder and Lorenz, 2016] state the summary Bitcoin market risk result as

[10] Value at Risk (VaR) is defined as the potential loss of an asset over a given time period (the liquidity horizon) at a given confidence level. As an example, if an asset's three-day VaR at 99% confidence level is £1M, there is only a 1% probability the asset's value will decline by more than this amount over the three-day liquidity horizon.

[11] Expected Shortfall is an alternative to VaR for measuring market risk. It is more sensitive to extremely rare loss events. The paper does not wish to focus on this metric but only mentions it for the sake of completeness.

follows:

> *"Using the traditional tail-risk measures value-at-risk and expected shortfall, we could quantify that extreme events lead to losses in Bitcoin which are about eight times higher than what we can expect from the G10 currencies. Once every 20 days you should expect a loss of about 10% on average."*

This volatile market risk profile diminishes cryptocurrencies' value proposition as an investment asset for large money-centre banks. These banks are compelled to comply with international capital adequacy rules established by the Basel Committee on Banking Supervision. The high Bitcoin VaR levels would compel a hypothetical cryptocurrency business unit within an institution to maintain significantly larger economic capital buffers. These buffers are designed to make an institution robust with respect to extreme investment losses.

What Is the Impact Of The Large Crypto-Volatility?

Professional portfolio managers combine high and low volatility assets to create investments with customisable levels of risk and return – many funds employ some version of the Markowitz minimum variance portfolio optimization methodology to structure such portfolios[12]. Hence, it stands to reason that a hyper-volatile cryptocurrency exchange rate might be an excellent addition to a portfolio with more mundane assets (like highly liquid stocks). In fact, there has been some academic work along this vein, and these works demonstrate significant increase in returns for portfolios that include a crypto-allocation[13]. These works do not fully model the considerable crypto-transaction costs – these costs would diminish the modelled returns. Nevertheless, these papers demonstrate cryptocurrencies have considerable potential to be a return-boosting component of managed investment portfolios. Indeed, the new crypto-futures contracts being introduced by mainstream exchanges may certainly be employed as proxies for cryptocurrency volatility exposure.

Institutional investors customarily employ an active hedging program to mitigate market risk. Such a program entails taking positions in financial derivatives to

[12] The Nobel Prize modern portfolio theory treatise is Ref. [Markowitz 1952].
[13] See Refs. [Beck 2016], [Klabbers 2017], [Trimborn 2017].

mitigate market risk exposure. The crypto-derivative market is quite immature and hence, there are few liquid hedging tools currently available[14]. Given the scarcity of hedging tools in the crypto-space and the outrageous market risks, it is doubtful that any financial institution will pursue a material investment program.

Finally, the extreme volatility of crypto exchange rates dissuades vendors from transacting in them. Consider the simple example where a vendor waits for a number of Bitcoin MDL confirmations (typically vendors wait for six confirmations, which equates to an hour) to accept a transaction as final. The exchange rate can change dramatically in an hour, meaning the vendor may lose fiat value. Until crypto volatility dramatically declines, it is doubtful cryptos will gain a large footprint in commercial payment systems.

Snap, Crackle, Illiquidity Pop!

- There is evidence of crypto-exchange hacking activity causing intra-exchange illiquidity 'pops'
- Illiquidity pops are correlated with dramatic changes in crypto-exchange rates
- The recent equity market decline occurs as there is moderate to high correlation between crypto-exchange rates and equity indexes

The Index of Martin analysis above employed whole-year estimations of the Index.

[14] The Chicago Mercantile Exchange trades Bitcoin futures. See Table 3 for a list of exchange-traded crypto-options.

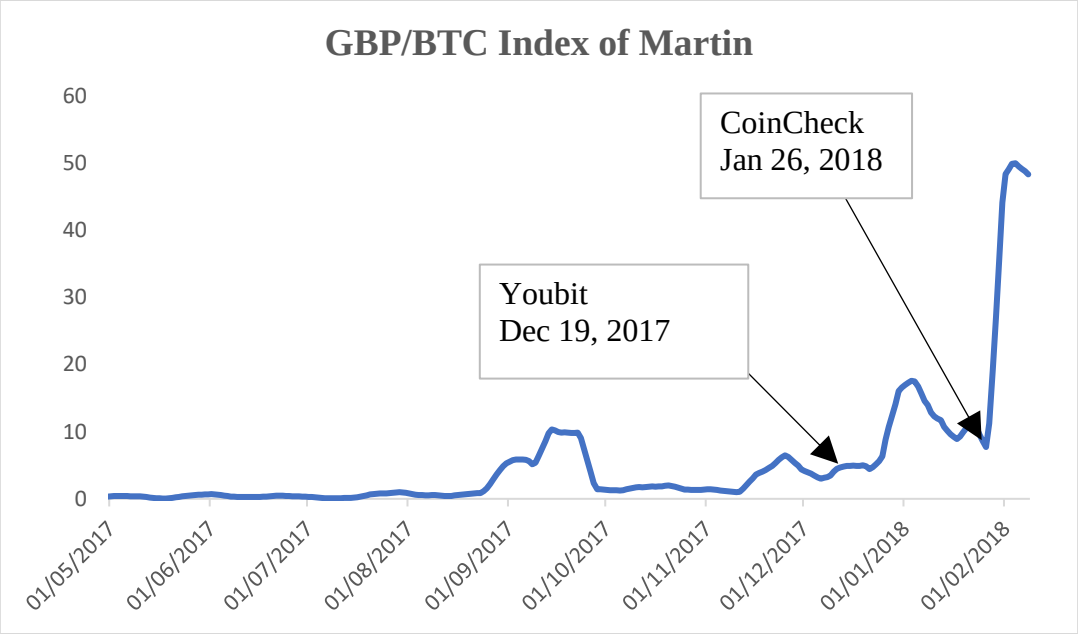


Figure 8 Index of Martin for the GBP/BTC exchange rate (LocalBitcoins trading venue), calculated using 14-day rolling windows. The figure suggests the Dec 2017 Youbit hack was soon followed by an illiquidity pop. Similarly, the CoinCheck hack appears to have been soon followed by a dramatic illiquidity pop.

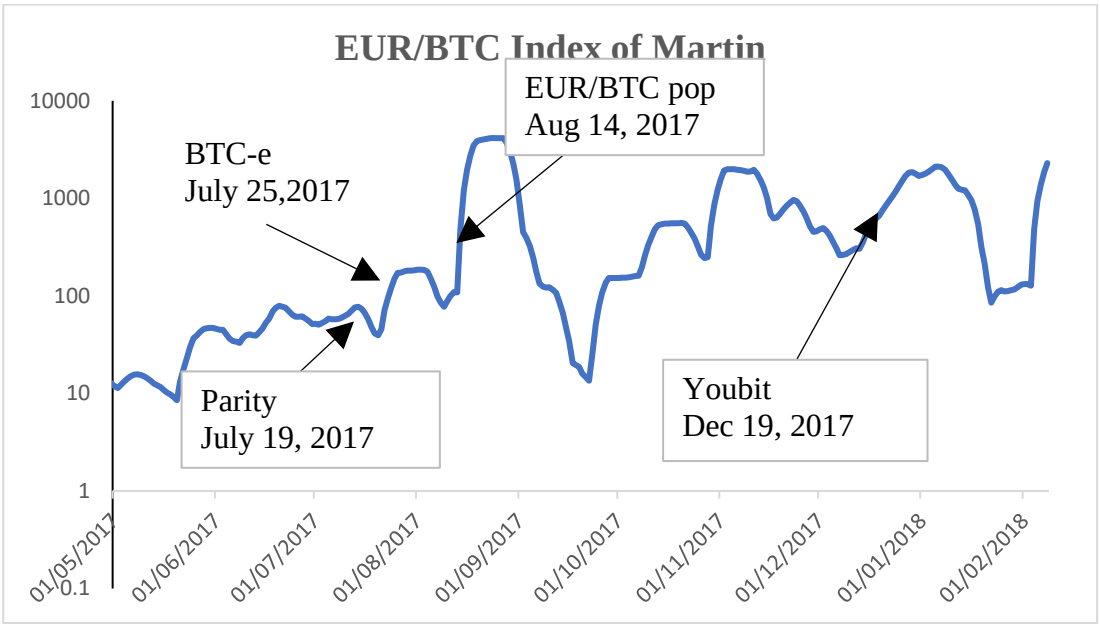


Figure 9 Index of Martin for the EUR/BTC exchange rate (LocalBitcoins trading venue), calculated using 14-day rolling windows. The figure suggests connections between the Parity hack, the BTC-e shutdown and the Youbit hack and illiquidity pops in this rate. Similarly the dramatic short-term increase in the exchange rate that occurred Aug 14, 2017 occurred during an order-of-magnitude illiquidity pop.

The Index of Martin analysis in Section A above employed whole-year estimations of the Index. By employing 14-day rolling window estimations of the Index, one obtains more granular liquidity information. The current study employed this

methodology to assess changes in the liquidity of the GBP/BTC (Figure 8) and EUR/BTC (Figure 9) exchange rates on the LocalBitcoins crypto-trading venue[15]. As shown, hacks that occur on other exchanges and MDLs (e.g., the Ethereum Parity MDL) are associated with sizeable increases in the illiquidity on LocalBitcoin (recall higher Index of Martin means higher illiquidity) exchange.

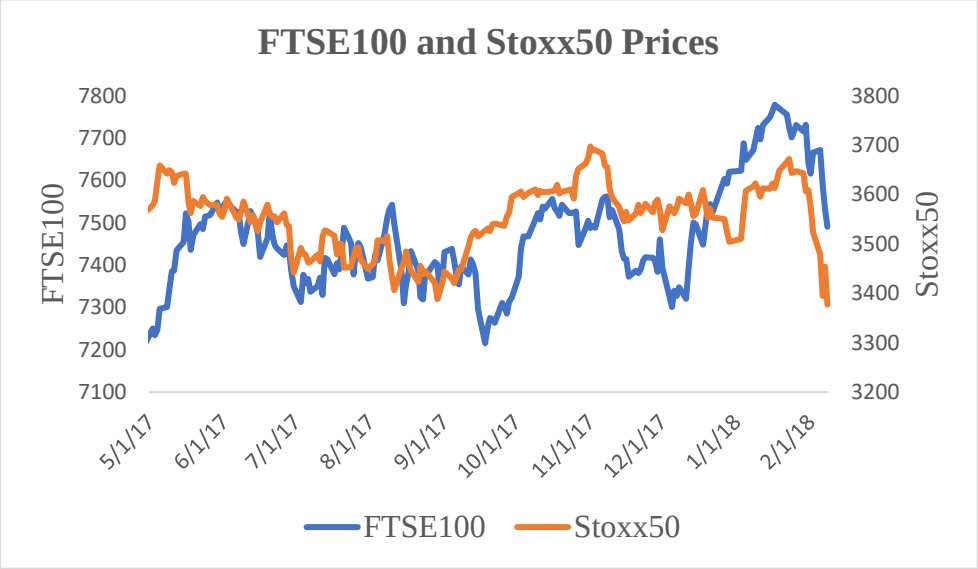


Figure 10 FTSE100 and Stoxx50 equity indexes for 2017.

The recent declines in the equity markets over Jan-Feb 2018 are indicated in Figure 10 for the FTSE100 and Stoxx50 equity indexes. The large declines in the equity markets occur alongside large declines in the corresponding Bitcoin exchange rates on the LocalBitcoins exchange, see Figure 11. The long-term correlation between Bitcoin exchange rates and the equity markets is near-zero[16]. Nevertheless, correlation over a two-week window near 29 January, 2018 (when the sharp decline started) increased to 52% for GBP/BTC and 19% for EUR/BTC. Although this does not suggest a causative connection, it does manifest short-term association between the equity and crypto-markets.

[15] LocalBitcoins is slightly different from most crypto-exchanges. It is an Over the Counter market. This technical difference does not impact the conclusions in this section.

[16] In fact, the one-year correlation between the FTSE100 index and the GBP/BTC exchange rate is 6%. Likewise, the one-year correlation between the Stoxx50 index and the EUR/BTC index is -6%.

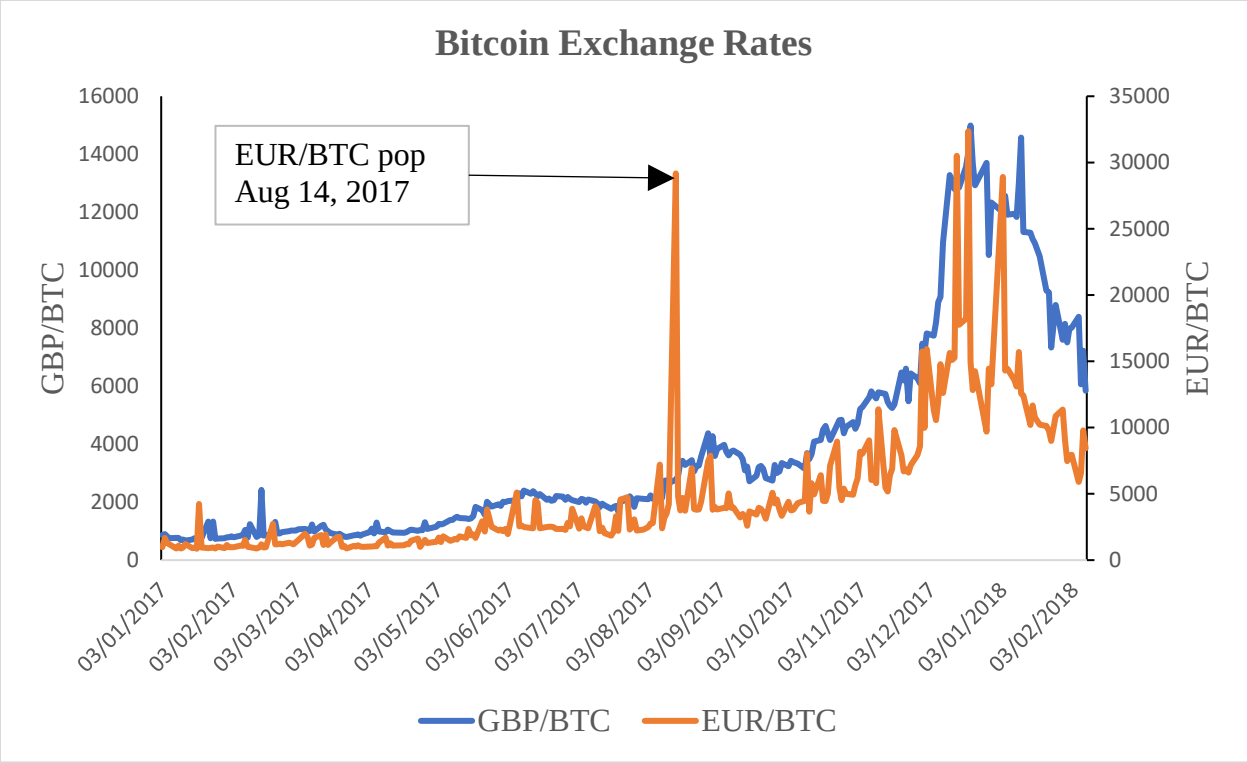


Figure 11 GBP/BTC and EUR/BTC exchange rates over the past year (LocalBitcoins trading venue). The dramatic increase in the EUR/BTC exchange rate occurred with an illiquidity pop, as evidenced by the EUR/BTC Index of Martin (see Fig 9). Post Jan 29, 2018 both rates are falling as is the equity market (see Fig 10). These recent market declines evidence moderate to high positive correlation between these exchange rates and the equity market.

Recalling Figure 3, one would expect an illiquidity pop to be associated with a sizeable change in a crypto-exchange rate. Figure 9 (the Index of Martin for EUR/BTC) and Figure 11 (the EUR/BTC exchange rate) evidence this correspondence – the dramatic increase in the EUR/BTC rate on Aug 14, 2017 occurred during an illiquidity pop.

It is apparent that the Index of Martin may be a useful liquidity monitoring metric for the cryptocurrency exchanges. This study has shown that it can resolve intra-exchange liquidity differences. It may also provide capture 'liquidity flow' between the various crypto-exchanges.

- The Index of Martin is a simple liquidity monitoring metric that can indicate the occurrence of 'illiquidity pops' in the cryptocurrency markets

The Liquidity And Market Risk Headline Is…

The liquidity and market risks are quite substantial in the crypto-markets. To a large extent they are not hedge-able. Hence an investor must thoughtfully assess her appetite for assuming these types of risks. The number of vendors that transact in cryptos will be small until the exchange rate volatility becomes manageable and hedge-able.

3. Smart Contracts – The Legal Risks

- ISDA standardisation of smart legal contracts will support scalability of these digital contracts, helping to cement their adoption by global investment banks

- The United Kingdom's common law system is inherently flexible enough to facilitate smart legal contracts and to quickly respond to the opportunities and challenges that they may present (including the question of enforceability)

- In the near-term, institutions are likely to adopt a hybrid contact model that combines an ink-signature on an ISDA Master Agreement with some of the operational clauses of the financial agreement being executed by the smart contract code

Cryptocurrencies are an exciting new asset that have captured speculator attention since their introduction in 2009. As detailed in Sections 1 and 2, the crypto-market is extremely illiquid and volatile and is executed on infrastructure with questionable reliability. Investors can realise outsized returns that are boosted by the illiquidity premium. Judging from the small number (< 1000) of companies that accept crypto-payments[17], it is fair to say most are not interested in cryptos *per se*. On the other hand, commercial interests, especially investment banks, have substantial interest in smart contracts, which are applications built on the blockchain-enabled distributed ledger technology. A *smart contract* is a computer protocol intended to automatically facilitate the negotiation or performance of a legal contract[18]. Figure 12 illustrates how a smart contract sits in a distributed ledger system. The smart contract reads/writes values to the ledger. In this way, it updates the state of the records stored on the ledger. Whereas some transactions/events are sourced and transmitted on-ledger, others (as indicated by the arrows) are off-ledger.

[17] See a list of companies that accept Bitcoin for payment at [Chokun 2018].

[18] See Ref. [Wikipedia 2018]. Here you will want to refer to Nick Szabo's original papers e.g. Nick Szabo, 'Smart Contracts' (1994); Nick Szabo, 'Formalizing and Securing Relationships on Public Networks,' (1 September 1997)

Work in the smart contract space is being accomplished by industry collaborations. For example, most major investment banks are participating in the R3/Corda consortium, which is investigating private/permissioned blockchains for financial applications. Many investment banks have parallel innovation programs building prototype smart contract systems that automate trade capture and post-processing. At present, smart contracts are not ready to replace paper-based legal contracts in the financial domain. Unresolved legal risk issues are an important barrier to widespread adoption of the technology. Z/Yen discussed these legal risk issues with Dr Anna Donovan, Vice Dean (Innovation) of the University College London Faculty of Laws and member of the UCL Centre for Blockchain Technologies. Her insights are summarised below.

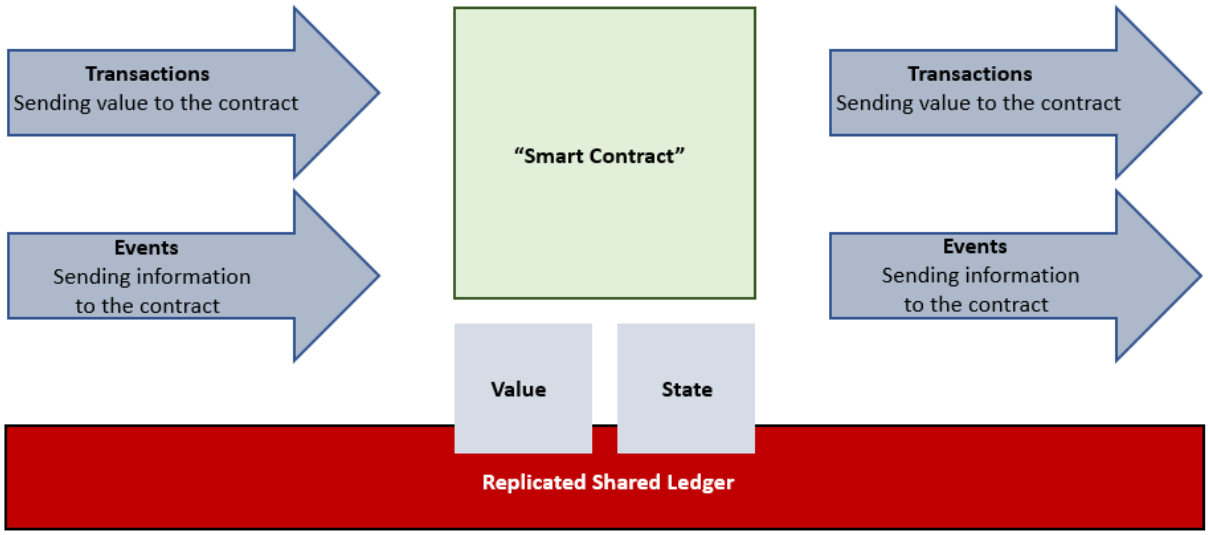


Figure 12 Schematic representation of a smart contract within a distributed ledger framework. The ledger provides a single transaction record for all participants. The smart contract automates performance of legal contract terms that update the ledger. From [Murphy, et.al., 2016]

It is helpful to illustrate some of the legal challenges that smart contracts present by reference to a concrete example, a so-called *interest rate swap*. Swaps occupy the largest share of the OTC (Over the Counter) derivative market with $381 trillion notional outstanding, which is 60% of the entire OTC derivative market[19]. A swap directs Party A to pay a fixed interest rate to party B (usually semi-annually), who pays to Party A a variable rate (customarily quarterly). It is standard practice for the

[19] See Ref. [BIS 2015].

legal contract behind every swap to follow the 2002 ISDA Master Agreement[20]. This template specifies responsibilities, payment schedules, dispute resolution, counterparty default provisions, etc. The ISDA legal construct has robustly stood the test of time in multiple jurisdictions, demonstrating the value that (quasi) standardization can bring, and cementing the importance of swaps in global finance.

As will be detailed in Section 4, despite the clear efficiencies that the current model brings in contrast to individual and bespoke negotiation, the current swap business workflow is still inefficient and expensive. Hence, there is considerable interest in replacing paper-based swap contracts with smart legal contracts that self-execute on a distributed ledger. Indeed, ISDA itself has undertaken significant research in this space.[21] So, for our hypothetical swap contract, Party A may publish a smart swap legal contract onto a blockchain. Cash flows would be automatically executed by the smart contract; hence, the smart contract code ensures perfect performance of the operational clauses of the contract as codified.

During our interview, Dr Donovan explained that the immediate benefits of smart contracts are clear; they reduce transaction costs, increase certainty through automated performance and, as a consequence, reduce the associated litigation risk and costs. However, as she went on to outline, smart legal contracts do present a number of challenges and raise several critical legal questions. For example, automated performance is not always legally final. The ISDA White Paper raises the issue of a payment being made that due to intervening events can be set-aside on insolvency grounds.[22] Beyond illegality, it is clear that circumstances may arise where practical performance does not reflect the parties' intentions. For example, goods are delivered triggering the payment obligation under the smart contract, but it transpires that the goods are not fit for purpose or of the quality expected by the receiving party. Other issues might arise if the smart contract code is either wrong or does not reflect the intentions of the parties. A high-profile example of this issue is the DAO, a digital decentralised autonomous organization. It was a venture capital fund operated entirely as a smart contract on the Ethereum

[20] ISDA (International Swaps and Derivatives Association) is a global financial derivatives industry standards-making body.

[21] See: ISDA and Linklaters, 'Whitepaper: Smart Contracts and Distributed Ledger – a Legal Perspective,' (August 2017)

[22] ISDA White Paper (n 5), 13.

blockchain. The DAO raised over $150 million in the Ether cryptocurrency. A node connected to this public blockchain utilised a provision of the code to direct $50 million worth of Ether cryptocurrency from the fund. Clearly this reallocation of DAO funds was unintended. Nevertheless, it was executed in a manner consistent with the open-source DAO smart contract code, giving rise to the question of whether the affected investors had a legal recourse?

Dr Donovan notes that the English common law is particularly well placed to respond to these challenges. Predicated on a system of precedent, the common law is able to respond quickly to developments in commercial relationships but, crucially, does so in a principled way. As a consequence, the common law is agile enough to foster the innovation that distributed ledger technologies offer, whilst protecting the reasonable expectations of the parties should issues arise. One example of this existing flexibility can be seen by considering the question of whether smart contracts are legally enforceable contracts. For an enforceable contract to be formed, English common law stipulates that four attributes must be present:

1. Offer and acceptance
2. Consideration (or value) that passes between the parties
3. Intention to create legal relations
4. Certainty/completeness of terms

Of note, is that the common law does not mandate that the contract adopt a particular format (e.g., paper-based or digital). Hence, as long as a smart legal contract demonstratively has these features, it is subject to English law, and likely to be enforceable in the U.K. Clearly, each of these requirements will require careful consideration in respect of the structure of the smart contract in question. However, the common law has consistently proven itself able to respond to developments in commercial relationships, be it a car parking ticket machine[23] or an online transaction,[24] and there is no reason why this would not continue to be the case in light of this latest technological development.

[23] Thornton v Shoe Lane Parking Ltd [1970] EWCA Civ 2

[24] Chwee Kin Keong v Digilandmall.com Pte Ltd [2005] 1 SLR(R) 502

Recall that, presently, swap contracts are based on the ISDA Master Agreement. This template is foundational to the most liquid financial market on the planet, the interest rate swap. ISDA is presently working on the next generation template for smart legal contracts, the Common Domain Model[25]. Just as adoption of the paper-based Master Agreement has facilitated global adoption of swaps for international finance, so will standardisation enable smart legal contract to gain traction in the capital markets. Standardisation will enable interoperability and scalability of the smart paradigm.

How Smart Legal Contracts Will Disrupt Paper Contracts

Dr Donovan expects that in the near-term a hybrid model smart contract will often be deployed. That is, party A and party B will both sign a traditional paper-based agreement, either with an additional clause that stipulates that the operational clauses will be executed by the related smart contract code, or that incorporates smart contract code[26]. Disputes could be addressed by off-chain arbitration or perhaps by an on-chain automated dispute resolution process. This latter approach could potentially employ the extant blockchain consensus protocols to resolve disputes. Research in this area combines the law and computer science to synthesise robust solutions[27].

At present, there is no case law that tests the enforceability of smart legal contracts *per se*. The US Securities and Exchange Commission (SEC) has promulgated several crypto-related enforcement actions[28]. In a similar vein, there is no smart contract specific law in the United Kingdom. Dr Donovan explained that the UK has, to date, adopted a "watch and wait" approach to introducing specific regulatory provisions regarding smart legal contracts -

> *"I think it's interesting that a number of jurisdictions, and the UK is a prime example of this, have been willing to say, 'we want to help foster innovation as well as protect against harm.' As such, we are seeing an approach in this*

[25] Prof. Chris Clack of the University College London Dept. of Computer Science has accomplished considerable research on this topic-see Refs. [Clack 2016], [Clack 2017], and [Clack (CDM) 2017].
[26] On this, see Clack *et al* (n 9). As an aside, the legal enforceability of digital signatures is well established by UK and EU laws and regulations. The UK Electronic Communications Act of 2000 and the EU Regulation 910/2104 affirm the authenticity of digital signatures. English common law then speaks to their validity/enforceability.
[27] Ref [CodeLegit 2017] details a prototype automated dispute resolution system.
[28] See Ref. [Naftalis, et. al., 2015].

> *jurisdiction that allows innovation to develop until the need to intervene has fully presented itself. When there is a better understanding of the potential harm that may arise with distributed ledger technologies, which may well be the case with Initial Coin Offerings for example, that is when we are likely to see greater regulatory intervention."*

So, there you have it. ISDA is working on the standardisation of smart legal contracts, computer scientists are developing natural language processing schemes that are executable on the blockchain, and attorneys/lawmakers are working within the common law framework to create (as required) new legal frameworks that cover smart legal contracts or to fully understand how the existing frameworks can accommodate this new technology. The OTC derivative industry will certainly overcome the legal challenges.

- The resulting adoption of smart legal contracts is the material business value blockchain can bring to capital markets

It is doubtful that the actual crypto-tokens will ever occupy a material part of a FTSE 100 companies earnings statement. On the other hand, it is quite likely that in the near future those income statements will aggregate market values and exposures that are implemented as smart legal contracts.

4. Smart Contracts – A Path To Reduce Counterparty Credit Risk

- The vanilla exchange-traded crypto-derivative market is immature
- Executing OTC smart derivatives on a distributed ledger enables one version of the state of a deal, thereby facilitating material operational cost savings in the OTC derivative industry
- The OTC derivatives market must embrace transformational change to realise the benefits of smart derivative contracts
- The OTC derivative market will embrace MDL technology and gain operational cost savings and counterparty credit risk reduction

Section 4 of this report applies the lessons from Sections 1 and 2 on cryptocurrency liquidity, market, and operational risks, as well as the legal risks identified by Dr Donovan, to a case study. These lessons help describe the impact of smart derivative contracts on counterparty credit risk. *Counterparty credit risk* is one's estimate of potential losses should the counterparty fail to meet its obligations, perhaps due to bankruptcy or a large margin call. According to the Bank of International Settlements, the global derivatives market value exceeds $15 trillion [BIS 2016], hence smart derivative contracts have the potential to make an enormous impact. At the moment, exchange-traded smart derivative contracts have a tiny footprint on a few thinly capitalised exchanges. As the technology matures, investment banks and corporate hedgers will quickly exploit the operational cost savings that the MDL can bring to financial derivatives.

Let's begin by outlining the current state of affairs in the derivatives domain. A derivative is a financial contract whose value depends on one or more financial observables. Most are familiar with the exchange-traded equity option derivative market. There are three fully-functioning mutual distributed ledger crypto-derivative exchanges (and one planned) listed in Table 3. The three active exchanges provide liquidity for three future contracts (each with a different future

delivery date) and three European-style option expiries[29], where at each expiry the exchange has a large spectrum of strikes. As with conventional exchanges, they provide margining and insurance facilities that mediate counterparty default risk.

Table 3 List of Exchange-Traded Crypto-Derivatives

Exchange Name	Domicile	Derivatives Listed
Quedex	Gibraltar	1,2,3, month futures and European-style options on USD/BTC FX rates
Deribit	Netherlands	1,2,3, month futures and European-style options on USD/BTC FX rates
Digitex	Seychelles	BTC/USD, ETH/USD & LTC/USD future. 2018 – Q4 planned start
Teraexchange (planned)	USA	USD/BTC forwards, overnight to 2Y delivery tenor

[29] A European-style exercise option contract gives the holder the right, but not the obligation, to buy (a call option) or sell (a put option) an underlying asset at the terminal expiration date of the option. Alternatively, the so-called American-style exercise derivative provides that right every day up to expiration. Only European crypto-options are currently available.

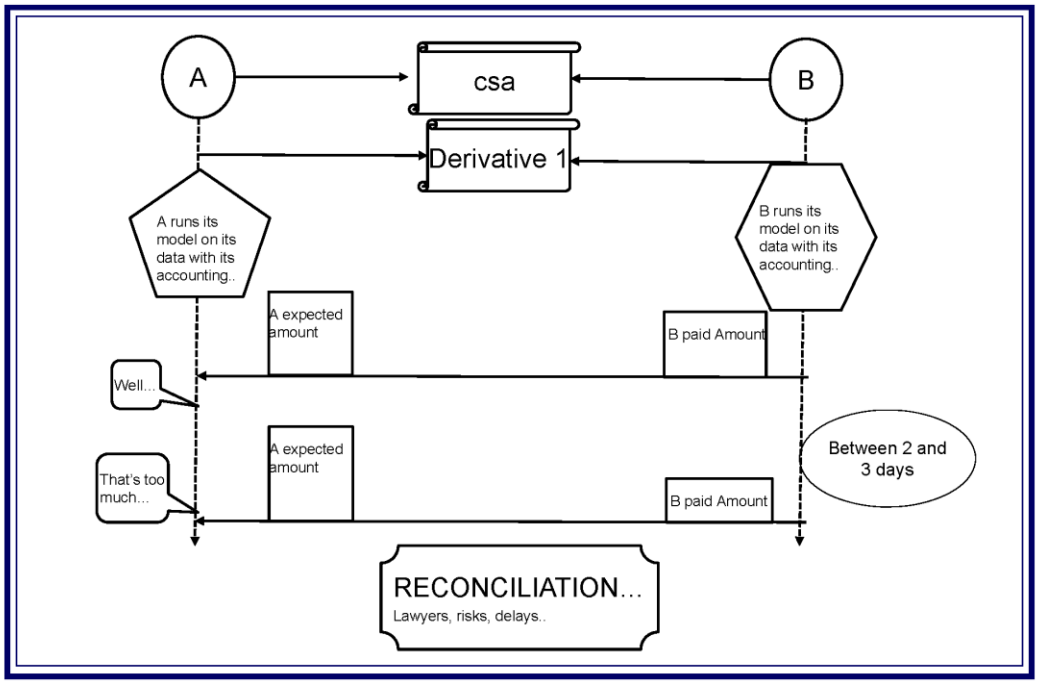


Figure 13 Functional relationships in the legacy OTC derivative reconciliation process. From [Morini 2017]

Contrary to these operational crypto-derivative exchanges, there have only been a few Proof of Concept trial OTC trades executed on mutual distributed ledgers. The legacy OTC derivatives market is populated by many intermediaries working under the existing ISDA rules regime. Let's recall the hypothetical interest rate swap, where Party A pays Party B a fixed interest rate semi-annually and Party B pays Party A a variable rate quarterly[30]. Typically, these payments occur over a 2Y-30Y period specified in the contract. The bilateral cash flows are collateralised with initial and variation margin with terms specified by the ISDA-standard Credit Support Annex (CSA) document. These functional relationships between A, B and intermediaries in this legacy OTC derivative system are schematically indicated in Figure 13. Multiple parties, including Parties A and B, as well as other intermediaries are responsible for calculating cash flows, collecting them, and

[30] It is apparent that disagreements may occur if each Party A and B calculates different values for the variable-rate payments. If the calculations are executed by the smart contract, there would only be a single version of this calculation that both parties would comply with *fait-accompli*.

transferring them. This system allows for multiple versions of the state of the swap contract. Disputes may lead to slow-moving arbitration or adjudication. The advantage of encapsulating all this operational functionality into a smart contract is that there is only one version of the contract's state – it is calculated by the smart derivative contract code. All the counterparty default risk mitigation provided by the CSA may be retained and, in fact, improved by the smart contract.

[Morini 2017] details how the legacy OTC derivative system illustrated in Figure 13 can be modified to be effectively implemented with smart contracts native to a public mutual distributed ledger (e.g., Ethereum). His model contrasts with the R3/Corda consortium's approach *ala* a private/permissioned MDL. [Morini 2017] points out several transformational changes to the OTC derivative business model that would have to occur in order for this model to gain traction, including:

- The smart contracts require access and control of the counterparties' crypto-wallets

- The counterparties will have to agree to off-chain *oracles* that will provide real-time market data observables and computations. Potentially, these services could be implemented on sub-chains whereby the data feeds would be determined by MDL consensus.

- Counterparty default risk management and mitigation is currently handled by a few Centralised Counterparties (CCPs), thereby concentrating counterparty default risk with these CCPs. This systemic risk may be reduced by replacing CCPs by smart contracts. Alternatively, the CCP's could incorporate smart contracts into their current operating model to affect this systemic risk reduction. The Depository Trust Clearing Corporation (DTCC), in the US, already operates two CCPs [DTCC 2016].

Despite the considerable benefits detailed in [Morini 2017], the technology is still immature and not quite ready to disrupt the legacy OTC derivative workflow. In addition to the legal risk issues that are still being worked on by ISDA, Dr Donovan, and others, there is another systemic and operational risk that requires attention. Miner front-running has recently been observed[31] . Cornell University researchers

[31] See Ref. [Swende 2017].

have detailed analyses of how it occurs and offered potential strategies to eliminate it[32]. Recall that on a public MDL, like Ethereum, transactions are plainly visible to all nodes. Miners order transactions to create blocks. Hence, the miners are in a uniquely powerful position to order transactions (or to insert virtual transactions) for their benefit. This front running activity was in fact observed during the Bancor ICO[33]. It is quite like front running in the securities market context.

Whereas [Morini 2017] advocates a public/permissionless smart OTC contract structure, Adjoint, a London based smart contract software vendor, maintains a private/permissioned architecture is well suited for the regulated financial market space. Z/Yen discussed Adjoint's open-source Uplink smart contract software with Somil Goyal, the firm's COO.

Uplink supports, among other things, OTC derivative contracts. The Uplink distributed ledger is devoid of cryptocurrencies and miners. Hence Uplink is decoupled from any operational, liquidity, and market risk factors of a particular crypto-token. In addition, the Uplink mutual distributed ledger does not have miners, hence miner front-running is absent.

Contrary to Ethereum's Solidity smart contract instruction set, Uplink is not so-called *Turing-complete*. As a result, it does not have the security vulnerabilities of Ethereum that allows for unintended smart contract behaviour (*ala*, the Ethereum DAO hack). Adjoint is a member of ISDA's Common Domain Model (CDM) committee. The CDM will be the next-generation of the ISDA Master Agreement – it will be the smart contract version of the OTC derivative template. Adjoint intends to implement the ISDA vision as it evolves. According to Mr. Goyal,

> *"The objective of the Common Domain Model is to move to a model which is 'common', and works across the domain [i.e., inked paper ISDA Master Agreements, trade confirmations in PDF format, collateral transfers effected via phone calls, etc.]. So as much as possible, I've got one digital artifact that covers, perhaps not all of these domains, but maybe 70, 80, 90% of them. And*

[32] See Refs. [Sirer and Daian 2017], [Breidenbach, et. al., 2017].

[33] The presence of frontrunning can be inferred by monitoring the mempool of transactions waiting to be added to blocks.

that is where we see the power of digitisation technologies on the one hand, and distributed ledger and smart contracts on the other hand coming in."

All of the challenges facing widespread adoption of smart contracts by the OTC derivatives industry are near-term solvable: smart contract code/standards need to be developed, the resulting software needs to be developed with discipline and rigorous testing to reduce the possibility of malicious hacks, the legal issues need to be addressed, and miner systemic risk needs to be mitigated. The OTC derivative market will certainly embrace MDL technology and gain operational cost savings and counterparty credit risk reduction.

Conclusions

Extracting the key takeaways from the preceding sections provides us with the following conclusions:

- Mutual Distributed Ledgers should employ best practice software development processes and information security protocols
- The impact of Meltdown and Spectre on MDLs and crypto-wallets has yet to be quantified but may be quite severe
- The extreme illiquidity and hyper-volatility make cryptocurrencies compelling assets for speculators, but diminish their value proposition for vendors and regulated financial service firms
- The Index of Martin is a simple liquidity monitoring metric that can indicate the occurrence of 'illiquidity pops' in the cryptocurrency markets
- ISDA standardisation of smart legal contracts will support scalability of these digital contracts, helping to cement their adoption by global investment banks
- The United Kingdom's common law system is inherently flexible enough to facilitate smart legal contracts and to quickly respond to the opportunities and challenges that they may present (including the question of enforceability)
- The OTC derivatives market must embrace transformational change to realise the cost-saving benefits of smart derivative contracts

A number of non-commercial MDL software developers have not exercised adequate software performance testing discipline. As a result, a number of avoidable hacks have occurred. Before mutual distributed ledger technology will

be able to transform the financial derivative space, truly reliable infrastructure must become a commodity. The R3/Corda industry consortium and a number of commercial software houses are pursuing this track. Much of this work is tightly connected to the evolution of the ISDA Common Domain Model – as the specification maps the ISDA Master Agreement to the smart contract domain, more robust smart contract software will be developed. Intel and other hardware vendors must solve the Meltdown and Spectre vulnerabilities – the open source community is too far removed from the proprietary design details of the microprocessors that run distributed ledgers. This process must continue because the open-source software development community is too isolated from the standards-development process.

In theory, smart legal contracts are enforceable in the United Kingdom. ISDA predicts smart contracts will play a meaningful role in the financial derivatives industry within five years. In the near term, inked-contracts and smart contract code will be combined to create smart legal contracts. Work is on-going to create ink-free smart legal contracts.

The cryptocurrency market is quite volatile and major bad events happen almost weekly. These dynamics recently prompted World Bank Group President Jim Yong Kim to say "…the vast majority of cryptocurrencies are basically Ponzi schemes[34]."

The underlying mutual distributed ledger technology is evolving rapidly – it's reasonable to expect that given these factors, the conclusions in this paper may have to be amended in the near future

This report has covered a lot of territory: software security vulnerabilities in the distributed ledger framework; an enumeration of the liquidity, market, and legal risks inherent in the cryptocurrency markets and smart contract paradigm; a description of the new business model the OTC derivative market must embrace; the foundational importance of ISDA standardisation before MDLs will be adopted by the global derivatives market. All the challenges are near-term solvable.

Rational business unit heads in investment banks must dismiss the popular hype

[34] Ref. [Hagan 2017].

surrounding the hyper-returns and risks of cryptocurrencies. There is considerable gold in the underlying MDL infrastructure – once the legal and economic risks are addressed the OTC derivative industry will realise exceptional benefits. The importance of ISDA standardisation cannot be understated – it is essential. Fortunately, it is an ISDA priority.

For a variety of reasons, the crypto-market is absent of liquidity. As it matures and as natural selection eliminates weaker exchanges and MDLs, liquidity will materially increase[35]. Z/Yen will execute a follow-up crypto-liquidity study to assess the evolution of the market. Stay tuned.

[35] After the massive January 2018 CoinCheck exchange failure, Japan's Financial Services Agency ordered all of Japan's other cryptocurrency exchanges to report on risks to their systems. This and other regulatory actions may cull the weaker crypto-exchanges [Harding 2018], leaving more robust exchanges and a more liquid crypto-market.

Glossary of Key Terms

Anti-Money Laundering	The set of procedures, laws and regulations designed to stop the practice of generating income through illegal money-laundering actions. The UK's body of AML legislation consists of four acts: Terrorism Act of 2000, Anti-terrorism, Crime and Security Act of 2001, Proceeds of Crime Act of 2002, and Serious Organised Crime and Police Act of 2005.
Blockchain Consensus Protocol	Allow secure updating of a distributed blockchain shared state. Consensus algorithms must be resilient to failures of nodes, partitioning of the network, message delays, and message corruption. They also have to deal with malicious nodes. Examples include Proof of Work (PoW), Proof of Stake (PoS) and Practical Byzantine Fault Tolerance (PBFT).
Counterparty Credit Risk	The risk that a counterparty will not pay an obligation stipulated in a financial contract. For example, a counterparty with a public junk bond rating would have a higher counterparty risk than one with an investment grade rating.
Cryptocurrency	A digital asset designed to operate as a medium of exchange. It employs cryptography to secure its transactions. Contrary to fiat currencies, cryptos employ decentralised consensus control, typically via a mutual distributed ledger. Examples include Bitcoin (btc), Ether (eth), NEM, Cardano (ada), Ripple (xrp), and IOTA (miota).
Double Spending	A potential security vulnerability in cryptocurrencies whereby the same single digital token may be spent more than once. This is possible because a digital token consists of a digital file that can be duplicated or falsified.
Know Your Customer	The process of a business identifying and verifying the identity of its clients. Most often a process connected with AML regulations. The Money Laundering Regulations 2007 are the underlying rules that govern KYC in the UK.
Liquidity	The degree to which one may transact an asset without materially impacting its prevailing market price.
Market Risk	The sensitivity of the value of a financial instrument to changes in market observables, e.g., prices, rates, volatility, etc. For example, the change in value of an interest rate swap as the 3-month Libor rate changes is a much-used market risk metric.

Mutual Distributed Ledger	A consensus of replicated, shared, and synchronised digital data across multiple data users. There is no central administrator or centralised data storage - each user has a full and complete replication of all the data.
Oracle	An oracle is an off-blockchain data feed. It is typically provided by third party services. Oracles provide external data that are used to trigger smart contract executions when pre-defined conditions meet. As an example, a smart swap contract might employ an oracle that sources Libor rates.
Order Book	The list of orders that a securities trading venue (e.g., a stock exchange) uses to record the interest of buyers and sellers in a particular financial instrument. A so-called matching engine uses the order book to determine which buy orders can be matched to sell orders.
Operational Risk	The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. The Basel Committee enumerated seven categories of Operational Risk: Internal Fraud; External Fraud; Employment Practices and Workplace Safety; Clients, Products, and Business Practice; Damage to Physical Assets; Business Disruption and Systems Failures; Execution, Delivery, and Process Management.
Over the Counter (OTC) Derivative	Financial derivative contracts that are traded (and privately negotiated) directly between two parties, without going through an exchange or other intermediary. Examples include interest rate swaps, credit default swaps, and forward rate agreements.
Smart Contracts	A computer protocol that automates the negotiation and performance of a contract. Smart contracts sit within a distributed ledger to provide trackable record of transactions.

Principal Authors

Rodney Greene

Rodney Greene is a quantitative finance professional with over 15 years' experience as a fixed- income and equity derivative quant at leading investment banks and hedge funds, including Royal Bank of Canada, Citigroup and Morgan Stanley. During the financial crisis of 2007-2009 he drove P&L gains exceeding 15% at a municipal derivative trading desk. His collateral optimization algorithms increased a prime broker's financing capacity several billion dollars. As a model risk quant he drove derivatives trading desks to achieve compliance with US central bank guidelines while simultaneously (and counter-intuitively) achieving cost savings.

Rodney's focus as a front-office quant has been on discount curve construction (e.g., B-spline basis function interpolation with smoothness constraints), Monte Carlo-based derivative valuation methods (e.g., multi-index Libor Market Model and multi-factor Heath-Jarrow-Martin models) and computationally optimised strategies for flow trading (e.g., partial derivative equation methods for equity derivative valuation). As a model risk quant he focused on Value at Risk (VaR)-based margining models, portfolio credit derivative models, and Over the Counter (OTC) fixed income derivative models. He co-authored firm-wide model risk management policies and drove their value-adding execution.

Robert ('Bob') McDowall

Robert ('Bob') McDowall is a former Member of the States of Alderney, one of the Channel Islands within the Bailiwick of Guernsey, where he served as Chairman of the Policy & Finance Committee, the senior decision-making Committee and now has a number of consulting and advisory roles in the private sector. He is an advisor to the Cardano Foundation with particular responsibility for oversight of the delivery of the Distributed Futures Ledger Research Programme by the Z/Yen Group. Bob is a frequent contributor to industry thought and comment in the international,

national and the financial industry press. He has over 35 years' experience in the Banking and Securities and Investment Industry. Bob has an LL.B from University College London. He is a Member of the Court of the Tin Plate alias Wireworkers Livery Company and is a former President and a Trustee of the Folklore Society based at the Warburg Institute in London.

Acknowledgements

The authors would like to thank all those who have contributed time and expertise to this research, notably Dr Anna Donovan of UCL Faculty of Laws and Somil Goyal of Adjoint for sharing their significant subject matter expertise for this report. Any misinterpretations or errors are, of course, our responsibility.

References

[AltCoin 2017] Bitcoin and Ethereum vs. Visa and PayPal – Transactions per Second (April 2017). http://www.altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/

[Badev and Chen, 2014] Badev, Anton and Matthew Chen, Bitcoin: Technical Background and Data Analysis, Federal Reserve Board white paper (October 2014). https://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf

[Baliga 2017] Baliga, Arati, Understanding Blockchain Consensus Models, Persistent Systems Ltd white paper (April 2017). https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf

[Beck 2016] Beck, Matthew, Hedging Global Liquidity Risk with Bitcoin, Grayscale Investments whitepaper (December 2016), https://grayscale.co/wp-content/uploads/2018/01/Hedging-Global-Liquidity-Risk-with-Bitcoin_Final.pdf

[BIS 2015] Bank of International Settlement, Statistical release - OTC derivatives statistics at end-December 2014 (April 2015), https://www.bis.org/publ/otc_hy1504.pdf

[BIS 2016] Bank of International Settlement, report on Derivatives Markets, end of 2016.

[Breidenbach, et. al., 2017] Breidenbach, Lorenz, et. al., To Sink Frontrunners, Send in the Submarines (August 2017), blog on http://hackingdistributed.com/2017/08/28/submarine-sends/.

[Cheng 2017] Cheng, Evelyn, Bitcoin led the best-performing ETFs this year, CNBC news (December 2017), https://www.cnbc.com/2017/12/29/bitcoin-led-the-best-performing-etfs-this-year.html

[Chokun 2018] Chokun, Jonas, Who Accepts Bitcoins As Payment? List of Companies, Stores, Shops , article on 99bitcoins.com (January 2018), https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/

[Clack 2016] Clack, Christopher D., et. Al., Smart Contract Templates: essential requirements and design options , Barclays bank whitepaper (August 4 2017), https://arxiv.org/abs/1612.04496

[Clack 2017] Clack, Christopher D., et. Al., Smart Contract Templates: foundations, design landscape and research directions, Barclays bank whitepaper (August 4 2017), http://arxiv.org/abs/1608.00771

[Clack (CDM) 2017] Clack, Christopher D., Design discussion on the ISDA Common Domain Model, UCL Dept. of Computer Science whitepaper (December 2017), https://arxiv.org/pdf/1711.10964.pdf

[CodeLegit 2017] CodeLegit Whitepaper on Blockchain Arbitration, https://docs.google.com/document/d/1v_AdWbMuc2Ei70ghITC1mYX4_5VQsF_28O4PsLckNM4/edit#heading=h.p2owquwx39n

[Conti, et. al., 2017] Conti, Mauro, Sandeep Kumar E, Chhagan Lal, Sushmita Ruj, A Survey on Security and Privacy Issues of Bitcoin, Department of Mathematics, University of Padua white paper (July 2017). https://arxiv.org/pdf/1706.00916.pdf

[Dimpfl 2017] Dimpfl, Thomas, Bitcoin Market Microstructure, University of Tuebingen - Department of Statistics and Econometrics whitepaper (April 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2949807

[Donovan 2018] Donovan, Anna, Smart Contracts – The Legal Challenges, transcript of interview (January 2018).

[Donovan 2017] Donovan, Anna, (Shadow) Banking on the Blockchain: Permissioned Ledgers, Interoperability and Common Standards, In: chiu, H and MacNeil, I, (eds.) Shadow banking, legal and regulatory risks and future directions and challenges.

[DTCC 2016] Embracing Disruption: Tapping the Potential of Distributed Ledgers to Improve the Post Trade Landscape, DTCC white paper (January 2016).

[Eyal and Sirer, 2013] Eyal, Ittay and Emin Gun Sirer, Majority is Not Enough: Bitcoin Minig is Vulnerable, Department of Computer Science, Cornell University (November 2013).
https://arxiv.org/pdf/1311.0243.pdf

[Fischer, et. al. 1985] Fischer, Michael, Nancy Lynch, Michael Paterson, Impossibility of Distributed Consensus with One Faulty Process, Journal of the Association for Computing Machinery, vol 32 No. 2 (April 1985).
https://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf

[Gervais, et. al., 2016] Gervais, Arthur, et. Al., On the Security and Performance of Proof of Work Blockchains , Proceedings of the ACM Conference on Computer and Communication Security (CCS) (2016).
https://eprint.iacr.org/2016/555.pdf

[Gramoli 2017] Gramoli, Vincent, From Blockchain Consensus Back to Byzantine Consensus, In Future Generation of Computer Systems (2017).
http://poseidon.it.usyd.edu.au/~gramoli/web/doc/pubs2/Blockchain2Byzantine.pdf

[Hacken 2017] Hacken Ecosystem, The Rush for HashPower-How the Integrity of the Proof-of-Work Cryptocurrencies Can Be Compromised by the Excessive Concentration of the Computational Power (November 2017).
https://hacken.io/wp-content/uploads/The-Rush-for-Hashpower.pdf

[Hagan 2017] Hagan, Shelly, Cryptocurrencies Are Like Ponzi Schemes, World Bank Chief Says, GARP (February 7, 2018), https://www.garp.org/#!/risk-intelligence/all/all/a1Z1W000003PvNKUA0

[Harding 2018] Harding, Robin, Japanese regulators raid cryptocurrency exchange coincheck, Fiancial Times (February 2018),
https://www.ft.com/content/2a689690-07dc-11e8-9650-9c0ad2d7c5b5

[Hertig, 2018] Hertig, Alyssa, What Meltdown and Spectre Flaws Mean for Crypto, coindesk.com (January 6, 2018).
https://www.coindesk.com/meltdown-spectre-cpu-flaws-mean-cryptocurrency/

[IBM 2017]Ponemon Institute, 2017 Cost of Data Breach Study, Global Overview, study sponsored by IBM (June 2017).
http://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf

[Klabbers 2017] Klabbers, Sjoerd, The added value of bitcoin in a global market portfolio, Radboud Universiteit Nijmegen Financial Economics Master's Thesis (2017),
http://theses.ubn.ru.nl/bitstream/handle/123456789/4434/MTHEC_RU_Sjoerd_Klabbers_s4384458.pdf?sequence=1

[Kovacs, 2018] Kovacs, Eduard, Mitigations Prepared for Critical Vulnerability in Intel CPUs, Security Week (January 3, 2018).
http://www.securityweek.com/mitigations-prepared-critical-flaw-intel-cpus

[Kroeger and Sarkar, 2017] Kroeger, Alexander and Asani Sarkar, The Law of One Bitcoin Price?, Federal Reserve Bank of New York white paper (January 2017).
https://www.philadelphiafed.org/-/media/bank-resources/supervision-and-regulation/events/2017/fintech/resources/law-of-one-bitcoin-price.pdf?la=en

[Loi 2017] Loi, Hio, The Liquidity of Bitcoin, International Journal of Economics and Finance; Vol. 10, No. 1; 2018 , pp. 13-22.
http://ccsenet.org/journal/index.php/ijef/article/view/71641/39575

[Mainelli 2007] Mainelli, Michael, Liquidity: Finance In Motion or Evaporation?, Z/Yen white paper (September 2007).
https://www.gresham.ac.uk/lectures-and-events/liquidity-finance-in-motion-or-evaporation

[Markowitz 1952] Markowitz, H.M., Portfolio Selection, The Journal of Finance, 7(1) pp 77-91 (March 1952),
https://www.math.ust.hk/~maykwok/courses/ma362/07F/markowitz_JF.pdf

[Moore and Christin 2013] Moore T., Christin N. (2013) Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In: Sadeghi AR. (eds) Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg. https://fc13.ifca.ai/proc/1-2.pdf

[Morini 2017] Morini, Massimo, How the business model must change to make Blockchain work in Financial Markets. A detailed example on Derivatives, two years later, Banca IMI Whitepaper (November 2017).

[Murphy, et.al., 2016] Murphy, Sean, et.al., Can smart contracts be legally binding contracts?, R3 and Norton Rose Fulbright whitepaper (November 2016), http://www.nortonrosefulbright.com/knowledge/publications/144559/can-smart-contracts-be-legally-binding-contracts

[Nakamoto 2009] Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, working paper (May 2009), https://bitcoin.org/bitcoin.pdf

[Naftalis, et. al., 2015] Naftalis, Benjamin, et. al., Enforcement Trends in Cryptocurrency- Cryptocurrency is on the rise...and so are enforcement actions, Latham and Watkins Client Alert Commentary (December 2015). https://m.lw.com/thoughtLeadership/lw-enforcement-trends-cryptocurrency

[Osterrieder and Lorenz 2016] Osterrieder, Jorg and Julia Lorenz, A statistical risk assessment of Bitcoin and ist extreme tail behavior, Zurich University of Applied Sciences, School of Engineering white paper (November 2016). https://ssrn.com/abstract=2867339

[Peaster 2018] Peaster, William, Massive Intel Hardware Vulnerability Discovered: Crypto Users Affected?, Bitsonline (January 3, 2018). https://www.bitsonline.com/massive-intel-hardware-vulnerability/

[Persaud 2003] Persaud, Avinash, Liquidity Black Holes: what are they and how are they generated, Singapore Foreign Exchange Market Committee Biennial Report, 2001-2002 (April 2003). https://g24.org/wp-content/uploads/2016/01/Liquidity-Black-Holes-what-are-they-and-how.pdf

[Rosenfeld 2014] Rosenfeld, Meni, Analysis of hashrate-based double-spending , whitepaper (February 2014), https://arxiv.org/abs/1402.2009

[Schroders 2015] The illiquidity conundrum: does the illiquidity premium really exist? , Schroders whitepaper (August 2015), http://www.schroders.com/hu/sysglobalassets/digital/insights/pdfs/the-illiquidity-conundrum.pdf

[SEC 2016] Williams, Mark, Continued Comments on SR-Bats BZX-2016-30, Securities and Exchange Commission public comment letter (November 2016). https://www.sec.gov/comments/sr-batsbzx-2016-30/batsbzx201630-26.pdf

[Sirer and Daian 2017] Sirer, Emin Gun and Phil Daian, Bancor is Flawed, blog on http://hackingdistributed.com/2017/06/19/bancor-is-flawed/ (June 2017).

[Speciale 2018] Speciale Alessandro, Draghi Says ECB Studying Digital Currency Risks for Banks, Bloomberg (February 5, 2018), https://www.bloomberg.com/news/articles/2018-02-05/draghi-says-ecb-studying-digital-currency-risks-for-banks

[Spence 2002] Michael Spence (2002). "Signaling in Retrospect and the Informational Structure of Markets". American Economic Review. **92** (3): 434–459. https://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2001/spence-lecture.pdf

[Stavroyiannis 2017] Stavroyiannis, Stavros, Value-at-Risk and Expected Shortfall for the major digital currencies, Department of Accounting & Finance, Technological Educational Institute of Peloponnese, Greece white paper (August 2017). https://arxiv.org/pdf/1708.09343.pdf

[Swende 2017] Swende, Martin, Blockchain frontrunning, blog (July 2017), http://www.swende.se/blog/Frontrunning.html

[Trimborn 2017] Trimborn, Simon, et. al., Investing with cryptocurrencioes – A liquidity constrained investment approach, Humboldt- Universität zu Berlin white paper (July 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2999782

[Verhage, Julie, et. al., 2018] Verhage, Julie, Whanwoong Choi, Kyungji Cho, Bitcoin's 43% Arbitrage Trade Is a Lot Tougher Than It Looks, Bloomberg Markets (January 9, 2018). https://www.bloomberg.com/news/articles/2018-01-09/bitcoin-s-43-arbitrage-trade-is-a-lot-tougher-than-it-looks

[Wikipedia 2018] Wikipedia contributors, "Smart contract," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=Smart_contract&oldid=820101586 (accessed January 29, 2018).

[Yongxing 2014] Yongxing, Chen, Subversive Miners-Strategies/Attacks in Bitcoin, UCL whitepaper (June 2014). http://www.nicolascourtois.com/bitcoin/Chen.pdf

[Zheng, et. al., 2016] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. (2017). Blockchain Challenges and Opportunities: A Survey. International Journal of Web and Grid Services. https://www.researchgate.net/publication/319058582_Blockchain_Challenges_and_Opportunities_A_Survey

Distributed Futures is a significant part of the Long Finance research programme managed by Z/Yen Group. The programme includes a wide variety of activities ranging from developing new technologies, proofs-of-concept demonstrators and pilots, through research papers and commissioned reports, events, seminars, lectures and online fora.

Distributed Futures topics include the social, technical, economic, and political implications of smart ledgers, such as identity, trade, artificial intelligence, cryptography, digital money, provenance, FinTech, RegTech, and the internet-of-things.
www.distributedfutures.net

Cardano Foundation is a blockchain and cryptocurrency organisation based in Zug, Switzerland. The Foundation is dedicated to act as an objective, supervisory and educational body for the Cardano Protocol and its associated ecosystem and serve the Cardano community by creating an environment where advocates can aggregate and collaborate.

The Foundation aims to influence and progress the emerging commercial and legislative landscape for blockchain technology and cryptocurrencies. Its strategy is to pro-actively approach government and regulatory bodies and to form strategic partnerships with businesses, enterprises and other open-source projects. The Foundation's mission is the promotion of developments of new technologies and applications, especially in the field of new open and decentralised software architectures.
www.cardanofoundation.org

"When would we know our financial system is working?" is the question underlying Long Finance's goal to improve society's understanding and use of finance over the long term. Long Finance aims to:

- expand frontiers - developing methodologies to solve financial system problems;
- change systems - provide evidence-based examples of how financing methods work and don't work;
- deliver services - including conferences and training using collaborative tools;
- build communities - through meetings, networking and events.

www.longfinance.net

Z/Yen is the City of London's leading commercial think-tank, founded to promote societal advance through better finance and technology. Z/Yen 'asks, solves, and acts' on strategy, finance, systems, marketing and intelligence projects in a wide variety of fields. Z/Yen manages the Long Finance initiative.

Z/Yen Group Limited
41 Lothbury, London EC2R 7HG, United Kingdom
+44 (20) 7562-9562 (telephone)
hub@zyen.com (email)
www.zyen.com

