Cryptocurrency and Blockchains: Retail to Institutional

Rand Low* and Terry Marsh**

Forthcoming: *Journal of Investing*
Last Revised: May 19, 2019

Abstract

A reduction in cost of traditional financial intermediation was one of the main motivations cited by Satoshi Nakamoto in his/her/their 2008 proposal for: "… an electronic payment system based on cryptographic proof instead of trust." We begin here with some back-of-the-envelope calculations of these potential cost savings and benefits from the customer perspective. We then discuss the public blockchain ledger and various solutions to two important problems that are constraints on the public blockchain's trustless consensus, *viz.* "mining" costs in proof-of-work and governance issues. We speculate that foreseeable institutional implementations will often involve integration of permissioned blockchains with public blockchains. We then discuss exchanges for trading cryptocurrencies, the second component of the crypto blockchains, and in particular their "teething problems" along with the evolution of a subset of them into increasingly "industrial strength" entities. We suggest that with a more industrial strength infrastructure in place, self-executing smart contracts are virtually natural counterparts for more traditional passive investment products. We end with a discussion of Security Token Offerings (STOs) and the newer Initial Coin Offerings (ICOs): STOs are an interesting hybrid between the ICOs and traditional IPOs; they could conceivably pave the way to a long-time-coming "direct electronic IPO" market.

****Rand Low* is an Honorary Fellow at the University of Queensland Business School (Australia)**
Mailing Address: University of Queensland, School of Business, Colin Clark Building, St. Lucia, 4072 QLD
Telephone: +61-7-3365-1111
E-Mail: r.low@business.uq.edu.au

*****Terry Marsh* is Professor Emeritus at U.C. Berkeley and an Advisor to Strike Derivatives Inc. in New York.**
Mailing address: Quantal International Inc, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111.
Telephone: 415-744-5301
E-Mail: terry.marsh@quantal.com

We thank Salvatore Calvo, Kam Fong Chan, Ray Kamath, Luke Kiernan, Andrew Lawrence, Nigel Noriega, and Charlie Walden for helpful discussions and comments. The views and opinions expressed in this article are those of the authors and do not necessarily reflect the views or position of Strike Derivatives.

1. Introduction

Cryptocurrencies and blockchains have both near-religious advocates and equally passionate detractors. Here, we ask: if an institutional-strength version of the technology were to emerge that encompassed the middle ground, what might that middle-ground look like? That is, how might an open-source, "trustless," decentralized, peer-to-peer (i.e. *sans* middleman) solution morph from its nascent current retail[1] space into an institutional-grade infrastructure? In particular, how might the investment industry be impacted and/or involved?

A ***blockchain*** is a decentralized, distributed and public digital ledger that is used to record transactions, in a "chain" of blocks, across many computers, and so that no record can be altered retroactively without the alteration of all subsequent blocks. The blocks are linked using cryptography.[2] For a public blockchain, the records encompass transactions between people who don't know each other, but nevertheless a middleman is not required to verify the transactions. A ***cryptocurrency*** ("crypto") is "a peer-to-peer digital cash system" that uses cryptography for security -- a cryptocurrency like Bitcoin can be considered an application of a public blockchain that records those cryptocurrency transactions.[3] ***Security tokens*** are issued as part of crowd-funding and have been used for participating in the development of blockchain applications. Tokens operate on top of a blockchain and as such have been relatively easy to create – they account for around 80% of coins in existence -- and we will consider their role in Initial Coin Offerings (ICOs) and Security Token Offerings (STOs): It is the crowd sale version of funding via ICOs and STOs that is considered by many to be the truly revolutionary feature of blockchains that will endure.[4]

It seems logical that, in predicting whether and how crypto and blockchains might evolve in the institutional space, one should start with their value proposition. The original vision[5] for Bitcoin was: "…an electronic payment system based on cryptographic proof instead of trust." A catalyst in giving form to this vision has been continuing enhancement in computer power and database technology.[6] Yet skeptics rightly ask whether a secure cryptocurrency and blockchain truly have a unique value for recording payments or otherwise: After all, digital payment systems *sans* the public blockchain are also enabled by the same gains in

[1] Some 80% of current cryptocurrency trading is estimated to be retail.

[2] The basic description is from Wikipedia.

[3] Similar to a bank that charges an administrative fee in dollars for keeping track of your dollar transactions, record-keeping for Bitcoin transactions is performed by blockchain participants who are paid in Bitcoins for doing so.

[4] "…you can safely say that Ethereum found its Killer App as a distributed platform for crowdfunding and fundraising" (What is an Initial Coin Offering? Raising Millions in Seconds, Feb 21, 2019): https://blockgeeks.com/guides/initial-coin-offering/

[5] Satoshi Nakamoto, 2008, "Bitcoin: A Peer-to-Peer Electronic Cash System": https://bitcoin.org/bitcoin.pdf

[6] It is the same boost in computer and database power that is the enabler that has us all talking about artificial intelligence (AI) and machine learning on centralized platforms networked via the Internet, i.e. the Facebooks, Amazons, Apples, Netflix's and Googles, of the world. It seems reasonable to claim that the same enhanced computer power and information technology (IT) could spawn a distributed and anonymous infrastructure that promises trustless transfers *cum* an immutable record for those transfers

computer and database technology. It is argued that Dotcoms from the late 1990s eventually gave us genuinely new capabilities, whereas cryptocurrency might at best allow us do things that we do now, only slightly better than the alternatives. Besides, the middleman *cum* contract law and regulation for record keeping of transactions is a time-honored and trusted technology. Moreover, even if crypto grew to be a dramatically better medium-of-exchange that replaced fiat currency transactions, a seigniorage-starved but digitally-wise government could step in and displace the existing business[7]. For crypto to truly qualify as a useful currency, it needs to retain value in addition to being a medium-of-exchange, but the stability of its value has not been reassuring historically. Finally, even for the criminally-motivated, transactions in crypto-currency are more easily traceable than suitcases full of fiat notes.

One very practical way of assessing the potential importance of crypto-blockchain technology is to start with a look at how much it could save in transaction costs by cutting out the middleman, an important benefit emphasized by its founders. We do this by looking first at a simple example of a foreign exchange wire transfer within the current Swift framework, and explore the cost at which the payment could instead be done with a blockchain and cryptocurrency. We then briefly consider a second example of domestic bitcoin payment of State taxes where foreign fiat currency is not involved. We get into the details of blockchains in Section 3: how one could use them in practice, and their strengths and weaknesses. In Section 4, we discuss cryptocurrencies, one application of a blockchain, and the exchange infrastructure that currently supports crypto trading. In Section 5, we discuss the possible mainstream use of blockchains and cryptocurrencies in investing. We separately consider applications to existing passive investment products and services, and new financial products like ICOs and STOs (Initial Coin Offerings and Security Token Offerings) that are part of crowd-funding for cryptocurrency projects themselves.

2. Payment Alternatives: Cryptocurrency or Fiat Currency?

We already have electronic systems for payments that are considered reasonably reliable and trustworthy, if somewhat clunky and expensive: The Fed wire system and the bank plumbing that goes with it move some $3 trillion in fiat currency daily, while SWIFT[8] is the well-known messaging system that connects and directs banks in settling some $6 trillion daily in electronic transfers of fiat foreign exchange funds. Clearing and settlement are on different networks.

[7] An additional concern for investors is the fragmentation occurring in cryptocurrencies that could reduce network externalities in their use. One conceivable result of the fragmentation could be that a central bank "blesses" one of the cryptocurrency protocols by adopting it as their digital currency – of course this would be anathema to the original proponents of private, i.e. government-free, digital currencies. Indeed, as Raskin and Yermack (2017) discuss in detail, a "central bank controlling and tracking a national digital currency would have immense power to observe and potentially to control an individual's finances" – this would be true irrespective of exactly which protocol is chosen. Central bank control over the digital currency may also pose the risk that it can create lots of the currency in a catastrophe, similar to the way in which that central bank could theoretically print lots of fiat currency. Proponents of crypto-currencies remaining beyond the control by central banks point to the limited supply of crypto and protection from just these catastrophe "printing press" scenarios. On the other hand, such catastrophes have indeed been rare events: at least in past global crises, individuals have had sufficient confidence that the U.S. government won't resort to the printing press to avoid defaulting on its USD-denominated obligations; indeed, if anything, "flight to the dollar" has occurred instead.

[8] Society for Worldwide Interbank Financial Telecommunications.

An initial reference point for assessing the value proposition for blockchains and cryptocurrencies is to compare them with these centralized wire transfer systems for currencies. For example, we analyze a May 18, 2018 foreign exchange (FX) transaction with USD in a U.S. bank account and a need to make payments in Japan in JPY. The transaction required completion of a tedious paper application form and payment of the hefty bid-ask spread between two of the world's most liquid currencies. At that point, the transaction went into a black box, with yen emerging several days later in a bank account in Japan. There was zero transparency – the transaction had to involve trust, literally "blind trust," a sequence of third-party middlemen, including both an intermediary and an end-point bank in Tokyo. No inbuilt immutable record of the transaction existed. Virtually all transfers like this one are eventually reconciled and cleared or reversed. Yet there have also been famous cases of funds "disappearing," e.g. the hack of the Bank of Bangladesh to send money via SWIFT to unknown Philippines accounts. Returning to the May transaction, all was above board and it eventually closed, but a not-so-small fraction of the funds still "disappeared" in the form of all-in transaction costs of 2.82%: the yen received per each USD paid on May 15, 2018 was 107.7935 versus the Federal Reserve noon buying rate of 110.25,[9] for a purchase spread of 2.28%, plus a "ticket cost" of 54 bps.[10]

One point of comparison to these existing network layers is IBM's Blockchain World Wire which uses cryptocurrency – specifically a stable coin --- as a "bridge asset" on a permissioned blockchain with public access. The network includes multiple currencies and banks "at the endpoints." Transactions are to be transparent and in real-time. Cost estimates are not available, but we are assured that transfers "…will cost a fraction of the cost and time of traditional banking and payment systems." As an outside estimate of alternative costs, we can consider a "home-made" version of the Blockchain World Wire transaction, again starting with USD fiat currency in a bank and using bitcoin as the bridge crypto asset. The USD could have been sold for Bitcoin (BTC) on Coinbase on May 15 at a spread of $0.01 and price of $8344.78 for a percent spread less than 0.00012, i.e. less than a hundredth of a basis point. Coinbase would add a 0.25% liquidity taker fee for Coinbase Pro in the small trade category, or 1.49% in Coinbase Consumer.[11] The BTC "bridge asset" would have needed to be traded back into fiat YEN. The home-made cost would have been 2 x (0.25% fee plus a 0.012% spread), i.e. 52 bps. If the initial funds started out in a BTC wallet rather than a USD bank account, one leg of these costs would vanish. The Blockchain World Wire does illustrate an entirely realistic development path where some parts of the transactions process will use crypto and be recorded on blockchains, while others are replaced by digital networks for trading and record-keeping.[12] Moreover, some of compliance or regulatory

[9] The benchmark rate used in the calculation is generously calculated as the "noon buying rate in New York for cable transfers payable in the listed currencies": https://www.federalreserve.gov/releases/h10/Hist/. If the midpoint of 110.3408 is used, the cost is slightly higher: 2.85%.

[10] Perhaps this was a bargain! The World Bank estimated in 2015 that the cost of sending funds overseas from one of the G8 countries was 6.89%: //remittanceprices.worldbank.org/sites/default/files/rpw_report_december_2015.pdf.

[11] Some consider this expensive. As a comparison, the fee on Binance (a non-U.S. exchange) would be 0.20% on a small trade.

[12] One example of the technology "mix and match" is Coinbase's April 2019 announcement that it will team up with global payments processor Visa to create a Coinbase Card which allows users to "spend crypto as effortlessly as the money in their bank."

checking, like AML, that happens in the background, may be amenable to some kind of eventual facilitation via low-cost smart contracts that are coded instructions running on the blockchain.

A second comparison of fiat and cryptocurrency as alternative mediums-of-exchange involves only a single fiat currency. On January 3, 2019, the company Overstock announced that it would begin to pay Ohio state taxes in bitcoins. In terms of relative costs to Overstock which keeps a Bitcoin wallet, Ohio would impose a 1% fee (waived for early filers) against a 2.5% fee for credit card fiat payments, i.e. the same zero cost as for non-real-time checks.[13]

If an entity keeps a bitcoin wallet, costs are minimal. This has led to the suggestion that one of the potential revolutionary usages might come from a subset of the "great unbanked" – the estimated two billion people globally without current access to banking but who do have access to mobile devices. However, the unbanked have recently tended, in the U.S., to be part of a backlash to all digital payments, e.g. the threats against cashless Amazon Go as "discriminatory" because the unbanked can use only cash (*sans* bitcoins!).

3. Blockchains

The basics of blockchains are reasonably well-known and it is easy to Google a detailed explanation[14]. As a quick summary: a blockchain is a ledger kept on a decentralized network. The ledger is a public record of transactions "chained" in blocks.[15] The blocks provide version control, such that it's easy to see previous versions of the ledger and determine that the current ledger is valid (i.e., that it originated from a previous valid version of the ledger). The transactions are validated in a process that is "trustless" such that no centralized third-party record-keeper (i.e., a bank) is required. That is, users do not have to trust any one party to securely and accurately validate a consensus as to transactions. The node (network participant) that does the most work "proves" their commitment to properly securing and validating transactions in a block.

The 'Bitcoin Network' is the best known blockchain; it is a ledger that records the current state of the ownership of Bitcoin. The ledger is updated every 10 minutes[16] with the nodes' consensus as to who-owns-what given the transaction records that the nodes receive on their computers (*via* say a Bitcoin client program). The nodes are called 'miners', and they compete for Bitcoin for the validation work that they do. For a miner to prove their commitment to do the validation work absent an *à priori* trust in that commitment, the miner needs to solve a difficult hashing algorithm problem on the block of transactions, with the

[13] In early crypto days it is completely plausible that usage is driven as much by "first mover" preference as it is by pure costs. But this is unlikely to drive longer-term institutional demand (much the same as it doesn't on a mature Internet).

[14] Vaidya (2016) provides a clear description of the steps involved in the Bitcoin blockchain proof-of-work, including the much-lauded dice analogy to it: https://medium.com/all-things-ledger/decoding-the-enigma-of-bitcoin-mining-f8b2697bc4e2

[15] Bitcoin block size was originally a 1MB block, but not every blockchain has a hard 1MB limit. The transactions are blocked because if transactions were validated just one-at-a-time, the likelihood of multiple workers submitting simultaneous solutions ("orphans") is high.

[16] Every 15 seconds in the case of Ethereum (ETH).

easily-verifiable winning solution for the block sent to all nodes. The new block contains a reference to the previous highest block, in a way that sequential blocks can be connected together, thus guaranteeing accuracy of the past records, and so deterministically describing the sequences. This is the origin of the ‘chain’ piece of the blockchain. Not only is the chain of blocks public and thus transparent, but the blocks are also immutable insofar as it is almost impossible to corrupt any piece of the existing record. Blockchains are gradually being applied well beyond Bitcoins, indeed beyond cryptocurrency transactions especially where understanding the provenance of goods and materials used in the manufacture or sale of a product are of vital importance (e.g., shipping logistics, supply chain management, pharmaceuticals, collectible antiques, fine art, etc.)

a. Blockchain trilemma

Unfortunately, there exists the 'Blockchain trilemma' problem that is inherent in the proof-of-work mechanism currently used in Bitcoin. The Blockchain trilemma (also known as the Scalability Trilemma) focuses on the challenges in developing blockchain technology that offers the characteristics of decentralization, security, and scalability without compromising any of the above. Fundamentally, Ethereum Founder Vitalik Buterin states that blockchains can only achieve 2 out of the 3 characteristics at any one time[17]. Decentralization describes networks that are permissionless and censorship-resistant as all decisions performed on the blockchain are by consensus across all nodes. Security is defined as blockchain data that is immutable with no single or central point of failure. Scalability describes an information network has sufficient throughput to process thousands or millions of actions on the blockchain as required.

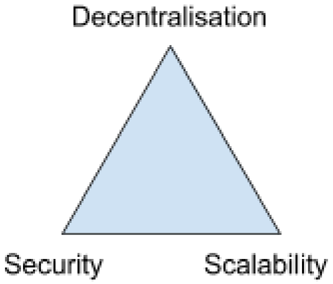

Fig 1. Blockchain/Scalability Trilemma

Decentralization is a key tenet tenets of blockchain advocates. Decentralization allows the network of nodes to be permissionless and censorship-resistant; however, as decentralized systems depend on consensus of information across a number of nodes this requires

[17] Financial economists will appreciate the analogy of this conundrum to the 'Impossible Trinity' in monetary economics where only two policy positions of free capital flow, fixed exchange rate, and sovereign monetary policy are possible. It is by understanding the ‘Impossible Trinity’ that allowed George Soros to have broken the Bank of England on Sept. 16, 1992.

achieving ‘Byzantine Fault Tolerance’[18]. As such, Bitcoin and Ethereum are currently using ‘Proof-of-Work’ computations to be Byzantine Fault Tolerant. However, the proof-of-work mechanisms are compute-intensive calculations that suffer from two well-known problems for institutional applications. The first one is that the compute-intensive calculations consume a lot of power: The Bitcoin Energy Consumption index (https://digiconomist.net/bitcoin-energy-consumption) indicates that if we currently ranked the amount of electrical power used to mine Bitcoin as we might rank a country’s electrical consumption, it would be 55th in the world, just behind Singapore (52nd) and Hong Kong (54th). Interestingly, the power consumption is endogenous – if Bitcoin prices drop precipitously, heavy-energy-use becomes unprofitable, thinning out the ranks of the miners[19]. It is easy to see that this could quickly threaten the viability of “proof-of-work” Bitcoin; also, a sudden decrease in network hashing power to fewer miners increases the well-understood risk of a ‘51% attack,’ i.e. if more than half the hashing power is owned by one group, they could begin to rewrite portions of the chain.” The second problem with the intensive computation providing proof-of-work and the redundancy necessary to run the decentralized framework is that it slows down the update speed. This slowness is frequently perceived to be an impediment to low-latency institutional applications. The slow speed is not necessarily a problem when the blockchain is being used for record-keeping for transactions in say real-estate or a carbon-exchange transaction, where latency is not an issue.

Not surprisingly, research into modifying the way in which proof-of-work is necessary to achieve decentralized consensus, is a hot area. The speed issue *per se* is not surprising in the network IT business -- the problems of scaling are the rule rather than the exception as new network businesses “ramp up” (Google’s search engine was a good example).[20] But the argument is that speed is an inherent problem for blockchain networks, given that the trust is demonstrated by a proof-of-work that requires time. One avenue of blockchain research is focused on “proof-of-stake” as a replacement for proof-of-work in ledger updating. Tendermint-Cosmos is an example.[21] Both the genius and the problem in proof-of-work is that the nodes that do the most work have the highest chance of being consensus winners in validating a new block. The alternative proof-of-stake idea is that to make the nodes who commit the biggest stake have the highest chance of being the winners (and we can trust this since they have the most to lose in not being trustworthy). In short, trust is established not by dedicated hard work but rather by having a lot of skin in the game.

[18] Byzantine Fault Tolerance describes the challenge of ensuring that multiple network nodes are communicating safely and achieving consensus across a network without being disrupted by a faulty or malicious node that can undermine the entire information network.

[19] A recent *Financial Times* article discusses the effects of variations in crypto profitability on its viability: https://www.ft.com/content/98d52c50-fd37-11e8-aebf-99e208d3e521

[20]As chronicled in the New Yorker article “Binary Stars” (December 10, 2018, pp. 28-35), Google in its early days faced critical issues in scaling up search technology to keep up with the growth of the Web, particularly with respect to speed and hardware reliability issues. Google developed a system to spread its index across arrays of computers as if it was a single (centralized) database.

[21] There are more complicated “moving parts” in Tendermint than described here. See: https://www.tendermint.com/docs/introduction/what-is-tendermint.html

Another approach involves "asynchronous consensus," or perhaps more accurately, asynchronous trust. The idea behind this approach is that the proof of accuracy in recording the streamed events can be provided retroactively, as opposed to immediately when events occur and data is fed. This asynchronous approach affords external validation of the data, a complete audit trail, and real-time data delivery at familiar data feed rates.

Another common variant of the blockchain decentralized ledger technology is private or permissioned blockchains that require permission to read the blockchain information and to authenticate new blocks of transactions. As examples, Ripple is a permissioned blockchain, as is the IBM Blockchain World Wire mentioned at the outset. Private permissioned blockchains mean that proof-of-work is no longer needed for a trustless decentralized consensus – the private arrangements centralize commitment to the process of validation and security – like turning up to work each day in a corporate hierarchy per trusted agreement as opposed to validating trust with an outside contractor. Permissioning solves the energy-hog problem, though purists question whether discarding trustless decentralization has in effect discarded the baby with the bathwater as one can argue that a centralized ledger/private/permissioned blockchain is simply a fancier implementation of already existing database technology by well-established firms such as Oracle and SAP.

Nonetheless, given the importance of governance issues for institutions, along with practicalities such as operational "black swan events" (every day!) in networked environments, not the least things like dropped data connections and latency, it seems a safe prediction that the institutional future will see more combinations of permissioned/private blockchains[22] with public blockchains where the latter play a complementary role in transparency and verifiability. The right question doesn't involve a religious choice of private OR public blockchains, but instead has to do with the efficient boundary between tasks "inside" a hierarchical corporate/regulatory structure and tasks accomplished by contracting with network nodes in the "outside" market – we might expect Coase's (1937) insights as to "the Nature of the Firm's" (private blockchains) boundaries to change with computer/information technology, but it seems unlikely that they'll be obsoleted in a new purely decentralized public blockchain utopia.[23] It is likely that going forward a combination of public and private blockchains interacting with one another (also known as blockchain

[22] "I am not talking about selling software here. I am talking about transactional revenue by way of our ownership of a new kind of network that's enabled by blockchain; it's all about new transactional networks" (Jesse Lund, IBM Head of Blockchains for Financial Services).

[23] Coase's well-known "practical approach" here stands in marked contrast to that of the crypto-anarchists: "Coase has always asked economists to be keen observers, trying to understand why things operate as they do, rather than pure theoreticians, wondering why the world doesn't conform to their theoretical models of reality. And he led the way by observing industrial organizations and structures up close before theorizing about them," Federal Reserve Bank of Dallas, *Economic Insights,* Vol 8(3). Compare this with (say) the late self-described crypto-anarchist May (1992): "Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation."

interoperability) will be the norm. As such, developments in these area is being made by new protocols such as the Cosmos and Polkadot networks.

b. Blockchain Governance

The open-source decentralized blockchain is designed specifically so that there is a "consensus reconciliation" of transactions reached algorithmically, *sans* a middleman and *sans* a clearing corporation. By construction, an encoded "nexus of rules" in the blockchain protocol (scripts) is NOT designed to solve governance problems that might arise when there is an unforeseen albeit inevitable short-coming in those rules. If a valuable component of the decentralized network is the protocol for smart contracts and dApps (decentralized applications for smart contracts) discussed later, then a "law of unintended consequences" will surely expose governance issues – this is, after all, deliberately new governance territory.

One such example involves the controversy surrounding Augur's blockchain-based prediction market where a dispute has arisen involving the timing specification for bets on the 2018 November Midterm election. The outcome state specified was: who would control, i.e. "win," the U.S. House of Representatives after the election. The dispute is that on December 10 when the Augur contract expired, the controlling party was still the Republican Party (changeover occurred on January 3, 2019), but most would consider that the Democratic Party was the winner of the November election. Formally, the problem will be resolved by Augur token-holders who report outcomes, but if the dispute can't be solved, the dissident Augur protocol will likely "fork" (split off) – it is not obvious that such a dispute resolution mechanism will suffice as part of a "mature" financial market apparatus. There is some research aimed at governance in the context of the decentralized system: "Based on the concept of distributed jurisdiction, [Kaal and Calcaterra (2018)] suggest an open source platform ecosystem for smart contracting dispute resolution that allows users to opt into a conflict resolution mechanism that enables more nuanced crypto solutions and produces greater certainty in the process."

Walch (2015) aptly sums up the general governance problem:

> "…the operational risks spawned by decentralized, open-source governance, including that no one is responsible for resolving a crisis with the software; no one can legitimately serve as "the voice" of the software; code maintenance and repair may be delayed or imperfect because not enough time is devoted to the code by volunteer software developers (or, if the coders are paid by private companies, the code development may be influenced by conflicts of interest); consensus on important changes to the code may be difficult or impossible to achieve, leading to splits in the blockchain; and the software developers who "run" the Bitcoin blockchain seem to have backgrounds in software coding rather than in policy-making or risk management for financial market infrastructure."

4. Cryptocurrencies and Exchanges

Bitcoin is the most well-known of the cryptocurrencies, but there are now better than 2,500 others, among the most popular of which are: Ethereum, Ripple, Dash, Litecoin and Monero. These cryptocurrencies can be bought and sold on exchanges or OTC, or they can be "earned" as fees for doing the work of recording transactions on the blockchain. Users' balances are custodied in digital wallets by firms like Electrum, Exodus, and Jaxx. All transfers on the network are encrypted and recorded in the publicly-viewable blockchain.

As the "new kid on the block" with primarily retail users at present, it is perhaps not surprising that interface and facilities to trade and invest in cryptocurrencies are decidedly state-of-the-art IT. There are more than two hundred Exchanges that allow trading of cryptocurrencies against fiat currencies like USD, Yen and Euros. In USD transactions, the major exchanges include Coinbase, Gemini Trust, CEX.IO, Bitstamp, Bittrex, Kraken, Coinbase Pro and Bitfinex. One can use the Coinbase Consumer app with an easy-to-use interface and real-time trade graphics, to purchase Bitcoin by specifying currency and amount, entering credit card (or digital wallet) information, and pressing "Buy." The acquired cryptocurrency can be custodied in a Coinbase digital wallet[24]. With such an easy-to-use and efficient process, "what's not to like?" ask the proponents.

Ignoring the obvious risk of losing one's private encryption key to the digital wallet – which is akin to losing a very secure password -- some other key risks that can be mitigated are the reputation of the exchange, and cyber intrusions, i.e., hacking, that lead to coins being stolen from the exchange, which can be insured against. Secure storage of one's cryptocurrency is an important factor to consider and as mentioned above, many services exist such as on-line wallets, software wallets, and hardware wallets -- hardware wallets are off-line devices that require two-factor authentication for all transactions. Since hardware wallets are offline, hackers are unable to hack into the user's account,[25] and two-factor authentication has the added security that all transactions require the user's approval.

As the business becomes institutional, we can certainly expect to see industrial-strength custodians plus clearing and settlement. Yet the first impression is often that the trading infrastructure for cryptocurrencies still somewhat resembles the "Wild West", and certainly there are academic studies and anecdotes of failure of the law of one-price across exchanges for an obviously fungible asset like Bitcoin. Lack of governance in the infrastructure has of course been part "the original design"– the ideal of decentralized and trustless trading, settlement and transaction record-keeping prompt memories of early Internet visionaries "setting the data free." The problem with the disruptor's decentralized vision is of course that trading across multiple venues where all traders get access to the best possible price *ipso facto* inherently requires centralization! For example, in the case of exchange-traded equities, Regulation NMS rules usually require brokers to fill market orders at the national best bid or offer (the "NBBO") or better across trading venues. Market participants can access the NBBO by feeds from two centralized Securities Information Processors ("SIPs") to which all exchanges are required to report their best bids and offers. Bartlett and McCrary (2017) show that the SIPs achieve the centralization objective quite well: their evidence is that there is minimal profitability[26] in buying quote data directly from exchanges to arbitrage latency in

[24] Most exchanges in practice use a small number of wallets (hot wallets, as opposed to "cold wallets") to hold short-term capital, which is convenient for the exchanges but also a vulnerability. This paper (https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf) uses network analysis techniques to determine the 'market share' of BTC custody.

[25] It has been pointed out to us that hacking is a risk for conventional systems as well as for crypto – the familiar ATMs are regularly hacked or hijacked around the world!

[26] They estimate $11.6 million of gross profitability on $3 trillion in transactions.

the SIP update processing which is in the order of 400 to 700 microseconds (depending on which "Tape" feed).

There is certainly no corresponding international or national market system or centralized order book and quote feed like SIPs for crypto exchanges. But even *sans* this centralization, a set of eight or ten "institutional-grade exchanges" has already started to emerge. In a recent SEC application, Fusaro and Hougan (2019) identified a group of ten "for real" exchanges – Bitfinex, Bitflyer, Binance, Bitstamp, Bittrex, Coinbase, Gemini, Itbit, Kraken, and Poloniex – that "…trade extremely tightly" with only rare sustained deviations from a uniform price.[27]

On the face of it, the Bitwise "trade tightly" observation is at odds with Makarov and Schoar's (2018) academic evidence that: "…there are large arbitrage opportunities in bitcoin prices across exchanges that open up recurrently across different exchanges and often persist for several hours, and in some instances even days and weeks. These departures from the law-of-one-price exist even in the face of significant trading volumes on the exchanges." However, Makarov and Schoar themselves actually note that much of the apparent arbitrage breakdown *across* international exchanges could be attributable to identifiable arbitrage obstacles, e.g. trading on the Korean exchanges has not been feasible for non-Koreans since early 2018; exchanges tend to trade crypto against their native currencies (e.g. bitFlyer in Japan is active when the U.S. is sleeping, but mainly in trading BTC against JPY, not BTC against USD). Also, there is a reasonably widespread "street view" that some 95% of apparent crypto volume is fake, so the failure of the law of one price across exchanges that simply *report* significant volume is not surprising.

Research evidence for wash trades and other forms of price manipulation in cryptocurrency trading has been presented in Gandal et. al. (2018) and Griffin and Shams (2018)). The SEC has also recently drawn attention to the crypto spot market shortcomings in its rejection of the Gemini Trust application to list and trade shares in a bitcoin ETP called the Bitcoin Trust. In its rejection, the SEC expressed concern that: "…because the underlying commodities market for this proposed commodity-trust ETP is not demonstrably resistant to manipulation…the ETP listing exchange must enter into surveillance-sharing agreements with, or hold Intermarket Surveillance Group membership in common with, at least one significant, regulated market relating to bitcoin."

For institutional users, the bottom line currently seems to be that while the trading facilities are still evolving, it makes sense to simply stick with one of the trustworthy exchanges listed above – trustworthiness appears to come at little or no extra cost! If not: (a) don't necessarily trust standard measures that rely on minor-exchange volume numbers, including VWAP price measures – it is easy to see that if there was a boost in volume to manipulate price, then VWAP for the respective exchange will be doubly impacted by the manipulation; (b) "fortify" order-entry and pre-trade analytics, particularly for liquidity-taking market-sweep orders and the like; (c) remember that the usual option in a market maker's firm quote will not exist in "last look" bid-ask quotes that will likely arise in crypto OTC trading as they have in the fiat-FX markets. That is, we wouldn't expect orders executing at a last-look quote to perfectly align with prices for firm quote executions; and (d) remember that order depth and volume in any marketplace can "disappear" in a sharp market downturn, which applies *à fortiori* to fake volume, a non-trivial issue when fake volume currently makes up such a large fraction of reported minor-exchange volume.

[27] Even if we don't adjust for bid and ask price differences in comparing exchanges, bid-ask spreads are tiny, e.g. one-hundredth of one cent on a $5,000 bitcoin.

In a crypto market that will conceivably develop market-on-close auctions and crossing networks operating alongside continuous quote-driven markets, it is easy to see that if rules governing pricing increments, sweep rules and trade-through rules, priority rules, limit order cancellation etc. are not properly "harmonized," there will be more than "one price," but the deviations won't necessarily reflect failure of the law-of-one-price, indeed cross-sectional pricing differences could suggest enhancements, not lack of sophistication! Also, it is hard to imagine that all the rough-and-tumble of trading could in the near-term be completely be run algorithmically by smart contracts (below) in a decentralized governance setup?

One might speculate that, especially with the visible hand of regulators like the SEC, the retail "Wild West" majority of exchanges will eventually drop out or grow into institutional-strength entities. Perhaps the FX markets might be suggestive as to the lines along which a "crypto trading world" will develop, albeit that at first sight the FX market appears to be organized differently from today's crypto markets. The spot FX market is a dealer market with customer order-flow and inter-dealer order flow (brokered and bank-to-bank) - as discussed above, one of crypto's aims is to "disrupt" the wall between customer and the middleman inter-dealer market -- only dealers in the current FX market see customer order flow, and then it is only that for their own customers. This customer order flow appears to drive ultimate FX pricing. We can envisage a development cycle whereby more mature investors attract/demand a more sophisticated trading venue, which in turn attracts more seasoned investors, retail and institutional.

One potentially important class of retail investors that may be a participant in developing this area is high-net-worth investors. A report by Accenture-US states that "87 percent of high net worth investors (HNWI) use digital services[28] for financial services." Particularly for younger HNWI who are comfortable with the technology behind innovations like cryptocurrencies and blockchains, they could believe that the investment alpha (or transaction cost saving) "outweighs" the current crypto volatility.

On the other hand, Silicon Valley HNWI aside, one might speculate that a better template for crypto market growth is not the FX environment today, but rather FX back in the early post-Bretton Woods days in 1976 when there was very little experience with freely-fluctuating exchange rates, George Soros was "breaking the Bank of England," and researchers were trying to understand the determinants of changes in previously-fixed FX rates, if only to hedge them. Most especially, in those "old days," relationship client management meant that the institutional clients looked to their investment banks and brokers for "education" and assistance in that new world.

But if cryptocurrency is today roughly at a stage that resembles post-Bretton Woods, the glaring difference with FX in 1976 is that banks *are not* stewards of the new financial technology this time. Moreover, in the brave new transactional world that has replaced relationship banking, it's hard to see how the education gets done – learning on the Web sounds good until (inevitably) some investors lose money! At any rate, it seems safe to predict that some of the familiar institutional structure would be co-opted into a new crypto-land, e.g. traditional custodians replacing retail "wallets" and the greater integration of blockchain infrastructure into existing prime-brokerage borrowing and lending, and into

[28] Of course, "digital services" can have many meanings, ranging from automated bill-paying services to re-balancing investment portfolios and executing security trades.

clearing and settlement operations (Bitcoin blockchain advocates would argue that clearing and settlement can always be part of a public blockchain). In the end, perhaps the evident chaos in the emergence of crypto and blockchain technology is in part a change in the business model for financial innovation more generally, i.e. this time the disruption is at least somewhat "different."

Another interesting question is also likely to eventually surround the trade data and cost. Currently established securities exchanges do quite well from the sale of market data -- especially low-latency feeds; trading services become the adjunct to the generation and supply of data rather than vice versa! Data might want to be free, as the Internet idealists once proclaimed, but perhaps more realistically it might want to be low fee with relatively low-cost entry into the crypto exchange business. Data issues will be especially interesting given the recent attention that the SEC is giving to the level of fees for existing market data.

5. Crypto-Blockchain and Investing

Here we discuss three ways in which the decentralized distributed ledger technology and cryptocurrencies may have a foreseeable impact on the investment industry. One is in applications of smart contracts in the passive factor-investing space that has grown so enormously in the last decade. The second is in crowd-sourced funding of development in the crypto-blockchain area via Security Token Offerings (STOs) and newer versions of Initial Coin Offerings (ICOs). The third is in a movement towards Decentralized Finance, colloquially known as DeFi, that encompasses disruptions in finance in areas such as lending, trading, derivatives, hedging and prediction markets.

a. Smart Contracts for Passive Investments?

Smart contracts are self-executing contracts where the rules and points of agreement can be written in computer code and thereby be stored and replicated on a network of computers that run a blockchain. The bookkeeping to keep track of money earned and transfers made (e.g. reinvestment of dividends, voting, dealing with splits etc.) in accordance with the terms of the contracts could then be done on the blockchain. To the extent that the selling point of passive investing is its rules-based nature, it seems tailor-made to run via smart contracts on a blockchain architecture.

A blockchain dApp (decentralized Application) uses smart contracts to execute commands and retrieve information from the blockchain – it is similar to the familiar Web applications that run on everyone's computer, but instead of using APIs to connect to an online database, it connects to the smart contract. An investment example of a dApp is Melonport which bills itself as a blockchain (Ethereum) protocol for digital asset management where "participants can set up or invest in digital asset management strategies in an open and competitive manner." The idea of an App that "sits on top of" an existing technology is not new: As ETFs gained popularity, various industry observers promoted them as vehicles that emulate mutual fund functions but utilize existing trading and securities market infrastructure. ETFs (with non-crypto constituents) sitting on blockchain infrastructure seems an almost-obvious step in the same direction. Of course, embedding a lot of governance rules into the code takes work.

b. ICOs and STOs

Turning to investments in projects and private companies that are building services on blockchain and crypto infrastructure, those illiquid investments most resemble those that, a decade ago, would have been done by angel-investors or venture capitalists. ICOs (Initial Coin Offerings) briefly became a significant source of funds for financing sdevelopment, with some 14 Billion of USD raised from 2,167 issues from 2014 until 2018.[29] About 15% to 20% of these issues were typically listed on exchanges. "Funding projects with a token on Ethereum became the blueprint for a new and highly successful generation of crowdfunding projects…investing in tokens on top of Ethereum is charmingly easy: You transfer ETH, paste the contract in your wallet – …The tokens appear in your account and you are free to transfer them as you want."[30] By 2018, ICOs had come to be derided by many as "crowd funding without regulation,"[31] where the "crowd" seems to have been made up primarily by a combination of retail investors and specialized crypto funds. Funds raised have gone to developers of dApps and new cryptocurrencies – the most famous of the latter[32] being the $18MM raised in 2014 in the Ethereum ICO.

After mid-2018, especially amidst a fall in crypto prices, there was a so-called "crypto winter" in the issue of ICOs, which are being both "cleaned up" in terms of regulation and accountability and quickly supplemented by Securities Token Offerings (STOs), sometimes called asset token offerings. There were 119 STO issues in 2018, mainly in the last quarter. A STO is similar to an ICO insofar as investors receive tokens for their investment, but the security token represents ownership of the underlying asset (as recorded on a blockchain). The STO is an interesting crowd funding hybrid between an ICO and securitization of the issuing company's assets via a traditional IPO, but with considerably more regulatory oversight than for older ICOs. It is also argued that instead of the IPO with its roadshows and underwriters and subscription price etc., the better analogy for the STO is the direct listing

[29] Source: https://www.icodata.io/stats/2018.

[30] Ethereum is often referred to as an 'ecosystem' for tokens which finance smart contract applications on the Ethereum platform.

[31] It is widely claimed that early ICOs had a Wild West flavor to them, although it is not clear that ICOs failed at higher rates than comparable angel or VC projects. Zetzsche et. al (2017) make the case for the prosecution: "…many ICOs are offered on the basis of utterly inadequate disclosure of information, and the decision to invest in them often cannot be the outcome of a rational calculus. Many of the hallmarks of a classic speculative bubble are present in many, but certainly not all, ICOs." In studies of ICO price behavior, Momtaz (2018) and Hu, Parlour, and Rajan (2018), show a median issue-day-return around 1.5% and median 1-week return of -10.3% respectively. Momtaz reports longer-run median returns on ICOs around negative 30% over the period 2014 - April 2018. Clearly the distribution of returns is substantially positively skewed.

[32] Ripple funded the development of its platform with an ICO in 2013, so perhaps it deserves the honor of "most famous."

that Spotify did on the NYSE in April 2018. Indeed, STOs and more recent ICOs are widely viewed as “more mature” versions of the latter’s earlier brethren.[33]

The STO is typically restricted to accredited investors; includes a document like a prospectus or a sophisticated version of a whitepaper; consist of “digital shares” (tokens) settled on a new blockchain protocol like BTC or ETH and held by custodians; and sometimes uses intermediaries familiar from the IPO process. STOs look like IPOs except that they involve the direct issue of “digital shares” (security tokens). As STOs are issued at an earlier growth stage than that of an IPO issue, secondary trading of them also takes place at an earlier stage. That in turn means that we will likely see low liquidity and market-makers that most resemble the OTC market for equities.

Moving to investments in STOs rather than ICOs is in part like moving from valuation and investing in technologies to the valuation of companies, e.g. like valuing and funding Pets.com or Amazon.com in the dotcom era, versus valuing “the” Internet as a network (initial R&D on the Internet was of course funded by the government, in contrast to blockchain). It will be interesting to see the data on how STO prices (in fiat currency) move relative to the movement of the price of the native cryptocurrency, e.g. Ethereum.

c. DeFi

If Bitcoin showed the way for decentralizing a currency away from a central bank, DeFi is a movement towards decentralizing all financial services (e.g., lending, margin trading, derivatives, hedging, prediction markets, exchanges, etc.) towards a peer-to-peer system of investors, therefore omitting banks and financial institutions as intermediaries altogether. Overwhelmingly, most projects in the DeFi space are taking place on Ethereum due its inherent capabilities in area of complex smart contracts. As lending and borrowing is a key activity for banks, we describe the more well-developed borrowing and interest-bearing deposit platforms are MakerDAO and Dharma.

MakerDAO is a borrowing platform that allows users to open collateralized debt positions (CDPs) by posting Ether (ETH) as collateral to borrow against. The MakerDAO platform will make available to the depositor of the ETH collateral an amount of Dai[34] which is a stablecoin whose value is stable relative to the US dollar. The value of collateral that is locked up must be greater than 150% of the DAI borrowed, which translates to a maximum loan-to-value ratio (LTV) of approximately 67%. Any breach of the LTV threshold will resulted in liquidation of the collateral to cover the value of Dai that has been lent. The value of Dai is stabilized by using a Dai savings rate that changes according to the deviation of the market price of Dai from the USD. For example, if the market price of Dai is below 1 USD,

[33] It is interesting that IPO on-line auctions to distribute primary share offerings and championed by WR Hambrecht & Co. arguably did not have the success of ICOs and STOs. Perhaps the STO heritage in IPOs is more mature than we note: Wikipedia states that: “Financial historians Richard Sylla and Robert E. Wright have shown that before the Civil War, most early U.S. corporations *sold shares in themselves directly to the public* without the aid of intermediaries like investment banks.[3] The direct public offering or DPO, as they term it,[4] was not done by auction but rather at a share price set by the issuing corporation.”

[34] DAI is also purported to be the only “decentralized” stablecoin.

the Dai savings rate will increase in order to incentivize more Dai holders and less CDP holders, which will therefore increase the market price towards the 1 USD target price. The action of altering the Dai savings rate is performed by the Maker Governance Community. As such, one can see that such actions are analogous to a central bank governor altering the overnight rates to target monetary policy, except the Maker Governance community consists of all individuals holding the Maker token. What makes MakerDAO a unique preposition is that its roadmap, will allow for Multi-Collateral Dai that will accept other forms of collateral ranging from other cryptocurrencies, fiat currencies, all the way towards securitized products such as mortgaged-backed securities. Such innovations will have interesting repercussions for the financial industry as exposure to such complex investment products have been the sole purview of investment banks and hedge funds.

Dharma is a peer-to-peer lending platform that allows depositors and lenders to be discoverable towards each other. Depositors can define their risk profile by specifying their desired loan terms such as collateral type, duration, interest rate, etc. Once a borrower has agreed to the loan terms, the collateral is locked up in a smart contract and the borrower receives the principal immediately. In this manner, the innovation of Dharma above other P2P lending platforms such as Lending Club are in the use of smart contracts to alleviate custodial and governance issues in any breach of contract during the lending process.

6. Summary

Our objective here has been to provide a non-judgmental overview of the ongoing development in cryptocurrency and distributed-ledger blockchain technology. We began with a concrete illustration of how the technology is beginning to improve on the cost of existing "plumbing" for international fund transfers and for domestic payments like taxes – interestingly that circles right back to the original Satoshi Nakamoto (2008) objective to lower costs and payment uncertainties by replacing financial intermediation with decentralized ledger technology.

We then discussed the details of blockchain and cryptocurrencies, and in particular problems that most would agree need to be solved in order that the technology achieve escape velocity in investment markets.[35] We focused on the problem of proof-of-work in establishing trust in the validation process in blockchains, how it increases latency and consumes energy, and possible solutions. We then addressed some of the problems in trading cryptocurrency, problems that are being resolved as the exchange, settlement, and custody process is steadily attaining "institutional strength" – in particular, a small group of Exchanges are virtually already there.

[35] We have focused on financial/investing applications. As a non-financial application, the recent Barron's article: "Blockchain technology has hit a stumbling block" (December 21, 2018) describes issues that have arisen in the *TradeLens* project to track shipping documents on a blockchain. Arguably we are artificially differentiating "financial" and "non-financial applications. Chod *et. al.* (2018) suggest that both financial and nonfinancial benefits accrue jointly – they: "…identif[y] an important benefit of blockchain adoption—by opening a window of transparency into a firm's operations, blockchain technology furnishes the ability to secure favorable financing terms at lower signaling costs," i.e. the non-financial application to supply chain verification is integral to financing.

Finally, we discussed "game changer" aspects of the technology for investing: One is passive investment applications that use smart contracts built on top of the block-chain. The second is the crowd-source funding of blockchain-crypto development: ICOs and STOs that seem to be attaining a good deal more prominence than did various previous renditions of on-line auctions for IPOs. It is conceivable that STOs will finally pave the path to a "direct IPO" market. It is anticipated that with the rise of DeFi, many other traditional banking and finance activities from hedging, derivatives, margin trading, and lending will be disrupted by removing financial intermediaries and the need for counterparty risk management by using smart contracts to enforce agreements between both parties engaging in any financial transaction.

Perhaps the safest bet for predicting the future is that it is likely not an either-or outcome for blockchain/crypto versus other digital network solutions, but rather one where they are combined according to their relative strengths in ways that we don't see yet.

References

Bartlett, Robert P. III, and Justin McCrary, 2017, "How Rigged Are Stock Markets? Evidence from Microsecond Timestamps," U.C. Berkeley, July 28.

Chod, Jiri, Nikolaos Trichakis, Gerry Tsoukalas, Henry Aspegren, and Mark Weber, 2018, "Blockchain and the Value of Operational Transparency for Supply Chain Finance," https://ssrn.com/abstract=3078945

Coase, Ronald H., 1937, "The Nature of the Firm," *Economica*, 4 (November), 386-405.

Fusaro, Teddy, and Matt Hougan, 2019, "Presentation to the U.S. Securities and Exchange Commission, Bitwise Asset Management, March 19.

Gandal, Neil, Tali Oberman, Tyler Moore, and JT Hamrick, 2018, Price Manipulation in the Bitcoin Ecosystem," CEPR, Discussion Paper 12061.

Griffin, John M., and Amin Shams, 2018, "Is Bitcoin Really Un-Tethered"? University of Texas-Austin, June 13.

Howell, Sabrina T., Marina Niessner, and David Yermack, 2018, "Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales," ECGI Working Paper Series in Finance, Working Paper No. 564/2018, June 21.

Hu, Albert S., Christine Parlour, and Uday Rajan, 2018, "Cryptocurrencies: Stylized Facts on a New Investible Instrument," May 3: https://ssrn.com/abstract=3182113

Kaal, Wulf A., and Craig Calcaterra, 2018, "Crypto Transaction Dispute Resolution," Forthcoming in: THE BUSINESS LAWYER, SPRING 2018
Makarov, Igor, and Antoinette Schoar, 2018, "Trading and Arbitrage in Cryptocurrency Markets," Working Paper, NBER and CEPR.
Momtaz, Paul P., 2018, "The Pricing and Performance of Initial Coin Offerings," UCLA.

Raskin, Max, and David Yermack, 2016, "Digital currencies, decentralized ledgers, and the future of central banking," in Peter Conti-Brown & Rosa Lastra (eds.), *Research Handbook on Central Banking*, Edward Elgar Publishing, spring 2017.

Vaidya, Kiran, 2016, "Decoding the enigma of Bitcoin Mining – Part I: Mechanism," Medium.com
Walch, Angela, 2015, "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk," *NYU Journal of Legislation and Public Policy*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2579482##