THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

ALTERNATIVE CAPITAL MARKETS

#49 APRIL 2019

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

ALTERNATIVE MODELS

ALTERNATIVE RISKS

ALTERNATIVE MARKETS

DEAR READER,

Welcome to edition 49 of the Capco Institute Journal of Financial Transformation.

Disruptive business models are re-writing the rules of our industry, placing continuous pressure on financial institutions to innovate. Fresh thinking is needed to break away from business as usual, to embrace the more rewarding, although more complex alternatives.

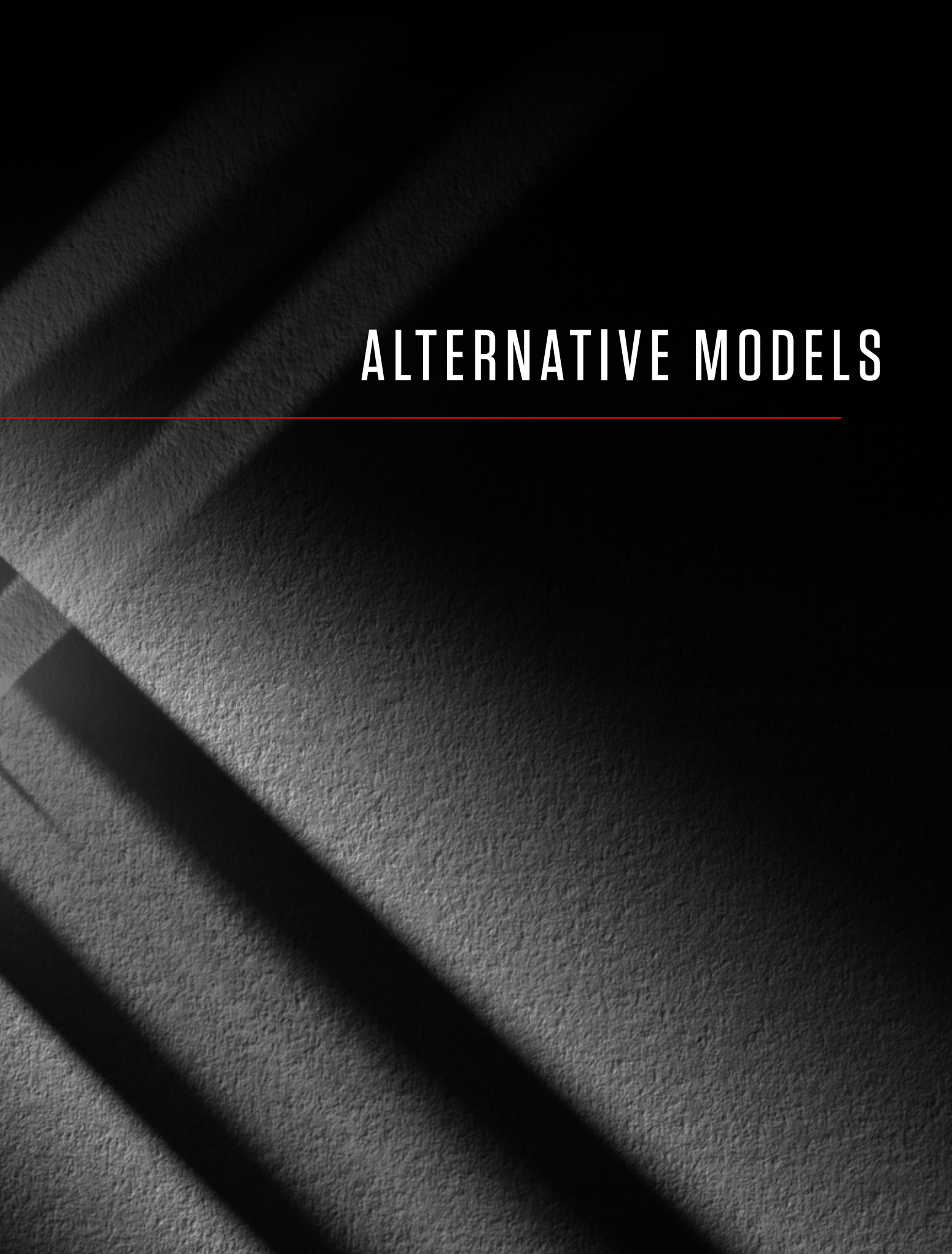
This edition of the Journal looks at new digital models across our industry. Industry leaders are reaching beyond digital enablement to focus on new emerging technologies to better serve their clients. Capital markets, for example, are witnessing the introduction of alternative reference rates and sources of funding for companies, including digital exchanges that deal with crypto-assets.

This edition also examines how these alternatives are creating new risks for firms, investors, and regulators, who are looking to improve investor protection, without changing functioning market structures.

I am confident that you will find the latest edition of the Capco Journal to be stimulating and an invaluable source of information and strategic insight. Our contributors are distinguished, world-class thinkers. Every Journal article has been prepared by acknowledged experts in their fields, and focuses on the practical application of these new models in the financial services industry.

As ever, we hope you enjoy the quality of the expertise and opinion on offer, and that it will help you leverage your innovation agenda to differentiate and accelerate growth.

Lance Levy, **Capco CEO**



ALTERNATIVE MODELS

BITCOINS, CRYPTOCURRENCIES, AND BLOCKCHAINS

JACK CLARK FRANCIS | Professor of Economics & Finance, Bernard Baruch College, CUNY

ABSTRACT

The U.S. has approximately 1,600 cryptocurrencies. No cryptocurrency is qualified to be called money because none has been designated by the U.S. government as being legal tender. Cryptocurrencies are called virtual currencies because they possess a few of the qualities of money. In this article, three issues related to cryptocurrencies are analyzed. First, bitcoins are considered, because they are the principal cryptocurrency. Second, an assessment of the processes the Federal Reserve and the central bank of Sweden are going through to evaluate the possibility of issuing some not-yet-fully-defined new form of electronic currency. Third, an examination of the viability of blockchain, which was introduced as an internal component of bitcoin, as a successful stand-alone technology.

1. INTRODUCTION

Bitcoin is the oldest digital currency in the U.S. It was created in 2009 by the mysterious Satoshi Nakamoto, whose true identity has never been verified.[1] Bitcoins are electronic entries in a public ledger that is verified frequently by people called bitcoin "miners." Bitcoins are the most popular of the hundreds of different cryptocurrencies that have recently sprung into existence. Bitcoins and about 1,600 other cryptocurrencies have become so popular that some people have suggested using them as money.

Economics textbooks explain that **money** is used as a means of **payment** that serves three essential purposes: a **medium of exchange**, a **unit of account**, and a **store of value**. Any verifiable record that performs these three functions qualifies to be called money. Thus far, it sounds like cryptocurrencies might qualify.

Most of the monies used around the world are **fiat currencies**. The U.S. dollar, British pound, the euro, and Japanese yen are well-known fiat currencies. **Fiat money** is not backed by any collateral. Cash, checks, and bank notes are also examples of fiat money. Fiat money has value only if the federal government declares it to be legal tender that can be used to make full and final payment of legal debts. The U.S. government has not declared that any cryptocurrency be **legal tender.** So, cryptocurrencies are not qualified to be used as a fiat currency and, thus, should never be called money.

In 2012, the European Central Bank defined a **virtual currency** to be "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community." In 2013, the U.S. Treasury Department went on to say a virtual currency is "a medium of exchange that operates like a currency in some environments but does not have all the attributes of real currency." Bitcoins meet these requirements.

Economics textbooks tell us that to function effectively, money should possess five qualities. First, it must be portable. Second, its value should be stable. More specifically, the value of money should not fluctuate randomly to any significant extent. Third, it must be

[1] A nine-page paper titled "Bitcoin: a peer-to-peer electronic cash system," by Satoshi Nakamoto in 2009 introduced and explained bitcoin and the initial blockchain database. See http://bitcoin.org/bitcoin.pdf. Also, see Berensten and Schar (2018a).

fungible, or freely interchangeable. Fourth, to prevent counterfeiting, it must be easily identifiable. Fifth, it must be a virtual currency. No cryptocurrency is free from significant random fluctuations, is fungible, and is sufficiently easy to identify to prevent counterfeiting. Once again, it seems that cryptocurrencies are not money. Furthermore, they cannot be called fiat currency because the U.S. government never declared they are legal tender. If cryptocurrencies are not money, not fiat currencies, and not legal tender, what are they? Cryptocurrencies are virtual currencies.

CoinMarketCap.com documents the existence of over 1,600 cryptocurrencies in the U.S. in 2018. Every one of these cryptocurrencies qualifies to be called a virtual currency. But, as mentioned above, none are qualified to be called money.

2. HISTORICAL DEVELOPMENT OF CRYPTOCURRENCIES

Before he passed away in 1814, a German philosopher, Johann Gottlieb Fichte, became a founding figure of the philosophical movement known as German idealism. Of particular interest here, Fichte developed a theory about the ethics of currency. Recently, another philosopher evaluated the extent to which Bitcoin meets Fichte's standards for a just and ethical currency. She concludes that "Bitcoin forsakes the general welfare and is, as such, unethical by Fichtean lights" [Scharding (2018)]. Several financial economists support this negative view of cryptocurrencies [Angel and McCabe (2015)].

Sweden recently voiced an interest in creating a "cryptocurrency" that is managed by its central bank and can be used by the public as legal tender in Sweden. This is a logical proposal about altering Sweden's money supply. It is incorrect to call Sweden's altered money supply a cryptocurrency because it has been and will continue to be controlled by a central bank. To be called a cryptocurrency, a currency must be independent from a central bank; it must be decentralized.

A high-ranking Federal Reserve official indicated that the U.S. government is not favorably disposed toward cryptocurrencies [Derby (2018)]. The Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) displayed similar inclinations [Eaglesham and Michaels (2018)].

The SEC recently rejected nine applications to list and trade various new exchange-traded funds (ETFs) on bitcoins (BTC) from several different applicants. One of these applications was submitted by ProShares in conjunction with the New York Stock Exchange's (NYSE) ETF exchange named Arca. The SEC also rejected other similar proposals that were to be traded on the Chicago Board of Options Exchange (CBOE). The SEC's rejection letter said the Exchange has not demonstrated "that its proposal is consistent with the requirements of the Exchange Act Section 6(b)(5), in particular, the requirement that a national securities exchange's rules must be designed to prevent fraudulent and manipulative acts and practices."

In a similar but different rejection letter, the SEC stated that the bitcoin futures markets lacked "significant size" and the resources needed "to prevent fraudulent and manipulative acts and practices," as evidenced by the fact that the exchange proposed sharing its surveillance responsibilities with ProShares Funds rather than handling the responsibility single-handedly.

The SEC's disapprovals repeated the concerns the agency had already articulated in its March 2017 initial rejection of a high-profile bitcoin ETF application from Cameron and Tyler Winklevoss. A few months later, the SEC issued a final rejection because, among other factors, the Winklevoss' petition claimed that crypto markets are "uniquely resistant to manipulation." In its rejection, the SEC said that "the record before the Commission does not support such a conclusion" [Huillet (2018)]. Several other opinions from high-ranking people in the U.S. government also voiced reservations about the cryptocurrency industry that is currently springing up in the U.S.

3. BITCOINS

Satoshi Nakamoto, the secretive founder of the Bitcoin Blockchain in 2009, worked actively in developing it until 2010. Since then, the bitcoin digital currency and the blockchain technology have continued developing together, as well as along separate paths of their own. These pathways are numerous, and some are so disparate that a complete review of the literature could fill a volume. Consequently, instead of a review of the literature, references are provided in the footnotes and as a list of references at the end of this paper.

3.1 Introduction to bitcoins

Bitcoin is an international decentralized digital virtual currency that works without a financial intermediary, central bank, or third party of any kind. All transactions are handled by direct communications between the counterparties. Each transaction can be verified within a network of nodes using thorough cryptographic records that are maintained in a publicly distributed electronic ledger book called the **bitcoin blockchain**. The bitcoin blockchain is a ledger that is shared, replicated, and frequently re-finalized in order to achieve a continuous consensus among all blockchain users.

From the user's perspective, the bitcoin blockchain is a database management system that facilitates the exchange of bitcoins for other currencies, products, and services. Each entry is cryptographically linked to the entries before and after it. A **bitcoin wallet** is a software that facilitates receiving, storing, and sending bitcoins. In 2017, researchers at the University of Cambridge estimated that there were between 2.9 and 5.8 million unique electronic wallets that contain cryptocurrencies, and most of these were bitcoin wallets [Hileman and Rauchs (2017)].

Manufacturing bitcoins is called **bitcoin mining**. In addition to being used to carry out transactions, 12.5 new bitcoins can also be used to pay any **miner** who completes the electronic computations needed to create a new investment transaction in a bitcoin blockchain.[2] Some people are attracted to bitcoin mining as a source of income.

During 2017 and 2018, bitcoin, ethereum, and ripple were among the most popular cryptocurrencies. These, along with hundreds of other cryptocurrencies, each comprise an independent **decentralized autonomous organization (DAO)**. Each DAO operates according to a set of rules that has been written into a computer program, and they compete against each other to gain investors.

Ethereum permits the construction of more sophisticated DAOs by using **smart contracts**. Smart contracts permit yes or no decisions to be made at some nodes before proceeding to the nodes that follow. Each of these DAOs generate a different price path for its cryptocurrency as they all compete to find speculators or investors who are sufficiently bullish about the currency to buy some.

Cryptocurrency prices are not based on the value of silver, gold, any other collateral, or any significant stream of income. Most, probably all, cryptocurrencies have no intrinsic value.[3] The prices of cryptocurrencies, digital tokens, and other crypto assets are based only on expectations about their future prices. Essentially, the buyer of a cryptocurrency is willing to buy it only because they believe it will sell at a higher price in the future.

The prices of bitcoins and other cryptocurrencies fluctuate freely over a wide range of values in an unconstrained manner. Between their creation in 2009 and 2012 the price of bitcoins fluctuated wildly at prices below U.S.$100. They were new and adequate information about them was unavailable. By 2013, their prices were varying in the U.S.$100 to U.S.$200 range. By 2016, the price bounced around between U.S.$300 and U.S.$600. In early 2017, the price passed through U.S.$1,000 and accelerated up to U.S.$7,500 by the end of that year. This rapid price inflation is not the only striking feature, the prices are also extremely volatile. The price of a bitcoin has sometimes zigzagged up and down by 10% in a single day. The price of bitcoins peaked at an all-time high of U.S.$19,783 in December 2017, and then quickly fell to U.S.$7,178 in February 2018. By early 2019, the prices of bitcoins had collapsed to between U.S.$3,600 and U.S.$3,900. The prices of stocks and bonds virtually never experience this much volatility because they are backed by tangible assets, well-defined streams of income, and significant business contracts.[4]

One reason that some people prefer to use bitcoins or other cryptocurrencies that are based on the blockchain technology is because these instruments are more difficult to hack or counterfeit than cryptocurrencies that are not based on the blockchain technology. The bitcoin blockchain ledger system records every bitcoin transaction electronically. Up-to-date electronic copies of this historical database are continuously circulated among those who own and trade bitcoins. These circulating electronic ledgers are large and, if the cryptocurrency is successful, grow continually. The large and growing

[2] If the creation of new bitcoins continues at the present rate, the number of bitcoins in existence will gradually approach a maximum ceiling value of 21 million bitcoins within the next few years. This ceiling exists because the rewards for bitcoin miners is halved whenever 210,000 blocks are completed. If all the owners of bitcoins in existence at that time can agree on it, it is theoretically possible (but not highly likely) to renegotiate a new bitcoin mining protocol that will permit bitcoin mining to proceed.

[3] The U.S. dollar, the euro, the Canadian dollar, the Swiss franc, and many other well-known currencies have no intrinsic value either. These fiat currencies are created by government decree.

[4] Three independent discussions of these points are: Popper (2018a), Russolillo (2018a), and Vigna and Michaels (2018).

ledger that accompanies a successful cryptocurrency makes it difficult to manipulate. The IBM Corporation and several other respected organizations foresee sufficient value in the blockchain electric ledger system to motivate them to develop and sell blockchain computer software for purposes that are unrelated to cryptocurrencies [Marr (2018)].

Although police can track every transaction through a bitcoin blockchain ledger, unfortunately the design of the blockchain system does not require the blockchain users to associate their identity with their bitcoin address (also known as their "hash," as explained below). This information gap has stymied more than one police investigation of bitcoin thefts [Popper (2018a)]. In other words, the blockchain ledger system does not make the cryptocurrencies that use them as safe as many people think.

> "The digital-currency exchanges bear little resemblance to the well-financed, well-regulated places where stock and bond investors trade and where people do their banking."

3.2 Advantages of cryptocurrencies over the U.S. banking system

Those who obtain cash by conducting initial coin offerings (ICOs), such as owners of cryptocurrency exchanges, owners of cryptocurrencies, and others that might benefit from cryptocurrency trading, tend to argue that cryptocurrency markets are superior to the U.S. financial system for the following reasons:

- **Simplicity:** no financial intermediaries or other third parties facilitate trading in cryptocurrencies. All counterparties only deal directly with each other.
- **Privacy:** a blockchain ledger contains a different node for each different person or organization. Each of these nodes is represented by a long and complicated alpha-numeric called a "**hash**." A hash is a computer function that converts alpha-numeric input into an encrypted output of a fixed length. The counterparties in a bitcoin transaction never learn the name, address, or anything else about each other. Thus, all bitcoin transactions and all bitcoin users remain anonymous. This complete privacy attracts criminals and scares away law-abiding investors who would like to have their transactions audited.
- **Inexpensive:** the bitcoin blockchain is costly to maintain, but it is much cheaper to operate than a monetary system made up of numerous commercial banks and a central bank that verifies every transaction and stands ready to correct errors.
- **Robust:** no central point or any system relevant nodes exist that could cause the blockchain system to collapse.

The bitcoin blockchain system verifies transactions by operating as a **consensus building mechanism**. Anyone who wishes may download the bitcoin blockchain software and become a new bitcoin miner. Bitcoin miners collect one or more pending bitcoin transactions, verify their legitimacy, and assemble them into what is called a **block candidate**. If a bitcoin miner can convince all the existing network participants to add their new block candidate to the latest existing version of the bitcoin blockchain, that bitcoin miner will receive a fixed **block reward** payment of 12.5 new bitcoins. Although some cryptocurrency traders hope to earn their living by mining bitcoins, not a large number seem to be successful in that endeavor.

One of the world's largest cryptocurrency miners is a Hong Kong based company named Bitmain Technologies Ltd. In 2018, Bitmain was discussing having an initial public offering (IPO) in Hong Kong, rather than having an initial coin offering (ICO) [Russolillo (2018b)]. Bitmain's major competitors include two other Hong Kong companies, Canaan Inc. and Ebang International Holdings Inc., and a company named Bitfury in the country of Georgia [Alderman (2019)].

Bitcoin miners that successfully process a block of transactions are paid the sum of the block reward and the **transaction fees** that are attached to each transaction in the block. The size of the block reward is set by the bitcoin protocol and cannot depend on anything the miners do. It is a different story for the transaction fees, as they are set by the investors who send the transactions to the miners. The tradeoff the investors face is simple; the higher the fee you offer, the faster the miners will process your transaction. The essence of this economic competition is that the miners must not only participate in a hashing race, but they must also compete to process those that have the highest transaction fees attached.

The idealistic promise of blockchain is, essentially, to replace a reputation-based consensus between regulated banks with a trustless algorithm that is free from human foibles. Unfortunately, this promise of blockchain overlooks standard technology like Microsoft's SQL Server, which is a well-known computer software that has been achieving reputation-based consensuses quickly and efficiently for decades.[5]

3.3 The scaling problem

One of the most stubborn problems facing bitcoin, blockchain, and every other cryptocurrency is the slow speed at which they can handle transactions. For example, when more than a few different computer systems are mining bitcoins at the same time, there are limits on how many transactions they can share and store at the same time. This is called the **scaling problem**. More specifically, bitcoin can handle no more than about seven transactions per second. Ethereum is faster than bitcoin; it can handle about fourteen transactions per second. However, no cryptocurrency comes close to the 50,000 transactions per second that VISA handles routinely. This technical constraint seriously limits the potential growth of all cryptocurrencies [Sorkin (2018), Vigna (2018a)].

Law et al. (1997) concluded that the potential risks in electronic commerce are magnified when the users are anonymous. In particular, they point out that false advertising and fraud are encouraged when anonymity is widespread. These problems are evident in the cryptocurrency industry.

Longfin Corporation, an alleged cryptocurrency firm, provides a good case study of such risks. LongFin Corporation, whose shares were listed on Nasdaq in December 2017, saw its share price skyrocket after launch, such that within weeks the firm had a market value of U.S.$5.5 billion. However, LongFin was headquartered in a shared Manhattan office that had only three desks and no computer when the Wall Street Journal investigated the office. Much of LongFin's fast gain occurred on December 18, 2017, when its share price rose over 500% after acquiring Ziddu, a smaller firm focused on blockchain-technology solutions and micro-lending. But LongFin's stock price then went on a downhill roller coaster ride after the Wall Street Journal reported that LongFin had failed to disclose important information and had misstated some facts. LongFin's founder and CEO, Venkat Meenavalli, had issued over two million shares to three acquaintances as payment for their consulting services. Then, after the corporation's share price had risen sharply, those individuals illegally sold large blocks of their new shares even though the shares were not registered for sale. In response, the SEC obtained a court order to freeze U.S.$27 million of the sales proceeds to prevent the funds from being transferred outside the U.S. The websites for LongFin and Ziddu contained enticing promises, but no historical or pro forma financial statements [Back and Eaglesham (2018)].

4. CRYPTOCURRENCY EXCHANGES

Risks associated with investing in cryptocurrencies extend beyond the coins to include the markets where the cryptocurrencies are traded. Within the U.S., cryptocurrencies are bought and sold through approximately 190 cryptocurrency exchanges, which can be tracked through coinmarket-cap.com. Many other cryptocurrency exchanges exist outside of the U.S. Very few of these digital-currency exchanges are regulated by any laws or government agencies. Cryptocurrency traders who go to a cryptocurrency exchange expecting to find convenience and safety will not usually find what they were expecting. The digital-currency exchanges bear little resemblance to the well-financed, well-regulated places where stock and bond investors trade and where people do their banking. Cryptocurrency exchanges match buyers and sellers for a fee, and if the trader desires, stores the trader's coins in that cryptocurrency exchange's electronic wallet.

Most cryptocurrency exchanges are modest websites that sprung up during 2016-2017. Cryptocurrency hackers pursue cryptocurrency traders, electronic wallets, and cryptocurrency exchanges. Some of the largest cryptocurrency exchanges have lost millions of dollars of their clients' money. The following losses, for example, have been reported by cryptocurrency exchanges: Youbit lost U.S.$35 million in 2017, DAO lost U.S.$55 million in 2016, Bitfinex lost U.S.$77 million in 2017, BitGrail lost U.S.$170 million in 2018, Mt. Gox lost U.S.$450 million in 2014, and Coincheck lost U.S.$534 million in 2018 [Vigna (2018b, 2019a)]. Initially, there were no reports of any cryptocurrency exchanges reimbursing their customers for their losses. However, in March 2018, Coincheck set a new precedent by spending hundreds of millions of dollars

[5] Microsoft's SQL Server is a relational database management system (RDBMS) that supports a wide variety of transaction processing, business intelligence, and analytic applications in corporate IT environments. Oracle's Database and IBM's DB2 are two other competing database management technologies that are also popular because they have been performing very well for years.

to compensate 260,000 of its customers whose currency holdings had been stolen while held in trust by Coincheck [Bhattacharya and Russolillo (2018)]. Similar refunds by the other cryptocurrency exchanges have not yet been reported.

Most cryptocurrencies are not designed to be tax friendly. The cryptocurrency exchanges are no better. Some "fly-by-night cryptocurrency exchanges" have vanished suddenly, wiping out all records of the clients' taxable transactions [Roose (2018), Vigna (2019b)].

Nothing requires any cryptocurrency exchange to submit to any regulations, and most of them do not submit to any regulations. However, a few ethical cryptocurrency exchanges exist. For example, Cameron and Tyler Winklevoss's Gemini Trust, which owns and operates Gemini, Coinbase's GDAX, and Japan's BitFlyer have voluntarily registered with the New York State's Department of Financial Services. This New York state agency seeks to detect and prevent fraud and market manipulation. In addition, the few cryptocurrency exchanges that also trade stocks, options, or futures within the U.S. come under federal legislation governing trading in those securities. Stock trading is governed by the SEC, futures trading is governed by the CFTC, and options trading is governed by both the SEC and the CFTC. Many states have also Secretaries of State that enforce securities trading laws. However, few cryptocurrency exchanges are legally required to submit to strict federal standards to prevent fraud, provide fair access, and to regulate securities trading [Michaels (2018)]. The few unusually ethical cryptocurrency exchanges discussed in this paragraph provide operations for cryptocurrency traders that are less risky than the typical cryptocurrency exchange, but none are likely to be as safe as the thousands of commercial banks that are governed by and audited periodically by the Federal Reserve, Office of the Comptroller of the Currency, and, in some states, the Secretary of State.

5. MOB PSYCHOLOGY

Mob psychology is a branch of social psychology that deals with the psychology of crowds and the psychologies of the individuals that comprise those crowds. Mob psychologists have highlighted three commonalities that characterize the members of a frenzied crowd: (1) members of the crowd have the impression that everyone in the crowd has the same feelings they do; (2) each individual in a crowd has the erroneous feeling that they are not personally responsible for the actions of the crowd in which they are a participant; and (3) the intensity of the two previous beliefs increases with the size of the crowd.

Cryptocurrencies are not backed by any tangible assets, and they are traded in unregulated markets. Without any tangible price determinants, the unbridled forces of supply and demand determine cryptocurrency prices. Supply and demand are largely determined by the feelings and emotions of the crowd of people trading the cryptocurrency. In other words, the emotions and feelings of a group of cryptocurrency traders determines the market price of a cryptocurrency. This is not a rational economic process. Mob psychology explains more about the behavior of cryptocurrency traders than economics. People conducting initial coin offerings (ICOs) can and have enriched themselves by selling cryptocurrencies to not-so-clever cryptocurrency buyers who have unrealistic expectations about getting rich [Popper and Lee (2018), Economist (2018)].

6. BUSINESS OPPORTUNITIES IN THE CRYPTOCURRENCY INDUSTRY

The cryptocurrency industry provides many profitable business opportunities. Unfortunately, many of these activities are unethical, illegal, and/or dangerous. Harmful activities that are facilitated by the cryptocurrency industry include the following:

Fraudulent divorces: dividing the family wealth is a bone of contention in many divorces. This source of contention can be diminished if one or both spouses secretly hides wealth in a cryptocurrency prior to entering the divorce process. Such divorce fraud would be difficult to detect because anonymity is a characteristic of cryptocurrencies.

Tax evasion: some cryptocurrency transactions avoid the use of U.S. dollars by swapping cryptocurrency for goods and/or services instead of selling them for money. Cryptocurrency transactions can be opened in one country and liquidated in another country. And, some "fly-by-night cryptocurrency exchanges" have vanished suddenly, which wipes out all records of the clients' taxable transactions [Roose (2018)]. If appropriate planning precedes these transactions, they can be conducted without the knowledge of the U.S. Government's Internal Revenue Service (IRS). The existence of cryptocurrencies facilitates such illegal tax evasion schemes.

Money laundering: some drug, gambling, and prostitution rings, and some cryptocurrency manipulators generate cash flows that criminals want to conceal from the police and IRS. A cryptocurrency can be purchased with "dirty money" and liquidated later to obtain "clean money." These simple transactions facilitate and encourage criminal activities by laundering criminals' ill-gotten gains [Michaels et al. (2018)].

ICOs: an ICO is an online crowdfunding technique used to introduce a new cryptocurrency to the market. A new cryptocurrency was born almost every day during 2017. The founders of many of these ICOs create digital tokens that are like bitcoins and sell them to the public before they have even developed a clear plan for a product. When buyers pay for their new digital tokens those transactions provide immediate income for the ICOs founders. Unfortunately, the cryptocurrencies purchased with U.S. dollars are not as liquid as the U.S. dollars that financed the purchase. Each transaction involves fees that are more expensive than the commissions charged by U.S. government registered securities brokers. Furthermore, large random fluctuations in the conversion rate between a cryptocurrency and U.S. dollars creates substantial additional risk. Finally, not all cryptocurrency promoters are truth tellers.[6]

Valueless investments: during 2017, the market prices of many cryptocurrencies shot up and then fell by half while stock market investors enjoyed a bull market throughout that year. The random price volatility of virtual currencies occurs because the prices of cryptocurrencies and digital tokens are based on irrational supply and demand forces rather than on tangible collateral, contractual income, or meaningful contracts. Some cryptocurrencies become worthless because the ICO founder was a criminal who spent their investors' money selfishly on themselves. Furthermore, even if the investors' money remains invested in the cryptocurrency, mob psychology is a better way to determine cryptocurrency prices than rational economic analysis [Vigna (2018c), Andolfatto and Spewak (2019)].

Cryptocurrency exchanges: most cryptocurrencies are not traded on organized security exchanges that are supervised by the SEC or any other reputable governmental body. Nearly all cryptocurrencies are traded over-the-counter at opaque and unregulated exchanges that are not well-protected from cyber-attacks. In 2016, for example, the Commodity Futures Trading Commission (CFTC) reached a U.S.$75,000 settlement against a cryptocurrency exchange named Bitfinex for offering leveraged trading without the CFTC's advanced approval [Vigna and Michaels (2018)]. Furthermore, in 2018, computer programs written to manipulate the prices

[6] For example, the SEC halted a Dallas-based ICO by AriseBank in 2018 because the advertisement made fraudulent claims, https://bit.ly/2DVU3An

of cryptocurrencies in their unregulated markets were criticized by the office of New York Attorney General Barbara D. Underwood [Vigna and Osipovich (2018)].

Theft: it turns out that the well-publicized electronic blockchain ledger system that is supposed to make bitcoin burglarproof can, unfortunately, attract thieves instead of discouraging them. While police can track every transaction through Bitcoin's blockchain ledger, the design of the blockchain system permits its users to omit providing any information about themselves or their address. This information gap has made some bitcoin thefts unsolvable [Popper (2018b)]. More specifically, the police may be able to use the blockchain ledger system to track transactions to the criminal's computer but if the criminals are using someone else's computer the task becomes impossible.

Counterfeiting: unlike the U.S. dollar, most cryptocurrencies are easy to counterfeit. Section 8.1 below provides facts about how and why cryptocurrencies attract counterfeiters.

None of the activities listed above earn large tax revenues for the government, enrich ethical business enterprises, increase commercial activity, or provide transparency for the cryptocurrency's investors. Nevertheless, some U.S. futures exchanges and options exchanges are creating derivatives on bitcoins that increase their liquidity and enable the not-so-liquid cryptocurrency markets to become more liquid by trading derivatives based on them [Rubin (2018)]. Different nations are dealing with cryptocurrencies in different ways.

7. THE ACCEPTANCE OF CRYPTOCURRENCIES BY NATIONAL GOVERNMENTS

Consider a few national governments' vastly different assessments of cryptocurrencies. By 2018, China, Bolivia, Lebanon, and Iceland banned cryptocurrencies. India enacted restrictions on cryptocurrency transactions [Russolillo and Hunter (2018)]. In contrast, Canada recognized bitcoins as a form of barter. And, Japan and Australia both defined bitcoins to be legal tender.

Sweden's central bank, the Riksbank, is preparing to switch to a new digital currency called the e-krona. The e-krona will perform all the tasks of the krona but in a digitized fashion [Alderman (2018)]. Sweden welcomed bitcoins to compete with the e-krona. The e-krona resembles a new electronic currency that Berensten and Schar (2018a), two Federal Reserve research economists, suggest for the U.S.

In 2018, a group of scheming entrepreneurs met in Puerto Rico to establish a cryptocurrency industry for that U.S. territory. Puerto Rico offers the unparalleled tax incentives of no federal income taxes, no federal capital gains taxes, low local taxes, and no requirement to be an American citizen to obtain these valuable tax benefits. A member of this group, Mr. Brock Pierce, who has been sued for fraud in the past [Mora et al. (2014)], established himself as a director of the Bitcoin Foundation and co-founded a block-chain-for-business company named Block.One. Block.One had an ICO that brought in U.S.$1.5 billion during several months of 2017 and 2018. This U.S.$1.5 billion may become personal income for Mr. Brock Pierce or it may be invested in the cryptocurrency. The privacy and anonymity that characterize the cryptocurrency industry make it extremely difficult for the investors to find out what happened to their investments [Bowles (2018)]. As of yet, no reactions from the U.S. or Puerto Rican authorities have been reported.

8. WILL HISTORY REPEAT ITSELF?

The preceding list of unethical and illegal activities is troubling. Bitcoins were first launched in the U.S. in 2009. Since then, the U.S. has not developed any new laws to govern them. To understand the implications of the cryptocurrency industry for the U.S., this section reviews the history of free banking in the U.S. from 1836 to 1862. The next section discusses a well-documented historical crisis in the U.S. financial system that may unfold similarly in the U.S. cryptocurrency industry.

8.1 Lessons from the "free banking era" of 1837-1862

A total of 1,600 state-chartered private banks were issuing their own unique paper money in the U.S. in 1836.[7] The money issued by each bank had a special color and a unique design. Furthermore, every denomination of each bank's money also had a different color and a distinctive design. As a result, over 30,000 varieties of paper money, called bank notes, were issued by state banks with a minimum of bank regulation. The profusion of color and design differences in this paper money created

[7] Video entitled: U.S. money history, U.S. Treasury Department, Bureau of Engraving and Printing, viewed March 2018

lucrative opportunities for counterfeiters to profit. It was estimated that one-third of all the money in circulation was counterfeit in 1836.[8] This was the beginning of what the economic history books call the "free banking era" – it began in 1837 and lasted until 1862. During this period, hundreds of loosely regulated state-chartered banks could legally issue bank notes (that is, their own unique paper money) that was backed by the bank's gold and silver coin deposits. But few regulators checked to see if the issuing banks actually owned the collateral that was supposed to support the value of the money they issued. These state banks were also permitted to offer checking account services.

During the "free banking era," each state was allowed to regulate their own banks' reserve requirements, interest rates for loans and deposits, and the required capital reserve ratio.[9] This largely unregulated situation grew even riskier in 1837 when the Michigan Act authorized a Michigan state bank charter for any U.S. bank that could fulfill the Michigan Act's reserve requirements. Unfortunately, Michigan's state legislature provided inadequate resources to verify that the rapidly growing number of banks chartered in Michigan were meeting the state's reserve requirements. As a result, many thinly capitalized non-Michigan bankers found Michigan's bank chartering system to be an attractive launch pad. The Michigan Act made creating unstable banks easier in all states and lowered state supervision in the states that allowed entry by banks chartered in Michigan. As a result of these remarkably loose bank regulations, the real value of a bank note was often lower than its face value. And, to make the system even more troublesome, the day-to-day news about each issuing bank's financial strength caused continuously fluctuating and always negotiable exchange rates between the bank notes issued by different banks. For example, it might take three $1 bills printed by a small-town bank to buy two $1 bills issued by a nearby large city bank. Situations like this meant that if someone traveled from a small town to a large city they might have to take 50% additional small-town cash because of the unfavorable exchange rate differences.

Between 1837 and 1862, the free banking era shrunk the length of the average bank's life to a mere five years. About half of the banks failed, and about a third went out of business because they could not redeem their notes for gold and silver as they had advertised. The widespread fraud and uncertainty that resulted from inadequate bank regulation depressed the nation's economy and slowed economic growth between 1837 and 1862.

8.2 The beginning of the cryptocurrency industry, 2016-2018

The National Banking Act of 1863 brought an end to the Free Banking Era of 1837-1862. Among other things, the National Banking Act created:

- A system of national banks that had higher reserve standards and more ethical business practices than the numerous state banks, many of which were chartered in Michigan.
- A uniform national currency, which required all national banks to accept the national currency at its full par (face) value.
- The Comptroller of the Currency. The money printed by the Comptroller of the Currency was manufactured using uniformly high quality standards that greatly reduced the widespread use of cheaply printed counterfeit money.

Not surprisingly, some problems like those the U.S. banking industry experienced between 1837 and 1862 are found in the cryptocurrency markets of 2019.

Between 2016 and 2018, the U.S. cryptocurrency industry added over 1,000 new cryptocurrencies without any government regulations to guide the ICOs. These new cryptocurrencies operate under less regulation than the under-regulated banking industry during the free banking era of 1837 to 1862. Section 6 above lists eight illegal activities that offer profitable opportunities that the unregulated cryptocurrency industry facilitates.

9. MONETARY ECONOMICS

Although virtually anyone can become a bitcoin miner and create new bitcoins by simply downloading the software and working within the system, this process of mining is not working out as well as planned [Cong et al. (2018)]. In fact, a small number of large miners with expensive high-speed hardware sprung up in 2018 and they tend to dominate bitcoin mining. Creating cryptocurrencies in these somewhat centralized "bitfarms" threatens to further restrict the transparency of the cryptocurrency industry.

[8] Video entitled: A history of central banking in the U.S., Federal Reserve Bank of Minneapolis, viewed March 2018

[9] Video entitled: History of central banking in the United States, Wikipedia.org, viewed in March 2018

9.1 Contrasting different forms of currency

Several monetary economic issues can be addressed by contrasting the characteristics of various types of money.

9.1.1 CASH

U.S. dollars have an economic value that is inseparable from the coin or the note. Whoever has physical possession of the cash owns the corresponding value; no third party is keeping track of who is holding the cash. Cash money circulates freely and conveniently with no need for records documenting each transaction. Using cash creates no credit relationships. Furthermore, cash spenders do not need to open a bank account nor seek any permissions and, if desired, they can even remain anonymous. A central bank and the federal government's U.S. Treasury are the monopolistic issuers of cash. Cash is a productive asset that is used to increase the nation's income, and the demand for cash holdings is growing [Bates et al. (2009, 2018)]. The disadvantage of using cash is that the buyer and seller must both be present to complete a transaction. Consequently, very few cash transactions involving large sums can occur between distant counterparties.

9.1.2 DIGITAL CASH

Digital cash provides all the advantages of cash without the disadvantages. In addition, it can be copied and transferred electronically. Unfortunately, copying and transferring digital cash electronically facilitates fraud and thievery, which is lightly referred to as the "double spending problem" in the cryptocurrency industry.

9.1.3 COMMODITY MONEY

Gold and silver are popular examples of commodity money. Commodity money has most of the same characteristics as cash, with the main exception being how it is created. Most governments do not issue significant amounts of gold or silver. Miners must either work or pay cash to obtain gold, silver, or some other form of commodity money.

9.1.4 BANK DEPOSITS

Bank deposits exist in an accounting system instead of as tangible cash. Bank deposits are transferred by writing paper checks, with credit cards, and through various online transactions. Commercial banks compete to obtain bank deposits from both short-term depositors and long-term savers. Commercial banks and central banks keep records of every bank deposit and transfer. These financial intermediaries work to prevent fraud and they correct any errors soon after they are detected. In particular, bank deposits are very useful for paying large debts to distant creditors. Unfortunately, bank deposits are vulnerable to electronic failures, hackers, and incompetent politicians that can manage their nation's monetary system capriciously.

9.1.5 BITCOINS

Bitcoins are virtual monetary units. One bitcoin unit can be divided into 100 million **Satoshis**. Bitcoins do not circulate freely and conveniently like cash. And, unlike bank deposits, bitcoins cannot be used to pay bills unless a gracious counterparty agrees in advance to accept them as full and final payment. Bitcoins cannot pass through the Federal Reserve or any other audited centralizing system. Bitcoins are a virtual currency that can only be transferred through about 190 decentralized cryptocurrency exchanges in the U.S. These cryptocurrency exchanges are not transparent and do not operate for free, but they are significantly simpler and less costly to maintain than a central bank and the accompanying system of commercial banks that must undergo periodic audits. The bitcoin blockchain verifies transactions by using a consensus building mechanism that is operated and maintained by bitcoin miners. The problem that seems to be emerging with this consensus building mechanism is that a small number of wealthy bitcoin miners in China seem to be gaining control of the bitcoin mining business by buying larger computer systems and more electricity than most bitcoin miners can afford [Berensten and Schar (2018a)].

9.2 Acceptance of bitcoins

Bitcoins are a virtual currency that is managed by a decentralized network that was inconvenient to use for paying bills during 2016 through 2018. But, while most businesses still refuse to deal in cryptocurrencies, a slightly larger number of businesses adapted to cryptocurrencies in 2018. And in 2018, some cryptocurrency exchanges began actively trading one cryptocurrency for another at fluctuating exchange ratios. If the liquidity of bitcoins continues to increase (which seems possible), this development has the potential to disrupt the current payments infrastructure and financial system in the U.S. The questions that arise here are: can bitcoins and/or some other cryptocurrency become sufficiently liquid to displace cash money and bank deposits in the U.S.

financial system? Are such changes helpful or harmful to the U.S. economy?

10. DISCUSSIONS OF A NEW FEDERAL RESERVE ELECTRONIC MONEY SYSTEM

Two Federal Reserve research economists, Aleksander Berensten and Fabian Schar, proposed improvements in the current U.S. monetary system that will, among other things, prevent the kind of problems that arise with the 1,600 decentralized cryptocurrencies. Berensten and Schar suggest the Federal Reserve develop and operate a new form of central bank controlled electronic money that is based on the U.S. dollar [Berensten and Schar (2018b)]. Let us call this hypothetical new currency the e-dollar.

The Federal Reserve, or, the Fed, has been transferring money between the twelve Federal Reserve Banks in the U.S. for decades to prevent local money panics from developing. Berensten and Schar (2018b) suggest extending the present monetary system to become a larger and more centralized bank electronic money system that provides more services. They suggest enlarging the Fed's current interbank electronic system so that every adult, business, and governmental agency could have its own private bank account at the Fed. The existing 6,500 centralized commercial banks and the 1,600 decentralized cryptocurrencies could all continue to operate beside one another and compete with the Fed's hypothetical new e-dollar system.

The suggestion by Berensten and Schar (2018b) can be implemented in many different forms. For example, the central bank electronic money system could either be secretive and restrictive or transparent and available to everyone. More specifically, the system could handle direct transfers between individuals, like private payments of cash, or, alternatively, every transaction could be routed through something like the Federal Reserve check clearing system, which presently clears 50 million checks per day from banks around the world. If all the proposed new electronic bank accounts at the Fed were identified by a 50-digit alpha-numeric hashtag instead of the account owner's name, then everyone's privacy could be maintained and each transfer would resemble an anonymous cash payment that took place secretly. Alternatively, every transaction could carry the payer's and the recipient's names, and every transaction could be recorded electronically so that all transactions would be cheap and easy to audit as often as desired. If the Fed acts as a check-clearing middleman between electronic check writers and electronic check recipients, then the e-dollar would be a centralized currency rather than a decentralized cryptocurrency that encourages illegal behavior by carrying out undisclosed transactions that cannot be audited.[10]

The new central bank electronic money system currently under discussion by research economists at the Fed could be designed to be very useful and convenient. To encourage competition between the 1,600 cryptocurrencies, the existing centralized banking system, and the Fed's hypothetical e-dollar system, people could be allowed to ignore the Fed's new system and bank through their present commercial bank with paper checks and/or maintain a cryptocurrency account, if they wished. Thus, for instance, one individual person or company could have three separate accounts at a cryptocurrency organization, one of the traditional commercial banks that exist today, and the Fed's new electronic banking system. Economic theory suggests that this competition would most likely foster improvements in all three systems.

The Fed would probably pay interest on its millions of new e-bank accounts. And as one of its monetary policy tools, the Fed could adjust this one most-important interest rate from time to time. If a new central bank electronic money system paid interest to its depositors, the same interest rate should be paid to every account to keep from getting the nation's monetary policies (like controlling the level of interest rates) entangled with the nation's fiscal policies (such as the enforcing the structure of the federal income taxes). If the Fed paid a uniform single interest rate on every Fed account, the level of that interest rate would affect the demand for the new accounts at the Fed, the amount of cash held in every bank account in the U.S., and the prices of government bonds. This hypothetical introduction of numerous new interest-bearing checking accounts would strengthen the linkages between the Fed's monetary policies and every aspect of the U.S. economy [Halaburda and Haeringer (2018)].

[10] Hayek's (1976) views about concurrent currencies become relevant when considering how the current system of thousands of U.S. commercial banks, hundreds of cryptocurrencies, and the contemplated e-dollar system might compete with each other.

11. DIFFERENT BLOCKCHAIN APPLICATIONS

Bitcoin and ethereum are two competing cryptocurrencies that both use the blockchain technology. However, not all cryptocurrencies employ the blockchain technology. If we take an even broader perspective, we can find other uses for the blockchain technology that are unrelated to cryptocurrencies. For instance, IBM, Microsoft, and other software manufacturers sell blockchain software for non-cryptocurrency applications. Stated differently, blockchains and cryptocurrencies are separate products that can be purchased either separately or together. Some of these new non-cryptocurrency applications seem to be blossoming.

11.1 The IBM Corporation

IBM's Blockchain group has 1,500 employees. During the past 25 years IBM has worked with over 500 different clients to create and install blockchain technology in their organizations. One ambitious Blockchain project IBM has undertaken recently was the creation of a European trade consortium named we.trade. IBM helped Deutsche Bank, HSBC, and seven other banks go live with we.trade in June 2018 [Salzman (2018a)]. Similarly, IBM is working with Maersk to develop a blockchain named TradeLens that tracks important shipping documents through over 100 different organizations. Buyers, sellers, shipping companies, port authorities, and other participants are working together to develop TradeLens into an effective joint decision-making platform.

11.2 Microsoft

After Microsoft developed the well-known videogame console named Xbox, it built a blockchain that calculates the royalties due to Xbox game publishers almost instantly. Before this blockchain application was completed, Microsoft's Xbox publishers had to wait 45 days past the end of the month to find out how much they earned from the sales of their game. Working with Accenture and Mercy Corps, Microsoft built a blockchain system called ID2020 that can record data for up to 1.1 billion people. ID2020 can imbed identity documents and biometric information like fingerprints and retina scans into software that is both immutable and encrypted. The state of West Virginia used similar blockchain software to facilitate voting by veterans residing in foreign countries.

11.3 Medical records

A new medical records company named MedRec is an MIT-backed initiative designed to digitize family's medical records. Blockchain creates a family medical history that can be passed down from generation

to generation. It uses ethereum blockchain's smart contracts to execute scripts on the blockchain. MedRec uses metadata to protect the integrity of the data but still allows records to be accessed securely by patients across different providers.[11]

Despite such initiatives to apply blockchain in the non-cryptocurrency space, Gartner group's survey of chief information officers found that only 3.3% had deployed blockchain software [Salzman (2018b)].

12. CONCLUSION

A respected 19th century German philosopher, Johann G. Fichte, advocated that the nations of the world abolish world currencies that can be traded between nations and, instead, work to develop national currencies that can only be traded between citizens and within national borders. Fichte argued that using national currencies ensures that the currency's value is more likely to remain constant and that will help the nation's citizens maintain a level of welfare that will never decline: "All individuals are guaranteed that their present state of existence will continue into the future, and, through this, the whole is guaranteed its own quiet, steady continuity" [Fichte (2012)]. Fichte went on to propose a systematic account of the ethics for currencies. Professor Tobey Scharding employs Fichte's ethical philosophy to show that bitcoin forsakes the general welfare and is unethical [Scharding (2018)]. Following the philosophical suggestions of Fichte and Scharding, this paper reviews recent developments to show that the privacy provided by bitcoin and the other cryptocurrencies attracts criminals and facilitates illegal activities that are counterproductive to the maintenance of a peace-seeking, prosperous society. These findings have been supported by economics professors who take cognizance of the ethics involved in a nation's monetary system [Gray (2003), Angel and McCabe (2015)].

While the blockchain technology is not experiencing the ethics problems that are crippling the cryptocurrency industry, it is developing at only a modest pace. The blockchain technology has yet to experience a breakthrough of major proportions.

[11] For more information see: https://bit.ly/2Ns8rlv

REFERENCES

Alderman, L., 2018, "Sweden's push to get rid of cash has some saying, 'not so fast'," New York Times, November 21, https://nyti.ms/2S2WK6r

Alderman, L., 2019, "Despite bitcoin's dive, a former Soviet Republic is still betting big on it," New York Times, January 22, https://nyti.ms/2Rbuw8K

Andolfatto, D., 2018, "Blockchain: what it is, what it does, and why you probably do not need one," Review, Federal Reserve Bank of St. Louis100:2, 87-95

Andolfatto, D., and A. Spewak, 2019, "Whither the price of bitcoin?," Economic Synopses, Number 1, https://bit.ly/2SxeLi6

Angel, J. J., and J. McCabe, 2015, "The ethics of payments: paper, plastic or bitcoin," Journal of Business Ethics 132:3, 603-611

Back, A., and Eaglesham, J., 2018, "SEC accuses cryptocurrency company Longfin of securities violations," Wall Street Journal, April 6, https://on.wsj.com/2EaJWqs

Bates, T. W., C-H. Chang, and J. D. Chi, 2018, "Why has the value of cash increased over time?" Journal of Financial and Quantitative Analysis 53:2, 749-787

Bates, T. W., K. Kahle, and R. Stulz, 2009, "Why do U.S. firms hold so much more cash than they used to?" Journal of Finance 64, 1985-2021

Berensten, A., and F. Schar, 2018a, "A short introduction to the world of cryptocurrencies," Review, Federal Reserve Bank of St. Louis 100:1, 1-16

Berensten, A., and F. Schar, 2018b, "The case for central bank electronic money and the non-case for central bank cryptocurrencies," Review, Federal Reserve Bank of St. Louis 100:2, 97-106

Bhattacharya, S., and S. Russolillo, 2018, "Coincheck, roiled by hack, might have found its white knight," Wall Street Journal, April 3, https://on.wsj.com/2GEGuWS

Bowles, N., 2018, "Making a crypto utopia in Puerto Rico," New York Times, February 2, https://nyti.ms/2FEwOl3

Carlson, M., and D. C. Wheelock, 2018, "Furnishing an 'elastic currency': the founding of the Fed and the liquidity of the U.S. banking system," Review, Federal Reserve Bank of St. Louis 100:1, 17-44

Cong, L. W., Z. He, and J. Li, 2018, "Decentralized mining in centralized pools," Mimeographed manuscript, April 10, 1-34

Derby, M. S., 2018, "Fed's Dudley warns on dangerous 'speculative mania' around cryptocurrencies," Wall Street Journal, February 22, https://on.wsj.com/2sPrtMs

Eaglesham, J., and D. Michaels, 2018, "Crypto craze drew them in; fraud, in many cases, emptied their pockets," Wall Street Journal, December 26, https://on.wsj.com/2T8AAjy

Economist, 2018, "Initial coin offerings have become big business," September 1, https://econ.st/2DA8WpE

Fichte, J. G., 2012, by A. C. Adler, in Nakhimovsky, I., The closed commercial state: perpetual peace and commercial society from Rousseau to Fichte, Princeton University Press

Gray, R. T., 2003, "Economic romanticism: monetary nationalism in Johann Gottlieb Fichte and Adam Mueller," Eighteenth-Century Studies 36:4, 535-557

Haeringer, G., and H. Halaburda, 2018, "Bitcoin: a revolution?," July 8, SSRN, https://bit.ly/2X0xbWO

Halaburda, H., and G. Haeringer, 2018, "Bitcoin and blockchain: what we know and what questions are still open," SSRN, https://bit.ly/2GE2ils

Hayek, F. A., 2976, Denationalism of money, The Institute of Economic Affairs

Hileman, G., and M. Rauchs, 2017, "Global cryptocurrency benchmarking study," Cambridge University, https://bit.ly/2o3zHcW

Huillet, M., 2018, "SEC rejects 9 bitcoin ETF applications from ProShares, Direxion, and GraniteShares," Cointelegraph, August 23, https://bit.ly/2Pxi2se

Law, L., S. Sabett, and J. Solinas, 1997, "How to make a mint: the cryptography of anonymous electronic cash," American University Law Review 46:4, 1131-1162

Marr, B., 2018, "35 amazing real world examples of how blockchain is changing our world," Forbes, January 22, https://bit.ly/2GHZeVp

Michaels, D., 2018, "Cryptocurrency firm Coinbase in talks to become SEC-regulated brokerage," Wall Street Journal, April 6, https://on.wsj.com/2Kxo5JG

Michaels, D., J. Scheck, and S. Shifflett, 2018, "Firm tied to cryptocurrency entrepreneur faces SEC investigation," Wall Street Journal, November 15, https://on.wsj.com/2qO4rlv

Mora, N. M., E. Hall, and H. Schwarz, 2014, "Brock Pierce, associate of embattled X-Men director, joins the Bitcoin Foundation," BuzzFeed, May 11, https://bit.ly/2GrR7Nf

Popper, N., 2018a, "As bitcoin bubble loses air, frauds and flaws rise to surface," New York Times, February 5, https://nyti.ms/2nGvsWT

Popper, N., 2018b, "Bitcoin thieves threaten real violence for virtual currencies," New York Times, February 18, https://nyti.ms/2Gprtol

Popper, N., and S-H. Lee, 2018, "Hard lessons for cryptocurrency investors," New York Times, August 20, https://nyti.ms/2MqrcJu

Ramey, C., "The crypto crime wave," Wall Street Journal, April 26, https://on.wsj.com/2HuN3J7

Roose, K., 2018, "Think cryptocurrency is confusing? Try paying taxes on it," New York Times, March 21, https://nyti.ms/2IWsiHc

Rubin, G. T., 2018, "First futures contract to pay out in bitcoin poised for green light," Wall Street Journal, December 20, https://on.wsj.com/2GraJkB

Russolillo, S., 2018a, "Bitcoin's rise and fall looks just like dot-com's boom and bust…kind of," Wall Street Journal, March 19, https://on.wsj.com/2SCG1vp

Russolillo, S., 2018b, "Crypto meets Wall Street as bitcoin mining giant Bitmain files for IPO," Wall Street Journal, September 27, https://on.wsj.com/2NMyLuH

Russolillo, S., and G. S. Hunter, 2018, "Regulators world-wide are cracking down on cryptocurrencies. India's next," Wall Street Journal, April 6, https://on.wsj.com/2GHjul0

Salzman, A., 2018a, "Sorting the hope from the hype over blockchain," Barron's, August 17, https://bit.ly/2X1RUd6

Salzman, A. 2018b, "Reassessing blockchain's future," Barron's, December 21, https://bit.ly/2N41BD2

Scharding, T., 2018, "National currency, world currency, cryptocurrency: a Fichtean approach to the ethics of bitcoin," unpublished manuscript presented at the 26th Annual Conference on Pacific Basin Finance, Economics, Accounting and Management, Rutgers University, Livingston Campus, New Jersey, September 6-7

Sorkin, A. R., 2018, "Demystifying the blockchain," New York Times, June 27, https://nyti.ms/2Iy2WOs

Vigna, P., 2018a, "Crypto pioneer David Chaum says he's built a better bitcoin," Wall Street Journal, September 19, https://on.wsj.com/2xsH7gH

Vigna, P., 2018b, "Crypto investing comes with a big risk: the exchanges," Wall Street Journal, March 3, https://on.wsj.com/2CWV0DZ.

Vigna, P., 2018c, "What bitcoin rout? Sales of new digital tokens are still soaring," Wall Street, Journal, February 22, https://on.wsj.com/2CCivIo

Vigna, P., 2019a, "Two groups account for $1 Billion in cryptocurrency hacks, new report says," Wall Street Journal, January 28, https://on.wsj.com/2MDilkm

Vigna, P., 2019b, "A crypto-mystery: is $136 million stuck or missing?" Wall Street Journal, February 7, https://on.wsj.com/2RJ3m9s

Vigna, P., and D. Michaels, 2018, "Has the cryptocoin market met its match in the SEC?" Wall Street Journal, March 20, https://on.wsj.com/2GRrdQH

Vigna, P., and A. Osipovich, 2018, "Bots are manipulating price of bitcoin in 'wild west of crypto'," Wall Street Journal, October 2, https://on.wsj.com/2OAzizg

Williamson, S., 2018, "Is bitcoin a waste of resources?" Review, Federal Reserve Bank of St. Louis 100:2, 107-115

DESIGNING DIGITAL EXPERIENCES IN WEALTH

RAZA SHAH | Principal Consultant, Capco
MANISH KHATRI | Senior Consultant, Capco
NIRAL PAREKH | Managing Principal, Capco
MATTHEW GOLDIE | Associate Consultant, Capco

ABSTRACT

With the significant increase in mobile processing power over the last decade, intelligent, well-designed mobile applications have become the norm, and the wealth and investment management industries need to follow suit if they are to hold relevance. This article highlights how design thinking can enable curators of digital experiences to harness a human-centered approach to app design, thus maximizing the wallet-share of millennials. It breaks down the key areas needing attention during design, and showcases research suggesting how design and communication are essential in capturing a transient wealth and investment generation.

1. INTRODUCTION

Traditionally, wealth and investment management (WIM) firms have prided themselves on building strong customer relationships and delivering bespoke services through trusted personal advisers. We see this fiduciary-based relationship and trust continuing. However, businesses will need to adapt to changing customer expectations.

The younger generations are experiencing newer, more seamless, and personalized digital experiences in most aspects of their lives, and they are experiencing an unprecedented wealth transfer;[1] hence WIM organizations need to be at the top of their games to be successful. They need to provide best-in-class online, mobile, and face-to-face services to attract and retain these clients.

And, they are not only in competition with their old established peers. There are now nimble fintech players that are also trying to get in on the act and growing their market share, particularly in the increasingly significant millennial market. To help combat this, we believe that WIM organizations need to turn their attention to the latest and most innovative ways to stand out from the crowd, and suggest that developing a "design thinking" culture could be a critical differentiator.

Design thinking is an innovation methodology that focuses on understanding people's real problems and rapidly exploring a range of creative solutions. It accelerates the definition of high level, tangible requirements through close collaboration, rapid prototyping, and testing with end-users ahead of agile delivery. Having this methodology in place when creating your user experiences provides you with confidence that what you are designing and building is definitely what your customers need. In this article, we highlight the critical principles for business leaders and digital teams to consider when designing the user-experience (UX) for WIM services of the future.

[1] Research estimates that the figure for intergenerational wealth transfer in 2017 already crossed the £69 billion (over U.S.$90 billion) mark in the U.K. and in ten years' time this is expected to increase to £115 billion (over U.S.$150 billion) annually, an increase of 67% (Source: https://bit.ly/2lEdwsF).

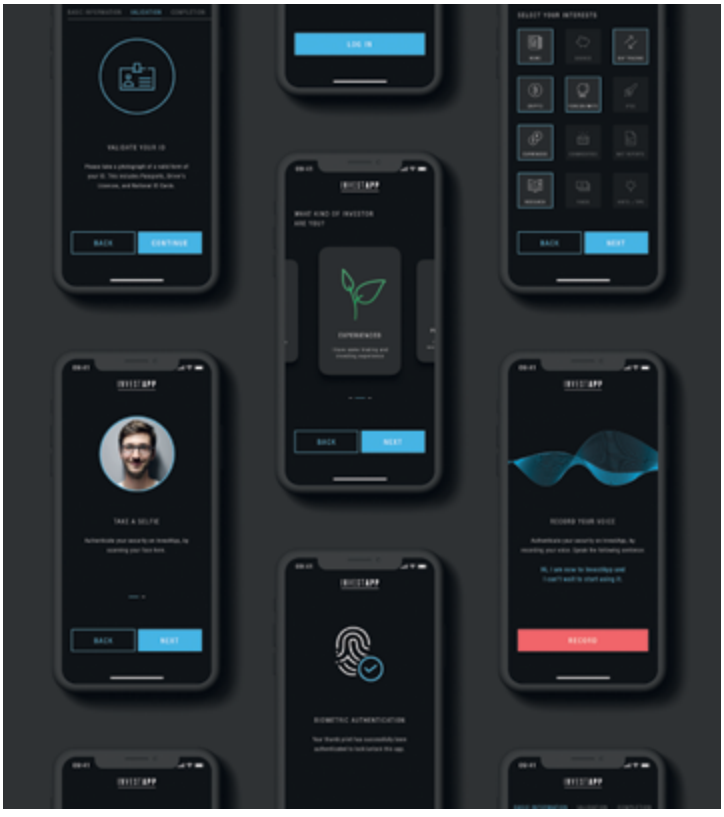
2. ONBOARDING AND LOGIN

Client onboarding is the first interaction the customer may have with your brand and so it is of paramount importance for setting the tone for the rest of their experience with your enterprise. Unfortunately, many processes today are time-consuming, clunky, and inefficient, which is a far cry from what could happen should a design thinking approach be in place.

Typically, a financial institution will collect documents and individually engage credit reference agencies to verify customer identity against other independent data sources on their behalf. However, it does not have to be this way, and by using the fundamentals of design thinking the onboarding process can be made significantly less painful.

2.1 Simplification

To generate a good experience right from the start, WIM firms should encourage customers to sign-up and create accounts via a single interface, such as a smartphone app. Being forwarded onto other channels through a mobile app is not streamlined, and with an increasing amount of neo-banks offering a straightforward onboarding process it is important that WIM organizations follow suit. It is also important for the process to include basic sign-up questions, stripping away anything that is superfluous and reducing the number of steps in the process to the absolute minimum. With the demand for mobile banking increasing at an unprecedented rate, ensuring the process is limited to a single device and interface will be key in making the process as genuinely mobile as possible.



2.2 Time-saving

Social logins are a great time saver that are appreciated by most consumers and benefit from the fact that digitization has enabled a quick and easy flow of information. No one wants to waste time filling out lengthy registration forms anymore. Javelin Strategy & Research and Jumio found that 38% of millennials abandoned their mobile banking applications because the process took too long [Jumio (2018)]. There are already examples of how this is being incorporated into digital platforms, such as Pinterest allowing you to log in with either your Facebook account or Google Mail, and industry relevant examples such as eToro, which has the same features. Other elements, including the auto-scanning of ID cards using a smartphone camera, can also be useful in saving time when uploading identification information, and are becoming more prominent in UX-led app designs.

2.3 Biometric authentication

Facial, fingerprint, and voice recognition, as well as other biometric technologies, are starting to replace the onerous methods of using multi-factor logins and passwords. Jumio (2018) found that 27% of millennials have left mobile banking because they forget their password and 22% felt authenticating themselves was time consuming – something that need not happen. Not only can biometrics bring about a faster and smoother onboarding experience, they can also provide greater levels of security than traditional PIN numbers or security questions once onboarding is completed. However, devices employ different standards, so it is critical to consider how a standardized interface would work as an experience for all investors.

2.4 Gamification

The onboarding process should be as easy and engaging as possible, and gamifying the experience or breaking down the onboarding process into digestible chunks, like

elements of a computer game, can make the process seem shorter. In addition, like a game, the onboarding process should allow for the process to be continued at a later time as well. With busy, modern lifestyles, the thought of having to set aside a lot of time for an onboarding process will be off-putting for consumers and needs to be a consideration for the process designers.

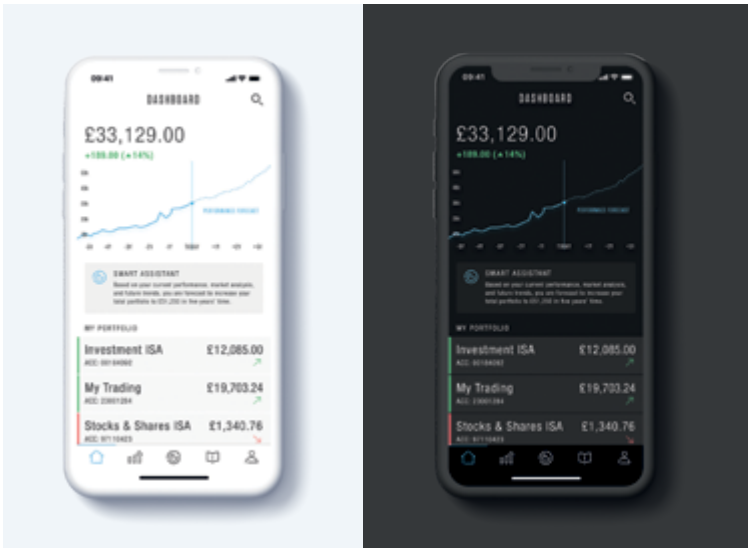
2.5 Referrals

Using referrals during the onboarding stage is a great way to get your own customers to become ambassadors of your app and help grow your user-base with little input or effort. To make the step more appealing to customers, monetary incentives for successful referrals should be considered – something already implemented by many other apps. However, above all else, the process needs to be straightforward and not time consuming. Regardless of offers and monetary incentives, the most likely way for a customer to proceed with a referral process will be if it contains a single, straightforward step. However, striking a balance is key. Some users find it off-putting if interfacing with a financial services platform is too easy, giving the impression that the platform is not fully secure. The challenge is to enable a thorough onboarding service that has complex operations happening beneath the surface of a streamlined, beautiful, user-friendly interface. To do this, prioritizing elements of the process that are slightly lengthier will be key in the balancing act. For example, keeping the referral process to a minimum number of interactions and steps, whilst having a multi-biometric authentication process, will help the user feel the process is secure, but straightforward. As Steve Jobs said: "Simple can be harder than complex: you have to work hard to get your thinking clean to make it simple" [BBC (2011)].

3. ACCOUNT VALUATION AND PERFORMANCE

Visualization should be the primary consideration when it comes to user experience on apps and web-platforms. The human brain processes visual information much more effectively than textual data, so it is imperative complex data is represented in a clean and concise way. The significant increase in mobile processing power and screen display quality has meant that many successful apps now lead with a design-led user experience. Quapital is an example of how the humble savings account can be elevated from the stereotype of a dry, functional subject, to something engaging and beautiful to use and look at. Importantly, though, the design does not come at the expense of convenience and functionality.

Consumers should have easy access to their wealth dashboards once the login process is completed, focusing on account valuation and performance to keep them engaged. Key information depending on specific scenarios should always be displayed to the user on a default screen for maximum convenience. For instance, in an investment app, the user will want to know how much they have invested overall, how much their investment has increased or decreased by, and likely a visual representation of actual/percentage changes too. This information should be laid out as simply as possible and should be the first thing the user sees, summarizing the key elements of their investments before they go to other areas of the app to delve deeper into them.



Visualization tools like infographics help tell the user the story of their finances by visually representing tedious, tabular data in an interactive, attention-grabbing visual and will help with the usability of an app. Adding interactivity to dashboards enables engagement with the data, especially with the help of sliders that can be used to foresee future positions through data analytics. This can provide powerful knowledge to the user, while providing an element of gamification in the process, and will be a significant factor in increasing the frequency of user interaction. The pension fintech, PensionBee, includes an interactive and user-friendly pension calculator to work out the required annual savings needed to receive your desired annual pension amount after retirement. By providing an interactive platform that combines all of the customer's pensions, the user becomes much more aware of their financial situation – increasing the likelihood that they will set themselves financial targets. In this instance, the interactive, user-focused design could lead to not just more frequent engagements with the app, but also an increase in monetary contribution as the user seeks to achieve personal financial goals that they may have previously been unaware of. WIM firms should consider a similar approach.

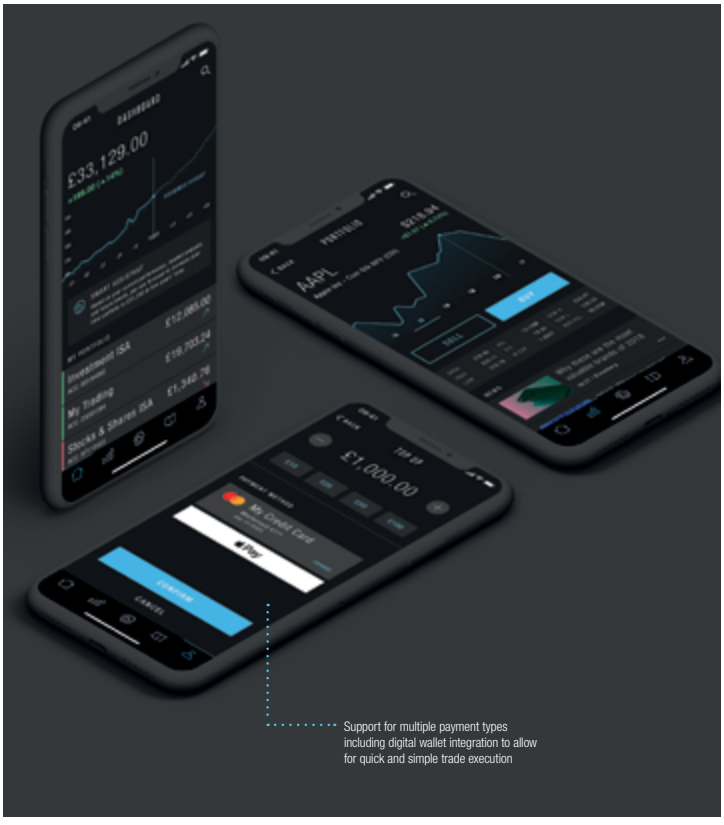
4. PERSONALIZATION OF SERVICES

Investors' goals, values, and preferences are influenced by their demographic segment, life stage, household balance sheet, and specific tax circumstances. Millennials may be saving for a down payment on their first home, whereas retiring Baby Boomers are focused on extracting equity from their home to fund retirement income. To design the best UX for financial products and services, we need to get to know our users better and identify what sets them apart from each other. A good way to identify the needs and motivations of users is by creating personas for each group. A persona is a representation of a certain segment or audience who will be using your products or services, outlining a high-level view of this specific user. Included in personas you will typically find a photo/icon of the user, a biography, wants/needs, pain points/frustrations, brand associations, and goals/aspirations. They can be a great way to create consensus among your team members in how and who your products and services should be positioned to, helping focus future marketing initiatives. A survey by Smart Communications (2018) found that nearly two-thirds of respondents are likely to switch vendors if communication expectations are not met. Combined with the fact that 45% of U.K. respondents specifically cited communications that are not relevant to them as influencing their decision to change vendors, and the ability to personalize marketing from personas becomes even more apparent.

The U.K. mobile-only bank, Monzo, takes personalization one step further through using customer payments data to provide personalized offers and advice. By analyzing daily commute costs, for example, Monzo's algorithms are able to suggest savings to customers, such as telling them to switch from a pay-as-you-go travelcard to an annual one. This also helps the bank in terms of building trust with the customer. Once the relationship involves personalized recommendations that will directly help the user, the app/service goes beyond a platform for solely managing money to something that is appreciated

by the consumer. The ability to be personalized needs to be considered by WIM firms. It does not necessarily have to be immensely complicated – even being able to customize the look and feel of a trading or investment app provides a level of micro-personalization that puts the user in control of their own UX. It is easy to overlook how often we already personalize things on a small scale; our mobile devices already have individual displays, sounds, layouts, apps, cases, and physical design. Money is an incredibly personal thing, so having the ability to customize how we interact with it should be high on the design agenda.

The areas and amount of personalization will differ depending on the brand in question. The City Index app, for example, allows users to drag and drop service icons to the bottom navigation pane, allowing them to choose which services they want easy access to from their navigation bar. This is a more functional approach to customization. Atom Bank, however, allows you to create a personalized name and logo for the app, such as Jenny's Bank or Peter's Bank, as well as a personal color palette – removing large elements of the brand from the product. This customization is far more targeted at the individual at a personal level, and less towards the functionality of the product. Looking at these different examples, it is no coincidence that neo-banks, which offer the highest levels of customization and personalization, are proving far more popular with millennials than any other age group. The ability to have an app looking and working how the user wants is growing in necessity, particularly if the product wants to appeal to what is becoming an increasingly significant millennial market.

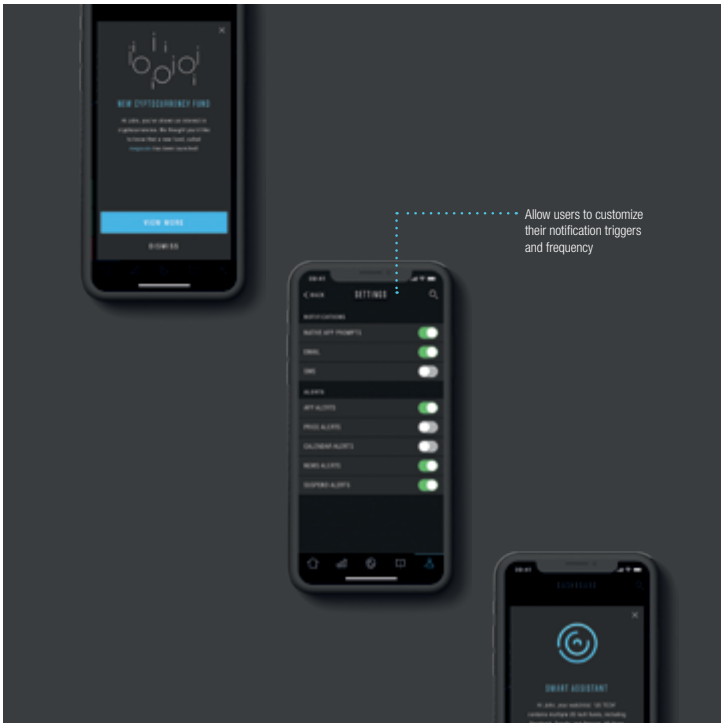


A recent YouGov poll found that just 36% of British consumers trust banks to work in their customers' best interests [Palenicek (2017)]. Evidently, trust is still an issue banks need to work on, more than ten years after the market crash. However, there is an opportunity for firms to understand which features are most frequently used, improve the refinement process, and tailor apps towards what is actually wanted. Most users will not want a generic "one-size-fits-all" approach to their app/service and the ability to tailor and personalize, be it the onboarding journey or the default section of an app, is fundamental in making users feel important. By helping users build personal relationships with their products or applications, you can also start to build trust – something that cannot be underestimated.

5. TOP UP/WITHDRAW FUNDS

As well as the traditional linking of bank accounts to a user's account, customers should also be given the option of using multiple sources of funds to top-up their accounts, including non-traditional payment sources such as PayPal, Apple Pay, Google Pay, Samsung Pay, etc. Customer trust with, and usage of, non-traditional payments has risen significantly in recent years, and WIM firms need to cognizant of this fact. WorldPay (2018) estimates that by 2021 over half of all online transactions will be made using alternative payment methods. Given this notable increase, early adopters of the technology, and the convenience it has to offer, will appeal to increasing market audiences. TransferWise, a foreign exchange money transfer service, is an early adopter and allows users to transfer money linked to their cards stored on their Apple Pay wallet to their platform. This seamless process involves entering a payment amount and simply using your fingerprint to authenticate the payment.

It is equally important to establish a seamless withdrawal process, whereby customer can withdraw their earnings at any point and then put it into their selected account



choice, with withdrawal fees clearly being communicated during the initial onboarding process. Not only is this process streamlined, it also builds on the trust element touched on earlier, which will be key for the sustainability of the brand. After all, the customer has earned the money, so they should be made clearly aware of any charges for moving it. According to an FDIC report, overdraft fees are the leading cause of involuntary bank account closures, highlighting how perceived deception, and the lack of trust that comes with that, impacts customers [Samolyk et al. (2013)]. But small steps towards a better customer relationship can be very impactful – they do not need to all need to be giant leaps. Small, engaging interactions, such as an animation to verify confirmation of top-ups, or push notifications to smart watches (which alert the user that their funds have been withdrawn successfully), may seem like basic facets, but ultimately, it is these regular micro-interactions for otherwise mundane tasks that have a lasting positive impact.

6. TRADE/INVESTMENT EXECUTION

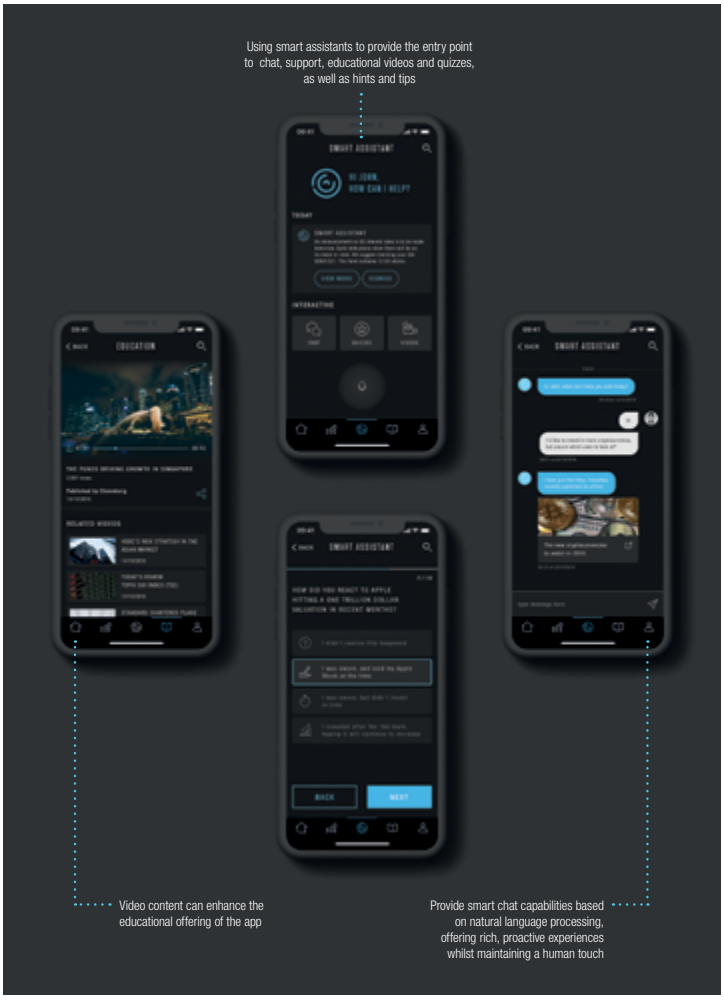
Arguably, the most critical action you are asking your users to perform is to place their investment, and trust, with you. Consequently, it is essential that this step of the process is one of the most seamless and simplified. The path from research, to selection and execution should be a logical one with minimal cognitive load; and setting alerts, limits, and stops should all be part of the final execution flow. If the app allows for different payment methods, the selection between them should be straightforward, with all the authentication being done when the payment type is registered during the onboarding process.

Innovative execution paths should also be considered. For example, when sending an email with research or news that includes your customer's top stock picks, it should have deep linking capabilities so that users can select a link in the news articles, taking them directly to the app and onto that stock's page – ready to be traded in a click or two. This will not only improve engagement levels with the app, but also helps with improving the personalization of the services. In addition, anything that can help support the user with their trading and investments will be largely beneficial and can significantly improve the overall user experience. Chatbots or virtual assistants are great for support and proactive prompts, as well as for how-to guides, and keep the user from having to use more than one interface. Furthermore, it is common, particularly

within trading services, to offer news when looking at a stock or share, rather than having to switch between separate news feeds.

7. NOTIFICATIONS AND COMMUNICATIONS

Notifications and alerts are important ways to keep the savvy trader up-to-date with the latest status of their holdings and the various events affecting their positions. Notifications for longer-term investment products are less frequent, but for an intra-day trader these are invaluable for keeping them informed when events take place that impact their portfolio. These events can be market developments, technical indicators, economic announcements, reaching specific price targets, or even system outages preventing trading during certain times. There are different ways to reach the user: alerts, push-notifications, emails, and in-app messaging can all be used to communicate with investors as events happen. The type of notifications, frequency, and event triggers should all be made customizable for the user, as without this the information may lose relevance to the individual and become useless. If the notifications are too frequent or irrelevant, the user may trivialize them, or turn them off, and subsequently miss opportunities when more important notifications are issued. A good example of this is the CMC Markets app, which gives users the power to set a multitude of notification options, as well as the events that should trigger them. The benefits of setting up and using pro-active notifications include:



- **Saving time:** customize your notifications to receive price alerts and then execute your trades, saving you time from monitoring price movements manually.
- **Quick response:** delivering push notifications when impactful news breaks, allowing you to make instant buy or sell decisions by a single click when not logged into the app.
- **Retain app usage:** notifications are a great way of increasing returns to your app and engagement with your user base, so long as they are relevant. Frequent, irrelevant notifications outside of user preferences may actually have the adverse effect and frustrate users to the point they leave the service. Research shows that 22.3% of people would stop using an app if they received two to five notifications a week, so any notifications they do receive need to be aligned to the topics they have requested [Gibb (2018)].

8. PARTNERSHIPS AND INTEGRATIONS

Established investment and trading companies can differentiate themselves from the competition by becoming early adopters of the latest financial technologies. Of course, building everything yourself (robo-advisers, machine learning capabilities, hyper-personalized dashboards, etc.) may be a step too far for your cost appetite, so forming a strategic partnership with a fintech that is providing a best-of-breed solution in their niche offering could be a more viable option. With this in mind, instead of viewing fintechs as competition, traditional financial institutions should investigate how strategic partnerships can be used to create an entity stronger than either individual unit could bring on their own. Benefits of these collaborations include cost reduction, quicker time-to-market, improved customer retention, and additional revenues.

U.K. challenger-bank Starling is a huge supporter of the partnership model and has even created a "marketplace" on their app that allows users to link their bank account to services from other fintechs, such as your pension details to your account via PensionBee or adding travel insurance via Kasko. A recent first in the U.K. investment world also occurred when AJ Bell launched a developer hub, allowing external apps to link their services to AJ Bell's Youinvest platform. AJ Bell is also working on a project that will allow its customers to request to be able to view their bank account, pension, and ISA details from external providers via their AJ Bell account.

> "WIM organizations need to turn their attention to the latest and most innovative ways to stand out from the crowd. We suggest that developing a "design thinking" culture could be a critical differentiator."

Application Programming Interfaces (APIs) underpin both these two collaborations and provide the channel to access data between partners. Allowing access to your data and transactional services via a robust API strategy will aid the execution of a smooth and secure partnership ecosystem. However, keeping and enforcing security standards is critical for both regulation and brand longevity purposes, and so must be considered at all times during the design.

There are many benefits to this model, but primarily it allows for an open ecosystem, which is an attribute that an increasing number of consumers are beginning to prefer. A single service that is paired with other services via APIs will allow open access, and this only helps when viewing their finances. For instance, a trading app could partner with a venture capital funding app and use their investment service within the trading app, allowing users to browse and select a start-up they wish to invest directly into. This would mean users would not need to switch between two apps, and both companies could benefit from an increase in usage as a result of the added simplicity. From a business perspective, the two respected parties could also work together to monetize the combined service.

9. EDUCATION / GUIDANCE

Investing can be an intimidating and complicated experience for the first-time investor who must navigate their way between a multitude of products, services, accounts, and fees, while usually also lacking the financial literacy needed to make smart investment decisions. In fact, a study by Schroders found that only 37% of participants knew what the correct description of an investment manager was. 10% thought investment managers were retail banks [Nicoll (2019)]. So, with an apparent lack of knowledge about what an investment manager does, why should we expect customers to be able to manage their own investments effectively? The companies that provide a simplified service execution, coupled with best-in-class learning resources will have a competitive advantage in winning business from millennials. In fact, some neo-banks are making education and guidance central to who they are. This is clearly expressed by Atom Bank's CMO Lisa Wood in an interview with Marketing Week: "It's not about the customer relationship with us, or our relationship with customers' money. The traditional old banks constantly reference their relationship with its customers, but our brand strategy is about helping people understand money much better" [Roderick (2016)].

Fundamentally, a customer base that understands a company's products and services is far more likely to transition to and use them. This simplification of services has already gained momentum within the retail banking but is not as prominent within the WIM industries. Considering the fact that products on offer within WIM are likely to be more complicated, education and guidance offerings will be key to adoption. Some examples of best practice within education and guidance include:

- **Demo account:** allow your users to first invest using a limited feature demo account from which they can invest on real life products by using a virtual currency. This will build up their knowledge of the markets and confidence in their abilities to execute investments using real currency. The IG Index app makes it easy for users to sign up for a demo account by simply logging in via Facebook to create a risk-free demo account with £10,000 (over U.S.$13,000) of virtual funds.

- **Features walkthrough:** once your new user downloads your app for the first time, a walkthrough of the main features using pop-up messages will help introduce them to the capabilities and service features of the app. These messages can also be displayed to introduce new features whenever your app is upgraded. However, keep this high level and simple. In line with a smooth onboarding process, this element needs to only highlight the key features and be easily interpretable, otherwise it may frustrate users.
- **Live/robo-chat:** allow users to access in-app chat features to converse with either real-life customer service representatives or even bots, programmed to answer common questions. The Capital.com trading apps enables users to chat with bots using natural language processing to answer queries. If chat-bots are used, it is important to ensure that the automated response language is in keeping with the brand language style and is simple to understand. Monzo has an award-winning terms and conditions due to the transparent, honest, and clear tone used, and is backed by research showing that people prefer simpler, more natural language.
- **Educational content:** short videos educating users on trading and investing best practices within your smartphone app would provide a one-stop shop for educating them. Like the robo-chat, language needs to be kept simple and clear if users are to gain maximum benefit from this. WIM comes with an element of risk, so providing users with the security of having some educational content is far more comforting. If this is done effectively, it will lead to more contact with the product.
- **Gamification:** use of items like leaderboards, badges, missions, and levels will encourage your users to increase their engagement with your apps. With the mobile gaming industry forecast [Statista (2019)] to be worth U.S.$74.6 bn by 2020 (80% more than in 2016), and with approximately 32.4m people in the U.K. playing games, the popularity of engaging with games is evidently growing. For example, in 2017, Wells Fargo launched a game called “Retirement City” with the intention of helping America’s workforce prepare for a better retirement. The game blends quizzes, videos, mini games, scoreboards, calculators, an online resource library, and other elements to deliver financial wellness concepts focused exclusively on retirement. Players in “Retirement City” pick one of 40 avatars and move through five neighborhoods on a simulated journey to retirement. Along the way, they earn badges and rack up points as they learn retirement-saving basics, make choices (pull-out-the-stops wedding or modest affair? New car or used car?) and see how life’s curves (your house has been damaged by a storm and now there are repair costs) affect long-term savings. This allows players to learn retirement concepts, and benchmark themselves against other players, blending finance and literacy concepts.

10. CONCLUSION

There are many design-focused initiatives, tasks, and methodologies that can have a huge impact on the overall experience of customers. Some are stringent rules, others are more flexible. But there are a number of ways in which you can work toward this:

- **Incorporate design thinking:** in apps, products, websites, or, in fact, any consumer-facing product. The key here is to have a deep interest and understanding of what your customers really want. Empathize with your customers, define their needs, and ideate by creating innovative solutions. Prototype solutions, test with your customers, iterate, and test again until you get it right. Gain feedback and reviews from your customers and ensure they are taken seriously.
- **Get senior stakeholder buy-in:** empower senior management and stakeholders by training them and getting them involved in the design thinking process. Invite them to focus sessions so that they can really see things from the end-user’s viewpoint. Projects will ultimately need a senior sign-off, so having a set of stakeholders that understand design thinking will allow for more customer-focused project visions and objectives.

- **Analyze key trends:** look at what your competition is doing. However, only relying on your competition to act first means you will always be playing catch up, so do not use this as your sole source of inspiration. Look at completely irrelevant industries and spot other success stories, because from this could stem an idea or an approach that could positively impact your business. To be genuinely creative and to offer something that no one else is, it makes sense that the source of inspiration will come from outside of the industry, so embrace this.
- **Embrace technological advances:** determine how they can create a positive impact, but make sure that you have a human-centered approach to innovation. Break the stigma that technology is only going to replace humans and use it to serve them better. Early adoption of technology can help establish a customer base with millennials that want the latest design thinking, as well as enhancing the customer experience. It also allows you to work with and learn from the technology earlier, whilst the competition is still getting to grips with deployment.
- **Be open:** sometimes it is not necessary to do everything yourself. For example, why build a new service when you can integrate a partner's service at a much quicker and cheaper cost? Being agile and reacting to changes in the market is critical, so a traditional in-house build, whilst allowing more control, might not offer the ability to act quickly. Furthermore, think about appealing to non-traditional customer bases. The ability to create a mobile WIM app means your services are reachable by everyone who owns a mobile device – use this to your advantage.

REFERENCES

BBC, 2011, "In quotes: Apple's Steve Jobs," British Broadcasting Organization, October 6, https://bbc.in/2EfJTlQ

Bright Local, "Local consumer review survey," Bright Local, https://bit.ly/29hKyhf

Gibb, R., 2018, "How consumers perceive push notifications in 2018," Localytics, January 10, https://bit.ly/2mppJ6J

Jumio, 2018, "38% of millennials abandoned mobile banking activities because the process took too long," Javelin Strategy & Research and Jumio, March 6, https://bit.ly/2T6jK9I

Nicoll, S., 2016, "Why should I care what an investment manager does?" Schroders, September https://bit.ly/2tE1gy2

Palenicek, J., 2017, "Most Brits trust banks but don't think they work in customers' interests," YouGov, https://bit.ly/2Vr5tB7

Roderick, L., 2016, "Atom Bank creates 1.4 million logos in bid to prove 'customer obsession'," Marketing Week, January 6, https://bit.ly/2bjTuUK

Samolyk, K., T. Critchfield, J. Galindo, and C. Watson, 2013, "Checking-account activity, account costs, and account closure among households in low- and moderate-income neighborhoods," FDIC, https://bit.ly/2H4QEQJ

Smart Communications, 2018, "The State of Meaningful Customer Conversations," June, https://bit.ly/2EnaeVg

Statista, 2019, "Mobile gaming app revenue worldwide in 2015, 2016 and 2020 (in billion U.S. dollars)," Statista, https://bit.ly/2E1iAV0

Worldpay, 2018, "Global payments report 2018," https://bit.ly/2PuGd9S

TOKEN OFFERINGS: A REVOLUTION IN CORPORATE FINANCE?

PAUL P. MOMTAZ | Ph.D. Candidate, Anderson School of Management, UCLA
KATHRIN RENNERTSEDER | Consultant, Financial Advisory, Deloitte
HENNING SCHRÖDER | Assistant Professor of Corporate Finance, University of Hamburg, and Hamburg Financial Research Center

ABSTRACT

Token offerings or initial coin offerings (ICOs) are blockchain-based smart contracts designed to raise external finance without an intermediary. The new technology might herald a revolution in entrepreneurial and corporate finance, with soaring market growth rates over the last two years. This paper surveys the market evolution, offering mechanisms, and token types. Stylized facts on the pricing and long-term performance of ICOs are presented, and lessons learned from the first wave of token sales are discussed.

1. INTRODUCTION

Initial coin offerings (ICOs), also referred to as token sales or token offerings, have gained rapid popularity since 2017. ICOs are smart contracts based on blockchain technology and designed to raise external finance without an intermediary [Momtaz (2019b)]. While the concept is mainly known under the term "initial coin offering," the term "initial" is factually misleading in nature. Firms usually fix the maximum token supply in the smart contract and hence rule out the possibility of "seasoned" offering under the same contract. But, in keeping with convention, we use ICOs and token offerings interchangeably.

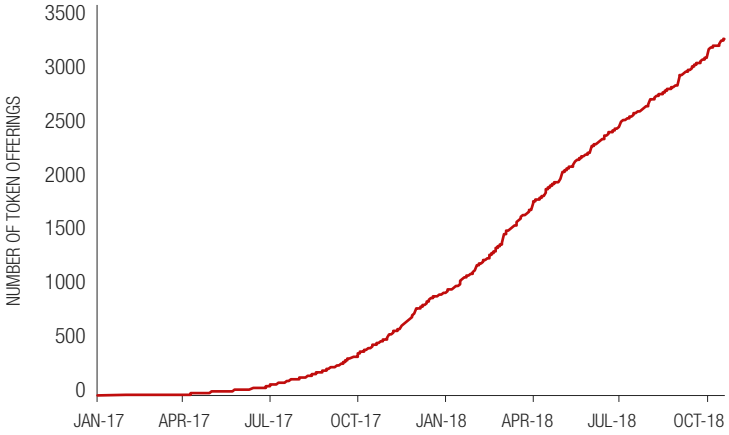
Token issuers make use of smart contracts that implement an automatic algorithm of the following type: if investor i sends funds in the amount of x to token issuer j, then i automatically receives y tokens from j in exchange, where x/y is the exchange rate that has been fixed ex-ante in the smart contract [Momtaz (2019b)]. The main innovation of this technology is that it eliminates the intermediary completely so that investors and token issuers can share transaction rents exclusively among each other. Another attractive feature of this new financing mechanism is that there are almost no transaction costs involved, making it also very attractive for entrepreneurial firms.

While token offerings are attractive to small firms, they are equally attractive to large firms, with increasing relevance for large corporates as the general acceptance of blockchain finance percolates financial markets and society at large. Two facts shall suffice to prove this point. First, the largest token offering so far (EOS, U.S.$4.2 bn) exceeds in terms of gross proceeds all cumulative proceeds raised by all entrepreneurial firms on the premier crowdfunding platform, Kickstarter, since its inception in 2009 [Fisch (2019)]. Second, the EOS token offering is in terms of gross proceeds comparable to the three largest IPOs during the same time period [Howell et al. (2018)]. This shows that token offerings may herald a revolution not only in entrepreneurial, but also in corporate finance for large companies. It also has wide applications for multi-national enterprises (MNEs) that aim to streamline their internal capital transfers across countries. An illustrative example is the announcement by J.P. Morgan that it aims to issue its own cryptocurrency, JPMorgan-Coin.[1]

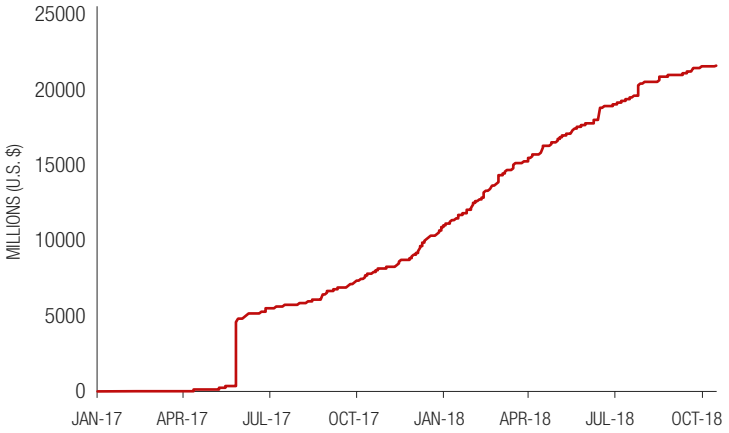
[1] https://bit.ly/2SGPpy1

Figure 1: The evolution of the token offering market

a) Cumulative number of token offerings



b) Cumulative funding volume of token offerings



In this article, we provide an overview of the market evolution, explain the mechanics of token offerings, compare token offerings to conventional sources of financing, review the market performance so far, and finally discuss lessons learned and next steps for this infant market to thrive.

2. MARKET OVERVIEW

The idea of token offerings was first applied in 2013 with a meagre investor demand [Boreiko and Sahdev (2018)]. The breakthrough year was 2017, when about 1,000 token offerings sought funding and the increase in market capitalization in these so-called alt-coins (the term comes from "alternative coins" in regard to the dominant coin, bitcoin) increased by about U.S.$370 bn, which is equivalent to the 10th largest corporation or the 32nd largest country in terms of GDP, and exceeds the entire European venture capital industry [Amsden and Schweizer (2018), Blaseg (2018), Momtaz (2018b)].

Figure 1 shows the cumulative number of token offerings and funding from January 2017 through October 2018. The market reached gross proceeds in the amount of U.S.$21.2 bn raised by 3,252 firms by October 2018, illustrating that much value is added in the after-market (compare U.S.$21.2 bn to U.S.$370 bn in after-market value). Still, the funding success is exceptional, since mainly early-stage firms or project groups, that have only developed an initial idea of their business, have initiated token offerings during the first wave of the market. As Figure 1b shows, June 2017 witnessed a steep incline in gross proceeds that is attributable to the EOS offering, raising U.S.$4.2 bn. Since then, more than 100 new token projects enter the market every month.

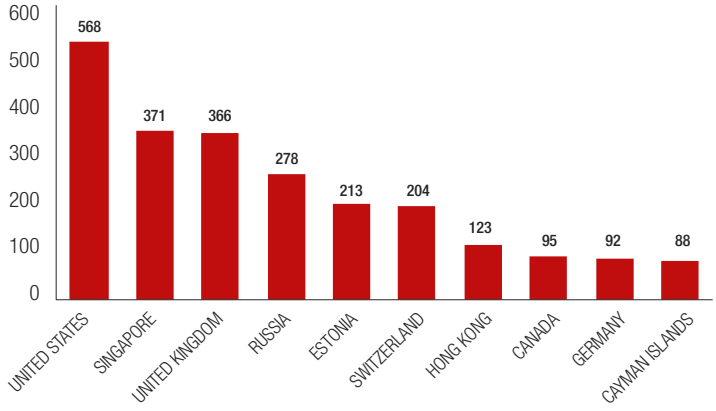
Figure 2a illustrates the token offering activity by country. The market for token offerings is prevailing in the depicted 10 jurisdictions contributing more than 73% of worldwide token offerings. Because firms that initiate token offerings provide digital services or products on decentralized online platforms, which are not confined by state borders, the data suggests that taxation strategies are currently less of a concern than in traditional financial markets [Huang et al. (2018)]. However, the dominance of countries such as Singapore and Switzerland that have expressed regulatory standpoints that promote token offerings (371 and 204, respectively, token offerings between January 2017 and October 2018) shows that blockchain-based funding activities foster more in markets with milder regulatory environments and lower degrees of legal uncertainty.[2]

As Figure 2b shows, the main share of token offerings takes place in platform services (15.0%), cryptocurrency (10.9%), and business services (6.5%). At the same time, it is notable that firms in traditional industries such as healthcare and utilities find their way into the market for tokens and pursue the expansion into new markets by pivoting into innovative business models based on blockchain services.

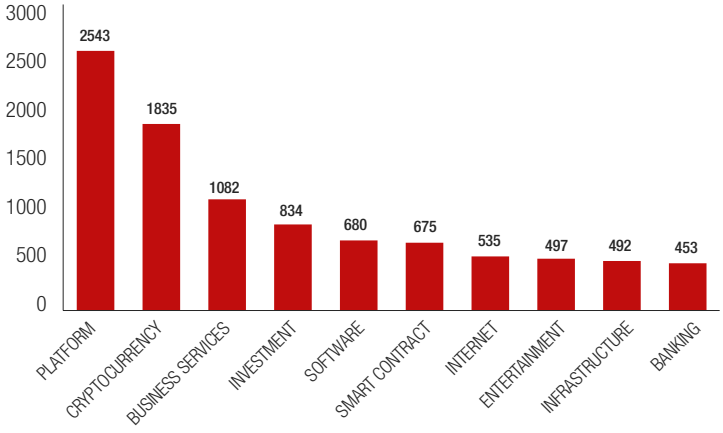
[2] An interesting question that has not been addressed yet in the context of blockchain finance is the extent of regulatory convergence across borders that is seen in many financial markets, e.g., in M&A markets [Drobetz and Momtaz (2019) and Dissanaike et al. (2018)].

Figure 2: Token offering activity by country and industry

a) Country overview



b) Industry overview



3. THE MECHANICS OF TOKEN OFFERINGS

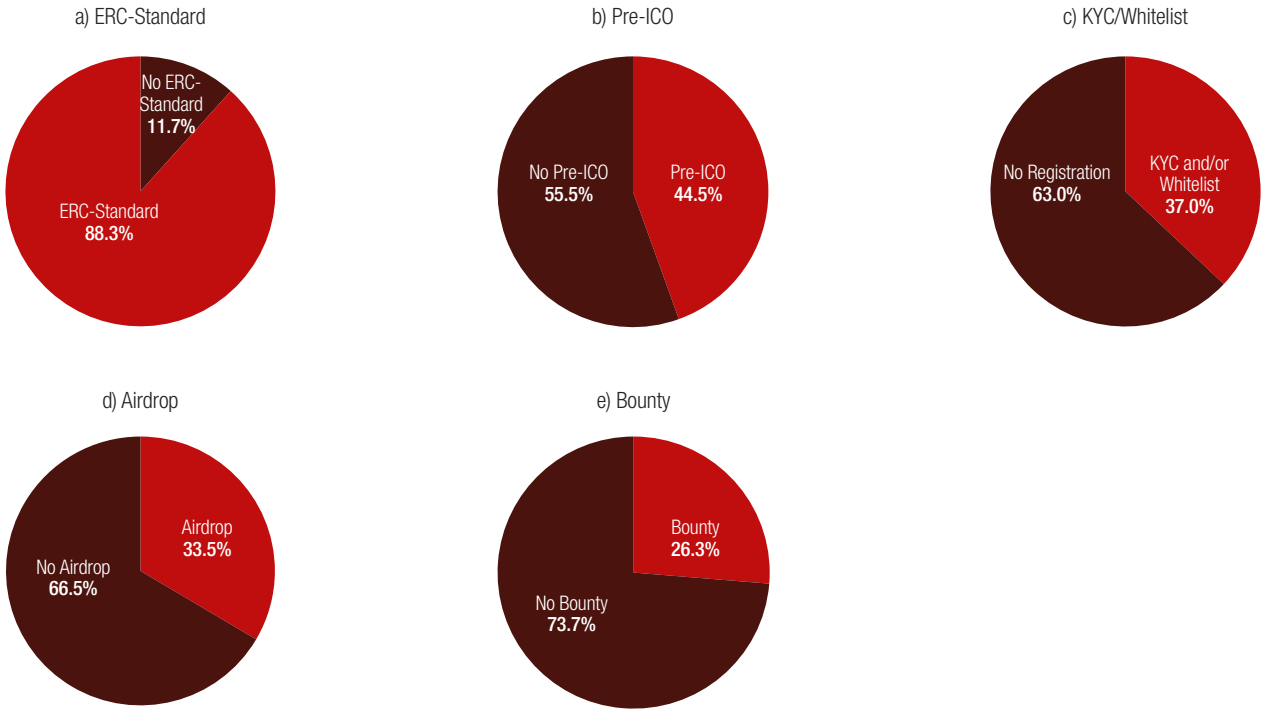
3.1 What are token offerings?

Token offerings are blockchain-based offerings of cryptographic tokens. Figure 3a shows that token offerings processed using the ethereum blockchain, a smart-contract framework that helps set terms and automate the exchange of tokens for fiat or digital currencies, dominate the market at a share of 88.3%. Boon for some and bane for others, token offerings help firms to raise finance without the need of a financial intermediary. Token offerings are advertised on designated online platforms and investors can send money directly in exchange for the offered tokens. An early claim of enthusiasts of the token offering mechanism was that it would help democratize finance by cutting out the middleman (or underwriter) and hence distributing all the gains among the platform users. However, institutional investors have entered the market and are able to dictate their terms and shape the market [Howell et al. (2018)]. In fact, many firms have sold large portions of their offered tokens to institutional investors in private pre-offerings at significant discounts (often up to 75%). Figure 3b shows that pre-offerings (or pre-ICOs) are executed in 44.5% of all documented token offerings.

The soaring growth of the token offering market can be explained by the combination of a few factors. First, token offerings are attractive to firms in need of external finance because the mechanism enables them to acquire funds very fast. Token offerings are set up in a few minutes at no cost using technical token standards such as the ERC-20. Most token offerings accept the major cryptocurrencies ethereum (85%) and bitcoin (41.8%), and, to a lesser extent, litecoin (14.7%), as the exchange currency from investors. The usage of cryptocurrencies makes transactions more rapidly verifiable and involves lower costs than payments using fiat money. Further, firms appreciate that this method is geographically unbounded as fundraising happens exclusively via the internet. Consequently, firms are able to approach all potential investors worldwide very efficiently. At the same time, token offerings can easily exclude pre-defined groups of investors and thereby avoid regulatory uncertainties. While U.S. investors are prevented to participate in 29% of token offerings, only 4.7% and less than 1% of token offerings refuse investments from Singapore and Russia, with China and Korea at 18% and 7.1%, respectively.

Second, token offerings are very attractive to investors for at least two reasons. One being the pseudo-anonymous nature of tokens, which makes it technically impossible to determine an investor's real identity. The only transparent feature known about the investors is their wallet address, i.e., the combination of numbers and letters that investors use to send and receive tokens. Although token transfers can be reconstructed using the information stored on blockchains, they never reveal the true identity. Hence, the term "pseudo-anonymous." Still, 37% of firms require verification of investor identities via KYC (know your customer) or whitelist registrations (Figure 3c). Within a KYC process, potential investors are obliged to provide personal data (e.g., photo IDs and email addresses), undergo approval processes, and sometimes even explain their intention to buy the token in question in a short

Figure 3: Token offering features



essay. With this, firms can prevent, inter alia, investors from countries where token offerings are prohibited, such as China and South Korea, from participating in the token offering. Whitelists are similar to a pre-order with advance payments, where interested parties are registered on the whitelist with their cryptocurrency wallet address as soon as advance payments are made. Thereby, projects can estimate the exact amount of funds they will raise and get more data on personal investor features and intentions if further KYC processes are part of the registration process. Whitelisting without KYC, however, only refers to the pre-approval of the future investors' cryptocurrency wallet address without personal data being transferred. This method is losing its popularity as firms risk violating the regulations in certain jurisdictions demanding mandatory identification of investors to prevent money laundering or terrorism financing. The other feature investors are attracted to is the immediate liquidity of the offered tokens. Most projects list their tokens within 30 to 60 days after the token offering on cryptocurrency exchange platforms [Momtaz (2018b)]. This gives investors the chance to exit an investment anytime.

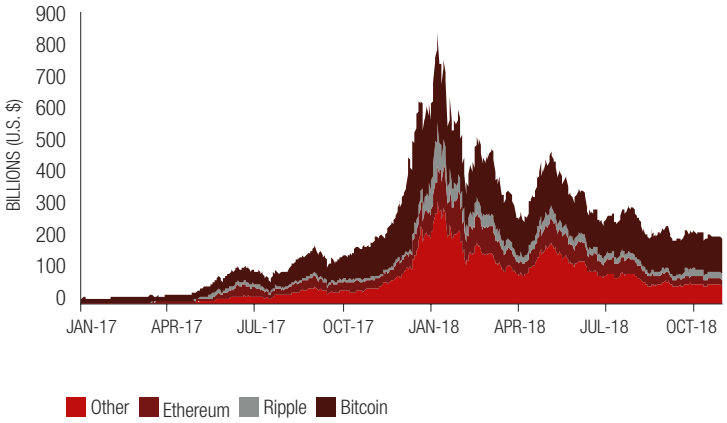
3.2 The typology of token offerings

There are six different token offering models [Momtaz (2019b)]:

1. Traditional token offerings (ICO): in a token offering in the traditional sense, firms offer different types of tokens (see below) in exchange for fiat money or cryptocurrencies. This token offering type is closely related to IPOs. Classic token offerings are often preceded by pre-offerings, in which firms raise money to finance the actual token offering and gauge market demand. If the token offering is approved by the SEC, it is often called a "security token offering" (STO).

2. Interactive token offering (IICO): IICOs counteract criticism of traditional token offerings related to token valuation. Many token offerings are uncapped, which means that they raise as much money as they can. A downside of this model is that the token valuation is not transparent to investors. The IICO model helps to overcome this issue by implementing a dynamic bidding system, in which investors can voluntarily bid and withdraw their bid during the bookbuilding process, which may result in an efficient price equilibrium.

Figure 4: Listed market volume



3. Initial supply auction (ISA): the ISA model is based on a mechanism that discriminates the token price. ISA transactions sell tokens at a high price that decreases gradually until the funding demand is covered. However, this model has received criticism as it does not reward early investors for taking higher risk and signaling quality to the market, leading to disappointed investors due to missing economic incentives and higher token offering failure rates [Hellmann and Puri (2002), Momtaz (2019a)].

4. Simple agreement for future tokens (SAFT): the SAFT model addresses legal concerns in other token offering models and is mostly employed in pre-offerings. The idea is to offer investors the right to receive future tokens (mostly of the utility type, see below) that will be incorporated into a specific platform. The model is adapted from the "simple agreement for future equity" contract.

5. Airdrops: airdrops are free giveaways of tokens to anyone with a known wallet address. This model is used to create knock-on effects for platform growth via user adaptation in 33.5% of token offerings (Figure 3d). The firm that issues the tokens is still able to raise funding by retaining a share of the tokens that can be traded against other cryptocurrencies once the token is listed.

6. Smartdrops: smartdrops operate in the same spirit as airdrops with the difference that smartdrops only distribute tokens among those users with interest in the specific platform's innovation. Hence, they are a popular way of introducing the new technology and fast-tracking community growth. In a similar vein, bounty programs, used in 26.3% of token offerings (Figure 3e), incentivize interested participants for various activities associated with the token offering (e.g., the creation of a token logo or advertising the token offering on social media channels in exchange for tokens).

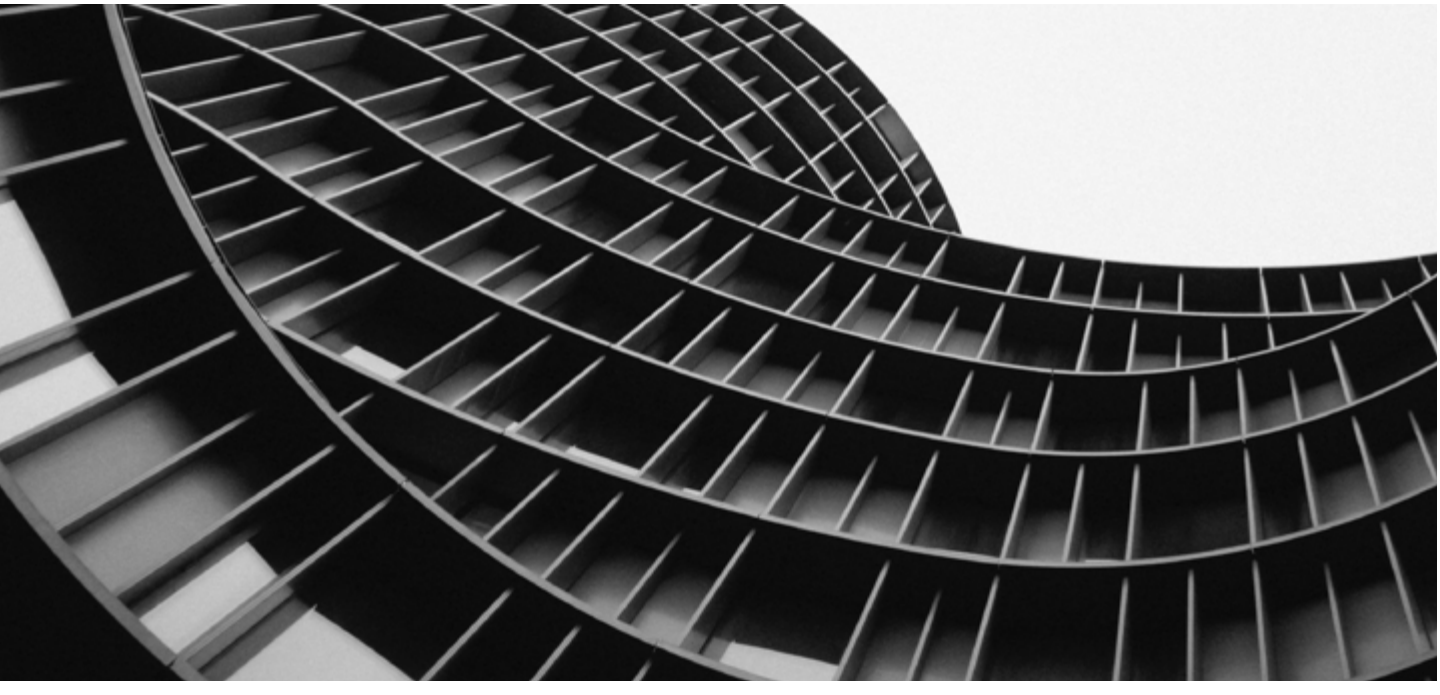
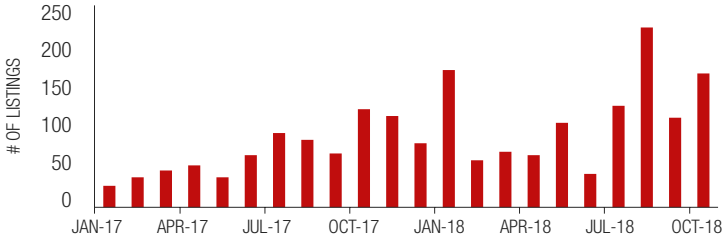
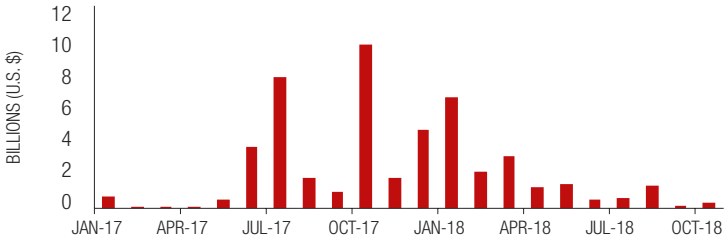


Figure 5: Listing activity

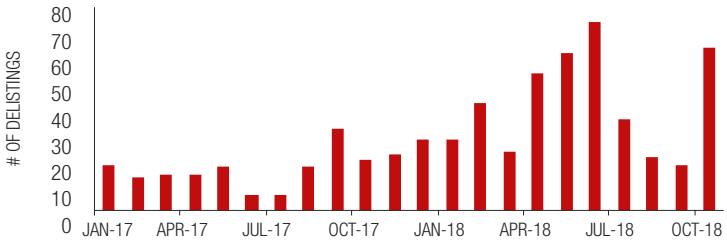
a) Number of listings



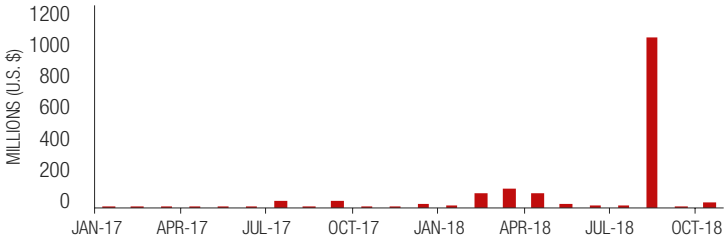
b) Listing volume



c) Number of delistings



d) Delisting volume



3.3 Token classifications

Depending on the implemented token features, token offerings can be viewed as something between venture capital financing, a crowdfunding campaign, and an initial public offering. While, in principal, each token may have very specific characteristics that distinguish it from others, we have seen an emerging discussion about token classifications. Though there does not exist any unique standard for classifying tokens, one may broadly distinguish four types:

1. Utility tokens: charter a promise that the investor can redeem the token like a voucher for the company's products or services. These tokens do not transfer ownership and control rights, and legal investor protection for this token type is currently almost nonexistent.

2. Security tokens: are in most jurisdictions subject to securities laws as their value is based on the performance of the underlying asset. If the underlying asset performs well, the token gains value and vice versa. However, a security token does not necessarily involve an ownership stake in the third-party asset or venture.

3. Equity tokens: are a sub-classification of security tokens, and constitute, in a sense, 21st century stocks, which record corporate ownership and corresponding voting rights on a blockchain. As with regular stock purchases, token holders own their given percent of the token-issuing enterprise.

4. Pure currency tokens: are digital currencies, with bitcoin being the most prominent example. In most jurisdictions they fall under asset regulations for the purpose of taxation. These tokens do not represent a stake in a third party but derive their value from regular market forces like a commodity.

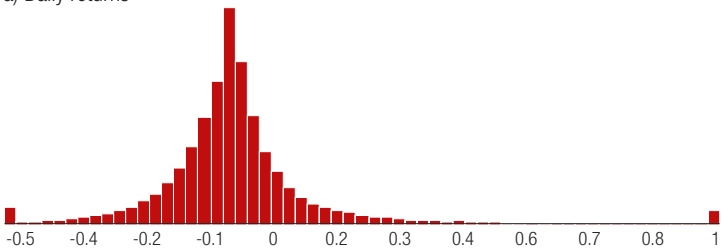
Although the public discussion about tokens suggests that investors often think of tokens in the sense of stocks, empirical evidence reveals that until today the crypto market has been dominated merely by utility tokens. About 69% of all token sales can be classified into this category and overall utility tokens reflect more than 90% of total funds raised. In contrast, only 5% (or 3% of total funds raised) are reflected by security tokens, with less than a handful of them being equity tokens.

Table 1: Performance on the first listing day

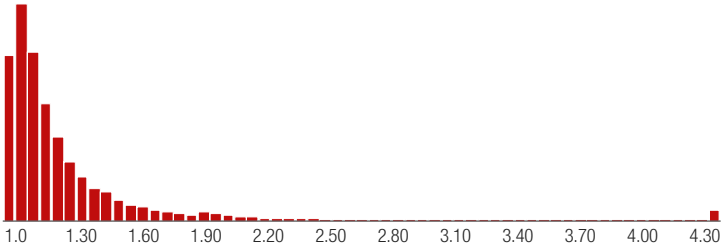
	N	MEAN	SD	MEDIAN	PERCENTILES	
					25TH	75TH
FIRST-DAY RETURNS	2,728	0.118	0.313	-0.015	0.021	0.137
HIGH/LOW-RATIO	2,728	3.245	54.181	1.057	1.177	1.494
LISTED CAPITAL (U.S.$MIL)	2,181	30.737	394.543	0.079	0.996	9.045
CIRCULATING SUPPLY (MIL)	2,181	145,632.4	6,330,972.0	4.830	33.059	206.353

Figure 6: Risk-return characteristics of listed tokens

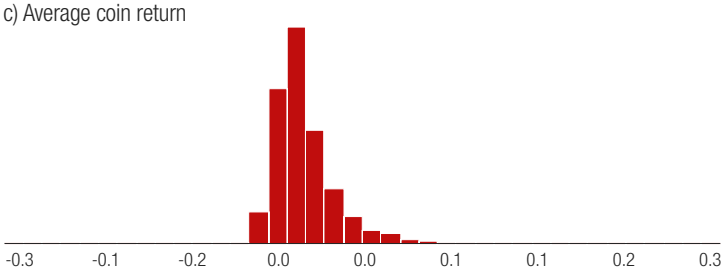
a) Daily returns



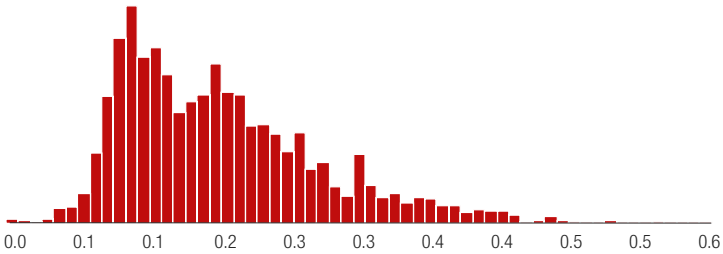
b) Daily high/low ratio



c) Average coin return



d) Coin volatility



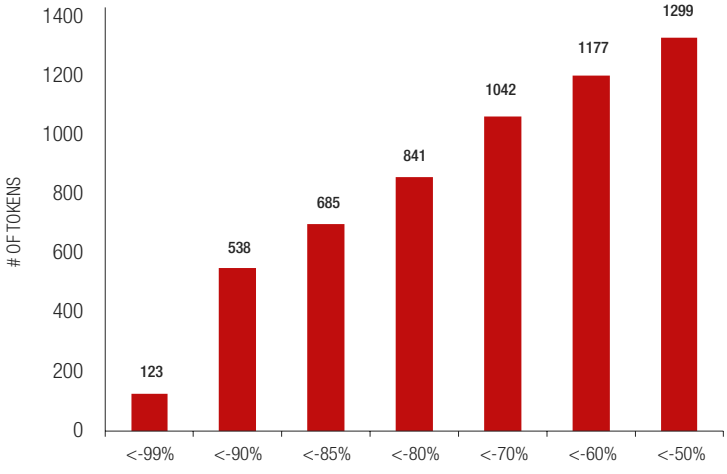
Despite this public view on utility tokens as quasi-stocks, they have in fact little in common with traditional equities. Among other things, it is probably the increased awareness of this mismatch between public expectations about utility tokens and their actual characteristics that has contributed to a slowdown in crypto market growth and investor interest in token offerings during the second half of 2018. The missing investor protection, the extremely uncertain upside they provide to investors, and the negative market sentiment induced by numerous examples of utility tokens that have been issued with fraudulent intent may explain a significant share of the uncertainty observed in the markets for listed crypto capital during the recent period [for a comprehensive analysis of investor sentiment in crypto markets see Drobetz et al. (2019)]. To get an overview of the historical performance of token offerings, the following section analyzes a comprehensive sample of listed tokens.

4. PERFORMANCE APPRAISAL OF LISTED TOKENS

Though not all tokens have been listed on exchange platforms after issuance, there are nevertheless market prices available for a large proportion of the overall crypto market. Using historical market data from Coinmarketcap for 2,728 listed tokens observed over the period from January 2017 through October 2018, this section presents an overview of the evolution of listed crypto capital as well as an assessment of the risk return profile and lifetime performance of the average token.

Figure 4 shows that listed market capitalization experienced a rapid increase during the second half of the year 2017 and peaked in January 2018. However, although there is a significant number of new listings during that time (see Figure 5a), the major share of the observed growth in market capitalization stemmed from

Figure 7: Overview of token-lifetime performance



a massive price increase in the dominating crypto assets; bitcoin, ethereum, and ripple. That is, the large number of token offerings and subsequent listings over our sample period has not significantly changed the market for listed crypto capital. This becomes even more obvious if we compare the total listing volume by month (Figure 5b) with the overall market capitalization. Furthermore, the decrease in market size for the period from January 2018 until October 2018 is accompanied by a notable wave of delistings (see Figures 5c and 5d). This observation is further in line with the negative trend in token offerings that we already discussed in the previous sections.

To better understand the characteristics of tokens that eventually get listed, Table 1 shows performance measures for all sample tokens on their listing day. First-day returns are significantly positive on average while median first-day returns are negative. The documented percentile values indicate that the distribution of first-day returns is right skewed with some extreme outliers driving the positive performance on average. A similar distribution is observed for token size as measured by the tokens market capitalization. The median token has a market capitalization of U.S.$0.08 mn while the average token has a total market value of U.S.$30.7 mn, indicating that the universe of listed crypto capital is driven by a few very large tokens. This picture is also supported when looking at the average (median) circulating supply of our sample tokens.

Emphasizing this investor perspective on token offerings, we note from Figure 6a that the distributional characteristics of daily returns over the full sample does not significantly deviate from that on the first listing day. Figure 6a reveals that the median daily token return is significantly negative. This negative median performance is accompanied by large daily fluctuations in token prices as shown by the widespread distribution of high/low ratios (Figure 6b). Analyzing the average daily performance at the token level, we see that the average token has a slightly positive daily return, though the distribution is right-skewed as well (Figure 6c). In line with the large high-low ratios, calculating daily return volatility at the token level confirms that token investments are extremely volatile and not comparable to stock investments in terms of their risk and return characteristics (Figure 6d). This average daily risk-returns profile of listed crypto assets transforms into a widespread distribution of token lifetime performance in the long run.

Although there are examples of token success stories, the majority of listed tokens shows a poor lifetime performance. Overall, 23% of all tokens that have ever been listed on an exchange platform are reported as inactive in the end. Based on our sample, only 36% of all listed tokens exhibit a positive lifetime performance. This heterogeneity in lifetime performance becomes particularly obvious in Figure 7, where 1,299 of our 2,728 tokens in the sample lose more than 50% in value over their observed lifetime. About 25% of all tokens even lose more than 85% in value. This poor long-term performance might be just a snapshot. However, it was observed during a period when token offerings have been extremely popular. Eventually, these figures demonstrate that investments in crypto assets come with substantial risks [for a more comprehensive review of the long-run performance of cryptocurrency and ICOs, see Momtaz (2018d)]. Strategies to deal with and regulate these risks will be the key to a blockchain-based capital market.

5. LESSONS LEARNED AND NEXT STEPS

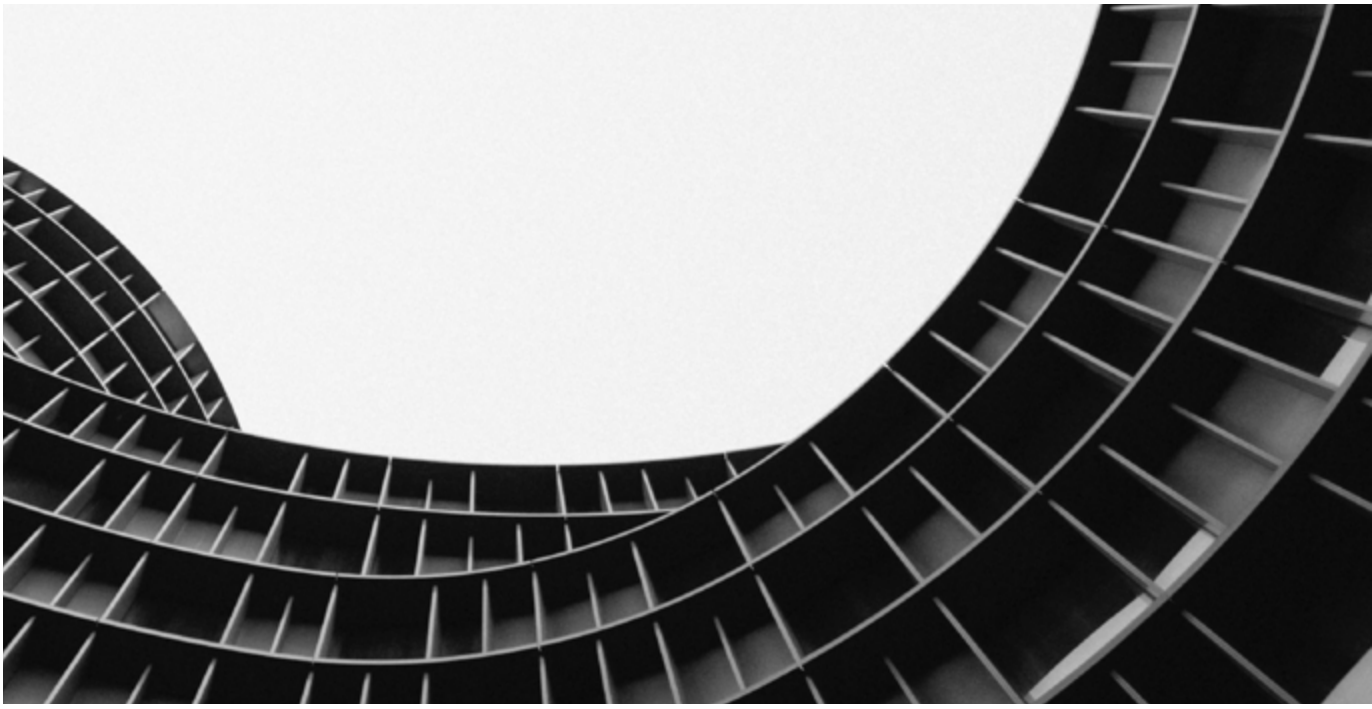
Token offerings may be a significant revolution in entrepreneurial and corporate finance. The technical flexibility of smart contracts makes it possible, in principle, to conduct each financial transaction on a blockchain, thereby saving time and money for all parties involved. Additionally, token offerings enable firms to achieve goals that cannot be reached by traditional financing

mechanisms such as the unification of the investment and payment instrument and future customer commitment [Momtaz (2019b)].

> "Information asymmetries and moral hazard are the main challenges that ventures, investors, and policy-makers need to address for this new industry to flourish."

However, for the token offerings market to mature, the blockchain-finance industry has to overcome at least two crucial roadblocks. First, perfect disintermediation creates a vacuum of trust [Rhue (2018)]. The first wave of token offerings that we witnessed over the past two years was unprecedented in terms of informational asymmetries. In the absence of hard information, investors rely on professional network profiles [Momtaz (2018c)] and the perceived emotional stability of CEOs during roadshows [Momtaz (2018a)] to gauge the quality of token offerings. But this information is by no means sufficient and hence concurrent studies of the role of information disclosure document conflicting evidence [Blaseg (2018), Howell et al. (2018)]. The high levels of informational asymmetries paired with the fact that the maximum token supply is usually fixed in a token offering may create a severe moral hazard in signaling [Momtaz (2019a), Malinova and Park (2018), Dittmar and Wu (2018)]. Fundraising firms can usually tap the market only once because the maximum token supply is predefined on immutable terms in the underlying smart contract. This may create a moral hazard because firms aim to maximize their funding amount. Momtaz (2019a) finds that firms exaggerate information in white papers, effectively a moral hazard in signaling, which the investors only learn in the aftermarket when the token price plummets. One potential way out of this dilemma is, paradoxically, the introduction of an intermediary in the market for token offerings. An intermediary would be involved in many transactions, hence has an interest to maintain a trustful relationship with the investor base. This creates an incentive to screen and monitor a firm's signaling and information disclosure, resulting in more efficient markets. The intermediated token offering model could still be superior to traditional methods of external finance by keeping transaction costs (e.g., associated with bookbinding, record-keeping, investor communications, and the settlement of these transactions) at a minimum.

Second, regulators have to catch up with the industry developments to improve investor protection without destroying already functioning market structures. Malinova and Park (2018) report that 85% of the activity in the market for token offerings is fraudulent. There are some impediments to the regulation. First, cryptocurrencies were born partly out of a preference for privacy and the pseudo-anonymous nature of token holders' identities may be an obstacle in identifying and prosecuting shady activities. Second, and more importantly, it is not clear how any national token-law enforcer would be able to prosecute a globally distributed platform on its own. We see two potential ways going forward: one is to create incentives for blockchain-based firms to opt into a national regulation. Switzerland practices such an "opt-in" approach already successfully, creating a competitive advantage over other jurisdictions. The other, perhaps complementary way is for national regulators to form a supranational institution to create international standards and guidelines for token offerings.



REFERENCES

Amsden, R., and D. Schweizer, 2018, "Are blockchain crowdsales the new 'gold rush'? Success determinants of initial coin offerings," working paper, McGill University and Concordia University

Blaseg, D., 2018, "Dynamics of voluntary disclosure in the unregulated market for initial coin offerings," working paper, Goethe University Frankfurt

Boreiko, D., and N. K. Sahdev, 2018, "To ICO or not to ICO – empirical analysis of initial coin offerings and token sales," working paper, Free University of Bolzano and Massachusetts Institute of Technology

Dissanaike, G., W. Drobetz, P. P. Momtaz, and J. Rocholl, 2018, "Does the enforcement of takeover law affect corporate acquisitions? An inductive approach," working paper, University of Cambridge

Dittmar, R. F., and D. A. Wu, 2018, "Returns to initial coin offerings: an empirical examination," working paper, University of Michigan

Drobetz, W., and P. P. Momtaz, 2019, "Corporate governance convergence in the European M&A market," Finance Research Letters, forthcoming

Drobetz, W., P. P. Momtaz, and H. Schröder, 2019, "Investor sentiment and initial coin offerings," Journal of Alternative Investments, forthcoming

Fisch, C., 2019, "Initial coin offerings (ICOs) to finance new ventures," Journal of Business Venturing 1, 1-19

Hellmann, T., and M. Puri, 2002, "Venture capital and the professionalization of start-up firms: empirical evidence," Journal of Finance 57, 169–197

Howell, S., M. Niessner, and D. Yermack, 2018, "Initial coin offerings: financing growth with cryptocurrency token sales," working paper, National Bureau of Economic Research

Huang, W., M. Meoli, and S. Vismara, 2018, "The geography of initial coin offerings," working paper, University of Ghent

Kim, J.-H., and L. Wagman, 2016, "Early-stage entrepreneurial financing: a signaling perspective," Journal of Banking and Finance 67, 12–22

Malinova, K., and A. Park, 2018, "Tokenomics: when tokens beat equity," technical report, University of Toronto

Momtaz, P. P., 2018a, "CEO emotions and underpricing in initial coin offerings," working paper, University of California Los Angeles

Momtaz, P. P., 2018b, "Initial coin offerings," working paper, University of California Los Angeles

Momtaz, P. P., 2018c, "Initial coin offerings, asymmetric information, and loyal CEOs," working paper, University of California Los Angeles

Momtaz, P. P., 2018d, "The pricing and performance of cryptocurrency," working paper, University of California Los Angeles

Momtaz, P. P., 2019a, "Entrepreneurial finance and moral hazard: evidence from token offerings," working paper, University of California Los Angeles

Momtaz, P. P., 2019b, "Tokens sales and initial coin offerings: introduction," Journal of Alternative Investments, forthcoming

Rhue, L., 2018, "Trust is all you need: an empirical exploration of initial coin offerings (ICOs) and ICO reputation scores," working paper, Wake Forest University

FUTURE-PROOFING INSURANCE: ASIA INSURERS GEARING UP FOR DIGITIZATION

ISABEL FELICIANO-WENDLEKEN | Managing Principal, Capco
EDITH CHOW | Principal Consultant, Capco
MATTHEW SOOHOO | Consultant, Capco
RONALD CHEUNG | Consultant, Capco[1]

ABSTRACT

Recent fundamental demographic and market shifts in Asia signal the need for insurers to look at the products, processes, and enabling technology required to stay relevant in the new era. Success in the region will require more than the insurers' own digital enablement. Effective application of emerging insurtech innovations specific to these markets will be critical to earn the right to play and win in the region. In this paper, we examine the economic and regulatory factors that are unique to Asia, as well as the diverse and evolving needs of regional consumers. An understanding of these factors and how they are inevitably linked to one another will help distill the nuances of what insurtech means to insurance companies and how it can help them gain competitive edge. This study delves into five key insurtech trends. It also looks at insurtech innovations and their use-cases that provide opportunities for insurers to shape their digital agenda and achieve growth in the region.

1. INTRODUCTION

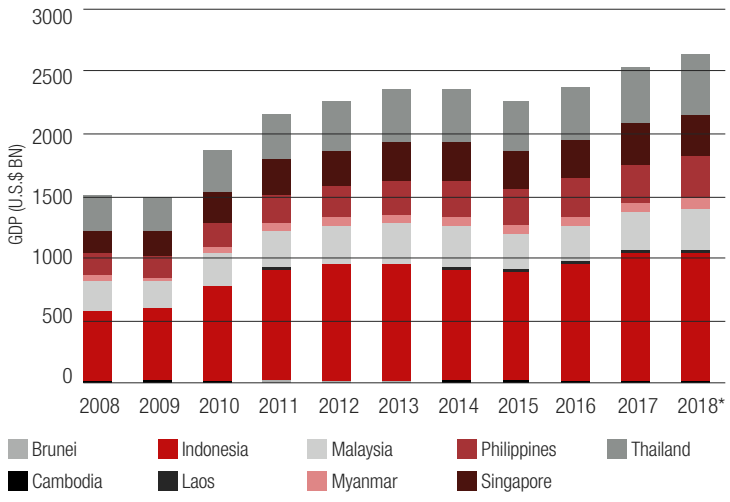
Major economic, societal, and technological trends are redefining the boundaries in which insurance companies operate in Asia. The region is experiencing unprecedented growth ushered in by urbanization and a burgeoning middle-class wealth. Coupled with lower regulatory barriers in certain countries, it offers important growth opportunities for insurers amidst a lackluster global outlook. These opportunities are currently underpinned by a wave of emerging insurance technologies and the unique demands of Asian consumers that in turn have profoundly impacted the way insurers operate in this increasingly competitive market.

There have been significant strides made by the industry to adopt emerging technologies to complement the value chain, adjust their business models and products, or entirely change the way they operate. In recent years, the insurance industry has embraced digital transformation in a bid to improve distribution, product margins, and, above all, to match or exceed customer expectations.

Recent fundamental demographic and market shifts in Asia signal the need for insurers look at the products, processes, and enabling technology to stay relevant in the new era. Success in the region will require more than the insurers' own digital enablement. Effective application of emerging insurtech innovations specific to these markets will be critical to earn the right to play and win in the region.

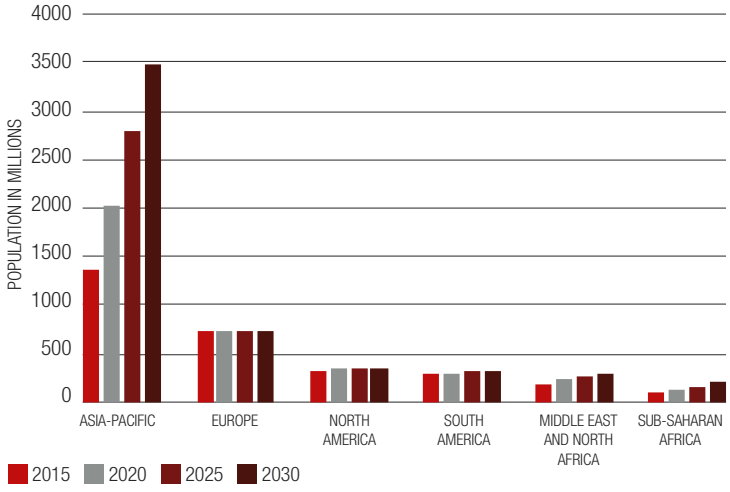
[1] The authors would like to thank Dominic Poon, Consultant, Capco for his contribution to this article.

Figure 1: ASEAN GDP growth (2008-2018)



Source: Statista.com

Figure 2: Global middle class growth forecast



Source: Statista.com

In this study, we examine the economic and regulatory factors that are unique to Asia, as well as the diverse and evolving needs of regional consumers. An understanding of these factors and how they are inevitably linked to one another will help distill the nuances of what insurtech means to insurance companies and how it could help them gain competitive edge. This study delves into five key insurtech trends. It also looks at innovations and their use-cases that provide opportunities for insurers to shape their digital agenda and capture growth opportunities in the region.

2. CHANGING ENVIRONMENT – ASIA IS THE BRIGHT SPOT

2.1 Understanding the potential of Asia

To gain a good understanding of the insurance industry in Asia, we need to take into account the macroeconomics of the region, as the industry's growth often moves in tandem with the economic progress of a country. In the era of tempered global economic growth, Asia is one of the bright spots. From a general insurance standpoint, Asian countries (excluding Japan) accounted for 76% of the overall global insurance industry premium growth in 2017 (U.S.$157 billion).[2] Life insurance experienced a 14% growth in premiums, with China accounting for nearly 80% of it (U.S.$73 billion).[3]

Spotlight on China: China has been experiencing a steady GDP growth of around 6% year-on-year, helping it become the second largest economy in the world. Its insurance market has also grown to become the third largest in the world. In the period of 2010-2015 alone, the Chinese market grew by 80% to reach U.S.$385.5 billion in gross written premiums, outpacing Japan and the U.S.

Southeast Asia: during a similar period, economies of the Association of South East Asian Nations (ASEAN) has experienced similar growth. From 2008 to 2018, ASEAN GDP grew significantly from U.S.$1.7 trillion to U.S.$3 trillion (Figure 1).

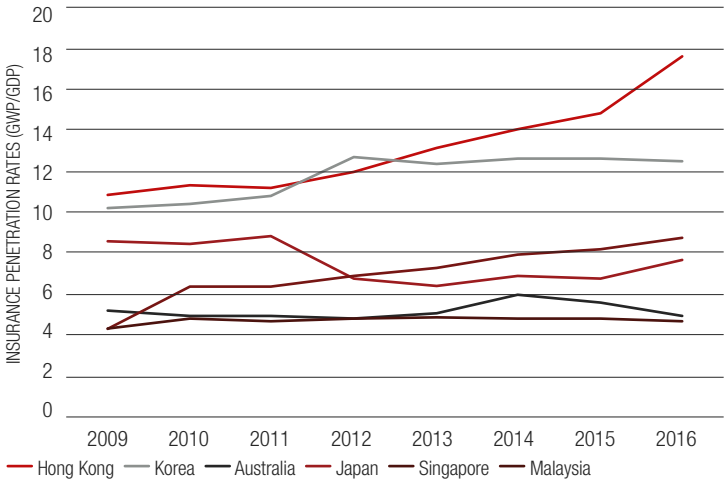
2.2 Shifting economic tides and customer preferences

Although the demographic changes in Asia's are impacting demand for insurance products, the industry must also account for the nuances of consumption patterns in the region.

Like their peers in the west, Asians consumers are open to innovation and value how new technologies are helping them connect with the rest of the world (smart phone users in the region have increased from 39 million in 2007 to potentially 1.81 billion in 2018).[4] The modern Asian consumer is also more educated and faced with more choices than previous generations. For these

[2] Asia Insurance Law Review, 2018, "Asia: region powers 76% of growth in global insurance markets," April 27, https://bit.ly/2Cic4FS
[3] Asia Insurance Law Review, 2018, "Asia: region powers 76% of growth in global insurance markets," April 27, https://bit.ly/2Cic4FS
[4] eMarketer, 2017, "Internet and mobile users in Asia-Pacific: eMarketer's country-by-country forecast for 2017-2021," November 21, https://bit.ly/2AQVIEv

Figure 3: Select APAC countries' insurance penetration rates (2009-2016)



Source: OECD

consumers, the traditional model of relationship-based sales for simple financial solutions and products is no longer adequate.

Asia's growing millennial generation has greater purchasing power than the baby boomers' and gen-Xers that came before them. Their "me-first" mentality has been continuously influenced by technologies, where internet access, coupled with pervasive social media, have changed the modes of consumption. Consumers now demand a multitude of choices at their disposal, price transparency, convenience, and simplicity with the aim of instant gratification. Personalized, face-to-face interactions accompanied by branch visits and meetings with insurance agents are no longer the expectation.

In addition, the number of people joining the middle classes in the region is also growing, by an average of 10.5% (Figure 2). One example is in Indonesia, where the middle and affluent classes are expected to grow to 135 million by 2030.

According to a recent report by the Brookings Institute, the new middle classes will be predominantly Asian with "almost nine in ten out in China, India and South and Southeast Asia." This offers great promise for businesses, including insurance companies, as this segment is projected to reach 4 billion people by 2020 and 5.3 billion globally by 2030.

Brookings Institute further calculates that the middle-class markets in China and India will reach U.S.$ 14.1 trillion and U.S.$ 12.3 trillion by 2030, respectively. By comparison, the U.S. middle class market is projected to be U.S.$15.9 trillion by 2030.[5]

In China, the domestic sharing economy has already reached U.S.$500 billion in 2016 and is projected to grow by an average annual rate of 30% over the next five years.[6] The way insurance is delivered has been greatly influenced by this shift in consumer demographics and preferences.

The combination of surging affluence, flourishing societal and political landscapes (evidenced by becoming home to 46% of the world's population by 2020), globalization of economic policies, and liberalization of regulations has set Asia on course to take a prime position in the demand for insurance, and digital as its preferred channel.

Despite the increase in premium growth, the region still has a long way to go to reach the more developed insurance markets of the worlds. The average per capita spending on insurance coverage is the around U.S.$357, which is considerably lower than the average for the rest of the world, which is U.S.$1,340. According to Forbes, Asia holds 43% of the world's population but only 13% of total premiums in 2016.[7] The combined market size of Indonesia, Thailand, the Philippines, Vietnam, and Malaysia in 2015 was only 13% of Japan's and 4.5% of the U.S., in terms of gross written premiums. The penetration rates for life and non-life insurance combined stands at about 1% to 5.5% for these five nations, as opposed to about 11% for Japan and 7% for the U.S.[8] This deficiency highlights the significant opportunity for insurers to capture the uninsured and further foster financial inclusion.

Countries that have experienced significant growth in penetration rates in the past seven years are Singapore, Hong Kong, and Korea, with the latter two being the highest in the region. Singapore has shown strong signs of stable growth and the potential to catch up with HK and Korea, per OECD data. Other countries in APAC have a stable penetration rate of around 5% to 7%, with HK leading the way at 17.6% (Figure 3). This could be considered as a benchmark, acting as a barometer towards which other countries can strive.

[5] Kharas, H., and K. Hamel, 2018, "A global tipping point: half the world is now middle class or wealthier," September 27, https://brook.gs/2xMJ5c7

[6] Yang, Y., 2018, "China's sharing economy is minting multibillion-dollar tech unicorns," South China Morning Post, March 8, https://bit.ly/2DtljVF

[7] Choi, M., 2018, "How Asia's entrepreneurs are disrupting the finance industry," Forbes, March 26, https://bit.ly/2DqBKSL

[8] Tani, S., 2017, "Insurance promises Asia much more than peace of mind," Nikkei Asian Review, March 23, https://s.nikkei.com/2R2eNZr

3. ALL ROADS LEAD TO DIGITAL

Insurance has always been a data business. It covers various risks by creating pools of funds based on different insurance lines factoring in loss probabilities as well as consumer behavior. Forecasting these risks with greater accuracy and providing transparency to consumers will positively impact insurance premiums and create opportunities for customer segmentation. This can also have the ripple effect of creating new business models and products.

Globally, the traditional agency and bancassurance models are slowly being replaced through richer data engineering. However, the biggest disruptions to the industry is coming from digital, in both consumer and peer-to-peer business models. A recent study has suggested that the global "digital insurance market" will grow at an annual CAGR of 13.7% for the next five years.[9]

Big Tech has since cannibalized the industry in terms of distribution, marketing, and product sophistication. Chinese tech giants Tencent and Alibaba together established Zhong An, the first online only property insurance company, and have jointly entered the market to capture a slice of the sizeable industry by leveraging their vast, pre-existing communities as a ready-made channel to distribute their insurance products. Simultaneously, new and innovative products that insure against trends and current events have led to the rise of micro insurance. For example, Zhong An's medical policy on "overdrinking" during the 2014 World Cup period offered medical fees for intoxicated fans. The company also offered a "Night Owl insurance," which also covered medical and emergency related expenses.

The industry has also recognized the value of digitization. The development of digital-only offerings such as Kyobo Lifeplanet, Singapore Life, and Vouch allows for more leads to be generated through the digital ecosystem than through traditional agents. In December 2018, the Hong Kong Insurance Authority granted a virtual insurance license to Bowtie, a Sun Life-backed digital start-up, which plans to directly offer consumers commission-free health-focused insurance products.[10] It is expected to be up and running by mid-2019. This direct-to-consumer trend poses a great threat to insurance agents and brokers.

Asian customers are increasingly tech savvy and mobile, with ever-increasing expectations from their insurance providers on products, services, and pricing – at every significant stage of their lives. In addition, individual consumers are increasingly relying on mobile phones as a channel to interact with their financial services providers. There has been a gradual increase of mobile phone user penetration throughout the region, expected to reach nearly 60% by 2019. Insurtech companies can offer prospective digital customers their services via mobile phones and bypass traditional agents.

4. DEAL FLOWS

The convergence of the aforementioned macroeconomic trends has resulted in an influx of global intellectual capital and an appetite for investments. There were U.S.$697 million of insurtech funding in Q4 2017 alone, and a total of U.S.$2.3 billion for the entire year – a 36% increase from U.S.$1.7 billion recorded in 2016. Industry incumbents and new entrants to the market have both pushed towards greater digitization.[11]

The Chinese market again shined brightest, where there was a 44% increase in funding to 173 tech start-ups from 2016 to 2017. The listing of Zhong An, the first digital-only insurer, was a milestone for the industry. With its successful IPO in Hong Kong in September 2017 it raised U.S.$1.5 billion, making it the largest insurtech company in the world. One of Zhong An's initial founders is Ant Financial, an affiliate of Alibaba, which operates the world's largest digital payment platform. Its strength in technology and client resources supported Zhong An's successful product development of an e-commerce insurance product. Such investments in the development and adoption of new insurance technologies is expected to result in savings of around U.S.$ 300 billion per year for the Asian insurance industry by 2025.[12]

Over the past two years alone, there have also been significant deals and partnerships between insurance companies and insurtechs across different Asian countries. The overarching goals of these deals are to improve the

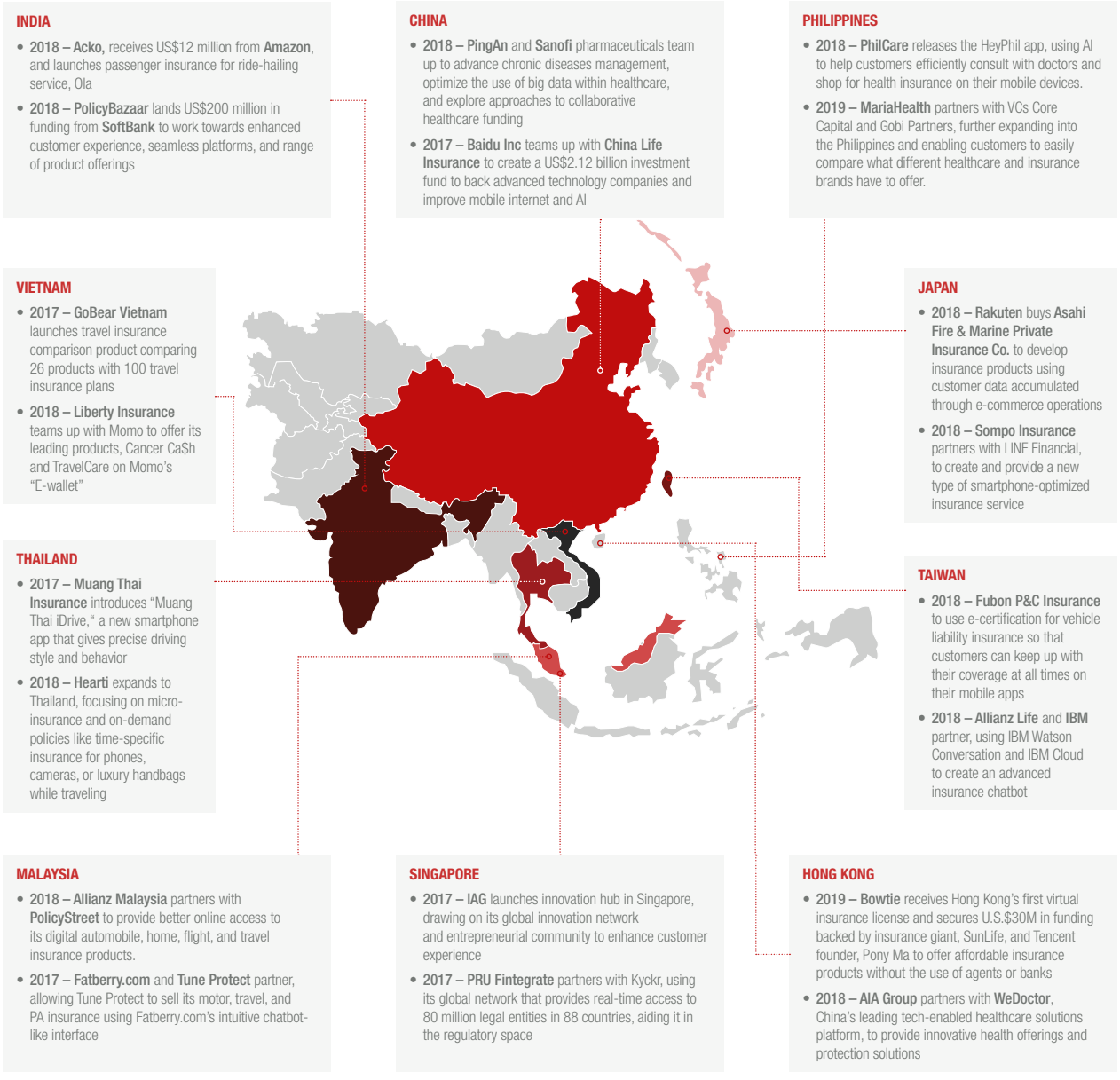
[9] https://bit.ly/2HnM9Cr
[10] Insurance Asia News, 2018, "Sun Life invests in 'virtual' Hong Kong startup Bowtie," December 21, https://bit.ly/2RDNoCi
[11] Willis Towers Watson, 2018, "Quarterly InsurTech briefing Q4 2017," February 1, https://bit.ly/2nEZ5Yk
[12] UBS, 2017, "Insurance, technology and Asia: how are they interconnected?" September 4, https://bit.ly/2RGTCBE

customer experience, create innovative products, gain market scale, and generate efficiencies. The highlighted partnerships in Figure 4 is a testament to the fact that Asia is supportive of insurtech's wider adoption. We expect more deals – partnerships, mergers, or outright acquisitions – to further accelerate the seamless delivery of the insurance value chain to the customers.

5. THE STATE OF PLAY – INCUMBENTS AND INSURTECHS

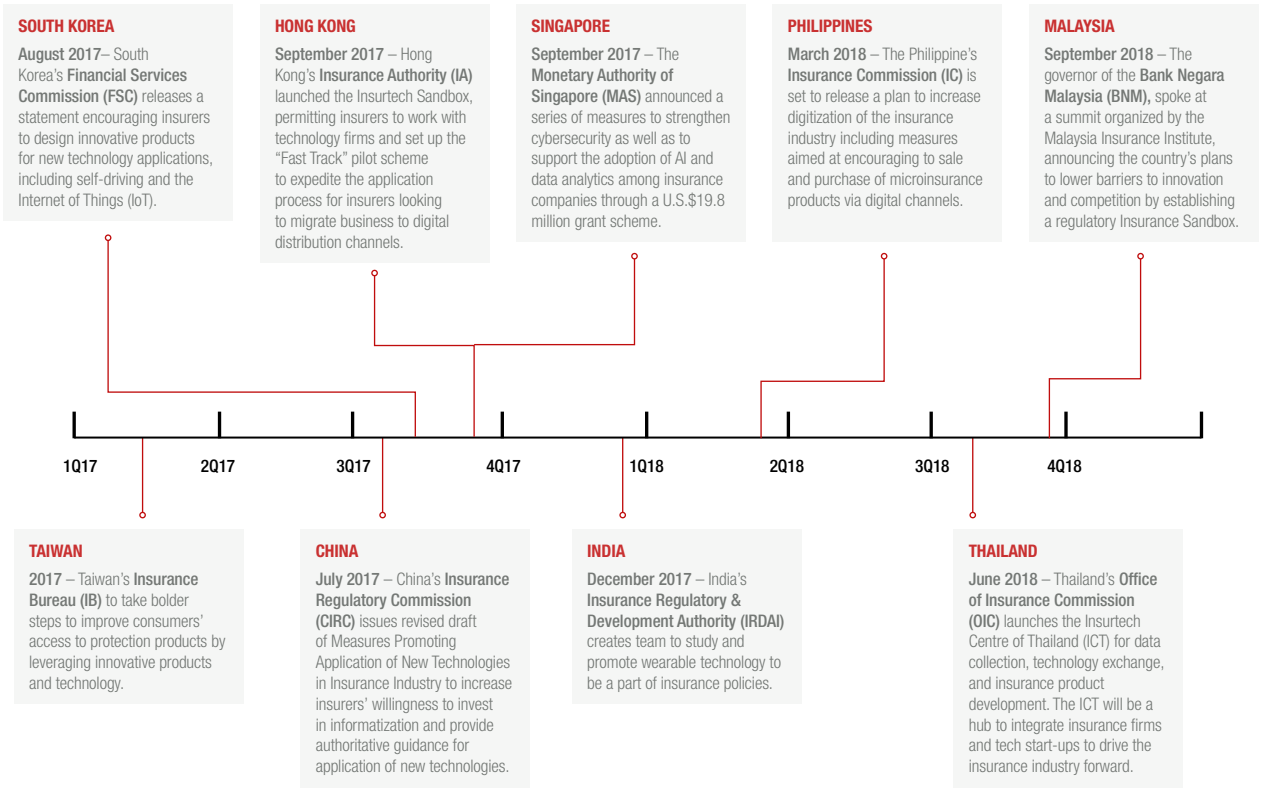
In an era where speed, convenience, and flexibility are no longer sources of differentiation but customer expectations, established players and newcomers alike have had to move up the learning curve quite rapidly. Banking and capital markets players have adjusted their digital agenda and placed innovation and technological

Figure 4: APAC insurtech deals landscape (note worthy deals and partnerships in the region)



Source: Capco Digital research and analysis

Figure 5: APAC regulatory landscape timeline



Source: Capco Digital research and analysis

transformation high on their list of priorities. The insurance industry is not far behind. It is collectively working on ways to accelerate their own transformations to keep pace with their consumers' changing needs and preferences.

However, the same questions that the early adopters of fintech faced in the banking and capital markets sectors, are now points of considerations for the insurance sector. At what rate should we pursue new technologies at the expense of our current working business models? Will it benefit our company and customers to be the first mover? Or is it a safer bet to be a fast follower? How should my organization approach and engage with emerging technologies?

What we observed in the earlier fintech wave was that the industry and emerging technologies could not be completely decoupled from one another. The key to having a meaningful technological impact and to unlocking the value of emerging technologies lies in the fusion between business and technology. This can only occur with a deep understanding of business, product, customer, and distribution channels. Insurers seem to be acutely aware of the potential of technology to disrupt their value chains but are still cautious in comparison to their banking peers. As of the third quarter of 2018, Asian insurers have spent U.S.$35.2 billion on technological advancements, up from U.S.$32.9 billion in 2016.

5.1 The regulatory landscape

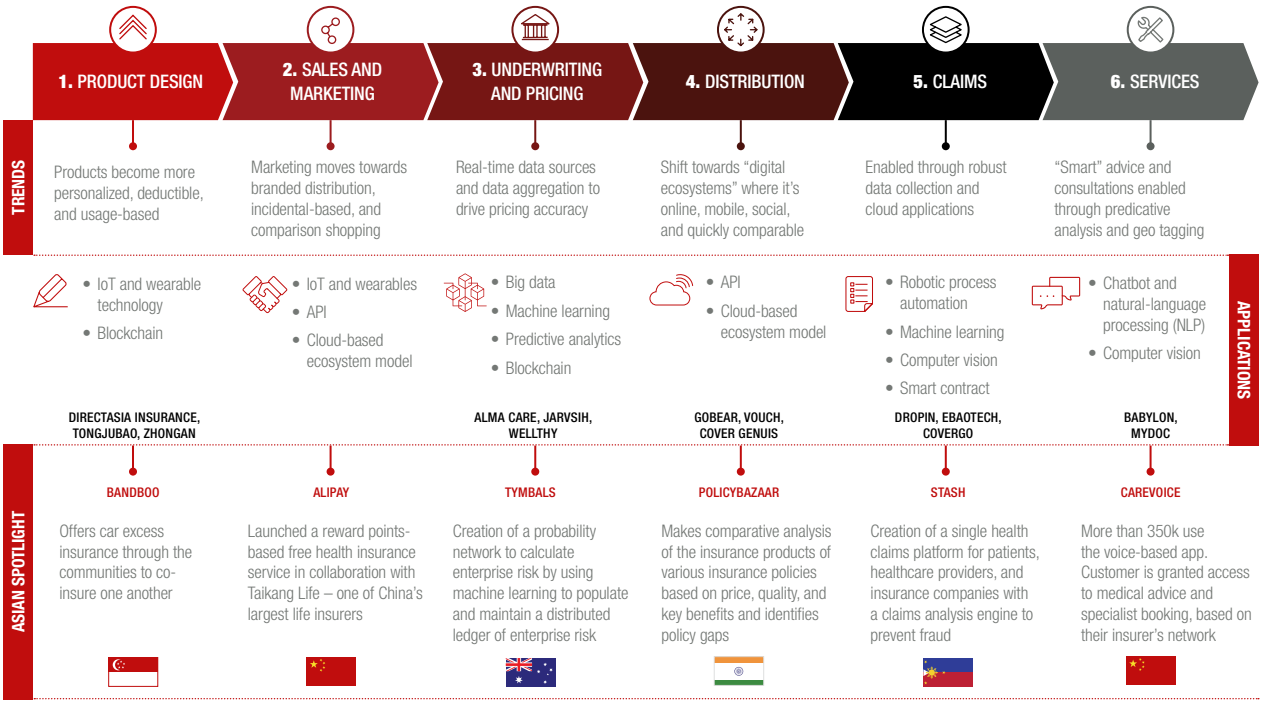
While the insurtech innovation wave has been in sync with macroeconomic developments, regulatory bodies have also played an important role. With the guidance and encouragement from these local agencies, several countries in the region have experienced tremendous growth in insurance technologies and their industry's and nation's overall health. Over the past year, emerging and

incumbent insurance companies have heeded the advice of their respective government regulators and followed their lead by partnering with technology firms to develop new products and simplifying the lives of insurance customers throughout the region.

Instead of pushing back and limiting the potential of these partnerships between insurance companies and technology firms, regulators such as Hong Kong's Insurance Agency (IA) and the Bank Negara Malaysia (BNM) are now launching programs to encourage the establishment of insurtechs. The IA recently set up their "Fast Track" pilot scheme to expedite the application process required for insurance companies when attempting to use digital, online distribution channels. It has led the way by launching an Insurance Sandbox that permits Hong Kong insurers to work with technology firms to experiment with new insurtech applications for their business operations. The BNM has also recently held a summit at the Malaysia Institute of Insurance, where the authority's governor spoke about the country's plans to lower barriers to innovations and competition by establishing their own regulatory Insurance Sandbox. Both of these regulatory bodies have made great strides in advancing these partnerships by lowering pre-existing barriers in a move that has become a necessary step in allowing the insurtech industry to thrive and provide customers with the products they demand.

Other countries have taken a different route to boost insurtech. By promoting the use of technology in their products and encouraging insurance firms to digitize, they have outlined a path for insurers to modernize their business strategy to help customers reap the benefits of insurance products of all kinds. The Monetary Authority of Singapore (MAS), the Philippines Insurance Commission (IC), and Korea's Financial Services Commission (FSC) have all announced plans to support the industry by promoting the development and application of new technologies in their products. The MAS has already gone as far as announcing a U.S.$20 million grant scheme that will encourage insurers to use AI, data analytics, and other advanced technologies in their products. The IC has targeted Philippine's large community of

Figure 6: The "super charged" insurance value chain



Source: Capco Digital research and analysis

unbanked customers by promoting the development of microinsurance products with awareness campaigns. Korea's FSC is now promoting the use of a number of different advanced technologies, such as self-driving, the Internet of Things, healthcare, and electric vehicles. As these countries continue to invest in the industry and promote such technologies, the APAC insurance industry can follow in the footsteps of the finance industry in capturing the attention of Asia's increasingly tech-savvy consumers.

To promote an industry as vast as insurance, the APAC nations must create the environment necessary to help ideas and knowledge grow. By forming teams and establishing innovation hubs that foster the growth of the industry, some government authorities have taken the first steps in that regard. The Insurance Regulatory & Development Authority of India (IRDAI) and Thailand's Office of Insurance Commission (OIC) have started the process of creating an environment that promotes forward-thinking and knowledge exchange. The IRDAI has created a team dedicated to studying how wearable technologies can be used in risk assessment, risk improvement, and policy design. They also intend to advance the life insurance sector by using wearable devices to analyze fitness and healthy lifestyle. The OIC has gone as far as building a center that is fully dedicated to the advancement of the country's insurance industry with a focus on research, development of technologies, increasing accessibility of knowledge amongst the public, and connecting regulators with start-ups.

As these prominent APAC nations take measures to remove regulatory barriers, facilitate innovation, and establish centers of innovation, it has become clear that APAC's growing number of tech-savvy customers can only benefit from the modernization of the industry. The application of technology in insurance has already been a success in Europe and North America, but now regulatory bodies in APAC nations are following suit and listening to the needs of their constituents.

5.2 Insurtech applications along the value chain

Insurance is a data-driven business. The industry will require even more sophisticated automation and technical expertise to achieve efficiency. Amassing data and subsequently tailoring offerings to the needs of individual and commercial customer segments are especially crucial.

We believe that the insurance opportunities offered by digitization and technologies that acquire, manage, and process data will be immense. Figure 6 presents examples of the ways in which technology is disrupting the industry.

By exploring ways to promote and support innovation and the sharing of knowledge within Asia's insurtech industry, various in-country regulators have created a climate of forward-thinking that can only help APAC catch up with its western counterparts – and possibly even surpassing them in certain instances.

6. TECH TREND SHIFTING CONVENTIONAL TIDES

We now examine the following top insurtech trends positively impacting – and even revolutionizing – the industry across the region. In some cases, companies adopt the cutting edge technologies pioneered by western innovators whilst customizing them for their respective local markets, while in other cases they develop their own technologies.

6.1 Insurtech trend 1: Open APIs as an accelerator

Trend: APIs (application programming interface) have accelerated digital and technological agendas within developed financial markets. While APIs were initially seen as a threat to financial providers, they are now seen as enablers to help create new and attractive customer experiences.

Implications: the growth of the ecosystem services has resulted in traditional insurers losing market share over the last few years. Customers now demand an inter-connected service marketplace that extends beyond insurance products and is an extension of their insurance products, such as financial planning, home security, or car maintenance. APIs help address this lack of insurer flexibility by allowing for extensive sharing of information and services with third parties and vendors. Integration with other product extensions allows insurers to create more touchpoints and provide better customer experience, create new digital products, increase sales and distribution, and eventually move into creating disruptive business models.

Increased competition is coming in the shape of Big Tech and global players. Alibaba and Tencent are using

Table 1: Open APIs use-cases across the insurance value chain

COMPANY	AXA SINGAPORE (Singapore)	ZHONGAN (China)
BUSINESS DRIVERS	• Provide "insurance as a service" to fintech partners, allowing customers access to AXA's different insurance products to increase cross-selling opportunities • Respond to the initiative from the Monetary Authority of Singapore (MAS) for players in the financial industry to publish open APIs	• Deepen cooperation with smaller companies within a specialized ecosystem of partners unable to develop their own platform • Offer "insurance as a service" to partners with access to niche customer pools
USE-CASE	• Opened up transactional API and partnered with SATS Ltd; integrating AXA within its "Ready to Travel" app, which allows users to get seamless insurance coverage while planning for their trips • Available for home, travel, and car insurance, with health and life offerings in the pipeline	• Zhong An opened up their APIs to offer customized insurance solutions for partners in various industries: – DXY.cn, an online community of physicians, offers bonus coverage and discounted premiums for patients undergoing regular sugar level blood tests – Xiaozhu.com, a short-term apartment sharing platform, offered home occupancy and accident insurance to homeowners and tenants – Mogujie, a social commerce website, offers personalized credit insurance with rates adjusted to spending and payment records
BENEFITS	• Expand distribution capabilities via partnerships with a variety of channels • Improve the customer experience	

their digital reach to create a fully digital-only insurance experience. Notably, the automobile industry is forging ahead to provide a "vehicle-to-everything" platform. Volkswagen and Tesla have started to offer insurance with a car purchase and Ford is working with Autonomic to create an open platform "Transportation Mobility Cloud" to build out infrastructure communications for cities. Success will belong to those that control the customer interface and its data.

What is next: open APIs allow various insurance companies' channel partners to integrate their services seamlessly across the customer journey. This will be a continuing trend as open APIs creates a win-win situation for all parties. Additional values are provided to the customer and the channel partners, while at the same time helping the insurance companies to expand their reach to new potential customer pools, join other ecosystems (e.g., Google Nest), and create their own API platform that can offer opportunities for further growth.

A case in point is Ping An insurance, which built an API platform that allowed the company to offer advanced auto claim technology to small and medium-sized insurance companies at an affordable price.

Improving the insurer's distribution channels is only potential source of benefit, ultimately open APIs have the potential of transforming the entire insurance value chain via the free-flow of customer information.

6.2 Insurtech trend 2: Positive behavioral reinforcement via IoT

Trend: altering people's behaviors without limiting their options or impacting them financially yields powerful results. Public and private sectors alike are looking at ways to nudge customers towards healthier lifestyles, with an eye towards promoting better outcomes for individuals and the society at large.

Implications: a well-established use-case is the black box insurance for the automobile. With the motion tracking feature in smartphones and telematics, this has promoted safe driving by rewarding a lower premium to drivers who demonstrate safe driving practices. With the recent development of wearables and smart devices, the approach could be leveraged in other fields of insurance. Wearables and smart devices that monitor health signs will give richer data on individuals, with a vast potential for insurers to leverage this information and customize the policy and reward the customers.

Table 2: IoT use-cases for behavioral reinforcement

COMPANY	QUEALTH (U.K.)	HEALTH2SYNC (Taiwan)	BEAM DENTAL (U.S.)	JARVISH (Taiwan)
BUSINESS DRIVERS	• Customers using multiple sources of fitness and well-being apps and devices to track their behavior • No centralized platform for storing and analyzing these health and fitness customer	• Glucometers are not connected to smartphones • No easy way to track blood level with existing glucometers in the market	• Conventional dental insurance does not help prevent costly dental problems • Unable to track the customer oral care behavior to personalize the policy	• Over 400 million motorcyclists in Asia with risks of fatality 20 times higher than car drivers and occupants • Insurance is expensive for riders • Pricing depends on demographics with no input from personal driving behavior
USE-CASE	• Aggregates health and lifestyle data and scores the risk of developing the Big Five preventable lifestyle diseases • Score is available as an API	• Connect glucometers with mobile app via phone dongle • Sync up precise blood sugar data	• Uses a smart toothbrush that tracks how users brush their teeth • Offer discount on premium to reward good oral care behavior	• Monitor rider behavior by sensors in the smart helmet • Evaluate the risk from tracked behavior data
TECHNOLOGY	• Smart device & IoT • Big data • Machine learning	• Smart device and IoT	• Smart device and IoT	• Smart device and IoT • Big data • Machine learning
BENEFITS	• Provide powerful risk analytics and prediction platform on assessing an individual's health • Insurers can access and build out their own apps and services via the data from API	• Track a user's blood sugar in a data-rich context • Enable insurers to reward good behavior (via tracked blood sugar level) by giving a premium discount • Incentivize patients to better control their blood sugar levels	• Beam's insurance plan is 10%- 25% cheaper than competitors • Ability to offer personalized policy according to data collected • Motivate individuals to improve oral care by lower premiums	• Enable insurers to offer customized policies ranked by evaluated risk levels from the tracked driver data • Promote safe driving behavior and reduction of the number of fatal accidents

What is next: IoT technologies will continue to offer both insurers and consumers considerable advantages – from improving the accuracy to price risk to lowering insurance premiums. A case in point is the emergence of healthtech companies, who create enormous opportunities for insurers. With the enormous amount of health, fitness, and lifestyle data maintained by these innovators, partnerships with healthtech players can generate significant advantages for both parties. This is not limited to healthtech companies alone. Other insurtech companies monetize their user base data and have thus developed a sustainable revenue stream through cooperating with the insurers.

Possessing rich data and deep understanding of users can help in the development of highly personalized products. In addition, these technologies offer the means to track positive behaviors, such as healthy lifestyles, good driving habits, and desirable building maintenance, and reward them with lower premiums. This will translate into deeply engaged customers and increased customer loyalty.

6.3 Insurtech trend 3: Cloud and blockchain enabling personalization

Trend: interoperability, as applied to the healthcare industry, emphasizes the importance of effective use of data in healthcare. This results in improving processes and patient care, thus generating more proactive treatment plans. Interoperability will pave the way for the adoption of data-driven operating models in the healthcare and insurance industries.

Implications: sharing of medical data is not only helpful to patients to receive the best medical advice and services, it also helps insurers have greater visibility about the medical background of patients. Insurers can provide a more personalized policy via predictive analytics of medical records, including family medical history, in the future. Interoperability between healthcare providers can help prevent the development of long-term illness and costly claims, thus promoting well-being of all patients in the long term.

Table 3: Cloud and blockchain use-cases for personalization

COMPANY	PING AN HEALTH CLOUD (China)	GEM (U.S.)	MEDREC (U.S.)
BUSINESS DRIVERS	• Patient's data are scattered among different organizations, making it difficult for them to access past records	• Organizational data silos rendering insurance value chains inefficient	• Lack of centralized repositories to store and handle medical records
USE-CASE	• PingAn Health Cloud members can, with the patient's permission, access their health records instantly, including information from providers and insurers • Offers health risk assessment, smart self-diagnosis, and triage using the data housed in the cloud	• GemOS allows patients, providers, and insurers to securely view a patient's health timeline in real-time, improving speed and transparency throughout the claims process. • Adds security via permissioned blockchains in which patients control access and there is a shared ledger system in which every new change is recorded.	• Indexed medical records on the blockchain linking access to the patient's medical records across multiple doctor databases • All relevant parties can access a patient's health records instantly with the patient's permission
TECHNOLOGY	• Cloud	• Blockchain (Ethereum) • Smart contracts	• Blockchain (Ethereum) • Smart contracts
BENEFITS	• Huge amount of aggregated data can be used to support the underwriting and pricing of health insurance products • Customers can enjoy personalized policies by sharing medical backgrounds with insurance companies • Healthcare data enables effective health risk assessments to identify diseases in the early stages of an illness and reduce claims	• Quick verification and reimbursement of health claims • Healthcare data enables effective health risk assessment to identify diseases in early stages and prevent claims	• Decentralized network allows for sensitive medical data to be shared with the blockchain technology securely • Aggregated and anonymized metadata could be obtained for predictive analytics by acting as miner to verify the exchange of information

Furthermore, the conventional approach for insurers to assess the risk and price a healthcare policy relies predominantly on health snapshots obtained at the single point of time when the customers onboard. The sharing of medical data and fitness data will allow insurers to have a comprehensive view of the customer's condition and lifestyle, in a continuously fluid fashion.

Other stakeholders, such as researchers, can also utilize the rich data available to foster a data-driven healthcare ecosystem.

What is next: insurers now have the opportunity to play a very significant role in the healthcare ecosystem. They can either establish and lead in creating a unique solution or enter into partnerships and alliances with emerging players. The next evolution of insurance will be primarily driven by data exchange and sharing between different stakeholders in the ecosystem – from new customer acquisition, fraud prevention, predictive analytics on risk and pricing, to instant claims processing. Being isolated from the ecosystem and missing this considerable opportunity results in a loss of competitive advantage in the long run.

6.4 Insurtech trend 4: AI, machine learning, and IoT leading to automation

Trend: recent advancements in blockchain and AI have brought about a high degree of automation that can profoundly influence the operations of the insurance industry. Machine learning has advanced greatly in recent years, particularly in deep learning and image recognition. By training neural networks with a vast number of sample photos, AI technology can be taught to recognize objects as well as details within images. In the property insurance context, AI can assess the level of damage, down to the parts impacted, in the event of a car accident. This offers the potential to replace some human activities for claim investigations and verification. For example, the level

of damage of a car and its parts in a vehicle accident. This makes it possible to replace some manual activities in claim investigations and verification used to be done by humans. Natural language processing (NLP) fuels the evolution of chatbots, which are now becoming more user-friendly and human-like. Chatbots are starting to handle more complicated customer service scenarios – Google Duplex can answer phone calls as humans can. And these AI technologies are made accessible as a cloud service from providers such as AWS (Amazon Web Services) and Google Cloud.

The proliferation of IoT technology may also advance automation. Insurers will be able to monitor homes and vehicles in real time, and if there is a catastrophe resulting in a large-scale claim, the insurer can mobilize satellites, drones, and weather open data immediately to prepare for the claims with matched policyholders. SkyClaim, a service developed by Skymatics, offers crop damage analysis reporting solutions for crop insurance. By using drones surveying and computer vision technology, it helps the insurers and the policyholders to easily determine the crop damage and yield loss.

Implications: claims management plays a very significant role in the customer experience of an insurance product. Further, rather than employing complicated claim forms manually filled by the customers and going into a lengthy reimbursement process, technology-advanced insurers are automating this by implementing smart contracts, open data, machine learning, and IoT technology. Traditional claims management will likely focus on more complicated and unusual claims, disputed claims where technology helps the negotiation, investigation, and settlement.

Table 4: AI, machine learning and IoT use-cases for automation

COMPANY	AXA'S FIZZY (France)	LEMONADE (U.S.)	ZHONG AN (China)
BUSINESS DRIVERS	• Written confirmation by the airline is required for claiming compensation for delayed flights • Verification of the delayed flight takes time and manpower	• Tech-savvy customers expect an instant response, and it is costly to maintain a well-training and responsive customer service team to be available 24/7 to assist the customers	• With the innovative insurance products developed by ZhongAn, there is a considerable amount of claims submitted • Fraudulent and exaggerated claims with photoshopped images
USE-CASE	• Offer instant and automatic payment if a customer's flight is delayed for more than two hours	• Submit claims and promptly receive payouts via chatbot • Guiding customers step-by-step throughout the claims process without involving human customer service	• Phone screen warranty – determine if the screen is in a good condition or broken from the photo sent by the customer • Automobile insurance – determine the damage to a car from pictures and estimate the loss from the photo sent by the customer
TECHNOLOGY	• Blockchain (Ethereum) • Smart contract	• Chatbot / NLP	• Computer vision • Machine learning
BENEFITS	• Offer a fully automated customer experience during the claims process • Compensation decision is triggered by external data (global air traffic databases), which underscores the improved credibility of the service • Eliminate the resource needed to handle the claim	• Makes the process simpler and faster, thus improving the customer experience • Built-in anti-fraud algorithms • Augment the customer services team • Cost saving	• Reduce the resource and time needed for investigation to process a claim • Prevent fraud by detecting if the image is manipulated • Improve the customer experience

What is next: automation in claims management will be moving from cost and resource savings to enhancing the customer experience by enabling instant and seamless claims process. With the rising population of millennials and tech-savvy users, using AI for customer service will be a core feature demanded. Insurers should either start developing their own capacity in AI or seeking the right technical partner to deliver the new customer experience.

Progress in IoT and blockchain will also build the foundations for smart contacts, enabling fully automated claims management. With more innovators in the blockchain field starting to introduce real-world data to the blockchain, insurers should consider the possibility of developing new products associated with the blockchain and offer completely automated claims management via smart contracts. In the future, the FNOL (first notice of loss) contact will not be made by the customer but triggered automatically by smart devices and smart contract monitoring open data.

6.5 Insurtech trend 5: Blockchain as the fraud police

Trend: the immutable nature of blockchain ensures that the records stored in the chain are almost certain to be genuine. A well-understood application of this nature of blockchain is cryptocurrencies, such as bitcoin. Transactions are stored and locked in the blockchain, and it is impossible for anyone to alter them; hence the integrity of the entire system can be generally ensured.

Implications: it is estimated that about 10% of global compensation claims for property damage or personal accidents are fraudulent, meaning that genuine customers end up paying more for their premiums. Using the records from blockchain can improve the management of fraud risk and result in lower premiums.

There are current use-cases of blockchain that can help to prevent insurance fraud by improving the provenance of property and the reliability of the tracking records in the supply chain. In addition, personal identity authentication mechanisms via smart contracts are now empowering insurers to verify the identity of those making claims. With these extra layers of verified information from the chain, insurers now can better control fraud risk and reduce the costs associated with fraudulent claims.

What is next: fighting insurance fraud will be a continuous effort and blockchain offers the prospect of perfect data integrity; it will be part of toolkit used to examine the reliability of claims via innovative solutions in the market.

Meanwhile, the amount of data available in the blockchain will continue to grow, the benefits of which go beyond just combating fraud. With the complete history of customers, such as the health and fitness data in the medical chain,

Table 5: Blockchain use-cases for fraud prevention

COMPANY	CIVIC (U.S.)	EVERLEDGER (U.K.)	STATWIG (India)
BUSINESS DRIVERS	• Medical identity thieves make claims on other peoples' policies, resulting in financial losses to insurers and customers	• Lack of data on luxury assets resulted in risk of scamming an insurer	• Logistics records can be easily manipulated • Insurers have difficulty in accessing and validating proof of loss of the shipments and process claims in cargo insurance
USE-CASE	• Authentication data shared with the requesting party with the user's approval • Alerts users via a push notification when their identity is being used at the time of the transaction	• Recording the lifecycle of a diamond using the Diamond Time-Lapse Protocol on blockchain • Shared records visible across the industry participants	• Provide real-time, tamper-proof, end-to-end tracking for shipments • Insurers are able to track shipments for proof of losses and offer risk reduction services
TECHNOLOGY	• Blockchain (Ethereum) • Smart contracts	• Blockchain (Ethereum) • Smart contracts	• Blockchain (Ethereum) • Smart contract • IoT
BENEFITS	• Insurer can easily validate whether the identity of the person submitting the claim is correct • Protect users against identity theft	• Prevent fraud in luxury property insurance • Manufacturers, sellers, and consumers of the diamond are stored in the blockchain trackable by the insurer; it is very challenging to commit fraud on such well-tracked assets	• Preventing fraud in cargo insurance claims

insurers will be able to undertake predictive analyses and accurately price their policy for each individual. This underscores the concepts discussed above on positive reinforcement and inter-operation of technologies like AI, blockchain, and IoT. These emerging technologies can reshape the insurance industry landscape.

7. CONCLUSION

The growth of the insurance industry in the Asian region is clearly linked to macroeconomic factors, as well as continued investment in the region. The demographic composition of Asian countries is rapidly changing. The rising purchasing power of the middle-class in urbanized areas with relatively low market penetration for insurance is a powerful growth driver in Asia. In addition, the rising millennial generation fuels innovation. The tech-savvy population increases propensity for early and easy adoption of digital solutions.

Insurtech is rapidly transforming markets in the West, and Asia is fast reaching its inflection point and will be the next catalyst for the transformation of the industry. Insurtech has contributed significantly to global premium growth in 2017, and we expect this trend to continue, creating outsized opportunities for traditional insurers as well as new digital insurance companies and big tech companies.

Increased competition in APAC is expected among incumbents and new players. Consequently, a solid understanding of the unique landscapes of the fast-growing markets in Asia and the agility to adapt to new trends via proprietary technology investment and partnerships will be critical to the success of insurers.

The unique macroeconomic dynamics of the Asian region as well as insurtech ecosystem innovation are being further aided by supportive governments and improved regulations. With the continued rollout of various initiatives initiated by the different insurance governing bodies the industry transformation will continue.

For these reasons, we expect further transformation of the traditional insurance industry in Asia. Relationship-based sales, currently the dominant approach in the region, will increasingly be characterized by disintermediation as customers continue to gain greater transparency on pricing and coverage ushered in by new technologies. Insurers will increasingly face the challenge of creating new value propositions and providing unique customer experiences. The strategic imperative rests on the insurers becoming adept and agile to harness the potential of insurtech, which will then enable them to stay ahead of the curve.

ALTERNATIVE RISKS

SEEING AROUND THE CYBER-CORNER: WHAT'S NEXT FOR CYBERLIABILITY POLICIES?[1]

KARIN S. ALDAMA | Partner, Perkins Coie LLP
TRED R. EYERLY | Director, Damon Key Leong Kupchak Hastert
RINA CARMEL | Senior Counsel, Anderson, McPharlin & Conners LLP

ABSTRACT

Cybersecurity coverage issues began to arise 20-25 years ago, when computers started becoming ubiquitous in the workplace. Initially, insureds sought coverage for cyber incidents under traditional policies, which led to somewhat metaphysical coverage issues like: what is data, exactly? Is it tangible property for purposes of CGL policies? Is data loss a direct physical loss covered under first-party property policies? The first cyber policy written to provide clarity on these issues and provide coverage specifically for cyber risks was introduced in 1997. But cyber policies, which are not standardized, raise different issues, such as the scope of coverage, which may develop more slowly than the risks of the cyberworld; whether the failure by an insured to implement cybersecurity measures may be grounds to disclaim coverage; and how novel policy language is to be construed. This article traces the historical coverage analyses, to set the stage for a discussion of common provisions of cyberliability coverages available today and the related issues that have arisen or may arise. It also discusses the slowly developing case law addressing cyber policies, and assesses what coverage and bad faith arguments and defenses may be raised as such policies continue to be addressed in the courts.

1. INTRODUCTION

Cybersecurity coverage issues began to arise approximately twenty to twenty-five years ago, when computers started becoming ubiquitous in the workplace. Historically, the coverage issue was metaphysical in nature: what is data, exactly? Could data constitute tangible property, for coverage under traditional CGL policies? Could data loss constitute a direct physical loss, for coverage under first-party property policies? These issues continue to arise today, as not all insureds purchase cyberliability policies, and instead – or in addition – may seek coverage under traditional policies in case of a cyber breach.[2]

Modern cyberliability policies are usually written to avoid this quandary. Different issues arise, though. These issues include the scope of coverage, which may develop more slowly than the risks of the cyberworld; whether any failure by the insured to implement cybersecurity measures may be grounds to disclaim coverage; and the impact of the novelty of policy terms and risks.

[1] Originally published in the Spring 2018 edition of Insurance Coverage, copyright 2018 American Bar Association. This article is partly based on Aldama, K. S., and T. R. Eyerly, 2018, "Cyber policies – the next wave," ABA Insurance Coverage Litigation Committee CLE Seminar, March. This article does not provide legal advice, and a given situation may vary from the facts discussed in this article. The views and opinions expressed in this article do not necessarily reflect the opinions of all of its authors on everything expressed herein, nor of their firms or clients.

[2] E.g., Zurich Am. Ins. v. Sony Corp. of Am., Index No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Cty. Feb. 21, 2014) (ruling no duty to defend underlying action alleging hacking of PlayStation online services existed under CGL policy).

This article traces the historical coverage analyses, as an aid to today's insurers, insureds, and coverage counsel. Next, it reviews common provisions of cyberliability coverages available today and the related issues that have arisen. Finally, now that some cyberliability coverage suits have been filed, the authors gaze into their crystal ball to see what coverage and bad faith arguments and defenses may be raised.

2. HISTORICAL AND CURRENT COVERAGE CASE LAW UNDER TRADITIONAL POLICIES

2.1 Traditional CGL policies

Traditional CGL policies usually provide coverage under Coverage A for "property damage," defining that term to require damage to tangible property.[3] ISO main forms dated 2004 and later provide that "electronic data is not tangible property."[4] As of May 1, 2014, ISO introduced optional forms, for use with CGL and general excess policies excluding coverage for risks of data breaches, disclosure of a third party's personal or confidential information, and notification and credit monitoring for individuals whose information was compromised.[5] These forms apply to both Coverage A and Coverage B.[6] A software exclusion, barring coverage for "personal and advertising injury" "[a]rising out of: (d) Computer code, software or programming used to enable: (i) Your web site; or (ii) The presentation or functionality of an 'advertisement' or other content on your web site," was recently held unambiguous, although the underlying action involved unauthorized distribution of software rather than a data breach.[7]

Even before these relatively recent policy terms and endorsements were introduced, many courts were reluctant to find that losses due to cyber breaches were covered under Coverage A.

One of the earliest cyber coverage cases, Seagate Technology, Inc. v. St. Paul Fire and Marine Ins. Co.,[8] involved underlying allegations that the third-party claimant had incorporated the insured's defective drives into its computers. Because the drives were not inherently dangerous products, and the underlying complaint did not allege resulting damage to other parts of the third-party claimant's computers, the CGL policy's "property damage" provisions were not satisfied, and the insurer had no duty to defend. Underlying allegations of loss of the third-party claimant's customers' information, and loss of business and damage to the third-party claimant's reputation, were not sufficient to create a duty to defend.[9] The court's reasoning was implicitly based on a requirement of damage to tangible property, as the court cited to principles from cases involving asbestos and construction defect coverage.[10]

In contrast to Seagate, America Online, Inc. v. St. Paul Mercury Insurance Co.[11] involved underlying allegations that incorporation of the insured's defective software caused resulting damage to the third-party claimants' computers. Specifically, the insured's software allegedly contained bugs that were incompatible with the third-party claimants' other software and operating systems, altering their software, disrupting network connections, causing the loss of stored data, and causing their operating systems to crash. Under the ordinary meaning of "tangible," "the physical magnetic material on the hard drive that retains data, information, and instructions is tangible property."[12] However, the court stated that this did not equate to a conclusion that "data, information, and instructions, which are codified in a binary language for storage on the hard drive, are tangible property."[13] The court concluded that they are not, and moreover, alteration of data, information, and instructions does not cause damage to the hard, tangible parts of a computer.[14] Thus, the insurer had no duty to defend.[15]

Coverage B, in contrast, does not require tangible property, but instead may provide coverage for specifically enumerated offenses.[16] Thus, data breaches have been found potentially covered under some CGL policies, especially those with non-standard language. In Hartford

[3] E.g., ISO Form No. CG 00 01 04 13 at 15.
[4] ISO Form Nos. CG 00 01 12 04 at 15, CG 00 01 12 07 at 15, CG 00 01 04 13 at 15.
[5] ISO, 2013, "Access or disclosure of confidential or personal information exclusions introduced," Commercial lines forms filing CL-2013-ODBFR at 3; ISO, 2013, "Access or disclosure of confidential or personal information exclusions introduced," Commercial general liability forms filing GL-2013-ODBFR; Ron Biederman, R., 2014, "ISO comments on CGL endorsements for data breach liability exclusions," Insurance Journal, July 18, https://bit.ly/2TVay4h (commenting on forms CG 21 06 05 14, CG 21 07 05 14, and CG 21 08 05 14).
[6] See n.5, supra.
[7] BF Advance, LLC v. Sentinel Ins. Co., No. 16-CV-5931-KAM-JO, 2018 WL 4210209, at *10-12 (E.D.N.Y. Mar. 20, 2018).
[8] 11 F. Supp. 2d 1150 (N.D. Cal. 1998).
[9] Id. at 1155.
[10] Id. at 1154-56 (citing cases including Armstrong World Indus., Inc. v. Aetna Cas. & Sur. Co., 45 Cal. App. 4th 1 (1996) and New Hampshire Ins. Co. v. Vieira, 930 F.2d 696 (9th Cir. 1991)).
[11] 347 F.3d 89 (4th Cir. 2003) (Virginia law).
[12] Id. at 94-95 (citing Webster's Third New International Dictionary of the English Language Unabridged 2337 (1993) for definition of "tangible" as "capable of being touched: able to be perceived as materially existent esp. by the sense of touch: palpable, tactile" and for definition of "tangible property" as "having physical substance apparent to the senses.").
[13] Id. at 95.
[14] Id. at 94-97.
[15] The court also held that the impaired property exclusion barred coverage. Id. at 97-99.
[16] E.g., ISO Form No. 00 01 04 13 at 6, 15.

Casualty Insurance Co. v. Corcino & Associates,[17] the third-party claimants alleged that the insured's job applicant posted their private, confidential, and sensitive medical and psychiatric information, which the co-defendant hospital had provided to the insured. The CGL policy at issue provided coverage for "electronic publication of material that violates a person's right of privacy."[18] The insurer did not dispute that the allegations fell within this coverage provision. The insurer argued, instead, that the policy's exclusion for "personal and advertising injury" "[a]rising out of the violation of a person's right to privacy created by any state or federal act" barred coverage. The court disagreed, concluding that the insured's argument, namely, that the rights to privacy were not created by state or federal acts, but rather by constitutional and common law principles, was reasonable.[19] The court rejected the insurer's argument that the insureds were in fact suing under state statutes, reasoning that those statutes codified constitutional and common law principles.[20]

In Travelers Indemnity Co. of America v. Portal Healthcare Solutions, LLC,[21] the underlying class members alleged that the insured, which was in the business of safekeeping medical records for its healthcare provider customers, posted their confidential medical records on the internet, such that they became publicly accessible. The non-standard CGL policies provided coverage for "electronic publication of material that … gives unreasonable publicity to a person's private life" (for the 2012 policy) and "electronic publication of material that ... discloses information about a person's private life (for the 2013 Policy)."[22] The policies did not define the term "publication." The court concluded that "exposing confidential medical records to online searching is 'publication,'" and because medical records were at issue, the publicity was "unreasonable."[23] Thus, the insurer had a duty to defend.

On the other hand, hackers' appropriation of third-party claimants' personal private information (PPI) from the insured's web portal was held not to constitute a "publication" in Innovak International, Inc. v. Hanover Insurance Co.[24] The policy at issue defined "personal and advertising injury" to mean "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[25] The court held that there was no potential for coverage, explaining that the insureds did not disseminate the third-party claimants' PPI, and the insureds' publication of software did not violate the third-party claimants' privacy.[26]

2.2 Traditional property policies

Traditional property policies usually require "direct physical loss."[27] Courts have come to divergent conclusions as to whether data is physical, although courts seem to be more likely to find that data is "physical" under a property policy than to find it is "tangible" property under a CGL policy.

In Ward General Insurance Services, Inc. v. Employers Fire Insurance Co.,[28] the court ruled that a database crash was not covered because there was no "direct physical loss." The database was deemed not "physical." The crash in that case was caused by human error during a system upgrade. The court reasoned that the risks at issue in the claim were human error or a defective program, neither of which was physical. "Unless the harm suffered, i.e., the loss of electronically stored data without loss or damage of the storage media, is determined to be a 'physical loss,' we cannot say that the risk encountered in this case, a negligent operator, constitutes a risk of direct physical loss."[29]

Other courts have concluded that data can be physical.

In Landmark American Insurance Co. v. Gulf Coast Analytical Laboratories, Inc.,[30] the insured stored its chemical analyses for customers as electronic data on a hard disk storage system. The storage system failed to read two hard disk drives, resulting in the corruption of data, in turn causing the insured to incur data recovery costs and loss of business income. The court relied on a tax case, South Central Bell Telephone Co. v. Barthelemy,[31] which concluded that electronic software data is physical.[32]

"When stored on magnetic tape, disc, or computer chip, this software, or set of instructions, is physically manifested in machine readable form by arranging

[17] No. CV 13-3728 GAF (JCx), 2013 U.S. Dist. LEXIS 152836, at *6-7 (C.D. Cal. Oct. 7, 2013).
[18] Id., at *6.
[19] Id., at *10-15.
[20] Id., at *11-14.
[21] 35 F. Supp. 3d 765 (E.D. Va. 2014), aff'd, 644 F. App'x 245 (4th Cir. 2016) (Va. law).
[22] Id. at 767.
[23] Id. at 767, 770-71.
[24] 280 F. Supp. 3d 1340 (M.D. Fla. 2017) (South Carolina law).
[25] Id. at 1343.
[26] Id., at *15-21.
[27] E.g., ISO Form No. CP 00 10 10 12 at 1.
[28] 114 Cal. App. 4th 548, 556-57 (2003).
[29] Id. at 554.
[30] No. CIV.A. 10-809 Section "B," 2012 U.S. Dist. LEXIS 45184 (M.D. La. Mar. 30, 2012).
[31] 643 So. 2d 1240, 1244 (La. 1994).
[32] Id., at *8-9.

electrons, by use of an electric current, to create either a magnetized or unmagnetized space … this machine-readable language or code is the physical manifestation of the information in binary form."[33]

The Gulf Coast court extended this reasoning to conclude that "tangibility is not a defining quality of physicality according to Louisiana law."[34] Thus, the electronic data at issue "has physical existence, takes up space on the tape, disc, or hard drive, makes physical things happen, and can be perceived by the senses."[35] The policy's "direct physical loss" requirement was, therefore, satisfied, and coverage existed.

In American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc.,[36] the insured sustained a power outage, causing its three mainframe computers to lose their programming information. Even after the insured's employees reloaded the programming information, the computers could not connect to a network that tracked the insured's customers, products, and daily operations, interrupting the insured's business operations for eight hours. The insured brought the network back to operation by bypassing a malfunctioning matrix switch. Even then, however, the insured's custom configurations were lost and had to be reprogrammed. The insurer disclaimed coverage on the basis that electronic data is not physical, and that the mainframe computers and matrix switch retained their inherent abilities to be reprogrammed with the insured's custom settings, so that they were not physically damaged. The court accepted the insured's broader definition of "physical damage," reasoning that "[a]t a time when computer technology dominates our professional as well as personal lives, … 'physical damage' is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality."[37] The court bolstered its conclusion by pointing to criminal statutes that indicated that tampering with another's computer system could cause damage.[38]

In Ashland Hospital Corp. v. Affiliated FM Insurance Co.,[39] the court predicted that Kentucky would conclude that "direct physical loss" includes heat damage that rendered a data storage less reliable. The court's discussion was scientific in nature, reviewing microscopic processes that can happen when lubricants and other components are exposed to heat, such that the loss would be deemed physical.[40]

Still other courts have relied on different policy provisions to determine whether coverage exists. For example, in Lambrecht & Associates, Inc. v. State Farm Lloyds,[41] the court based its ruling on the policy's definition of "electronic media and records" to include storage media and "data stored on such media" to conclude that loss of data due to a virus injected by a hacker was physical. In WMS Industries, Inc. v. Federal Insurance Co.,[42] the court did not reach the issue of whether loss of data could be physical. Instead, it concluded that there was no coverage because the dependent business income coverage required loss to flow from the central networked monitoring facility, whereas the loss at issue flowed from individual casinos that fed into the single, centralized jackpot.

3. MODERN CYBERLIABILITY POLICIES AND THE COVERAGE ISSUES THEY MAY PRESENT

3.1 Historical and currently available coverages[43]

The first cyber policy was introduced in 1997.[44] "Though groundbreaking as the first to address cybersecurity, it was a third-party liability policy only and was basically a 'hacker policy.'"[45]

[33] Id., at *9 (quoting Barthelemy, 643 So. 2d at 1246).
[34] Id.
[35] Id., at *10 (quoting Barthelemy, 643 So. 2d at 1246).
[36] Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., No. CIV 99-185 TUC ACM, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 19, 2000).
[37] Id., at *6.
[38] Id., at *7.
[39] Civ. Action No. 11-16-DLB-EBA, 2013 U.S. Dist. LEXIS 114730, at *13 (E.D. Ky. Aug. 14, 2013) (predicting Kentucky would conclude that "direct physical loss or damage" encompassed heat damage that rendered data storage network less reliable).
[40] Id., at *13-14.
[41] 119 S.W.3d 16, 23-26 (Tex. Ct. App. 2003).
[42] 384 F. App'x 372 (5th Cir. 2010) (per curiam, unpublished opinion) (Mississippi law).
[43] Aldama & Eyerly, Cyber policies – the next wave, includes a discussion of selected provisions, terms, definitions and exclusions that may appear in some policies.
[44] Brown, B. D., 2014, "The ever-evolving nature of cyber coverage," Insurance Journal, September 22, https://bit.ly/2EncSf2.
[45] Id.

Like the electronic world, cyber policies have evolved significantly since 1997. In 2016, over 130 insurers reported writing standalone cyber policies.[46] Also in 2016, over 500 insurers provided businesses and individuals with cyber coverage, with the vast majority of those coverages written as endorsements to commercial and personal policies.[47] Cyber coverages are not written on standardized forms, and the coverages offered differ significantly.[48]

According to NAIC, the range of available coverages includes a variety of first-party and third-party coverages:

- **Liability for security or privacy breaches:** this would include loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems.
- **The costs associated with a privacy breach:** such as consumer notification, customer support, and costs of providing credit monitoring services to affected consumers.
- **The costs associated with restoring, updating, or replacing business assets stored electronically.**
- **Business interruption:** including extra expense related to a security or privacy breach.
- **Liability associated with libel, slander, copyright infringement, product disparagement, or reputational damage:** this would include situations when the allegations involve a business website, social media, or print media.
- **Expenses related to cyber extortion or cyber terrorism.**
- **Coverage for expenses related to regulatory compliance:** this would include expenses incurred as a result of billing errors, physician self-referral proceedings, and Emergency Medical Treatment and Active Labor Act proceedings.[49]

Additional third-party coverages may include:

- **Liability due to breach of third parties' privacy:** such as damages based on publication, unauthorized disclosure, use, or destruction of confidential information or personally identifiable information (PII).
- **Losses due to denials or delays of access to systems:** including contingent business interruption claims. Such coverages do not typically include losses resulting from internet provider disruptions, however.
- **Losses due to transmission of malicious code or malware from the insured's affected system.**
- **Coverage for regulatory proceedings resulting from a cyber incident:** such as consumer redress funds or penalties due to payment card industry (PCI) data security standards.

The scope of available coverages seems likely to continue to evolve as the cyberworld creates new risks.

3.2 Case law involving cyberliability policies

Few cyberliability coverage cases have been decided to date. In P.F. Chang's China Bistro, Inc. v. Federal Insurance Co.,[50] the court ruled that the cyberliability policy did not provide coverage for PCI fees assessed by credit card companies following theft of the insured's customers' credit card information.

In that case, the insured (Chang's), a restaurant, allowed its customers to pay for meals by credit card, and entered into a Master Service Agreement (Agreement) with Bank of America Merchant Services (BAMS), under which BAMS processed credit card transactions for Chang's.[51] The Agreement provided that MasterCard could assess fees against BAMS if MasterCard incurred losses from a data breach to any client of BAMS, and also contained an indemnification provision. Chang's was hacked, and the credit card numbers of over 60,000 of its customers were posted on the internet. As a result, MasterCard incurred costs for fraudulent credit card charges, for notifying customers of the breach, and for providing new credit cards and personal identification numbers. MasterCard assessed about U.S.$1.72 million in fees against BAMS, consisting of U.S.$1.7 million for fraudulent charges, and about U.S. $200,000 to issue new credit cards and related costs. BAMS sought indemnification from Chang's, which Chang's agreed to, to avoid cancellation of BAMS credit card processing services. Chang's cyber insurer disclaimed coverage, and a coverage suit ensued.

The district court ruled that no coverage existed for the U.S. $1.7 million in fees for fraudulent charges, because the policy required "injury sustained ... by a Person

[46] Insurance Journal, 2017, "Cyber insurance premium volume grew 35% to U.S.$1.3 Billion in 2016," Insurance Journal, June 23, https://bit.ly/2BVZA7R
[47] National Association of Insurance Commissioners (NAIC), 2017, "Cybersecurity," December 12, https://bit.ly/1rgyJnD
[48] Greenwald, J., 2015, "Cyber insurance policies vary widely and require close scrutiny," Business Insurance, May 10, https://bit.ly/2SWe2Hu
[49] NAIC, Cybersecurity.
[50] No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 26, 2016).
[51] Id., at *2.

because of ... unauthorized access to such Person's Record,"[52] which the court interpreted to require that the third-party claimant be the person whose confidential records had been disclosed. Because BAMS was the third-party claimant, but not the person whose records were disclosed, there was no coverage.

Although the court found that there was potential coverage for the U.S.$200,000 in fees, the exclusion "for contractual obligations an insured assumes with a third-party outside of the Policy" was held to bar coverage.[53] The court found that Chang's had voluntarily agreed to indemnify BAMS, and that there was no evidence that Chang's would have had to indemnify BAMS absent the Agreement.[54] That the Agreement is standard in the industry, that merchants cannot accept credit card payments without such agreements, and that the insurer knew this was standard practice, did not impact the court's view.[55] Instead, the court looked to the facts that the insurer and insured were sophisticated parties, and that the insured could have requested coverage for PCI fees, but did not.[56] The coverage action settled while on appeal.

4. WHAT'S NEXT?

4.1 The genuine dispute and fairly debatable doctrines as defenses to bad faith allegations

The terms of cyberliability policies are new, non-standard, and have not, for the most part, been construed by courts. The facts regarding breaches are new, with constantly evolving security measures, and with cyber tortfeasors seemingly finding new ways to get around security measures. Thus, one key question is whether the genuine dispute and fairly debatable doctrines will be viable defenses to any allegations of bad faith.

The genuine dispute doctrine is based on the insurer's "genuine dispute with its insured as to the existence of coverage liability or the amount of the insured's coverage claim."[57] Although this defense originally applied to the legal issue of policy interpretation only, some recent cases have also applied it to factual disputes.[58] A "genuine" dispute exists only where the insurer's position is "maintained in good faith and on reasonable grounds."[59] To assert this defense, the insurer must have undertaken a reasonable and proper investigation. The genuine dispute doctrine is a defense to bad faith claims only, and not to breach of contract claims.[60]

The fairly debatable doctrine, a variant of the genuine dispute doctrine, is a defense to bad faith claims where the insurer's coverage position was based on a fairly debatable interpretation and/or application of the relevant policy language.[61]

Cases decided to date suggest that these defenses remain viable. Indeed, it may be easier for insurers to rely on these defenses due to the novelty of the policies and cyber risks – assuming, of course, that the insurer has conducted the requisite coverage investigation.

In Gulf Coast, even though coverage existed for the loss, the court granted summary judgment in favor of the insurer on the bad faith claim. The court stated: "[T]here is a conflicting body of case law on [the] issue of the classification of electronic data. For that reason, there exist 'substantial, reasonable and legitimate questions to the extent of the insurer's liability' to which reasonable minds could differ and clearly do based on the case law."[62]

Retail Ventures, Inc v. National Union Fire Insurance Co. of Pittsburgh, PA[63] reached a similar result. That case was based on a claim for coverage after hackers stole the insured's customers' credit card information and used it for fraudulent transactions. Credit card companies charged the insured over U.S. $4 million for charge backs, card replacement, account monitoring, and fines. The court held that coverage existed under a computer fraud rider to a blanket crime policy, which provided coverage for "Loss which the Insured shall sustain resulting directly from: A. The theft of any Insured property by Computer Fraud."[64] However, the insurer's disclaimer did not render it liable for bad faith. First, a wrongful disclaimer is not, by itself, bad faith under Ohio law.[65] Second, the district court found that the coverage question was fairly debatable, and the fact that the disclaimer letter and claim file did not reference the "resulting directly from" language did

[52] Id., at *4-5 (emphasis added).
[53] Id., at *6, *7-8.
[54] Id., at *8-9.
[55] Id.
[56] Id.
[57] Wilson v. 21st Century Ins. Co., 42 Cal. 4th 713, 723 (2007).
[58] Id. (citing cases).
[59] Id.
[60] Id.
[61] E.g., Reid v. Pekin Ins. Co., 436 F. Supp. 2d 1002, 1013 (N.D. Iowa 2006), aff'd, 245 F. App'x 567 (8th Cir. 2007); New England Envt'l Technologies v. Am. Safety Risk Retention Group, Inc., 738 F. Supp. 2d 249, 259 (D. Mass. 2010) (no liability under Mass. Gen. L. Ch. 93A where insurer's coverage position was "based on a 'plausible interpretation' of the policy's terms").
[62] 2012 U.S. Dist. LEXIS 45184, at *13.
[63] 691 F.3d 821 (6th Cir. 2012) (Ohio law).
[64] Id. at 826.
[65] See id. at 834 (citation omitted).

not show bad faith.[66] Third, the insurer's interpretation of Exclusion 9 (which provided that "[c]overage does not apply to any loss of proprietary information, Trade Secrets, Confidential Processing Methods, or other confidential information of any kind") was not unreasonable because "of the confidential nature of the customer information and the claim that ejusdem generis did not apply."[67] Finally, the insurer had conducted an adequate, reasonable investigation, and requesting a second opinion from outside coverage counsel did not make "the investigation so one-sided as to constitute bad faith."[68]

These defenses may not protect insurers in all cases, however, especially in states that recognize procedural bad faith. In Travelers Property Casualty Co. of America v. Federal Recovery Services,[69] the insured, which was in the business of electronic data storage, sought coverage under a cyber errors and omissions policy for claims that it had improperly retained possession of a customer's members' account data. The court ruled that the insurer had not breached the contract, because the policy provided coverage for an "errors and omissions wrongful act," defined as "any error, omission or negligent act," but the underlying action alleged that the insured had acted knowingly, willfully, and maliciously.[70] Thus, the insurer could not be liable for substantive bad faith. However, the court ruled that the issue of procedural bad faith could proceed to trial, because the insured alleged that the insurer improperly required it to receive suit papers before making an insurance claim, and the insurer did not "diligently investigate, fairly evaluate, and promptly and reasonably communicate with" the insured, so factual disputes remained, and the fairly debatable doctrine did not allow summary judgment in favor of the insurer.[71]

An issue that may well play into the analysis of coverage under cyberliability policies is the meaning of cyber-specific terms. In BF Advance,[72] the court looked to online dictionary definitions to interpret the terms "software," "code," and "programming," which appeared in the software exclusion, but which the policy did not define. While these terms are generally understood at this time, it is possible that new meanings could develop before dictionary definitions reflect the new meanings, leading to questions about policy interpretation.

4.2 Use of conditions and exclusions as a means to promote cybersecurity

With the exception of the "no voluntary payments" condition, courts have generally been reluctant to enforce policy conditions, often requiring the insurer to prove prejudice before an insured's failure or refusal to comply can serve as a basis to disclaim coverage. For example, in Lambrecht,[73] the insurer argued, among other things, that the insured had not complied with a condition of the traditional property policy because it did not notify the police that a law might have been broken when its computer was infected by a virus. The condition at issue required the insured to "notify the police if a law may have been broken."[74] The court ruled that by its language, the condition was not a condition precedent to coverage.[75] Thus, the insurer could not disclaim coverage based on the condition.

Many cyberliability policies require the insured to maintain cybersecurity measures. A currently pending case,[76] Columbia Casualty Co. v. Cottage Health System, may provide guidance on conditions, exclusions, and the materiality of representations in policy applications, in the context of a data breach. The case is based on an alleged data breach, in which confidential medical records of the insured hospital network's patients, which were electronically stored, were disclosed to the public on the internet.[77] The "NetProtect360" policy issued to the insured contains the following condition:

[66] Id. at 834-35.
[67] Id. at 835.
[68] Id.
[69] 156 F. Supp. 3d 1330 (D. Utah 2016).
[70] Id. at 1334-1337.
[71] Id. at 1337-40.
[72] 2018 WL 4210209, at *11.
[73] 119 S.W.3d at 26.
[74] Id.
[75] Id.
[76] The federal Cottage Health matter pending when this article was originally published in 2018. It has since been voluntarily dismissed without a substantive decision on these issues. Columbia Cas. Co. v. Cottage Health Sys., No. 16-56872 (9th Cir. Jan. 26, 2018). A subsequent similar action brought in the same court also was voluntarily discontinued based on a stipulation filed on January 25, 2018. Columbia Cas. Co. v. Cottage Health Sys., No. 2:16-cv-3759, 2018 WL 1859132 (C.D.Cal. Jan. 25, 2018).
[77] Complaint for Declaratory Judgment and Reimbursement of Defense and Settlement Payments, No. 2:15-cv-03432, at ¶¶ 2-6, 16 (C.D. Cal. May 7, 2015).

Q. MINIMUM REQUIRED PRACTICES

The Insured warrants, as a condition precedent to coverage under this Policy, that it shall:

1. follow the Minimum Required Practices that are listed in the Minimum Required Practices endorsement as a condition of coverage under this policy, and

2. maintain all risk controls identified in the Insured's Application and any supplemental information provided by the Insured in conjunction with Insured's Application for this Policy.[78]

Perhaps because conditions can be difficult to enforce, some cyberliability policies also exclude coverage if the insured has not taken cybersecurity measures. The declaratory relief complaint filed in Cottage Health System[79] alleges that the "NetProtect360" policy also contains the following exclusion:

Whether in connection with any First Party Coverage or any Liability Coverage, the Insurer shall not be liable to pay any Loss:

***

O. FAILURE TO FOLLOW MINIMUM REQUIRED PRACTICES BASED UPON, DIRECTLY OR INDIRECTLY ARISING OUT OF, OR IN ANY WAY INVOLVING:

1. Any failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application for this Insurance and all related information submitted to the Insurer in conjunction with such application whether orally or in writing;...

The policy also contains a condition incorporating the application, which contains numerous questions regarding cybersecurity, and making the insured's representations in the application material to the risk.[80] California law provides ample guidance on misrepresentations in applications for other types of policies,[81] although Cottage Health could provide guidance on such provisions specifically in the cyberliability policy context.

The policy at issue in Cottage Health contains a provision requiring ADR before any judicial proceeding is filed, prompting the district court to dismiss the complaint without prejudice,[82] and the appeal was voluntarily dismissed.[83] The insured then filed a complaint in state court,[84] where the case now appears to be headed for trial in the late summer or fall of 2019.[85] so it is possible that insurers and insureds will ultimately obtain some guidance regarding the enforceability of the exclusions and/or conditions at issue in Cottage Health.

Forensic investigation of alleged cyber losses[86] could also become an area for dispute, placing cooperation conditions and claims handling at issue. Causation of the alleged loss may be key to evaluating coverage, as the policy provisions quoted in this article indicate. In Southwest Mental Health Center, Inc. v. Pacific Insurance Co.,[87] the insurer made a spoliation argument, seeking to exclude evidence regarding the insured's computer itself in a coverage action, because one of the insured's employees had discarded the damaged drive a year after the loss. The court found that there was no spoliation because the insurer did not request the drive for inspection during that year, the insured discarded it as part of its "routine clean-up," and there was no indication that the insured had done so in an effort to prevent the insurer from determining the cause of damage.[88]

5. CONCLUSION

Given the wide variety of policies on the market and the ingenuity of cyber villains, insureds are well advised to select and negotiate their cyberliability policies carefully, based on an analysis of their specific needs and the specific risks to which they are exposed. Insurers may wish to carefully investigate cyberliability coverage claims, keeping in mind that the cyber landscape will likely continue to develop rapidly.

[78] Id., at ¶ 27.
[79] Id., at ¶ 26.
[80] Id., at ¶¶ 27, 29-31.
[81] E.g., Williamson & Vollmer Engineering, Inc. v. Sequoia Ins. Co., 64 Cal. App. 3d 261, 274-275 (1976).
[82] Columbia Cas. Co. v. Cottage Health Sys., No. 2:15-cv-03432, 2015 U.S. Dist. LEXIS 93456 (C.D. Cal. July 17, 2015).
[83] Columbia Cas. Co. v. Cottage Health Sys., No. 16-56872 (9th Cir. Jan. 26, 2018).
[84] Cottage Health Sys. v. Columbia Cas. Co., et al., No. 16CV02310, Santa Barbara, California Superior Court, Complaint (filed May 31, 2016).
[85] Id., Docket, at 8 (reviewed Feb. 23, 2019).
[86] See Seals, T., 2015, "ISACA lays out forensics in the data breach era," Infosecurity Magazine, March 24, https://bit.ly/2tve9u7
[87] 439 F. Supp. 2d 831, 840 (W.D. Tenn. 2006).
[88] Id.

LIFE AFTER LIBOR: WHAT NEXT FOR CAPITAL MARKETS?

MURRAY LONGTON | Principal Consultant, Capco

ABSTRACT

In the aftermath of the financial crisis, rigging scandals, and sanctions, the days of LIBOR, the London Interbank Offered Rate, are numbered. As the predominant interest rate benchmark for USD, GBR, CHF, and JPY derivatives contracts, replacing LIBOR will fundamentally change the financial services industry. In this paper, we share what businesses should expect to come next, and how they can prepare for the transition.

1. INTRODUCTION

Since 2008, there has been less liquidity in the interbank market to derive rates – this has been the natural result of the introduction of Basel III and its demands to require banks to reduce their reliance on short-term funding. Lehman Brothers and Northern Rock were the antagonists in the liquidity versus capital paradigm. Their inability to rollover short-term wholesale deposits was a catalytic factor in the 2008 crash. The regulatory response to this, Basel III, required institutions to demonstrate and maintain stronger capital ratios, reduce systemic risk, and show movement away from a top-heavy reliance on short-term interbank funding.

Running in parallel to Basel III, the FCA (Financial Conduct Authority) Wheatley Review of LIBOR in 2012 performed analysis across ten currencies and fifteen tenors ranging from overnight to one year. The review would act as the "blueprint" for LIBOR reform, with analysis focused on setting interest benchmarks and understanding the costs to banks of unsecured borrowing for a given currency and time period.[1] The review required greater regulatory oversight of LIBOR markets and elimination of the less liquid currencies and tenors from the required daily submission, "making explicit and clear use of transaction data to corroborate their submissions."[2]

The combination of Basel III's liquidity requirements and FCA's demand for a panel of experts to exercise "expert judgment" resulted in the Bank of England beginning their consultation for replacement "risk free rates" (RFRs, hereafter) in March 2015.

In July 2017, the FCA identified SONIA (Reformed Sterling Overnight Index Average) as the Pound Sterling RFR. Ultimately, this then led to the FCA's 2018 commitment to remove LIBOR by 2022. SONIA was chosen as the preferred risk-free alternative because it is able to evolve over time (demonstrating robustness to changes in underlying markets), it tends to be predictable (tracks Bank Rate very closely), and is already referenced in the liquid overnight index swap (OIS) market; hence making the transition easier.[3]

[1] https://bit.ly/2IlRJo9
[2] Ibid
[3] https://bit.ly/2TSoTSh

2. SO, WHAT IS GOING TO CHANGE?

Before looking at what will change, it is important to understand how the IBOR benchmarks have operated until recently. For two decades, participants have used IBORs as a way of measuring the overall "well-being" of the banking system – it was a very direct mechanism by which a bank would understand the financial health of other banks and how they are performing. End of day submissions by individual banks would be taken as gospel and the published rates would be accepted as stated. The non-binding quotes had no transactional data supporting them and there was no substantial evidence of the liquidity of the specified markets, thus allowing the interbank offered rates to be easily manipulated.

Inevitably, the introduction of the new RFRs will challenge the status quo and the subsequent reformation of the interbank offered rates will require market participants to change. With the main message from regulators and governing bodies reiterating the importance of integrity, robust transactional data, and protection against manipulation, the collaborative effort has already resulted in some very important moves away from the normal practice. Regulators and market participants will feel these changes as they mark an important paradigm shift in the way business has been practiced for the past twenty years.

By the end of 2021, market participants must provide a sound, tactical, and timely plan to move toward the near-risk free "alternative reference rates" (ARR). This was outlined by Andrew Bailey, Chief Executive of the FCA in July 2018,[4] marking the end of the well-established IBOR benchmark.

Secondly, new RFRs will be introduced. The Bank of England and other central banks have been working on this since 2015. The established working groups have identified their respective RFRs based on the guiding principles set out by the FSB (Table 1).

Thirdly, the new RFRs are overnight rates, based solely on real transactions, predominantly because of the recommendations of the Financial Stability Board (FSB) and the Financial Stability Oversight Council (FSOC) to pursue a two-pronged reform approach for strengthening global benchmarks. The first prong encourages the development of RFRs that are more firmly based on transactions and adhere to IOSCO principles for financial benchmarks. Members believe that there are certain financial transactions (predominantly derivatives) that are better suited to reference rates that are closer to risk-free. The second prong looks to strengthen existing IBORs and other potential reference rates based on unsecured bank funding costs by underpinning them to the greatest extent possible with transaction data.

Given that IBORs represent the average rate at which "panel banks" borrow money in the interbank market (thus reflecting credit and liquidity risks associated with lending), the difference between IBORs and RFRs are important to note from an economic point of view. In the first instance, RFRs are backward-looking, relying on sufficient and reliable market data – a stark contrast to what has previously existed. Where IBORs have looked at the future interest rates and market conditions when setting a rate, the new RFR methodology will not reflect future expectations in the market, thus causing fluctuations in funding risk.

Table 1: Overview of alternative reference rates

COUNTRY	WORKING GROUP	ALTERNATIVE RFR	ADMINISTRATION	COLLATERAL	PUBLICATION
U.S.	Alternative reference rates committee	Secured overnight financing rate (SOFR)	Federal Reserve Bank	Secured	April 2018
E.U.	Working group on risk-free reference rates for the Euro Area	Euro short term rate (ESTER) replaces EONIA	European Central Bank	Unsecured	October 2019
U.K.	Working group on sterling risk-free reference rates	Reformed sterling overnight index average (SONIA)	Bank of England	Unsecured	April 2018
SWITZERLAND	The national working group on CHF reference rates	Swiss average rate overnight (SARON)	SIX Swiss Exchange	Secured	Already published
JAPAN	Study group on risk-free reference rates	Tokyo overnight average rate (TONA)	Bank of Japan	Unsecured	Already published

[4] Bailey, A., 2018, "Interest rate benchmark reform: transition to a world without LIBOR," Speech by Chief Executive of the FCA, at Bloomberg, London – on transitioning from LIBOR to alternative interest rate benchmarks, https://bit.ly/2Y0YpgC

Secondly, RFRs are based on overnight rates, borrowed on a secured basis. This reflects the requirement for greater control over risk exposure.

Thirdly, IBORs have embedded credit premium, whereas RFRs have no premium, marking a shift away from the risk premium a borrower must pay to lenders as "compensation" for supplying funds at an unsecured rate.

Fourthly, each RFR is calculated on a currency-by-currency basis with no standardized/consistent approach. Cross currency issues will pose a challenge to many participants because the USD-LIBOR and EURIBOR have been the bedrock elements of the global funding markets (many banks will fund their domestic currency assets is USD markets, using cross-currency swaps to hedge funding with USD referenced in one leg and the local currency referenced in the other).

Finally, there is no certainty there will be a term rate for all currencies. While central banks are looking at the creation of forward-looking term rates, this is not guaranteed to work. It is, therefore, probable that many bank clients will likely opt for a new RFR, though some will certainly will opt for overnight rates.

3. WHAT WILL BE IMPACTED BY THIS CHANGE?

As with any regulatory change, there is speculation as to what market participants will do. Many participants are adopting a "wait and see approach" under the modus operandi that IBORs will continue to exist in some shape or form.[5] Some are expected to accept the fallback RFR and transition as and when confirmed. While, others are expected to adopt a "halfway house" approach and start trading out of IBOR-based products over time.

With the new RFRs building a benchmark that provides credible and robust reference rates, it is a given that both cash and derivatives markets will migrate. It is suggested that the former (cash) will find this transition the most difficult due to the unique nature of contracts and tighter links to IBORs. However, at the highest level, the following products will be impacted:

- All IBOR-based term/RCF/money market loans
- All IBOR-based commercial paper
- Trade discounts
- Liquidity deposits
- OTC Derivatives (cleared)

Given that the existing market value of all products that reference IBORs exceed U.S.$400 trillion in size[6] and OTC derivatives and ETDs represent approximately 80% of LIBOR-linked contracts,[7] we can state with confidence that OTC derivatives and ETDs, syndicated loans, securitized products, business loans, retails loans, floating rate notes, and deposits will all be impacted by this transition.

To understand the impact of this across the industry, let us take a very simple model where the Treasury Function of Bank "X" (which specializes solely in fixed-income securities) will have to change. For the purpose of this example, let us focus on repos (overnight unsecured lending rates, general collateral lending rates, treasury bill, or bond rates, etc.) and how a suite of products will be impacted by an IBOR to RFR transition.

The Treasury Function of the bank will need to map out a strategy for creating liquidity at a new rate, including its use of "price alignment interest" calculations and discounting. Should a fallback rate be selected, and LIBOR becomes obsolete, the bank will have to demonstrate a number of key requirements to regulators: liquidity, transaction volumes, resilience through periods of illiquidity, resilience to changes in regulatory approach, transparency of data, and evidence of governance structures against a new rate.

Market making capabilities will need to be determined from bank-wide business priorities, focusing on the commercial, client, process, infrastructure, and controls challenges:

[5] Garcia, C., and J. M. Schneider, 2018, "So long, Libor: transition is underway to SOFR and other alternative reference rates," View Point, PIMCO, August, https://bit.ly/2O9ctQL

[6] IIF, 2018, "Capital markets monitor: Libor transition: progress, but challenges remain," Institute of International Finance

[7] FSB, 2014, "Final report of the market participants group on reforming interest rate benchmarks," Financial Stability Board, July 22, https://bit.ly/2UJL8ac

- **Commercially:** what the implications of capital allocation means to new markets and initial product offerings.
- **Clients**: how the definition of client strategy for onboarding, categories, disclosures, etc., should be determined.
- **Process:** redefining of trade capture and operational support, aligned to commercial strategy and business decision.
- **Infrastructure:** how to implement infrastructure for new products, how to evaluate market data systems (legacy and new) and connectivity requirements, and the implementation of risk/pricing models for new products.
- **Controls:** assess legal jurisdictional and cross-border impact on existing regulations and create policy and procedures for new rates.

Although the above example focuses on the impact upon a Treasury Function in a fictional bank, it does show how banks will have to adopt new processes for impacted businesses. From an industry point of view, participation in working groups will be necessary to fully understand the changes coming, but also to provide feedback on RFR selection options and calculation methodology. The reason being two-fold: initially, to understand changes to trading and execution scenarios and, secondly, how the market infrastructure (middleware, CCPs, etc) will need to be setup.

Another important consideration is assessing the impact on existing loans or contracts maturing post LIBOR removal. For example, clients with loans that expire beyond 2021 will either need to refinance or convert their existing facilities to the appropriate RFR through an "amendment and waiver" request. This is a notoriously laborious and complex process. Furthermore, current market standards only cater for temporary unavailability of IBORs, there has been no definitive confirmation of what the market will look like with no IBOR benchmark. From a syndicate loan point of view, contracts typically require 100% syndicate consent before any change can be made to address the existing benchmark, let alone a new benchmark. Legally, new wording will have to be added to contracts that allows for majority lender consent and re-papering will require significant time and cost. Lastly, each borrower will need to agree the conversion mechanism with its lender group, subject to the RFR selected.

Any affected product (from a client point of view) will either need to be canceled or amended by the end of 2021. Any clients who benefits from hedge accounting will need to sync up with auditors to understand any potential impact. More importantly, clients will have to consider the impact on their cash requirements if interest costs can only be determined immediately before falling due.

4. WHAT NEXT?

In today's regulatory and operating environment, non-compliance and lax controls can be extremely costly. Financial institutions need to engage in an enterprise-wide transformation early to identify, prevent, and mitigate risk. A comprehensive IBOR transition program will comprise the following:

- Setting up a LIBOR/IBOR transition "project management office" (PMO) to build a structured program that will ensure the successful delivery of the LIBOR transition.
- Alignment of business lines and functional groups, including asset/liability management, collateral management, CCP & Clearing, etc.
- Impact and risk assessment.
- Implementation of the necessary adjustments and compliance solutions, including adjustment to multi-curve variation, changes to discounting curves, establishing a parallel discounting regime, and stress testing.
- Contracts and client communication management.

In conclusion, banks and asset management firms are already creating impact assessments to understand how the shift away from IBOR may affect their products and overall business, and to that end are working to develop wider IBOR transition programs. As organizations push ahead, they need to ensure that individual business lines and functional groups have the support needed to transition to, and make available, new RFR products, services, and offerings, particularly from a treasury and funding point of view.

AN IMPLEMENTATION FRAMEWORK TO GUIDE SYSTEM DESIGN IN RESPONSE TO FRTB REQUIREMENTS

OLIVIER COLLARD | Principal Consultant, Capco
CHARLY BECHARA | Director of Research & Innovation, Tredzone
GILBERT SWINKELS | Partner, Capco

ABSTRACT

The changes that must be made to a bank's infrastructure to implement the "fundamental review of the trading book" (FRTB) standards are transformational. The data and process requirements are such that pricing platforms need a complete overhaul to meet performance and latency goals. This article will present a viable design process, and the supporting framework, to fully leverage today's multi-core environments, be it cloud or otherwise.

1. INTRODUCTION

In order to implement the "fundamental review of the trading book" (FRTB), banks have to deal with requirements imposed by the Internal Model Approach (IMA) and Standard Approach (SA). A majority of banks will opt for an IMA approach, at least for a large part of their trading activities, in order to optimize their capital requirements. But even if banks go for IMA, they will have to compute SA in parallel to compare both.

Complying with FRTB requirements generally requires a significant rework of the front-to-back trading infrastructure to cope with "orders of magnitude" increases in the number of computations, an equally massive increase in volumes of data consumed and produced, and a need to harmonize the use of pricing and risk data and models across a complex process chain.

This article explains how the Reactive software design approach and the supporting Simplx open source framework from Tredzone™ can help address some of these challenges.

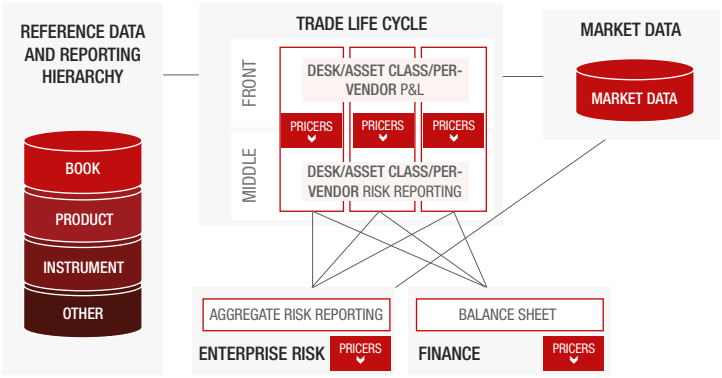
2. FRTB TECHNOLOGY IMPACTS

FRTB will have a number of technological implications for banks, including:

Massive increase in the number of computations
FRTB changes the approach to model risk for banks, based on notions like Expected Shortfall (ES), "Standardized Approach," and the concept of Non-Modellable Risk Factors for capital requirement computations. As a consequence current sensitivities-based optimizations will need to be reconsidered, using full revaluation methods instead. This requirement is expected to result in a tenfold increase in the number of P&L calculations required, further magnified by the ever-increasing need to move to real-time stress testing to provide transparency into capital consumption.

Harmonized processes and forms of governance
FRTB favors a realignment of governance and approaches between the front office and the risk department, leading to a consolidation of front-office risk engines. This trend challenges the existing reliance on trading and

Figure 1: Typical front-to-back trading architecture



risk packages from different vendors, often deployed based on the preferences of individual desks depending on the assets they trade. The P&L and risk attribution will be checked at the trading desk level. Consistency requirements mean that pricing data and libraries need to be streamlined across desks and across aggregated risk reporting stacks.

Data quality requirements and volumes increase consistency in pricing and risk calculations across the firm can only be achieved by ensuring that there is a single source of trade data, that market data, and everything that is calculated from it (like volatility surfaces and curves), have a single and common source, and that reference data used to enrich the trades (e.g., product taxonomies) are unique across the firm.

3. CURRENT ARCHITECTURE AND LIMITATIONS

Organizations often rely on a number of front-office systems, sourced from independent software vendors, with each responsible for a subset of a bank's assets or trading desks. This results in a "siloed" infrastructure, where separate risk reports are built for each platform.

Banks would address this lack of systems interoperability by deploying an additional, enterprise-wide risk layer. While successful at building a cross-asset view of the risk, this approach still relies on each underlying system's specifics about pricing algorithms, shock scenarios, risk factors, and reference data definitions (e.g., using different yield curves).

This often results in hard-to-explain valuation discrepancies among the business, risk, and finance views, with additional costs in computing hardware provisionning.

4. SYSTEM INFRASTRUCTURE REQUIREMENTS

The increase in calculations required by FRTB will likely push many conventional grids over their limits, thereby increasing the need to review systems in a fundamental way.

The requirement for computing power and the shift to a unified pricing framework motivates adoption of technologies and architecture models that (i) leverage highly parallel and resilient hardware grids for horizontal and vertical scale out, possibly spread across private and public clouds; (ii) deploy computing application frameworks that favor data and processing colocation (shared-memory, ideally in-process) for efficient processing of large datasets; (iii) are "implementation-technology aware," efficiently scheduling computations including pricing modules implemented as native C++ code or concurrently accessing GPGPUs; (iv) have low and deterministic scheduling overhead to match the front-office near-real-time requirements for pre-trade analysis; and (v) provide full control of systems with a rich and holistic development environment, supportive of agile approaches.

The introduction of new architecture components is an opportunity to consider technologies backed by open-source projects, reducing the silo (duplication, model coherence) effect that would result from mixing off-the-shelf solutions from different vendors.

5. SOLUTION DESIGN

5.1 Target architecture

Key to the IMA approach is the requirement to ensure the desk-by-desk P&L attribution. This requires the deployment of a unique cross-asset pricing framework, servicing the front office, risk, and finance functions alike with one "golden source" for trade, market, and reference data. Using a shared pricing framework also allows for efficient allocation of computing resources, with expected savings on infrastructure, better accountability and traceability, and back-testing.

Figure 2: Target front-to-back architecture

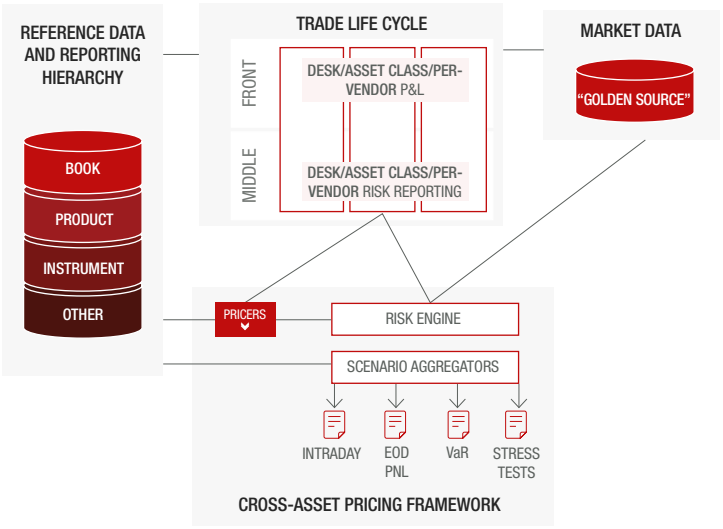
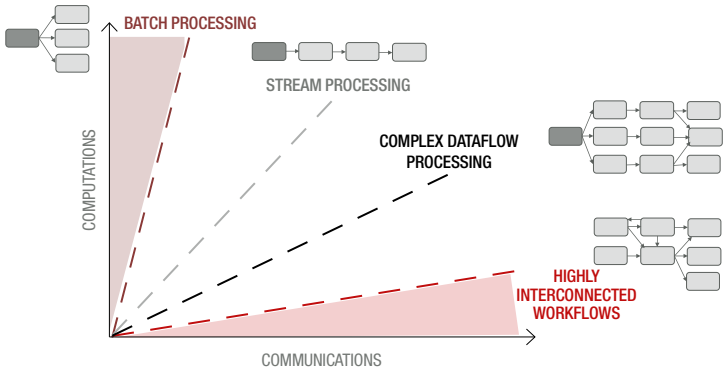


Figure 3: Computational application profiles



This "cross-asset" pricing framework becomes the single source of truth for all valuations, conforming to the intraday front office P&L computations for IMA and SA risk reporting.

The remainder of the article describes an approach to implementing such a pricing framework.

5.2 FRTB computational profile

Designing performance-driven applications requires careful characterization of the computational profile and a good understanding of the often-overlooked low-level execution environment. This is even more true when the solution design involves highly-parallel architectures.

Each application has a computational profile that results from a balance between the amount of CPU computations and the amount of communication between software modules. This spectrum is described as follows:

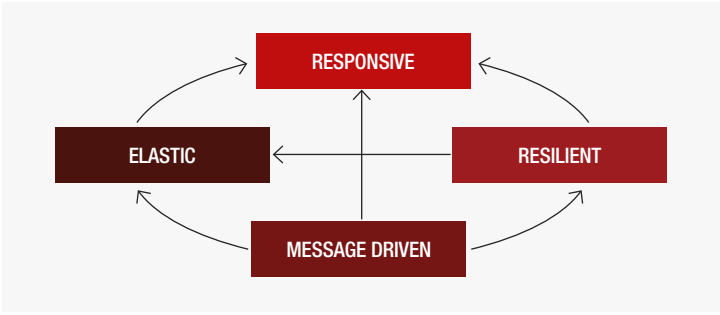
- **Batch processing** (a.k.a. "embarrassingly parallel processing"): consists of modules that require little to no synchronization (i.e., there is no or little need for tasks to communicate results between them).
- **Dataflow processing** (a.k.a. "stream processing"): software modules have only static dependencies upon each other, allowing the application to easily exploit a limited form of parallel processing. In this type of application one can emphasize the movement of data and model the application as a series of connections. Explicitly defined inputs and outputs connect the modules, which function like black boxes. A module runs as soon as all its inputs become valid, which makes the overall application inherently parallel.
- **Complex dataflow processing:** a more complex form of dataflow processing with multi-stage task dependencies. Efficient task scheduling can still be done statically.
- **Highly-interconnected workflows** (a.k.a. "complex event processing"): highly-interconnected workflows, combining data from multiple sources, where the frequency of communication between modules and their inter-dependencies are high and dynamic. Task scheduling needs to be done dynamically.

Each category has a corresponding set of proven solution patterns, programming models, frameworks, libraries, compiler features, or even dedicated hardware (e.g., GPGPU or general-purpose computing on graphics processing units).

FRTB system infrastructure requirements singularly mix all these computation models:

- The Expected Shortfall requires the computation of a high number of pricings, based on historical data or Monte Carlo scenarios. This matches both the "complex dataflow" and "batch processing" categories, typically addressed using a mix of multicore CPUs and/or GPGPUs.
- Sensitivities calculations have a "streaming" profile, where smart memory reuse between iterations is key to CPU performance optimization.

Figure 4: Actor Model



- Efficiently scheduling and refreshing computations based on trade, market, and reference data updates, qualifies for the highly interconnected workflow computation profile, with a strong requirement on multi-core scheduling in the context of large data transfers.

Implementing different computation models requires careful application design, with significant consequences on code complexity and maintainability. This complexity can be visualized using the Roofline performance model,[1] an intuitive approach to a platform performance expectations analysis in the context of a specific hardware.

The model identifies five performance ceilings that constrain runtime performance: processor peak performance (floating point operations per second or FLOPS), memory bandwidth, inter-process communication (instruction pre-fetching, non-uniform memory access), computation (instruction-level and task-level parallelism), and data locality (cache misses qualified as compulsory, capacity, or conflict misses).

A valid solution design under FRTB requirements must balance its module parallelization so that CPUs can be kept busy, avoiding waiting for data from remote or local storage, memory, cache on the CPU, or from OS thread synchronization, etc. The design must, therefore, carefully leverage the hardware (storage, cache, and memory) and properly schedule both IOs and computation threads on multicore platforms.

The FRTB requirements (more computations on growing data volumes combined with a need for real-time processing) is generally considered a strong case for asynchronous, distributed microservice-based architectures.

[1] https://bit.ly/2NB0ZFd
[2] https://bit.ly/2I2HXud

6. SOLUTION DESIGN METHODOLOGY

Reactive software is a design philosophy and a paradigm shift that combines building both large-scale reactive microservices and fine-grain reactive applications (one process). Based on asynchronous message-passing design, there exist a plethora of concurrent programming models that allow for building a reactive software from the ground up. The actor model is one such battle-proven programming model and is the design model supported by the C++ framework we will discuss below.

Reactive systems are software systems that satisfy the four properties depicted in the Reactive manifesto:

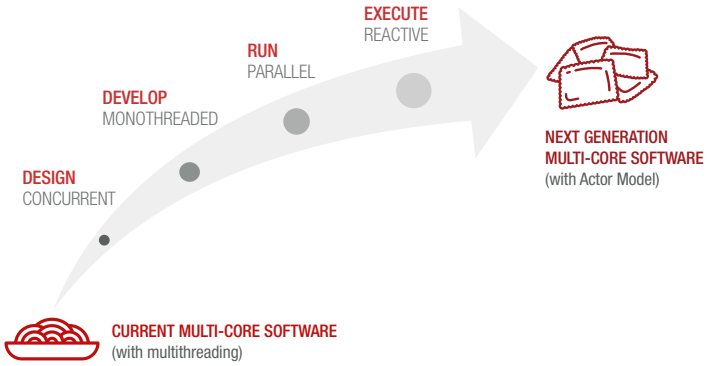
- **Responsive:** to the real-time user demands, as well as internal system components demands. Ensure service continuity.
- **Resilient:** system stays responsive in the face of failure. Resilience is achieved by replication, containment, isolation, and delegation.
- **Elastic:** system stays responsive under varying workload, achieving elasticity in a cost-effective way on commodity hardware and software platforms.
- **Message-driven:** systems rely on asynchronous message-passing to establish a boundary between components that ensure loose coupling, isolation, and location transparency.

The **Actor Model** is a concurrent computation model that uses "actors" as the universal primitive of concurrent computation. It was invented by Carl Hewitt in 1973. Back then, the CPU computing power (single core, 1 MHz, ~5000 transistors, slow I/O, expensive memory) and the application requirements (few concurrent users, small datasets, latency in seconds) did not justify or allow for such complex distributed and parallel systems.

Since then, the theory and practice supporting the Actor Model have matured and proved their worth to software developers and architects for concurrent applications development: actors ended up at the core of the highly respected Erlang programming language, and actors constitute the perfect ground for building Reactive Software, as depicted in the Reactive Manifesto.[2]

Actors form the base constituents of an application logic. Actors communicate with asynchronous events, relying on an execution infrastructure for routing and load-balancing messages transparently. The infrastructure is responsible for optimal actor distribution and monitoring, effectively

Figure 5: Structuring multi-core development



decoupling functional logic from the application's technical execution or deployment. The runtime transparently handles interactions between actors, using in-process communications when possible, and falling back to the network otherwise.

Actors are a very efficient concept, supporting the whole development to production lifecycle. By being directly mapped to functional concepts, actors shorten the distance between business and functional architectures; they encapsulate the logic at a level granular enough for splitting work between developers; they are directly usable concepts for testing; and they allow administrators to decide the topology dynamically, based on available hardware and application load.

7. SOLUTION FRAMEWORK

Implementing a reactive system requires an IT stack with full control over execution, as well as the development flexibility to express the computational problems we described.

A plethora of concurrent programming models and frameworks exist, defining abstractions intended to simplify the developer's job of mapping functional logic to computational resources. Some of these frameworks are successful at hiding the complexity of resource sharing and contention, especially in data-driven cluster deployments, but often fail at efficiently scheduling computations, trading off hardware resources for ease of implementation.

CPUs implement highly sophisticated architectures with multiple levels of parallelization:

- **Instruction-level parallelism (ILP):** several execution units per core and multiple instructions per cycle.
- **Data-level parallelism (DLP):** single instruction, multiple data (SIMD) instructions for vector-computing – multiple processing elements that perform the same operation on multiple data points simultaneously.
- **Thread-level parallelism (TLP):** several processing cores (a.k.a. "multicore") per CPU chip.

Data and instruction-level parallelisms are technical, low-level optimizations, available to native code compilers or virtual machines only. Thread-level parallelism, however, is where application developers and application frameworks come into the picture. This type of design is considered among the most challenging for developers to get correct: inter-thread synchronization and performance considerations (like thread scheduling, thread contention, and coherence) abound.

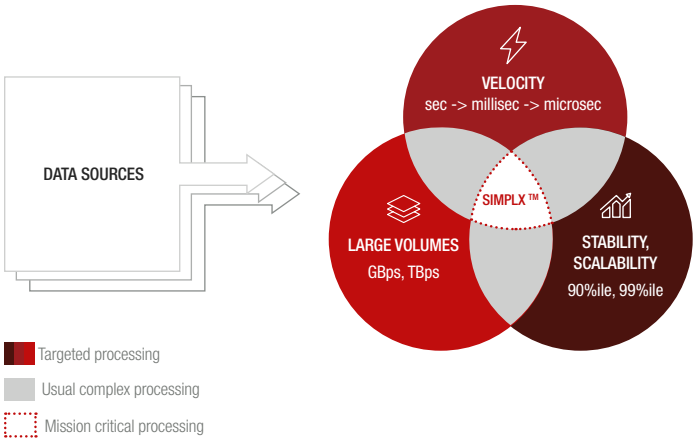
The downside of typical microservice architectures, and the frameworks they build upon, is a focus on the development lifecycle and functional decoupling of deployed artefacts, often trading resources overhead for operational efficiency. While the network resources latency overhead is generally well controlled, the subtler effects of the execution model and the performance bottlenecks raised by multicore execution and memory data transfers are less understood, especially by developers used to JVM development. Yet, mission-critical applications must optimize for multi-core systems and properly schedule communications between functional modules, avoiding message bus intermediaries (Appendix 1).

The ideal software stack allows for building a holistic system with the right balance between high volume processing, fast velocity, infinite scalability, and extreme stability. This calls for a framework fostering in-memory and in-cache computing, core-aware communications, asynchronous inter-thread, and process communication.

Functional drivers for the framework:

- Have **highly-available platform** with native resilience and recovery features.
- Have support for **service-oriented** development patterns.
- Have **loosely coupled** business and technical layers, supporting component composability and reusability, as well as code maintenance.

Figure 6: Ensuring a stable system under heavy computational loads handling large data volumes



- Enable **platform reactivity and responsiveness** with respect to more demanding user activities as well as burst activities.
- Increase **throughput scalability** with number of deployed hardware cores, and with **deterministic response time** (stability > 90 percentile).
- On demand, **compute the right functionalities** to enable the real-time processing based on the infrastructure resources.
- Target-deployment agnostic, addressing grids and clouds (whether hybrid or native) alike, through reconfiguration only.
- Have **real-time monitoring** of software transactions and in-process activities without impacting the performance.

8. SIMPLX™: OPEN SOURCE ACTOR MODEL FRAMEWORK AS ENABLER

Most of the frameworks implementing the Actor Model target JVM environments (e.g., Akka, Scala). Tredzone Reactive Toolset (a.k.a. Simplx™) is the only solution available for mission-critical and latency-sensitive applications implemented in C++ (Appendix 2).

The core technology is a multicore-optimized Actor Model runtime that is integrated in an application as a simple C++ API, and which is responsible for (i) managing the thread's lifecycle and multithreading low-level synchronizations, (ii) managing the cache memory and memory recycling, (iii) managing actor concurrency and scheduling on all cores, (iv) managing communications between actors and CPU cores, all in-memory, (v) adaptive communication performance: embedded throttling in API, (vi) low-level real-time performance monitoring, (vii) on-the-fly multicore deployment, (iix) multicore hardware optimizations and abstractions, and (ix) error handling and management.

Figure 7: Simplx™ ecosystem

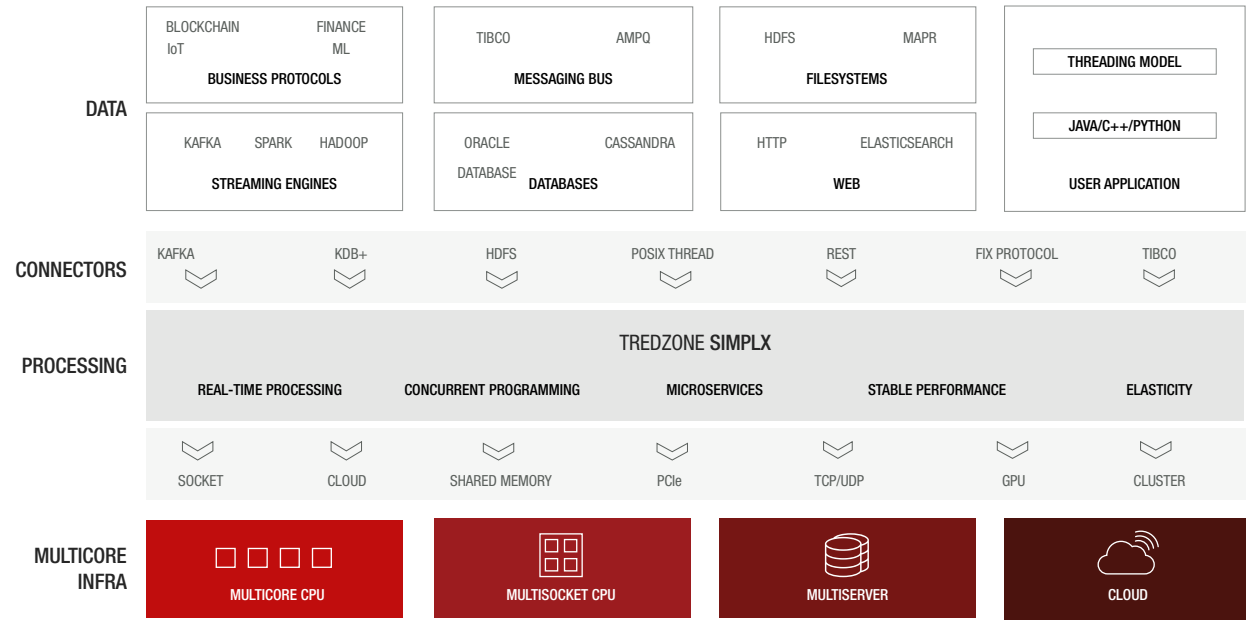
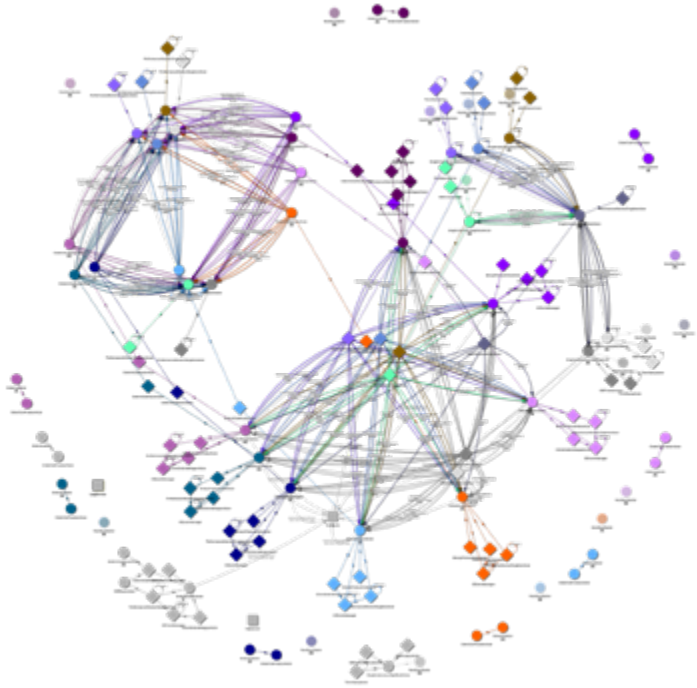


Figure 8: Simplx™ live application monitoring example



The core runtime technology has the following characteristics:

- **No vendor lock-in**, as open sourced under the Apache 2 license[3].
- **Low memory footprint, no "third-party" dependencies, in-memory and in-cache computing.**
- **Single threaded per core**, 100% distributed runtime architecture, enabling vertical scalability by adding more cores with no centralization bottleneck.
- **Clustered runtime architecture** allows for the composition of multiple runtimes to form a communicating cluster (for microservices), hence scaling **horizontally** when adding machines.
- **The core runtime is built in C++ 11.**
- **With multicore hardware portability** the runtime is portable to any multicore hardware architecture (x86, SPARC, ARM, etc.), and even exotic ones (Xeon PHI, Cavium, Kalray, etc.).
- **Operating system portability** works on Linux, Windows, and Mac.
- **Language agnostic** allows for the integration of the native C++ API with a Java or C# API, allowing the mix of actors implemented using a variety of programming languages in the same system. This may prove useful for building a complete FRTB platform, integrating modules from quants, market data providers, risk systems, etc.

In addition to the open-source runtime, Tredzone provide a rich set of DevOps tools to help with debugging, live monitoring (Figure 8), profiling and testing, as well as an ecosystem of convenience libraries and connectors to interface with databases, message buses, or GPGPU hardware.

9. CONCLUSION

FRTB requirements are pushing financial firms to consider alternatives to their existing risk platforms, including resorting to custom implementations. As banks outline a vision of their future infrastructure, their design should reflect the objectives outlined above: reactive and scalable, consistent through golden sources, as well as efficient through the use of standardized design patterns supported by proven frameworks.

This paper explained how a Reactive software design approach,[4] as implemented in Tredzone's Reactive Toolset™, can help address these challenges.

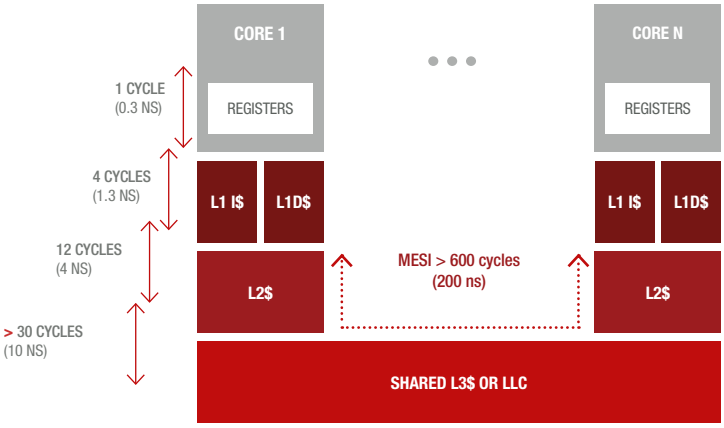
APPENDIX 1: MULTICORE CPU HARDWARE

The mid-2000s marked the end of the Moore's law era, when upgrading to higher-frequency hardware brought automatic performance enhancements. Instead, the industry turned to a model where performance gains come from adding more execution units (cores). But leveraging multicore architectures requires extra development and testing efforts, and a naïve approach of adding more threads often falls short of scalability expectations.

An application relying excessively on threads and/or synchronizations between threads will defeat operating system and hardware schedulers as application threads will inefficiently compete for data access. As documented in Figure A1, the main parameters that impact scalability are:

[3] https://bit.ly/2H3SRMp
[4] www.reactivemanifesto.org

Figure A1: CPU cache access latency



Assuming Freq = 3 GHz

- **Core resources contention** is due to hyperthreading for example. Several software threads want to access simultaneously to the same execution units, and thus processing is serialized and prioritized.
- **Cache memory contention** occurs when there is contention from the same core on its private cache memory (L1/L2) in case of operating system context switch, or when the problem size is too big to be stored in the private cache memory. This phenomenon is called cache thrashing. In multicore, cache thrashing occurs on the shared L3 cache (or LLC last level cache) between the cores. Hence, the impact is several hundreds of nanoseconds lost in latency. The solution is an intelligent software that improves the data locality in-cache processing in order to also improve the memory bandwidth utilization while keeping the CPU core busy doing local computation; this is a very difficult problem, and there is no easy solution today. This is a typical problem in HPC stencil computation.
- **Cache coherency** is a hardware mechanism that allows for core to core seamless communication whenever there is a software synchronization (mutex, barrier, etc.) or access to the same memory area by both cores. A simple cache coherency (one cache line) costs at least 600 cycles.

APPENDIX 2: THE EURONEXT USE CASE

In spring 2014, Euronext started a new phase of their history as an independent listed firm, span-off from ICE.

They immediately identified a major strategic priority: upgrade their technical infrastructure in order to make it easier to follow the fast-changing business requirements. This resulted in contradictory constraints: make performance fully predictable and reduce latency, cope with increasing and in practice unpredictable volumes, and cope with new functionalities, hence increasing complexity. These contradictory requirements sounded like an impossible mission. As is often the case, when faced with engineering challenges, the first reaction was to seek hardware capability improvements (newer multicore-based machines). However, close analysis concluded that relying on hardware upgrades alone would not significantly improve performance, while adding to the complexity of managing a large infrastructure.

The project itself was raising contradictory interests between stakeholders, making communication increasingly difficult and creating an increasingly tense dialog between implementation teams.

Tredzone demonstrated the value of its Simplx™ reactive toolset to Euronext. The inner features of its reactive-design approach, its optimal handling of cluster resources scheduling, and its extensive set of productivity tools proved essential to the performance, stability, and monitoring of Euronext's new platform. Tredzone's technology became the foundational backbone of Euronext's Optiq® trading platform. A distributed team iteratively released the new Optiq platform components over less than three years.

Optiq® achieved dramatic performance improvements, running 10 times faster (tens of microseconds) and at a high level of stability (99th percentile), while dividing the hardware footprint by four. This resulted in significant savings and a positive return on investment.

CYBER RISK FOR THE FINANCIAL SERVICES SECTOR

ANTOINE BOUVERET | Senior Economist, European Securities and Markets Authority[1]

ABSTRACT

Cyber risk has emerged as a major concern for the financial services sector. In this article, we outline the main channels through which cyber risk can affect a financial institution, and provide some insights based on recent cyber-attacks. We also outline a framework that can be used to estimate potential losses due to cyber risk for financial institutions.

1. INTRODUCTION: FINANCIAL INSTITUTIONS ARE HIGHLY EXPOSED TO CYBER RISK

Cyber risk has emerged as a systemic risk concern, following recent cyber incidents [IIF (2017), IMF (2017b), and OFR (2017)]. Indeed, recent surveys point to cyber risk as a main concern among market participants: it ranked first in the DTCC Systemic Risk Barometer (Figure 1), and second in the 2017 H2 systemic risk survey by the Bank of England [Bank of England (2017)]. Successful cyber-attacks, such as Wannacry in May 2017 or NoPetya in June 2017, have shown that they can lead to severe disruptions and major losses for the targeted firms.

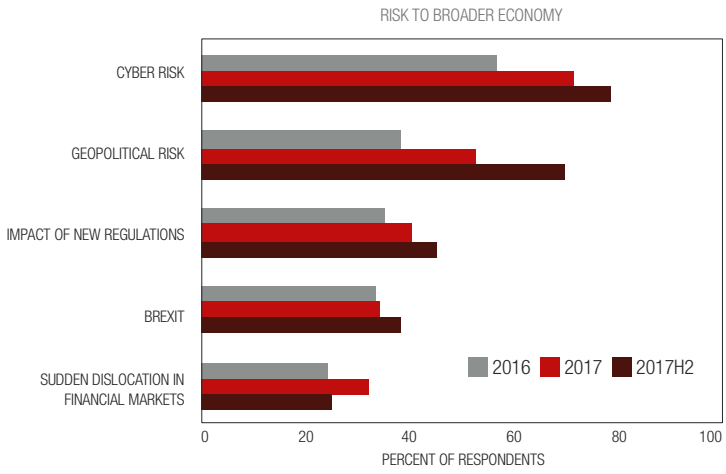
The financial services sector is highly exposed to cyber risk, across all types of countries. For illustrative purposes, we build an indirect measure of cyber risk by country for the financial services sector, using media coverage. An index is computed using the number of articles referring to cyber risk by country, divided by the number of articles referring to risk in the financial sector (Figure 3). As shown in the map, almost all countries are covered. The index is highest in countries that recently suffered from cyber-attacks, such as Bangladesh and the Baltic states.

Against that background, countries (and companies) have very different levels of cybersecurity. The International Telecommunication Unit (ITU) – an agency of the United Nations – provides a global cybersecurity index for the world. Their index is based on a range of factors, including legal, technical, and organizational arrangements, as well as capacity building and cooperation [ITU (2017)]. Figure 4 shows the cross-country heterogeneity regarding cybersecurity, with most "advanced economies" and "emerging markets" having a high value on the cybersecurity index (above the median), while middle income and low-income countries tend to have lower values.

In that context, it is crucial to understand how cyber risk can affect financial institutions and why the financial sector is particularly vulnerable to cyber-attacks.

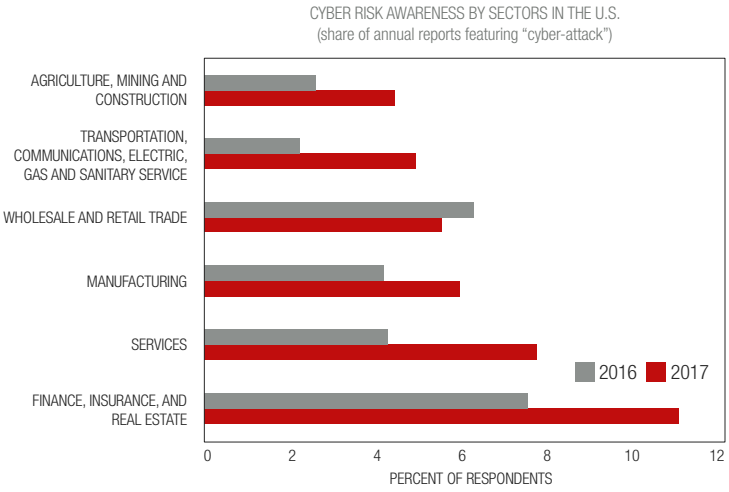
[1] The author alone is responsible for the content and writing of the paper. This article is based on work done by the author while he was at the International Monetary Fund. The views expressed are those of the author and do not necessarily represent the views of the IMF, its Executive Board, or IMF management. The views expressed are those of the author and do not represent the views of the European Securities and Markets Authority.

Figure 1: Survey of risks to financial stability



Source: DTCC Systemic Risk barometer

Figure 2: Reporting of cyber risk



Sources: SEC form 10-K; and staff calculations

2. HOW CAN CYBER RISK AFFECT FINANCIAL INSTITUTIONS?

Cyber risk can be defined as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems" [Cebula and Young (2010)]. Cyber-attacks can impact firms through the three main aspects of information security: confidentiality, integrity, and availability. Confidentiality issues arise when private information within a firm is disclosed to third parties, as in the case of data breaches. Integrity issues relate to the misuse of the systems, as is the case for fraud. Finally, availability issues are linked to business disruptions.

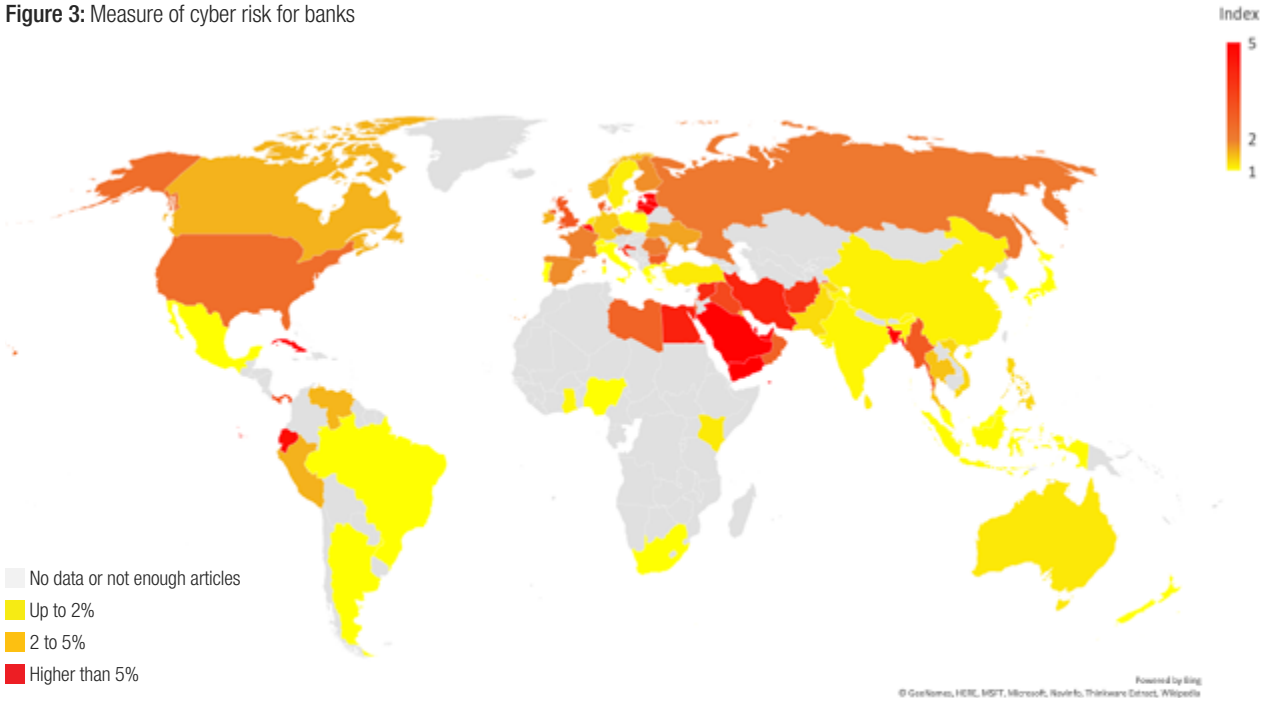
The three types of cyber-attacks have different direct impacts on the targets: business disruptions prevent firms from operating, resulting in lost revenue; fraud leads to direct financial losses; while the effects of data breaches take more time to materialize, through reputational effects as well as litigation costs. More generally, the risk of a loss of confidence following cyber-attacks could be high for the financial services sector, given the reliance of financial institutions on the trust of their customers. Regarding the financial system, business disruptions are more likely to have direct short-term contagion effects than fraud or data breach, which tend to mainly impact the targeted firm in the short term.

2.1 "Single point of failure" and critical infrastructures

Financial institutions are particularly exposed to cyber risk due to their reliance on critical infrastructures and their dependence on highly interconnected networks (Figure 2). Critical financial market infrastructures include payment and settlement systems, trading platforms, central securities depositories, and central counterparties. The critical infrastructures represent a "single point of failure" and any successful attack could have wide-ranging consequences. In that context, the ECB recently established the Euro Cyber Resilience Board for pan-European Financial Infrastructures [ECB (2018a)] and launched a public consultation on cyber resilience oversight expectations for FMIs [ECB (2018b)].

A business disruption of a financial market infrastructure or a set of large financial institutions could have a significant impact due to risk concentration [Kopp et al. (2017)] and the lack of substitutes in the case of "financial market infrastructures" (FMIs). If a payment and settlement system goes offline during the day, market participants would be unable to process transactions and, therefore, be exposed to liquidity and solvency risk. Similarly, if one or several large banks are disrupted and unable to process transactions, their counterparts would be subject to liquidity and solvency risk. Several papers have already looked at the impact of a disruption of a large market participant on FMIs, but not in the context of cyber risk. For example, Clarke and Hancock (2014) use

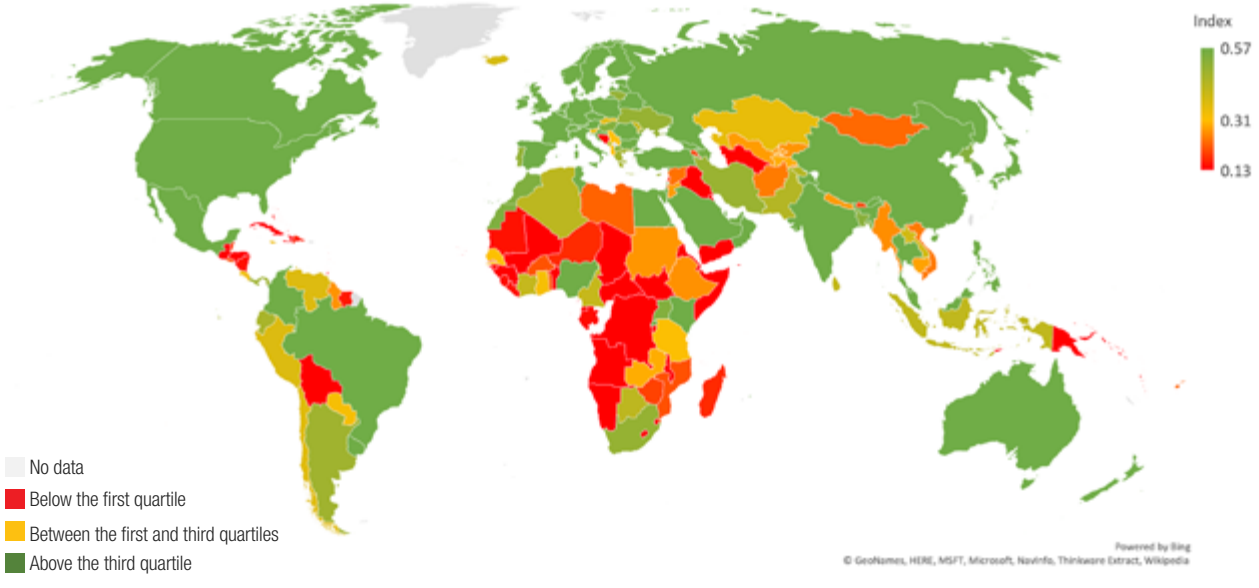
Figure 3: Measure of cyber risk for banks



Note: number of articles featuring "cyber-attack," "hack," "cyber risk," or "cybersecurity," and "banks," "bank," and "risk" divided by the number of articles featuring "banks," "bank," and "risk" by country. The index is not computed for countries with fewer than 25 articles on cyber risk (light blue). Only articles in English were included. Period range: January 2014-September 2017.

Sources: Factiva and author's calculations

Figure 4: Global cybersecurity index



Source: ITU (2017)

Table 1: Impact of disruption of infrastructures (all sectors)

SCENARIO	TARGET	LOSS (in U.S.$ bn)
ELECTRICITY BLACKOUT	Energy infrastructures	243-1,024
CLOUD SERVICE PROVIDERS HACK	Cloud providers	5-53
MASS VULNERABILITY ATTACK	Operating system	10-29

Sources: Lloyd's (2015, 2017)

the Bank of Finland payment simulator to analyze the impact of operational disruptions of the largest fifteen participants on intraday liquidity in the Australian Real Time Gross Settlement system. Their results show that the amount of unsettled payment varies according to the time of disruption and the participants' size.[2] Similarly, as part of their risk management framework, central counterparties (CCPs), and their supervisors, regularly assess the impact of events that could be the result of a cyber-attack leading to the business disruption of clearing members. For example, the recent stress tests of CCPs run by the European Securities and Markets Authority (ESMA) estimate the impact of the default of two large clearing members on the CCP (credit risk) and the consequences of the failure of a custodian (liquidity risk), but again not in the context of cyber risk.[3] To some extent, the stress test framework can also be used to model the impact of a successful cyber-attack on market participants.

The disruption of material infrastructures such as power grids and IT infrastructures (cloud providers or operating systems) could also have a large macroeconomic impact. Recent studies estimate that a disruption of part of the U.S power grid could lead to up to U.S.$1 trillion in losses and a disruption of IT infrastructures up to U.S.$53 bn (Table 1).

2.2 Business disruptions in the financial services sector

DDoS attacks on multiple financial institutions

U.S.: in September 2012, the websites of Bank of America, PNC, JPMorgan, US Bancorp, and Wells Fargo were targeted and one month later the websites of BBT, Capital One, HSBC, Region Financial, and SunTrust were also disrupted.

Czech Republic: on March 6, 2013, the websites of the central bank, three large banks, and the stock exchange were disrupted, with limited damages estimated at U.S.$0.5 mn.

Norway: on July 8, 2014, seven major financial institutions were attacked, leading to disrupted services during the day.

Finland: end of 2014, three banks (Op Pohjola, Danske Bank, and Nordea) suffered DDoS attacks that rendered their online services unavailable and for one bank prevented customers from withdrawing cash and making card payments.

Successful attacks on a financial institution could result in significant disruptions, although to date attacks have not caused large damages, based on publicly available information. A common method to disrupt firm business operations is to launch a "distributed-denial of service" (DDoS) attack on the targeted firms' servers – when a very large number of requests are sent to the targeted servers, overloading the system and making it unable to operate. For example, on August 10 and 11, 2011, the news website of the Hong Kong stock exchange suffered DDoS attacks. The stock exchange had to suspend trading in the shares of seven companies due to make interim results announcements as the result of the attack. No significant damages have been reported so far, as business disruptions were short-lived (from a few hours to a day or two) and only affected part of the banks' business operations (website and sometimes online payments). A recent report by Lloyd's estimates that a disruption of the top cloud provider in the U.S. for three to six days could lead to losses of around U.S.$24 bn [Lloyd's (2018)], with most losses occurring in the manufacturing and trade sectors, while losses for the financial services sector would be limited to U.S.$450 mn.

Cyber-attacks can also be used to undermine customers' confidence in an institution. For example, on June 27, 2014, Bulgaria's largest domestic bank, FIB, experienced a depositor run, amid heightened uncertainty due to the resolution of another bank – following phishing emails indicating that FIB was experiencing a liquidity shortage. Deposits outflows on that day amounted to 10% of the banks' total deposits and the bank had to use a liquidity assistance scheme provided by the authorities.[4]

Cyber-attacks can also target multiple financial institutions to disrupt the financial services sector. Several countries have been exposed to coordinated cyber-attacks on the banking sector using DDoS, although no significant damages have been reported so far (Box 1).

[2] For example, in Switzerland the simulation of the disruption of the two largest participants would result in 50% of unsettled transactions, with contagion effects across banks [Glaser and Haene (2007)].
[3] See ESMA (2018) for details about the methodology and stress test results.
[4] In this case and in the following examples, the information on cyber risk is based on data provided by ORX News sourced from publicly available information.

2.3 Fraud

Cyber-attacks can be used for fraudulent purposes, as evidenced recently by theft using SWIFT (Box 2). Access to confidential information, including clients' credentials used for online payment can be used by cyber criminals. In the ORX dataset, cyber-related fraud accounts for 90% of reported losses.

Emerging technologies, such as fintech, are also particularly exposed to cyber-attacks given their reliance on technology. Technological innovations may increase vulnerabilities to cyber-attacks, as specialized firms might have fewer controls and risk management procedures than large, vertically integrated regulated intermediaries [IMF (2017a)]. Greater use of technology could also expand the range and numbers of entry points into the financial system, which hackers could target. Fintech activities could also increase third-party reliance, where firms outsource activities to a few concentrated providers. In this case, the disruption of a provider could increase systemic risk due to the centrality of the provider in the financial system [FSB (2017)]. Cyber-attacks on fintech firms (mainly online exchanges allowing the trading of bitcoins and providing wallet services) have resulted in at least U.S.$1,450 mn in losses due to fraud since 2013 (Table 3).

The high degree of interconnectedness across firms can lead to rapid contagion effects. For corporates, due to the high interconnectedness across supply chains, a successful attack on part of the network could spread rapidly to other firms. For example, in June 2017, a

Recent cyber-attacks using SWIFT

Over the last three years, at least ten attacks were based on the SWIFT system – a messaging system used by financial institutions for financial transactions. Hackers accessed the victims' SWIFT credentials and sent fraudulent payment orders on behalf of the target (EM banks) to the hackers' bank accounts – in some cases transiting through AE banks and central banks. Initial losses amounted to U.S.$336 mn, while actual losses were around U.S.$87 mn, as some orders were frozen and some money was recouped.

Table 2: Impact of disruption of infrastructures (all sectors)

INSTITUTIONS	DATE	INITIAL LOSSES (U.S.$ MN)	CURRENT ESTIMATED LOSSES* (U.S.$ MN)
BANCO DEL AUSTRO (ECUADOR)	Jan. 2015	12.2	9.4
BANGLADESH CENTRAL BANK	Feb. 2016	81	66
UNION BANK OF INDIA	Jul. 2016	171	0
TP BANK (VIETNAM)	May 2016	1	0
AKBANK (TURKEY)	Dec. 2016	4	4
FAR EASTERN INTERNATIONAL BANK (Taiwan, Province Of China)	Oct. 2017	60	0.5
NIC ASIA BANK (NEPAL)	Oct. 2017	4.4	0.6
GLOBEX (RUSSIA)	Dec. 2017	1	0.1
UNIDENTIFIED BANK (RUSSIA)	Dec. 2017	Unknown	6
CITY UNION BANK (INDIA)	Jan. 2018	2	Unknown

* Current estimated losses are based on publicly available information. Targeted institutions are in the process of recovering the losses through legal proceedings.

Sources: ORX News, Financial Times

Table 3: Cyber-attacks on fintech firms)

INSTITUTION	DATE	ESTIMATED LOSSES (U.S.$ MN)
INPUTS.IO	Oct. 2013	1.3
GBL	Oct. 2013	5
BITCOIN INTERNET PAYMENT SERVICES	Nov. 2013	1
MT GOX	Jan. 2014	470
BITPAY	Dec. 2014	1.9
EGOPAY	Dec. 2014	1.1
BITSTAMP	Jan. 2015	5.3
BITFINEX	May. 2015	0.3
GATECOIN	May 2016	2
DAO SMART CONTRACT	Jun. 2016	50
BITFINEX	Aug. 2016	72.2
COINDASH	Jul. 2017	7
TETHER	Nov. 2017	31
NICEHASH	Dec. 2017	64
COINCHECK	Jan. 2018	534
BITGRAIL	Feb. 2018	170
COINSECURE	Apr. 2018	33

Sources: ORX News, Financial Times

ransomware targeting Ukraine lead to losses of at least U.S.$1.3 bn for multinational firms across sectors (transportation, construction, or food) linked to Ukrainian companies.[5] For financial institutions, a disruption of one large bank, making it unable to process transactions and post margins, could spread quickly to its counterparties and the financial market infrastructures, resulting in heightened liquidity and solvency risk.

[5] This estimate is based on the financial statements of listed firms following the attack. Saint Gobain estimates losses of around U.S.$350 mn in July 2017, A.P. Møller-Mærsk of U.S.$200-300 mn, Merck for U.S.$310 mn, Mondelez for U.S.$100 mn, and Fedex TNT Express for U.S.$300 mn.

2.4 Data breaches

Financial institutions are also particularly vulnerable to data breaches. Given their reliance on customers' data to conduct business, the financial services sector suffered the most incidents with data loss in recent years – including the Equifax data breach where hackers may have stolen personal information of more than 145 million U.S customers. The economic impact of data breaches is hard to assess since indirect effects (loss of clients, reputation risk) are likely to be more material than direct effects (recovery and litigation costs). In the U.S. alone, more than 260 million records were breached due to hacking over the last three years in the financial services sector (Figure 5). The Ponemon Institute estimates that the average cost per stolen record was U.S.$141 in 2017 [Ponemon (2017)]. Applying the Ponemon estimates, losses due to data breach over the last three years would be around U.S.$38 bn for U.S. financial firms alone.

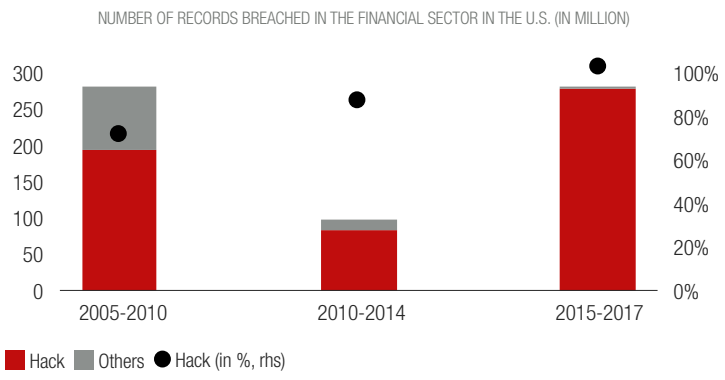
3. POTENTIAL LOSSES FOR FINANCIAL INSTITUTIONS DUE TO CYBER RISK

3.1 Background

Given the high degree of vulnerability of financial institutions to cyber risk, it is crucial for policymakers, risk managers, and executives to have a view of potential losses that financial institutions could face. Unfortunately, providing precise estimates of cyber loss is difficult for a variety of reasons. First, data on cyber-attacks are scarce, as it can take several weeks or months before the targeted institution is aware of the attack. Second, estimating the direct and indirect losses (reputational risk for example) is complicated and subject to uncertainties. Third, there is no common reporting template for cyber-attacks that would allow for a consistent collection of data. Finally, the modeling of cyber risk is still at an early stage.

Existing estimated of cyber losses range from U.S.$100 bn to close to U.S.$600 bn. Symantec (2013) reports an annual cost of cybercrime of U.S.$113 bn, using a survey to measure cyber-attacks and the average cost per attack. Anderson et al. (2013) estimate direct and indirect losses of around U.S.$215 bn using data from 2007-2012 on different types of cybercrime (online banking fraud, tax fraud, etc.), mainly from the U.K. and then extrapolated to the world. McAffee (2014) estimates global costs to be between U.S.$375 bn and U.S.$575 bn. However, most existing studies use very different data source and methodology to estimate losses, some of which are not directly tractable.

Figure 5: Data breaches in the U.S.



Source: Privacy Rights Clearinghouse

3.2 Overview of the model

Recently, I outlined a model that could be used to estimate losses due to cyber risks [Bouveret (2018, 2019)]. I applied an approach commonly used for operational risk assessment for banks, and the pricing for insurance contracts to cyber risk. The method is related to the Advanced Measurement Approach used by banks in the Basel II framework [Shevchenko (2010)]. The method is based on i) the frequency of events, ii) the distribution of losses, and iii) the aggregate distribution of losses, considering the frequency and loss distribution. The intuition is as follows: once we know the frequency of cyber-attacks per year and the distribution of losses due to cyber-attacks, it is possible to estimate the aggregated losses due to cyber-attacks.

The aggregate losses Z due to cyber risk are given by: $Z = X_1 + \cdots + X_N$

where the frequency N is a discrete random variable – the number of cyber-attacks per year – and $X_1, \cdots, X_N$ are positive random severities (losses). The aggregate losses are equal to the sum of individual losses due to cyber risk over the time horizon (one year).

I assume that the frequency of cyber-attacks follows a Poisson distribution, and that losses are independent. Since $X_1, \cdots, X_N$ are independent and identically distributed, and independent of N, the expected aggregated losses E[Z] are given by: $E[Z] = E[N] \times E[X]$

And since N follows a Poisson distribution, then $E[N] = \lambda$, which leads to $E[Z] = \lambda E[X]$

The average aggregate expected losses are entirely determined by the average frequency of cyber-attacks and the average losses per attack.

The next step is to determine the distribution of losses. Based on loss data provided by ORX news, I assume that most losses follow a lognormal distribution and that large losses follow a generalized Pareto distribution typically used to model fat tails (blackout scenarios). Once all the parameters of the models are estimated, I use 1 million Monte Carlo simulations to estimate the aggregate loss distribution [See Bouveret (2019) for technical details]. This amounts to 1 million years of data to ensure that the aggregate distribution cover a wide range of outcomes.

3.3 Results

Once the aggregate distribution of losses is obtained, it is possible to estimate directly the average losses due to cyber risks and compute risk indicators such as the Value-at-Risk (VaR, how much an institution might lose due to a cyber-attack over a given frequency and a given probability (i.e., 95%) and the expected shortfall (ES, average losses above the VaR).

In the baseline case, average losses due to cyber-attacks amount to almost U.S.$100 bn per year and median losses are at around U.S.$88 bn (Table 4). To put those figures in perspective, that would correspond to around 10% of banks' net income in 2016 (based on a sample of 7,947 banks). Those estimates point to sizeable potential aggregated losses in the financial services sector, far above publicly reported losses by financial institutions. However, estimated losses due to cyber risk are a fraction of operational risk losses for banks, which amounted to U.S.$260 bn in 2007 and U.S.$375 bn in 2009 [Hess (2011)].

Table 4: Distribution of aggregate losses

	BASELINE	SEVERE SCENARIO
AVERAGE	100	276
MEDIAN	88	254
95% VAR	167	405
95% ES	283	617
99% VAR	291	637
99% ES	599	1189

Source: Bouveret (2019)

Risk measures such as VaR and ES reflect the heavy tail of cyber losses with a 95% VaR at U.S.$167 bn and an ES at almost U.S.$283 bn in the baseline scenario. Losses would be even larger under the severe scenario, where the frequency of cyber-attacks would increase from around 990 attacks per year (baseline) to close to 2,800 attacks (twice the peak observed in 2013).

The estimated losses are several orders of magnitude higher than what the cyber insurance market can so far cover. The insurance market for cyber risk has grown recently to reach around U.S.$3 bn in premium globally in 2017 and is expected to reach U.S.$12 bn to U.S.$20 bn in the next decade [Fitch Ratings (2017)].

However, most institutions do not have cyber insurance – with take-up rates of less than 30% across sectors – and coverage is limited: the average coverage limit purchased in 2016 was around U.S.$3 mn [CIAB (2016)], which is far below the average and median losses observed in our dataset. Finally, it is challenging for insurers to price cyber risk due to uncertainty about exposures and risks of correlated exposures, as analyzed by Eling and Wirfs (2016) in the context of the insurability of cyber risk.

4. CONCLUSION

Cyber risk is a major concern for financial institutions given the vulnerability of the financial services sector to cyber-attacks. In this article, we have outlined the main transmission channels through which a successful cyber-attack can impact a financial institution, and we also documented some recent cyber-attacks. Finally, we provide a framework that could be used to estimate losses due to cyber risk (and showed that the estimates are far above reported losses by financial institutions). Looking forward, more needs to be done to improve cyber awareness in organizations and improve cyber resilience.

REFERENCES

Anderson, R, C. Barton, R. Böhme. M. J. van Eeten, M. Levi, T. Moore, and S. Savage, 2013, "Measuring the cost of cybercrime," in Böhme, R. (ed.), The economics of information security and privacy, Springer

Bank of England, 2017, "Systemic risk survey results – 2017 H2," November, https://bit.ly/2EX2ET6

Bouveret, A., 2018, "Cyber risk for the financial sector: a framework for quantitative assessment," IMF Working paper No. 18/143

Bouveret, A., 2019, "Estimation of losses due to cyber risk for financial institutions," Journal of Operational Risk, forthcoming

Cebula, J. J., and L. R. Young, 2010, "A taxonomy of operational cybersecurity risks," Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University

Clarke, A., and J. Hancock, 2013, "Payment system design and participant operational disruptions," Journal of Financial Market Infrastructures 2:2, 53-76

Council of Insurance Agents & Brokers, 2016, "Cyber insurance market watch survey: executive summary," Council of Insurance Agents & Brokers, April

Eling, M., and J. H. Wirfs, 2016, "Cyber risk: too big to insure? Risk transfer options for a mercurial risk class," Institute of Insurance Economics, University of St. Gallen

ESMA, 2018, "EU-wide CCP stress test 2017," European Securities and Markets Authority

European Central Bank, 2018a, "Establishment of a euro cyber resilience board for pan-European financial infrastructures," press release, 23 February

European Central Bank, 2018b, "Cyber resilience oversight expectations (CROE) for financial market infrastructures," Public Consultation Document, April

Fitch Ratings, 2017, "Cyber insurance – risks and opportunities," 13 November

FSB, 2017, "Financial stability implications from FinTech," Financial Stability Board June

Glaser, M., and P. Haene, 2007, "Simulation of participant-level operational disruption in Swiss interbank clearing: significant systemic effects and implications of participants' behavior," Payment and settlement simulations seminar, Helsinki, 28 August

Hess, C., 2011, "The impact of the financial crisis on operational risk in the financial services industry: empirical evidence," Journal of Operational Risk 16:4, 364-382

IIF, 2017, "Cybersecurity and financial stability: how cyber-attacks could materially impact the global financial system," Institute of International Finance September.

IMF, 2017a, "Fintech and financial services: initial considerations," Staff Discussion Notes No. 17/05, International Monetary Fund

IMF, 2017b, "Is growth at risk?" Global Financial Stability Report, International Monetary Fund, October

ITU, 2017, "Global cybersecurity index (GCI) 2017," International Telecommunication Unit, July

Kopp, E., L. Kaffenberger, C. Wilson, 2017, "Cyber Risk, Market Failures, and Financial Stability," working paper no. 17/185, International Monetary Fund

Lloyd's, 2015, "Business Blackout," Emerging Risk Report 2015.

Lloyd's, 2017, "Counting the costs – cyber exposure decoded," Emerging Risks Report 2017

Lloyd's, 2018, "Cloud down – impacts on the U.S Economy," Emerging Risks Report 2018

McAffee, 2014, "Net losses: estimating the global costs of cybercrime," Center for Strategic and International Studies, June

OFR, 2017, "Cybersecurity and financial stability: risks and resilience," OFR Viewpoint, Office of Financial Research, February

Ponemon Institute, 2017, "2017 cost of data breach study," June

Shevchenko, P., 2010, "Calculation of aggregate loss distributions," Journal of Operational Risk 5:2, 3-40

Symantec, 2013, "Norton report 2013"

WILL CRYPTOCURRENCIES REGULATORY ARBITRAGE SAVE EUROPE? A CRITICAL COMPARATIVE ASSESSMENT BETWEEN ITALY AND MALTA

DAMIANO DI MAIO | Financial Regulation Lawyer, Nunziante Magrone
ANDREA VIANELLI | Executive Director, Amagis LX and Legal & Compliance Manager, Amagis Capital

ABSTRACT

Since the start of the new millennium, financial markets have been through two major financial crises that have partly been blamed on regulatory shortcomings. In response, European regulatory authorities seem to have overreacted, and ended up limiting the freedom of the financial services industry. An industry-driven reaction to the overregulation has been the evolution of cryptocurrencies, which represent a new and disruptive form of business within the financial markets. Regulators the world over are struggling to determine what legal description crypto assets fall under, and hence how to regulate them. In Europe, where one would expect there to be greater uniformity in terms of how these assets are regulated, we find that there is a patchwork of national regulations that are anything but aligned. In this article, we will focus on the current regulatory framework applicable to crypto assets across the E.U., and in particular on two jurisdictions that have adopted radically different approaches to dealing with crypto assets, namely Italy and Malta.

1. INTRODUCTION

Crypto assets and the provision of certain investment services concerning those assets have been a hot-button topic among supervisors, practitioners, and academics, specifically on whether those assets and the respective services fall within the existing regulatory frameworks. In this article, we will focus on the current regulatory framework applicable to crypto assets across the E.U., and in particular on two jurisdictions that have adopted radically different approaches to dealing with crypto assets, namely Italy and Malta.

Before looking into the particular national regimes of Italy and Malta, however, we will initially assess the approach that ESMA is currently taking vis-à-vis crypto assets and its implications for the potential developments at the E.U. level.

At the national level, Italy's approach to cryptocurrencies regulation is a clear example of fragmentation and incompleteness compared to other European state members. Even though an initial attempt has been made to regulate these assets through level 1 measures (i.e., legislative acts) by the Italian legislators, we must emphasize that there a number of entities and ideas being considered that aim to provide a clear framework for cryptocurrencies in Italy. Indeed, the Italian supervisory authorities[1] and, in specific CONSOB,[2] have undertaken a guiding role in the context of the classification of

cryptocurrencies and their regulatory treatment. In this article, we will provide a brief critical illustration of the Italian approach towards crypto assets and their regime. Starting from a scrutiny of the relevant legal and regulatory frameworks, we will then examine their interpretation and implementation by the Italian supervisory authorities.

> "...the Italian definition of cryptocurrencies is based on the regulations associated with a specific category of providers engaged in exchange services between virtual currencies and fiat currencies."

To place the current Italian regulatory environment vis-à-vis crypto assets in perspective, we felt that it was useful to compare it with another E.U. jurisdiction that has adopted a proactive attitude toward crypto assets, namely Malta. Notably, the Maltese legislator and local regulator introduced a bespoke regime compatible with the E.U. regulatory framework and, in particular, MiFID II. Among the many important steps taken by the Malta Financial Services Authority (MFSA) to regulate this market, the "financial instrument test" represents one of the most innovative.

2. THE E.U. APPROACH

Following the request from the E.U. Commission in its 2018 FinTech Action Plan [EC (2018)], on the 9th of January 2019 the European Securities Market Authority[3] (ESMA) issued an advice, in coordination with a similar initiative from the EBA, to E.U. institutions on initial coin offerings (ICOs) and crypto assets.

Following a prolonged consultation and survey with several National Competent Authorities (NCAs) across 2018 and, in particular, analysis of certain existing cryptocurrencies, ESMA has identified a number of concerns in the current financial regulatory framework regarding crypto assets.

As a preliminary comment, four main macro categories have been identified by ESMA in conjunction with the relevant NCAs, namely (i) investment-type, (ii) utility-type, (iii) payment type, and (iv) hybrid-type crypto assets. The conclusions reached by ESMA with respect to crypto assets differ based on their classification as either (i) financial instruments, as defined under MiFID, or (ii) as those falling outside the perimeters of MiFID II.

Whilst ESMA acknowledges that with respect to the assets that fall within the parameters of MiFID there are areas that require potential interpretation or reconsideration of specific requirements to allow for an effective application of existing regulations, they reckoned that a lack of a clear regulatory framework in respect of "other crypto assets" may expose investors, particularly retail investors, to substantial risks. Among the key risks identified – though financial stability seems not to be a key concern – ESMA lists the risks of fraud, cybersecurity breaches, money laundering, and market manipulation.

Despite ESMAs recommendation that the Anti Money Laundering (AML) framework is applied to all crypto assets and activities involving crypto assets, additional interventions are also required to protect consumers, in particular, the insertion of appropriate risk disclosures in place.

Without delving deep into the definitions and comments by ESMA on blockchain-related concepts and the technicalities applicable to crypto assets, it useful to highlight the fact that while ESMA has acknowledged that member states aim "to bring to the topic both a protective and supportive approach," it has also raised concerns regarding the risks of regulatory arbitrage, which may harm the EU internal market, as a result of the impossibility of providing a level playing field across the E.U. As a result, ESMA has suggested that an EU-wide approach would be more preferable in order to provide homogenous protection for investors across the E.U., given also the peculiar cross-border nature of crypto assets.

[1] Bank of Italy and CONSOB are the Italian authorities that supervise and regulate the Italian banking and financial markets. The Bank of Italy "[a] the national supervisory authority seeks to ensure the sound and prudent management of intermediaries, the overall stability and efficiency of the financial system and compliance with the rules and regulations of those subject to supervision. Also, the Bank of Italy is the designated National Competent Authority (NCA) under the Single Supervisory Mechanism (SSM)" [Bank of Italy (2017)]. "CONSOB is the supervisory authority for the Italian financial products market; its aims are to protect investors and the efficiency, transparency and development of the market."

[2] CONSOB decision n. 20751, December 19, 2018; CONSOB decision 20740, December 12, 2018; CONSOB decision n. 20694, CONSOB decision n. 20695; CONSOB decision n. 20720; CONSOB decision n. 20656; CONSOB decision n. 20660; CONSOB decision n. 20573; CONSOB decision n. 20617; CONSOB decision n. 20593; CONSOB decision n. 2045; CONSOB decision n. 20555; CONSOB decision n. 20509; CONSOB decision n. 20491; CONSOB decision 20461; CONSOB decision n. 20480; CONSOB decision n. 20481; CONSOB decision n. 20461; CONSOB decision n. 20454; CONSOB decision n. 20381; CONSOB decision n. 20336; CONSOB decision n. 19866 February 1, 2017; CONSOB decision n. 20110, September 13, 2017; CONSOB decision n. 20207, December 6, 2017.

[3] According to the ESA's warning, "The VCs currently available are a digital representation of value that is neither issued nor guaranteed by a central bank or public authority and does not have the legal status of currency or money. They are highly risky, generally not backed by any tangible assets and unregulated under EU law, and do not, therefore, offer any legal protection to consumers" [ESA (2018)].

A look at the approaches adopted by two member states that are geographically close but quite different in terms of their attitudes toward crypto assets could offer an interesting overview of how valid ESMA's concerns are.

3. THE RELEVANT ITALIAN LEGAL FRAMEWORK ON CRYPTOCURRENCIES

The Italian legislative decree no. 231/2007, as amended by legislative decree n. 90/2017 of May 25, 2017 (the "Decree 231/2007"), represents a first attempt to provide a primary source of regulation for cryptocurrencies. More precisely, article 1, paragraph 2, letter qq) of the Decree 231/2007 has introduced the definition of virtual currencies as "the digital representation of value, not issued by a central bank or a public authority, not necessarily related to a currency that has legal tender value, used as a medium of exchange for the purchase of goods and services transferred, stored and negotiated electronically."

The definition appears to be consistent with the approach of the European Central Bank (ECB), which attempted to categorize cryptocurrencies in 2012 [ECB (2012)] and 2015 [ECB (2015)], the European Banking Authority[4] (EBA), ESMA, and the European Insurance and Occupational Pensions Authority's[5] definitions. According to the first qualification given by ECB, bitcoins are regarded as a "virtual currency scheme based on a peer-to-peer network. It does not have a central authority in charge of money supply, nor a central clearing house, nor are financial institutions involved in the transactions, since users perform all these tasks themselves. Bitcoins can be spent on both virtual and real goods and services" [ECB (2012)].

In its second report, the ECB stated that virtual currency is "not money or currency from a legal perspective" and has defined it "as a digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money" [ECB (2015)].

Digitization, decentralization, and utilization as a means of exchange: these are the relevant features of the Italian version of cryptocurrencies. However, the qualification of cryptocurrencies is limited to the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

Indeed, the Italian definition of cryptocurrencies is based on the regulations associated with a specific category of providers engaged in exchange services between virtual currencies and fiat currencies.

Pursuant to article 2 paragraph 2, letter ff) of the Decree 231/2007, these providers are defined as any natural or legal person providing on a professional basis, services related to the use, exchange, and storage of virtual currencies, and exchange services between virtual currencies and fiat currencies (VC Exchange Providers, VCEPs). The Decree 231/2007 applies VCEPs. This mean that they must comply with the obligations as set forth in the Decree, namely (i) apply customer due diligence measures; (ii) perform record-keeping measures; and (iii) report suspicious transactions.

In order to perform their activities, VCEPs must notify the Ministry of Finance of their operations in Italy.

Once the Ministry of Finance has received such notification, VCEPs must register[6] in a special section of the register of agents and ombudsmen held by the ombudsmen body (the "Registro tenuto dall'Organismo degli Agenti e dei Mediatori") and supervised by the Ministry of Finance.

According to article 8-ter of the Legislative Decree n. 141/2010, as amended by Legislative Decree n. 90/2017 on May 25, 2017 (the "Decree 141/2010"), the Minister of Finance establishes the methods and timing with which VCEPs are required to communicate to it their activity in Italy.

In this regard, the Minister of Finance issued a public consultation that ended on February 16, 2018. Once the communication sent by the VCEPs is received, the Minister of Finance is obliged to check the correct completion of the form, the validity of the attached documents, and the qualified digital or electronic signature, as well as compliance with the submission deadlines.

[4] According to EBA (2013), "A virtual currency is a form of unregulated digital money that is not issued or guaranteed by a central bank and that can act as means of payment." See also EBA (2014): "VCs are a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to a FC, but is accepted by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically."

[5] Idem.

[6] Article 17-bis of the Legislative Decree n. 141/2010 as amended by Legislative Decree n. 90/2017 of May 25, 2017

Article 5 of the public consultation provides a strict cooperation between the Minister of Finance, the Italian financial enforcement authority (Guardia di Finanza), and the Italian postal police. Such bodies shall exchange information on VCEP applicants in order to carry out investigations to prevent and monitor money laundering and terrorist financing.

VCEPs that are non-compliant are sanctioned with an administrative fine between €2,065 and €10,329 by the Ministry of Economy and Finance. This fine is applicable to any person providing VCEP services without being compliant with article 8-ter of the Decree 141/2010 (i.e., (i) they have not notified the Minister of Finance; or (ii) they are not registered in a special section of the register of agents and ombudsmen held by the ombudsmen body, the "Registro tenuto dall'Organismo degli Agenti e dei Mediatori") [D'Agostino (2018)].

Consequently, the Italian legislator has classified such activity within the regulatory perimeter.

However, so far the Ministry of Finance has not published the final regulation to duly enact the secondary legislation drafted in the public consultation.

In conclusion, we may suggest that Italy is a pioneer in the regulation of virtual currencies in Europe. Indeed, the Decree 231/2007 implemented in advance the provisions as set forth in the Directive 2018/843 of the European Parliament and of the Council of May 30, 2018[7] (the "Fifth Anti Money Laundering Directive"). This notwithstanding, the absence of an effective secondary legislation creates uncertainty within the market of VCEPs that aim to offer their services in Italy. In addition, we may find a hole in the regulation of crypto-to-crypto exchanges that do not fall under the obligations the Decree 231/2007 and Decree 141/2010.

Having provided a strict regulation for crypto-to-fiat exchanges and no regulation for crypto-to-crypto exchanges without a clear rationale for this choice, it appears that inconsistencies are present in the design of the regulations of cryptocurrencies by Italian legislators.

4. CONSOB APPROACH

Moving from the legislative to the regulatory approach (more precisely, the supervisory approach), CONSOB has increasingly focused its attention on cryptocurrencies issued between 2017 and 2019. Indeed, its intervention follows a series of warnings [Bank of Italy (2015, 2018)] issued by the Bank of Italy whereby the Italian central bank illustrates the features and risks of cryptocurrencies.

It is important to point out that the Bank of Italy has stressed that issuing virtual currency and conversion of virtual currencies and fiat currencies may entail a breach of the relevant rules of the Italian Consolidated Banking Act and the Italian Consolidated Financial Act for the provision of reserved activities.[8] Similarly, CONSOB has highlighted the legal risks of cryptocurrencies for consumers.

CONSOB points out[9] that without a legal framework in place it is impossible to implement an effective legal and/or contractual protection of consumers, who can be exposed to economic losses as a result of (i) fraudulent conduct and/or (ii) bankruptcy or disruption of online trading platforms where personal digital portfolios (e-wallets) are stored.

With the absence of a clear legal framework,[10] CONSOB is required to intervene on a case-by-case basis in order to clarify which rules should apply for certain market conducts.

Despite these efforts, leaving the regulation of cryptocurrencies in the hands of national regulators will not help budding entrepreneurs and creates regulatory arbitrage between E.U. members states.[11] In addition, it may impede the creation of a business-friendly environment for financial advisors and consumers willing to invest in cryptocurrencies.

[7] Article 4 of the Fifth Anti Money Laundering Directive provides that "Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with [such] Directive by 10 January 2020."

[8] With regards to the Italian Consolidated Act the relevant provisions are: Article 130 on deposit-taking, Article 131 on banking activity; Article 131-ter TUB on the provision of payment services. With regards to the Italian Consolidated Financial Act, see Article 166 on the provision of investment services. Please note that the breach of these rules is punished with a criminal sanction. For instance, article 166 paragraph 1 of the Italian Consolidated Financial Act provides the "Imprisonment from one to eight years and a fine from Euro four thousand and Euro ten thousand shall be imposed on any person who, without being authorized pursuant to this decree: a) provides investment services or activities or collective asset management services; b) markets units or shares of collective investment undertakings in Italy; c) sells financial product or financial instruments or investment services door-to-door or uses distance marketing techniques to promote or place such instruments and services or activities; and c-bis) carries out data communication services.

[9] CONSOB, "Risks for consumers: virtual currencies and cryptocurrencies," https://bit.ly/2BJNeQ4 (only in Italian).

[10] Or at least a creation of a limited legal framework aiming to regulate crypotcurrencies in connection with anti-money laundering.

[11] ESMA has recently highlighted that a "key consideration of the legal qualification of crypto assets is whether they may qualify as MiFID II financial instruments. (…) There is currently no legal definition of 'crypto assets' in the EU financial securities laws" [ESMA (2019)].

CONSOB has classified cryptocurrencies and their offerings as (i) financial products and (ii) financial products offerings.

While the MiFID II Directive provides a list of financial instruments,[12] the Italian implementation of that Directive has introduced the notion of financial products. According to article 1, paragraph 1 letter u) of the Italian Consolidated Financial Act, financial products shall mean financial instruments and every other form of investment of a financial nature. Consequently, the Italian national implementation of MiFID II has provided a broader qualification of the notion of financial instrument. This approach is the basis of CONSOB's decisions on cryptocurrencies.

CONSOB decision n. 28014/2019 analyzed an offering of a cryptocurrency where the structure of the operation was presented as an investment opportunity. The initiative was promoted in Italian by a company based in Bermuda for the launch of a new digital currency offering users the possibility of purchasing the aforementioned cryptocurrency to receive periodic returns, related to the amount of cryptocurrency, generated through an algorithm, in proportion to the amount of the purchased cryptocurrency.

Pursuant to article article 1, paragraph 1, letter t) of the Consolidated Financial Act, the "public offering of financial products" shall mean "any communication addressed to the public, in whatsoever form and by any means, that presents sufficient information on the conditions of the offering and of the financial products so as to enable an investor to decide to purchase or subscribe such financial products, including the placement through authorised entities."

In this regard, CONSOB is considering that:

- The elements of the public offering that are relevant for the purposes of the aforementioned provisions can be summarized as follows: (i) in circumstances where the activity concerns a specific "financial product," a category which includes – within the meaning of Article 1(1)(u) of the TUF – both the "typical figures" of "financial instruments" and "any other form of investment of a financial nature"; (ii) the existence of communications aimed to purchase or underwrite a specific financial product or products and containing, consequently, at least a representation of the essential characteristics

[12] "Financial instruments" are defined in Article 4(1)(15) of MiFID II as those "instruments specified in Section C of Annex I." These are inter alia "transferable securities," "money market instruments," 'units in collective investment undertakings' and various derivative instruments.

and conditions of the same; (iii) the representation of the offering in uniform and standardized terms and the consequent inability of the individual investor to intervene in the formation of the contractual agreement and the subsequent use of the sum transferred; and (iv) circumstances where the aforementioned offer is addressed to the public resident in Italy.

- The notion of "investment of financial nature" implies that these three elements are present at the same time: (i) an investment of capital; (ii) an expectation of return of a financial nature; and (iii) the assumption of a risk associated with the investment of capital.
- The structure of the operation in question provides that (i) the user uses their own capital for the purchase of the digital currency; (ii) by virtue of the aforementioned purchase, they are promised a predetermined return; and (iii) with the consequent assumption of a risk related to the use of the capital entrusted.

CONSOB noted that: (i) the initiative carried out by the crypto company was promoted in standardized and uniform terms, by means of a proposal containing a representation of the characteristics of the investment plans designed to enable investors to assess whether or not to join the offering; and (ii) there was unequivocal evidence that the offering in question was aimed at the public resident in Italy as the contents published on the website of the crypto company were also available in Italian.

Consequently, forbade the crypto company from making an offering of these types of financial investments to the Italian public.

5. REGULATING CRYPTO ASSETS AND INVESTMENT SERVICES RELATED TO CRYPTO ASSETS: A LEGISLATIVE APPROACH

Following several consultations and feedback from the industry, Malta became the first European jurisdiction to introduce a comprehensive regulatory framework applicable to the provision of blockchain-based financial services in or from within Malta. In this respect, the Maltese parliament published and approved three bills (the "Acts"), which came into force on November 1, 2018. The Acts set out, respectively, (i) the legal framework applicable to "initial virtual financial asset offering" (equivalent to ICOs) and the provision of certain investment services related to virtual financial assets (the "VFA Act"); (ii) the establishment of a Maltese Digital Innovation Authority; and (iii) the recognition and certification of "Innovative Technology Arrangement Services."

A high-level overview of the contents of the aforementioned Acts, with a particular focus on the VFA Act, is provided below.

5.1 The legal regulatory framework applicable to ICOs

The VFA Act regulates the statute of Initial Virtual Financial Asset Offering and the provision of certain investment services with respect to Virtual Financial Assets ("VFA Services"), setting out the framework applicable to service providers, issuers, and, in particular, the entities involved in the provision of the aforementioned VFA Services.

The offer of virtual financial asset (VFAs) to the public in or from within Malta and/or the admission to trading of a virtual financial asset on DLT exchanges fall within the scope of the VFAA. In terms of the VFAA, an ICO process may be broadly summarized as follows.

STEP 1: APPOINTMENT OF VFA AGENT

In terms of the VFAA, the issuer shall appoint an independent regulated entity (VFA Agent) to advise and guide the issuer as to its responsibilities and obligations to ensure compliance with the provisions of the VFAA. The VFA Agent shall act as point of liaison with the MFSA during the pre-ICO stage and shall be subject to several duties and on-going responsibilities, including the submission, on behalf of the issuer, to the MFSA on an annual basis of a certificate of compliance.

STEP 2: FINANCIAL INSTRUMENT TEST (FIT)

The first step consists of an assessment on the nature of the token under issue (using the terminology of the VFAA, a "DLT asset"). The issuer shall, through the appointed VFA Agent, categorize the DLT asset as (i) a financial instrument, (ii) electronic money (subject to the applicable legislation), or (iii) a virtual token (and then unregulated) through the so-called FIT.[13] If the token does not fall within any such categories, it shall classify automatically as VFA and shall fall within the scope of the VFAA. In particular, if the token qualifies as security token (i.e., financial instrument) it shall be subject to the harmonized E.U. securities law, including MiFID and the Prospectus

[13] The Test and its guidance may be accessed at https://bit.ly/2SODfUb.

Directive and its cross-border marketing will be subject to the aforementioned rules.

STEP 3: WHITE PAPER REGISTRATION

In order to conduct an ICO, the issuer shall publicly issue a "white paper" (WP). The WP shall be submitted by the VFA Agent (which is usually in charge of its drafting) to the MFSA ten working days before its circulation to the public and, upon MFSA acceptance, registered on a public register.

5.2 VFA services (including the operation of a VFA exchange, custody of VFA, and reception and transmission of VFA orders)

The scope of the VFA Act is extending to all those services, other than the launch of an ICO, listed under schedule 2 of the VFA Act, and carried out with respect to a VFA (hereinafter "VFA Services"). Indeed, the performance of any of the aforementioned VFA Services shall be subject to a licensing requirement with regards to the terms of Article 13 of the VFAA. In this sense, the entity interested in engaging in any of the aforementioned activities shall submit an application to the MFSA through a duly appointed VFA agent. As part of the application, several documents need to be prepared and submitted to the regulator. Among them, a program of operations setting out the systems, security access protocols, and any other matters as may be required to be set out by the MFSA. Notably, the VFA Agent shall be required to be satisfied that the applicant (including its ultimate beneficial owners and directors) is a fit and proper person to provide the VFA services concerned and will comply with and observe the requirements of the VFA Act.

6. FINAL REMARKS: IS ITALY READY TO COMPETE AGAINST MALTA ON CRYPTOCURRENCIES REGULATION?

DLT-based technologies are reshaping the traditional way of approaching investment products and investment services by both retail and institutional investors. New technologies have made it possible to create new products

to meet investors' demands and offering exposure to a new asset class, while, at the same time, making it easier for unsophisticated parties to have access to very risky and often unregulated products.

These developments have forced financial regulators across the globe, and, in particular, across the E.U., to reassess the current regulatory landscape and create a bespoke regime for crypto assets by means of creating a regulatory system capable of balancing investor protection and financial innovation.

National regulators in Europe are not unified in their assessments of whether crypto assets fall within the existing investment services frameworks. In addition, the one-size-fits-all approach may not be appropriate given the nature of each crypto asset and their continuing evolution.

Given the above, an interesting conundrum deals with the opportunity to adopt a national or supranational approach of dealing with crypto assets. Whilst the Maltese regulatory landscape offers a new and useful framework for facilitating a better understanding of the relations between crypto assets and the existing investment services regulatory framework, other member states, such as Italy, have adopted a different and more reluctant approaches.

Based on the considerations set out above and backing the approach adopted by the ESMA, we strongly support enhanced coordination across the E.U. to avoid a run to the bottom. Indeed, the bespoke national regime already existing in Malta may offer a very interesting starting point.

REFERENCES

Bank of Italy, 2015, "Warning on cryptocurrencies," June 30, https://bit.ly/2JXJh0d (only in Italian)

Bank of Italy, 2017, "Our role," July 30, https://bit.ly/2TY4mbz

Bank of Italy, 2018, "Warning to consumers on virtual currencies by the European Authorities," March 19, https://bit.ly/2SfCONu (only in Italian)

CONSOB, 2018, "Risks for consumers: virtual currencies and cryptocurrencies," Commissione Nazionale per le Società e la Borsa, https://bit.ly/2BJNeQ4

CONSOB decision no. 28014/2019, Commissione Nazionale per le Società e la Borsa

D'Agostino, L. 2018, "Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D. Lgs. 90/2017," Riv. dir. banc., dirittobancario.it, 5, 2018 (only in italian)

EBA, 2013, "Warning to consumers on virtual currencies," European Banking Authority, December 12, https://bit.ly/2Vaenmo

EBA, 2014, "Opinion on Virtual Currencies," European Banking Authority, July 4, https://bit.ly/2HPe8v2

EC, 2018, "FinTech action plan: for a more competitive and innovative European financial sector," European Commission, March, https://bit.ly/2HwsJqv

ECB, 2012, "Virtual currencies schemes," European Central Bank, October, https://bit.ly/23N8vPM

ECB, 2015, "Virtual currencies schemes – a further analysis," European Central Bank, February, https://bit.ly/1Ch16lJ

ESA, 2018 "ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies," European Supervisory Authorities, February 12, https://bit.ly/2Nml5lA

ESMA, 2019, "Advice on initial coin offerings and crypto assets," January 9, https://bit.ly/2CXSjFc

AI AUGMENTATION FOR LARGE-SCALE GLOBAL SYSTEMIC AND CYBER RISK MANAGEMENT PROJECTS: MODEL RISK MANAGEMENT FOR MINIMIZING THE DOWNSIDE RISKS OF AI AND MACHINE LEARNING

YOGESH MALHOTRA | Chief Scientist and Executive Director, Global Risk Management Network, LLC

ABSTRACT

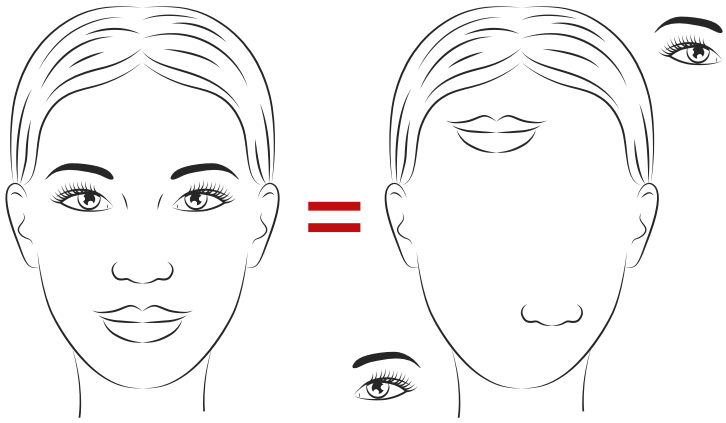
This article discusses how model risk management in operationalizing machine learning (ML) or algorithm deployment can be applied in national systemic and cyber risk management projects such as Project Maven. After an introduction about why model risk management is crucial to robust AI, ML, deep learning (DL), and neural networks (NN) deployment, the article presents a knowledge management framework for model risk management to advance beyond "AI automation" to "AI augmentation."

1. INTRODUCTION: PROJECT MAVEN

Project Maven, also known as "algorithmic warfare cross-functional team" (AWCFT), represents one of the first operational applications of Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), and Neural Networks (NN) technologies in defense intelligence. Its operational focus is on the analysis of full-motion video data from tactical aerial drone platforms, such as the ScanEagle, and medium-altitude platforms, such as the MQ-1C Gray Eagle and the MQ-9 Reaper. As noted by Maven CO, Air Force Lt. Gen. Jack Shanahan, "Maven is designed to be that pilot project, that pathfinder, that spark that kindles the flame front of artificial intelligence across the rest of the Department."

Supported by a budget of U.S.$70 million, Project Maven, executed in collaboration with AI researchers from industry, aimed to achieve the distinction of deploying AI deep neural networks (DNNs) in active combat theater within six months from launch. Given that defense intelligence services are "drowning in data," AI and DL technologies, such as DNNs, provide essential respite by automating tedious work activities, such as counting cars, individuals, and, activities, and typing their counts into PowerPoint files and MS-Excel spreadsheets. The success of the project was bolstered by building partnerships with AI experts in industry and academia and with Department of Defense (DoD) communities of drone sensor analysts.

Figure 1: Limitations in spatial representations of features



Collaboration with top AI talent from outside the defense contracting base facilitated accelerated adoption of commercial AI, ML, and DL technologies. The above project focused on development of agile iterative product prototypes and underlying infrastructures along with ongoing user community testing. In addition, key AI system development activities, such as labeling data, developing AI-computational infrastructure, developing and integrating neural net algorithms, and receiving user feedback, were all executed iteratively and in parallel. AI techniques for imagery analysis are extremely capable, yet developing algorithms for specific applications is not simple. For instance, AI systems require labor-intensive classification and labeling of huge datasets by humans for training of DL algorithms.

> "Machine Learning deals with computer programs that try to learn from experience for prediction, modeling, understanding data, or controlling something."

Maven needed individual labeling of more than 150,000 images for its first training datasets, with plans to have 1 million images labeled by January, 2018. Throughout the DoD, every AI successor to Maven will need a similar strategy for acquiring and labeling a large training dataset.

[1] MIT AI-Machine Learning Executive Guide: including Deep Learning, Natural Language Processing, Autonomous Cars, Robotic Process Automation: https://bit.ly/2PXfIQH, MIT AI-Machine Learning executive education course videos.
[2] Ibid.

Maven's success is clear proof that AI-ML-DL is ready to revolutionize many national security missions. Having met sky-high expectations of the DoD, it is likely to spawn 100 copycat "Mavens" in DoD C4I (Command, Control, Communications, Computers, and Intelligence).

2. ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, DEEP LEARNING AND NEURAL NETWORKS

Project Maven focused on autonomous classification of objects of interest from still or moving images using computer vision enabled by AI, ML, and DL. MIT management scientist Tom Malone defines AI in intuitive terms, such as "machines acting in ways that seem intelligent." MIT computer scientist Patrick Winston notes that: "AI is about the architectures that deploy methods enabled by constraints exposed by representations that support models of thinking, perception, and action."[1] In contrast to general AI, which can solve many different types of problems, as humans do, most AI systems are narrow AI machine-based systems with the capabilities of addressing a specific problem, such as playing Go or chess.

According to MIT computer scientist Tommi Jaakkola, ML deals with computer programs that try to learn from experience for prediction, modeling, understanding data, or controlling something.[2] In the case of Project Maven, such ML is from a training set of labeled examples of images of objects to make future predictions for classifying instances of such objects. As computers process data as bits, images need to be translated into geometrical representations called "feature vectors" composed of such bits. Feature vectors are essentially arrays containing numeric identifiers representing the specific attributes or features of the respective object. The problem is hence translated from a set of images into a set of vectors: a vector being a two-dimensional matrix with only one row but multiple columns of numeric data.

The training set contains a set of labeled vectors and the test set contains a set of images to be classified consisting of unlabeled vectors to match with respective labels. Using vectors and labels, ML algorithm translates the problem into a geometric form wherein each vector represents a point in n-dimensional space. The solution involves developing an ML algorithm to divide n-dimensional space into specific parts, each of which corresponds to a specific label. For image classification, such geometrical

Figure 2: GAN: CNNs see all images on the right as ostriches

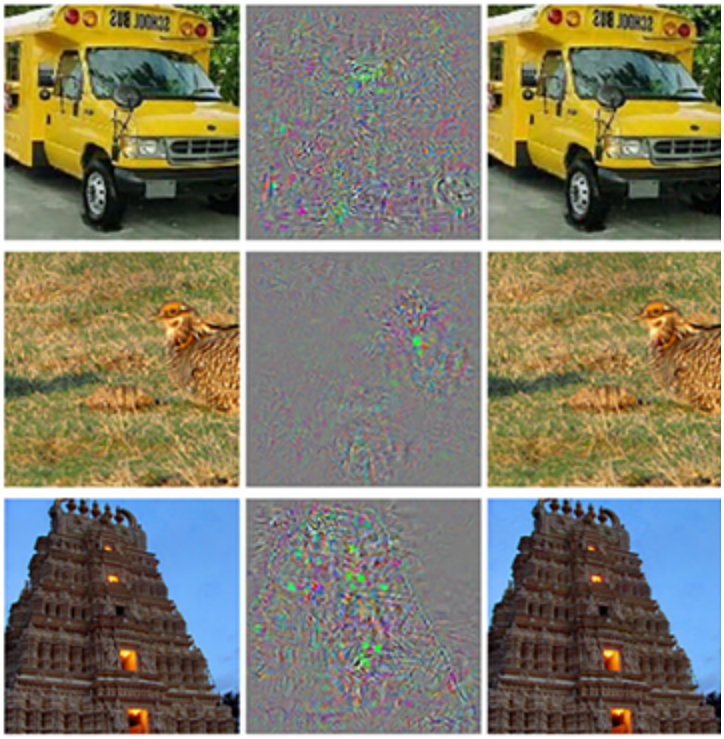
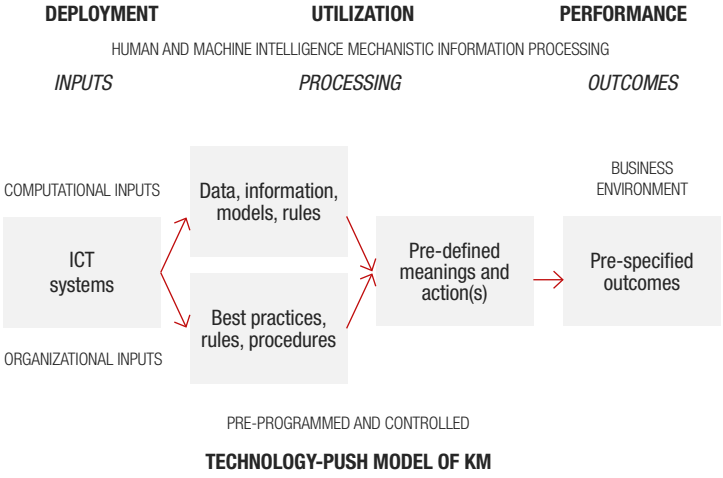


Figure 3: Technology-push inputs driven models: suitable for static and deterministic environmental and operational contexts



transformations use image filters to distinguish between low-level and high-level features such as edges (i.e., boundaries between objects and combinations of edges, curves, parts, and the object).

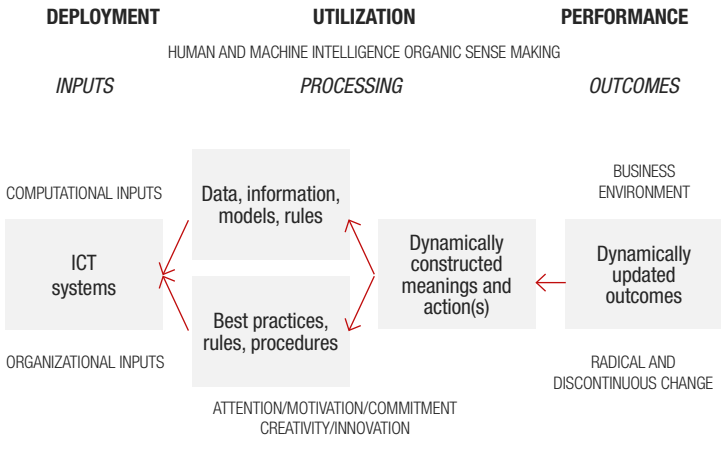
The image signal traverses different transformation layers for processing low- to high-level features with the ML solution being specification of transformation layers and how low-level features are combined. More granular specification and precision is feasible using multiple layers of transformation, with the number of such layers representing the **depth** of the model and the ML problem becoming a **deep** learning problem. Such DL architectures, which are based on fine tuning of millions of parameters across multiple layers of mathematical and geometrical transformations, pose **interpretability** and **trustability** challenges.

Algorithms called neural networks (NNs) are deployed to automate processing of text, voice, and images once they have been trained using millions of example images of such objects. NNs containing multiple transformation layers are called deep neural networks (DNNs). Three general types of DNNs are in common use for text, voice, and image processing. Convolutional neural networks (CNNs) are commonly used for classification of visual images and are an example of feedforward neural networks that have acyclic nodes with all inputs and outputs independent of each other. Recurrent neural networks (RNNs), in contrast, are used for natural language processing (NLP) of sequential information and contain cyclic nodes with outputs being dependent on previous computations. Long short term memory networks (LSTMs) are an extension of the most commonly used type of RNNs that better capture long-term dependencies for sequential information flows given much longer-term memory than vanilla RNNs.

3. WHY MODEL RISK MANAGEMENT IS MOST CRUCIAL TO ROBUST AI-ML-DL USE

As noted earlier, CNNs are commonly used for classification of still or moving images, such as in the case of Project Maven for autonomous classification of objects of interest. Geoff Hinton, a pioneer of CNNs, noted recently that: "I think the way we're doing computer vision is just wrong. It works better than anything else at present but that doesn't mean it's right." Simultaneously, his lecture notes[3] highlight "Why convolutional networks are doomed," observing that: "sub-sampling loses the precise

Figure 4: Strategy-pull outcomes driven models: suitable for complex and uncertain environmental and operational contexts



spatial relationships between higher-level parts such as a nose and a mouth. The precise spatial relationships are needed for identity recognition." (Figure 1)[4]

Mathematically, CNN ignores spatial relationships between the lower-level features such as eyes, nose, and, mouth; hence it computes the above two images in Figure 1 as being equivalent. Computer scientists and neuroscientists also note the challenges of interpretability and trustability that the fallibility of AI, and in particular DL, pose. Patrick Winston of MIT describes advances in AI in the past years as "computational statistics" rather than AI, observing that machines don't have common sense: "The computer that wins at Go is analyzing data for patterns. It has no idea it's playing Go as opposed to golf, or what would happen if more than half of a Go board was pushed beyond the edge of a table..."[5] Tomaso Poggio of the McGovern Institute for Brain Research at MIT, notes that "These systems are pretty dumb. We have not yet solved AI by far. This is not intelligence."[6]

The latest and, deemed greatest, innovation in AI-ML-DL is called Generative Adversarial Network (GAN). GAN is comprised of two nets, the "generator" generates new instances of data and the "discriminator" evaluates them for authenticity. The discriminator, which is a standard CNN, tries to determine whether a specific instance of data belongs to the actual training dataset or not. The generator is like an inverse CNN, which given random numbers generates an image. The goal of the generator is to pass fake images as authentic to the discriminator which then evaluates the images for authenticity based on its ground truth of real images. As seen in Figure 2, ML models are vulnerable to adversarial examples: small changes to images can cause computer vision models to make mistakes such as identifying a school bus as an ostrich. Human eyes cannot discern that images on the right are distorted versions of those on the left; CNN sees the three as ostriches.[7]

4. A KNOWLEDGE MANAGEMENT FRAMEWORK FOR MODEL RISK MANAGEMENT

For static and deterministic environmental and operational contexts, predictive modeling underlying AI-ML-DL is most optimal (Figure 3). Problems are defined in terms of static features (or attributes, characterizing respective objects) and feature vectors (i.e., mathematical arrays containing numeric representations of such features) that can be resolved optimally by pre-programmed and controlled mechanistic human and machine intelligence. As noted earlier, feature vectors are essentially arrays containing numeric identifiers representing the specific attributes or features of the respective object, a vector being a two dimensional matrix with only one row but multiple columns of numeric data.

However, in contexts characterized by complexity and uncertainty, as in Figure 4, predictive analytics based on historical data do not meet the dynamic target given pre-specified outcomes. Hence, anticipation of surprise is needed along with requisite variety to tackle dynamic uncertainty and complexity.[8]

Model risk management (MRM) is needed for environmental and operational contexts that do not match static and deterministic criteria with pre-defined and pre-programmed problems and solutions. MRM is a function of the variance in both inputs and outcomes, as observed in Figures 1 and 2, respectively. Use of any statistical or

[3] Hinton, G., "Taking Inverse graphics seriously," lecture notes, Department of Computer Science, University of Toronto, https://bit.ly/2Ud0KTy
[4] Pechyonkin, M., 2017, "Understanding Hinton's Capsule Networks. Part I: Intuition," Medium, November 2, https://bit.ly/2AcPGg0
[5] Refer to footnote 1
[6] Ibid.
[7] Elsayed, G. F. S. Shankar, B. Cheung, N. Papernot, A. Kurakin, I. Goodfellow, and J. Sohl-Dickstein, 2018, "Adversarial examples that fool both computer vision and time-limited humans," Cornell University, May 22, https://bit.ly/2U9LITF
[8] Malhotra, Y., 2005, "Integrating knowledge management technologies in organizational business processes: getting real time enterprises to deliver real business performance," Journal of Knowledge Management 9:1, 7-28

mathematical model entails model risk since the specific results are not measured but estimated using the specific statistical and mathematical models. An important insight from model risk management research and practices is that there is unlikely to be any perfect model (all models are wrong), and the best results can be obtained from combining the results from models based on different inputs (some models are useful) – "All models are wrong, but some are useful" – George E. P. Box. Hence, instead of relying on any one specific quantitative model, using a range of different plausible quantitative models, which can be robustly discriminated from one another, is a recommended strategy for minimizing the model risk. When results from multiple models are combined, analogous to the use of "ensemble models" such as in ensemble learning, the variance in the range of estimates across the respective models provides a succinct measure of model risk. The papers and presentations downloadable from the author's SSRN page (https://papers.ssrn.com/author_id=2338267) discuss multiple specific examples of model risk management in the context of complex systems, spanning quantitative finance and hedge fund trading systems and cyber risk insurance systems to AI-ML-DL-GAN applications in Space and Defense projects such as Project Maven. One example is the recent invited presentation to the CFA Society on Hedge Fund Chief Investment Officer Practices on using Auto-Machine Learning (Auto-ML) for Model Risk Management (https://bit.ly/2tlg3b7). The current article spans the focus from Cybersecurity, Finance, and, Insurance to broader applications of AI-ML-DL-GANs in the Defense & Space risk management contexts, such as the Project Maven.

> "In dynamic, complex, and uncertain environments, anticipation of surprise is more important than predictive analytics based on historical data as the past may not be the best predictor of the future."

Specific examples will include multiple variations of the CNNs and related models being used to address the limitations of any one given model. Furthermore, the capsule networks (CapNets), which are proposed as a solution for ameliorating many of the limitations of CNNs noted earlier, provide additional diversity in terms of different plausible models that can be robustly discriminated between. Broadening the range of estimates based upon diverse models provides a better assessment of risk in terms of variance.

5. CONCLUSION: BEYOND "AI AUTOMATION" TO "AI AUGMENTATION"

As illustrated in the case of GANs, small changes to images not discernible to humans can cause computer vision models to make mistakes, such as seeing a school bus as an ostrich. While it is easy for humans to see a bus as a bus, it is hard for AI-ML algorithms to do so. Many simple tasks that anyone can do, like recognizing objects or picking them up, are much harder for AI-ML-DL as a recent report by the consulting firm Deloitte notes.[9] On the other hand, many of the issues related to algorithmic bias may be traced back to bias in training data or the design of algorithms and models. The same report notes that "AI algorithms must be complemented by human judgment."

Remarking on the certainty of knowledge, Morris Kline had noted: "Insofar as certainty of knowledge is concerned, mathematics serves as an ideal, an ideal toward we shall strive, even though it may be one that we shall never attain. Certainty may be no more than a phantom constantly pursued and interminably elusive."[10] Emanuel Derman observed: "Models are at bottom tools for approximate thinking. The most important question about any model is how wrong it is likely to be, and how useful it is despite its assumptions. You must start with the model and overlay them with common sense and experience."[11]

There is no right model as the world changes in response to the ones we use. In addition, changing environmental and operational contexts make newer models necessary. Hence, knowing and applying the leading-edge developments in AI-ML-DL-GAN models is important for ensuring systemic and cyber risk management progress and growth aligned with world developments. It is, however, equally important to know the limits and boundaries of the models and related assumptions and logic by deploying "audacious imagination, insight, and creative ability"[12] as noted by the mathematician Morris Kline.

[9] Guszcza, J., H. Lewis, and P. Evans-Greenwood, 2017, "Cognitive collaboration: why humans and computers think better together," Deloitte Insights, January 23, https://bit.ly/2wetBzl
[10] Kline, M., 1980, Mathematics: the loss of certainty, OUP
[11] Derman, E., 1996, "Model risk," Goldman Sachs Quantitative Strategies Research Notes
[12] Refer to Footnote 10

ALTERNATIVE MARKETS

U.S. LAW: CRYPTO IS MONEY, PROPERTY, A COMMODITY, AND A SECURITY, ALL AT THE SAME TIME

CAROL R. GOFORTH | Clayton N. Little Professor of Law, University of Arkansas

ABSTRACT

The first crypto assets were all designed as replacements for fiat currency, and as such the label "cryptocurrency" made sense. That singular word accurately described bitcoin and all of the early altcoins. However, as innovators have developed additional functionality for crypto, it no longer makes sense to assume that all crypto are the same. Nonetheless, regulatory authorities in the U.S. continue to lump them together. That does not, however, mean that the various agencies are in agreement about how to classify crypto. In an effort to fit crypto assets into existing regulations, crypto in the U.S. is being simultaneously treated as money, as property, as a commodity, and as a security. This has led to conflicting and overlapping regulations, which are not likely to be harmonized unless and until regulators accept that not all crypto are the same, and that they should not all be regulated monolithically.

1. INTRODUCTION

Persons familiar with bitcoin and blockchain are generally well aware that there has been a remarkable proliferation of cryptocoins and tokens (sometimes just called "crypto") in the past few years. Sources such as CoinMarketCap list more than 2000 different active coins and tokens. While some of the coins in particular have clearly been designed to serve solely or predominantly as replacements for traditional, fiat currencies (led, of course, by bitcoin), many coins and tokens have been designed with additional functionality in mind. Ether, for example, fuels the Ethereum network, a platform on which most tokens are hosted. XRP is utilized by Ripple to facilitate cross-border financial transactions by banks and payment providers.

Despite the fact that many of these assets have utility other than simply serving as a replacement for fiat currency, U.S. regulators tend to lump crypto assets into a single category. That reaction has undoubtedly been encouraged by the fact that "cryptocurrency" is a term widely used to cover the universe of crypto, regardless of the nature of any particular coin or token. It may, therefore, be unsurprising that regulatory authorities also tend to treat all crypto alike, regarding it all as "virtual currency."

2. WHAT IS CRYPTO ANYWAY?

Originally, a regulatory approach that treated all crypto as a currency substitute may have made sense. The mysterious Satoshi Nakamoto's innovative whitepaper on bitcoin specifically talked about the need to replace traditional payment systems, and, of course, "bitcoin" includes the word "coin." In addition, bitcoin's closest and earliest progeny were all altcoins specifically designed to supplant fiat currencies, albeit with different attributes that each developer suggested made that coin a superior option. Given this history, and the perceived need for regulators to step in quickly to resolve problems and

abuses that were proliferating in the system, it might have been predictable that the word "cryptocurrency" would be used to talk about all such assets and that all crypto would be regulated in a similarly monolithic way.

This approach is now subject to criticism, particularly in the regulatory sphere, because not all currently-available coins and tokens are intended to or indeed actually do act like traditional currency. Currency generally serves exclusively as a medium of exchange, a store of value, and/or unit of account. One might, therefore, expect that coins and tokens would be regarded as "virtual" currencies when they are intended to act like traditional currency, serving only as a medium of exchange, a store of value, or a unit of account, while lacking intrinsic value or external utility, but this is not the case.

The problem of how crypto assets are understood goes beyond having a somewhat misleading label, because this unitary approach has lead most enforcement agencies in the U.S. to treat crypto as if it were all the same. Thus, if a regulatory agency treats some crypto as currency, it tends to treat all crypto that way. The same phenomenon exists for when it is classified as property, a commodity, and even as a security. Because different agencies in the U.S. have different regulatory powers and responsibilities, each tend to classify the very same assets differently in order to assert jurisdiction. Combined with the tendency to treat all crypto alike, and faced with the reality that there are bad actors in the space, the U.S. is now faced with a mix of overlapping, confusing, and extremely complicated regulations with which developers, issuers, and persons who facilitate the buying and selling of crypto must all comply. Sometimes even purchasers of crypto are affected.

2.1 FinCEN (and state banking authorities): Crypto is currency

One of the earliest U.S. regulators of crypto was the Department of Treasury, acting through FinCEN (the Financial Crimes Enforcement Network). FinCEN's mission pursuant to the Bank Secrecy Act (BSA) is focused on regulating the flow of money so that it is not used to fund illegal operations, such as terrorism, and cannot be funneled out of illegal operations through laundering schemes. It does this in part by subjecting "financial institutions" to a wide range of monitoring, record-keeping, and reporting obligations. Broker-dealers who might facilitate similarly illegal activities through transactions involving securities are also regulated.

Given the obvious importance of this mission, it is not surprising that when early cryptocurrencies were used to fund illegal operations on the so-called dark web, Treasury and FinCEN wanted crypto to be treated as virtual "money," making persons and businesses involved in selling and exchanging it subject to FinCEN jurisdiction. In early 2013, FinCEN issued guidance that defined virtual currency as any "medium of exchange" lacking legal tender status, which "either has an equivalent value in real currency, or acts as a substitute for real currency."[1] Any intermediary facilitating the use of any such virtual currency, therefore, became a "money transmitter," required to report to FinCEN, subject to inspection by it, and required to comply with the Anti-Money Laundering (AML) and Know-Your-Customer (KYC) requirements of the BSA.

Even given that there are legitimate public policy reasons for FinCEN to oversee such businesses, it should at least be recognized that FinCEN utilized a very broad definition of virtual currency in order to accomplish its objectives. Like any other property, crypto is always likely to have a value in "real" currency (regardless of whether it was designed to act as a substitute for fiat), and most coins or tokens can serve as a medium of exchange regardless of the developer's intentions, any utility that the assets might possess, or how they are marketed and to whom. While traditional currencies have no purpose other than acting as a medium of exchange, store of value, or unit of account, this limitation is not included in the FinCEN definition of virtual currency, which, therefore, serves to expand FinCEN's jurisdiction and the reach of any other agency using this definition. In other words, the FinCEN definition potentially makes issuers of crypto assets that were never designed or intended to act as a currency subject to rules that were specifically designed for persons engaged in the business of transmitting and exchanging money rather than other kinds of assets.

In addition to this federal regulation, there are state banking authorities to consider. To date, these state agencies have tended to use the same definitions as those employed by FinCEN, treating all crypto as virtual currency. For example, the Conference of State Bank Supervisors (CSBS) defines virtual currency as "a digital representation of value used as a medium of exchange,

[1] FinCEN, 2013, "Application of FinCEN's regulations to persons administering, exchanging, or using virtual currencies," FINA-2013-G001, March 18, https://bit.ly/2le57iz archived at https://bit.ly/2teTomF

a unit of account, or a store of value" that lacks legal tender status.[2] A proposed uniform act designed to help states decide when state money transmitter laws should apply to businesses involved with virtual currencies, first published by the Uniform Law Commission in 2017, also defines "virtual currency" as "a digital representation of value that: (i) is used as a medium of exchange, unit of account, or store of value; and (ii) is not legal tender…"[3] It offers a relatively burdensome set of regulations for such money transmitter businesses, but as of February, 2019, the Uniform Act had not been adopted by any American jurisdiction.

In fact, state money transmitter laws apply very differently depending on the jurisdiction in question. More than a dozen states require such businesses to either obtain a money transmitter license or some other form of authorization. New York, for example, requires a BitLicense in order for a business to operate as a cryptocurrency exchange. At the other end of the spectrum, at least ten states have decided either that no license is required or that none is required unless a "sovereign" currency is involved. Somewhere in the middle, almost half of all American states are either silent or are still undecided about how to treat crypto.

One problem with this state regulatory approach is that few money transmitter businesses involved with crypto are likely to be doing business in only a single state. Crypto is inherently an online business, where customers may come from all over. A business that interacts with customers from multiple states may well have to comply with federal banking requirements and then a mix of inconsistent (but often extensive and burdensome) state money transmitter requirements as well. And because all crypto are regarded as currency, these rules apply to every issuer of coins or tokens that have value, and potentially every person facilitating the exchange of such assets.

2.2 I.R.S.: Crypto is property, mostly

Another early actor in the U.S. was the I.R.S., which adopted a similarly broad definition of "virtual currency" in 2014. This early "guidance" from the I.R.S. focused on explaining "how existing general tax principles apply to transactions using virtual currency," and to that end, the I.R.S. defined virtual currency as "a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value."[4] This definition sweeps virtually all crypto within its scope, because once a crypto asset has any value in "real" currency (or if it is intended to act as a substitute for fiat), there is realistically no way that it can avoid being a medium of exchange, a unit of account, or a store of value in addition to whatever else it might be. This broad definition, applied across the board to all coins and tokens, allows for no difference in treatment based on the intended function of the asset, or how it is marketed or exchanged.

While agreeing that essentially all crypto should be treated alike, the I.R.S. elected not to classify it as "currency" under the Tax Code, deciding it was property instead of currency (as FinCEN had previously declared). This is a difference with important consequences. By classifying crypto as property, taxpayers are precluded from using cryptocurrencies to generate foreign currency gain or loss for U.S. federal income tax purposes. In addition, the I.R.S. has made persons involved in crypto transactions subject to the same record-keeping and reporting requirements as those involved in stock trading. Moreover, after December 31, 2017, it is clear that this kind of property is not eligible for the so-called "like-kind" exception that some investors had previously relied upon, meaning that profits and losses on any swap of one form of crypto for another, or even any sale and repurchase of the same kind of coin or token, must be reported and will be subject to tax.

Despite its general statement and approach, the I.R.S. has not been entirely consistent in treating crypto as property. In 2016, the I.R.S. had the Department of Justice issue a summons seeking to force Coinbase, Inc. to identify U.S. customers who had traded in convertible cryptocurrencies in the prior three years in order to combat systemic under-reporting of crypto transactions. In essence, in this context, the I.R.S. elected to treat Coinbase as a financial institution, with the currency at issue being the crypto assets which its customers were trading.

In addition to this kind of inconsistency, there are also some open issues with regards to how crypto should be treated for tax purposes. One prevalent question is whether crypto is ordinary property or a capital asset in the hands of an owner. The answer to this question determines whether a sale of the asset produces ordinary or capital gains and losses, and the I.R.S. has essentially

[2] CSBS, 2015, "State regulatory requirements for virtual currency activities," CSBS Model Regulatory Framework, September 15, https://bit.ly/2BkDGdT archived at https://bit.ly/2SavhV2

[3] ULC, 2017, Uniform Regulation of Virtual Currency Businesses Act § 102(23), first published October 9, https://bit.ly/2QiRCi0 archived at https://bit.ly/2TsfkWJ

[4] IRS Virtual Currency Guidance, 2014, I.R.S. Notice 2014-21, 2014-16 I.R.B. 938, released March 26; published April 14, https://bit.ly/2MODJmH archived at https://bit.ly/2GoPwHp

said that it depends. The I.R.S.' guidance on this point simply notes that stocks, bonds, and other investment property are generally treated as capital assets, while inventory and property held mainly for sale are not. This means each individual taxpayer will need to make an independent determination of how to characterize any virtual currencies that it owns when it sells or exchanges the asset.

There are also open tax issues arising out of particular events relating to virtual currencies. For example, all American taxpayers who owned bitcoin prior to July, 2017 received what is known as an "airdrop" when a group of miners introduced a fork and created Bitcoin Cash. This resulted in bitcoin owners receiving one unit of Bitcoin Cash for every bitcoin owned. It is, however, unclear if the I.R.S. expects to treat this transaction like a dividend, on which tax would be owed immediately, or if recipients are required to report gain and pay tax only when the Bitcoin Cash is sold.

> "...even when every agency agrees independently that it is important not to stifle innovation in the space, if multiple authorities regulate and have enforcement powers over the same asset and same transactions, the total regulatory burden can easily become excessive."

None of this, however, takes away from the general I.R.S. conclusion that crypto is property for purposes of the federal income tax code. This is, of course, only the story at the federal level, since most states also impose their own level of taxes.

Many states are silent on the taxation of crypto assets, leaving open the question of how the interests or transactions involving them will be taxed at the state level. With regards to state income tax, there are some states that have specifically adopted the federal approach and a few that have expressly rejected it. Most states are silent or are studying the issue. State tax issues can also include sales tax as well as income tax, and states are not at all consistent in their approach to that kind of taxation either. Specifically, with regard to sales tax, most states have yet to act, although a few have said that transactions in any virtual currency are subject to such taxes while some have concluded that they are not. Among the states that do apply sales tax, the question of how to calculate the tax (based either on the value of the crypto or the value of the other property) is also handled inconsistently. A few advisors have gone so far as to recommend that persons owning large amounts of crypto relocate to a tax-friendly jurisdiction before selling or exchanging the interest.

2.3 CFTC: All crypto is a commodity

The Commodity Futures Trading Commission (CFTC) also traces its involvement in the regulation of virtual currencies back to 2014, and its definitions are consistent with those used by FinCEN and the I.R.S. On the other hand, its conclusion as to the result of that definition is not.

The CFTC released a "Primer" on virtual currencies in 2017, which explicitly relies on the I.R.S. approach to define virtual currency as "a medium of exchange, a unit of account, and/or a store of value" that acts like a "real" currency while lacking "legal tender status."[5] If a coin or token fits within this broad definition of virtual currency, the CFTC takes the position that it is a commodity. This does not appear consistent with the previously discussed FinCEN position (which would subject businesses involved in the exchange of crypto assets to regulation as money transmitters), given that in 2008 FinCEN concluded that brokers and dealers in commodities regulated by the CFTC would generally not be money transmitters.

It is, however, fairly obvious why the CFTC believes that it needs to be active in the space. The CFTC is particularly concerned with fraud and manipulation in the markets that it oversees, including not only futures and derivative markets but also spot markets for commodities. The prevalence of fraudulent trading activities helps explain the breadth of the CFTC's definition and its approach to what it claims within its jurisdiction. This approach does not take into account any differences in the varied coins and tokens available today, but it does mean that the CFTC has both regulatory oversight and enforcement authority over any futures contract or derivative involving virtual currencies. On the other hand, consistent with its Congressional mandate, the CFTC has only enforcement power when it comes to direct trades in a virtual currency and lacks the ability to regulate by setting standards for spot trading in crypto.

[5] LabCFTC, 2017, "A CFTC primer on virtual currencies," U.S. CFTC, October 17, https://bit.ly/2DaEHW2 archived at https://bit.ly/2RC2PpX

2.4 The SEC: Crypto is a security, usually

The Securities Exchange Commission (SEC) is the final major player at the federal level in the U.S. when it comes to regulating crypto. The SEC has been very active because of a pervasive concern that unsophisticated investors have been preyed upon by unscrupulous issuers and third parties. In a 2017 Investor Bulletin warning the public about the risks of participating in Initial Coin Offerings (ICOs), the SEC specifically adopted the prevailing definition of virtual currency, agreeing that it is "a digital representation of value that can be digitally traded and functions as a medium of exchange, unit of account, or store of value."[6] On the other hand, the same bulletin noted that "[v]irtual tokens or coins may represent other rights as well." The SEC, therefore, does not claim to regulate based on whether or not a particular interest is properly regarded as a virtual currency, and instead looks at whether the asset is being sold as an investment contract.

That approach is known as the Howey test in reference to the U.S. Supreme Court case [SEC v. Howey Co., 328 U.S. 293 (1946)] that set out the elements of an investment contract. This test considers the following: (1) is there an investment, (2) of money or something of value, (3) in a common enterprise, (4) where the investor expects profits, (5) based primarily on the entrepreneurial efforts of others? If the answer to all these questions is yes, then the interest is a security. Not surprisingly, the SEC has concluded that new issues of coins or tokens will almost certainly involve the sale of securities.

On the other hand, under this approach, some virtual currencies will not be regulated as securities. The SEC has now decided that the two most heavily capitalized crypto assets, bitcoin and ether, are not securities, based not on how the assets or their developers behaved when both were first introduced, but on where the markets are today. Ownership of bitcoin and ether is so widely dispersed that the market determines profitability, rather than there being any particular third party upon whom an investor would be relying to create value. Thus, these interests are not currently regulated by the SEC as securities.

In addition to the SEC, which regulates securities at the federal level, sales of crypto may also be regulated by state securities authorities. For example, as of mid-2018, a number of jurisdictions had initiated enforcement proceedings against allegedly fraudulent ICOs under state law, including Texas, Massachusetts, New Jersey, and North Carolina. While many states rely

[6] SEC, 2017, "Investor bulletin: Initial Coin Offerings," July 25, https://bit.ly/2v5xHDZ archived at https://bit.ly/2RC3Pud

on the Howey investment contract test to determine when various interests are securities, other states have declined to follow this federal approach, often relying on a "risk capital" test instead. This test asks whether (1) the offeree furnished value to the offeror, (2) at least some of the value is subject to the risks of the enterprise, (3) this was induced by representations that gave rise to a reasonable understanding by the offeree that a valuable benefit over the initial value would be returned to the offeree as a result of the operation of the enterprise, and (4) the offeree has any right to exercise practical and actual control over the management of the enterprise. Because compliance with federal law does not automatically insure compliance with state requirements, this can produce conflicting requirements on developers and sellers of crypto. (Similarly, compliance with the state requirements is irrelevant to the question of whether the SEC requirements have been met.)

At the other end of the spectrum, Wyoming was the first state to expressly exempt so-called "utility tokens"[7] from the state securities laws so long as the developer or seller files a notice of intent with the secretary of state; the purpose of the token is for consumption and shall be exchangeable for goods, services, or content; and the developer or seller did not sell the token to the initial buyer as a financial investment. Compliance with the Wyoming statute does not affect federal requirements.

2.5 Other agencies

The previous sections of this article deal with those federal agencies having the largest roles in regulating crypto in the U.S., but other federal agencies can also become involved in particular instances. For example, the Federal Trade Commission has halted specific activities that have amounted to deceptive advertising involving crypto assets. In fact, in recognition of the reality that crypto can be used by persons intending to defraud the public, the FTC has an active Blockchain Working Group.

Similarly, the Department of Justice (DoJ) (acting through various U.S. Attorneys General) becomes involved when it comes to pursuing potential criminal liability. The DoJ investigates and litigates on behalf of the U.S. and has done so in the context of enforcement actions in coordination with various federal agencies. The DoJ does not promulgate regulations, but when intentional violations amount to crimes under other regulatory regimes, the DoJ prosecutes actions on behalf of the U.S. It does not, however, adopt its own definitions of crypto or virtual currencies, and it does not impose requirements in addition to those overseen by other federal agencies.

Criminal violations of state laws can and have resulted in similar enforcement actions at the state level, and as mentioned earlier, various state agencies are also active in regulating crypto asset transactions.

3. WHY CLASSIFICATION MATTERS

Under current law, crypto assets (and especially any newer coins or tokens) are likely to be simultaneously treated as currency by FinCEN, property by the I.R.S., commodities by the CFTC, and securities by the SEC. Not only is crypto itself classified differently by each of these agencies, but transactions involving these assets are likely to be subject to multiple regulatory requirements that do not always align. One of the biggest problems is that even when every agency agrees independently that it is important not to stifle innovation in the space, if multiple authorities regulate and have enforcement powers over the same asset and same transactions, the total regulatory burden can easily become excessive.

Most regulators in the U.S. agree that blockchain and many of its developments are important and potentially revolutionary, and that technological improvements in the space are highly desirable. J. Christopher Giancarlo, the Chairman of the CFTC, for example, has cautioned legislators about the need for a "proper balance of sound policy, regulatory oversight and private sector innovation," in order to insure the growth of "new technologies [that] will allow American markets to evolve in responsible ways and continue to grow our economy and increase prosperity."[8] The SEC Chairman has also commented on the need to balance legitimate industry needs with appropriate and efficient regulation while avoiding over-regulation.

It is, however, far from clear that this nuanced balancing of regulations and the need of industry to be free to innovate is actually happening. Consider, for example, the regulations imposed by the SEC upon the sale of any crypto asset that it characterizes as a security. The SEC requires any such coin or token to be either registered or exempt from registration before it can be sold. In either

[7] There is no indication that Wyoming intends this to apply only to technical tokens, so a crypto asset operating on its own blockchain could also fit this definition, providing it has a viable function.

[8] U.S. CFTC, 2018, Speeches & Testimony, Written Testimony of Chairman J. Christopher Giancarlo before the Senate Banking Committee, February 6, https://bit.ly/2D8TAID archived at https://bit.ly/2BjRVQq

case, there are substantial anti-fraud requirements in place to protect potential investors, and the SEC is used to policing fraud in the securities markets, either alone in civil actions or together with the DoJ in the case of criminal violations. Registration with the SEC requires incredibly detailed disclosures formatted in very specific ways, and most exemptions under the securities laws are also designed to ensure that investors have access to material information before making a purchase. It would seem that very little is gained by having additional agencies require similar information in different formats, and it does not seem necessary to have the same kinds of fraud policed by other agencies such as the CFTC (which claims jurisdiction over fraud and manipulation in spot markets involving any commodity, including all crypto).

In point of fact, even when the regulations of a single agency are examined, the risk of bad actors has obviously weighed very heavily in various administrative decisions. Consider the SEC's reaction to various requests to approve exchange traded funds (ETFs) that would deal in bitcoin. An ETF is essentially an investment vehicle that would allow investors to buy a "basket of securities" through a brokerage firm on a stock exchange. Multiple observers have concluded that a crypto ETF is "crucial to bringing legitimacy to crypto trading."[9] Unfortunately for investors, the SEC has so far declined to approve any such ETF, rejecting several applications for bitcoin ETFs to date. Its stated rationale has been that the proposals created too much of a risk of "market manipulation and fraud."[10]

This may be a reasonable conclusion when viewed from the perspective of the particular proposals that the SEC was evaluating, but the result is a potentially significant limitation on the viability and success of crypto-based operations in the U.S. To the extent that innovation in the space is desirable, this consideration appears to have been less important than avoiding the risk of bad behavior. Perhaps this too is understandable in light of the heavy burdens generally placed on ETFs. ETFs are regulated under both the Securities Act of 1933 and the Securities Exchange Act of 1934 as well as the Investment Company Act of 1940, making them one of "the most stringently regulated investment products available in the United States."[11] If, however, the existence of a viable ETF trading platform is indeed important for the long term viability of crypto, the unwillingness of the SEC to approve any of the options presented to it is troublesome. Certainly, the bitcoin market has been depressed since the SEC's decisions to reject so many ETF applications (although other factors may account for the relatively low trading value).

On the flip-side of over-regulation, the existing overlap of authority and jurisdiction of various regulatory authorities also means that certain kinds of issues or transactions can fall in the cracks where no agency has clear jurisdiction. Consider what happens when the SEC determines that some kinds of crypto are not securities, which is exactly what has happened with regard to bitcoin and ether. Clearly, the markets for these interests require some oversight and ideally prospective regulation as well, because of the continuing risk of fraudulent and manipulative behavior.

In cases such as this, the CFTC might appear to be the logical choice, since both bitcoin and ether are regarded as commodities by the agency. However, it is clear that under the current statutory mandates, the CFTC lacks authority to regulate spot markets and transactions not involving a futures sale of any virtual currency (or other commodity). According to testimony from the Chairman of the CFTC before the Senate Banking Committee in early 2018, "the CFTC does not have authority to conduct regulatory oversight … including imposing registration requirements, surveillance and monitoring, transaction reporting, compliance with personnel conduct standards, customer education, capital adequacy, trading system safeguards, cybersecurity examinations, or other requirements."[12] The availability of after-the-fact enforcement power in the event of fraud and manipulation seems inadequate in light of the established fact that such events have occurred in the past, and appear likely to happen in the future.

[9] For example, see Roberts, D., 2018, "Amid 2018 crypto crash, 3 kinds of believers come into focus," Yahoo Finance, September 8, https://yhoo.it/2048zaX archived at https://bit.ly/2Bf6NPV

[10] Young, J., 2018, "Why did the SEC reject all derivative-backed bitcoin ETFs?" CCN, August 23, https://bit.ly/2WlxZQ9 archived at https://bit.ly/2UHGKYK

[11] Vanguard, "Who regulates ETFs," https://vgi.vg/2SsBvyH archived at https://bit.ly/2GcqmfT

[12] Written testimony of Chairman Giancarlo, cited at note 8 above.

4. WHERE MIGHT THE U.S. GO FROM HERE?

Most countries do not have the range of overlapping regulatory authorities that exist in the U.S., but realistically it seems unlikely that the U.S. will choose to do away with any of the agencies in question or to remove crypto from the jurisdiction of any existing agency in order to consolidate oversight power. Certainly, prior attempts to consolidate functions of the CFTC and SEC have not progressed very far. Legislators and regulators alike have specifically recognized that existing authorities have differing areas of expertise. Courts have approved of the concurrent jurisdiction that currently exists, as (for example) between the CFTC and SEC in the case of crypto assets. It would, therefore, make sense, when these agencies meet and when Congress determines that it is appropriate or necessary to exercise additional oversight, that a more concerted effort is made to coordinate enforcement and regulatory oversight. This is likely to require a more nuanced approach, where cryptos are not all treated as being alike, and where the specific expertise of each agency is highlighted and respected.

> "To avoid the problems of over-regulation, agencies will need to accept a change in perspective. This requires a paradigm shift that moves away from treating crypto as a single kind of asset, when in reality they are not."

For example, the reality is that not all crypto is intended to function as a currency, and it probably should not be regarded as such. Some crypto is clearly being designed to function as a substitute for traditional investment vehicles, and those kinds of interests seem well aligned with the SEC's expertise in regulating investments. Crypto that does work as a currency substitute would seem to fit within the CFTC's framework, and derivatives and futures contracts involving crypto would similarly seem to belong with the CFTC. FinCEN and other banking authorities might be able to apply regulations based on whether an intermediary acting to facilitate transactions in a given crypto asset are acting more like a financial institution in converting currency or a broker-dealer in exchanging securities. It is, however, not at all clear that every crypto asset should be regarded as a currency substitute such that intermediaries are treated as money transmitters. Ideally, the I.R.S. should buy into this kind of differentiation as well.

5. CONCLUSION

When crypto was new, it made sense to think of it a "cryptocurrency," and it made sense to lump all of the early altcoins together. That is no longer the environment in which cryptos operate.

Nonetheless, in the U.S., most regulators continue to treat crypto monolithically, applying regulations to all crypto regardless of how it functions and who (if anyone) has control over its further development. The SEC has at least suggested that it might be willing to treat some crypto as something other than a security, although its chairman has also opined that "every ICO" he has seen has involved the sale of securities. In order to avoid the existing situation, where the same interest is classified differently by different regulators, and multiple agencies claim authority to regulate the same interest, it is important to recognize that cryptos are not all the same. Unless and until this happens, cryptos are likely to be poorly regulated.

To avoid the problems of over-regulation, agencies will need to accept a change in perspective. This requires a paradigm shift that moves away from treating crypto as a single kind of asset, when in reality they are not. Hopefully, American regulators will realize this, and act on this reality, sooner rather than later.

BEHAVIORAL BASIS OF CRYPTOCURRENCIES MARKETS: EXAMINING EFFECTS OF PUBLIC SENTIMENT, FEAR, AND UNCERTAINTY ON PRICE FORMATION

CONSTANTIN GURDGIEV | Trinity Business School, Trinity College Dublin (Ireland) and Middlebury Institute of International Studies at Monterey (CA, USA)

DANIEL O'LOUGHLIN | Trinity Business School, Trinity College Dublin (Ireland)

BARTOSZ CHLEBOWSKI | Trinity Business School, Trinity College Dublin (Ireland)

ABSTRACT

In recent years, cryptocurrencies have emerged as an exciting, innovative, and highly unorthodox asset class, primarily used for investment and trading purposes by globally-distributed investors. Although cryptocurrencies have attracted significant academic attention, there are currently no credible universally-accepted methodologies for determining their prices and returns. This study explores the use of sentiment analysis to model the effects of four different categories of sentiments towards the cryptocurrency markets to predict the direction of price: positivity/negativity (towards the underlying technology, development, and price of each cryptocurrency) and fear, uncertainty, and bullishness/bearishness in the financial markets. Investor sentiment is shown to successfully predict the price direction of cryptocurrencies, indicating that there is a potential for herding and anchoring biases among investors in crypto assets. Moreover, our analysis shows that cryptocurrencies can be used as a hedge against the stock market during times of market uncertainty, though not necessarily during times of investor fear.

1. INTRODUCTION

Since the second quarter of 2017, investors' interest in cryptocurrencies, and the blockchain technology underlying these new assets, has risen dramatically, stimulated by both the supply of the new crypto assets into the markets and surging cryptocurrency valuations. These developments coincided with the explosive growth in traditional and social media and search activities relating to coverage of the blockchain technologies and cryptocurrencies. Although Bitcoin remains the most well-known and important, in terms of market capitalization, cryptocurrency to-date, numerous sub-classes of crypto assets have emerged, including crypto coins (e.g., Bitcoin, Ethereum, Ripple, Litecoin, Iota, and Cardano), stable coins (cryptocurrencies targeting a pegged relationship to major currencies, namely the U.S. dollar, e.g., Tether and MakerDao), and crypto-tokens (cryptocurrencies backed to specific applications and initial coin offerings or ICOs, such as Tron, Byton, Vechain, and others). In addition, innovative technological applications were also grafted

onto existent blockchains (e.g., Bitcoin Cash, Bitcoin Gold, and Bitcoin SV).

By mid-2018, more than 2,000 various cryptocurrencies had been listed on exchanges where billions of dollars' worth of trading volume occurs daily [CoinGecko.com (2018)]. These markets vary in terms of trading platform sophistication, security, regulatory coverage, liquidity, and the degree of anonymity and inter-connectedness within the crypto assets trading universe and with the traditional financial intermediaries.

As of mid-January 2019, total market capitalization of cryptocurrencies traded on specialist exchanges stood at just under U.S.$123.8 billion, with Bitcoin's market cap being U.S.$64.83 billion, followed by Ripple at U.S.$13.75 billion and Ethereum at U.S.$13.48 billion [Coinmarketcap (2018)]. Although Bitcoin's market cap had fallen from U.S.$229.12 billion to U.S.$67.1 billion during 2018, it was still significantly higher than what it was at the beginning of 2017, when its market cap was U.S.$16.05 billion. Aiding market liquidity and price discovery, in December 2017, the Chicago Board Options Exchange (CBOE) and the Chicago Mercantile Exchange (CME Group) both launched their own Bitcoin futures products.

The cryptocurrencies asset class has emerged as the new speculative investment vehicle, trading and buy-and-hold asset class for retail and sector-related (crypto assets mining and ICO-issuing) investors. However, despite a large volume of academic and investment (sell-side and buy-side) research into cryptocurrencies, there are no established and agreed methods, or credible tools, that investors can use to analyze and value these assets [Brown (2018)].

From the investment practitioner's perspective, Bitcoin generates no cash flows and investment returns are generated solely through increases in price, hence making them difficult to price. An added complication is that the after-tax returns of cryptocurrencies are subject to different tax regimes based on where the investor is domiciled. For example, under some tax regimes, investors in crypto assets accrue tax liabilities on capital gains arising from trading, not from closing of long positions, which further complicates the practical evaluation of returns of cryptocurrencies. The third issue relates to the poor quality of data reported by the exchanges, especially with regards trading volumes [Koetsier (2018), Sharma (2018)].

While most recent studies find that the markets are now dominated by the buy-and-hold investors [Gurdgiev and Corbet (2018), Wilson (2018), and Celeste et al. (2018)], given the chances of earning massive profits from buying cryptocurrencies, the herd mentality still remains prevalent within the market [Bishop (2017), Kharpal (2018)]. Consequently, from a purely behavioral perspective, an increasingly promising methodology for modeling demand for crypto assets is through capturing herding and other behavioral aspects of the investors' choices via sentiment analysis ("opinion mining"), which provides information on revealed preferences for an asset by actual and potential investors.

This study applies sentiment analysis to the cryptocurrency market. It is hypothesized that some of the sentiment factors that affect stock prices also affect cryptocurrency prices. We further hypothesize that since there is a lack of deep fundamentals pricing in cryptocurrencies markets, behavioral considerations of individual investors should dominate. As the result, we test whether the behavioral implications of sentiment have a greater impact on cryptocurrencies than on liquid assets such as equities. Given that the market is dominated by novice investors, cryptocurrencies should be more prone to irrational decision-making due to behavioral biases [Baker and Ricciardi (2014)].

In this article, we apply investor sentiment identification methods to the ten largest cryptocurrencies (based on their market capitalizations as of the end of May 2018 – the period that captures the markets with significant presence of retail and novice investors an precedes the sustained and large-scale sell-off in the markets that began in the second half of 2018). Our aim is to identify some of the behavioral factors that may affect the price of cryptocurrencies.

We consider the following behavioral factors:

- **Fear:** as measured by the market "fear index" (VIX).
- **Uncertainty:** as measured by the U.S. Equity Market Uncertainty index (EMUI).
- **Positivity/negativity:** as measured by using the opinions of the Bitcointalk.org forum participants.
- **Bullishness/bearishness:** in the overall financial markets, as measured by the CBOE put/call ratio.

Fear, uncertainty, and bullishness/bearishness are three behavioral or sentiment factors that directly impact the

equity markets and indirectly other risky assets, including cryptocurrencies. In contrast, positivity/negativity sentiment is reflective of the investor sentiment specific to crypto assets.

We use a panel-data regression model based on the behavioral factors mentioned above. The sample used consists of daily observations from January 1, 2017 to May 9, 2018, excluding weekends and public holidays (i.e., 340 days). This time window allows us to analyze the dynamics of the cryptocurrency markets as characterized by significant change in holdings from the early crypto adopters/enthusiast investors to the increased interest from retail investors through the second half of 2017.

After addressing issues with stationarity and heteroscedasticity, a generalized least squares model with robust standard errors and log transformed variables is used to examine short-term price-sentiment relationships.

The study makes three contributions to the broader literature on the investment aspects of cryptocurrencies. Firstly, many of the published quantitative studies of cryptocurrencies specifically focus on Bitcoin, or the top three cryptocurrencies, including (usually) Bitcoin, Ehtereum, and Ripple. While cryptocurrencies are heavily correlated to the price of Bitcoin (see Table 2 in the data section below), adding more cryptocurrencies increases the robustness of the study. This study uses Bitcoin and nine other cryptocurrencies in a panel-data regression model that covers more than 90% of the entire value of the cryptocurrencies market. Secondly, behavioral finance and sentiment analysis are a growing field of research, with to-date minimal application to the crypto assets. Thirdly, use of behavioral indicators, such as sentiment factors, allows for a different view of the overall market framework, complementary to the Fractal Markets Hypothesis (FMH) but contrasting with the Efficient Markets Hypothesis (EMH). The former is increasingly being shown to be of descriptive value in the case of crypto assets as compared to the latter [Celeste et al. (2018), Gurdgiev and Harte (2018)].

2. REVIEW OF THEORETICAL AND EMPIRICAL LITERATURE

The cryptocurrency market has received a great deal of interest in recent years, and especially since the start of the bull markets in crypto assets around the end of the first half of 2017, followed by the large-scale bear market and crash that followed from the late January 2018.[1]

2.1 The FMH, EMH, and crypto assets

Much of the contemporary financial theory rests on the foundations of EMH, which states that current prices reflect available information [Fama (1970)]. The EMH forms the very basis of the rational models in financial analysis, models based on the underlying assumption that representative agents act as rational investors with some degree of foresight, precluding behavioral biases from systemically influencing market prices. What kind of information the prices reflect is determined by which version of EMH one subscribes to.[2] EMH allows one to treat market prices as random processes that do not convey any useful information about the future of the market.

If, however, price series are characterized by long-memory processes (processes that retain the effects of new information arrival over time during the price adjustment process), they are not independently distributed but follow patterns that could be detected and exploited [Cajueiro and Tabak (2004)], violating EMH fundamentals.

Given the long-memory consistent nature of financial markets, several alternatives to EMH have been produced over the years. The better-known alternative hypotheses include Adaptive Market Hypothesis (AMH) [Lo (2005)], which applies the principles of evolution of biological organisms to financial markets, and Fractal Market Hypothesis (FMH), postulating that markets have a self-similar structure that ensures their stability [Peters and Peters (1994)].

FMH is of particular importance when considering long-term effects of markets behavior or memory processes, and thus the more suitable framework for thinking about cryptocurrencies markets. FMH states that markets are fractal when there is sufficient liquidity provided by participating investors. Investors must have heterogeneous time horizons and investment expectations to provide liquidity. In other words, investors can be driven by behavioral biases, such as herding, anchoring, recency,

[1] At the start of January 2019, Bitcoin was down almost 80.2% on its peak, although still up 310.5% on the levels at the start of January 2017.

[2] Generally, the "strong" form of EMH states that all information, public and private, is reflected in stock prices, while the "weak" form states that markets reflect all past market information. "Semi-strong" levels of efficiency fall somewhere in between the two extremes, positing rapid adjustments to market as well as to fundamental, economic, and market-related information.

etc. Investors interpret market information differently, because they have different goals, which makes them differentially attentive to different type of news. Market bubbles and crashes are explainable under FMH: certain investment horizons become dominant, which creates an imbalance between buyers and sellers, impacting liquidity supplied to the markets, and sends asset prices exponentially higher, or plunging.

Since cryptocurrencies constitute a novel asset class, they simultaneously raise questions regarding informational efficiency, data quality, and behavioral biases that pivot on these considerations. They also present an exciting case regarding the choice of an appropriate theoretical framework that can aid our understanding of the price formation mechanisms.

Celeste et al. (2018) provide a detailed summary of literature and empirical evidence, including own data analysis, to support the application of FMH to the cryptocurrencies, in contrast to EMH. From our point of view, the validity of the FMH framework in cryptocurrencies markets analysis lends additional robustness to the study of the impact of sentiment and behavioral factors on crypto assets valuations.

2.2 Sentiment analysis overview

Behavioral research has shown that both information and emotion play an important role in human decision-making [Dolan (2002), Kahneman and Tversky (1979)], and influencing investment choices [Nofsinger (2005)]. Using this knowledge, Bollen et al. (2011) used 9.8 million public tweets sent in 2008, creating a sentiment dataset, to investigated whether public mood is correlated to the Dow Jones Industrial Average or DJIA (as a proxy for the stock market). The results showed that the daily changes in the DJIA could be predicted by the public mood sentiment analysis with 86.7% accuracy. Guo et al. (2017) show that, while not always, investor sentiment can predict stock prices.

Cryptocurrency enthusiasts are very active on social networks, such as Twitter and Reddit, as well as on specialist forums, such as Bitcointalk.org, and their interactions, while reflective of the investor sentiment, can have both first and second order effects on the pricing of cryptocurrencies. The first order effects can relate to the immediate mood or sentiment status of the market's participants. A positive average sentiment across all investors can have the effect of reflecting the bullishness of the investors.

The second order effects are more varied. Firstly, there is a selection bias, similar to the effects of long-only investors in the CAPM setting with heterogeneous beliefs [He and Shi (2007)]. More bullish investors can dominate negative sentiment investors, skewing the demand and pricing observed in the markets towards the former. Secondly, indirect effects of current sentiment can be transmitted through sentiment anchoring (implying potentially autoregressive nature of sentiment and its effects on demand for and pricing of cryptocurrencies). Thirdly, to the extent that sentiment itself is anchored in investors cross-referencing each other through social media forums, there can be positive reinforcement of sentiment within these venues that can support complex pricing dynamics, including pump-and-dump schemes that have been previously detected in the crypto assets markets.

It could also be argued that the accuracy and quality of the information being communicated declines as information progresses through social media channels, where people's motives and interpretations differ, further influencing the decisions of readers. Baker and Wurgler (2007) studied the relevancy of investor sentiment and discovered that companies that were young, unprofitable, highly volatile, and had low market capitalization were very sensitive to investor sentiment. From a theoretical perspective this makes sense, since valuing these stocks is more difficult, which would make biases more "insidious" and increase the chances of valuation mistakes. This increases the value of information concerning these stocks to investors, but also increases the noise component in the information set. Cryptocurrencies are similarly young, unprofitable (profits mostly come from capital gains, similar to gold, but are harder to book due to lower liquidity and higher trading costs, and tax treatment of trading in cryptocurrencies), and highly volatile. In other words, cryptocurrencies have a similar disposition to sentiment as stocks with low liquidity.

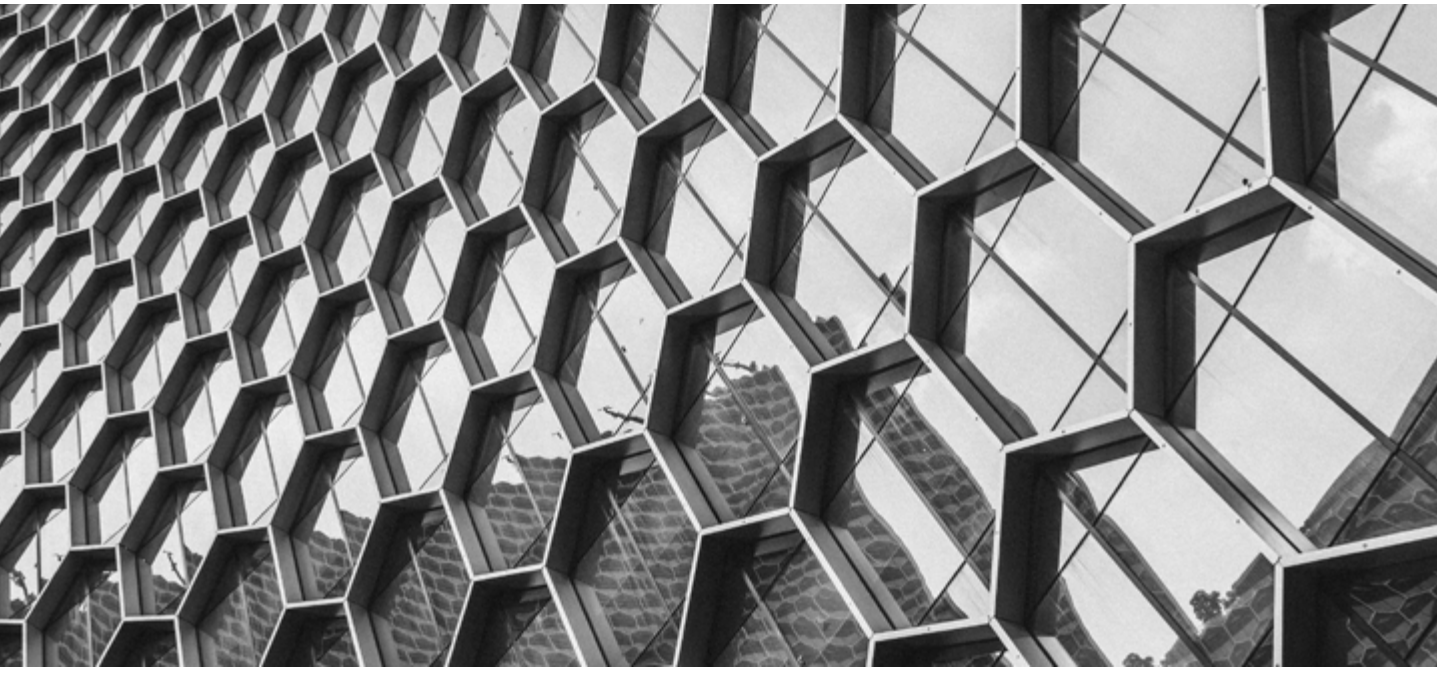
Many of the studies find that investor sentiment is significant in predicting prices. However, it is important to note that much of the literature on the subject focuses on one country or region, which reduces their application to cryptocurrencies, as they are traded and held globally. Controlling for the single country bias, Zouaoui et al. (2011) find that countries with lower institutional investors' involvement are more susceptible to stock price movements occurring due to changes in the investor sentiment. With regards to cryptocurrencies,

while some hedge funds are introducing cryptocurrencies to their portfolios, the majority of traditional institutional investors have hardly made a material impact on the cryptocurrency market [Kharpal (2017)]. Considering these facts, investor sentiment could be a significant factor in the price movement of cryptocurrencies, to a far greater extent than their impact on other, more liquid, more geographically isolated, and more established asset classes, such as equities.

In applying sentiment data to predicting stock prices, Heston and Sinha (2017) explored textual processing and its usefulness in predicting stock returns. The study concluded that news on a daily basis can predict stock returns for one to two days. However, news taken on a weekly basis can predict stock returns for one quarter. If the news stories are positive, then a quick increase in price is expected, but the study also found that prices have a long-delayed reaction after the release of bad news. For this study, textual processing similar to the kind used in Heston and Sinha (2017) is applied to comments made on cryptocurrency forums rather than in general news forums/venues. For robustness, we pair this with indices that measure broader markets sentiment.

2.3 Social media positivity in the markets

In discovering whether increased attention towards, and popularity of, cryptocurrencies is a driver of prices, Bouoiyour and Selmi (2015) looked at Bitcoin's association with investors' attractiveness to Bitcoin, its exchange-trade ratio, its monetary velocity, its estimated output volume, the hash rate, the price of gold, and the Shanghai market index. Their study is interesting since it presents several factors that may influence prices. Their study showed that around 20% of Bitcoin's price is driven by investors' attractiveness to Bitcoin, as determined by the volume of Google search queries. The other variables in the study have an insignificant impact on price except for the Shanghai market index, which accounts for approximately 10% in Bitcoin price variation. While the results indicate that positive sentiment (conveyed through the variable: "attractiveness to Bitcoin") affects Bitcoin's price, the authors showed that the remaining 70% of Bitcoin's price movements is explained by "its own innovative shocks," which is an ambiguous explanation, effectively relying on using the residual as the signal of systemic unexplained component of price formation.



Kristoufek (2015) looked into the Google Search data and Wikipedia searches for the term "Bitcoin." The study showed that both search engines provide similar information. During the price bubble that took place in the first quarter of 2013, the price of Bitcoin was actually led by increased interest. A similar dynamic appeared for the second bubble that started in October 2013, although those findings were not statistically reliable. When the crash of the first 2013 bubble occurred, an increase in interest still correlated to the price of Bitcoin, however, it interestingly converted to being negatively correlated. Ciaian et al. (2016) mention several studies that suggest new investors' decisions to go long cryptocurrency might become altered by the influence of public attention (e.g., attention in forums). New investors favor those investments that are under the influence of public attention because such attention reduces search costs. This availability bias then triggers a high price response due to an increase in demand. The study furthers the argument that cryptocurrency prices may be influenced by comments on popular specialist social forums, such as bitcointalk.org.

> "...cryptocurrencies can be used as a hedge against the stock market during times of uncertainty, although not during times of fear."

Adding to the literature regarding social media and how it affects cryptocurrency prices, Martina et al. (2015) analyzed 1.9 million tweets mentioning Bitcoin and spanning 60 days to see if the sentiment analysis of the tweets was associated with Bitcoin's prices. The results affirmed that positive tweets may be used to predict changes in Bitcoin prices three to four days in advance. However, the study only covers a 60-day period and the authors recognize that analysis over the longer time horizon may produce results of a higher quality. Li et al. (2018) also examined tweets as a medium for investor sentiment to predict the price movement of one small-cap cryptocurrency called ZClassic. 130,000 tweets were gathered, analyzed, and then assigned a value of either positive, negative, or neutral. They found that using sentiment analysis of tweets proved successful in predicting the price movements of ZClassic. The range of data only spanned 3.5 weeks.

Kim et al. (2016) showed that through the sentiment analysis of cryptocurrency forums, investors can predict, in part, price changes for Bitcoin, Ethereum, and Ripple. The fluctuation in the price of Bitcoin was significantly correlated with the amount of topics, positive comments, and replies made on the Bitcointalk.org forum. This result was stronger (with an accuracy of 79.6%) when a lag of six days was applied to sentiment variables. Ethereum and Ripple also showed significant results. However, the forums used for analyzing the sentiment, forum.ethereum.org and xrpchat.com, are exclusive to these two cryptocurrencies. This may create a bias in the data because these forums will only contain the opinions and comments of registered users, who likely signed up because they are interested in that particular cryptocurrency. A forum that invites discussion regarding all cryptocurrencies might be more suited to this type of sentiment analysis, since it will likely invite more discussion from people with negative sentiment towards the respective cryptocurrencies.

Phillips and Gorse (2018) considered four cryptocurrencies (Bitcoin, Ethereum, Litecoin, and Monero) and used the discussion forum Reddit (which has a large cryptocurrency user base) to investigate if the amount of posts per day, subscriber growth, and amount of new authors per day is correlated with price. Their study also included Google search volume and Wikipedia view data. By using wavelet coherence analysis, they found that in the short term, increases in online activity led to a decrease in price. In the medium term, online activity is positively correlated with changes in price. It also found that Wikipedia views lacked consistency and that the data from Reddit proved to be a better predictive indicator in the long term.

Mai et al. (2018) tested the predictability of Bitcoin price by analyzing the sentiment in posts regarding Bitcoin on Twitter and the Bitcointalk.org forum using a python script and the Natural Language Toolkit 3.0. The results proved that days with more positive posts preceded days with increases in Bitcoin price. One additional positive forum post was associated with a rise of 3.53 basis points in the price of Bitcoin the following day.

The Natural Language Toolkit 3.0, while proven effective in analyzing sentiment, may not be the best application in studying sentiment of cryptocurrencies. This is due to the specific vocabulary, slang, and acronyms associated with cryptocurrencies. The methods used in our study, in contrast to Mai et al. (2018), address this problem by

manually building a lexicon that includes crypto-specific words and applying this to the same forum used in the Mai et al. (2018) study, Bitcointalk.org. In addition, we cover a larger set of cryptocurrencies. Similar to some of the studies mentioned above, applying a positive, negative, and neutral value to each comment appears to be an appropriate way of measuring investor sentiment found in the cryptocurrency forums.

2.4 Fear and uncertainty in the markets

Ciaian et al. (2016) also incorporated macroeconomic and financial developments in their study. The authors rely on Dimitrova (2005), which explores how a decrease in the price of stocks causes foreign investors to sell financial assets that they hold. In turn, this creates a depreciation of the respective currency. However, according to Ciaian et al. (2016), this may stimulate the price of Bitcoin if investors exchange their stock investments with investments in Bitcoin if it is viewed as a safe haven or a hedge for currencies. Consequently, stock market indices have an expectation to be negatively correlated with the price of Bitcoin. Bouri et al. (2016) found that Bitcoin had an inverse relationship with the U.S. VIX, but that its hedging capabilities existed only until the Bitcoin crash of 2013. Based on methodology developed in Ciner et al. (2013), Bitcoin could have potentially acted as a safe haven for VIX prior to the crash of 2013.

Contrary to the belief that Bitcoin cannot be used as a hedge, Dyhrberg (2016) explored the its hedging capabilities by using a GARCH (or Generalized Autoregressive Conditional Heteroscedasticity) model. The results show that Bitcoin does have safe-haven properties when used against the FTSE index as well as the U.S. dollar in the short-term. Baur et al. (2015) found that Bitcoin can act as a hedge against traditional assets such as equities, precious metals, currencies, energy instruments, and bonds. Bouoiyour and Selmi (2015) suggest that while Bitcoin can be used as a hedge in the short-term, it is far from being a safe-haven asset. Notably, these studies pre-date Bitcoin and crypto assets' explosive dynamics over 2017-2018 period.

In light of the aforementioned findings, it seems appropriate to look at the hedging potential for cryptocurrencies against market fear proxies. We do so below by integrating the CBOE's VIX index into our analysis.

Kristoufek (2015) also found no evidence of Bitcoin being a safe haven asset after observing its relationship with the Financial Stress Index (FSI) and price of gold in Swiss francs – the former being a proxy for financial uncertainty and the latter being considered a safe-haven in itself. According to the study, when uncertainty increases, the price of Bitcoin also increases. However, there are few long-term intervals that produce statistically significant results, and this undermines the overall result. The instability of hedging relationships is a feature commonly linked to higher measures of uncertainty (as opposed to volatility) in market environments. From this point of view, it may also be interesting to look at the U.S. Equity Uncertainty Index, in addition to volatility index or VIX, which tracks financial uncertainty, to see if a different indicator of uncertainty may generate statistically significant results.

Following Kristoufek's (2015) study on the sentiment of uncertainty, Chulia et al. (2017) used the U.S. EMUI to see how uncertainty affects emerging and mature markets. Using daily data from 1998 to 2016, they found that spikes in uncertainty reduce stock market returns. Bouri et al. (2017) used Bitcoin price data and a global volatility index data to determine how it is impacted by uncertainty. They found that, similar to the equity market, Bitcoin does act as a hedge against uncertainty. Again, it would be interesting to see if the EMUI has a symmetric effect on a broader universe of crypto assets.

In summary, it appears that the price of cryptocurrencies could be influenced by uncertainty. To explore this, uncertainty is introduced in this study using the U.S. Equity Market Uncertainty index, as it provides daily data and its correlation with cryptocurrencies has as yet not been investigated.

2.5 Bullishness/bearishness in the markets

Mao et al. (2015) studied the effect of online bullishness on international financial markets, finding that both Twitter and Google bullishness not only have a positive correlation to investor sentiment, but also have a lead on established investor sentiment surveys. It was also shown that high levels of bullishness on Twitter can be used to predict stock return increases.

Bandopadhyaya and Jones (2008) investigated the use of the CBOE put/call ratio (PCR) in analyzing investor sentiment. The PCR is a contrarian indicator where an

increase in the PCR relates to an increase in pessimism in the market. As a measure of investor sentiment, it was concluded that the PCR approximates non-economic factors that may drive price changes better than the VIX, and thus act as a better measure of market sentiment. Our study focuses on the PCR's correlation with the cryptocurrency market.

3. DATA COLLECTION AND PRELIMINARY ANALYSIS

The data used in this paper are sourced from CoinGecko, CBOE, Bitcointalk.org, and FRED. The data is collected from January 1, 2017 to May 9, 2018. The reason for this timeframe is because there is little or no forum participation before 1st January 2017. The frequency of the data is daily. The cryptocurrencies used in the study were: Bitcoin, Ethereum, Ripple, Litecoin, NEM, Dash, Monero, Lisk, Verge, and Stratis. Some cryptocurrencies have been omitted from the actual top ten digital currencies, as per their market capitalizations, because they either did not exist in January 2017, or the cryptocurrency represented a "fork" or a spin-off of the original (e.g., Ethereum Classic).[3]

3.1 Explanatory variables

The U.S. Equity Uncertainty Index is used as a measure of uncertainty in the U.S. equity markets [Baker et al. (2013)]. Data for Cryptocurrency Forum Sentiment was extracted from the comments on the popular cryptocurrency forum Bitcointalk.org, using web-crawler platform Import.io as follows: for each comment made it received a score of +1, -1 or 0 depending on whether it was positive, negative, or neutral toward cryptocurrency price dynamics. When extracting the forum data, quotes were removed to avoid double-counts of the same comment. Once all the comments were collected, they were analyzed for whether they were positive, negative, or neutral comments. We addressed the issues raised in Loughran and McDonald (2011), who show that using general sentiment analysis on topics in accounting and finance leads to high rates of misclassification, by using a lexicon-based sentiment analyzer specifically created for the purpose of this study, using the Loughran-McDonald master dictionary. We also manually tested the sentiment analyzer to confirm its accuracy in detecting the general mood of comments in the discussion threads. The CBOE PCR was used as a bullish/bearish sentiment indicator: when the ratio is rising, it suggests that investors believe the market is declining [Qian (2009)]. Lastly, the VIX or the "market fear gauge," an index quoted by the CBOE, was used as a benchmark measure of expected short-term (30 days forward) volatility [Whaley (2009)].

Table 1: Descriptive statistics of the variables

VARIABLE	N	MEAN	STANDARD DEVIATION	SKEWNESS	KURTOSIS	MIN	MAX
BITCOIN	340	5537.432	4533.999	0.9951446	3.223341	784.28	19188.05
ETHEREUM	340	366.0573	314.8953	0.9253896	3.139247	9.6268	1361.44
DASH	340	336.4864	304.2355	1.35203	4.583646	11.2054	1493.591
LISK	340	7.197206	8.062563	1.265486	3.65157	0.101672	32.74986
LITECOIN	340	81.97478	80.38994	1.172157	3.604904	3.734	360.662
MONERO	340	126.7323	120.109	0.9846647	2.912851	11.198	542.3255
NEM	340	0.2838645	0.3171296	2.336845	9.328439	0.0032964	1.794839
RIPPLE	340	0.4171065	0.5135199	2.386356	10.41572	0.005376	3.22005
STRATIS	340	5.057671	4.348135	1.12152	4.552691	0.048092	22.76509
VERGE	340	0.0253526	0.0421381	2.130654	7.452737	0.0000104	0.2071443
UNCERTAINTY	340	26.59985	52.6277	7.418349	68.87616	4.94	591.21
FORUMSENT	340	-0.1205882	1.686364	-0.7488451	5.491211	-8	5
PUTCALL	340	0.9270294	0.1288307	0.6000725	4.301916	0.64	1.54
VIX	340	12.738	4.061839	2.415084	10.46591	9.14	37.32

[3] The cryptocurrency prices are skewed and have a high kurtosis, warranting a log transformation of the raw data.

Table 2: Correlations between cryptocurrencies

	BITCOIN	ETHEREUM	DASH	LISK	LITECOIN	MONERO	NEM	RIPPLE	STRATIS	VERGE
BITCOIN	1.0000									
ETHEREUM	0.8695	1.0000								
DASH	0.9560	0.8795	1.0000							
LISK	0.8479	0.9562	0.8803	1.0000						
LITECOIN	0.9402	0.9037	0.9256	0.8960	1.0000					
MONERO	0.9528	0.9378	0.9452	0.9336	0.9614	1.0000				
NEM	0.8162	0.8755	0.8852	0.8591	0.8247	0.8604	1.0000			
RIPPLE	0.7777	0.8779	0.8197	0.8844	0.8267	0.8627	0.9374	1.0000		
STRATIS	0.7882	0.8735	0.8468	0.8034	0.7896	0.8131	0.9126	0.8314	1.0000	
VERGE	0.7621	0.8185	0.8107	0.8606	0.8177	0.8554	0.8837	0.9143	0.7657	1.0000

3.2 Transforming the data

A log transformation of each variable was taken. The motivation behind this was to:

1. Narrow the scale of data to lessen any non-linearity (creating more reliable results).

2. Neutralize the mostly-positive skewness and lower the high kurtosis as seen in Table 1 above.

To test the variables for stationarity, two-unit root tests were conducted including the Augmented Dickey-Fuller test and the Phillips-Perron test. The results of the unit root tests indicated presence of a unit root in the LnPrice variable but not in any of the other variables. In solving the non-stationary LnPrice variable, we first-difference the variable [Engle and Granger (1987)], making the LnPrice variable stationary.

3.3 Descriptive statistics

The descriptive statistics and correlation matrices for the variables are presented in Table 1. Table 2 shows the correlation matrix between the ten different cryptocurrencies chosen for this study.

As expected, all ten cryptocurrency variables show high volatility – with standard deviations lying close to the mean and large dispersions between the minimum and maximum observations present. The correlation matrix between the ten cryptocurrencies shows a high correlation between them all. This implies that when one cryptocurrency rises, other cryptocurrencies tend to rise at the same time, and adds to the robustness of the study in terms of choosing a panel data model.

4. MAIN RESEARCH HYPOTHESIS AND RESULTS

The primary objective of this research is to create an econometric model and conduct a panel data regression analysis that explores the significance of investor sentiment on the price movement of cryptocurrencies using four independent variables.

Hypothesis 1: Investor sentiment has predictive power over the price of cryptocurrencies. Under conditions of rising market uncertainty, we expect that the price of cryptocurrencies should rise [Kristoufek (2015), Bouri et al. (2017), Sarwar (2017)]. This hypothesis implies that cryptocurrencies can act as a short-term hedge or a flight-to-safety asset against the stock market during the times of elevated market uncertainty.

Hypothesis 2: Cryptocurrencies are a hedge against the stock market in times of uncertainty. The positive and negative sentiment of the cryptocurrency market in this study is conveyed using the sentiment captured from the cryptocurrency forum Bitcointalk.org. Using this as the proxy for overall market sentiment, it is hypothesized that when the sentiment of the market is positive, the price of cryptocurrencies should increase. Our forum sentiment hypothesis adapts the theory of the herding behavioral biases, which owes its roots to Keynes (1930), and the general herding literature in finance.

Table 3: Random-effects model regression results

DEPENDENT VARIABLE:	d_*ln*price		
INDEPENDENT VARIABLES:	COEFFICIENT	Z-SCORE	P-VALUE
*ln*uncertainty	0.006125	2.34	0.019[b]
*ln*forumsentiment	0.048116	4.74	0.000[a]
*ln*putcall	0.007496	0.65	0.515
*ln*VIX	-0.039498	-9.16	0.000[a]
Constant	-0.078847	-2.00	0.046[b]
Random effects GLS	Number of observations	3390	
	Number of groups	10	
R-Sq	Within	0.0119	
	Between	0.0587	
a, b, c are significant levels at 1%, 5%, and 10%, respectively			

Hypothesis 3: Cryptocurrencies experience an increase in price when sentiment towards its underlying technology, development, and price is positive. It is hypothesized that an increase in bullishness in the financial markets (a decrease in the CBOE PCR) will result in an increase in the price of cryptocurrencies [Mao et al. (2015), Bandopadhyaya and Jones (2008), Li and Wang (2017)].

Hypothesis 4: When investors are mostly bullish/bearish in the financial markets, cryptocurrencies will experience an increase/decrease in price. In following the literature, it can be assumed that, similar to stocks, a rise in the VIX will result in a fall in price of cryptocurrencies [Ciaian et al. (2016)]. This is because fear can be assumed to be a more serious and negative emotion than uncertainty, and when investors are in fear with respect to the direction of the stock market prices, they will be apprehensive in investing their money in any risky asset, including cryptocurrencies.

Hypothesis 5: Cryptocurrencies are not a hedge against the stock market during times of fear.[4] From a methodological point of view, we specify a panel data model that will allow us to test the hypotheses stated above.[5]

The following is the formal representation of the model:

$$\Delta ln\text{price}_{it} = \beta_1 + \beta_2\, ln\text{uncertainty}_{it} + \beta_3\, ln\text{forumsentiment}_{it} + \beta_4\, ln\text{putcall}_{it} + \beta_5\, ln\text{VIX}_{it} + \omega_{it} \quad (1)$$

where:

$$\omega_{it} = \varepsilon_{it} + u_{it} \quad (2)$$

The composite error term in (5.2) has two components: ε_i, which is the cross-section or individual-specific error component, and u_{it}, which is the combined time series and cross-section component.

"Δ*ln*price" is the dependent variable, which is the first difference of the natural logarithm of each of the ten cryptocurrencies included in this study. The independent variables include "*ln*uncertainty," which is the log of the U.S. Equity Uncertainty Index. "*ln*forumsentiment" represents the log transformation of the Bitcointalk.org forum's sentiment results and also includes the constant as mentioned in section 3.3 above; "*ln*putcall" is the log transformation of the CBOE PCR data and "*ln*VIX" is the log transformation of the VIX index.

Based on implementation of the GLS model for random effects panel data estimation, we obtain the results presented in Table 3.

The "*ln*uncertainty" variable shows a statistically significant result with a p-value of 0.019. This implies that an increase in the U.S. EMUI results in a small increase in the cryptocurrencies prices. This supports the hypothesis that cryptocurrencies are a potential hedge or a flight-to-safety/safe haven against the stock market during times of uncertainty.

The "*ln*forumsentiment" variable is also highly statistically significant with p-value 0, implying that positive investor sentiment has a positive effect on the price of cryptocurrencies.

The "*ln*putcall" variable p-value of 0.515 fails to produce statistically significant results, providing no support for the hypothesis that "when investors are mostly bullish in the financial markets, cryptocurrencies will experience an increase in price." An explanation for this may be because the CBOE PCR only accounts for puts and calls on its own exchange and does not account for those traded on other exchanges and geographical markets, where high cryptocurrency purchasing participation is taking place, such as Asia and Europe.

[4] In dealing with hedging or flight-to-safety/safe haven hypotheses, we refer to Ciner et al. (2013) methodology.

[5] Tests used in deriving the optimal specification for the model are available from the authors upon request.

The "*ln*VIX" variable was statistically significant with a p-value of 0. The result supports the hypothesis and current literature that cryptocurrencies are negatively correlated to the VIX and that they are not a hedge against the stock market during times of fear. Because of cryptocurrencies' negative correlation to the VIX and similar relationship to equities in instances of fear, this would imply that it is important for cryptocurrency investors to conduct global macro analysis when making investment decisions.

5. CONCLUSION

Dynamic attributes of cryptocurrencies, such as volatility and uncertainty, are important issues that impede this new asset's growth because they increase risks, reduce stability and resilience of hedging properties, and drive behavioral biases into investment and trading strategies and actions of investors. Today, cryptocurrencies and broader crypto assets reflect the adverse effects of an investment environment that is characterized by volatility, uncertainty, complexity, and ambiguity (VUCA). Consequently, it is almost impossible to identify stable (over time and across markets conditions) macro- and microeconomic determinants of cryptocurrencies prices.

This research has sought to quantify the relationship between investor sentiment and the monetary value of cryptocurrencies. The hypotheses addressed span behaviorally rich areas of investors' sentiments and the perceptions of market uncertainty. Based on the existing literature on behavioral finance, four emotions of investor sentiment were identified: fear (across all financial markets, as proxied by the CBOE VIX index), uncertainty (across the U.S. equity markets, as measured by the U.S. EMUI), positivity/negativity sentiment toward cryptocurrencies (based on specialist fora comments relating to crypto assets), and bullishness/bearishness across the broader financial markets (as measured by the CBOE's Total PCR).

From examining the results, investor sentiment can be used to predict the price direction of cryptocurrencies. Moreover, the results indicated that cryptocurrencies can be used as a hedge against the stock market during times of uncertainty, although not during times of fear. When there is an overall positivity in the cryptocurrency marketplace amongst investors and cryptocurrency enthusiasts, a rise in cryptocurrency prices is expected. Likewise, when sentiment turns sour, prices do tend to fall. This suggests that there is a strong presence of herding biases in the behavior of cryptocurrency investors. Finally, it was shown that the overall bullishness/bearishness of the financial markets does not have an impact on the price of cryptocurrencies, suggesting that anchoring and recency biases, if present, are non-linear and potentially environment-specific.

The findings presented in this study have implications for investors, cryptocurrency adopters, and academics. From an investor's point of view, the results from this under-researched branch of investment analysis can be used to build on the information already presented in previous studies of the subject and improve the accuracy with which the price direction of cryptocurrencies is predicted. This information is also useful to cryptocurrency adopters, in that it helps them understand the different forms of sentiment and their relationships with cryptocurrencies.

REFERENCES

Baker, K. H., and V. Ricciardi, 2014, "How biases affect investor behavior," European Financial Review February-March, 7-10

Baker, M., and J. Wurgler, 2007, "Investor sentiment in the stock market," Journal of economic perspectives, 21:2, 129-152

Baker, S. R., N. Bloom, and S. J. Davis, 2013, "U.S. equity market uncertainty index," Economic Policy Uncertainty, https://bit.ly/2nX0d9l

Bandopadhyaya, A., and A. L. Jones, 2008, "Measures of investor sentiment: a comparative analysis put-call ratio vs volatility index," Journal of Business and Economics Research 6:8, 27-34

Baur, D. G., Hong, K. J., and A. D. Lee, 2015, "Bitcoin – currency or asset?" Melbourne Business School, 2016 Financial Institutions, Regulation & Corporate Governance (FIRCG) Conference, https://bit.ly/2TpMMgl

Bishop, J., 2017, "Meet the man traveling the world on $25 million of bitcoin profits," Forbes, July 7, https://bit.ly/2WDqPg3

Bollen, J., H. Mao, and X. Zeng, 2011, "Twitter mood predicts the stock market," Journal of Computational Science 2:1, 1-8

Bouoiyour, J., and R. Selmi, 2015, "What does bitcoin look like?" Annals of Economics & Finance 16:2, 449–492

Bouri, E., G. Azzi, and A. H. Dyhrberg, 2016, "On the return-volatility relationship in the Bitcoin market around the price crash of 2013," Economics Discussion Papers no. 2016-41, Kiel Institute for the World Economy (IfW), Kiel, https://bit.ly/2DOq2RS

Bouri, E., R. Gupta, A. K. Tiwari, and D. Roubaud, 2017, "Does bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions," Finance Research Letters 23, 87-95

Brown, A., 2018, "How to make sense of cryptocurrency valuations," Bloomberg, April 17, https://bloom.bg/2TrTAdB

Cajueiro, D. O., and B. M. Tabak, 2004, "The Hurst exponent over time: testing the assertion that emerging markets are becoming more efficient," Physica A: Statistical Mechanics and its Applications 336, 521–537

Celeste, V., S. Corbet, and C. Gurdgiev, 2018, "Fractal dynamics and wavelet analysis: deep volatility properties of bitcoin, ethereum and ripple," working paper, https://ssrn.com/abstract=3232913

Chulia, H., R. Gupta, J. M. Uribe, and M. E. Wohar, 2017, "Impact of U.S. uncertainties on emerging and mature markets: evidence from a quantile vector autoregressive approach," Journal of International Financial Markets, Institutions & Money 48, 178-191

Ciaian, P., M. Rajcaniova, and D. Kancs, 2016, "The economics of bitcoin price formation," Applied Economics 48:19, 1799-1815

Ciner, C., C. Gurdgiev, and B. Lucey, 2013, "Hedges and safe haves: an examination of stocks, bonds, gold, oil and exchange Rates. International Review of Financial Analysis 29:C, 202-211

CoinGecko.com, 2018, CoinGecko, https://www.coingecko.com/en

Coinmarketcap, 2018, https://coinmarketcap.com/

Dimitrova, D., 2005, "The relationship between exchange rates and stock prices: Studied in a multivariate model," Issues in Political Economy 14(1), 3-9

Dolan, R., 2002, "Neuroscience and psychology: Emotion, cognition, and behavior," Science 298:5596, 1191-1194

Dyhrberg, A. H., 2016, "Hedging capabilities of bitcoin. Is it the virtual gold?" Finance Research Letters 16, 139-144

Engle, R. F., and C. Granger, 1987, "Co-integration and error correction: representation, estimation, and testing," Econometrica 55:2, 251-276

Fama, E. F., 1970, "Efficient capital markets: a review of theory and empirical work," Journal of Finance 25, 383-417

Freedman, D. A., 2006, 'On the so-called 'Huber sandwich estimator' and 'obust standard errors,' The American Statistician 60:4, 299-302

Guo, K., Y. Sun, and X. Qian, 2017, "Can investor sentiment be used to predict the stock price? Dynamic analysis based on China stock market," Physica A: Statistical Mechanics and its Applications 469, 390-396

Gurdgiev, C., and S. Corbet, 2018, "Ripples in the crypto world: systemic risks in cryptocurrency markets," International Banker, June, https://bit.ly/2WFteXl

Hayes, A. S., 2017, "Cryptocurrency value formation: an empirical study leading to a cost of production model for valuing bitcoin," Telematics and Informatics 34:7, 1308-1321

He, X., and L. Shi, 2007, "Zero-beta CAPM with heterogeneous beliefs," 20th Australasian Finance & Banking Conference 2007 Paper, https://bit.ly/2G7wrdm

Heston, S. L., and N. R. Sinha, 2017, "News versus sentiment: predicting stock returns from news stories," Financial Analysts Journal 73:3, 67-83

Kahneman, D., and A. Tversky, 1979, "Prospect theory: an analysis of decision under risk," Econometrica, 47:2, 263-291

Keynes, J. M., 1930, A treatise on money, in two volumes. s.l.: Macmillan & Company

Kharpal, A., 2017, "Central banks could hold bitcoin and ether for the first time in 2018, cryptocurrency CEO says," December 18, https://cnb.cx/2AVY6rC

Kharpal, A., 2018, "Bitcoin headed to $100,000 in 2018, says analyst who predicted last year's price rise," January 16, https://cnb.cx/2Dc6MLz

Kim, Y. B., J. G. Kim, W. Kim, J. H. Im, T. H. Kim, S. J. Kang, and C. H. Kim, 2016, "Predicting fluctuations in cryptocurrency transactions based on user comments and replies," PLOS One, 11(8), p. e0161197, https://bit.ly/2G6HEuC

Koetsier, J., 2018, "Report: top crypto exchange bithumb faking up to 94% of trading volume; bithumb denies allegations," Forbes, December 19, https://bit.ly/2HOrLea

Kristoufek, L., 2015, "What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis," PLOS One 10:4, p. e0123923, https://bit.ly/2D4Dol9

Li, X., and C. A. Wang, 2017, "The technology and economic determinants of cryptocurrency exchange rates: the case of bitcoin," Decision Support Systems 95, 49-60

Lo, A. W., 2005, "Reconciling efficient markets with behavioral finance: the adaptive markets hypothesis," Journal of Investment Consulting 7:2, 21-44

Loughran, T., and B. McDonald, 2011, "When is a liability not a liability? Textual analysis, dictionaries, and 10-Ks," Journal of Finance 66:1, 35-65

Mai, F., S. Zhe, B. Qing, X. Wang, and R. H. L. Chiang, 2018, "How does social media impact bitcoin value? A test of the silent majority hypothesis," Journal of Management Information Systems 35:1, 19-52

Mao, H., S. Counts, and J. Bollen, 2015, "Quantifying the effects of online bullishness on international financial markets," ECB Statistics Paper, vol. 9

Martina, M., I. Lunesu, and M. Marchesi, 2015, "Bitcoin spread prediction using social and web search media," UMAP Workshops, https://bit.ly/2DPTCGO

Nofsinger, J., 2005, "Social mood and financial economics," Journal of Behaviour Finance 6:3, 144-160

Peters, E. E., and D. Peters, 1994, Fractal market analysis: applying chaos theory to investment and economics, John Wiley & Sons

Phillips, R. C., and D. Gorse, 2018, "Cryptocurrency price drivers: wavelet coherence analysis revisited," PLOS One 13:4, p. e0195200, https://bit.ly/2D4n1LK

Qian, H., 2009, "Time variation in analyst optimism: an investor sentiment explanation," Journal of Behavioural Finance 14, 182-193

Sarwar, G., 2017, "Examining the flight-to-safety with the implied volatilities," Finance Research Letters 20, 118-124

Sharma, M., 2018, "Report suggests 87% of the trading volumes at top 25 cryptocurrency exchanges could be fake," Crypto News Review, December 17, https://bit.ly/2MKOJ4B

Whaley, R. E., 2009, "Understanding the VIX," Journal of Portfolio Management 35:3, 98-105

Wilson, T., 2018, "As bitcoin trading shift shape, big money stays away," The Globe and Mail, December 7, https://tgam.ca/2RCBunD

Zouaoui, M., G. Nouyrigat, and F. Beer, 2011, "How does investor sentiment affect stock market crises? Evidence from panel data," Financial Review 46:4, 723-747

INTERBANK PAYMENT SYSTEM ARCHITECTURE FROM A CYBERSECURITY PERSPECTIVE

ANTONINO FAZIO | Directorate General for Markets and Payment Systems, Bank of Italy
FABIO ZUFFRANIERI | Directorate General for Markets and Payment Systems, Bank of Italy

ABSTRACT

This paper outlines how a paradigm shift is required when approaching cyber risk management for interbank payment systems, which are affected by the growing interconnectedness of systems, the digitization of financial services, and the continuously evolving cyber threats. In this scenario, cyber threats may derive from a wider number of actors, who are constantly active on the internet and able to exploit an increasing number of vulnerabilities and attack vectors to achieve their goals. Financial institutions should, therefore, assume that specific cyber threats can overcome any defense. Firstly, the paper outlines the theoretical reasons for this necessary paradigm shift. Secondly, it aims to highlight the importance of all the stakeholders in strengthening the cyber resilience of payment systems, in particular the central and enabling role of messaging service operators, by providing an analysis of a real case study – the recent Bangladesh Bank cyber fraud. Finally, the paper aims to encourage discussion on the new paradigm and the adequacy of current regulatory frameworks and supervisory approaches.

1. INTRODUCTION

Banks and payment services providers, particularly in the field of retail payments (card and internet payments), are generally considered the most exposed to cyber threats due to the economic motivation of cyber criminals and the relative ease with which the end-user, typically the weakest link in the security chain, can be attacked. Yet, some recent cases, such as the cyber fraud against the Bangladesh Bank or the Shadow Brokers' leaks, are of particular concern because they also highlight vulnerabilities within the interbank environment and financial infrastructures, until now areas considered less exposed to cyber risks. Such cases demonstrate that cyber-attacks have the potential to affect even the core elements of the global financial system, and given the broad interconnectedness of systems may have implications for financial stability.

To address these emerging risks, financial regulators and supervisors have launched several initiatives, both at national and cross-border level (G7, BIS, FSB, and so on), to enhance the cyber resilience of the financial systems. At the same time, the financial industry has set up programs in order to improve security for participants within the financial system (e.g., the SWIFT Customer Security Program).

However, some of these actions are based on a traditional paradigm, which assumes that all interbank payment system security relies on trust among its participants and operators, as they are a closed system. The increasing digitization of financial services, coupled with the extreme interconnectedness of the financial sector, means that a more in-depth understanding of the mutual risks posed by logical and physical interconnections is required. Consequently, cybersecurity needs to be approached

in two complementary ways: that financial institutions should be aware that attackers are able to overcome their counterparts' even strong defenses, which means that they cannot consider them as fully trusted entities, and that operators of central infrastructures (payment systems and messaging services) should adopt proactive measures to help improve the overall security of the system.

2. INTERBANK PAYMENT SYSTEM ARCHITECTURE

This paper does not intend to provide a comprehensive overview of interbank payment system architecture but will focus on some specific elements deemed relevant to the topic under discussion.

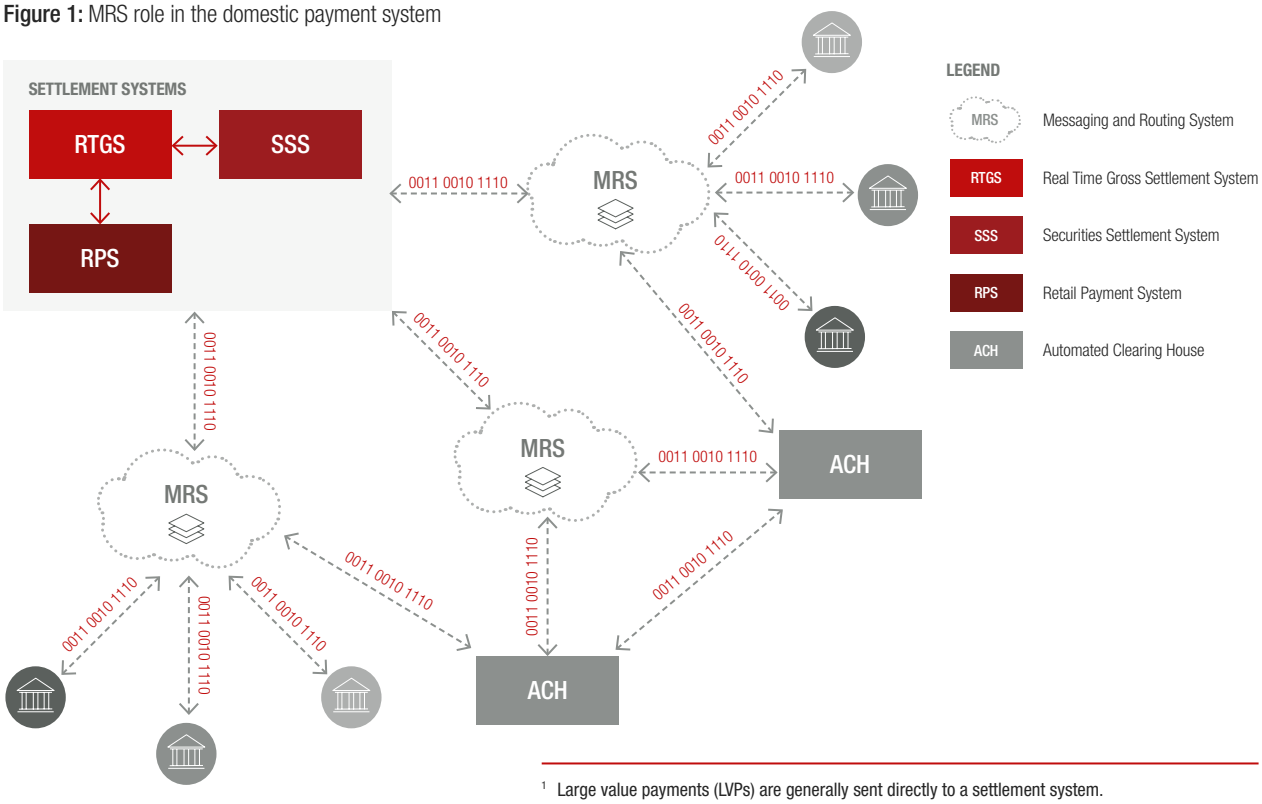
2.1. Messaging and routing functions in interbank payment systems

Payment systems facilitate commercial and financial transfers between buyers and sellers, and for this reason are important components of a country's financial system. They comprise a set of financial institutions, supporting technological infrastructures, and setups that share rules, processes, and standards to make payments efficient and secure.

Despite the adoption of international standards, every country's payment system has its own features, reflecting banking and financial history as well as the technological development of information and communication infrastructures.

Financial institutions communicate with each other **through a messaging and routing system (MRS)**. Transactions, labeled with codes identifying the beneficiary's bank, are routed through automated clearing houses (ACHs)[1] that manage the transmission and reconciliation of payment orders and determine the final balances to be settled. Usually, transactions are settled in different systems according to the type of payments and instruments, namely large value real time gross settlements (RTGS), retail payment systems (RPS), or securities settlement system (SSS), through the debiting/crediting of the accounts of the parties involved in the transaction. Accounts are generally opened at central

Figure 1: MRS role in the domestic payment system



[1] Large value payments (LVPs) are generally sent directly to a settlement system.

banks to ensure settlement finality for each transaction and foster trust and confidence in the whole system (Figure 1).

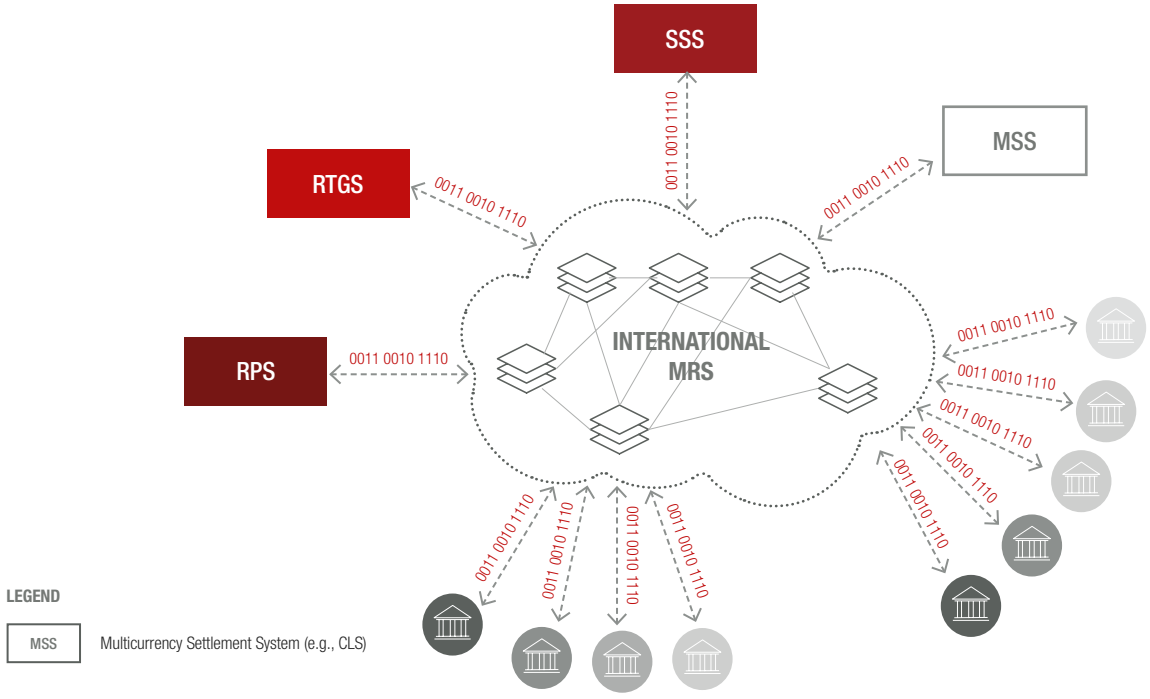
When the parties of the transaction belong to different countries that do not share common infrastructures and/or procedures, the payment cycle is similar to that described above, but the international MRS functions as a hub where all transactions are channeled and, therefore, plays an even more central and critical role in the smooth functioning of the system. In this case, settlement can even not occur in the account systems of a central bank, and obligations can be handled by bilateral banking accounts (correspondent banking). Such a method can also be used between banks belonging to the same country, leveraging the services of common network infrastructures (Figure 2).

For historical reasons, only one company is currently playing the role of the international MRS, namely SWIFT.[2]

2.2 Payment system security architecture

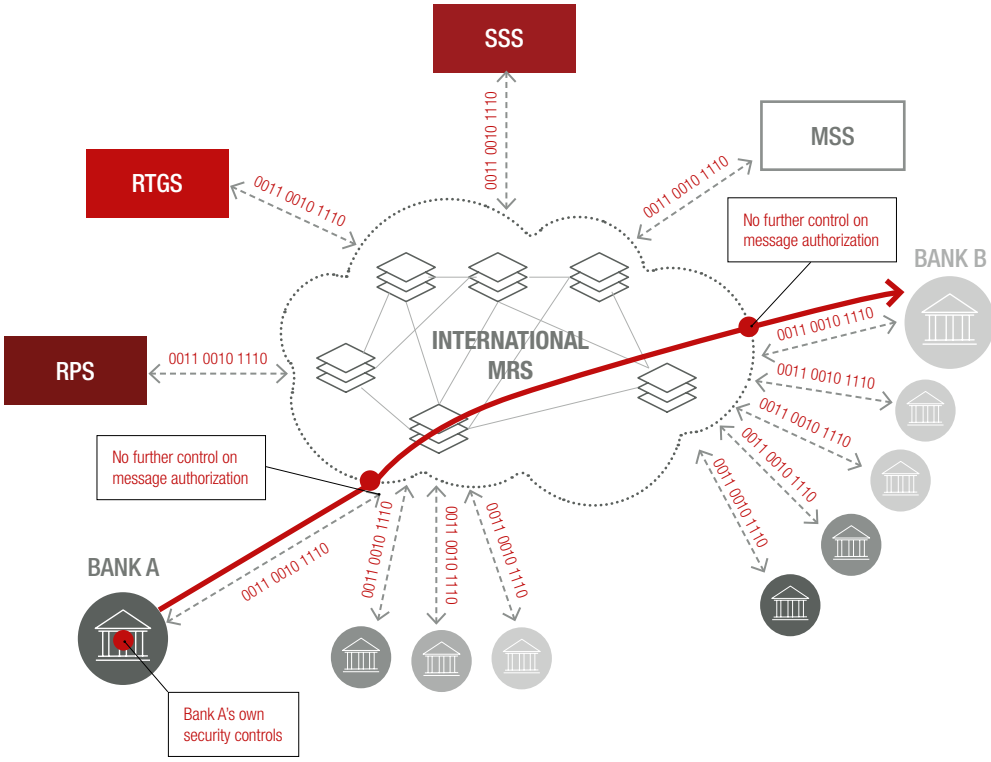
In the second half of the twentieth century, when electronic payment systems were created, all stakeholders (financial institutions, automated clearing houses (ACHs), settlement systems, and so on) were looking for a fast, automated, secure, easy, and low-cost way to operate their financial and commercial transactions. Hence, they set up infrastructures that directly connected financial institutions and operators (banks, ACHs, settlement systems, and so on) through some information and communication technical companies (service providers), mainly owned by the same banks. The answer – and

Figure 2: Role of MRS in the cross-border/international payment system



[2] SWIFT (Society for Worldwide Interbank Financial Telecommunication) is a Belgium-based cooperative society linking more than 11,000 financial institutions, including 193 central banks, in more than 200 countries. "In 1973, 239 banks from 15 countries got together to solve a common problem: how to communicate about cross-border payments. The banks formed a cooperative utility, headquartered in Belgium. SWIFT went live with its messaging services in 1977, replacing the Telex technology that was then in widespread use, and rapidly became the reliable, trusted global partner for institutions all around the world. The main components of the original services included a messaging platform, a computer system to validate and route messages, and a set of message standards. The standards were developed to allow for a common understanding of the data across linguistic and systems boundaries and to permit the seamless, automated transmission, receipt and processing of communications exchanged between users" (www.swift.com).

Figure 3: Messages flow through the cross-border/international payment system



the result – was a 'closed' system of financial entities (mainly banks or bank-owned entities), where a bank receiving a message from another bank could be sure of the authenticity of the sender and of the integrity of the message. The system's security architecture reflected the structural "trust" shared by the participants. As a consequence, once "in," there was no need to closely control messages flowing between participants, as the sender and the receiver trusted each other as well as their messaging and routing systems (trust paradigm).

For example, with regards to the cross-border interbank payment system where, as mentioned above, the MRS is provided by SWIFT, a payment message going from Bank A to Bank B is not subject to any other authorization control when entering/exiting the SWIFT network. Controls are eventually implemented only in Bank A's own infrastructure and completely rely on Bank A's ability to make its infrastructure safe (Figure 3).

3. PAYMENT SYSTEMS AND CYBERSECURITY

In recent years, several cyber disruptions in critical sectors have demonstrated that the scenario has completely changed.

Participants in payment systems, both at national and international level, are connected to the internet, and are, therefore, individually and collectively exposed to cyber risk.[3] Although the economic analysis of the cyber risk is still in the early stages (see Box 1), the new scenario and its embedded digital innovations are having a profound effect on the financial environment.

The role of technology in the provision of financial services is becoming paramount. Interconnections among operators in financial markets have greatly increased, due to widespread digitization. From the attackers' side,

[3] Cyber risk can be defined as the risk stemming from operating in cyberspace, a global domain within the information environment consisting of the interdependent network of information system infrastructures including the internet, telecommunications networks, computer systems, and embedded processors and controllers [NIST (2013)].

the incentives and reasons for violating the financial system are increasing as well. There is a wide range of motivations, for example: "hacktivists," who seek merely to disrupt activity; cyber criminals, motivated by financial gain; terrorists, aiming to cause political and financial instability; and "nation-state related actors" attempting to interfere with or gain access to sensitive information, or to cause systemic instability [CPMI (2014)]. Attackers are also using increasingly sophisticated and evolving tactics, techniques, and procedures (TTPs) to exploit potential weaknesses in the technology, processes, and people of financial institutions (e.g., advanced persistent threats – APT – which are driven by intelligence gathered on the potential victims through social engineering actions and then delivering malware into a company's IT systems). At the same time, the entry points through which a participant in payment systems can be attacked are multiplying and include counterparties, vendor products, and employee workstations. Moreover, through the payment systems, the financial sector provides services to other critical sectors; consequently, a successful cyber-attack against payment systems can have implications for/repercussions on the wider economy.[4]

[4] An insight into the cross-sector dimension of cyber threats and coordination amongst critical sectors (e.g., energy, telecommunications, and transport) is highly relevant from a policy perspective in order to implement an effective protection of cyberspace. This topic is on the G7 agenda and that of other international cyber working groups.

Open cybersecurity issues from an economic perspective

Despite the increasing importance of securing cyberspace in the digital age and the growing attention paid by the media to cybersecurity, the economic analysis of cyber risk does not yet appear complete. Further insights seem necessary both from macro – and microeconomic perspectives. Being related to the development of the internet and digital technologies, cybersecurity has been studied so far with reference to the theories of internet economics, which emphasize the role of externalities, price structures, costs, coordination failures, lock-in effects, and so on. It still lacks a more detailed analysis of cyber risk peculiarities (e.g., borderless and cross-sector) and emerging trends, such as the asymmetry and evolving nature of the cyber threats,[5] the scarcity of reliable and comparable data on cyber risks (vulnerabilities, number of attacks, costs of security, and so on), and the lack of coordination, cooperation, and shared tools to face cyber-attacks effectively.

Some general government commitments to foster an open, secure, interoperable, and reliable cyberspace[6] are a first step towards a more tailored and specific analysis of cyber risks. Authorities and operators, mainly in the U.S. after 9/11 [Kaplan (2016)], are already facing the widespread perception of **cyber insecurity** and its possible economic impacts, which could significantly reduce investment in technology, slow the pace of its adoption, and hamper trade integration in knowledge-intensive sectors, thus affecting economic growth [WEF (2014)]. In this context, although the financial authorities have started to tackle the problem with several forward-looking initiatives (see Box 2), the effectiveness of public responses to cyber-attacks are still under scrutiny: "We are extremely inefficient at fighting cybercrime; or to put it another way, cyber crooks (…) and their activities impose disproportionate costs on society: cybercrimes are global and have strong externalities, while traditional crimes such as burglary and car theft are local" [Anderson et al. (2012)]. Privacy, proprietary data, and national security concerns limit the type of information that can be exchanged, especially at the global level. This should be discussed, if for no other reason than because it puts the greater onus on individual participants.

In order to respond to the scarcity of available and reliable data, international authorities are promoting the development of common definitions and methodologies for collecting data on the technical characteristics of vulnerabilities and the economic impact of cyber-attacks, even in the well-developed financial sector [G7 (2016b)]. An important contribution to the economic evaluation of cyber risks comes from the OECD's studies on the possible insurance coverage for cyber risk, which should provide a means for companies and individuals to transfer a portion of their financial exposure to insurance markets [OECD (2017)]. Moreover, insurance markets and companies can potentially contribute to the management of cyber risk by promoting awareness, encouraging measurement, and providing incentives for risk reduction. According to the approach promoted by some international organizations [CPMI-IOSCO (2016)], cybersecurity requires an interdisciplinary and holistic approach, which, going beyond technology, encompasses governance, company culture, and business processes. Furthermore, recognizing the borderless and cross-sector nature of cyber threats makes it clear that cybersecurity is a matter of the ecosystem of each financial institution and of the whole financial sector. Consequently, cybersecurity requires a shared responsibility and a common endeavor on the part of important stakeholders, which amplifies the risk of coordination failures. Bearing this in mind, each entity must be deeply aware of the cyber risks that may come from, or that it may pose to, other connected entities. However, the Bangladesh cyber fraud (see below), as well as the more recent global cyber-attacks (e.g., the 2017 Wannacry and Petya/NotPetya attacks) that are based on targeting third-party partners to infiltrate organizations, shows that the effective handling of such unconventional and unprecedented risks requires a paradigm shift [Cœuré (2017)].

From a microeconomic perspective, an enrichment of the theoretical framework might come from a better understanding and knowledge of **governance approaches/practices on cybersecurity**.[3] In the U.S., the National Association of Corporate Directors (NACD) is promoting schemes for self-assessing the "cyber literacy" of boards; verifying the impact of cyber risk on enterprise-wide risk, compliance, risk management, staffing, and budgets; suggesting cybersecurity considerations during the M&A phases; and developing metrics and dashboards for making decisions [NACD (2017)]. From a policy perspective, the analysis of the proper (optimal) regulatory framework to foster cybersecurity requires a coordinated and balanced approach between different fields of regulation, such as financial stability, conduct, and privacy [Caron (2016)]. Moreover, the intense public/private cooperation, which seems to be needed to properly detect and manage cyber risk – according to some per sector/per country cases[8] – still deserves a thorough analysis in order to become an international standard.

[5] Compared with the threats facing traditional domains (air, sea, land, and space), cyber threats have the following inherent characteristics that make them severely asymmetric and more difficult to counter effectively: low entry cost (malware as a service), global accessibility (no physical boundaries), fast (micro-seconds), automatically and remotely controlled (i.e., remote command and control system of the botnets), and rapid evolution of threats in terms of diversification and sophistication (i.e., tactics, techniques and procedures use by threat actors).

[6] The concluding statement of the G7 Leaders' Summit of May 2016 reads: 'We strongly support an accessible, open, interoperable, reliable and secure cyberspace as one essential foundation for economic growth and prosperity" [G7 (2016a)]. Similarly, in G7 (2017) point 15.

[7] "Consistent with effective management of other forms of risk faced by a Financial and Market Infrastructure (FMI), sound governance is key. Cyber governance refers to the arrangements an FMI has put in place to establish, implement and review its approach to managing cyber risks (…) It is essential that the framework is supported by clearly defined roles and responsibilities of the FMI's board (or equivalent) and its management, and it is incumbent upon its board and management to create a culture which recognizes that staff at all levels, as well as interconnected service providers, have important responsibilities in ensuring the FMI's cyber resilience" [CPMI-IOSCO (2016), pages 1-2)]. See also, NBB (2017), pages 86-87.

[8] CERTFin, the Italian Financial Computer Emergency Response Team, a cooperative public-private initiative promoted by the Bank of Italy and the Italian Banking Association, aims to enhance the cybersecurity of the financial sector by providing services in the following main areas: information sharing and threat intelligence, cyber knowledge and security awareness, and incident response and crisis management.

In such an open and more hostile environment, financial entities can no longer presume to be in a safe, club-like,[9] isolated environment, since attackers, given their asymmetrical capabilities,[10] can overcome **any defense, at a system and individual levels**. This means that a paradigm shift, from "trust" to "resilience," is required. In essence, there is a greater onus to design and build secure infrastructure architecture and establish a comprehensive risk management framework. For this reason, some international authorities have already suggested that financial entities design their internal controls based on the assumption that defenses have been breached and attackers have already infiltrated the systems ["the attacker is already in" assumption; CPMI (2014)].

Following the "resilience paradigm," financial entities should manage cyber risk by taking into account at least three perspectives. Firstly, the timely detection and sound understanding of potential intrusions are essential enablers for enhancing an organization's response capabilities. Secondly, the security capabilities of any counterpart are an essential element of the framework. Finally, although counterparts could be perceived as reliable due to their application of security best practices, they could potentially be "penetrated by advanced and persistent adversaries" and should, therefore, not be deemed as a fully trusted entity.

The aforementioned assumptions are already embedded in leading international security standards and best practices, as well as in the recent approach and guidance of the international financial regulators and bodies. In particular, the National Institute of Standards and Technology (NIST) states in Principle 6: "Assume that external systems are insecure"; "an external domain is one that is not under your control. In general, external systems should be considered insecure. Until an external domain is deemed to be 'trusted,' system engineers, architects, and IT specialists should presume that the security measures of an external system are different than those of a trusted internal system and design the system security features accordingly" [NIST (2004)].

[9] Maybe this could be the last but most obvious step of a process that started many years ago with globalization.

[10] The asymmetry is due to attacking costs being lower than those for defending, as tools and malwares are available on the dark web and ready to use even for unskilled people (cybercrime as a service), crime imputation is very complex, and cybercrime regulation is uneven in different countries and attackers can operate from less regulated countries.

Payment systems – cyber initiatives

Given the critical role that financial market infrastructures (FMIs), including payment systems, play in promoting the stability of the financial system, the Committee on Payments and Market Infrastructures (CPMI) of the Bank of International Settlements (BIS) has sought to understand the current cyber risks faced by FMIs and their level of readiness to deal with worst case scenarios effectively [CPMI-IOSCO (2014)]. The CPMI and the International Organization of Securities Commissions (IOSCO) also agreed to act on cybersecurity by setting up the joint Working Group on Cyber Resilience for FMIs (WGCR) with a mandate to i) investigate the potential implications of cyber-attacks against FMIs, including the implications for financial stability; and ii) provide guidance both to authorities (regulators, overseers) and to FMIs to enhance the cyber resilience of the financial sector.

As a result of a detailed investigation into potential cyber risks for the financial system, the WGCR finalized its Guidance on cyber resilience for financial market infrastructures ["Cyber Guidance" – CPMI-IOSCO (2016)] in November 2015, which aims to instill international consistency into the industry's ongoing efforts to enhance its cyber resilience. In addition, the Cyber Guidance provides authorities with a set of internationally agreed guidelines to support consistent and effective oversight and supervision of FMIs in the area of cyber risk.

In accordance with these initiatives, local authorities are looking to improve the cyber resilience of payment systems. In Europe, for example, the Eurosystem's overseers have recently launched an Oversight Cyber Resilience Strategy for financial market infrastructures [ECB (2017)]. This strategy is built on three pillars: 1) cyber resilience of individual financial market infrastructures; 2) resilience of the financial sector as a whole; and 3) establishment of a forum that brings together market actors, competent authorities, and cybersecurity service providers [Cœuré (2017)].

Furthermore, the initiatives described are integrated with similar work by banking supervision authorities and, more generally, by financial system authorities. It is worth mentioning that the G7 countries have drawn up a set of fundamental elements of cybersecurity for the financial sector, as well as three further recommendations on the effectiveness of cybersecurity assessments, third-party risks, and coordination with other critical sectors [G7 (2016b)].

Moreover, The Financial Stability Board (FSB) highlighted the need to monitor cyber risk arising from financial technology (fintech), to identify the supervisory and regulatory issues from a financial stability perspective, and to mitigate the adverse impact of cyber risk on financial stability among the top three priority areas for future international cooperation [FSB (2016,2017)].

It should be said that there are differing views on the need to specifically regulate cyber risk. Those who argue against the need for regulation claim that given the evolving nature of cyber risk it is unsuitable for specific regulation and that cyber topics are already covered by existing regulations relating to technology and operational risk. On the other hand, it is argued that a regulatory framework is needed to deal with the unique nature of cyber risk, and with the growing threats resulting from an increasingly digitized financial sector.

Moreover, the discussion also concerns the optimal level of prescriptiveness, which could be achieved with a principle-based or a more prescriptive approach. In the first case, competent authorities should develop flexible supervision procedures in order to adapt to the rapidly changing cyber issues.

The "CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures" recommends that an FMI should identify the cyber risks that may come from, and that it poses to, entities in its ecosystem and coordinate with relevant stakeholders, as appropriate, as they design and implement resilience efforts with the objective of improving the overall resilience of the ecosystem[11] [CPMI-IOSCO (2016)].

Furthermore, the "G7 fundamental elements on cybersecurity for the financial sector" highlight that financial entities and authorities should take into account the interconnections and interdependencies in the ecosystem to design and assess effective cybersecurity controls both at the single financial institution and at sector level [G7 (2016b)].[12]

Referring again to Figure 3, in this new scenario, Bank B should not trust the message coming from Bank A, because Bank A belongs to an external domain, which should be considered insecure. No one can assume that the IT infrastructure of Bank A has not been compromised and that the payment message is in fact authorized.[13] Consequently, the payment message authorization should be checked somewhere in the flow of the SWIFT network or when it arrives at Bank B.

Summing up: payment systems and the main financial infrastructures were created on the basis of a trusted model where participants could exchange information through a sort of "closed" and secure IT environment. From a cybersecurity perspective, this is no longer true,

[11] The BIS and board of the IOSCO issued their cyber guidance in June 2016 to provide supplementary details related to the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities with the objective of limiting the escalating risks that cyber threats pose to financial stability. Although the guidance is directly addressed to FMIs, it broadly discusses the financial system or ecosystem, specifically noting that given "the extensive interconnections in the financial system, the cyber resilience of an FMI is in part dependent on that of interconnected FMIs, of service providers and of the participants."

[12] Element 3, Risk and Control Assessment, states that "in addition to evaluating an entity's own cyber risks from its functions, activities, products, and services, risk and control assessments should consider as appropriate any cyber risks the entity presents to others and the financial sector as a whole. Public authorities should map critical economic functions in their financial systems as part of their risk and control assessments to identify single points of failure and concentration risk. The sector's critical economic functions range from deposit taking, lending, and payments to trading, clearing, settlement, and custody."

[13] It means that the message could be sent by a cyber criminal on behalf of Bank A. A similar artifact message could be a fraudulent payment disposal or even potentially contain portions of a malicious code that could affect Bank B.

even if systems are still designed and implemented on the premise that all counterparties can trust each other.

Against this backdrop, all the participants in a payment system are potentially subject to a specific cyber risk (SCR), until a change in the system architecture is pursued and applied.

4. BANGLADESH BANK CYBER FRAUD

A relevant case study about the aforementioned topics is represented by the Bangladesh Bank (BB) cyber fraud, where cyber criminals exploited customers' IT vulnerabilities to gain unauthorized access to the SWIFT messaging system.

The SWIFT messaging system comprises a set of codes to standardize information across languages, an encrypted network across which messages are passed, and software that financial institutions use to send messages through the network. Its architecture was designed, as described above, assuming the "trust paradigm." Messages entered in the SWIFT network by an institution are considered trustworthy and passed to the addressed institution without any further security control (Figure 3).

In February 2016, the BB was the target of a significant cyber fraud,[14] which, among other things, caused its governor to resign.

After gaining unauthorized access to the BB's computers, criminals submitted several fraudulent payment orders through the SWIFT network from the accounts BB had at the Federal Reserve Bank of New York (Fed), for a total amount of U.S.$951 million. Though the majority of fake orders were blocked or recovered, the attackers succeeded in laundering U.S.$81 million from casinos in the Philippines.

The joint analysis of the BB and SWIFT, together with external consultants, showed that it was a large-scale APT (advanced persistent threat) cyber-attack, large enough to compromise the entire BB IT environment and lasted at least two months. The malware used would have also compromised the device for connecting to the SWIFT network (Alliance Gateway), thus enabling the transfer of funds from accounts at the Fed to accounts opened in the Philippines. Most relevant traces of these activities were deleted by the malware itself.

SWIFT immediately declared that the company had no liability for the incident, as the BB's IT environment was not adequately secure and was heavily compromised, allowing the attackers to take control of the SWIFT infrastructure at the bank. Nevertheless, SWIFT, in the interests of the financial community, delivered an "update" of its software to prevent the traces of transactions on the SWIFT network from being deleted on local computers, thereby assisting their customers in detecting this type of illegal activity.

In the months that followed, news about other similar cases appeared in the press. The frauds affected private financial institutions in Ecuador, Vietnam, and other countries in underdeveloped areas. At the time of writing this article, there is no certainty that these kinds of attacks are no longer affecting financial institutions [Constantin (2016), Finkle (2016)].

Given the occurrence of further similar cases, SWIFT launched a program to strengthen the security of the entire ecosystem connected to the SWIFT network. The SWIFT Customer Security Program (CSP) is based on three mutually reinforcing ideas: (1) financial institutions, considered the weakest link of the chain, will first need to protect and secure their local IT environment; (2) users will then need to enhance their capacity to prevent and detect fraud through their commercial relationships (i.e., with their counterparts); and (3) users will need to continuously share information and prepare against future cyber threats (the intelligence on the cases of cyber fraud is collected by SWIFT on behalf of the whole community).

The first part of the program requires the community of SWIFT users to implement a set of core security standards (16 compulsory and 11 optional security controls). They mainly relate to the user's security environment, access to its systems (including the adoption of multi-factor authentication), and the monitoring of unusual transactions on the basis of the behavior patterns of the participant.

The CSP also includes a set of enforcement measures through which SWIFT intends to monitor the effective

[14] The information about the Bangladesh Bank cyber fraud reported in this paper has been collected from a number of public sources, mainly press articles and the SWIFT website.

implementation of requirements from clients. The measures are mainly based on self-assessment and enhancing transparency measures, with supervisors being informed about the non-compliance of individual users. Drastic measures, such as the suspension of services to non-compliant banks, which could eventually lead to extreme consequences such as the interruption of operations, are not included in the program.

> "A paradigm shift, moving from "trust" to "resilience," should guide the building of the new security architecture and risk management framework."

According to the cybersecurity principles outlined in Box 2, SWIFT itself recognizes that it is also essential to prepare for the possibility that a direct counterparty has been breached, and that financial institutions may receive suspicious traffic over the SWIFT network that originates elsewhere.

For this reason, in the second part of the CSP, SWIFT suggests that financial institutions check that they are only doing business with trusted counterparties, using the SWIFT's Relationship Management Application (RMA), which supports customers by enabling them to control their counterparty relationships over SWIFT and by providing a pre-transaction check that prevents unauthorized receipt of transactions.

Finally, the third part of the CSP regards information sharing and intelligence as being paramount. The reason is that the financial industry is global, and so are the cyber challenges it faces. What happens to one company in one location can be replicated by attackers elsewhere. It is, therefore, vital to share all relevant information and to inform SWIFT if there is a problem, which is an obligation for all SWIFT customers. SWIFT's dedicated Customer Security Intelligence team has been introduced to help limit community impact by sharing anonymous information in a confidential manner about indicators of compromise (IOCs) and by detailing the modus operandi used in known attacks.

Moreover, SWIFT regularly informs its customers about important cyber intelligence, new market practices, and recommendations.

5. THE NEW PARADIGM

In general, although a counterpart can be considered trustworthy, because it is applying security best practices, it could still be potentially "breached by advanced and persistent adversaries," and should, therefore, not be considered as a potentially "risk free" counterparty (resilience paradigm).

As for any kind of risk, cyber risk needs to be managed with an appropriate risk management framework.[15] Given the evidence of an increasing likelihood of compromise, coupled with the potentially high impact of its occurrence (quite high likelihood-high impact), any form of risk acceptance should be excluded. At the same time, considering the evolving nature and peculiarities of cyber risks, avoiding it appears unrealistic. Therefore, only the following strategic approaches remain valid: transfer or mitigation, or a combination of both.

The first could simply consist of exploring the possibility for financial institutions to sign insurance contracts to cover the cyber risk stemming from other actors of the interbank payment system.

Regarding mitigation, the easiest action could be that the counterparties (the endpoints of the interbank payment system) should enhance their security defenses, through a set of security requirements, as is happening with the SWIFT CSP program. Once again, this approach is not enough in light of the new "resilience paradigm," where it is assumed that the "attacker is already in," no matter what the defense level is. Assuming that the attacker could overcome any kind of defense, the only measure for bolstering the endpoint security capability is equivalent to a residual risk acceptance, which, as we said, is not adequate in the case of a quite high likelihood, high impact risk.

Further mitigation actions should, therefore, be introduced, with the interbank payment system considered as an ecosystem and, above all, not only limited to its endpoints (i.e., banks):

1) Given its central role in the system and when considered as an active player, the MRS could be asked to implement a set of centralized controls on the authorization of messages flowing through the infrastructure.

[15] International standards propose four possible ways to manage risks: accept, mitigate, transfer, and avoid (see, for example, ISO3100).

2) An alternative, if the MRS is considered as a mere message carrier with a passive role, is that the message sender and receiver can be thought of as being directly and physically connected. In this case, it should be up to the receiver to implement controls on received messages. For example, exchanging acknowledgement messages with the sender, likewise in the case of securities transactions.

3) Each participant could be required to enhance their response capabilities in order to counter the potential frauds stemming from its payment system counterparts.

6. CONCLUSION

Interbank payment systems were designed on the basis of the "trust paradigm," due to the closed network environment where intermediaries were connected through secure and reliable IT services providers. In this context, all interconnected entities essentially trust each other and the cyber threats would mainly come from insiders (e.g., disloyal employees).

Due to the increasing digitization and openness of financial services within the internet, the paradigm has changed and cyber threats can arise from a broader number of financial and non-financial motivated threat-actors active on the internet 24/7 and capable of exploiting an increasing number of vulnerabilities and attack-vectors to achieve their goals (i.e., activists, cyber criminals, proxy-state, and nation–state actors). Financial entities can no longer assume that they are in a safe, club-like, isolated environment, since attackers are able to overcome any defense.

So far, despite the evolving environment (characterized by increasing IT consumerization, intensive digitization of the economy, and evolving cyber risk landscape), the security architecture of payment systems seems to have remained essentially the same, based on the "trust paradigm," which financial institutions rely on but at the cost of being exposed to **specific cyber risks (SCR)** for the entire financial community.

A paradigm shift, moving from "trust" to "resilience," should guide the building of the new security architecture and risk management framework. For this reason, some international authorities have already suggested that financial entities design their internal controls based on the assumption that defenses have been breached and attackers have already infiltrated their systems.

The most prominent example of the urgency regarding that shift is the BB cyber fraud (and other similar cases not solved yet), which involved financial institutions

and the international MRS, SWIFT. On several public occasions, SWIFT has claimed that its system was not actually directly compromised in any of the attacks, but this argument may be misleading. The system is no less vulnerable whether the attacks target its core infrastructure or the connections to it. Therefore, even when using a well-known, secure, and trusted network, like SWIFT, the financial institution receiving a message (which remains the only entity responsible for controlling message flows and protecting itself) should have a security framework in place to protect itself, as if it were exposed to a potentially hostile environment.

Against this backdrop, the implementation of the cybersecurity controls included in SWIFT's Customer Security Program as mitigation measures for the SCR may not be enough for a number of reasons. Firstly, because the enforcement may not be easy to achieve in the short term.[16] Secondly, because it is not completely clear who will guarantee the financial entities' compliance and how, and above all because the system will continue to rely only on the previous "trust paradigm."

Regulators and supervisors should seek effective approaches to cope with the new scenario. In particular, further investigations are needed to explore potential actions and to find feasible solutions for the proper management of the SCR, both in terms of transferring and mitigating it. In this context, a detailed analysis of the role of MRSs should be carried out, as they could be considered an active part of the entire interbank payment system or a technological infrastructure, at the very least. Finally, the current regulatory frameworks and supervisory approaches, although successful in fostering an awareness of cyber-related issues, should be evaluated and eventually revised to verify whether they fit with the SCR or whether they need additional requirements.

REFERENCES

Anderson, R., C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, and S. Savage, 2012, "Measuring the cost of cybercrime," working paper, https://bit.ly/2DHTokO

Biancotti, C., 2017, "Cyber-attacks: preliminary evidence from the Bank of Italy's business surveys," Occasional Papers 373, Bank of Italy, https://bit.ly/2S7xrUD

Biancotti, C., R. Cristadoro, S. Di Giuliomaria, A. Fazio, and G. Partipilo, 2017, "Cyber-attacks: an economic policy challenge" in VOX CEPR's policy portal, https://bit.ly/2G9Qxmq

BIS-BIOSC, 2016, "Guidance on cyber resilience for financial market infrastructures," Bank for International Settlements and Board of the International Organization of Securities Commissions June 2016

Caron, F., 2016, "Cyber risk response strategies for financial market infrastructures," in NBB Financial Stability Report, 171-185

Cœuré, B. G. 2017, "Remarks by Benoît Cœuré, Member of the Executive Board of the ECB, at the High-Level Meeting on Cyber Resilience," European Central Bank, Frankfurt am Main, June 19, https://bit.ly/2WtQurp

Constantin, L., 2016, "Up to a dozen banks are reportedly investigating potential SWIFT breaches," CSO, May 27, https://bit.ly/2RofzjS

CPMI, 2014, "Cyber resilience in financial market infrastructures," Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions, November, https://bit.ly/2z3BWGa

CPMI-IOSCO, 2016, "Guidance on cyber resilience for FMI," Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions, June

Crisanto, J. C., and J. Prenio, 2017, "Regulatory approaches to enhance banks' cybersecurity framework," FSI Insights on policy implementation no, 2, Financial Stability Institute, August 2, https://bit.ly/2vidrzK

ECB, 2017, "Cybercrime: from fiction to reality. Ensuring cyber resilience in financial market infrastructures in Europe," European Central Bank, June 19, https://bit.ly/2FW0MeN

Finkle, J., 2016, "SWIFT discloses more cyber thefts, pressures banks on security," Reuters, August 31, https://reut.rs/2Se0wMe

FSB, 2016, "Financial Stability Board agrees 2017 workplan," Financial Stability Board, press release, November 17

FSB, 2017, "Financial stability implications from FinTech: supervisory and regulatory issues that merit authorities' attention," Financial Stability Board, June 27

Danielsson, J., M. Fouché, and R. Macrae, 2016, "Cyber risk as systemic risk," in in VOX CEPR's policy portal, https://bit.ly/2DHKAvv

G7, 2016a, "Leaders' declaration," Ise-Shima, May, https://bit.ly/2sRZLMI

G7, 2016b, "G7 fundamental elements of cybersecurity for the financial sector," October, https://bit.ly/2CTSzUF

G7, 2017, "Leaders' communique," Taormina, May, https://bit.ly/2rQxQKS

Kaplan, F., 2016, Dark territory. The secret history of cyber war, Simon & Schuster

NACD, 2017, "Cyber risk oversight," National Association of Corporate Directors, Directors Handbook Series, Washington, January

NBB, 2017, "Enabling technologies in FMIs and payment systems," in The financial market infrastructures and payment services report, National Bank of Belgium, Brussels

NIST, 2004, "SP 800-27 Rev A, Engineering principles for information technology security (a baseline for achieving security)," Revision A, Recommendations of the National Institute of Standards and Technology, June

NIST, 2013, NISTIR 7298 Rev 2, Glossary of key information security terms, May

OECD, 2014, "Measuring the digital economy. A new perspective," Organization for Economic Co-operation and Development, Paris, https://bit.ly/1p5B7CP

OECD, 2017, "Supporting an effective cyber insurance market," OECD Report for the G7 Presidency, Organization for Economic Co-operation and Development, Paris

Westby, J., 2012, "Governance of enterprise security," CyLab 2012 Report, Carnegie Mellon University, May 16

WEF, 2014, "Risk and responsibility in a hyperconnected world," World Economic Forum, Washington, https://bit.ly/1dYeLMZ

[16] Users will self-attest against the SWIFT security controls during 2017, and only in 2018 will SWIFT mandate a sample of its users to demonstrate this self-attestation with confirmation from an internal or external audit. This sample will be used to ensure the quality of the self-attestation process, and will look for structural/framework issues such as common difficulties in interpreting a specific control.

HAS "ECONOMICS GONE ASTRAY"? A REVIEW OF THE BOOK BY BLUFORD H. PUTNAM, ERIK NORLAND, AND K. T. ARASU[1]

D. SYKES WILFORD | Hipp Chair Professor of Business and Finance, The Citadel

ABSTRACT

This review is intended to highlight the major contribution that the new book by Blu Putnam, Erik Norland and K. T. Arasu, titled Economics Gone Astray, has made to our understanding of economics. A deeper understanding of the role that simplifying assumptions play in economic modeling (and thus the periodic disconnect from reality of the models in practice) is essential if "thinking like an economist" continues to be a badge of respect, not a comment of derision. The challenges of not appreciating the simplifying assumptions, especially those that involve feedback loops and unintended consequences, are exactly the issues Putnam, Norland, and Arasu are addressing in this book. They learned the hard way in the marketplace, not of ideas, but the marketplace of reality. Their experience permeates the book and helps address this fundamental problem that we have in economics. It is an essential read for those who have an interest in the subject, and value how it helps its students develop their thinking in a logical manner.

During my second year as a graduate student, my eventual dissertation advisor asked, "When will you start thinking like an economist?" It probably took me another two years to grasp the power of this question. Economics, in specific macroeconomics and monetary theory, provided a methodology – a set of logical ways of thinking – that would prove necessary (more than just useful) to my career in the City, on Wall Street, as well as in the classroom. For this training, I am grateful. Those educated in the dark arts of economics – well dismal arts – tend to be more analytically consistent and objective, whether those arts are applied in financial markets, the policy arena, or the classroom, than those who avoided the dismal science.

In order to be consistent and orderly in our analysis, however, many of us often fall back on crutches created to quickly analyze problems, even if these crutches may not be applicable in a more dynamic marketplace (or economy). In fact, we economists, in our desire to make models that fit our view of the world – mathematical elegance over understandable (or for many of us, profitable) results – often ignore the implicit assumptions necessary for those models to work out so elegantly. And in many cases, it is those assumptions that are the interesting aspect of analysis that separates the successful analysis, or policy, from those that simply lead to failures. All too often, we like to jump to a model that is easily generated, especially with cheap computing power available, rather than ask the hard question: do the assumptions implicit in our models hold? Or, how dangerous is it to apply this model's projections if the assumptions imbedded in it do not hold?

[1] Putnam, B. H., E. Norland, and K. T. Arasu, 2019, *Economics Gone Astray,* World Scientific Publishing Company

Or, is the power of a generally agreed upon proposition really in the assumptions needed for it to be useful at all?

To this last point consider the analysis of the capital structure of a firm and the Modigliani-Miller (M&M) theorem.[2] To simplify the theory, the model made some heroic assumptions, such as no taxes, no transactions costs, similar borrowing terms for investors and companies, and the same information available to investors and companies. As Professor Clifford Smith of the University of Rochester taught me, the key is to understand the assumptions that make the M&M model useful. Without understanding when an assumption is broken, one cannot truly understand many of the actions taken to change the capital structure of a firm. This is a lesson that we often ignore in other areas of economics, especially in macroeconomic modeling.

> "Make the mistake (of fitting a model while ignoring reality) once and one gets a second chance. Make it twice and you are fired!"

Over and over in the my own career, I have found that the assumptions behind the models we were applying, whether to forecast foreign exchange rates (one of my first jobs), or to analyze the impacts of a devaluation (my first set of disagreements with my bosses at the Federal Reserve Bank of New York, my first job as an economist), or to understand this new market called "swaps," or to understand why I was losing money in a trading book when I thought I had all of the models correctly estimating the outcome (oil swaps business) were broken. And, maybe my favorite is how I learned that most of the applied Markowitz portfolio models were often totally inconsistent with the underlying theory (if you ignore enough of the model's inherent assumptions, there is no wonder outcomes seem not to fit reality); sadly, I had to learn the hard way.

The challenges of not appreciating the simplifying assumptions, especially those that involve feedback loops and unintended consequences, are exactly the issues Putnam, Norland, and Arasu are addressing in their book. They learned the hard way in the marketplace, not of ideas, but the marketplace of reality. Their experience permeates the book and helps to address this fundamental problem that we have in economics.

To paraphrase the old adage, economics education "giveth and taketh away." It gives us a truly wonderful way to make rational decisions, but reliance on modeling (yes, an essential part of what it means to be an economist) often causes us to miss the critical elements, often buried in assumptions, that will make our decision useful or lead to unintended consequences. Look no further than the 2008-09 financial crisis or the on-going Greek debt crisis, or any number of historical mind-numbing crises that provide ample examples of unintended consequences of "good analysis."

Economics Gone Astray sets the stage in the first paragraph of the introduction. To quote: "We cut through the assumptions that economists often employ and how many traditional practices often lead them woefully astray." Indeed, the authors have designed this book to provide explanations of reality, like the good economists that they are, when that reality does not coincide with what one might expect from his or her favorite model. Yes, we all have our favorites and as all good economists we will fight tooth and nail with reality to prove we were right all along. For the macroeconomist that is tuned to the market, it makes little sense to argue with reality, but rather it makes more sense to try to understand why that reality did not fit with the one predicted by our models. Make the mistake once and one gets a second chance. Make it twice and you are fired!

The book brings home lessons about many issues that we simply ignore all too often in our analyses, such as noted in Chapter 13 "Death by simulation." Economists use back-tested simulations to demonstrate how their investment strategies might have worked in the past. Often these simulations, based on elegant models, provide answers that work for a while, even in the real world, before blowing up.

In the classroom, we tend to introduce students early to these modeling techniques, sometimes ignoring the necessary conditions (underlying assumptions) of our models. It is one of the great dis-services that a teacher can make. Admittedly, I did not teach an introductory course for many years. I did not want students to discuss policy without understanding the necessary conditions for the economy to function in the first place.[3] One need

[2] Modigliani, F., and M. Miller, 1958, "The cost of capital, corporation finance and the theory of investment," American Economic Review 48:3, 261–297

[3] In all fairness I believe many of the newer "introduction to economics" texts do stress, at least to some degree, basic issues such as property rights, rule of law, contract law, etc. before constructing simplified models.

go no further than to observe politicians, some touting a major in economics, making statements that sound as if they learned nothing at university. They probably remember their favorite model that yielded their chosen suggested policy prescription, without ever understanding when that policy prescription was useful and when, well, silly. There may be no hope for those we half-educated, but there is hope that we do a better job in the future. *Economics Gone Astray* is a big step toward that goal. Solving this fundamental problem in our profession is essential. The book makes economics real and practical to the student by focusing upon the dynamic nature of markets and economies, while putting theory (and results) into perspective. It moves discussion from jargon to explanation, by adapting many of the practices that market economists find essential to do their jobs.

> "There may be no hope for those we half-educated (in classroom economics), but there is hope that we do a better job in the future. Economics Gone Astray is a big step toward that goal."

The authors do not intend for their book to replace the textbook, which is essential to moving a student to the next stage of "thinking like an economist." Rather, it is a tool to be used in conjunction with the normal text in order to highlight the economics of a dynamic world. This is a world in which politics are not stagnant, complex institutional arrangements are variable, demographic changes disrupt the economic environment, global trade agreements are dynamic, new complex financial instruments are created almost daily, and markets are defined by a process of scratching for any advantage (efficiency). These are the factors we truly love about free markets, but these are also the factors that we sometimes ignore to make our macro models seem coherent over time.

As one of my favorite economists, who will remain nameless, stated: "when you make it up (forecast), do so to the 5th decimal." *Economics Gone Astray* argues that such precision is too often the case; we do the math, make the forecast or policy or pronouncement, but forget that these models actually believe us. It "thinks" we have considered all of those other issues that we had to assume away in order that our forecast is to the 5th decimal point. GIGO (i.e., garbage in, garbage out) is rampant in what economists do.[4] To this point, remember how safe collateralized debt obligations (CDOs) were shown to be under the assumptions that best fit the needs of the regulations in 2007 and how wrong those models were in 2009. Most of those regulations, and accepted models, were designed in response to a crisis where the models of the day were deemed inadequate. And yes, those original, deemed inadequate, models were needed since the ones they replaced were found to be inadequate and so on. One of the areas where (quant trained, mathematical) economists are in demand is in the area of risk management. Why? We seem to get it wrong time after time and consequently build bigger and better mathematical models to explain what went wrong before and why it will not go wrong this time. Yes, just one more chance to get it right before the next crisis![5]

Economics Gone Astray provides the macroeconomics teacher a tool to discuss some of the realities as the models of the classroom are actually applied to the economy. Discussions of inflation, not from one model or another's perspective, but per the reality of a dynamically changing economy where even the meaning of money changes. Does that mean Fisher's equation of exchange, 6 MV=PT, is dead? No, but it does mean we have to think differently about the implications of the power of the Fed to finetune an economy or even to generate inflation. It certainly does not mean we ignore the lessons taught to us by Milton Friedman and Anna Schwarz,[7] but to the contrary we need to understand those lessons in today's context; today the marketplace is global, and financial markets are dynamic and ever changing. Or, how can we

[4] In the Introduction to *Economics Gone Astray*, the authors discuss the words of the great Professor Alfred Marshall, Mary Paley's Professor of Political Economy at Cambridge University, who wrote the best-selling economics text of his time (late 1800s, early 1900s). The quote is worth repeating here: "But I know I had a growing feeling in the later years of my work at the subject that a good mathematical theorem dealing with economic hypotheses was very unlikely to be good economics: and I went more and more on the rules: (1) Use mathematics as a short-hand language, rather than as an engine of inquiry. (2) Keep to them till you have done. (3) Translate into English. (4) Then illustrate by examples that are important in real life. (5) Burn the mathematics. (6) If you can't succeed in 4, burn 3. This last I did often."

[5] Personally, I love to teach the history of financial risk management; doing so allows one to show all of the mistakes that have led to the latest and greatest model, which we will gladly teach to the latest group of students. Hopefully this lesson will not be lost on them as they learn the math and models they must know if they are to call themselves risk managers.

[6] Fisher, I., 1911, The purchasing power of money, Augustus M. Kelley Publishers

build productivity models without understanding structural changes? What policies work and do not work to spur productivity in a dynamic economy? They are unlikely to be the same ones that worked 20 years ago.

One of my favorite chapters in the book is the one that discusses the impacts of demographic changes on the integrity of our forecasting. Ignoring the demographic realities often lead to policies that are counterproductive and forecasts that are simply wrong. The focus here is on the long-term implications of changing demographics, the implications of rural to urban movement of people for growth (and the implications for immediate increases in productivity), and the reality of a declining labor force in many advanced countries. Forecasters have to understand this reality. With a zero (or negative) population growth, should one expect Japan to grow at 3% a year? Should we expect macroeconomic policies of the 60s, so successful in Japan of the 1960s through the 1980s, to succeed today? Ignoring this in our classrooms, which most textbooks do, will leave the economics student only half-educated (and often totally bored).

There is even a chapter on machine learning, which explains why it will be much more difficult to build a successful financial model with artificial intelligence than just matching faces, recommending a book, or beating a human at chess. The challenge, compared to winning chess, for example, is that one cannot ignore the feedback loops in how markets function, where each action by a market participant gets a reaction. Different players have different objectives, the rules change often, and some players cheat.

For students to become engaged in the discipline it must be made interesting and geared to the reality they are experiencing. *Economics Gone Astray* is designed to do just that. It brings alive analysis of issues faced today. Connecting theories and models to reality in forecasting and analysis is essential if we as a profession are to keep the next generation of students engaged. The chapter on "Bitcoin economics" touches something all students want to understand. Or, a discussion of volatility and uncertainty can highlight the issues that the student will face when trying to apply the modeling techniques that arise in a basic portfolio theory course. Many of those courses will not differentiate the concepts and will ignore the assumptions behind models, going straight to the models. For example, finance classes often focus on the mathematics and modeling. As usual, that activity can completely miss the assumptions implied in the models. In chapter 9, **Volatility and uncertainty,** the theme is to appreciate that volatility may not measure risk appropriately and uncertainty may not create volatility. The chapter highlights an issue that economists should focus upon, but often conflate, when making simplifying assumptions.

Make a concept interesting and the student will somehow store that information for when it is needed. Connecting economics to reality excites students in a way that theory alone cannot. Two more chapters that are essential reading for any student who reads the Wall Street Journal or The Financial Times are Chapters 15 and 16. Chapter 15 highlights the different approaches taken by the Federal Reserve and the European Central Bank for dealing with the financial panic of 2008, a topic for every macro class, but one in which the key assumptions are often overlooked even though they are critical to understanding the pros and cons of quantitative easing. Chapter 16 tackles one of the more widely discussed issues in today's marketplace: prescriptions for Fed policy. Just listen to CNBC almost any day to hear both the dual mandate and/or the Taylor Rule discussed. In *Economics Gone Astray*, the Taylor Rule is analyzed using a Bayesian approach, turning it from a fixed approach to a dynamic one for policy analysis.

For those of us who believe that we live in a dynamic economy, these last two chapters punctuate the real issues that economics faces. Tom Sowell, Senior Fellow at the Hoover Institution, Stanford University, brought this home when discussing his basic economics course as a student; to paraphrase, "and then what happens" once a policy is implemented, not so much on the first round but the resulting, (unintended) consequences of the policy as it fully plays out in the economy.[8] *Economics Gone Astray* makes the dynamic factors at play in an economy come alive not only for the student, but also for those of us who get stuck in a general equilibrium rut. This book is strongly recommended for those of us who want to bring our profession to life once again. Why? Because thinking like an economist is important. We just need to think dynamically!

[7] Friedman, M., and A. J. Schwartz, 1963, A monetary history of the United States, 1867-1960, Princeton University Press

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO