The future of raising finance - a new opportunity to commit fraud: a review of initial coin offering (ICOs) scams

Tiwari, Milind; Gepp, Adrian; Kumar, Kuldeep

Published in:
Crime, Law and Social Change

DOI:
10.1007/s10611-019-09873-2

Published: 01/05/2020

Document Version:
Peer reviewed version

Licence:
Other

The future of raising finance - A new opportunity to commit fraud:

A review of Initial Coin Offering (ICO) scams

Abstract

Over one billion US dollars were invested in blockchain in 2016. The potential application of blockchain extends far beyond cryptocurrencies. One use of blockchain is an Initial Coin Offering (ICO), a digital method of raising finance involving issuance of tokens in exchange for cryptocurrencies or fiat money. It is a cheaper, easier and quicker way to raise funds compared with traditional public offerings. However, it has raised a new opportunity for fraud. An estimated ten percent of ICO funds have been lost to fraud. Using case-study analysis, this study determines characteristics of such fraud schemes and the regulatory changes made in response to them. The study reveals key lessons for investors in terms of proactive steps that can be taken to protect themselves from being victims, for issuers to ensure awareness and take steps to secure investors' trust, and for regulators to promote a safe environment. To the best of our knowledge, this study is the first to document the effect of ICO fraud schemes on the regulatory environment, which is going through a series of amendments to provide protection against such fraudulent schemes. Additionally, it provides direction for future research to further investigate the risks of this new method of raising funds.

This is a post-peer-review, pre-copyedit version of an article published in Crime, Law and Social Change. The final authenticated version is available online at: http://dx.doi.org/10.1007/s10611-019-09873-2.

1. Introduction

More than one billion US dollars have been invested in blockchain technology in 2016 because of potential benefits that the technology may provide (Kennedy 2016). The potential application of blockchain extends far beyond cryptocurrencies. The innovation and prominent use of blockchain technology has given birth to a new way of raising finance known as the Initial Coin Offerings ("ICOs" or "ICO"). This new method is a cheaper, easier and quicker way to raise funds compared with traditional public offerings. In an ICO, the issuer issues tokens to investors in exchange for other cryptocurrencies or fiat money during a specified time frame, sometimes to raise funds for development activities pursued by the issuer. The issued tokens will facilitate owner-access to services provided by the issuer, or may be used as an independent virtual currency. The investment in an ICO does not grant ownership in the company, as is the case in an initial public offer (IPO), but is considered an investment in a virtual product which is likely to appreciate in the future. The appreciation is based upon investment in the technology provided, growth of business and increased demand for the virtual product being offered.

An ICO should not be confused with crowdfunding. Crowdfunding facilitates solicitation of investments or donations by providing a platform to leverage the geographical and social reach of the internet to connect fundraisers to a vast number of potential supporters (Fleming and Sorenson 2016). The two methods of funding may appear similar, but they have important differences. In terms of accessibility, crowdfunding is generally limited to a certain country or to regions, whereas ICOs are accessible to a wider range of investors. In terms of product, ICOs generally fund technology-related products while crowdfunding may span various categories such as hardware, software, technology and food. However, in recent times, ICOs have expanded beyond technology offerings. Differences also exist in relation to crowdfunding and

This is a post-peer-review, pre-copyedit version of an article published in Crime, Law and Social Change. The final authenticated version is available online at: http://dx.doi.org/10.1007/s10611-019-09873-2.

ICOs related to their regulations; the regulations related to ICOs and their evolvement will be briefly discussed in this paper.

The excitement around other cryptocurrencies and the urge to be part of something innovative has led to a surge in raising funds through an ICO, particularly by tech start-up firms. In 2017, an amount close to four billion US dollars was raised through ICOs (Ernst & Young 2017). This method of raising funds did not require compliance with securities regulations and hence provided a way to avoid compliance costs. This made it easier to pursue business development activities, especially for start-ups. There is no doubt this new way of raising finance is creating new opportunities, but at the same time it has provided an opportunity to commit fraud. The frenzy around ICOs and lack of due diligence before investing in them provides an opportunity for fraudsters to easily carry out their operations as is evident from the fact that more than ten percent of funds raised through ICOs have been lost to fraud (Ernst & Young 2017). Consequently, it is essential to examine the modus operandi of these large-scale fraudulent schemes to protect investors from falling prey to such schemes in the future and losing their hard-earned money. Additionally, it is necessary to be able to distinguish between potential fraudsters and genuine firms seeking to raise funds so as not to stifle the growth opportunities presented by this new fund-raising method. These modi operandi will remain a source of reference for regulators to enhance the regulations surrounding such means of raising funds.

Research makes it clear that the risk posed by terrorism used to be underestimated as was the scale and extent to which it could affect people (Kotabe 2005). A proactive approach towards ICO frauds might help prevent repeating the mistake committed in the case of terrorism. Consequently, the primary objective of the paper is to analyze the instances of ICO frauds to determine the characteristics of such schemes. An analysis was conducted on cases available in the public domain. There are plenty of smaller, alleged ICO scams, but there is often little information about these and the reliability of the information that is available is questionable.

This problem doesn't exist with cases that government authorities are involved with and so they are the focus in this paper.

It is essential to understand the regulatory environment and the historical changes that have taken place, as different countries have different regulations and what may be considered illegal in one country may be acceptable in others (Kshetri 2005). These differences provide opportunities to perpetuate fraud. Hence, the second objective of this paper is to cast light on the regulatory steps taken in different jurisdictions about ICOs and what is the current regulatory stance concerning ICOs. The jurisdictions covered in this paper represent those in which either a clear regulatory position has been taken or in which meaningful ICO activity, in terms of the amount of funds raised, has taken place. The information provided can inform both issuers and investors of the country-specific regulatory developments in which an ICO is being offered and the extent to which the offering is compliant with existing or possible future regulations. The motivation is to aid genuine issuers in avoiding the cost of non-compliance and for investors to check the degree of compliance of an ICO being offered, and to some extent determine its legitimacy and security of the funds being invested. The provided discussion can also inform future policy discussions relating to this emerging field.

The blockchain technology, because of its essential feature of virtual immutability, is being brought to use in a wide range of fields such as supply-chain and logistics, financial data verification and real-time updates of financial information, among others. It has also provided a unique opportunity for firms to raise funds via ICOs to finance their operations. As mentioned above, ICOs differ from other methods of raising funds in terms of accessibility, cost, time efficiency, projects funded and regulations involved. However, the benefits of ICOs come at the cost of creating a new opportunity for perpetuating fraudulent activities. To the best of our knowledge, this study is the first to document the effect of ICO fraud schemes

This is a post-peer-review, pre-copyedit version of an article published in Crime, Law and Social Change. The final authenticated version is available online at: http://dx.doi.org/10.1007/s10611-019-09873-2.

on the regulatory environment, which is going through a series of amendments to provide protection against such fraudulent schemes.

The paper also contributes to the literature by providing key insights for the concerned stakeholders (issuers, investors and regulators) to help them be proactive in countering ICO fraud. Proactive methods are outlined for investors to protect themselves. Information is provided for issuers to ensure awareness and to help them take steps to secure the trust of investors. Finally, insights are provided for regulators to aid them in providing a safe regulatory environment.

The paper is organized as follows: the section on blockchain provides an insight into the technology upon which ICO is based, along with its various uses and current application. This is followed by an introduction on ICOs and the regulatory steps taken in meeting the country-specific regulations. The paper then analyzes four cases of ICO frauds, namely, AriseBank, RECoin and Diamond Reserve, PlexCorps and Benebit, to analyze their respective modus operandi in cheating the investors. Finally, the paper provides key insights for investors, issuers and regulators, followed by conclusions and potential implications.

2. Blockchain

One of the major technological revolutions of the 21st century has been the blockchain. A blockchain can be described as a digitalized version of a ledger which is decentralized and distributed among the users of its peer-to-peer network (Underhill 2018). In simple terms, it can be understood as a text file which records events – for instance, transactions through consensus among participants of the network with no involvement of an intermediary.

The blockchain comprises a chain of blocks which essentially are a record of all transactions that have taken place in its network. This aggregation of transactions in units called *blocks*

and their addition to similar existing *blocks* in a chain takes place through a cryptographic technique composed of what is called a *Proof of Work* (Sullivan and Burger 2017). *Proof of Work* is the mathematical procedure used to authenticate and validate transactions, and to add new blocks of transactions in a blockchain. The mathematical procedure in a blockchain network is performed by nodes called *miners* and the act of using this mathematical procedure is termed *mining*. Once a transaction is *mined*, a solution is produced called a *hash*. This is demonstrated in Figure – it has three blockchains; each hash is verified by a comparison to the corresponding hash in the other blockchains. In this case, all hashes are consistent in each blockchain and so all are valid. In practise, there would be a much larger number of blockchains distributed throughout the entire network, which is why blockchain is known as 'distributed ledger technology' (DLT). The other simplification made in Figure 1 is that the *hashes* are two-digit numbers, when in reality they are very long and complicated. It is important to notice that the *previous hash* matches the *new hash* of the previous block. For example, Block 3's *previous hash* of 34 matches the *new hash* from the previous Block 2, which is another level of validation. That is, each block contains information from both previous blocks and the current event, and the integrity and authenticity of each item is checked against previous events. Since the hash value of the previous block is part of the computation of the hash value of the current block, it provides assurance about transaction history and saves time in verifying and tracing transactions to their source.

- **Fig1** Example of Working Blockchain Network[1]

When, any transaction or event takes place on the blockchain the ledger gets updated for all users. That means in case of inaccuracy the *hash* solution produced will not match the *hash* in other blockchains in the network, which will result in it and future blocks on that chain becoming invalid, as demonstrated in Figure 2. In this case, consider that a hacker changed the amount from $20 to $30 in Block 2 of Blockchain 1. This results in a hash of 89, which is

different from 34, the corresponding *hash* in the other blockchains in the network. Consequently, Block 2 in Blockchain 1 is invalid, which automatically invalidates all future blocks as well (Block 3 in this case). Thus, a hacker can't successfully change only one blockchain, because the rest of the network will realize the data have been corrupted.

- **Fig2** Example of Hacker Modifying Block 2 of Blockchain 1 from Fig1

Blockchain can be broadly classified into two types, namely, public or open blockchain, and private or closed blockchain. A private blockchain is a closed network and requires permission for access to the network and therefore it limits access to those who are thought to be known and trusted. On the other hand, a public blockchain does not require any sort of permission to access the network. Consequently, anyone can have access by downloading and running the software required for the network (SEC 2018).

One such example of a public blockchain is the Bitcoin, a virtual currency which facilitates transactions among its users in absence of a central intermediary, that is, without a financial institution. Anyone can join the network by downloading the Bitcoin software and participate in the network. The blockchain of Bitcoin is updated when its participants validate a particular transaction. It is important to understand that Bitcoin is just one example of a currency that uses blockchain. There are numerous others such as Bitcoin Cash, Ether, Litecoin, Tether and so on.

A version of electronic cash was proposed by Satoshi Nakamoto in 2008 that uses blockchain in the absence of a financial institution (Nakamoto 2008). He proposed a way to avoid reliance upon trust by facilitating the use of coins authenticated by digital signatures and avoiding the problem of double-spending by recording the history of transactions immune to being changed. The proposed system will be protected from an attack if the majority of participants in the network do not want the attack. Nakamoto's proposal was based on

This is a post-peer-review, pre-copyedit version of an article published in Crime, Law and Social Change. The final authenticated version is available online at: http://dx.doi.org/10.1007/s10611-019-09873-2.

individual interest being collectivized and need for changes to be incorporated through a consensus rather than top-down hierarchical approach, using the network of participants to validate an event.

The main features of blockchain technology can be identified in terms of its decentralization and encryption. It is depicted through its reliance upon its network of participants rather than a central authority and the ability for anyone to access the network and view the event at any time. And the use of encryption in maintaining security of record of transactions allows the technology to have a variety of uses.

2.1 Uses of blockchain technology

Blockchain technology has uses beyond financial transactions. Businesses are interested in ways to improve the accuracy and reduce the costs related to the hiring process (Moore 2017). Blockchain can be used by a human resource department for selecting better employees through having access to a wide variety of information about candidates that is known to be authentic and immune to tampering (Catalini and Gans 2017). The data related to potential candidates would be stored in a virtual database that could be queried by human resource departments to obtain an authenticated pool of candidates meeting the required criteria. Additionally, job seekers would be able to exercise control over sharing of their personal data.

Financial data related to companies could also be verified using blockchain-enabled databases that are accessed through the entity's website. As it is with real-time updates provided for bank account transactions, corporate financial information could be provided in real time (Gepp et al. 2018). The incorporation of blockchain technology could provide real-time verification in this process. It would provide transparency to financial statements and even highlight off-book transactions and accounts which are hidden (Tapscott and Tapscott

2017). This would represent a big step forward in addressing the problem of financial statement fraud, the cost of which has been estimated at more than 1.2 trillion US dollars worldwide (Gepp 2016).

The ability to provide real-time information updates through blockchain technology can also be utilized in legal matters, especially related to patent law where the timing of getting an idea recorded becomes essential. Real-time updates are also relevant to the logistic industry to facilitate tracking supplies of numerous parts in an efficient manner (Mansfield-Devine 2017). The maritime trading systems are plagued by security concerns relating to supply-chain issues (Barnes and Oloruntoba 2005); blockchain could serve as a solution to this problem.

Blockchain technology can also be applied to contractual agreements, both short-term and long-term in nature. Furthermore, the technology can be used by companies to interact with customers on an individual basis to market their products. The data related to customers would be under their control and it would not be possible for companies to profile the customers based on their online activity. However, customers could choose to grant companies access to their data, thus benefitting both the companies and customers by precisely matching the needs of both the parties. This would result in substantial cost savings through more efficient marketing.

Blockchain technology could also provide assurance to customers about the quality of a product or service. A likely application is within the precious stones industry (Knight 2017). The technology is used to identify the source of procurement of precious stones as well as their authenticity. Each event or transaction in the blockchain is validated by the previous transaction, thereby ensuring that the asset, in this case precious stones, is what it claims to be. Moreover, it helps to avoid the great degree of dependence on a central authority

responsible for keeping track of records, thereby reducing the cost of tracking and storage of data (Mansfield-Devine 2017).

In broad economic terms, blockchain technology offers multiple advantages: (i) reducing the cost of determining the authenticity and (ii) reducing the cost of establishing networks by avoiding reliance upon intermediaries (Catalini and Gans 2017). The desire of a financial lending world without intermediaries could become a reality; however, such a transformation would also imply broadening the scope of regulatory implementation from national borders to a global approach (Lagarde 2017).

2.2 Current application of blockchain technology

Apart from its widely publicized use in cryptocurrencies, blockchain technology is being used very actively by corporates and even by governments. One such example is in Estonia where the government has implemented the technology in application of its e-Residency program. This has enabled citizens to have improved control over their and access to their electronic records. The use of technology in maintaining identity information also grants it security from data breaches because of the decentralization (Sullivan and Burger 2017).

Another application of blockchain technology is in global trade operations by Maersk, a global logistics and transportation company, which is partnered with IBM, a leader in providing blockchain technology solutions (IBM 2018). IBM is also partnered with Sichuan Hejia Company Limited to take advantage of blockchain technology solutions in procurement of pharmaceuticals. Amazon Web Services (AWS) provides support to various blockchain applications such as Sawtooth, Corda R3, PokitDok and Samsung Nexledger, by providing a cost-efficient and secured development platform (AWS 2018). It has been reported that the advantages of blockchain technology are being considered by other companies such as Walmart, British Airways, UPS, and FedEx (Krauth 2018). Even the NASDAQ and New

York Stock Exchange are trying to tap into the advantages of blockchain technology (Tapscott and Tapscott 2017). The numerous advantages it offers beyond the present public view of cryptocurrencies clearly highlight the tremendous potential of the technology and its capability to disrupt and transform current business practises.

3. Initial Coin Offerings

The use of blockchain technology has paved the way for raising finance via a new method. An essential feature is its virtual immutability which prevents a single user from making changes to the chain (as demonstrated in Figure 2 above). Consequently, this has resulted in firms using this technology to raise funds through an Initial Coin Offering (ICO).

An ICO, also known as an Initial Token Sales (ITS), refers to a digital method of raising finance whereby the issuer offers tokens to investors in lieu of other well-established cryptocurrencies or fiat money. The idea is to raise capital to finance future development activities of the business as well as to generate excitement and an established user-base for an entity's future offerings.

The creation and dissemination of coins (or tokens) in an ICO uses blockchain technology to facilitate wide participation of investors. The ease with which funds can be raised and the growing popularity of ICOs is evident from the fact that a study on funds raised by 372 ICOs found that a total of USD 3.7 billion has been raised in 2017 (Ernst & Young 2018). ICOs are generally viewed by start-ups as an important channel for raising funds (Underhill 2018). However, with the growing popularity even established firms have launched or are planning to launch their respective ICOs, which is evident from the examples of Perth Mint and IAGON (Garvey 2018).

This is a post-peer-review, pre-copyedit version of an article published in Crime, Law and Social Change. The final authenticated version is available online at: http://dx.doi.org/10.1007/s10611-019-09873-2.

The surge in fundraising through an ICO can be attributed to its being quick and cost-efficient. This is derived from the time and cost saved from compliance with securities laws and regulations which must be taken into consideration in the case of traditional methods of raising funds. Moreover, the use of blockchain technology attracts investors because it is a new innovation with the potential to yield huge returns (Underhill 2018). Investment in an ICO is different from investment in an IPO, because the investment and ownership of coins acquired in an ICO does not guarantee ownership in a company, which is the case in an IPO. The ICO process begins with the announcement of an ICO by the issuer followed by marketing of the ICO through the company's website and other social media channels, and eventually the offerings of coins through an ICO within a designated time-period. The announcement of an ICO is accompanied by the release of a white paper, which can be considered similar to a prospectus in case of an IPO. The white paper contains information about the project, coins being offered, the rights available to investors, lifecycle of the project, other legal terms and conditions, and more. It becomes necessary to understand that while the white paper serves a function like a prospectus, it is typically less detailed and does not adhere to any specified guidelines (Underhill 2018).

The wide variety of ICOs also draws attention to the kind of coins being offered. At times, these may facilitate the holder to access products or services of the issuer or which the issuer intends to develop from funds raised through the ICO (ESMA 2017). Generally, this is the most common type of coin offered, where it facilitates access to services by payment exclusively through the coin. An example is the entity Token Report, which through an ICO offered Token Clarity coins enabling users of those tokens to access databases dedicated to tracking other ICOs (Underhill 2018). The other most common type of coins offered through ICOs facilitates users to use them as normal currencies where acceptable or be able to get them converted into fiat currencies (Underhill 2018; ESMA 2017). As per Lu (2019), partner

at 256 Ventures (an early stage crypto-investment fund), the classification of tokens into "security" and "utility" tokens can be attributed to the US securities laws and may not be applicable to countries such as Australia and therefore Lu suggests a classification based on the rights the tokens generate. On reviewing literature across countries, he proposed a classification of tokens with a jurisdictionally neutral mindset. He classified tokens as:

- Investment tokens representing those that are considered assets and promises a financial return or benefit in the future,
- Utility tokens similar to digital coupons that provide its participants with access or utility to an entity's product or service in the future and
- Payment tokens representing those which may be used as means of payment.

The coins in an ICO are usually offered through one of two formats. The issuer may issue the coins during or immediately after the sale. The other more common method is a pre-sale in which the coins are not developed for distribution and are scheduled for distribution at a later date (Underhill 2018).

3.1 ICOs versus Crowdfunding

According to Schwienbacher and Larralde (2010), crowdfunding can be defined as financing a venture by individuals instead of professional parties. Similarly, Mollick and Nanda (2015) refer to crowdfunding as funding projects by drawing small amounts of funds from a relatively larger number of individuals without the use of standard financial intermediaries. In cases of crowdfunding, investors have clear expectations in lieu of their investment – in some cases they expect nothing and in others they expect returns in the form of products, equity or monetary repayments with interest (Beaulieu et al. 2015; Gleasure and Feller 2016).

Zetzsche et al. (2017) view ICOs as a combination of crowdfunding and blockchain. Crowdfunding and ICOs are similar in that their mechanism for raising funds allows investors early access to fund new ventures. Additionally, both provide an alternative mechanism for funding operations to businesses that are not of interest to venture capitalists or other institutional investors. Further, they do not rely on traditional financial intermediaries for raising funds and are generally cost-effective in comparison to an IPO.

However, ICOs and crowdfunding have key differences. Crowdfunding involves the use of a central platform hosted by a third-party provider while an ICO makes the use of blockchain and a decentralized peer-to-peer (P2P) network for raising funds (Schweizer et al. 2017). In an ideal scenario, crowdfunding platforms and banks serve as trusted entities for transactions whereas in case of an ICO the verification of transactions takes place through a network-wide consensus (Arnold et al. 2019). In terms of accessibility, crowdfunding is generally limited to a certain country or regions whereas ICOs are accessible more broadly. ICOs generally fund technology-related ventures while crowdfunding often spans various categories such as hardware, software, technology and food. However, in recent times, ICOs have expanded beyond technology offerings, an example of that is providing tokens for real estate ventures (Bailey 2018; Zmudzinski 2019). There are also differences in investor expectations and risk. ICO investors expect to earn a profit for their investment whereas crowdfunding investors may or not expect returns from their investment. Additionally, in a crowdfunding project, investors have clear expectations about the outcome on completion, but clear expectations regarding the outcome from ICO funding is often absent. Differences also exist in relation to regulations; regulations pertaining to crowdfunding are more certain and regulators have been overwhelmingly more positive towards crowdfunding. The less certain regulations relating to ICOs are discussed in this paper.

4. Regulatory Steps towards ICOs in Key Jurisdictions

As of December 2017, there was no specific regulatory framework focussed exclusively on ICOs, but the growing popularity, surge in volume of raising finance through ICOs, and the rise in fraudulent instances involving ICOs, prompted regulatory authorities across the globe to issue guidelines, make key announcements and sometimes take action (Chance 2018).

The regulatory developments and their evolution in jurisdictions that have taken a clear regulatory stance or in which a meaningful amount of funds have been raised through ICOs are discussed below.

- Australia

  ICO activity has been on the rise in Australia. It is evident from the fact that the Perth Mint, one of the biggest gold refiners in Australia, is developing blockchain products backed by gold (Garvey 2018). In response to this growing focus on ICO, the Australian Securities and Investments Commission (ASIC) issued guidelines pertaining to ICOs in September 2017 (ASIC 2017). The guidelines aim to provide a clear sense of direction to businesses wishing to raise funds through the medium of ICOs. Through the guidelines, ASIC informed the businesses and investors alike that whether an ICO falls under the purview of Australian Corporations Act will depend upon the structuring and operations of the ICO as well as the rights gained through the ownership of coins offered through the ICO. Hence, if an ICO exhibits traits of a security it will be subject to the Australian Corporations Act and if it does not resemble a security it will fall under the purview of general law and consumer law of Australia related to the offer of products or services (Chance 2018). The main focus of the regulatory guidance issued in 2017 was the Australian Consumer Law and the Corporations Act. In 2019, the regulatory guidance was updated to incorporate detailed obligations for cryptocurrency firms to comply with under the Australian Corporations Act, the ASIC Act and other laws. The guidance

covered the requirement to hold an Australian financial services (AFS) license and widening the scope of consumer protection.

- China

In September 2017, the People's Bank of China issued a circular banning ICOs (Borak 2018) declaring them illegal, stating that ICOs may promote crimes pertaining to financial fraud, Ponzi schemes, illegal securities offerings and more (Chance 2018). The Chinese regulators have been active in persuading foreign-listed Chinese companies to abandon plans for raising funds through ICOs. An example of this is Renren, a Chinese social networking website, which dropped its ICO plans in January 2018 (Yang et al. 2018). The Chinese government continues to maintain its stance against cryptocurrencies including the issuance of ICOs as illegal (Congress 2018b; Williams 2019).

- France

In October 2017, the French Regulatory Authority, Autorité des Marchés Financiers (AMF), published a discussion paper to obtain views of key stakeholders relating to various possibilities of regulatory frameworks that can be applied to ICOs (AMF 2017). The discussion paper considered the creation of a best-practise guide for ICOs, or extending securities regulation to ICOs or developing a new set of regulations pertaining to ICOs. Additionally, the AMF announced a program to provide guidance for a framework regulating ICOs and protecting investors and issuers, called UNICORN (Universal Node to ICO Research and Network). The bill was passed in 2019 regulating the country's crypto industry including the establishment of a legal framework for ICOs. The bill provided the issuers of ICOs with an option to apply for approval from AMF if they complied with requirements such as (i) incorporation or registration within the jurisdiction, (ii) providing adequate information about the token, project and the company

and (iii) complying with the necessary anti-money laundering (AML hereafter) and counter financing of terrorism (CFT hereafter) requirements (Helms 2019).

- Hong Kong

The regulatory authority in Hong Kong, the Hong Kong Securities and Futures Commission (SFC), released a press statement in September 2017 relating to ICOs (SFC 2018). Consistent with the views of Hong Kong Monetary Authority (HKMA), the SFC identified digital coins offered in ICO as a virtual commodity subject to regulations of Hong Kong securities law, depending upon the features they exhibit. Further, if the coin offerings fell under the definition of "security" then the activities of such coin would be regulated and subject to Hong Kong's product or license authorization requirement (Chance 2018). The statement further warned investors of the risks of investments in ICOs. The regulatory authorities are still under the process of developing regulations to govern ICOs. As of December 2018, the SFC was set to tighten the regulations on cryptocurrencies including requirements such as ICOs for token which have been in existence for at least 12 months. The implementation of regulations shall take place in stages (Kihara 2018).

- Japan

The amendments in Payment Services Act (PSA) of Japan in early 2017 defined cryptocurrencies as "Virtual Currencies" and virtual currency exchanges as "Virtual Currencies Business Operators" and were required to be registered with Japan's Financial Services Agency (JFSA 2017). As of December 2018, no regulations pertaining to ICOs existed in Japan and the need for regulatory framework for ICO in Japan by JFSA is under evaluation (JFSA 2017; Chance 2018). In the meanwhile, the Japan Cryptocurrency Business Association (JCBA) came up with its recommendations on ICO regulations in

2019 (JCBA 2019). The focus of the regulations was to expand cryptocurrency in Japanese domestic exchange, establishing clarity over the definition and regulations for security and utility tokens (Tashiro 2019; Yakubowski 2019).

- Russia

Russia is only second to the US in terms of the number of ICO projects originating from a particular country (Ernst & Young 2017). The Russian government's approach towards cryptocurrencies has shifted from being cautious to acknowledging its presence and growth. However, at present we found no regulations pertaining to cryptocurrencies. In June 2017, the Russian central bank along with the Ministry of Finance made an announcement to develop regulations to regulate cryptocurrencies (Chance 2018). The Russian Ministry of Finances introduced a draft bill on digital financial assets in 2018. It limited the participation in ICOs to only qualified investors with exceptions to this condition to be decided by the Russian Central Bank. It also provided definitions for "digital assets" and "digital rights" (Congress 2018a). As of June 2019, the bill is still under consideration before it can be enacted for implementation.

- Singapore

Unlike that of many other countries, the approach adopted in Singapore towards cryptocurrencies has been positive (ACCA 2018). In 2017, the Monetary Authority of Singapore (MAS) stated that if coin offerings through an ICO resemble a security offering then it will be regulated within the purview of the Securities and Futures Act (SFA) (MAS 2017b). Further, consistent with the US SEC, the issuers of such coins are required to issue a prospectus, and registration is applicable. Further, in a joint report with Commercial Affairs Department (CAD), the financial crime division of Singapore Police issued a warning to investors about the potential risks of investing in ICOs (MAS 2017a).

The MAS updated its guidelines for businesses interested in raising funds through an ICO in 2018. It laid down guidelines for businesses to act in compliance with AML and CFT regulations. The guidelines required all the parties related to an ICO to comply with AML and CFT policies. Additionally, a requirement to have license to undertake issuing and advising on matters related to ICOs was made mandatory (2018).

- South Korea

South Korea ranks third after the US and Japan in the market for bitcoin trading and is the largest exchange market for Ethereum's cryptocurrency – the Ether (Kim 2017). As per government data, around USD 89 million were raised in ICOs in September 2017 (Kim 2017). As a result, just as with China, the Financial Services Commission (FSC hereafter), the South Korean regulatory authority, banned ICOs in the country (Kim 2017; Nakamura and Kim 2017). The regulatory authority cited growing risk of financial scams and speculation as the reasons behind the move. However, unlike the Chinese, the South Korean public could invest in foreign ICOs (Kim 2017). In the first half of 2019, the FSC continued to maintain its stance of a ban on domestic ICOs and citing it to be a "high risk" engagement. The stance was in response to a survey conducted by the Financial Supervisory Services (FSS) with respondents being companies who had conducted ICOs in foreign countries (FSI 2019; Khatri 2019).

- Switzerland

Switzerland has emerged as one of the key jurisdictions of raising funds through ICOs, raising 600 million US dollars, which is a quarter of the total funds raised in ICOs in 2017 (Australian 2018). In September 2017, the Swiss Financial Market Supervisory Authority (FINMA) stated that investigations were undertaken to probe the breaches of regulatory provisions by ICO (FINMA 2017). The report further defined ICO as an initial public

offering in a digital form that makes use of blockchain technology. Consistent with regulators in other countries, FINMA stated that the structuring of an ICO will determine the application of securities law, and if applicable, regulations relating to banking law, anti-money laundering and terrorist financing, among others, shall apply. The Swiss regulatory authority also warned the investors about the risks related to investment in ICOs. In a follow-up to the guidelines issued in 2017, FINMA published guidelines regulating the treatment of ICOs in 2018 (FINMA 2018). FINMA determined the application of financial regulations on a case-by-case basis as each ICO is different from each other. It further provided a clarification over its classification of tokens into payment (when used as means of value transfer), asset (when used as equity claim or debt) and utility tokens (when facilitating access to a service or application by means of blockchain-based infrastructure). Additionally, compliance with AML and CFT regulations for payment tokens was made mandatory (FINMA 2018).

- United States

The United States (US) was among the first countries to initiate the development of a regulatory framework towards ICOs. The laws and regulations applicable to ICOs in the US vary, based on the location of issue, the investors to which the ICO is being directed and the kind of services that are or will be provided. Where an investment is made in an entity with a profit motive that depends on the managerial efforts of others rather than the utilization of investment based on its functionality for personal consumption, then offering of such coins will be considered securities and will fall under the purview of the regulator, the Securities Exchange Commission (SEC), and will be subject to its security laws (Chance 2018; Tew and Freedman 1973). In other words, if an investment in a coin offered through an ICO is made to earn profit rather than utilize the coin on the basis of

its functionality for personal use then the coin would be considered a security and a subject of security regulations under the Howey Test (Chance 2018).

To establish clarity about what falls under the purview of securities regulation, the SEC released an investigative report on an entity called the DAO in July 2017 (SEC 2017a). The coins offered by DAO exhibited characteristics of a security. The SEC also stated that classification of coin offerings as security depends upon a number of factors and the assessment of a coin as a security shall vary on a case-by-case basis; hence, at present no applicable regulatory guidance exists on the issue (Chance 2018). Further, in October 2017, LabCFTC, a division of the US Commodity Futures Trading Commission (CFTC), stated that if ICO coins do not meet the conditions of the Howey Test they could be considered commodities and be a subject of their jurisdiction (LabCFTC 2017). In May 2019, the SEC organized a public forum comprising experts from industry and academia to facilitate communication and a better understanding around DLT and digital assets (SEC 2019).

- United Kingdom

In 2014, the Bank of England (BoE) downplayed the risk posed by cryptocurrencies to the stability of UK's financial system (Ali et al. 2014). The Financial Conduct Authority (FCA) of the UK is yet to take definite measures towards development of a regulatory framework for the ICO market in the UK. However, the FCA has been cautious about its approach towards ICOs and has warned against investing in them by terming them speculative and high-risk instruments (FCA 2017). In 2018, the governor of BoE raised concerns over the need to regulate cryptocurrencies (Kharpal 2018). As of June 2019, any definitive measure regulating cryptocurrencies, including ICOs, in the context of UK is yet to be taken.

5. Cases of ICOs Fraud

In 2017, in the US alone, the eagerness to bypass securities law using an ICO was evident from the fact that not one ICO was registered with the SEC. The lack of an established regulatory framework to regulate ICOs not only created confusion in the market for issuers but also provided an opportunity for people with ill intentions to carry out fraudulent activities relating to pump-and-dump schemes, pyramid and Ponzi Schemes and even money laundering (Underhill 2018). An ICO is an attractive opportunity for fraudsters because of a range of factors including a lack of due diligence and information (DeVoe 2018).

An ICO is accompanied by issuance of a white paper, but unlike in a prospectus the information provided is not always accurate and detailed. Furthermore, the information provided cannot be verified, which leads to potential fraudsters using false information to mislead. Moreover, fraudsters may also create websites with vague and incomplete information. They may further make use of various social media channels and even use celebrity endorsements to attract the attention of investors in huge numbers to perpetrate the fraud scheme on a large scale (Underhill 2018).

There are numerous examples of ICO frauds such as Opair and Ebitz, Confido, Prodeum, OneCoin and Optioment. Recently, in April 2018 in Vietnam, over 600 million US dollars were identified to be lost to ICO fraud schemes through the two ICOs, namely, iFan and Pincoin, but detailed information about the case is yet to be made public (Floyd 2018). There are plenty of relatively small, alleged ICO scams, but because of a lack of reliable information, this study focused on cases that government authorities are involved with. The specific criteria for choosing the cases included (i) the case being discussed in online media and websites that specifically focus on cryptocurrencies, (ii) involvement of regulatory authorities in the investigation of such cases, (iii) the scheme garnering considerable attention

from investors and (iv) a substantial amount being raised in the scheme. The four chosen cases are discussed below, which have and still act as a source for regulatory developments.

5.1 AriseBank

As per the company's website, AriseBank, also known as AriseBank Limited or AriseBank Foundation, LLC, was co-founded in early 2017 by Jared Rice Sr and Stanley Ford with headquarters in Dallas, Texas. It was marketed as a decentralized bank with the ability to provide a wide-range of banking products compatible with over 700 virtual currencies. Further, it was marketed as being among the world's largest platforms for cryptocurrency with the sole aim to establish it as a form of fiat money and change the dynamics of the banking sector (Aitken 2018).

In October 2017, AriseBank launched its ICO and a test version of its banking operations. The ICO was promoted on social media, the company's website and through celebrity endorsements. Around the same time, it issued a white paper giving an overview of the products and the management team. The paper also gave a brief overview of the bank's own digital currency called "AriseCoin" and its plan of offering it through the ICO. The AriseCoin ICO started in November with a "private sale", followed by a "pre-sale" in December. The bank released a press statement in January claiming to have raised around 600 million US dollars out of its goal of one billion. The coin distribution was scheduled for February, 2018 (SEC 2018).

In January 2018, a "Cease and Desist" order was issued by the Texas Department of Banking to AriseBank, prohibiting them from misleading investors about their engagement in the banking business in the State of Texas. Following this, the US Securities and Exchange Commission (SEC) filed litigation against AriseBank in the Federal District Court of Texas.

The SEC filed litigation to stop the issuance of securities by AriseBank for violating several sections of US Securities Exchange Act on the following grounds(SEC 2018):

- Issuance of unregistered securities

The securities law in the US makes it mandatory for companies to disclose their financial information by registering their securities with SEC. The idea is to enable investors to make rational investment decisions based on available information. Since AriseCoin ICO was a security without registration of the coin or the bank with SEC, there was a violation of the Act. Also in 2017, the CEO of AriseBank Jared Rice Sr made false claims of AriseCoin not being a subject of regulations by the SEC.

- Use of misleading and false information

In January 2018, AriseBank made false claims about acquiring a Federal Deposit Insurance Corporation (FDIC) insured bank, KFMC Bank Holding Company, which facilitated offering secured services to its customers. However, no records supporting FDIC-insurance were found. FDIC had no records of any change in ownership involving the parties mentioned, rendering the claims to be false and misleading to investors.

Further, in its white paper, AriseBank claimed to offer its own Visa cards that would facilitate payment for goods and services using any of the 700 cryptocurrencies that the customers could hold in their respective AriseBank account. It was stated that the card was being provided in partnership with Marqeta, a payment solution firm. However, the claims also turned out to be false when Marqeta publicly denied an association with AriseBank.

- Omission of material information

AriseBank provided brief information about the background of its executives on the company's website as well as in its white papers. However, none of these sources mentioned the criminal background of its two key executives. Such information would be important to investors in their decision-making.

As a result of the violations, the court froze assets of AriseBank and its co-founders and this ensured recovery of the various digital currencies held by AriseBank.

5.2 RECoin and Diamond Reserve

RECoin Group Foundation, LLC (RECoin) was a limited liability company incorporated in 2017 with its headquarters in Las Vegas, Nevada, and was marketed as a company involved in real estate investment and smart contracts for real estate through an ICO. Another such entity was Diamond Reserve Club, also known as DRC World Inc, which was incorporated in 2017 with its headquarters in San Juan, Puerto Rico. The principal business of DRC was investment in diamonds through funds raised through an ICO. DRC was also marketed as obtaining discounts with retailers for investors in DRC. Both the companies were solely owned and managed by Maksim Zaslavskiy (SEC 2017c). Between July and September, 2017, Zaslavskiy raised 300,000 US dollars from investors in digital coins in RECoin and then DRC during their ICOs (SEC 2017c).

The purported objective of these ICOs was the conversion of fiat currency or other digital currencies such as Bitcoin into a digital token that would derive its value from investment in an underlying asset. The underlying asset in the case of RECoin was real estate, whereas in the case of DRC it was diamonds. It was claimed that appreciation of investment or growth in business, or demand for coins, would drive the value of coins (SEC 2017c).

This is a post-peer-review, pre-copyedit version of an article published in Crime, Law and Social Change. The final authenticated version is available online at: http://dx.doi.org/10.1007/s10611-019-09873-2.

In September 2017, the SEC filed litigation against Zaslavskiy and his companies seeking to stop issuance of securities for violating several sections of the US Securities Exchange Act on the following grounds (SEC 2017c):

- Issuance of unregistered securities

  Since the securities being offered through the ICO of RECoin were not registered with SEC, there was a violation of the Securities Exchange Act. Further, in case of DRC, an attempt to bypass the registration regulation was made by Zaslavskiy through marketing the ICO as an Initial Membership Offer (IMO), offering membership in the entity rather than investment.

- Use of misleading and false information

  To attract investors, false and misleading claims were made by Zaslavskiy on various platforms such as social media, the companies' websites and in the ICO white papers. First, it was claimed that investment in RECoin and DRC ICOs granted investors ownership of digital coins when none existed. Secondly, it was falsely claimed that the RECoin ICO was successful in raising four million US dollars when only 300,000 were raised. Thirdly, while none existed, it was claimed that RECoin and DRC had a team of professionals in the field to facilitate investments of funds raised. Finally, false claims were made about potential returns to investors from investment in these ICOs.

5.3 PlexCorps

PlexCorps, also known as PlexCoin and traded as SidePay.Ca, was an unincorporated entity controlled by Dominic Lacroix. As per the company's website, the company comprised a team of over forty professional experts dispersed across the globe working towards the

primary objective of increasing the accessibility of cryptocurrencies to the general public (SEC 2017b). According to one of the white papers, PlexCorps was based in Singapore.

The PlexCoin ICO was launched through a pre-sale by PlexCorps in August 2017. The company's website stated that PlexCoin had the potential to become the mainstream cryptocurrency (SEC 2017b). Further, one of the white papers declared an expected return in excess of 13 times the original investment within a month (Shin 2017). Subsequently, the PlexCoin ICO raised 15 million US dollars (SEC 2017b).

In December 2017 SEC filed litigation against PlexCorps, Dominic Lacroix and his partner Sabrina Paradis-Royer, seeking to stop the issuance of securities for violating several sections of US Securities Exchange Act on the following grounds (SEC 2017b):

- Issuance of unregistered securities

  Since the securities being offered through the ICO of PlexCoin were not registered with the SEC, there was a violation of the Securities Exchange Act. Further, an attempt to bypass the registration regulation was made by Lacroix by marketing the coins being offered through PlexCoin ICO as cryptocurrencies rather than securities.

- Use of misleading and false information

  In circumstances similar to the previous case study, false and misleading claims were made by PlexCorps and Lacroix on various platforms such as social media, the company website and ICO white papers. First, it was claimed that appreciation in the value of PlexCoin tokens was based upon the investment of funds raised through the ICO. Secondly, PlexCorps's team was claimed to comprise over forty experts with the headquarters in Singapore. However, the claims were false as the entity comprised only a few employees based in Quebec. Thirdly, claims were made to keep the identity of

PlexCorps executives hidden to avoid competition and issues relating to privacy. However, the main reason to keep the identity of Dominic Lacroix a secret was his past record of being a violator of securities law in Canada. As a result, fake names were used to carry out the business activities and Lacroix's involvement in the business was denied. False claims were also made about potential returns to investors from investment in PlexCoin ICO.

- Misappropriation of funds

One of the objectives of the PlexCoin ICO was to raise funds to develop other products of PlexCorps, but a portion of funds raised through the ICO was misappropriated by Lacroix and his partner for personal expenditure.

5.4 Benebit

Benebit was a blockchain-based decentralized platform that facilitated interaction among geographically diverse entities (Top ICO List 2018). The primary motive was to create a platform enabling customers to store and trade points from loyalty-based programs using cryptocurrencies (DeVoe 2018). As per the company's website, the goal was a decentralized global network for virtual customer loyalty currency (Sedgwick 2018).

Benebit's ICO pre-sale event was promoted by an ICO Syndicate, a community of investors interested in ICOs. Benebit aggressively promoted its project, spending over 500,000 US dollars on marketing its campaign, hiring a public relations team and being active on social media. This drew the attention of potential investors and led to the development of a base of approximately 9,000 followers on a social media channel (Shome 2018). However, the website and all its accounts on social media were pulled down once it was identified that the pictures of the management team were fake, having in fact been taken from a school website.

The scam resulted in loss of investor funds somewhere between 2.7 million and 4 million US dollars (DeVoe 2018).

There were two key factors behind the success of Benebit's ICO scam:

- Element of Legitimacy

  The huge expenditure incurred from promoting the Benebit ICO led to a big following for the ICO across various social media platforms. This was further supplemented by positive reviews and high scores from various ICO reviewing websites, which granted the Benebit ICO legitimacy and convinced investors that the scheme was authentic (Shome 2018).

- Lack of Due Diligence

  One of the important aspects of investing in a new opportunity involves conducting due diligence on the entities and its key executives. This process was overlooked in the case of Benebit, leading to successful execution of the scam (DeVoe 2018). Third-party promoters of Benebit did not undertake a verification procedure on the passport details of key executives of Benebit, which also contributed to the fraud being possible on such a large scale (Shome 2018).

6. Key Insights

The approaches to regulate ICOs differ across jurisdictions. Some countries such as China and South Korea have imposed an outright ban on ICOs, while the US have laid down clear guidelines around ICOs and others such as Malta and Singapore which have left no stone unturned in attracting businesses by providing a specific regulatory and administrative framework for ICOs (Mondaq 2019; Lu 2019). Malta, in particular, has earned itself the title of "Blockchain Island" (Mondaq 2019). The presence of such a wide variation in the regulatory approaches and a continued lack of clarity at the global level makes it essential to

have a set of guidelines to assist investors, issuers and regulators. Key insights for these concerned stakeholders are discussed below.

6.1 Insights for Investors

It is important to remember that not all ICOs are carried out with the purpose of cheating investors. However, it is essential for investors to take necessary steps to protect themselves against the possibility of fraud. Based on the evaluation of the cases mentioned above, the following recommendations are made to investors to help them determine the legitimacy of an ICO.

- *ICO white paper*: Investors should not be enticed solely by the claims of the issuer and the marketing strategies adopted to lure them; instead, an investor should read all white papers in detail to understand the nature of the proposal and assist in determining its feasibility. Additionally, the long-term plans of the issuer in relation to the ICO should be evaluated; in most cases this information should be mentioned in a white paper. A lack of clarity in long-term goals and objectives could be an indicator of fraud.
- *Offering's Utility*: A deep analysis of the value proposition of the product or service being offered through an ICO is recommended for investors to determine whether the proposal has sufficient benefits to warrant investment, and whether it is feasible that these benefits could be realized. This information would be a useful indicator about the proposed ICO's legitimacy.
- *Management Due Diligence*: A detailed background check on all key executives would assist in determining the legitimacy of the proposed ICO. Thorough diligence would serve in protecting investors from fraud; this would include reverse searches of social media profiles, criminal record checks and an evaluation of past job history.

- *ICO Ratings and Reviews*: Investors should inform their decision-making with a variety of sources including both the ratings provided by rating agencies and expert opinions available on multiple cryptocurrency websites. As is the case with traditional IPOs, in the case of ICOs ratings and reviews do not guarantee protection, but they are still a good preliminary source of information to consider.

6.2 Insights for Issuers

Prior ICO scams where investors have lost their money have tarnished the reputation of genuine firms aiming to raise funds through ICOs. In the light of the growing cases of fraud through ICOs, it has become necessary for genuine issuers to provide as much information as possible to differentiate themselves from ICO scams and gain the trust of investors. The following recommendations are made to issuers.

- *Plain language:* Without compromising on accuracy, issuers should use plain language that is relatively easy to understand. This will aid investor comprehension and help to differentiate them from fraudsters.
- *Public disclosure of information*: To secure the trust of the investors, genuine issuers in all white papers should adopt the best practise of providing detailed information about their management team. This would facilitate verification background checks for management, something that investors are strongly encouraged to conduct.
- *Helpdesk*: As a best practise, ICO issuers should establish a helpdesk to answer the queries of investors and to explain the ICO offering and underlying technology if the investors require clarification. It is important that this helpdesk also refers to professional financial advisors and third-party information sources such as government guidelines where appropriate.

- *Regulatory guidance*: In the absence of a clear, detailed regulatory framework, issuers are encouraged to seek guidance from the relevant regulators and develop a legal framework to avoid any issues in the future. This will become increasingly important as new laws and regulations are adopted. In addition to avoiding any compliance issues, this approach is also an important step in building trust with investors.

The above-mentioned steps are recommended as best-practise to issuers to increase transparency and provide improved assurances as to the legitimacy of ICO investments. This will help genuine issuers attract investors in the long run.

6.3 Insights for Regulators

The uncertainties surrounding ICOs as new instruments make the role of regulators crucial. To ensure the safety of investors, and to provide a proper framework for issuers to adhere to, the following recommendations are made to regulators:

- *Dedicated unit*: Regulators should consider establishing a separate unit that exclusively investigates matters related to ICOs. This would allow the unique features of ICOs to be properly considered. This dedicated unit could develop a tailored framework providing clear guidelines to potential issuers, while safeguarding investors.
- *Low-cost compliance*: For many issuers, especially start-ups, a major advantage of raising funds through an ICO lies in saving on compliance costs compared with a traditional IPO. As a result, to save on the cost of compliance, ICOs are viewed as a way of bypassing security regulations. A possible remedy is to establish a low-cost compliance framework for ICOs which would encourage issuers to comply with the regulatory framework and at the same time maintain the attractiveness of raising funds through an ICO.

- *Mandatory registration*: A mandatory registration requirement for ICOs signals to issuers that there is regulatory oversight, which is a subtle encouragement of legitimate behaviour. Registration may also provide investors a sense of security regarding the funds being invested and promote an active marketplace.

A well-defined regulatory framework would establish clarity. This clarity would in turn encourage compliance from issuers. Investors would also be able to evaluate the extent of compliance associated with an ICO and use that information to assist them in determining the risk from investing in that ICO. As lower cost is one of the key features of ICOs, it is important that regulatory frameworks ensure the cost of compliance is relatively low to encourage compliant behaviour from issuers.

6.4 Notes on Recommendations

At a broad level, these recommendations help to highlight the aspects to be considered by the relevant stakeholders so that an innovative opportunity for financing operations could be utilized to its full extent and hence yield returns to all those involved.

It is critical to understand that adopting the above recommendations for investors does not guarantee complete protection from ICO fraud. Rather they are precautionary measures that can facilitate the discovery of fraud in the initial stages. For instance, in the case of AriseBank, following the recommendation of *Management Due Diligence* would have revealed the criminal background of the key executives involved. This would have acted as a red flag for investors in their decision-making or have been discovered by a dedicated regulatory unit. The same is true in Benebit where the information about the management was fake.

7. Conclusion and Implications

A common modus operandi for ICO fraudsters has been revealed from analyzing four prominent cases. ICO fraudsters make attempts to attract investors using various social media channels and celebrity endorsements. In addition, information on the company websites and white papers is usually vague and intensively technological, and it presents the product in a complicated manner. Further, the old tactic of promising unexpectedly high investment returns is present in all cases. Finally, the coins in the cases analyzed were either offered in stages or were advertised to be offered at a discount for a limited period. The motive is to highlight the urgency and promote a fear of missing out on huge investment returns.

The study provides implications for both investors and issuers. Investors should not jump on the first available opportunity to invest in an ICO. It is essential to read the white paper and to ensure that the concept adds value. The business motive for the ICO and the feasibility of the proposed product or service development should be evaluated. In the absence of regulations protecting the rights of those investing in an ICO, it becomes particularly important for a potential investor to conduct due diligence on the management team of the issuer. It is also essential to obtain views from various online forums about the project being undertaken through an ICO and views of rating companies. Traditional ratings given by the likes of Moody's and S&P do not guarantee the success of a company, and in a similar manner, ratings given to companies aiming to raise funds through an ICO may not be completely reliable. However, it is an added measure which might be helpful to an investor.

The cases analyzed should highlight to a potential issuer the need to adhere to regulations in order to avoid being subject to fines and penalties by regulators at a later stage. The issuers should evaluate their offerings to determine whether they qualify as a security or not, and if it is required obtain independent legal guidance. Issuers wishing to genuinely raise funds

through an ICO need to overcome the negative association because of previous ICO scams. To build trust with investors, we recommend increased transparency through the public disclosure of detailed information using easy-to-understand language and establishment of a helpdesk to attend to any queries.

Regulators also have a key role to play. There is a need for a regulatory framework specific to ICOs that protects investors whilst maintaining the low-cost advantage of ICOs as a method of raising funds. One recommendation is clear: the mandatory registration of all ICOs.

The adoption of the recommendations in this paper by investors and issuers, as well as the development of a tailored regulatory framework, will foster growth in the ICO market through reducing the prevalence of fraud. The findings from this initial study of ICO frauds lay a foundation for future research to analyze further ICO cases and develop a detailed best-practise guide in relation to ICOs for all stakeholders.

This is a post-peer-review, pre-copyedit version of an article published in Crime, Law and Social Change. The final authenticated version is available online at: http://dx.doi.org/10.1007/s10611-019-09873-2.

References

ACCA (2018). ICOs: Real deal or token gestures? http://www.accaglobal.com/content/dam/ACCA_Global/professional-insights/Initial-coin-offerings/pi-initial-coin-offerings.pdf. Accessed 5 March 2018.

Aitken, R. (2018). U.S. SEC Halts Alleged Crypto ICO Scam From 'Decentralized' Bank Seeking $1 Billion. https://www.forbes.com/sites/rogeraitken/2018/01/30/u-s-sec-halts-alleged-crypto-ico-scam-from-decentralized-bank-seeking-1-billion. Accessed 12 February 2018.

Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). The economics of digital currencies. *Bank of England Quarterly Bulletin*, Q3.

AMF (2017). L'AMF lance une consultation sur les Initial Coin Offerings et initie son programme UNICORN. http://www.amf-france.org/Actualites/Communiques-de-presse/AMF/annee-2017?docId=workspace%3A%2F%2FSpacesStore%2F5097c770-e3f7-40bb-81ce-db2c95e7bdae. Accessed 1 February 2018.

Arnold, L., Brennecke, M., Camus, P., Fridgen, G., Guggenberger, T., Radszuwill, S., et al. (2019). Blockchain and Initial Coin Offerings: Blockchain's Implications for Crowdfunding. In *Business Transformation through Blockchain* (pp. 233-272): Springer.

ASIC (2017). Initial coin offerings. http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/. Accessed 5 February 2018.

Australian, T. (2018). Swiss town Zug aims to become crypto-safe haven. Accessed 8 March 2018 via ProQuest database.

AWS (2018). AWS Blockchain Partners: Accelerating your distributed ledger journey. https://aws.amazon.com/partners/blockchain/. Accessed 22 February 2018.

Bailey, M. (2018). Melbourne start-up Konkrete to 'tokenise' property with ASIC-compliant coin offering. (Vol. 2019).

Barnes, P., & Oloruntoba, R. (2005). Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management. *Journal of International Management, 11*(4), 519-540, doi:https://doi.org/10.1016/j.intman.2005.09.008.

Beaulieu, T., Sarker, S., & Sarker, S. (2015). A Conceptual Framework for Understanding Crowdfunding. *CAIS, 37*, 1.

Borak, M. (2018). The final crackdown? China moves to completely ban and block cryptocurrency trading at home and abroad. https://technode.com/2018/02/05/china-ban-block-cryptocurrency-trading-at-home-abroad/. Accessed 16 February 2018.

Catalini, C., & Gans, J. S. (2017). Some Simple Economics of the Blockchain. *Rotman School of Management Working Paper No. 2874598; MIT Sloan Research Paper No. 5191-16., Available at SSRN: https://ssrn.com/abstract=2874598*.

Chance, C. (2018). Initial Coin Offerings – Asking The Right Regulatory Questions. https://talkingtech.cliffordchance.com/content/micro-cctech/en/fintech/initial-coin-offerings/_jcr_content/text/parsysthumb/download/file.res/Initial%20Coin%20Offerings.pdf . Accessed 12 April 2018.

Congress, T. L. L. o. (2018a). Regulation of Cryptocurrency Around the World. The Law Library of Congress.

Congress, T. L. L. o. (2018b). Regulation of Cryptocurrency: China. https://www.loc.gov/law/help/cryptocurrency/china.php. Accessed Web Page 2019.

DeVoe, R. (2018). Benebit – The Biggest ICO Exit Scam In History Nets Up to $4 Million. https://www.coinbureau.com/ico/benebit-biggest-ico-exit-scam-history-nets-4-million/. Accessed 1 February 2018.

Ernst & Young (2017). EY research: initial coin offerings (ICOs). http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf. Accessed 12 February 2018.

This is a post-peer-review, pre-copyedit version of an article published in Crime, Law and Social Change. The final authenticated version is available online at: http://dx.doi.org/10.1007/s10611-019-09873-2.

Ernst & Young (2018). Big risks in ICO market: flawed token valuations, unclear regulations, heightened hacker attention and congested networks. http://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf. Accessed 12 February 2018.

ESMA (2017). ESMA highlights ICO risks for investors and firms. European Securities and Markets Authority (ESMA).

FCA (2017). Distributed Ledger Technology: Feedback Statement on Discussion Paper 17/03. https://www.fca.org.uk/publication/feedback/fs17-04.pdf. Accessed 8 February 2018.

FINMA (2017). FINMA Guidance 04/2017 Regulatory treatment of initial coin offerings. https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20170929-finma-aufsichtsmitteilung-04-2017.pdf?la=en. Accessed 8 February 2018.

FINMA (2018). Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs). FINMA.

Fleming, L., & Sorenson, O. (2016). Financing by and for the Masses: An Introduction to the Special Issue on Crowdfunding. *California Management Review, 58*(2), 5-19, doi:10.1525/cmr.2016.58.2.5.

Floyd, D. (2018). Vietnam Investigates ICO Fraud After $660 Million in Losses Reported. https://www.coindesk.com/vietnam-investigates-ico-fraud-660-million-losses-reported/. Accessed 14 April 2018.

FSI (2019). ICO Survey Results and Future Direction. South Korea: Financial Services Commission.

Garvey, P. (2018). Blockchain-backed gold: Mint's answer to bitcoin. Accessed 12 February 2018 via Proquest Database.

Gepp, A. (2016). Addressing the problem of financial statement fraud: Better detection through improved models. In *8th Asia-Pacific Interdisciplinary Research in Accounting (APIRA) Conference*. Melbourne, Australia.

Gepp, A., Linnenluecke, M. K., O'Neill, T. J., & Smith, T. (2018). Big data techniques in auditing research and practice: Current trends and future opportunities. *Journal of Accounting Literature, 40*, 102-115, doi:https://doi.org/10.1016/j.acclit.2017.05.003.

Gleasure, R., & Feller, J. (2016). Emerging technologies and the democratisation of financial services: A metatriangulation of crowdfunding research. *Information and Organization, 26*(4), 101-115.

Helms, K. (2019). France Adopts New Crypto Regulation. https://news.bitcoin.com/france-cryptocurrency-regulation/. Accessed Web Page.

IBM (2018). Maersk and IBM to Form Joint Venture Applying Blockchain to Improve Global Trade and Digitize Supply Chains. https://www-03.ibm.com/press/us/en/pressrelease/53602.wss. Accessed 7 February 2018.

JCBA (2019). Recommendation on New ICO Regulation.

JFSA (2017). Details of Screening for New Registration Application as Virtual Currency Exchange Service Provider https://www.fsa.go.jp/en/news/2017/20170930-1/02.pdf. Accessed 9 February 2018.

Kennedy, J. (2016). $1.4bn investment in blockchain start-ups in last 9 months, says PwC expert. https://www.siliconrepublic.com/start-ups/blockchain-pwc-investment. Accessed 12 February 2017 2017.

Kharpal, A. (2018). Bank of England's Carney calls for more regulation around the 'speculative mania' of cryptocurrencies. (Vol. 2019).

Khatri, Y. (2019). South Korea Will Maintain ICO Ban After Finding Token Projects Broke Rules. (Vol. 2019).

Kihara, T. (2018). Hong Kong to tighten cryptocurrency rules. (Vol. 2019).

This is a post-peer-review, pre-copyedit version of an article published in Crime, Law and Social Change. The final authenticated version is available online at: http://dx.doi.org/10.1007/s10611-019-09873-2.

Kim, Y. (2017). Behind South Korea's Cryptocurrency Boom. https://www.technologyreview.com/s/609561/behind-south-koreas-cryptocurrency-boom/. Accessed 8 February 2018.
Knight, W. (2017). The Technology Behind Bitcoin Is Shaking Up Much More Than Money. https://www.technologyreview.com/s/604148/the-technology-behind-bitcoin-is-shaking-up-much-more-than-money/. Accessed 14 February 2018.
Kotabe, M. (2005). Global security risks and international competitiveness. *Journal of International Management, 11*(4), 453-455, doi:https://doi.org/10.1016/j.intman.2005.09.004.
Krauth, O. (2018). 5 companies using blockchain to drive their supply chain. https://www.techrepublic.com/article/5-companies-using-blockchain-to-drive-their-supply-chain/. Accessed 15 February 2018.
Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management, 11*(4), 541-562, doi:https://doi.org/10.1016/j.intman.2005.09.009.
LabCFTC (2017). A CFTC Primer on Virtual Currencies. https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf. Accessed 8 February 2018.
Lagarde, C. (2017). Central Banking and Fintech—A Brave New World? In *Bank of England conference, London*. https://www.imf.org/en/News/Articles/2017/09/28/sp092917-central-banking-and-fintech-a-brave-new-world (accessed 25 February 2018): International Monetary Fund.
Lu, D. (2019). Submission to the Treasury's review into Initial Coin Offerings (ICOs).
Mansfield-Devine, S. (2017). Beyond Bitcoin: using blockchain technology to provide assurance in the commercial world. *Computer Fraud & Security, 2017*(5), 14-18, doi:https://doi.org/10.1016/S1361-3723(17)30042-8.
MAS (2017a). Consumer Advisory on Investment Schemes Involving Digital Tokens (Including Virtual Currencies). http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/Consumer-Advisory-on-Investment-Schemes-Involving-Digital-Tokens.aspx. Accessed 4 February 2018.
MAS (2017b). A Guide to Digital Token Offerings. https://www.iosco.org/library/ico-statements/Singapore%20-%20MAS%20-%20A%20Guide%20to%20Digital%20Token%20Offerings.pdf. Accessed 4 February 2018.
MAS (2018). Monetary Authority Of Singapore: A Guide to Digital Token Offerings. Monetary Authority of Singapore.
Mollick, E., & Nanda, R. (2015). Wisdom or madness? Comparing crowds with expert evaluation in funding the arts. *Management Science, 62*(6), 1533-1553.
Mondaq (2019). ICOs and ICO Regulations in Malta. http://www.mondaq.com/x/800132/fin+tech/ICOs+And+ICO+Regulations+In+Malta. Accessed Web Page 2019.
Moore, D. A. (2017). How to Improve the Accuracy and Reduce the Cost of Personnel Selection. *California Management Review, 60*(1), 8-17, doi:10.1177/0008125617725288.
Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf. Accessed 18 February 2018.
Nakamura, Y., & Kim, S. (2017). Cryptocurrencies Drop as South Korea Bans ICOs, Margin Trading. https://www.bloomberg.com/news/articles/2017-09-29/cryptocurrencies-drop-as-south-korea-bans-icos-margin-trading. Accessed 8 February 2018.
Schweizer, A., Schlatt, V., Urbach, N., & Fridgen, G. (2017). Unchaining Social Businesses–Blockchain as the Basic Technology of a Crowdlending Platform.
Schwienbacher, A., & Larralde, B. (2010). Crowdfunding of small entrepreneurial ventures.

SEC (2017a). Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO. https://www.sec.gov/litigation/investreport/34-81207.pdf. Accessed 4 February 2018.
SEC (2017b). SEC V. PLEXCORPS (a/k/a and d/b/a PLEXCOIN and SIDEPAY.CA), DOMINIC LACROIX and SABRINA PARADIS-ROYER. https://www.sec.gov/litigation/complaints/2017/comp-pr2017-219.pdf. Accessed 5 February 2018.
SEC (2017c). SEC V. RECOIN GROUP FOUNDATION, LLC, DRC : COMPLAINT WORLD INC. a/k/a DIAMOND RESERVE CLUB,: and MAKSIM ZASLAVSKIY. https://www.sec.gov/litigation/complaints/2017/comp-pr2017-185.pdf. Accessed 4 February 2018.
SEC (2018). SEC V. ARISEBANK, JARED RICE SR., and STANLEY FORD. https://www.sec.gov/litigation/complaints/2018/comp-pr2018-8.pdf. Accessed 4 February 2018.
SEC (2019). SEC Staff to Hold Fintech Forum to Discuss Distributed Ledger Technology and Digital Assets.
Sedgwick, K. (2018). Benebit ICO Does a Runner with $2.7 Million of Investor Funds. https://news.bitcoin.com/benebit-ico-runner-2-7-million-investor-funds/. Accessed 1 February 2018.
SFC (2018). SFC warns of cryptocurrency risks. https://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=18PR13. Accessed 3 March 2018.
Shin, L. (2017). $15 Million ICO Halted By SEC For Being Alleged Scam. https://www.forbes.com/sites/laurashin/2017/12/04/15-million-ico-halted-by-sec-for-being-alleged-scam/#63e741d51569. Accessed 5 February 2018.
Shome, A. (2018). Benebit ICO Scammed Investors for At Least $2.7 Million. https://www.financemagnates.com/cryptocurrency/news/benebit-ico-scammed-investors-least-2-7-million/. Accessed 1 February 2018.
Sullivan, C., & Burger, E. (2017). E-residency and blockchain. *Computer Law & Security Review, 33*(4), 470-481, doi:https://doi.org/10.1016/j.clsr.2017.03.016.
Tapscott, D., & Tapscott, A. (2017). How Blockchain Will Change Organizations. *MIT Sloan Management Review, 58*(2), 10.
Tashiro, M. (2019). Japan's Crypto Association issues ICO regulation recommendations Brave New Coin. (Vol. 2019).
Tew, J. A., & Freedman, D. (1973). In Support of SEC v. W.J. Howey Co.: A Critical Analysis of the Parameters of the Economic Relationship Between an Issuer of Securities and the Securities Purchaser. *University of Miami Law Review, 27*, 407-450.
Top ICO List (2018). Benebit ICO. https://topicolist.com/ico/benebit. Accessed 20 February 2018.
Underhill, J. (2018). Initial coin offerings: Fraudsters use new technology to perpetrate old schemes. https://www.fraud-magazine.com/article.aspx?id=4295000887&Site=ACFEWEB. Accessed 31 March 2018.
Williams, R. (2019). ICO Regulations- Which are the Countries with Restrictions? *CryptoNewsZ*.
Yakubowski, M. (2019). Japan: Crypto Industry Trade Group JCBA Issues Guidelines for ICO Regulation. (Vol. 2019).
Yang, S., Xie, H., & Chen, L. Y. (2018). Renren to Scrap ICO After Talks With China Regulators, Sources Say. https://www.bloomberg.com/news/articles/2018-01-09/renren-is-said-to-scrap-ico-after-talks-with-china-regulators. Accessed 4 February 2018.
Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Ffhr, L. (2017). The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators. *SSRN Electronic Journal*, doi:10.2139/ssrn.3072298.
Zmudzinski, A. (2019). Dubai Real Estate Giant Emaar to Launch ETH Token, Considers ICO in Europe. (Vol. 2019).

[1] Initial concept for this figure was provided by Alexander Lee, "Blockchain—A Visual Explanation," Medium, https://medium.com/@kkomaz/blockchain-a-visual-explanation-afe82d19a234 (accessed 15 February 2018).