Journal of Metaverse
Review Article
Received: 2022-04-27 | **Reviewing:** 2022-04-28 & 2022-07-24 | **Accepted:** 2022-07-25 | **Online:** 2022-07-25 | **Issue Date:** 2022-12-31
Year: 2022, **Volume:** 2, Issue:2, Pages:56-61

Financial cybercrime in the Islamic Finance Metaverse

Klemens Katterbauer
Center for Islamic Metafinance
EUCLID University
Bangui, Central African Republic
katterbauer@euclidfaculty.net
0000-0001-5513-4418

Hassan Syed
EUCLID University
Bangui, Central African Republic
hassan@euclidfaculty.net
0000-0001-7641-5198

Laurent Cleenewerck
EUCLID University
Bangui, Central African Republic
cleenewerck@euclid.int
0000-0002-9267-0428

***Abstract* — Financial cybercrime in the metaverse has become increasingly more significant for authorities, corporations, and individuals to address, requiring new regulatory and compliance frameworks, as well as novel cybersecurity mechanisms in order to prevent these crimes. Financial cybercrimes in the metaverse have increased in the last years significantly, with either the massive stealing of cryptocurrencies from exchanges or the sale of fake or dubious NFT and other financial products that have lost significant value within a short period of time. Cybercrimes in the metaverse have taken place at significant scales and given the infancy of regulations as well as the virtual nature of these activities, only few crimes have been prosecuted. Islamic finance may represent a considerable opportunity for the metaverse via connecting the financial services and instruments to real and virtual assets free of speculation. The article provides several recommendations for regulators to address these cybercrime challenges and how Islamic finance can assist in these cybercrimes.**

Keywords—Islamic finance, metaverse, cybercrimes, blockchain

I. INTRODUCTION

Fraud and financial crime is a trillion-dollar industry, where companies may spend around 8.2 billion USD on anti-money laundering controls in 2017 alone, with the number rising. Financial crimes have increased year on year, with both detected and undetected crimes increasing significantly. Furthermore, fraud itself may cause significantly associated cost that make these cybercrimes even costlier [1]. Generally, banks face various risks arising from cybercrime, including the vulnerabilities that relate to financial and fraud crimes in automation and digitization, the massive growth in transactions, and the integration of financial systems within countries. Cybercrime and malicious hacking have significantly intensified. Financial crimes have led to a significant number of regulators that revise rules and account for illegal trafficking and money laundering [2]. There have been economic sanctions, which target both countries, public and private entities. Institutions are more and more realizing that conventional approaches to combating financial cybercrimes are not sufficient, and this requires them to become more nimble. In order to enhance detection, interdiction, and prevention, there is a distinction between fraud and financial crime. New cyberthreats have led to a blurring of these two concepts, and criminal activities have become more complex and interrelated. Legally, there is no distinction in regulation between the two concepts, but the difference arises primarily due to organizational aspects. Normally, financial crimes relate to money laundering and other criminal transgressions, which includes bribery and tax evasion. These involve the use of financial services to support criminal enterprises. The challenges typically arise as a result of compliance issues, specifically when financial institutions avert fines with anti-money laundering activities [3].

Fraud can be generally considered as a host of crimes, which involve forgery, credit scams, and insider threats. This involves both the deception of financial personnel or services in order to achieve theft. Fraud is generally considered as a loss problem and financial institutions apply advanced analytics for the detection and real-time interdiction. The challenges arise from the fact that these crimes often are often together and merge in the metaverse [4].

The Carbanak attacks in 2013 represented a great illustration of financial cybercrimes and fraud. This totaled more than 1 billion USD, and the criminals gained access to the system via phishing, and the fraudulent inflation of balances enabled them to dispense the cash at ATMs. The first weak link was via spear-phishing, which involved the sending of emails with an attachment that installed the Carbanak backdoor (*Figure 1*). This allows to open the backdoor and steal its credentials. With access to the PC, the backdoor allows to search for Admin PCs that allow inflating balances and mimics the behavior of the admins. The criminals then inflate the balances and subsequently retrieve the funds via wire transfer or cash dispense at ATMs [5].

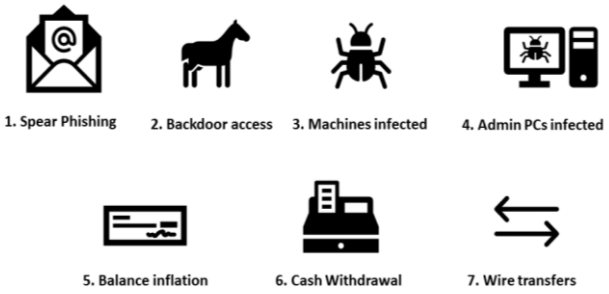

Figure 1: Cyber profile attack format

The challenge arose from the fact that the crime was simultaneously conducted against several banks and utilized their knowledge of the cyber environment, the banking processes, and controls. Furthermore, the criminals were fully aware of the vulnerabilities that arose from the organization's silos and governance. Furthermore, several channels, such as ATMs, credit and debit cards in addition to wire transfers were deployed [6]. This combination of various different methods outlines that fraud, cyberattacks and financial crimes are integrated with each other (*Figure 2*).

Figure 2: Convergence of crimes.

The existing silo approach to these interconnected risks represents a key challenge for many banks and financial providers. Until recent times, most of the fraud is based on transactions where the criminals exploit the weaknesses in the controls of the corporation. These fraud activities can be encountered relatively with channel-specific and point-based controls. Identity-based fraud activities have increased significantly where fraudsters exploit natural or synthetic data [7]. The ambitions of attacks are more ambitious in terms of scope and present everywhere. Digital trust is a critical component of customer experience for many financial service providers and banks, which requires a seamless, secure and speedy digital interface. Challenges arise from the demand for faster risk management, which requires to have solutions available. Challenges arise from the rising cost and lack of comprehensive regulations that address these challenges [8].

Given the growing digitalization and development of the metaverse, many institutions aim to combine efforts to combat financial crime, fraud and cybercrime.

Important is to define the nature of risk-management activities and to be clear about the roles and responsibilities, such that there is complete and clearly delineated coverage. The main countermeasures to combat financial crime involve the identification and authentication of the customer, the monitoring and detection of transactions, and the analysis of behavioral anomalies in addition to the mitigation of risks. The combination of data sources together with analytics enhances visibility and provides a greater insight to enhance detection capabilities [9].

In order to understand better the potential designs that can be considered for dealing with cybercrimes and fraud, there are various operating models that may be taken. These are collaborative, partially integrated, and unified models.

The collaborative model is amongst the most common forms where the domains related to financial crime, fraud, and cybersecurity are independent and have separate roles, responsibilities, and cybersecurity. Each of the units has its own independent framework, cooperating on any risk taxonomy and the data and analytics related to the monitoring of transactions, as well as fraud and other breaches. The challenge is that such an approach limits the transparency related to financial-crime risk, and there may be some coverage gaps in addition to overlaps amongst the groups. Integration is relatively limited as well.

A different approach is the partial integration model for cybersecurity and fraud, which has been taken up by many institutions and regulators. The units maintain their independence but work on a consistent framework and taxonomy. This follows some accepted rules and responsibilities. This implies that a consistent framework for the prevention, risk identification, and assessment process is integrated. Consistency in threat monitoring and detection is improved, but the existing organizational structures do not lead to enhanced transparency. There is furthermore only limited benefit of scale, and the operational units represent a challenge [10].

The final unified model integrates financial crimes, fraud, and cybersecurity operations into a single framework. This leads to the maintenance of common assets and systems via which all the risks are managed in the enterprise. This allows having a single view of customers and the sharing of analytics. This allows to enhance enterprise-wide transparency and outline the underlying risks.

While these new models have led to improvements in how corporations deal with certain forms of cybercrimes, the metaverse represents a completely new challenge in how financial crimes are conducted.

The word "metaverse" has been encountered everywhere in recent years, with Facebook changing its name officially to Meta [1]. Non-fungible tokens (NFT) have become one of the major words of the year, where these tokens form a key part of the virtual universe. This has also led gamers and developers to move into this space, making it more and more attractive to conventional consumers. While there has been considerable attention around the virtual universe, understanding the environment behind the virtual universe and what value it creates is of critical importance. The land prices related to digital land have been on the rise, with Republic Real Estate launching a fund for investors to purchase virtual land [2]. The fund will purchase virtual land across various online metaverses and transform them into hotels, stores, and other uses. This shall lead to an increase in the value of these properties amongst consumers.

While virtual land has, due to its connotation with physical land, attracted considerable interest, the art sector related to NFTs has experienced an even more significant rise, and there is the expectation that equities and bonds will be hosted on a digital asset platform that is built around blockchain technology. Another key area of the metaverse is the gradual online-only shopping and experience, which implies that individuals purchase assets that are entirely virtual. There are several stores that sell clothing and accessories entirely online, which only exist in the metaverse. Furthermore, there are virtual fashion shoes solely for the virtual world, which has attracted considerable investment amounts. The growing remote work operational model, in addition to the growing utilization of artificial intelligence and virtual technologies, has opened up new business models providing customers with different experiences in the virtual world. Another key change is the move towards remote work, where the metaverse can make remote work more permanent and immersive in order to maximize efficiency and interaction. This will enable stronger interaction and engagement of the employees [3].

Given the growing importance of the metaverse, the financial industry has been looking into how to create value within the metaverse space and how fintech solutions can

deliver financial services in this new environment. Furthermore, metaverse technology creates new business model opportunities that may strengthen the utilization of crypto-technology as an alternative financial system.

The technologies behind the metaverse combine technologies such as virtual reality (VR) and augmented reality (AR). This leads to an interactive, immersive and collaborative virtual 3D universe. The idea is that these individual universes may be integrated with each other as well as allowed to connect across the world in various environments. This may be in the form of games but also in terms of real estate, commercial transactions, and other associated environments [4].

As outlined by Facebook's transformation into Meta, financial data and transaction management will become key parts of the metaverse enabling individuals and corporations to transact and operate within these universes. For example, there are digital assets for purchase, such as the World of Warcraft and the Habbo Hotel, and these assets may be even moved from one universe into the other [1].

The current metaverse is a composition of the capabilities of various social media and video game enterprises that build upon their user base and platform in order to connect these individuals. While this first glance may give the impression that the metaverse is solely about gaming, it has become more of another virtual world where individuals may be fully immersed and conduct most of their life within the metaverse. This may range from dating to having their social interactions within the metaverse, but also conduct business across it. This may be in the form of leading a real enterprise or a digital enterprise within the metaverse. Overall, this will lead to someone being completely immersed in the metaverse and living their daily lives within this universe.

II. BLOCKCHAIN AND ITS IMPACT ON FINANCIAL CYBERCRIME

Blockchain technologies have facilitated the development of cryptocurrencies in the last decade. Cryptocurrencies are a collection of binary data that act as medium of exchange, and the individual ownership is stored in a ledger. The ledger is a general database that utilizes strong cryptography in order to secure transaction records. Most cryptocurrencies are fiat currencies that are not backed by or convertible into commodities, such as gold. While most cryptocurrencies have posited their decentralized nature there are several crypto schemes that utilize validators in order to enhance security and maintenance. Furthermore, proof-of-stake models provide the owners with the option to put the tokens as collateral. They subsequently obtain the token in proportion to the amounted stake, and with ownership of the token, there are additional benefits such as network fees, newly minted tokens, or other reward mechanisms. Cryptocurrencies distinguish themselves in their most modern form in terms of that they are not issued mostly by central authorities. While there have been initiatives from central banks to adopt digital currencies, such as the digital yuan or digital euro, most of the existing cryptocurrencies do not have a central authority that controls them but rather rely on decentralized control. This provides some unique opportunities to reduce transaction costs and enable direct transactions without the need for a middleman [15].

While this has opened an entirely new business model, it has also changed the world of crime. Cryptocurrencies pride themselves on being decentralized and independent, which makes them also difficult to trace, given that transactions may pass by conventional banking institutions and central banks. This lack of centralized supervisory allows individuals to perform transactions without any middlemen validating the transaction. Such transactions share similarities with cash transactions that allow individuals to remain totally anonymous. The most famous and recent example of governments aiming at preventing crime and reducing black market transactions is India, where the government invalidated all 500 and 1000 INR banknotes. The assumption was that removing these banknotes as legal tenders overnight would require criminals to declare and deposit their funds in banks, which allows the authorities to track whether someone has extensively underreported transactions as compared to their overall funds [16]. While the disruption has led to considerable economic challenges for the general population, the benefits from the initiative have been limited. The main challenge that arose is that many of the transactions and wealth stored from illegal businesses were already in forms other than banknotes or already processed via the banking system. Additionally, much of the wealth accumulated is also in the form of property, industrial investments, and foreign currencies. Nevertheless, criminals face the challenge that banknotes are issued by a central authority, which makes it a challenge to freely utilize the funds and transfer them across their operations. For wire transfers, the transactions are typically processed via major transaction centers that are subject to restrictions within the jurisdiction they are located in. For example, almost all USD transactions move through the SWIFT network, with US-based institutions performing the intermediary role. If a criminal is flagged within such a transaction, then the transaction may not go through as well as the funds may be frozen. While this has not proven to be failsafe, it has led to a significant reduction in the ability of criminals to utilize the conventional financial system for committing crimes and transferring funds.

Cryptocurrencies distinguish themselves in terms of their decentralized nature, which implies that two parties may conduct a transaction directly between themselves. This implies the absence of a centralized validating party that would otherwise validate and control the transaction. The advantage for criminals is that these transactions can be executed independently and cannot be easily traced. In a simple example, hostage-takers may receive the ransom amount in bitcoin, which can be easily stored and exchanged on the global cryptocurrency market without the ability of authorities to trace the transactions. Furthermore, as the bitcoins are not uniquely identifiable in the blockchain, this further makes these transactions and what was conducted with the received bitcoins impossible to trace [17].

This lack of transparency and anonymity for transacting parties represents an encouragement for criminals to engage in crimes. As the oil pipeline cyberattack has demonstrated, criminals may have a strong preference for cryptocurrency payments given its anonymity and ease of moving around. A USD transaction would require a more elaborate scheme of setting up different bank accounts in various jurisdictions and then converting those funds into banknotes that may be

transported across borders. The Bangladesh Central Bank heist was such an example. Even the transport across borders of these banknotes is a challenge by itself and may lead to confiscation. In contrast, transferring cryptocurrencies from one wallet to another and going from cold storage to hot storage can be done within seconds, which significantly simplifies criminal activity [18].

The recommendation to regulators is to address these challenges with dedicated regulations related to blockchain technology and cybercrime. This may be in the form of real name verification for transactions of cryptocurrencies and the requirement for digital wallet providers to know their customers.

III. VPNs and Proxies and Their Impact on Financial Cybercrime

Virtual private networks and proxies represent another key area of crime facilitation. Virtual private networks extend private networks across the public network and enable users to both send and receive data across shared or public networks in the same form as if they were directly connected to each other. The benefits of VPNs are significant, as it allows to increase functionality, security, and the management of private networks as well as allow individual members to make central resources accessible from anywhere. VPNs have long been of strong interest for criminals to mask their operations and imitate the access of websites from various locations. Specifically, modern VPN services allow the VPN to utilize several VPN gateways and proxies in order to access the internet. Any website that is accessed solely sees the public IP address of the proxy irrespective of where the accessing computer is really located. This masking of the IP address and location allows individuals to access the internet from anywhere without being recognized. This also makes it challenging for law enforcement to determine where the access was made from and may also implicate on purpose a wrong IP address or computer in order to make law enforcement believe that they have caught the criminal [19].

A very famous example was the case of the provider "DoubleVPN" that was recently taken down. The main advantage of the VPN provider was to allow ransomware operators and phishing fraudsters to gain high anonymity via multiple interconnected VPN connections that enabled multiple layers of encryption. While the masking by itself is, in most circumstances, not a crime, the ransomware and phishing attacks conducted by these criminals is, in most circumstances, the crime. While many governments impose restrictions on the encryption technology that can be sold within the jurisdiction and have the right to request the decryption of data, access, and ability to decrypt modern encrypted VPN connections has become significantly more challenging. Improved encryption technology has made it far more complex to decrypt and extract information, which enhances the ability of criminals to evade law enforcement [20].

IV. Islamic Finance Cybercrimes in the Metaverse

The metaverse has become a major feature of attraction that will encompass some of the challenges existing social media and platforms face. Specifically, there have been several financial misconducts where individuals utilized social media in order to compromise individuals and extract financial gain from them. While the metaverse is created, it encompasses all of the challenges that may arise from the creation of a new virtual world. Given that this virtual world shall provide a complementary dimension to everyday life, where individuals interact and engage, this makes the challenges of financial crime even more prominent [21].

As Islamic finance has gained prominence as a facilitator for fairer financial relationships and its connection to real value creation, Islamic finance will also play a critical role in the metaverse. The metaverse represents a significant opportunity to provide Islamic financing in the metaverse and link the financing opportunities to the metaverse operations. Given that the metaverse is a virtual reality of the world, existing challenges related to cybercrimes for Islamic finance will be amplified in the metaverse. A key aspect is that the metaverse will be a virtual world but will be connected extensively to the physical world but allow to do things that are not possible in the physical world. For example, one may instantaneously travel and purchase items in the metaverse without the need for extensive physical travel or being subject to certain regulations. While the metaverse is famous for its integration of 3D virtual reality, augmented reality, open-source development, and artificial intelligence. Peer-to-peer payments and non-fungible tokens are other key features that will be present in the metaverse [22, 23].

This clearly outlines several challenges that may lead to the exploitation of these instruments. The financial cybercrimes in the metaverse encompass various forms. First, competitive gaming within the metaverse may lead to a compromise of the game in favor of one party, leading to significant losses of other players. Cybercriminals exploit weaknesses in the security of games in order to manipulate these. While being perceived as legitimate, the games are biased and lead to negative effects for the individuals.

Another key factor in Islamic finance in the metaverse and potential cybercrimes is the presence of cryptocurrencies. Cryptocurrencies have taken on various forms, be it in the form of volatile and unpegged ones, such as CRO or ETH, and stablecoins that are pegged to a financial asset. All of these experience challenges as they are mostly unregulated and are not covered by depositor protection.

Cryptocurrencies are generally permissible in Islamic finance as they are a means of exchange for the trading of physical goods. While volatility and the arising speculative nature has been a challenge, they do not make cryptocurrencies impermissible. Furthermore, cryptocurrencies being utilized for illegal activities and cybercrimes do not make these cryptocurrencies impermissible or prohibited. The main challenge arises that these cryptocurrencies may evade regulatory oversight and may be utilized for impermissible activities [24]. For example, cryptocurrencies may be utilized for gambling and related activities in the metaverse, which are clearly forbidden in Islamic finance. Individuals may either request financing for these illegal activities, or may try to disguise the activities utilizing existing financing forms. Such cybercrimes and compliance issues with respect to Shariah law have to be taken into account and compliant [25].

The development of non-fungible tokens and growing interest by investors in the metaverse have led to enormous valuations of such assets. This has also been observed in the metaverse, where non-fungible tokens represent ownership of an asset. While in many instances the NFT is connected to physical assets, this may not be the case, and the NFT may refer to a virtual asset that may be more closely considered fraudulent as compared to having any real value. Islamic principles forbid uncertainty and any fraudulent behavior, which acts as a significant deterrent for cybercriminals being able to exploit such instances for their own benefit. Given that there has to be either a connection to a physical asset or a virtual asset with limited speculative room, this necessarily reduces the possibility of fraud.

Regulators should focus on developing a comprehensive legal framework for Islamic finance in the metaverse that takes into account cybercrimes related to the Islamic financial products.

V. Conclusion

Financial cybercrime in the metaverse has become increasingly more significant for authorities, corporations, and individuals to address, requiring new regulatory and compliance frameworks, as well as novel cybersecurity mechanisms in order to prevent these crimes. Financial cybercrimes in the metaverse have increased in the last years significantly, with either the massive stealing of cryptocurrencies from exchanges or the sale of fake or dubious NFT and other financial products that have lost significant value within a short period of time. Cybercrimes in the metaverse have taken place at significant scales, and given the infancy of regulations as well as the virtual nature of these activities, only few crimes have been prosecuted. Islamic finance may represent a considerable opportunity for the metaverse via connecting the financial services and instruments to real and virtual assets free of speculation.

Acknowledgment

We would like to thank EUCLID University for supporting this work.

References

[1] E. R. Leukfeldt, A. Lavorgna and E. R. Kleemans, "Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime.," *European Journal on Criminal Policy and Research,* vol. 23, no. 3, pp. 287-300, 2017.

[2] J. Nicholls, A. Kuppa and N. A. Le-Khac, "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape.," *IEEE Access,* 2021.

[3] E. R. Leukfeldt, E. W. Kruisbergen, E. R. Kleemans and R. A. Roks, "Organized financial cybercrime: Criminal cooperation, logistic bottlenecks, and money flows.," *The Palgrave Handbook of International Cybercrime and Cyberdeviance,* pp. 961-980, 2020.

[4] J. M. Karpoff, "The future of financial fraud.," *Journal of Corporate Finance,* vol. 66, p. 101694, 2021.

[5] S. Hasham, S. Joshi and D. Mikkelsen, "Financial crime and fraud in the age of cybersecurity.," McKinsey & Company, 2019.

[6] S. Kwon, J. Jeong and T. Shon, "Digital forensic readiness for financial network.," in *2019 International Conference on Platform Technology and Service (PlatCon)*, 2019.

[7] S. Y. K. Wang and M. L. Hsieh, "The ATM Hacking Case," in *Digital Robbery*, Springer, 2021, pp. 15-32.

[8] S. Varga, J. Brynielsson and U. Franke, "Cyber-threat perception and risk management in the Swedish financial sector.," *Computers & Security,* p. 102239, 2021.

[9] O. A. Erin, A. D. Kolawole and A. O. Noah, "Risk governance and cybercrime: the hierarchical regression approach.," *Future Business Journal,* vol. 6, pp. 1-15, 2020.

[10] S. M. Karsh, "Emerging Innovation Risk Management in Financial Institutions of United States.," *Economics and Business Quarterly Reviews,* vol. 4, no. 2, 2021.

[11] S.-M. Park and Y.-G. Kim, "A Metaverse: taxonomy, components, applications, and open challenges.," *IEEE Access,* 2022.

[12] N. G. Narin, "A Content Analysis of the Metaverse Articles," *Journal of Metaverse ,* pp. 17-24, 2021.

[13] K. B. Wilson, A. Karg and H. Ghaderi, ". Prospecting non-fungible tokens in the digital economy: Stakeholders and ecosystem, risk and opportunity.," *Business Horizons,* 2021.

[14] I. Wohlgenannt, A. Simons and S. Stieglitz, "Virtual reality," *Business & Information Systems Engineering*, pp. 455-461, 2020.

[15] E. Reddy and A. Minnaar, "Cryptocurrency: A tool and target for cybercrime.," *Acta Criminologica: African Journal of Criminology & Victimology,* vol. 31, no. 3, pp. 71-92, 2018.

[16] B. Sivathanu, " Adoption of digital payment systems in the era of demonetization in India: An empirical study.," *Journal of Science and Technology Policy Management,* 2018.

[17] A. Trozze, J. Kamps, E. A. Akartuna, F. J. Hetzel, B. Kleinberg, T. Davies and S. D. Johnson, "Cryptocurrencies and future financial crime.," *Crime Science,* vol. 11, no. 1, pp. 1-35, 2022.

[18] F. M. Teichmann and M. C. Falker, "Cryptocurrencies and financial crime: solutions from Liechtenstein.," *Journal of Money Laundering Control,* 2020.

[19] W. Ronhaar, W. B. Zehner and R. Langhorne, "Zero Identity—The New Cybersecurity Paradigm," *Marketing of Scientific and Research Organizations,* vol. 42, no. 4, pp. 97-109, 2021.

[20] A. Shah and D. Chudasama, "Investigating Various Approaches and Ways to Detect Cybercrime.," *Journal of Network Security,* vol. 9, no. 2, pp. 12-20, 2021.

[21] M. Ayub, Understanding Islamic Finance, Chichester: John Wiley & Sons, 2007.

[22] M. K. Hassan and R. N. Kayed, "The global financial crisis, risk management and social justice in Islamic finance.," *Risk Management and Social Justice in Islamic Finance,* 2009.

[23] H. Mohamed and H. Ali, Blockchain, Fintech, and Islamic finance: Building the future in the new Islamic digital economy., Berlin: Walter de Gruyter Gmbh & Co KG, 2018.

[24] U. Oseni and N. Ali, Fintech in Islamic finance, Routledge, 2019.

[25] C. Paldi, "Understanding riba and gharar in Islamic finance.," *Journal of Islamic Banking and Finance,* vol. 2, no. 1, pp. 249-259, 2014.