

Cross-strait Virtual Currency Crime and Anti-Money Laundering Trends

兩岸虛擬貨幣及洗錢犯罪趨勢

Wei, Chih-Chieh (魏至潔)*

Specialist, Anti-Money Laundering Office, Executive Yuan

Abstract

The movement of people across the Taiwan Strait will not be realized from 2020 to 2021 due to travel restrictions due to the COVID-19 epidemic. However, virtual currency crimes and money laundering on both sides of the strait continue to penetrate below the table through various channels. This article hopes to use a superficial study of cross-strait crimes related to virtual currency to explore the growth and decline of cross-strait virtual currency crimes and the correlation with money laundering crimes under the epidemic. Virtual currency is an epoch-making invention in human history. Decentralized block chain technology redefines currency

* The author is Certified Anti-Money Laundering Specialist (CAMS), Certified Fraud Examiners (CFE), Certified Bitcoin Professional (CBP), Certified Global Sanctions Specialist (CGSS) and APG Assessor (2020-2022 Brunei), Bachelor of Political Science, National Taiwan University, currently studying at the School of Law of National Yangming Chiaotong University. Special thanks to Cross-strait Status Research & Analysis Division, Investigation Bureau, Ministry of Justice and Lincy LIN specialist of Ministry of Justice of inviting and proofreading.

and the relationship between people and money. Virtual currency itself has no difference between good and bad. However, how many crimes use the name of virtual currency to cause many victims. To investigate such crimes requires brand-new thinking and skills in order to actually stop the crime. It is worth mentioning that the decline in virtual currency crime data due to the isolation policies of various countries may be an unexpected result. Whether similar crimes cannot be spread due to interpersonal alienation is worth our continued observation.

Keywords: Virtual Currency, COVID-19 Epidemic, Criminal Typology, Anti-money Laundering, Cross-strait Crime



I. Preface

Prohibition of going abroad is enacted worldwide because of the coronavirus; however, the restriction only confine the flood of people, but fail to block the flood of “money” and the flow of criminal proceeds. Therefore, the money flow that can be estimated may be greater than the flow before the epidemic.

Since Satoshi Nakamoto published his first paper¹ about “decentralized virtual currency” on the internet in 2008, virtual currency has subverted our traditional imagination of money. “Money” seems to transform from paper money to a string of numbers, a pile of wallet address and private key or public key. Perhaps we are still accustomed to the sense of security of cash, but virtual currency has already changed our world quietly. The Financial Action Task Force (FATF) is the international norms maker for global money laundering prevention and combating terrorism financing. From 2018 to 2019, FATF warned that criminals liked to use virtual currency for black market trading, and money laundering in dark web. FATF has successively released documents such as virtual asset guidelines and virtual asset red flag indicators in 2019 and 2020.² These have become the legal basis for law enforcement agencies for many countries around the world in supervision for virtual assets.

Today pandemic is still ongoing, we would like to explore the typology and trend of cross-strait virtual currency crimes and money laundering from

¹ Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” (October 31, 2008), download date: March 25, 2021, 《Google》, <https://bitcoin.org/bitcoin.pdf>.

² FATF, “FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers” (June 2019), and “FATF REPORT Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing” (September 2020), visited date: March 17, 2021, 《FATF》, [https://www.fatfgafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc\(fatf_releasedate\)](https://www.fatfgafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)).

the cash flow movement aspects. Hopefully this will bring more new ideas for law enforcement agencies.

II. Overview of Virtual Currency

After Bitcoin released, virtual currency, digital currency, encryption currency (cryptocurrency) and other emerging terminology emerged on the internet. This is a complete new concept, so the definition is still ambiguous. In 2013, the US Treasury Department Financial Crimes Enforcement Network (FinCEN) defined it as: “a medium of exchange that can operate like currency but does not have all the attributes of ‘real’ currency, as defined in federal regulations, including legal tender status.”³ In 2014, the European Banking Authority defined it as “a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money.”⁴ In 2015, FATF issued guidelines on basic methods of virtual currency risk to the world,⁵ and it still used “Virtual Currency” to define Bitcoin and other encryption or digital currency. In June 2019, FATF held annual meetings in the United States, inviting member states to discuss the upcoming virtual assets and industry risk-based approach.⁶ However, some member states considered the definition of “virtual currency” too

³ Wikipedia, “virtual currency” (April 6, 2014), visited date: March 18, 2021, 《Wikipedia》, <https://zh.wikipedia.org/wiki/%E8%99%9A%E6%8B%9F%E8%B4%A7%E5%B8%81>.

⁴ Wikipedia, “virtual currency” .

⁵ FATF, “Guidance for a Risk-Based Approach to Virtual Currencies” (June 2015), visited date: March 18, 2021, 《FATF》, <http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html>.

⁶ FATF, “Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers” (June 2019) , visited date: March 18, 2021, 《FATF》, <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>.

narrow, and couldn't cover all the concepts around the world; therefore, they settled for "virtual assets" out of recommendation from experts and vote result.⁷ FATF also announced the 12-month review mechanism, that is, until June 2020, all member states should follow FATF guidelines to legislate or amend relevant municipal laws in line with international standards.

From the evolution of the definition of "virtual currency", it is not difficult for us to find that countries around the world, especially powerful countries, are anxious about virtual currency control. This article will define the "virtual currency 'as' digital encrypted currency using cryptography to the center of the block chain technology, but does not include two-way exchange game currency, points, etc." For the sake of article's acceptability, the definition "virtual assets" by FATF will be referred as "currency" in this article, which is also different from our traditional understanding of the currency concept defined by the central bank. Due to different regulatory standards in different countries, virtual currency may not be used in daily trading and payment. Take China as an example. Virtual currency is only regarded as a tradable "financial commodity", similar to stocks or futures, and cannot be used in daily life or instant payment; therefore, it's not "currency".

In mainland China, where the traditional market or even beggars do not accept cash banknotes, the concept "you don't necessarily have to bring wallet when going out but be sure to have your smart phone" has become Chinese people's payment habits, and even "face scan" can complete

⁷ Peiling Tsai & Chih-Chieh Wei, participated in 2019 "Prevention of money laundering Financial Action Task Force organization" The 30th of 3 times and the General Assembly working group (Working Group Meetings and Third Plenary Meeting of FATF XXX 2019) report go abroad" (September 2019), pp. 13, 24-25.



the payment. It seems to have completed the “Great Leap Forward” in the history of human finance. Such drastic changes are of course related to the internal financial situation and stability maintenance in Mainland China. Due to anonymity of cash and the difficulty of tracking the cash flow, it is easy to cause criminal investigation breakpoints and high risks of money laundering. Therefore, mainland China directly introduces mobile payments to track every transaction, making the transparency of cash flow possible. Although mobile payment market is booming in China, the first country to ban virtual currency is also China. The main reason for its illegality is the aspiration from People’s Bank of China to issue its own virtual currency. RMB digitization is a long-term policy; therefore, in order to maintain government full control and monetary stability, any virtual currency development in China is not allowed. The development of RMB digitization has been 6 years, and is expected to come out in 2022. The goal is to replace parts of the legal currency and banknotes, and then digital RMB(e-CNY) exchanges RMB in circulation, so it will not increase the total amount of currency.⁸ However, during the period before e-CNY is officially introduced, there are frauds and hypes of virtual currency, which is deeply correlated with its characteristics. The followings will focus on the discussion and analysis of the characteristics and the abuse in crime.

1. Features of virtual currency

Currently, there are more than a thousand kinds of virtual currencies with different characteristics. Take Bitcoin as an example. Its most outstanding features can be summarized as: limited number, infinite

⁸ Tai-Jie Jian, “China People’s Bank to implement digital RMB fastest in 2022 on the road” (October 7, 2020), visited date: March 18, 2021, *《Anue News Network》*, <https://news.cnyes.com/news/id/4530148>.



divisibility, cannot be forged, transaction security and anonymity, etc.⁹ Limited number attributes to the founder Satoshi's design. The cap of Bitcoins issuing is 21 million, and the output is cut in half every 4 years, so in 2020 the supply is about 18 million. When all Bitcoins are issued, there will be no new Bitcoin. The amount control creates its scarcity value. Infinite divisibility: each coin is split down to decimal 8 digits unlimitedly, based on a mathematical virtual currency fundamentals and password. Therefore, the transaction, which is not necessarily limited to the number of entities, is very convenient. Cannot be forged and transaction security: Bitcoin is built on the basis of block chain technology, allowing multi-node decentralized verification. In short, block chain technology is the science of verifying the authenticity of transactions through complex cryptography and computer operations. Finally, anonymity: all Bitcoins transactions are transparent, including source and destination, that are made public on the Internet; however, it only shows the location of the virtual wallet or IP node, that can't lead us to track the real users unless the transaction adopts a real-name system. The transaction in dark web or private transactions exclude us from identifying the information of the buyers and sellers.

2. Being abused for crime

In recent years, as the prevention and control of money laundering and combating financing terrorism rules and regulations get increasingly stringent, the illegal proceeds acquired through traditional money-laundering technique and dirty money encountered obstacles. Therefore,

⁹ Soft Currency of Knowledge, "than the special characteristics of the coin - the five main characteristics and differences in legal tender," visited date: March 29, 2021, *《Soft Currency of knowledge network》*, <https://know.zombit.info/%E6%AF%94%E7%89%B9%E5%B9%A3%E7%9A%84%E7%89%B9%E6%80%A7/>.

anonymity of virtual currency lead to wide use from terrorist organizations, and many are used for the laundering of criminal proceeds and illegal transactions. Virtual currency trading has become a common payment instrument in many famous dark web, such as Silk Road. A few years ago, before terrorist organizations got familiar with virtual currency trading operation, they used conventional illegal business to obtain financial resources. In recent years, they all turn to virtual currency. According to The New York Times reports,¹⁰ the terrorist organization Qassam Brigades has raised funds through virtual currency by setting up website rendering seven languages, since the end of 2018. It provides video demonstrating Bitcoin transaction that can't be supervised by law enforcement authorities. Terrorist organizations have learned how to conceal cash flow track by not using any real bank account with any Bitcoin transaction, so law enforcement agencies have no way to track the customer information. Terrorist organizations obtain whole control over money flow and successfully form a breakpoint in the investigation.

III. Virtual Currency Crime Typology in Taiwan

According to the Judicial Yuan's Legal Information Retrieval System, there are 334 cases with the keyword¹¹ "virtual currency" from 1 Jan, 2020 to 16 Mar, 2021. According to classification criteria, 187 cases related to virtual currency crime (including fraud), accounting for 55.95%; 48 cases

¹⁰ Xiuyu Liao, "Western countries cut off the flow of gold, where does the 'holy warrior' money come from?"; "specific special coins become popular means of financing a terrorist organization!" (August 20, 2019), visited date: March 18, 2021, 《Wind Media》, <https://www.storm.mg/article/1611037>.

¹¹ "Judicial court legal information retrieval system, judgment query system," visited date: March 18, 2021, 《Judicial Court》, <https://law.judicial.gov.tw/FJUD/default.aspx>.

related to Banking Law (commonly known as money absorption cases), accounting for 14.37%; 29 cases related to Money Laundering Control Act, accounting for 8.68%; 23 cases related to Narcotics Hazard Prevention Act, accounting for 6.88% . The followings are the common crimes of virtual currency in Taiwan.

1. Crime of fraud

Taiwanese government conducted its first national money laundering and terrorist financing risk assessment during 2017 to 2018. At that time, fraud ranked second out of the eight types of high-risk crimes, and its crime threat risk was second only to drug crimes.¹² The author analyzes the court cases from the past year concerning virtual currency fraud crimes, where most victims were lured into virtual currency investments, and got mislead. Telecommunications fraud, LINE messages and Internet scams are the main types.

2. Violation of Banking Law

Criminals often claim that they have channels to invest in various virtual currencies and have a fixed proportion of income. After raising a large amount of funds, they will withdraw all the funds so as to “massacre” the victims. According to Article 29-1 and the Article 29 of the Banking Act, non-banking operators must not accept deposits, fiduciary managers trust funds, public property or apply for domestic and foreign exchange business; the other borrower, receiving investment, or the addition of other shareholders in name, accepting money or absorbing funds from a large number of people, and agreeing or paying dividends, interest, dividends

¹² Anti-Money Laundering Office, Executive Yuan, “National Money Laundering and Terrorism Risk Assessment Report” (April, 2018), downloaded date: March 19, 2021, 《*Anti-Money Laundering Office, Executive Yuan*》, <https://www.amlo.moj.gov.tw/1461/16645/16721/post> .

or other remunerations that are not equivalent to the principal , in order to accept deposits, so the illegal act of absorbing money is suspected of violating the Banking Law .

3. Violation of Money Laundering Control Act

In this type of crime typology, most of the fraud groups swindled victims by providing remuneration, and ask the victim for a virtual currency investment account for the fraud group as straw man accounts,¹³ or use them as money mules. These are found to have violated Article 14 and Article 15 of the Money Laundering Control Act.

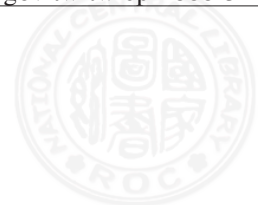
4. Violation of the Narcotics Hazard Prevention Act

Mostly, this type of crime is to use virtual currency to purchase drug-containing products from foreign countries, which violates Article 4, Item 2, Article 17, Item 2, and Item 3. and other provisions of Narcotics Hazard Prevention Act. Therefore, from such cases, we found that virtual currency has become the common payment tool to buy drugs or illegal goods online.

5. Summary

Based on the above research and analysis, we can summarize the

¹³ According to the Court of Justice in Criminal Tribunal released 108 annual stage characters of the 3101 number of violations Money Laundering Control Act press releases , Grand Chamber said: “perpetrator to provide financial account ATM card and password I do not The person you know is not a money laundering act referred to in Article 2 of the Money Laundering Prevention and Control Act , and is not a principal offender of the general money laundering crime in Article 14 (1) of the same law ; if the perpetrator knows the account subjectively, it may be used as a specific crime for accepting and withdrawing money The use of the income, after being withdrawn by others, will have the effect of blocking the flow of funds to avoid state prosecution and punishment. It is still provided based on the intent to help, and it should be used to help the crime of general money laundering in Article 14 Paragraph 1 of the same law” (December 16, 2020), visited date: March 18, 2021, 《*Judicial Yuan*》, <https://www.judicial.gov.tw/tw/cp-1888-341426-62a49-1.html> .



main crimes of virtual currency in Taiwan. However, some types of crimes cannot be clearly distinguished according to their criminal behavior because they may also violate other crimes. That is, one act contains several crimes. Most of the virtual currency-related crimes are investment fraud, and only a few are online drug purchase. It is noteworthy that most crimes are committed through web network, LINE, etc.

Table 1 Taiwanese Courts of Virtual Currency Criminal Judgments Summary (January 1, 2020 to March 16, 2021)

Taiwanese courts virtual currency criminal offenses substantive judgments			
The name of law	Criminal appearance	Law	Representative judgment
The Criminal law fraud crime	LINE Investment Information Fraud, Telecom , Internet Fraud	Article 339 and Article 339-1 to 4 of the Criminal Law of the Republic of China.	Taiwan New Taipei District Court No. 1215 criminal judgments(2019)
The Banking Law	Investment Scams / Ponzi Scam	Article 29 and Article 29-1 of the Banking Law.	Taiwan High Court No. 23 criminal judgments(2020)
The Money Laundering Control Act	Straw man account/ money mule	Article 14 and Article 15 of the Money Laundering Control Act.	Taiwan Taipei court No. 166 criminal judgments(2020)
The Narcotics Hazard Prevention Act	Use virtual currency to purchase drug-containing products	The newly revised Narcotics Hazard Prevention Act Article 4 Item 2, Article 17, Item 2 and Item 3.	Taiwan High Court's Criminal Judgment No. 4052(2020)

Source: Organized by author.



IV. the Typology of Virtual Currency Crime in Mainland China

In China, virtual currency is called “digital currency”, due to the conservative attitude of Chinese official. Since 2017 the competent authorities “Chinese People’s Bank” has implemented a comprehensive virtual currency ban to suppress virtual currency developments; hence, any act involving virtual currency or block chain is considered a violation of the law. On March 19, 2021, the Supreme People’s Court of China and the People’s Bank of China jointly issued the “Typical Cases of Punishing Money Laundering Crimes”,¹⁴ and “virtual currency money laundering” appears in the official document as “typical money-laundering case”, demonstrating the high-strength supervision control over virtual currency crime from China. There are many virtual currency crimes concerning money laundering, and China’s official declared that virtual currency was one of the emerging criminal methods of money laundering.

According to the judge’s conviction of China Judgment Documents Network¹⁵ classification, there are roughly several kinds: organization crime so called MLM¹⁶ or pyramid schemes, illegal absorbing public deposits crime, fraud, extortion, illegal business and illegal control of computer information systems and other crimes. The features are: involving many victims, and high amount of proceed of crime. The important types of crimes are discussed below.

¹⁴ China Supreme People’s online conference hall, “Punishment of the crime of money laundering typical case” (March 19, 2021), visited date: March 23, 2021, 《China Supreme People’s online conference hall》, https://www.spp.gov.cn/spp/xwfbh/wsfbt/202103/t20210319_513155.shtml#2 .

¹⁵ “Chinese instruments referee Network,” visited date: March 24, 2021, 《Wen Shu》, <https://wenshu.court.gov.cn/> .

¹⁶ MLM means Multiple-Level Marketing.



1. Organizing and Leading MLM Activities Crime

In recent years direct marketing activities have been very popular in mainland China, so the suspects use virtual currency or block chain to attract downline members to virtual goods investment through illegal pyramid membership structure. They transfer the fund overseas until they get sufficient money.

2. Illegally Absorbing Public Deposits Crime

This crime is similar to the violation of Article 29 of the Banking Act, Article 29-1 provisions of absorbing public deposits. The criminal often use virtual currency or block chain investment to attract a large of victims. It is the typical Ponzi scam model to absorb funds, and when the time is right, the funds are transferred overseas, and the main suspects disappear into thin air.

3. Fraud

Most fraud cases in China involve foreign exchange, gold scam and other investment scams. In recent years, almost all the frauds are virtual currency and block chain investments, using communication software, internet or telephone. According to “2019 Research Report on Internet Fraud Trends”,¹⁷ types of phishing in China are: financial fraud, dating scams and part-time fraud. The number of financial fraud per capita loss is up to 134,522 RMB, much higher than investment fraud, loan or credit card fraud.

¹⁷ The Hunted platform, “2019 phishing and scam trends report” (January 9, 2020), visited date: March 24, 2021, 《*The Hunted*》, <https://zhuanlan.zhihu.com/p/102011078>.

4. Summary

The crimes related to virtual currency in China are mostly virtual currency and block chain investment, through fraudulent ponzi schemes, money-absorbing or fraud as the main criminal typology. Virtual currency is not the actual subject. The main criminal typology in China is a little different from Taiwan; However, the nature of fraud remains the same, which shows that cross-strait criminal groups use virtual currency as a propaganda to commit financial fraud achieve high probability of success.

V. Important Cases Across the Strait

1. Important cases in mainland China

(A) PLUS TOKEN platform absorbing funds case

1. Facts

In May 2018 , PLUS TOKEN launched “Asia’s first STO Exchange”,¹⁸ “Multifunctional cross-chain decentralized wallet”, “Moving bricks” (earning price difference from carrying out arbitrage transactions on different exchanges at the same time), “Currency loan”, “Global digital currency payment function”, “block chain game”, “ calculate the mine “.¹⁹ It attracted investors in major block chain websites and forums in China. May 2019, in just one year PLUS TOKEN has recruited more than 2.7 million registered members.

The PLUS TOKEN utilizes the MLM model to attract members on the

¹⁸ STO is the abbreviation of Security Token Offerings, which is the issuance of security tokens.

¹⁹ Peckshield , “15 Billion Chinese Funds PlusToken’s new bottles of old wine defrauded tens of billions, OTC became an important channel for deposits and withdrawals” (December 1, 2020), visited date: March 24, 2021, 《BLOCKTEMPO》, <https://www.blocktempo.com/chinese-police-seized-4-2-b-from-plustoken-scam/> .



internet. It generated returns for older investors by acquiring new investors, who were promised a large profit at little to no risk. Both fraudulent arrangements were premised on using new investors' funds to pay the earlier backers. Though PLUS TOKEN declared the members could withdraw the money at any time, but the handling fee is 4% higher if the withdrawal is within 28 days; therefore, most investors stay on the platform for over 28 days, forming a lock-up period of funds, and also allowed the criminals to transfer funds. During the 28- day period, investors continue to receive dividends, so they gradually increase their trust in the platform and were willing to invest more money.

Until June 27, 2019, PLUS TOKEN Web Purse began to close withdrawals, but the platform official did not explain the situation. During this time there were still many investors believe in the platform. However, meanwhile the perpetrators transferred money, and bought real estate, cars and other luxury goods for money laundering. Even senior coin miners originally earn 1.5 million RMB monthly, but lost everything²⁰ because of the fraud in the end.

2. Holding

The Intermediate People's Court of Yancheng City, Jiangsu Province, China, sentenced in December 2020 that PLUS TOKEN illegally used the network pyramid scheme for unauthorized fund-raising of RMB 15 billion. The seized digital currency was handled in accordance with the law, and the funds and income were confiscated.

²⁰ Block Beats, "The Largest Funding Plustoken Victims confessed painfully: From a monthly income of 1.5 million yuan to unwilling to believe" (August 3, 2020), visited date: March 24, 2021, *《BLOCKTEMPO》*, <https://www.blocktempo.com/plustoken-victim-confession/>.

(B) Chen's virtual currency laundering case

China submitted this case to FATF workshop as case studies in 2021, confirming virtual currency as new money laundering techniques. Its importance is that, in this case money laundering judgment had been confirmed before the predicate offences were convicted. It shows that money laundering offense is independent, and separate from the predicate offences.

1.Facts

From August 2015 to October 2018, Chen, the main suspect of this case, incorporated a financial information services company, without government approval, selling periodic fixed income financial products. The funds are mainly used for the company payment of principal, interest and private use. Later The company refused to compensate the victims. He launched digital currency trading platform, issuing virtual currency, to attract investors. He falsified transaction information and covered up funding crunch by limitation on large withdrawal or lying about hacking. In June, 2018, Chen transferred illegal payments 3 million RMB to a personal bank account. In August, 2018, Chen got divorce to conceal illegal proceeds, but still had his ex-wife transferred 3 million RMB to their personal bank accounts. In addition, Chen made his ex-wife sell the vehicles (illegal proceeds) at below market price for cash. Chen bought coins' private key from a Bitcoin miner, and used Bitcoins abroad.²¹

2.Holding

Shanghai Pudong New Area People's Court in 23, December 2019,

²¹ China Supreme People's Court, "The Supreme People's Court and Central Bank jointly issued typical cases of punishing money laundering crimes" (March 19, 2021), visited date: March 24, 2021, *《China Supreme People's online conference hall》*, https://www.spp.gov.cn/spp/xwfbh/wsfbt/202103/t20210319_513155.shtml#1.

found Chen guilty of money laundering and sentenced for two years and fined 20 million RMB. Chen did not appeal so the decision has taken effect. Although Chen's pyramid schemes was not yet part of the judgment, Chen's absconding abroad didn't affect the judgement, according to the new criminal law amendment of China. The significance of the case is that confirmation of predicate offences doesn't affect the judgement of money laundering.

2. Case Brief of Taiwan: Virtual Currency Fraud Website Case

(1) Facts

30 -year-old Yu, the main suspect of fraud syndicate, used knock-outs photos on dating APP to solicit victims for virtual currency investment "TINANCE", which assured profit from exchange rate. He declared that the virtual currency TTC increased every day to lure victims for investment. After Criminal Investigation Bureau arrested 12 people for questioning, there were at least 34 people have been cheated in just three months, with loss of more than 50 million NTD.²²

(2) Money laundering trick

Criminal Investigation Bureau not only seized 7 million cash, but also found a flash drive like "Cold wallet", containing Bitcoin for about 6 million NTD value. Now fraud syndicates adopt criminal proceeds in a slim and light "cold wallet"²³ with encryption. Such pattern changes the three stages of laundering. The money laundering practices and crime patterns in the second phase "layering", are gradually different.

²² Lin Yuping, "Tall handsome, white Formica virtual currency to attract investment 34 people cheated 50 million yuan" (November 6, 2020), visited date: March 25, 2021, *《China Times Network》*, <https://www.chinatimes.com/realtimenews/20201106004691-260402?chdtv>.

²³ Liu Wenyuan, "[flash drive value 6 million NTD] seemingly insignificant little things to prosecutors and police headache in big trouble" (February 14, 2021), visited date: March 25, 2021, *《Mirror Weekly》*, [HTTPS://www.mirrormedia.mg/story/20210208soc028/](https://www.mirrormedia.mg/story/20210208soc028/).

VI. Conclusion

In conclusion, currently the typologies of cross-strait virtual currency and money laundering are identical. Virtual currency and block chain are solicited as investment, through ponzi schemes to swindle money out of victim, and these are parts of financial fraud. It is worth noting that the crime syndicate turn the illegal proceeds from cash to virtual currency in cold wallets. Unless the law enforcement caught the suspects red-handed, and seized cold wallet immediately, it is difficult to match the true identity of the perpetrators. With no private key, even if there are large amount of money in the wallet, you cannot withdraw it to exchange into legal currency, or proceeds with subsequent seizure and confiscation procedures. Therefore, offenders using virtual currency as a means of money laundering, will be more difficult to trace the source of funds and cash flow. It also forms a breakpoint in the investigation, which will be a challenge for law enforcement.

The cases of cross-strait virtual currency and money laundering seem to have no connection. However, "Everything that rises must converge" quoted by Flannery O'Connor. Due to anonymity and rapid flow of virtual currency, and the fact that both sides share the same language, it's possible that there is cross-strait cooperation. With the outbreak of COVID-19 epidemic, many countries have taken "work from home" prevention measures, to reduce physical contact among people, leading to a surge of internet use that increases dark web use and phishing mails. On the other hand, the number of virtual currency criminal cases dropped 83%.²⁴

It's possible that without face-to-face interaction, success rate of virtual

²⁴ Chainalysis, "The 2021 Crypto Crime Report" (February 16, 2021), download date: March 25, 2021, 《Chainalysis》, <https://go.chainalysis.com/2021-Crypto-Crime-Report.html>.

currency frauds declines, but It does not mean the law enforcement can have a gap year to take a rest. Criminal investigation is like climbing cliffs, and when we face the abyss of crime, the slightest mistake will likely bring disaster. Law enforcement agency should continue to improve investigative thinking mindset and keep studying emerging crimes to practice social fairness and justice.

