Economics, Law and Policy
ISSN 2576-2060 (Print) ISSN 2576-2052 (Online)
Vol. 4, No. 1, 2021
www.scholink.org/ojs/index.php/elp

Original Paper

Analysis on Criminal Governance of Bitcoin-related Corruption Cases

Zhang Zize[1]

[1] College for Criminal Law Science, Beijing Normal University, Beijing, 100875 China

Received: March 9, 2021 Accepted: May 17, 2021 Online Published: May 28, 2021

doi:10.22158/elp.v4n1p37 URL: http://dx.doi.org/10.22158/elp.v4n1p37

Abstract

Bitcoin is extremely easy to be used in corruption cases due to its pseudonym, easy circulation, easy cross-border and other characteristics. As a decentralized electronic account book, the circulation of regulatory funds is jointly confirmed by each node in the bitcoin network, which can ensure the authenticity of the criminal evidence and is not easy to be lost or damaged. It provides great convenience for evidence collection in bitcoin corruption cases. However, there are also shackles in criminal governance, such as how to prove the subjective intent of the bribe takers, the impact of fluctuations in market value on the identification of the case and, most importantly, how to effectively recover stolen goods across borders. Therefore, the difficulty of bitcoin-related cases does not lie in the "anonymity" that some scholars believe, but lies in the determination of subjective intent, the determination of the amount of the crime and the international judicial assistance in recovering the stolen money.

Keywords

Bitcoin, cross-border digital forensics, international judicial assistance

1. Bitcoin Can Be Used as the Object of Corruption Cases

Although Bitcoin was officially issued by Satoshi Nakamoto in 2009, its entry into the eyes of most Chinese was a few years later. Taking the results obtained by Baidu search engine as an example, and taking cctv.com as a domain name to search for "Bitcoin", the earliest relevant web page appeared in 2013. In recent years, the wide application of block chain technology, which is the core of Bitcoin, and the continuous fluctuation of the market value of Bitcoin, make the name of Bitcoin a household name. The Financial Action Task Force on Money Laundering defines Virtual currency as "a digital representation of value that can be digitally traded and functions as,

(1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction". Bitcoin has the characteristics of decentralization (Bitcoin is the first distributed virtual currency. The entire network consists of users, with no central bank. Decentralization is the guarantee of bitcoin's security and freedom), worldwide circulation (Bitcoin can be managed on any computer connected to the Internet. No matter where they are, anyone can mine, buy, sell or collect bitcoin), exclusive ownership (The manipulation of Bitcoin requires a private key, which can be kept in isolation on any storage medium. No one can access it except the user himself), low transaction costs (Bitcoin can be exported free of charge, but eventually a transaction fee of about 1 bit cents will be charged for each transaction to ensure faster execution), no hidden costs (As a means of payment from A to B, Bitcoin has no onerous limits and formalities. Payment can be made by knowing the other party's bitcoin address), cross-platform mining (Users can explore the computing power of different hardware on many platforms), etc. Therefore, it now has a variety of bitcoin trading platforms and mining platforms. The number of criminal cases searched out by using "bitcoin" as the keyword on the "China Judgements Online" has been increasing year by year (Through the search condition of "Full Text: Bitcoin, Cause of Action: Criminal Case", the number of cases as of December 31, 2020 was found to be 2020(425)2019(323), 2018(177), 2017(72), 2016(44), 2015(16) and 2014(5), respectively, thus increasing year by year). However, there are few judging documents concerning corruption cases, which may have various reasons, such as criminal implicit case, the standard's varing from place to place whether the court's judging documents for corruption cases are open to the public, and so on. However, from a purely theoretical point of view, the possibility that bitcoin is used in corruption cases exists.

Taking bribery cases as an example, the following types of bitcoin-related corruption cases can be drawn by distinguishing the briber and the briber using legal currency or bitcoin (all assume that A is the intended briber and B is the national staff):

(1) The briber's legal tender and the briber's bitcoin: In this case, the transformation between legal tender and bitcoin must be involved. For example: A bought some bitcoins for B's account on a bitcoin website;

(2) The briber bitcoin, the briber bitcoin: A transfers some bitcoins directly or indirectly to B's bitcoin account on the Internet; A borrowed money from B to buy Bitcoin. When borrowing money, 1 Bitcoin could be exchanged for 2,000 yuan. After A had borrowed money from B, the market value of Bitcoin soared and it was returned to B's account in the form of Bitcoin;

(3) The briber's legal tender, the briber's legal tender & the briber's bitcoin, the briber's legal tender: in both cases, the forms of crime will become interesting and diverse. For example, B recommended Bitcoin from a website to A at the wine bureau, so A paid B hundreds of thousands of dollars to help B fry the coins; A sold B the bitcoin products on its website, and B spent 50,000 yuan to buy 50 bitcoins. A few months later, the market value of these bitcoins was enough to quadruple the money B had

invested hundreds of times.

There are countless corruption cases involving bitcoin. Here are three considerations:

First, it is used to prove that Bitcoin can be used in corruption cases. Bitcoin is not completely banned or classified as contraband in China. The People's Bank of China, the Ministry of Industry and Information Technology, the China Banking Regulatory Commission, the China Securities Regulatory Commission and the China Insurance Regulatory Commission have issued the "Notice on Preventing Bitcoin Risks" and the People's Bank of China, the Central Internet Information Office and the Ministry of Industry and Information Technology have issued the "Notice on Preventing the Financing Risks of Token Issuance" on September 4, 2017, all of which do not prohibit the issuance of Bitcoin. Entering "Bitcoin" into commonly used search engines can even search out Bitcoin websites in China, which can be identified as property in corruption cases;

Second, in bitcoin-related cases, it is difficult to determine the value of bitcoin. We know that there is a corresponding amount standard for the conviction of corruption and bribery cases, such as the Interpretation on Several Issues Concerning the Applicable Law in Handling Criminal Cases of Corruption and Bribery issued by the Supreme People's Court and the Supreme People's Procuratorate, etc. The market value of Bitcoin fluctuates very fast. And corruption involving bitcoin and corruption involving equity trading are similar to some extent, but their supervision is far from the same. The fluctuation of shares is controlled by a certain extent and is subject to central supervision. However, the state does not have relevant laws and regulations to directly regulate the price fluctuation of Bitcoin, which is a decentralized trading method. And if it wants to force intervention, according to the mechanism of Bitcoin, there are only two ways to supervise the market of Bitcoin: one way is to directly change the account book by controlling the computing power in the Bitcoin network to more than half, and the second way is to directly deny access to the website of the Bitcoin platform from the firewall or ISP. However, no matter what measures are taken, it is undoubtedly rough and unfair to other netizens who have obtained Bitcoin in good faith and legally. How to calculate the market value of bitcoin and how to incriminate it in corruption cases and how to prove the intent of the bribe takers are still in judicial practice.

Third, Bitcoin, as a seemingly "emerging" item, will undoubtedly be favored by criminals because of its "anonymity". In the search for articles about bitcoin and corruption on "https://www.pkulaw.com/" and "https://www.cnki.net/", some authors, even the authors of articles published in domestic core journals and doctoral dissertations, believe that the "advantage" of bitcoin in corruption cases lies in its anonymity. The author believes that for a corrupt official who has fully read Bitcoin founder Satoshi Nakamoto's White Paper on Bitcoin and understood its meaning, anonymity is definitely not the reason for accepting bribes by using Bitcoin. The reason for choosing Bitcoin should lie in the volatility of the market value of Bitcoin, in order to resist the convenience such as the identification of the amount involved in the investigation and trial as well as the proof of subjective intent, and the convenience of converting into French currency for cash withdrawal in some foreign countries. As for the anonymity

mentioned by these scholars, the author believes that from a theoretical point of view, Bitcoin is just a sharp weapon against the anonymity of transactions and corruption.

2. Bitcoin Helps to Extract Evidence from Corruption Cases

(1) Bitcoin is "pseudonym" rather than "anonymous"

The main argument that Bitcoin is anonymous focuses on "what exists in the transaction record is a string of numbers". Some scholars even think that this string of numbers can be changed at will. "Public and private keys can be generated randomly, and both parties to the transaction can regenerate a pair of keys during each transaction. The real identity can be hidden one at a time in a secret way, making the transaction difficult to track, control and lock". These obviously did not fully understand the mechanism of bitcoin, but only completed the formal syllogism inference and reached the wrong conclusion.

Satoshi Nakamoto defines "an electronic currency as a string of digital signatures in which each owner sends the electronic currency to the next owner by signing a random hash of the previous transaction and the next owner's public key and appending the signature to the end of the electronic currency. And the payee is able to verify the owner of the chain by verifying the signature". "As an additional precaution, users can have each transaction generate a new address to ensure that these transactions are not traced back to a common owner. However, due to the existence of parallel inputs, some degree of traceability is still inevitable, as parallel inputs indicate that these currencies all belong to the same owner. The risk here is that if one of a person's public keys is confirmed to belong to him, many other transactions of that person can be traced back".

From the perspective of cryptography, the public key can be regarded as the receiving address to a certain extent, and the private key and the public key correspond one by one in the sense of calculation. If the private key is replaced, the public key must be inconsistent with the receiving account. Therefore, replacing the private key is equivalent to replacing the account, and a transaction channel must be established between the original account and the new account in order to achieve its criminal intent such as money laundering. The so-called "one secret at a time" is practically impossible.

Judging from Satoshi Nakamoto's statement, the "new address" he mentioned applies to money laundering activities, referring to the establishment of multiple collection accounts for "parallel input", then these parallel inputs are reasonable for the regulatory system to believe that the collection accounts in this transaction belong to one owner. At this time, the economic common sense of "putting eggs in different baskets to reduce risks" is not applicable. As long as a public key address of a payer and a payee is confirmed as a bribe-giver or a bribe-taker, most of the series of bribery they conduct through Bitcoin will surface.

Bitcoin's privacy policy is shown in the figure. Hide the identity information and make the transaction public. Just like the recent reform of the COVID-19 case flow report in Beijing, Shanghai and other places, only the track is mentioned and no one is mentioned. However, it can be expected that the

communities where the cases live, the work units where the cases work, and how the children of the cases pick up and drop off can all correspond to the cases through these tracks. For Bitcoin, the final flow of Bitcoin to the account, the receiving address of online purchases and the ip address of purchases can all accurately locate or depict the owner. Therefore, from the perspective of investigation, the so-called "anonymity" does not exist, but is based on the erroneous conclusion drawn through excessive "diversion". The public key in bitcoin should be regarded as a kind of "pseudonym" for the owner's identity information rather than "anonymity" or "one secret at a time" as many scholars believe.

(2) The transaction records of bitcoin are stored in a decentralized way

Satoshi Nakamoto proposed a "time stamp server". The timestamp server adds a timestamp by randomly hashing a set of data in the form of a block and broadcasts the random hash. Obviously, a timestamp can prove that specific data must indeed exist at a specific time, because the corresponding random hash value can only be obtained if it exists at that time. Each timestamp should incorporate the previous timestamp into its random hash value, and each subsequent timestamp will follow the previous timestamp, forming a chain. This is the block chain technology that is now widely used to prove that the transaction does exist.

The Bitcoin transaction node always considers the longest chain as the correct chain and continues to work and expand. If two nodes simultaneously broadcast different versions of a new block, the other nodes will receive the block at different times. In this case, they will work on the basis of the first received block, but will also keep the other chain in case the latter becomes the longest chain. The deadlock will be broken until the next proof of work is found, and one of the chains is proved to be longer, then the nodes working on the other branch will switch camps and start working on the longer chain. The so-called "new transaction to broadcast" does not actually need to reach all nodes. As long as the transaction information reaches enough nodes, they are quickly integrated into one block. If a node does not receive a specific block, the node will find that it is missing a block and it can request to download the block itself.

In short, the authenticity of transactions on the Bitcoin network can be confirmed through several blocks, and the traders themselves can also confirm. However, there are both connections and differences with the so-called "de-centralization" of platforms such as Weibo: for users in Weibo, certain information can indeed be searched through a built-in search module, but this information cannot be guaranteed to be true. Generally, only when the account number is more than the information released by the government media has certain credibility. And sometimes it will delete itself for some reasons. In the bitcoin network, the transaction records brought out by a public key address searched by

the built-in search module can be proved to be reliable by algorithms, and will never be deleted once it exists. As criminal evidence in corruption cases, it has natural advantages and availability.

(3) The cost of altering the transaction records of bitcoin is too high

Satoshi Nakamoto has made bitcoin's algorithm open source in its white paper, so many fraud cases under the guise of fake bitcoin have been born in recent years. Apart from the subjective malignity of these fraudsters, these fake bitcoins are also extremely vulnerable to attacks due to their cost and tamper with electronic account books, thus causing economic losses. Judging from the aforementioned Bitcoin transaction recording mechanism, as long as the network with 51% of the computing power of the whole network is controlled by any individual or organization, it can tamper with its transaction records, manipulate transactions and currency value at will. Up to now, bitcoin has a net-wide computing power of 149.81 EH/s, and a mining machine with a computing power of 95TH/s costs at least 20,000 yuan. The cost of tampering is definitely an astronomical figure. For a rational "criminal economic man", it is not advisable to carry out such a large-scale operation in order to cover up the gains, either financially or in the wake of such an accident.

Based on the above three points, bitcoin can do:

First, according to the matching mechanism of public key and private key, the public key can be depicted by the orientation of bitcoin in the transaction record and finally located to the specific identity information in the criminal lawsuit process of corruption cases; Second, Guarantee the authenticity and legality of transaction records. Due to the distributed storage mechanism, the risk of illegal evidence collection can also be greatly reduced during the evidence collection process. However, it should be noted that in the judicial context of evidence adjudication, another piece of evidence that is generally considered to be the "king of lawsuits" today is relevance. To a certain extent, the transaction mechanism of bitcoin can accurately identify the bribery subject and the time of bribery, and can prove the relevance to bribery. However, for the bribery subject, the relevance to bribery cases still needs to be explored in the judicial practice, as the receipt of bitcoin does not need to be confirmed by the payee.

3. Limitations and Countermeasures of Bitcoin's Application in Recovering Bribes

In general, there are at least the following difficulties in bitcoin corruption cases:

(1) The identification of the entity

As mentioned above, how to define a state functionary's intention of accepting bribes is a big difficulty. For example, when being investigated, he could not define whether he knew the increase of bitcoin in his account, whether he needed to report his bitcoin account, whether he needed to check his bitcoin account regularly, and declare truthfully, etc., and infer from the side whether he had intention to accept bribes. At present, some countries have explored the practice of reporting public officials' bitcoin accounts.

In the case of taking bribes in the form of "speculation of money", due to the volatility of the market value of bitcoin and the absence of relevant laws and regulations to limit its volatility in the international community, the determination of the amount of bribes in the whole criminal process still needs theoretical and practical consideration if it is mechanically valued based on the market price of bitcoin at the time of the crime.

(2) Improvement of the recovery mechanism

As for the circulation channels of bitcoin and French currency within a country, some countries have already established regulatory measures for encrypted currencies such as bitcoin. For example, the Australian Anti-Money Laundering and Anti-Terrorism Finance Act requires encrypted money transactions to be registered, identified and authenticated, suspicious transactions reported and recorded. Malaysia's Anti-Money Laundering and Anti-Terrorism Finance Act requires encrypted money transactions to identify and verify customers and beneficiaries, monitor customer transactions, report suspicious transactions and keep records, and also to publish the price of encrypted money and the method of determining the price to improve transparency. Exchanges are also required to report details to banks as reporting agencies. The Estonian Anti-Money Laundering Law requires a license for the encrypted money exchange service provider and the encrypted money wallet service provider. Belarus Anti-Money Laundering Law stipulates that operators of encrypted money platforms and exchange service providers are required to fulfill anti-money laundering obligations. The regulatory measures of various countries mainly focus on the connection between Bitcoin and reality, such as the encrypted currency exchange, the encrypted currency exchange service provider and the encrypted currency wallet service provider, which are all intermediaries of encrypted currency activities. However, Article 3 of China's Anti-Money Laundering Law stipulates: "Financial institutions established within the territory of the People's Republic of China and specific non-financial institutions that are required to fulfill their anti-money laundering obligations shall, in accordance with the law, take preventive and monitoring measures, establish and improve a customer identification system, a system for keeping customer identification information and transaction records, and a system for reporting large-value transactions and suspicious transactions to fulfill their anti-money laundering obligations". Article 35 stipulates: "The scope of specific non-financial institutions that should fulfill their anti-money laundering obligations, the specific measures for their performance of anti-money laundering obligations and their supervision and management shall be formulated by the anti-money laundering administrative department of the State Council in conjunction with the relevant departments of the State Council". However, the "specific non-financial institutions" approved by the central people's bank do not include internet websites that provide services such as bitcoin registration and trading. In other words, China still lacks effective legal supervision over the circulation between bitcoin and legal tender. Therefore, it is necessary to carry out supervision and early warning measures in our country, at least for the institutions that exchange bitcoin for legal tender.

In addition, the difficulty of China's anti-corruption work lies in foreign enforcement. For example, some scholars pointed out that one of the key issues in cross-border recovery of stolen goods in China is the recognition of confiscation decisions. China generally implements "confiscation of all personal property". However, some countries have different provisions on individual property rights. The laws of these countries have their own conditions, procedures and evidentiary standards for freezing, seizing and confiscating the assets of natural or legal persons. The existing international treaties all emphasize that relevant international cooperation should be carried out "to the extent permitted by the law" in the countries where the assets flow. Can bitcoin be the object of the recovery? Legally, the United Nations Convention against Corruption states that "proceeds of crime" refers to any property that is directly or indirectly generated or acquired through the commission of a crime; "Property" refers to all kinds of assets, whether material or immaterial, movable or immovable, tangible or intangible, and legal documents or instruments evidencing property rights or interests in such assets. However, there are still many disputes about whether Bitcoin can be collected from the bitcoin-related crimes uncovered in foreign countries, such as how to auction the bitcoin involved, and whether it is legal to freeze the relevant accounts of the accounts involved. When bitcoin is involved in the recovery of stolen goods from abroad, it will inevitably involve the game and competition between cyberspace sovereignty and judicial sovereignty.

(3) Cross-border digital forensics and international judicial assistance

The confirmation of the subject information of bitcoin inevitably involves the relevant subject converting bitcoin into French currency or using bitcoin to purchase physical objects. At present, due to the fact that most domestic bitcoin websites need real-name information such as identity card numbers and the strict supervision of domestic financial institutions, the criminal pattern of domestic corruption cases mostly involves the conversion of hard currency such as U.S. dollars abroad or the use of bitcoin by their children to purchase goods. The main way is to obtain evidence from relevant shopping websites and bitcoin exchange websites. At this time, cross-border evidence collection is involved, among which cross-border digital evidence collection is the most important.

In the 1990s, the main use of the Internet was for military exchanges in the United States. After that, due to the increase in demand for commercial networking, the Internet began to advocate "Internet sovereignty", believing that the Internet is a product of science and technology and should be independent of government control, and that the Internet space is an independent space different from the physical space, with the characteristics of decentralization. However, the control of the underlying technology architecture of the Internet is very centralized. The world's top-level domain name resolution server is regulated by the U.S. government, which has been refusing to transfer ICANN's management rights under the pretext of "security concerns". The center's unilateralist control of the internet. Countries have also begun to notice the harmfulness of Internet unilateralism. The European Union has also changed its previous position and promoted the supervision model of the United Nations network domain servers in order to speed up the internationalization of ICANN and IANA and

involve the government. The US Department of Commerce is under global pressure to unilaterally regulate ICANN and hand it over to the UN. In the same year, the UN Expert Group on Information Security reached an important document, confirming that the "UN Charter" and other norms and principles of international law are applicable to national activities in cyberspace. Each country's understanding of sovereignty gradually extends from territorial sovereignty to cyberspace, forming the current "warring States" pattern of internet space governance, i.e., two camps in the world: on the one hand is the principle of NATO countries' leading and preemption, i.e., in non-territorial space, the actors are first-in, thinking and matching first according to their own advantages and disadvantages, the interests of the weak do not need to be considered, and the formulation of international cyberspace rules should meet the best interests of the vested interests; On the other hand, developing countries tend to adhere to the principle of "common property of mankind" and emphasize that all countries should enjoy equal network sovereignty regardless of their advantages or disadvantages. Even if they do not currently have the corresponding equipment and technology research and development capabilities, they should have the right to reserve by making relevant rules.

In the field of evidence, these problems are represented as a game of international jurisdiction over data mastery, mainly from two perspectives: the "data storage location model" and the "principle of sovereignty over cyberspace". Since the criminal jurisdiction of a country has always been based on the regions within its sovereignty, the actual storage location of electronic data has become the basic consideration for the actual exercise of jurisdiction—the data storage location model. From the traditional and widely accepted point of view, the acquisition of electronic data stored in foreign countries can only be achieved through mutual legal assistance in criminal matters on the basis of mutual respect for national sovereignty. However, both the above-mentioned mutual legal assistance in criminal cases and the unilateral use of computer technology for cross-border electronic evidence collection have obvious defects. In order to fully tap and control the data resources of service providers operating across borders in the criminal justice and network supervision systems, there has been an increasingly significant trend of "data localization" in the world in recent years. Under the condition that the local storage of data is mandated by law, the retrieval and application of data in criminal justice need not be carried out in a cross-border way, so that data sovereignty can be effectively implemented in criminal justice. The United States claims no sovereignty over cyberspace. Since the mid-1990s, American academic circles have launched an in-depth discussion on whether cyberspace has sovereignty or not, and the official view based on safeguarding American interests has gradually become clear. On the other hand, the United States is facing an "unbalanced" dilemma in the area of criminal judicial assistance in cross-border electronic evidence collection. If we follow the traditional data storage model, the U.S. law enforcement agencies cannot smoothly access the vast amounts of data held by these enterprises.

Cross-border data collection of bitcoin-related corruption cases needs to be effectively explored in combination with the Budapest Convention on Cybercrime, the GDPR, the U.S. Cloud Act and the second supplementary protocol to the Budapest Convention of the European Union. Only in this way can China effectively and timely detect bitcoin-related corruption cases and recover national assets. In addition, bitcoin, as a global circulation product, countries cannot interfere in its mechanism. However, it can be effectively monitored according to the flow characteristics of bitcoin, such as tracking suspicious bitcoin conversion into legal currency, and using artificial intelligence to predict and analyze the money laundering behavior of some accounts in a short period of time for effective early warning, etc.

4. Conclusion and Prospect

Bitcoin-related crimes are not untraceable due to their anonymity, as some scholars think. There are also many successful cases of tracking criminal behavior abroad. On the contrary, due to the decentralized block chain technology of Bitcoin, evidence collection is more convenient than traditional corruption cases, reducing the risk of illegal evidence collection and lowering the technical threshold of evidence collection subjects. Even some “network chivalrous men” full of romantic feelings can use social engineering and other methods to find out criminals hidden under the network. Individuals can obtain evidence by themselves so that criminals can accept legal sanctions, and the authenticity of the evidence can be fully guaranteed. The space that needs to be improved may lie in whether the evidence obtained by individual “chivalrous men” can be used as the basis for deciding a case, how to confirm the effectiveness of the evidence in the cross-examination link of the court, and how to balance the privacy of the prover with the purpose of criminal proceedings. However, in specific practice, the entity aspect will involve the problem of subjective intent identification of the bribe taker and the problem of the amount involved in the case. In the aspect of recovering the stolen goods, a new path needs to be explored. How to accurately locate the bitcoin account involved in the case and auction it to recover the stolen money requires the exploration of relevant practice and the formulation of laws and regulations. Strengthening supervision in the conversion link between bitcoin and the legal currency in reality and using artificial intelligence technology for anti-money laundering early warning can also effectively prevent corruption cases involving bitcoin. Finally, due to the global circulation of Bitcoin, cross-border digital forensics is bound to be involved in specific cases. At this time, countries need to work together to improve the relevant international judicial assistance mechanism.

References

Bitcoin's Network computing power. (2021). Retrieved January 19, 2021, from https://btc.com

How the FBI Disposes of the Huge Bitcoin Seized from the Silk Road. (2021). Retrieved January 18, 2021, from https://www.bitcoin86.com/news/1204.html

Huang, Z. (2015) China's current legal obstacles and solutions to pursue and flee overseas. *China's Party and Government Forum*, *2015*(2).

Lei, Y. (2019). *China Bitcoin Channel Capital Flight Research*. Central University of Finance and Economics in 2019 doctoral thesis.

Price of mining machines. (2021). Retrieved January 19, 2021, from https://shop.bitmain.com.cn

Satoshi, N. (n.d.). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Shi, Y. A., & Wang, Y. J. (2019). Criminal Governance of Bitcoin Money Laundering Crime. *Journal of the State Prosecutors College*, *2019*(2).

South Korea's New Initiative: The Government Promulgates a Bill to Require Public Officials to Declare Encrypted Monetary Investments. (2021). Retrieved January 19, 2021, from http://www.shilian.com/m/view.php?Aid=130637

The Financial Action Task Force (FATF), Virtual Curencies: Key Definitions and Potential AML/CFT Risks. (n.d.). Retrieved from http://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-AML-cft-risks.pdf

The Founder of the Silk Road Demands the FBI to Return the Bitcoin Seized. (2021). Retrieved January 18, 2021, from http://www.btc001.net/btc/1715.html

The website of the National Supervision Committee of the Central Commission for Discipline Inspection, the full text of the UN Convention against Corruption. (2021). Retrieved January 18, 2021, from http://www.ccdi.gov.cn/special/lygz/flfg/201310/t20131008_11282.html

Xinhua. (2021). *"Only the track is mentioned but no one is mentioned", the new report on the current situation is worth advocating*. Retrieved January 25, 2021, from http://www.xinhuanet.com/2021-01/24/c_1127019082.htm

Zeng, L. (2020). Characteristics, Difficulties and Prospects of Cross-border Recovery of Encrypted digital currency as a Corrupt Asset. *Journal of International Economic Law*, *2020*(1).