Cryptocurrency fraud schemes analysis

Irina Astrakhantseva[1,*], *Roman* Astrakhantsev[2], and *Alexey* Los[2]

[1]Ivanovo State University of Chemistry and Technology, Sheremetevskiy avenue, 7, 153000, Ivanovo, Russia
[2]National Research University Higher School of Economics, Myasnitskaya str., 20, 101000, Moscow, Russia

Abstract. The article focuses on the relevance of establishing legal norms for virtual currency, which is currently working in the gray zone. The article substantiates why cryptocurrency was referred to other property in the framework of civil law. The author suggests a definition of cryptocurrency to introduce it into legislation. Attributes of cryptocurrency theft are considered. The most attention is given to fraud, in particular different types of cryptocurrency phishing, and possible ways of criminal prosecution for cryptocurrency theft.

1 Introduction

In the past decade, the innovative technology of distributed ledgers (blockchain) has become an integral element of our lives. However, the use of blockchain, smart contracts, and cryptocurrencies is still uncertain both economically and legally. Legal vacuum as to governing cryptocurrency as property under civil law is a strong hindrance to implementation of this technology [1].

In our view, it is principally these new and distinctive features of cryptocurrency as an asset – its intangibility, cryptographic authentication, decentralization, consensus-based management, and use of distributed ledgers – which have given rise to disputes on legal and property status of cryptocurrencies.

Money laundering, unlawful practices, theft, fraud, and crimes: the world of alternative digital currencies is attractive because of its lack of controls, in particular as far as anti-money laundering and combating the financing of terrorism are concerned. Virtual currency provides anonymity and does not require the personal identification that facilitates cybercrimes. To open an account in virtual currency, a user must provide the minimum information, and all a user needs to gain access to a profile is a desktop computer, tablet computer, or a smartphone. Simplicity in use and portability create a perfect environment for cyber-crimes.

Cryptocurrency transactions have no boundaries and may be instantly made all over the world. There is no certain jurisdiction to enforce law and apply restorative justice. Virtual currency functions outside the boundaries of the law in a grey zone since there is no intermediate to exercise control over it. Therefore, it is especially important now to set regulations that would facilitate development of this technology and restrain its illegal use (in fraud and other crimes).

* Corresponding author: i.astrakhantseva@mail.ru

2 Cryptocurrency wallets and cryptocurrency exchanges

To understand possible ways of stealing cryptocurrency, we will need the concept of a "cryptocurrency wallet" – a way of storing a digital currency in the form of a cryptographic hash which contains a value. The concept of a crypto wallet is not similar to a customary wallet that contains several currencies which may be stored or deleted. Cryptocurrency payments require that all wallet value (cryptographic hashing of all the amount) be paid; then, a difference between the payment amount and the total value of that wallet will be returned. At this point, we get a new hash address.

There are cryptocurrency exchanges which enable fiat money to be acquired in exchange for cryptocurrency. Using these platforms, cryptocurrency can be exchanged in a similar way to foreign currency assets. In 2020, there are over 300 such exchanges [2]. They represent an electronic platform that enables exchanging fiat money for a cryptocurrency and vice versa as well as exchanging some cryptocurrency for another cryptocurrency. Therefore, exchanges are involved in transferring funds from a bank account to a cryptocurrency wallet account. This is the first stage to regulate such transactions. Thus, cryptocurrency exchanges that are registered in the U.S.A. must report on anti-money laundering and combating the financing of terrorism.

3 Cryptocurrency in the system of rights under civil law

Russian science as well as judicial practice demonstrate various approaches to legal nature of a cryptocurrency. For example, K. Nikitin [3] refer to approach applied by common pleas courts and arbitration courts in 2015–2017 that cryptocurrencies are not defied in Russian regulations as an item of property protected by rights under civil law that makes it impossible to apply them officially. We cannot agree with this approach because cryptocurrency turnover in Russia is not prohibited and actually exists as confirmed by judicial practice.

Since a cryptocurrency may function as a method of payment, it may be, due to its economic nature, referred to a type of monetary assets or money. Money may be in the form of a banknote, coin, or an entry in accounts. Also, some functions of money may be fulfilled by near money, such as securities or liquid assets, and now also by a digital code (cryptocurrency). In research works (V. K. Shaydullina), we may find the opinion that a cryptocurrency is a payment instrument and a universal financial instrument [4]. Again, we cannot absolutely agree with this opinion. Presently, many actors in the market recognize cryptocurrencies and for that reason they acquire similarity to money. Money is issued by national central banks. However, the government is not engaged in any manner in cryptocurrency mining. Therefore, a cryptocurrency does not constitute money since it is not issued by the government, its value is not guaranteed, and no one is obliged to accept it as a payment instrument.

Also, it seems doubtful that a cryptocurrency may be referred to a foreign currency since it is not an official payment instrument of a foreign country. Therefore, it may not be referred to a category of foreign currency assets. However, A. I. Savelyev [5] presumes that cryptocurrencies may become foreign currency assets in future. We feel this is undoubtedly the case: the present state of affairs could continue until any of the United Nations member states recognizes a cryptocurrency as an official payment instrument in its territory.

Cryptocurrencies and electronic money have one thing in common: no single individual is responsible for providing cash in exchange for them. When using electronic money, a recipient has the right to request payment of certain nominal value in the form of electronic money and/or cash, and such payment procedure includes a verifying intermediary unlike with cryptocurrencies (peer-to-peer network). The principle of cryptocurrency decentralization does not include any operator to accept and execute instructions. The

platform protocol fulfills this function itself. So, we may conclude that a cryptocurrency may not be referred to electronic money. However, there is judicial practice referring cryptocurrency to electronic money and conditional electronic currencies used by certain websites.

There are opinions in works (V. Kisly) referring a cryptocurrency to uncertified securities [6]. When a cryptocurrency is transferred from one person to another, no obligations or rights to claim occur. Also, there is no securities issue resolution in case of a cryptocurrency. There is such concept as mining that may be analogously compared with securities issue as creation of new structures to ensure cryptocurrency platforms operation. However, a securities issue is centralized while cryptocurrency mining is decentralized. A cryptocurrency may be destroyed by sending it to any non-existing address. Uncertified securities may not be destroyed because their quantity is strictly controlled by a register holder. Therefore, we are of the opinion that a cryptocurrency in its nature may not be referred to securities.

Recently, the most popular approach in the scientific community classifies a cryptocurrency as “other property” (A. V. Savelyev [5]). We share this opinion that a cryptocurrency may be classified as “other property”. This term means items of property protected by rights under civil law that are not expressly mentioned in article 128 of the Russian Federation Civil Code while they are involved in civil transactions.

4 Cryptocurrency as property. Definition of ownership

Today we have the situation that cryptocurrencies may be freely transferred even if they are banned or restricted.

To make a cryptocurrency legitimate, we suggest including this term in article 128 of the Russian Federation Civil Code. Definition of a cryptocurrency in regulations must be technically neutral to the highest possible extent and be based on its essential and functional characteristics.

We suggest the following definition of cryptocurrency to be used by the legislative authorities. Cryptocurrency means cryptographically protected property existing only in the form of information in an information system that is based upon the distributed ledger technology and that may be stored, transferred, and traded electronically.

Introduction of such concept as a cryptocurrency enables including it in the existing system of rights under civil law, namely, in the current category of property. The above definition highlights only a digital aspect of a cryptocurrency existence and use, it suggests that this asset may be included in transactions; also, it differentiates between the notions of a cryptocurrency, non-cash money, and electronic money.

Strictly speaking, the term "property" describes not a thing itself but legal relationship related to this thing, namely, the rights that may be exercised according to legal regulations. And one of fundamental issues to be solved here is recognition of ownership to this specific type of property. Definition of ownership to cryptocurrency may become of great importance in future for regulating succession in such cases as inheritance, bankruptcy, fraud, theft, abuse of trust, extortion, and kickback.

Since Roman law, division of rights to rights in rem and rights in personam has been the ground for classifying rights to property. We believe that a cryptocurrency may be referred to rights in rem though it is not a tangible thing (immaterial thing). We can already note that a cryptocurrency shows signs of ownership. We suppose that a starting point for determining the ownership to cryptocurrency must be the fact that a right holder will be the owner of this asset provided that he or she lawfully obtained access to a private key, analogously to a title holder who lawfully obtains possession of a tangible asset.

5 Definition and attributes of cryptocurrency theft

An item subject to theft means property of another person that is not in ownership or legal possession of an offender. Property may be taken as a result of theft, fraud, extortion, misappropriation and misapplication, theft by taking property openly, and robbery. It is generally believed that the taking of property is recognized as such subject to the aggregate of tangible, economic, and legal attributes [8].

The economic attribute implies that a cryptocurrency has certain value. This attribute is inherent in a cryptocurrency since there are cryptocurrency exchanges that allow buying and selling digital currencies online.

The legal attribute is also inherent in a cryptocurrency. According to judicial practice and the above analysis, ownership to cryptocurrency wallets is established if an actor lawfully obtained access to a private key and it is possible to identify an account of a user and a certain person.

The tangible attribute means that property must have general material characteristics. A cryptocurrency exists only as information in electronic form. However, recent works in criminal law contain discussions that things which are not tangible in their nature but are protected by rights under civil law may be subject to unlawful encroachment. Therefore, the tangible attribute may not play a key role in defining an item subject to theft. Besides, non-cash money and electronic money are an item subject to theft according to judicial practice notwithstanding they have no tangible attribute.

So, cryptocurrencies have a required and sufficient set of attributes to identify ways how those assets may be taken.

6 Fraud in cryptocurrency theft

Cryptocurrency exchanges enabling conversion into fiat money may be potentially involved in such fraudulent schemes as personal data theft, mass-marketing fraud, imitating, phishing, malware, and extortion.

To use these schemes and avoid being detected, frauds create accounts using data of a "stolen" identity obtained by hacking email, server, and other devices containing personal data. Besides, cryptocurrency represents a new industry applying a new technology which neither users nor law enforcement agencies entirely understand. Frauds often use mass marketing promising significant financial profit.

Phishing is a kind of social engineering to obtain a user's account data. In case of cryptocurrency, frauds would try to obtain a user's name, password, or private keys. The most common of them are Punycode and Fake Airdrops. With Punycode, a user is sent an email that redirects him or her to a fraudulent website that looks completely the same as an official source but with another web address. For example, Blockchain.com vs Blockchàin.com. A fraud website offers a user entering login data that he or she uses to access the official website. Fake Airdrops is another way of phishing where users are fraudulently made to send their personal data, including email address, cryptocurrency wallet address and actual data on a crypto wallet value by imitation of official disbursement of coins by email or in social media.

Phishing attacks became a common thing and they are difficult to detect. There is no certain transaction that could establish whether a user became a victim of phishing attack or not. Phishing comes to light when a client informs cryptocurrency exchanges of that or a questionable activity occurs in the client's account that is expressed in a sudden activity of the client, access to the account from a new device (as determined by a finger print from a device), access from several IP addresses, or suspicious requests as to the client's account status. Although any of such transactions or actions do not constitute possible fraud alone, a

combination of them creates a fraud actions pattern. Detection of such pattern and subsequent prevention of such actions prevent cryptocurrency theft.

Using phishing is punishable under article 272 of the Russian Federation Criminal Code since criminals unlawfully access computer information protected by law (access to information that is not sanctioned by its owner or another legal user). A mandatory attribute of an external element of a crime includes such actions as destructing, blocking, modifying, or copying user credentials and content of a cryptocurrency wallet.

Taking into account that judicial practice has defined a cryptocurrency as another property since 2018 (and we share this approach), it is possible to determine its value through cryptocurrency exchange rate and, then, correlate it with the official exchange rate of the Ruble set by the Central Bank. Therefore, a cryptocurrency theft due to determining its value is punishable under articles 158 and 159.3 of the Russian Federation Criminal Code.

Extortion through betrayal of confidence is fraud bringing financial and non-pecuniary damage to its victims through winning confidence (complaining about being out of money or that a child fell ill and so on). Frauds ask to create an account in a cryptocurrency exchange; then, they ask to transfer money through cryptocurrency as a convenient way to make an anonymous and instant international funds transfer. It is rather difficult to reveal such schemes because a victim transfers funds voluntarily engages. To reduce such crimes, a cryptocurrency exchange has to place warning notices as it is in bank transfers when a significant number of new users as well as access to an account from multiple IP addresses do not correspond to a stated physical address of the client.

This type of extortion is punishable under article 159 of the Russian Federation Criminal Code (Extortion: Theft of Another Person's Property or Acquisition of Rights to Such Property Through Deception or Abuse of Trust).

Mass-marketing fraud is a type of phishing applying mass communication methods (email, messengers, mass mailing, and social media). This type of fraud suggests that criminals are to carry out certain actions physically. For example, creating a false account in social media on behalf of an official cryptocurrency exchanger or using a verified but hacked account with a plenty of followers offering mass disbursement of cryptocurrency (as a promotion) in exchange for users' credentials. Users are encouraged to send decimals places to provided addresses allegedly in exchange for amounts ten times more than such investments. Besides, users are encouraged to make reposts.

A determining factor in this type of fraud may be the monitoring of newly registered users to compare with regular activities. Mass marketing in social media is more successful than email phishing. That is why it is necessary to monitor social media and detect causes of users mass registration to prevent cryptocurrency theft and fraud. Such schemes are punishable under article 159 of the Russian Federation Criminal Code

Personal Data Theft. The mentioned method is applied to create new accounts. A criminal may unlawfully act disguised under the name of an unaware third party (victim). For example, frauds create accounts to check bank accounts and, then, withdraw funds from such compromised account. Criminals may use personal data associated with an account of a certain person while using bank account details of another person. Not all cryptocurrency exchanges have tools to verify accounts; they only check that a bank account is valid but do not check who is its holder.

Creation of accounts using stolen personal data may be used for stratification in money laundering process. A criminal accumulates cryptocurrency in a wallet; then, such cryptocurrency is exchanged for another cryptocurrency, and, after that, that criminal withdraws funds concealing illegal earnings. Potentially, a cryptocurrency exchange transaction may detect personal data theft. Discrepancies in information provided during registration and exchange may indicate that an account was created using stolen personally identified data.

Personal data theft is punishable under article 137 of the Criminal Code. A privacy breach is punishable under article 183 of the Russian Federation Criminal Code. Unlawful access and disclosure of information constituting trade, tax or banking secrecy are punishable under article 159.6 of the Criminal Code (Fraud in the Field of Computer Information).

Fraud with ICO. ICO is applied to initially raise capital by offering users acquisition of digital coins in exchange for fiat money. In case of ICO in the U.S.A., a company that raises funds for creating digital coins must comply with certain rules when registering and issuing prospectus in the Securities and Exchange Commission (SEC). The ICO boom is comparable to the IPO boom and dot-com boom in the late '90s. Fraudulent ICO is fraud aiming at gaining funds from investors for an opportunity to support a new technology or creation of a new cryptocurrency without real intention to develop or create it. To reduce such offers, cryptocurrency exchanges must thoroughly check their business clients according to the Know Your Customer (KYC) procedure. In respect of a crypto platform operation proceedings may be instituted under article 159 of the Russian Federation Criminal Code.

7 Conclusion

Transformation of economic and legal relations influence the process of implementing innovative digital technologies. Such new features as intangibility, cryptographic authentication, decentralization, consensus-based management, and application of distributed ledgers in cryptocurrencies make it difficult to classify crimes in this area. Virtual currency operates in a grey zone. Mainly, cryptocurrency exchanges are the place where a crypto asset becomes fiat money. And this is the place where legal regulation must start.

Though the notions and features of a cryptocurrency and non-cash money have something similar, digital currency may be referred to other property under civil law and be defined as cryptographically protected property that exists only as information in the blockchain system.

When referring a cryptocurrency to immaterial things, we can establish ownership to it by lawfully obtaining a private key. Since a cryptocurrency has legal and economic properties, it is prone to unlawful taking. The most common way of taking this asset is fraudulent taking (personal data theft, mass-marketing fraud, imitating, phishing, malware, and personal extortion).

While user interface and access to innovative blockchain technology become easier, the number of cryptocurrency-related crimes, such as larceny, fraud, theft by taking property openly, robbery, extortion, misapplication, and kickback, will grow.

References

1. David Chaum. Blind signature for untraceable paymants, https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.
2. Mayning kriptovalyuty, https://mining-cryptocurrency.ru.
3. K. Nikitin, Rynok tsennykh bumag, 7 (2016)
4. V.K. Shaydullina, Vestnik universiteta (State University of Management), **2**, 137 (2018)
5. A.V. Savelyev, Zakon, **8**, 136 (2017)
6. V. Kisly, Klassifikatsiya i pravovoe polozhenie kriptoaktivov, https://zakon.ru/blog/2017/06/13/klassifikaciya_i_pravovoe_polozhenie_kriptoaktivov
7. O. Wyman, Blockchain in Capital Markets: The Prize and the Journey, http://www.dltmarket.com/docs/BlockchainInCapitalMarketsThePrizeAndTheJoumey.pdf

8. Guidance on Cryptoassets. Financial Condact Authority (FCA), https://www.fca.org.uk/publication/consultation/cp19-03.pdf.
9. Legal statement on cryptoassets and smart contracts UK Jurisdiction Taskforce, https://www.lexology.com/library/detail.aspx?g=002956de-cd49-46ab-9218-f80a1cc92ad3#:~:text=The%20UK%20jurisdiction%20taskforce%20of,are%20enforceable%20by%20the%20courts.
10. New York Codes, Rules and Regulations, Title 23. Part 200 "Virtual Currencies, https://govt.westlaw.com/nycrr/Document/I85908c68253711e598dbff5462aa3db3?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default)&bhcp=1
11. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO. Securities and exchange commission, https://www.sec.gov/litigation/investreport/34-81207.pdf.
12. O. Wyman, Blockchain in Capital Markets: The Prize and the Journey, http://www.dltmarket.com/docs/BlockchainInCapitalMarketsThePrizeAndTheJoumey.pdf.