

## **Crime in Era of Digital Technology: What Can Change with Cryptocurrency Status Clarification for Development of Information Environment of Vietnam?**

**Le Trung Kien**

The People's Police Academy, Vietnam.

**Nguyen Huy Binh**

The People's Police Academy, Vietnam.

*Received March 14, 2021; Accepted June 30, 2021*

*ISSN: 1735-188X*

*DOI: 10.14704/WEB/V18SI04/WEB18141*

---

### **Abstract**

The present paper analyses the aspects of investigations of crime involving cryptocurrencies as a payment instrument. Ever since their emergence, cryptocurrencies have come to be actively used by criminals in all types of illegal activities, such as drug trafficking, money laundering, illegal arms trade, payments for criminal services and many other crimes. The paper aims to establish the methods of crime investigation to track data on cryptocurrency transactions and identify and show up the participants of illegal operations. The author shows that the development of computer and digital information technologies and the Internet has brought about the ever-increasing prevalence of cryptocurrencies in all social domains, including the shadow sector, i. e., the criminal world. Figures are provided illustrating the overall circulation of cryptocurrencies in the world and its illegal segment. Explaining the attractiveness of cryptocurrencies for criminal structures, the author points at its anonymity and inadequate regulation of various aspects in laws. An analysis is provided of the practice of countries where cryptocurrency circulation is not only permitted but regulated to a maximum possible extent. The impact of such regulation for the state of the shadow cryptocurrency market is shown. The research further concerns the potential for bringing international expertise to the Socialist Republic of Vietnam. Potential methods of crime investigation concerning shadow cryptocurrency transactions are outlined, helping to identify and show up the participants involved. Forecasts are provided as to the development of modern forensics and the emergence of new forensic methods helping to uncover cryptocurrency-related crime; proposals are drawn for amending criminal and criminal procedure laws to facilitate investigations in the new context.

### **Keywords**

Legal Regulation, Investigation, Forensic Method, Internet, Digital Information Technology.

## **Introduction**

The development and adoption of new information and communications technology powering further advance of computer equipment, its ubiquitous penetration in all domains of human operation is the main driver of the digitalisation of social relations. Humanity has actively leveraged technological advances in day-to-day routines (Veselovsky et al.: 2020; Deeva et al.: 2020).

Paper money circulation has been increasingly replaced by technology instruments. People have come to largely hold their monetary assets in electronic equivalents (Kirillova et al.: 2019).

Among technology instruments used in payments for goods and services, currency has increasingly gained traction as it provides convenience, i. e., mobility, in various types of use. For now, cryptocurrency suits this characteristic (Deriugin, Zhizhileva: 2019).

Meanwhile, the rapid advance of information technology has posed a risk for the effective protection of human rights. Today, information can be retrieved, obtained and transferred within and across national borders with the resources of the Internet. Current attempts at regulating the use of information technology are often bordering on compromising human rights (Skripak et al.: 2020; Krivova et al.:2020; Aleksina: 2020).

Unfortunately, the upsides of new technology are often abused for illegal purposes. Criminals have actively and efficiently harnessed the information and communications environment and capabilities of new technologies to engage in all sorts of illegal activities. Society, and particularly its criminal segment, are engaged in the virtual environment in various forms (Deriugin, Zhizhileva: 2019).

According to a study by the United Nations, the estimated amount of money laundered globally in one year is 2-5% of global GDP, or \$800 billion-\$2 trillion. The figures include considerable numbers of crimes involving virtual money. As its legal status is undetermined and given the difficulty of detecting such offences, their number is growing significantly. At the end of 2018, illegal activity involving Bitcoin was estimated at around \$76 billion per year (46% of Bitcoin transactions), which is close to the scale of the U.S. and European markets for illegal drugs. Moreover, approximately one-fifth (23%) of the total dollar value of transactions and approximately one-half of Bitcoin wallets (49%) are in some way associated with illegal activity involving crypto algorithms. Experts at international forums and law enforcement officials highlight negative trends toward using Bitcoin for virtual settlements in various types of crime. Specifically, law enforcement

officials at summits in the Asia-Pacific region in 2018-2019 isolated one of the most serious threats of crime involving cryptocurrency (Group.iB: n.d).

Cases of crime involving cryptocurrency are observed in the Socialist Republic of Vietnam, too. In April 2018, ICOs of two cryptocurrency startups, Ifan and Pincoin, operating under the business name Modern Tech, resulted in \$660 million of losses for investors. The situation prompted an immediate response from the government, launching an official probe of the incident. An official probe was announced, which showed 32,000 investors were affected. There is still no full clarity concerning the organisers of the ICOs and actual financial losses, however, the announcement of a probe is just one step taken by the authorities. Soon after the incident, Prime Minister of Vietnam Nguyen Xuan Phuc published a directive "On enhancing management of activities related to Bitcoin and other virtual currencies for the Central Bank and securities market regulator" (Markarian: 2017).

However, forensics as a toolkit and science of criminal investigation would inevitably get involved in the process and has actively contributed new knowledge and technical advances for gathering, investigating and analysing material evidence obtained during crime solving and investigation.

The issues of countering cryptocurrency-related crime were addressed by researchers such as E. S. Markarian (2017), M. Iu. Makukha (The Blockchain Journal: 2018) and many others.

Even with the wide body of scholarly research, there is yet no well-formulated doctrine on cryptocurrency legalisation and its influence on the state of things in crime investigation. Research hypothesis: The legal vacuum around the status of cryptocurrencies and financial control is not a significant factor facilitating illegal activities of criminal structures earning income from trade in prohibited goods and services or engaging in money laundering by way of converting cryptocurrencies to fiat money.

## **Results**

Some researchers link the difficulties of cryptocurrency-related investigations to the lack of developed legal parameters and a set scope of safe cryptocurrency transactions (Alizade, Volevodz: 2017). To a major extent, it is due to the lack of clear understanding among local and international experts as to the importance of applying risk-oriented analysis in cryptocurrency studies to weigh economic advantages against crime potential of crypto instruments (Popper, Ruiz: 2017). The lack of a comprehensive analysis of criminal trends

in the use of cryptocurrencies inevitably affects performance in countering crime (Alizade, Volevodz: 2017).

Without regulation, the crypto market is unstable and hard to predict. It is hard to see what the regulatory landscape would look like in six months, let alone after a year-long period. E. g., Asian economies have revised their approaches to regulating cryptocurrencies, some for the better, some for the worse. Crypto regulation is checkered in Asia. There are countries positioning themselves as global industry leaders.

For instance, Japan regulates cryptocurrencies and regulators permit purchases of goods and services in exchange for cryptocurrencies. The country's cryptocurrency exchanges are licenced and subject to regular audits. These measures enhance Bitcoin reputation and make it more reliable and trustworthy for the Japanese. This, in turn, results in a greater number of users and holdings of Bitcoin (Freitas: 2020).

The only country in mainland Indochina where cryptocurrency circulation is regulated and permitted is Thailand. Authorities in Thailand have long been unable to determine a stance on digital assets. The country's Central Bank would even issue a recommendation some time ago to avoid the use of cryptocurrencies. Authorities were also outspoken on the dangers of crypto trade and opening crypto exchanges (Freitas: 2020).

More recently, Thailand's approach to regulating cryptocurrencies has involved the development of guidelines and laws to protect consumers and ensure national competitiveness on a global scale.

In the summer of 2018, the country took steps to provide for the licencing of crypto businesses to operate in the country. Seven cryptocurrencies were also legalised, including Bitcoin, Ethereum, Bitcoin Cash, Ethereum Classic, Litecoin, Ripple and Stellar, without explanations why these specific coins would get a legal status (Freitas: 2020). A bit earlier, in the spring of the same year, authorities introduced double taxation of all crypto transactions. Given that money laundering is a pressing problem of the country, a crypto exchange has to disclose the details of its operations to regulatory authorities to get and retain a licence. Unauthorised ICOs incur prison sentences and fines of up to \$16 thousand (Freitas: 2020).

In Vietnam, Bitcoin regulations are taken rather stringently. Bitcoin as a means of payment has been prohibited since January 2018. The government said that crypto assets are about money laundering, terrorism funding and tax evasion. The fine for violations of these rules

is 150 to 200 million Vietnamese Dongs. Currently, the issuance, offering and use of Bitcoin and other similar virtual currencies as a means of payment in Vietnam is prohibited (Tetkin: 2018).

There was further tightening of control of the industry in Vietnam after, as mentioned above, two ICO startups deceived 32,000 local investors into a total loss of \$660 million. The State Securities Commission of Vietnam (SSC) prohibited the use of cryptocurrencies for local companies and funds. They are not allowed to take part in the issuance, transactions or broker transactions related to digital money (Tetkin: 2018). The July 2018 ban restricted specific types of activities involving cryptocurrencies but citizens could still legally buy and hold BTC in Vietnam. In July 2018, the country also introduced a restriction on equipment imports for cryptocurrency mining. Mining itself is not prohibited in Vietnam (Freitas: 2020).

Then, too, a directive was issued in Vietnam, prohibiting lending institutions from providing services to cryptocurrency subjects, which was primarily explained as efforts to counter money laundering (Tetkin: 2018).

Since then, regulation of virtual currencies in the country has remained unchanged and there is almost no regulatory framework for the country's existing crypto exchanges.

However, despite this state of things in regulations, local firms have spent years trying to set them up and running. In 2019, the government gave permissions for operation in Vietnam to several select cryptocurrency companies. For example, Linh Thanh Group (Vietnam) and Kronn Ventures (Switzerland) obtained a licence to launch the country's first regulated cryptocurrency exchange (Antipov: 2020). More recently, several international companies have targeted the Vietnamese market and even in January, the Binance exchange introduced the option to buy cryptocurrencies for Vietnamese Dongs.

Now, in 2020, the Vietnamese Finance Ministry decided to create a research group to focus on cryptocurrencies and introducing political proposals on regulation. The group would include nine members led by Chairman of the SSC Pham Hong Son. Moreover, the group will include representatives from the General Department of Taxation, the National Institute for Finance of Vietnam, the customs service and the Department of Banking and Financial Institutions of the State Bank of Vietnam (Antipov: 2020). The research group should engage in studies of blockchain technology, cryptocurrencies, and should help the government to better understand the regulatory issues.

The coming years or even months might see some easing of the rules, as the restrictive stance is only a partial ban against digital currencies which only applies to their use as a means of payment. The situation is changing.

It is clear that transparency of cryptocurrency exchange operations for the regulator is a requirement that will become more widespread not only in Asia, but globally, too.

If the ban is though lifted, transactions in purchasing, selling or exchanging one cryptocurrency for another would be facilitated only by operators of financial asset exchange, being legal entities and operating under exchange licences or a licence of a trade system. An operator of financial asset exchange would become the owner of a wallet, and the user would only have one of the keys to sign disposals of the wallet holdings. Transactions with holdings of the wallet opened and used against the rules and outside control of the Central Bank will be deemed illegal. In such situation, the settlements market will be divided into an official vs. a shadow segment, including some cryptocurrency transactions registered and controlled by the state and all the rest, which encompass all of today's transactions. This shift in the noncash settlements market is what the country's law enforcement system should be preparing itself to.

## **Discussion**

The emergence of forensics in Vietnam came rather late in the poor country after a long war; its development in Vietnam comes primarily from a practical vein and access to materials for studies is limited. The level of coordination between academic and practical institutions is inadequate. Currently, academic talent is not properly qualified to retrieve and analyse scholarly works in foreign languages. Many lack experience and basic practical knowledge. Therefore, studies of acute current issues fall behind the demands of the time (Nguyen, Ta: 2019).

It is crucial to study efficient methods and tools to solve crimes committed in Vietnam, particularly in high-tech spheres, but for now, it seems rather challenging.

The challenge is that papers and research projects on forensics studied by students and graduates in police institutions fall short of practical demands. Modern criminals fully engage all scientific and technological capabilities to commit crimes. And as long as the system of investigation methods, tools, techniques and tactics falls short of modern requirements, the potential of detecting, combating and preventing crime will be significantly restricted (Nguyen, Ta: 2019).

The list of problems is even wider, but a solution can only be found today, in our view, through the accelerated and intensified development of applications for digital forensics, which is only getting initial advancement with the leading forensic specialists in the world. One of the approaches proposed by scholars is based on the idea that digital forensics supports the research credibility of propositions of traditional forensics (Bagmet: 2019). Digital forensics is merely meant to specify the following relevant criminal patterns. 1. The aspects of illegal activities seeking to interrupt the normal course of operation of information systems and their components. 2. The aspects of illegal activities seeking to use information systems and components as tools for committing other crimes. In designing the norms of criminal law, specifically digital terminology should be better avoided. E. g., the general chapter of many criminal codes of foreign countries today contains a basic regulation that everything stated in the code equally applies to data in the electronic (digital) form. Those codes are not overloaded with articles with remarks. Foreign forensic specialists approach the digital environment in life not in terms of a revolution in forensics but rather as presenting certain specifics in traditional forensics. The digital economy would inevitably bring about a revision of the existing criminal and criminal procedure laws. 3. The aspects of developing, changing, transferring and destroying information on electronic carriers, in information and telecommunications networks, in the virtual environment during the preparation, execution and covering up of the crime. Digital forensics serves to guide all official authorities and information security services toward a competent approach in searching and capturing digital evidence. 4. The aspects of the investigation of digital information stored in individual information items and the information environment of an electronic information carrier.

For now, not only in the Socialist Republic of Vietnam but globally, there is yet no integral, universal and efficient forensic method to detect such crime and gather evidence on the investigated case. Consequently, the situation now looks somewhat like a paradox when crime involving cryptocurrencies continues to exist without, though, any accessible and efficient method to detect and prevent it. The lack of adequate control of committed crime by itself provokes an illusion of impunity among those who commit it. Such kind of a forensic method should be based on only fundamental functional principles of cryptocurrencies (Iakovlev: 2018). Those include: - decentralised issuance; - lack of opportunity (at least yet) and particularly technical opportunity to control and regulate circulation; - anonymity of cryptocurrency users amid the fully open circulation of cryptocurrency coins and possibility to track cryptocurrency transactions; - lack of territorial and administrative barriers to create and use a cryptocurrency; - availability of an anonymous opportunity to complete all types of transactions irrespective of national legal

requirements in a specific country (Iakovlev: 2018). Accordingly, taking into account the degree of anonymity in using cryptocurrencies, there has to be a defined limit where such anonymity ends and gives way to the so-called "points of access" to private data of an actor executing cryptocurrency transactions in violation of national legal norms. Given that crypto wallets are, as a rule, anonymous, one of such "points of access" can be a cryptocurrency conversion (purchase and sale) transaction in exchange for fiat money. It is exactly when such transaction is completed by crediting (debiting) an amount of fiat money to the bank account of the seller (buyer) of cryptocurrency coins that the opportunity emerges to identify the transaction participant or at least the respective actor acting on behalf of such participant or in some relation to the former (Iakovlev: 2018). The second "point of access", though not necessarily providing visibility into the identity of the actor engaging in illegal cryptocurrency transactions but still enabling certain relatively determinate guesses concerning the respective identity is the complex analysis of data on connections of the anonymous person with previously established individuals and analysis of data of anonymous and actual individuals, specifically in the Internet telecommunications network (Iakovlev: 2018). It is specifically in such a way, according to the FBI, that Ross William Ulbricht, the owner of the Internet marketplace Silk Road, was detected and subsequently held liable (Veselovsky et al.: 2020). This purpose can be successfully met by using software to draw a diagram of connections or by engaging schemes plotted by an expert analyst. The most efficient method would be a complex approach based on human analytics and computing capabilities. Using these two methods in combination is today the most efficient method to detect cryptocurrency-related crime and, besides, a source of evidence in subsequent criminal investigations. They should make the foundation of the forensic method to detect crime involving cryptocurrencies and investigate criminal cases of this type.

## **Conclusion**

Accordingly, the current state of cryptocurrency-related crime control in the Socialist Republic of Vietnam cannot be deemed satisfactory. The introduction of legal regulation of legitimate cryptocurrency circulation seems insufficient to make it satisfactory. In case of cryptocurrency legalisation, a fraction of the market associated with crime such as fraud, drug trafficking, money laundering, would still remain in shadow. This conclusion confirms the research hypothesis and indicates the need to develop digital forensics based on the principles of traditional forensic doctrines. It is necessary to draw on global practices to develop forensic methods for searching and capturing digital traces and identifying actors completing anonymous transactions with cryptocurrencies and to ensure technical capabilities for forensic departments. It is also necessary to revise the criminal and criminal

procedure codes to make sure the applicable terminology supports the development of digital evidence and its inclusion. The problem domain addressed here is overly expansive to cover it in a single paper. Also of interest are the aspects of certain methods to identify actors conducting anonymous transactions with cryptocurrency; searching and capturing their digital traces and further analysis is a practicable extension of the subject in further research.

## References

- Aleksina, S.B. (2020). Trends in the Development of Distribution and Retail Sales of Consumer Goods in the Context of Integration Processes in the Russia's Trade. *International Journal of Management*, 11(4), 232-243.
- Alizade, V.A., & Volevodz, A.G. (2017). Judicial practice on crimes of criminal communities (criminal organizations) in the sphere of illegal drug trafficking using the information and communication network Internet and cryptocurrency. *The forensic library. Science Magazine*, 6(35), 281-299.
- Antipov, G. (2020). Vietnam will study cryptocurrencies to create regulations. Coinspot. <https://coinspot.io/law/asia-and-africa/vietnam-izuchit-kriptovalyuty-chtoby-sozdat-reguliruyushhie-pravila/>
- Bagmet, A.M. (2019). On detecting and investigating cryptocurrency-related crime, in: A.M. Bagmet (ed.), Proceedings of the International research and practical round table. "Illegitimate use of cryptocurrencies and methods of control", Moscow, Russia. Moscow: Moscow Academy of the Investigative Committee of the Russian Federation, 14-16.
- The Blockchain Journal. (2018). Vietnam investigates fraudulent ICOs worth \$ 660 million. <https://thebcj.ru/2018/04/12/vietnam-rassleduet-moshennicheskie-ico-na-660-mln-dollarov/>
- Deeva, T.V., Nikiporets-Takigawa, G., Lustina, T.N., Podsevalova, E.N., & Didenko, E.N. (2020). Blockchain Technologies and Smart Contracts: New Technological Methods to Regulate Transactions and Trade Operations. *International Journal of Emerging Trends in Engineering Research*, 8(7), 3659-3664.
- Deriugin, R.A., & Zhizhileva, A.A. (2019). Prospects of further development of forensics in the knowledge society, in: D.V. Bakhteev (ed.), Proceedings of the Russian national research and practical conference, "21th century technologies in law", 2019, Yekaterinburg, Russia. Yekaterinburg: Federal State Budgetary Educational Institution of Higher Education "Ural State Law University", 40-46.
- Freitas, C. (2020). Legal status of cryptocurrencies in Asia: the current state. Currency.com. <https://currency.com/ru/pravovoj-status-kriptovalyut-v-azii>
- Group.iB. (n.d). Illegitimate cryptocurrency trade is rising. <https://www.group-ib.ru>
- Iakovlev, A.N. (2018). Digital forensics as a factor in protecting the digital economy. In: S.V. Valov (ed.), Proceedings of the International research and practical conference, "Forensics in the developing knowledge society", Moscow, Russia. Moscow: Academy of Management of the Ministry of Internal Affairs of the Russian Federation, 325-331.

- Kirillova, E., Bogdan, V., Lagutin, I., & Gorevoy, E. (2019). Legal status of smart contracts: characteristics, role, meaning. *LEGAL CUC*, 15(1), 285-300.
- Krivova, A.L., Kurbakova, S.N., Afanasyev, V.V., & Rezakov, R.G. (2020). Capabilities of cloud services and webinars effectiveness of teaching humanities students. *Latin American Utopia and Praxis: International Journal of Ibero-American Philosophy and Social Theory*, (5), 135-146.
- Markarian, E.S. (2017). Aspects of cryptocurrency-related crime investigation, in: V.N. Sinyukov (ed.), Proceedings of the Eleventh research and practical conference, "Ensuring human rights and freedoms in the modern world". Moscow: Limited Liability Company "Prospekt", 259-263.
- Nguyen, V.T., & TA, K.K. (2019). On the ways of development of forensic science in the Socialist Republic of Vietnam. *Civil service and personnel*, 4, 155-157.
- Popper, N., & Ruiz, R. (2017). *Leading Online Black Markets Are Shut down by Authorities*. The New York Times.
- Skripak, I.A., Aynazarova, S.N., Ukhanova, E.V., Tkachenko, A.E., & Erina, L.S. (2020). Digital virtualization technologies in distance learning. *International Journal of Advanced Trends in Computer Science and Engineering*, 9(2), 1808-1813.
- Tetkin. M. (2018). The Vietnamese government has introduced another cryptocurrency ban. RBC. <https://www.rbc.ru/crypto/news/5b71874f9a794764ed529964>
- Veselovsky, M., Izmailova, M., Bitkina, I., Krasnyukova, N., & Stepanov, A. (2020). Enhancement of government innovation policy in digital transformation of russian companies. *Revista Inclusiones*, 306-319.
- Ahmad, H., & Dowaji, S. (2019). A semantic approach for outlier detection in big data streams. *Webology*, 16(1), 184-195.