CRYPTO-ASSET TRANSACTION ARBITRAGE

Andrej Lipták

Financial Investigation Department, National Centre for Specific Crimes
Ministry of Interior of the Slovak republic, Pribinova 2, 812 72 Bratislava, Slovak republic
andrej.liptak@minv.sk, andrej.liptak@akademiapz.sk
https://www.researchgate.net/profile/Andrej-Liptak/research

Abstract

Using qualitative and quantitative research methods, this study article examines the principles and processes of crypto-asset transactions, identifying opportunities for transaction reversal and outlining methods to achieve this goal. The objective is to provide theoretical insights into addressing situations involving unwanted or unethical crypto-asset transactions, offering guidance to authorized entities, professionals, and the general public on preventive measures and corrective actions in the realm of crypto-asset-related crime. This contribution addresses the need to tackle current crypto-asset-related criminal activity, which encompasses a broad spectrum of illicit actions facilitated by offenders using crypto-assets. Unlike traditional fiat systems, where fiat currency serves as a means of exchange, crypto-assets offer an alternative. They not only enable the transfer of financially relevant information but also allow for the storage and immutable recording of data on a network, with automated tasks based on specified conditions. The article aims to offer theoretical knowledge and practical advice to authorized entities, law enforcement professionals, the professional and the general public regarding preventive measures and corrective actions in the realm of crypto-asset-related crime.

Keywords: crypto-asset, transaction, mempool, replacement, simulated transfer

Introduction and the problem statement.

This contribution stems from the need to address the current state of criminality, which is characterized by the use of crypto-assets. This term is derived and will be used in this contribution based on Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance). Crypto-assets represent an alternative to the commonly used financial system based on legal, institutional, and technological aspects, otherwise known as the fiat financial system. Where financial assets of the fiat financial system, such as fiat currencies, can alternatively be represented by crypto-assets for the same purpose. In this sense, criminality related to crypto-assets is a very broad area, as wherever fiat currencies are used as a tool for committing criminal activities, as proceeds from criminal activities, as reward for the commission of a criminal offense, or as a bribe or motivation and incentive for committing criminal activities, crypto-assets can under similar conditions also be used. Therefore, crypto-assets cannot be considered solely as part of a specific type of criminality, as their scope is much broader. However, crypto-assets not only represent an alternative option for transferring financially relevant information. Crypto-assets enable the storage of individual pieces of information, i.e., data on the network, ensuring their immutability, allowing for the networked placement of logically ordered source code with automated task execution according to specified conditions. Certain types of criminal activities can also be conducted within the crypto-assets system, just as analogously on social networks or networks with a special access.

The subject of this contribution is, considering the current development of crypto-assets-related criminality in Slovakia and worldwide, to present, using methods and techniques of qualitative-quantitative research, the possibility of reversing a crypto-assets transaction. The term transaction evokes the transfer or movement of subjectively assessable values, which is too narrow a denomination concerning crypto-assets. The essence of a crypto-assets transaction is primarily the transfer and movement of data and information, and only when participants in the network assign financial character to this data can we regard a crypto-assets transaction as the transfer and movement of assessable values. However, in this contribution, we will abstract from any meaning of the term transaction other than this narrow essence of crypto-assets transaction. In this contribution, we analyze the basic principles of crypto-assets transactions, we dissect the process of constructing a transaction until its inclusion in a distributed transaction database. We identify the possibilities of reversing a crypto-assets transaction in the individual stages of this process and mediate the conditions, methods, and individual actions aimed at such reversal of a crypto-assets transaction.

The assumed result is the processing of a logically ordered aggregate, which will provide theoretical groundwork for acting prophylactically in the situation after the execution of an unwanted or reprehensible crypto-asset transaction. The purpose of the contribution is to highlight the possibilities of modification and recovery of assessable values in the form of crypto-assets if a crypto-assets transaction, for example, in fraudulent behavior, has already been initiated. The contribution answers the question: "What to do after executing a crypto-assets transaction that morally should not have been executed?". The aim of the contribution is to provide authorized enforcement agencies with a structure for implementing technical prophylactic measures in performing tasks defined by generally binding and internally related regulations; to the professional public, an insight into the issue of crypto-assets-related criminality in this specific and unusual area of execution and moral manipulation with crypto-assets transactions; to the general public, guidance and options for proceeding in cases where unwanted crypto-assets transactions have been executed.

Foundation.

Crypto-asset transactions involving financial relevant information can, under certain conditions, be analogously compared to transactions in the electronic fiat financial system, which are most commonly represented by electronic bank transfers of fiat currency funds. In the case of transferring fiat currency via electronic bank transfer, it is necessary for the initiator, the party authorized and having control to transfer fiat currency, to initiate such a transaction. The initiation of the transaction is often carried out through electronic banking applications, following proper registration and login, by entering the necessary details into a preset form, where the initiator must invariably provide the bank account identifier IBAN as the destination address, i.e., the recipient of the fiat currency, and the amount of fiat currency being transferred.

Confirmation of the information in the application form initiates the transaction by creating a request, which is then sent cryptographically from the application, and thus from the device where the fiat currency transaction was initiated, through the network to the banking institution for processing the desired transaction. The processing of the transaction is centralized and automated, with actions to verify the validity and truthfulness of the initiated fiat currency transaction, i.e., whether the initiator is an authorized holder of the sending fiat currency, or whether at the time of initiating the fiat currency transaction, he had a sufficient amount of fiat currency, etc. Often, after the initiation of the transaction, after the request is created and sent to the bank, this process becomes irreversible at this stage. The actual processing, realization, and confirmation of the fiat currency transaction take approximately several hours depending on the electronic banking services provided. Cancellation of such a fiat currency transaction is technically possible, but it requires the willingness of the banking institution to undertake immediate actions in favor of its client. Actions aimed at urgent cancellation of the transaction often involve additional fees and the necessity of visiting an institution branch, which includes providing explanations, filling out additional forms, and similar procedures. This, coupled with the time pressure resulting from the expected irreversible confirmation of the fiat currency transaction, presents a situation where failure of doing so is almost certain. After confirming the fiat currency transaction, the banking institution, based on the details of the initiated fiat currency transaction, such as domestic transfer, international transfer, transfer between banking institutions, etc., processes the request for the return of fiat currency, which is then sent to the banking institution operating the recipient's IBAN. The processing time for domestic transfers is approximately 30 days, and for international transfers approximately 180 days, with the actual return of fiat currency not guaranteed. [1]

Similar procedures apply to other financial institutions utilizing various payment methods that facilitate the transfer of financial assets or other assets electronically through data transmission.

Analogously, one can view crypto-asset transactions in a similar manner. To execute a transfer of crypto-assets, the transaction must be initiated. The initiation itself can be carried out either through a software interface, an application on a mobile device, or through specialized ATMs, known as crypto-assets ATMs or "crypto-ATMs," which handle the initiation of the transaction. This involves gathering the necessary input information for the transfer of crypto-assets, creating a request, encrypting it, and then sending it for processing. In comparison to the fiat currency bank transaction discussed earlier, there is a notable difference here. In the case of a sent request for processing and confirmation of a fiat currency transaction, it is addressed directly to the banking institution that registered the IBAN identifier for the initiator and often operates the application or software interface through which the fiat currency transaction was initiated. The process is characterized by centralization, meaning there is a single central authority - in this case, the chosen banking institution - that is present from the initiation of the transaction to its final confirmation.

However, the transfer of crypto-assets is a decentralized process, sometimes even referred to a distributed process. This means that the initiator of the transaction, whether he’s using the application or crypto-ATMs, cannot process and confirm the transaction separately. In cases where the initiator of the crypto-assets transaction is also a network node responsible for processing and verifying the validity and truthfulness of the transaction (referred to as a "full node"), as well as a node in the network performing the activities of the consensus mechanism and recording information into the distributed transaction database (referred to as a "mining node"), and after meeting certain conditions gains the ability to record transactions into a block of transactions (known as mining a block), which is then added to the distributed transaction database - blockchain, and no other longer copy of the distributed transaction database exists, then it is possible for this initiator to both initiate and confirm such a crypto-asset transaction, which is considered relatively immutable.

The aforementioned request for processing a crypto-asset transaction is subsequently sent to entities responsible for verifying the correctness of the initiated transaction, whether it contains all the necessary elements for its confirmation, such as the correct format of the recipient's identifier for crypto-assets, i.e., the public address, which is the equivalent identifier to IBAN in the case of fiat currency transactions, and other details that will be addressed.

[1] See https://podnikam.sk/prevod-penazi-ako-prebieha-kolko-trva/.

Furthermore, the truthfulness of the declared information in the initiated crypto-asset transaction is verified, such as whether the initiator possesses the crypto-assets they plan to send. This is verified by checking whether in the distributed transaction database, which contains only confirmed transactions, there is information about a sum of previously sent crypto-assets to the public address of the initiator that is at least equal to the amount the initiator plans to send to the recipient. After verifying the initiated crypto-asset transaction and evaluating its validity, the transaction is marked as either satisfactory or unsatisfactory. Each device operates with a specific digital space referred to as device memory, where necessary digital records are performed. A transaction marked as unsatisfactory is then within the memory of such a device labeled as over writeable, meaning that it is no longer relevant, and further action is not taken with it. On the other hand, a transaction marked as satisfactory is stored in the device's memory and awaits confirmation and inclusion into the distributed transaction database.

The confirmation of a crypto-asset transaction falls within the control of other nodes in the network, entities that, according to the network's rules, have the authorization to confirm this verified and valid crypto-asset transaction by including it in the distributed transaction database, or the so-called blockchain (Šanta Ján and Šanta Ivo 2022), which represents the final handling of the crypto-asset transaction. The likelihood of immutability and integrity of the confirmed and recorded crypto-asset transaction is subsequently directly proportional to further subsequent confirmed transactions and thus with the passage of time. The temporal aspect from the initiation of the transaction to its confirmation and inclusion in the distributed transaction database is influenced by several factors.

The most important objective factor is the type or kind of distributed transaction database, or the type of crypto-asset. In Table No. 1, we list 10 crypto-assets in descending order according to their traded value in terms of the equivalent in the US dollar. [2]

Table 1

Order	Crypto-asset	DLT (Distributed ledger technology)	Volume for December 2023 v USD	Transaction confirmation in minutes
1	Tether USDT	Ethereum Virtual Machine (EVM) - Tron	1 006 822 913 419	14-2
2	Bitcoin BTC	Bitcoin	540 528 857 257	40
3	Ethereum ETH	EVM	198 178 245 871	14
4	USDC	EVM	103 670 462 597	14
5	Solana SOL	Solana	56 173 143 728	1/60
6	First Digital USD FDUSD	EVM, Binance Beacon Chain (BNB Chain)	55 604 681 385	14-10
7	Binance Coin BNB	BNB Chain	31 241 791 015	10
8	SEI	Cosmos Atom	23 379 894 961	1/120

[2] See https://www.statista.com/statistics/944355/cryptocurrency-transaction-speed/ and also https://coinmarketcap.com/currencies/volume/monthly.

Order	Crypto-asset	DLT (Distributed ledger technology)	Volume for December 2023 v USD	Transaction confirmation in minutes
9	Wrapped Ether WETH	EVM	23 135 056 513	14
10	Internet Computer ICP	Internet Computer	18 884 333 797	1

On the surface, there exists an entity that, through a user-friendly interface, can easily execute fiat currency transactions or crypto-asset transactions after completing several steps. However, in the background, there are several tasks necessary for the proper initiation, packaging, encryption, sending, processing, verification, and subsequent confirmation of individual transactions. By understanding these component tasks, subsequent analysis can lead to theoretical and practical insights relevant to desired operations, such as in this case, the reversal of a crypto-asset transaction. (Šanta Ján and Šanta Ivo 2023).

The Mempool.

Understanding the specifics of the transaction confirmation process for crypto-assets is essential in this regard. Initiated fiat currency transactions move data from the sender to the recipient in a centralized manner. Verification of whether the fiat currency transaction has been confirmed at the recipient's end can be confirmed by the sender by obtaining information from the entity executing the transaction confirmation, such as a banking institution. At that time, the sender only has information that the transaction was initiated and sent for processing and confirmation, primarily through an application or other software interface of electronic banking. It is recommended that access to this software interface is restricted to the sender, i.e., the account holder or authorized user associated with the account. The recipient of the fiat currency transaction receives confirmation information from the centralized banking entity only after the transaction is confirmed, typically through software interfaces of electronic banking linked to his account. By centralizing the transaction process, only the centralized entity has the information and capability to reverse such a fiat currency transaction.

In contrast, in the crypto-asset transaction system, information transfer is decentralized. Verification of a crypto-asset transaction sent by the initiator to the network is performed by decentralized entities, nodes in the network, or hardware-software interfaces designated for this purpose according to the rules of the crypto-asset. These nodes are characterized by maintaining a list of all crypto-asset transactions in their memory, which they receive and verify. This means that crypto-asset transactions are not verified by a single centralized entity that has the authority to control the original transaction list, but by many decentralized entities, network nodes, each of which possesses the original list of crypto-asset transactions. Of course, this raises doubts about the information security of individual nodes within the crypto-asset system. But we need to take to the consideration the fact, that the centralized fiat currency transaction system has an original transaction list in a much smaller number, which actually means the increase of the risk of unwanted modification of this transaction list compared to the crypto-asset transaction system, where currently more than 10,000 entities possess this transaction list. However, on the other hand, the list of fiat currency transactions is much better protected in terms of physical, object, regime, administrative, and cybernetic security than the list of crypto-asset transactions, mainly because any device capable of basic data verification tasks can lead and thus be a node in the crypto-asset network.

After verification by multiple nodes in the network, the initiated crypto-asset transactions are considered verified but still unconfirmed and stored in a temporary storage of the node. This temporary storage is referred to as the "mempool," an abbreviation for "memory pool." The summary of transactions that the mempool can contain directly correlates with the size of the memory allocated within the hardware interface for storing verified but unconfirmed transactions. (Florian, Beaucamp, Henningsen and Scheuermann 2019).

However, the confirmation of transactions lies within the competence of other network nodes equipped with sufficient computational power derived from their hardware-software setup to perform the mathematical and cryptographic operations necessary to confirm unconfirmed transactions and record them in the aforementioned list of all transactions - distributed transaction database. Transactions of crypto-assets recorded in this list of transactions are considered confirmed, and their reversal is deemed nearly impossible. The recording of a transaction, like the entire process of executing a crypto-asset transaction from initiation by the sender, is decentralized and thus transparent. A sender with sufficient technical capabilities can monitor this process throughout its duration. Those lacking such technical capabilities can rely on crypto-asset wallet service providers. In this regard, a crypto-asset wallet functions equivalently to an electronic banking application. However, as mentioned, the difference between the process of executing fiat currency and crypto-asset transactions lies primarily in decentralization and transparency, resulting in the fact that influencing the crypto-asset transaction process is sometimes easier than influencing the fiat currency transaction process. It is worth noting that crypto-asset transactions are recorded in the list of transactions in blocks, specific data files according to network rules. In the case of the Bitcoin network, these blocks are limited to 1 megabyte, sufficient to confirm approximately 3,000 transactions. Blocks of confirmed transactions in the Bitcoin network are recorded in the list of transactions approximately once every 10 minutes. As for unconfirmed crypto-asset transactions in the mempool, its size is naturally higher because confirmed transactions stem from unconfirmed ones, meaning the number of unconfirmed transactions awaiting recording can never be less than the number of confirmed and recorded transactions in the next block. (Wang, Tong, Wu, Pang, Chen, Luo, and Han 2023.)

The mempool is limited to approximately 300 megabytes, which equates to around 60,000 pending unconfirmed transactions. Upon recording a crypto-asset transaction into the list of all transactions, a node that has obtained authorization to record transactions into this list receives a reward in the form of crypto-assets in two ways. The first form entails the automatic release of crypto-assets as per the network rules, which incentivizes network nodes to record crypto-asset transactions. The second form involves rewards derived from recorded transactions. The initiator of the transaction determines the reward associated with the crypto-asset transaction during its construction. This reward serves as a catalyst or inhibitor of the speed of the process of executing the crypto-asset transaction and its recording in the list of all transactions, which is the subject and commonly the purpose of the entire transaction process. In general, a verified unconfirmed crypto-asset transaction in the mempool is sorted according to the value of this predetermined reward. The higher the reward, the greater the likelihood that the transaction will be recorded in the list of all transactions sooner than those transactions set with a lower reward. This fact stems from the reality that the node with the right to record transactions into the list of all crypto-asset transactions, utilizes economically costly hardware-software devices to generate the highest possible computational power, thus demanding the highest possible reward for recording a transaction. One form of reward is consistently dictated by the network rules, while the other form of reward is determined by the initiators of the transactions themselves, which are located in the mempool. The node with the right to record crypto-asset transactions has the discretion to select from all unconfirmed transactions in the mempool approximately 3,000 transactions and record them into the overall list of transactions.

Based on this, it is possible to some extent to predict the time when certain transactions will be recorded in the list of all transactions based on observing the values designated for nodes performing the recording of individual transactions in the mempool. The stability of the time prediction is primarily determined by the fact that the competition for transaction recording is extremely vast and demanding in terms of the overall computational power, e.g. in the Bitcoin network, which is currently at approximately 500 million terahashes per second (TH/s), representing a value of around 8 billion USD for illustration, solely by the hardware interface designated for recording crypto-asset transactions. From this, it follows that the entities responsible for recording transactions into the list of transactions are significantly motivated to select from the mempool those unconfirmed transactions with the highest reward value.

The mempool is not rigid; the quantity of transactions cannot be precisely determined, especially considering the decentralized nature of the crypto-asset network. However, the same decentralization, along with the transparency of the network, ensures the availability of data and information that can be analyzed, measured, and quantitatively examined with a certain degree of predictive accuracy. It is worth mentioning that the number of unconfirmed transactions placed in the mempool is limited by the size of the mempool itself. If the mempool is full, it is unable to accommodate a larger number of transactions in its memory. In such cases, the mempool rejects these transactions and redirects them to another mempool, or deletes those crypto-asset transactions with a lower designated reward for the nodes performing the recording into the list and replaces them with those that have a higher included reward. The inclusion of a transaction into the mempool is a phase very close to the recording of the transaction into the list of all transactions. Transactions in the mempool are stored depending on the nature of other transactions in the network, typically for about 14 days. Automated prediction of transaction recording in the mempool, is able to relatively reliably determine, whether and when the transaction will be confirmed during normal network operation.[3]

This calculation and prediction can consensually consider the quality of a transaction, which, although unconfirmed, is initiated, verified, and meets all the conditions for inclusion in the list of all transactions, and given the current practice at the moment, which is mostly sufficient for network participants to consider this transaction as valid and behave towards it as if it were a completed transaction. In fact, the inclusion in the mempool and the determination of the expected time of recording, or the expected confirmation of the transaction, are so significant that crypto-asset wallet providers mediating simple user interfaces for their clients utilize this moment as sufficient evidence to inform the intended recipient of the crypto-assets about the received assets, even though the transaction has not been fully confirmed, i.e., it has not been actually recorded in the list of all crypto-asset transactions. It can thus be inferred that by manipulating the reward designated for nodes performing the recording into the list of confirmed transactions, one can influence the time required to confirm such a transaction. (Mikhaylov, Dincer, Yuksel, Pinter, and Shaikh 2023).

Replacement of crypto-asset transaction.

Based on the analyzed facts so far, it can be said that the process of executing crypto-asset transactions is transparent and decentralized, independent of any single entity, and is relatively

[3] See https://github.com/mempool/mempool.js.

observable in each of its partial phases. Independence also allows the initiator of a crypto-asset transaction to create, or initiate, multiple transactions arbitrarily. The verification of a crypto-asset transaction occurs only after its initiation, construction, and submission for verification. This means that the initiator has the ability to construct purposeful transactions. An example might be an unethical situation where the initiator, who is the controller of a certain amount of crypto-assets, perhaps having received 1 Bitcoin in a transaction in the past, which successfully went through the entire execution process and was duly recorded in the list of all transactions, therefore considered valid, constructs two transactions at one moment, both involving the transfer of 1 Bitcoin to two different recipients represented by two distinct public addresses.

Given the general nature of the network, nothing prevents both transactions from being considered acceptable to proceed with the process of executing crypto-asset transactions until proven otherwise. Due to the decentralization of the network, the initiator can send these transactions to different nodes for verification. Both transactions reference the same transaction history, which is valid, so it's possible that both transactions will be independently marked as valid, verified, and included in the mempool. It's important to note that as these transactions progress through the execution process, the likelihood of one of them being rejected by the network diminishes. These already verified crypto-asset transactions, each separately included in two different mempools, are queued based on the reward designated for nodes performing transaction confirmation.

Even in such a highly unlikely scenario, which could be accelerated by offering high rewards to nodes performing transaction recording, where each transaction is independently recorded in the list of confirmed transactions by a separate node responsible for transaction confirmation, both transactions will be recorded in the list of all transactions and become confirmed. At this point, emphasized by the fact that crypto-asset wallet service providers have already notified the recipient about the received crypto-assets before the actual recording and confirmation of the transaction, a problem arises because the same crypto-assets with the same history have been spent twice, i.e., 1 Bitcoin has been spent twice. This could lead to infinite expansion of crypto-assets in an unethical manner, against the rules of the crypto-asset network.

Such a scenario is however rightly so, assumed by the network. From the initiation of the transaction to its recording in the list of all transactions, i.e., its confirmation, not even a few seconds may pass, especially if the initiator is knowledgeable, operates their own verification node, designates significantly high rewards for nodes performing transaction confirmation, or operates the confirmation node themselves and manages to obtain the right to record such transactions. To ensure the legitimacy of the list of all transactions for other participants, it needs to be shared among other network nodes. These nodes verify not only initiated transactions but also the entire list of recorded transactions and continuously monitor their validity.

If a record of all transactions containing both of these transactions, immoral but logically constructed, verified, and even logically recorded, were sent to the other nodes in the network, it would be rejected by the other nodes after subsequent, relatively quick verification. Not only would it be rejected, but the node that recorded this transaction would also be marked by the other nodes as a node attempting to manipulate the network, and they would no longer accept any information from it. Consequently, the node would lose the stable reward for transaction recording, as well as the reward from transactions designated by the transaction initiators that would otherwise be due to it. Additionally, it would lose the network's trust and essentially the ability to record transactions in the list of all transactions. This problem is known as double-spending, and it is essential to understand its nature and the measures taken by the crypto-asset network to address this issue, as its qualities can be exploited in replacing a transaction. (Rondelet and Kilbourn 2023.).

Results.

By synthesizing the examined phases of crypto-asset transaction processes, technological aspects ensuring the execution of crypto-asset transactions, and knowledge gained from comparing the system of executing crypto-asset transactions with the system of executing fiat currency transactions, it has been found that:

- The execution of crypto-asset transactions is governed by the rules of a decentralized and transparent network with constant monitoring capabilities of all phases of the crypto-asset transaction process.
- The execution of fiat currency transactions is governed by the rules of a centralized entity that oversees the entire process of executing fiat currency transactions.
- The process of executing both crypto-asset and fiat currency transactions occurs within a relatively short time frame, with the time frame for crypto-asset transactions being influenced by the determination of transaction fees.
- Reversing a fiat currency transaction is not practically possible after the transaction is constructed and sent for verification, processing, and confirmation.
- Reversing a crypto-asset transaction is possible by replacing it during the transaction verification and mempool inclusion phase, and under certain conditions, even after its confirmation.

Utilization for the purposes of simulated transfer.

The results of the study should be presented on a modeled case, which represents a specific utilization of the method of crypto-asset transaction arbitrage. It is necessary to remind that this modeled case is just a small excerpt from the overall potential of arbitrage for individually targeted crypto-asset transactions.

Simulated transfer, according to the Act No. 301/2005 Coll. – Criminal Code, Act No. 300/2005 Coll. – Penal Code (hereinafter referred to as the "Penal Code"), according to special legal regulations of the Slovak republic, and in accordance with criminal law theory, refers to simulating a purchase, sale, or other method of transferring the subject of fulfillment. This subject of fulfillment is conditioned by a special permit for possession, or its origin or purpose is causally linked to the commission of a criminal offense. Simulated transfer can be executed only after meeting the material and procedural conditions specified by currently valid and effective generally binding legal regulations. (Marková, Strémy, Šanta and Janko 2021).

Modeled case.

On January 15, 2024, an unknown attacker fulfilled the characteristics of a criminal offense according to § 189 of the Penal Code, para. 1 and para. 4 letter b) by threatening to erase data from the critical infrastructure institution's database, over which he gained electronic factual control, demanding ransom in the form of crypto-assets, by sending 50 Bitcoins to the provided public address representing the crypto-asset wallet (hereinafter referred to as the "perpetrator's wallet") within one hour, causing damage of approximately USD 2 000 000. Among other actions, a simulated transfer was promptly implemented as one of the means of operational-tracking activities. After securely setting up a unique state crypto-asset wallet (hereinafter referred to as the "state wallet") and obtaining 50 Bitcoins into the possession of the state wallet, the authorized authority established the procedure for the simulated transfer. The construction of the transaction, where the initiator of the transaction would be the public address of the state wallet, the recipient the public address of the perpetrator's wallet, a sum of 50 valid and legitimately obtained Bitcoins, and transaction fees, i.e., rewards for nodes securing the confirmation of crypto-asset transactions at such a level that the transaction would be ranked in the mempool queue so that the crypto-asset transaction would not be confirmed and recorded in the list of all transactions immediately, but at the same time, it would not be removed from the mempool. Removing the transaction from the mempool could lead to a loss of information in the network, which the perpetrator could interpret as a failure to comply with his request and thus to the subsequent deletion of the critical infrastructure institution's data database. Confirmation and recording of the transaction in the list of all transactions would comply with the perpetrator's request, thereby not achieving the purpose of executing the simulated transfer. To determine the most ideal value of transaction fees, the mempool of all available nodes was analyzed, and a calculated presumable prediction was made. The next step was to create a second public address of the state wallet and construct an arbitrage transaction of crypto-assets, consisting of the initiator, which was the first public address of the state wallet, the recipient, which was the second public address of the state wallet, a sum of 50 Bitcoins, and transaction fees high enough so that after placing the arbitrage transaction into the mempool along with the original transaction, there would be a significant preference for confirming the arbitrage transaction. The actual execution of the simulated transfer consisted of sending the original crypto-asset transaction with optimized fees to the public address of the perpetrator's wallet, notifying the perpetrator of the construction of the crypto-asset transaction, and requesting access to the critical infrastructure institution's database. After notifying the perpetrator about the constructed transaction, crypto-asset related facts were monitored in the network, and it was found that the crypto-asset transaction was included in the mempool, which was enough to pursue the access to the ransomed data from the critical infrastructure institution's database. After analyzing this data, the data has been immediately backed up, followed by the immediate sending of the arbitrage crypto-asset transaction, which surpassed the original transaction in the mempool and was confirmed and recorded in the list of all transactions before the original transaction. Due to double-spending measures, the original transaction was rejected and removed from the mempool, resulting in gaining access to the ransomed data from the critical infrastructure institution and returning the 50 Bitcoins.

The terminology used in concurrence to study done by Ján Šanta and Ivan Šanta. (Šanta Ján and Šanta Ivo 2023).

Conclusion.

Reversing a fiat currency transaction is contingent upon necessary cooperation and collaboration with centralized entities that guarantee and secure the fiat financial system, given the centralized nature of the transaction process. Reversing such a transaction occurs by halting the flow of data, thereby interrupting the automated procedures resulting from the hardware-software interface used in initiating or further processing the transaction. The flow of data, which has left one centralized entity, where the software interface, such as internet banking, is often managed, does not possess the authority and technical capability to interrupt this flow of data and thus prevent the transaction from being executed. Up to this point, very close and very prompt cooperation with this entity is necessary, which is associated with performing a multitude of administrative and bureaucratic tasks. The likelihood of reversing a fiat currency transaction after its initiation and sending from the software interface of the initiating entity to the entity ensuring the verification and confirmation process of the transaction is highly improbable.

Reversing a crypto-asset transaction is contingent upon one's own knowledge and abilities, given the decentralized and transparent nature of the transaction process, whereby the transaction flow can be influenced until the transaction is recorded in the distributed transaction database, which is generally considered an irreversible moment and thus the final processing of the transaction. Up to this point, a crypto-asset transaction can be replaced by manipulating the fees designated for nodes responsible for recording the transaction in the distributed transaction database, i.e., the list of all confirmed crypto-asset transactions. By initiating a copy of the transaction early, where there is an interest in its replacement and therefore cancellation, while simultaneously increasing the fees for the mentioned nodes, there is a preference in the crypto asset-network, usually in the mempool, for the copy of the transaction, despite the fact that the original transaction with the same history was initiated, constructed, and verified earlier from a time perspective. The timeframe for possible manipulation of transactions depends on the determination of fees in the original transaction, whereby it holds that the smaller the fees for the mentioned nodes in the original transaction, the more time is needed for its final confirmation, which also creates more time for its reversal, but it also depends on the type of crypto-asset used, depending on the speed of the entire processing and confirmation process of the transaction of that crypto-asset.

These facts can be prophylactically utilized in the legitimate activities of authorized entities, as well as by any initiators of crypto-asset transactions who meet the conditions of asymmetric cryptography of the given crypto-asset system.

References:

Šanta Ján and Šanta Ivo. 2023. *Virtuálne meny - trestnoprávne a niektoré analyticko-ekonomické aspekty.* Prague: Leges.

Marková Veronika, Strémy Tomáš, Šanta Ján and Janko Sebastián. 2021. *Trestné právo procesné. Všeobecná časť*. Plzeň: Aleš Čeněk.

Šanta Ján and Šanta Ivo. 2023. K najaktuálnejšej počítačovej a inej kriminalite súvisiacej s virtuálnymi menami. *Justičná revue.* 75 (5): 636-650.

Šanta Ján and Šanta Ivo. 2022. Riziká investovania do virtuálnych mien z ekonomického a trestnoprávneho hľadiska. *Justičná revue*. 74 (3): 365-378.

Wang Kai, Tong Maike, Wu Changhao, Pang Jun, Chen Chen, Luo Xiapu and Han Weili. 2023. Exploring Unconfirmed Transactions for Effective Bitcoin Address Clustering. *Cryptography and Security (cs.CR).:* https://doi.org/10.48550/arXiv.2303.01012

Mikhaylov Alexey, Dincer Hasan, Yuksel Serhat, Pinter Gabor and Shaikh Ahmed Zaffar. 2023. Bitcoin mempool growth and trading volumes: Integrated approach based on QROF Multi-SWARA and aggregation operators. *Journal of Innovation & Knowledge.* 8 (3): https://doi.org/10.1016/j.jik.2023.100378

Rondelet Antoine and Kilbourn Quintus. 2023. Mempool Privacy: An Economic Perspective. *Cryptography and Security (cs.CR).:* https://doi.org/10.48550/arXiv.2307.10878

Florian Martin, Beaucamp Sophie, Henningsen Sebastian and Scheuermann Bjorn. 2019. Erasing Data from Blockchain Nodes. *IEEE Security & Privacy on the Blockchain (IEEE S&B):* https://doi.org/10.48550/arXiv.1904.08901