# Practical Analysis of Traceability Problem in Monero's Blockchain

Michal Kedziora[a] and Wojciech Wojtysiak
*Faculty of Computer Science and Management,*
*Wroclaw University of Science and Technology, Wroclaw, Poland*
*michal-kedziora.com/#contact*

Keywords: Blockchain, Cryptocurrency, Traceability, Monero.

Abstract: This paper presents an analysis of the cryptocurrency security based on the traceability problem in the Monero Blockchain. Researchers found a weakness in Monero transactions in the beginning of the network existence, where the real input could be deduced by the elimination. We decided to do further research on the newest data available after several Monero updates where introduced and implemented to evaluate, if this weakness is still available in the recent transactions. The analysis of the existing sizes of "Ring Signature" in transactions in subsequent versions of the Monero network has proven that the minimum required size for a given version is most often used, which can in some rare situation potentially lead to the creation of a user profile, and identifying transaction.

## 1 INTRODUCTION

Cryptocurrencies are becoming an increasingly popular method of electronic exchange of funds. They are based on a peer-to-peer system that, using cryptographic techniques. The basis of their operation is cryptographic evidence, which allows a transaction between two parties, without the participation of a trusted third party(Nakamoto, 2008). This approach prevents the cancellation of transactions and allows you to reduce the commission, which increases the safety of sellers, and deposit mechanisms can be introduced to protect buyers. Due to the many disadvantages and limitations of Bitcoin(Kedziora et al., 2019), such as the lack of appropriate technologies to ensure the privacy of cryptocurrencie, Monero has been proposed(Van Saberhagen, 2013)(Wijaya et al., 2016), which provides higher transaction security standards and meets two main features:

- Untraceability - For each transaction, the connection between the sender and the recipient can not be tracked.
- Unlinkability - You can not combine two transactions sent to the same recipient.

The first property in Bitcoin currency is not kept, because all transactions are publicly available in Blockchain blocks, and thus a connection between the parties to the transaction can be determined. The lack of the use of masking algorithms, thanks to the in-depth analysis of Blockchain can also lead to the connection of network users and their transactions, and hence the disclosure of many confidential information from publicly available data(Li et al., 2017)(Mell, 2018)(Maurer, 2016)(Biryukov and Pustogarov, 2015). In Monero, the above restrictions have been offset by the use of several mechanisms. The sender's identity is protected by the addition of additional false source addresses, and thanks to a one-off public key for each "output", a unique address is created, and the real one is unavailable to the public in Blockchain. In spite of this, for transactions dated before the introduction of many network improvements in 2017, research has shown that a significant portion of them can be traced(Noether, 2014)(Noether and Noether, 2014).

The aim of the paper is to analyse in practice the mechanisms implemented in the Monero system to ensure the security and anonymity of transactions is confirmed, and there is no possibility to conduct analysis on transaction data sets exported from Blockchain for current time intervals to examine the possibility of merging transactions with their real inputs.

### 1.1 Monero's Blockchain

Monero is one of the most valuable privacy-oriented cryptocurrencies. It was presented in November

[a] https://orcid.org/0000-0002-7764-1303

Kedziora, M. and Wojtysiak, W.
Practical Analysis of Traceability Problem in Monero's Blockchain.
DOI: 10.5220/0009325802610268
In *Proceedings of the 15th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2020)*, pages 261-268
ISBN: 978-989-758-421-3

2013 in a document describing the 'CryptoNote v 2.0' technology by Nicolas van Saberhagen, and the first implementation is dated September 12, 2014. The Monero network is updated usually every six months(Noether et al., 2014). Since the first implementation, 8 major updates have been created, each time introducing a series of changes that increase the level of security and comfort of using cryptocurrencies(Alonso, 2018).

The ring signature technology in Monero is used to protect the privacy of the sending transaction. It is a kind of electronic signature in which a group of potential transaction participants is combined to create a unique transaction authorization(Courtois, 2016). The right signer, or ”one-time key”, associated with the ”output” of the transaction, and the others - acquired from past transactions recorded in Blockchain, are equal and impossible to identify. Together, they form a list of ”inputs” of transactions, of which only one is appropriate. This allows masking the origin of the transmitted cryptocurrency. To eliminate the possibility of double release, ”Key image” was used. It is a cryptographic security key, which is part of every transaction signed ”Ring Signature”. Each ”output” transaction has only one ”Key image”, and their list is stored in Blockchain, so that anyone who extracts the currency can verify that no resulting transactions have been doubled. Monero users have a pair of public keys as public address(Mercer, 2016). Adress is based on Diffie-Hellman exchange created before each transaction made by user. The one-time keys for the output are:

$$K_0 = H_n(rK_{B_1})G + k_{B_2}G = (H_n(rK_{B_1}) + k_{B_2})G \quad (1)$$

$$k_0 = H_n(rK_{B_1}) + k_{B_2} \quad (2)$$

where r is random number such that 1 < r < N, and public key is $K_0 = H_n(rK_{B_1})G + k_{B_2}$. The rG value is used to calculate a Diffie-Hellman like shared secret. Then $k_{B_1}rG = rK_{B_1}$ is calculated. A private key $k_{B_1}$ is called also the view key, as it allows to verify if an output is valid and properly addressed(Alonso, 2018).

The operating principle looks as follows, if user X wants to send Monero to user Y, with the size of the ring six, one of the ”inputs” will be taken from the X wallet and placed in the ring, and the rest of the past transactions saved in Blockchain. Together they form a group of six potential signers, and from outside it will not be possible to determine which ”input” is the right one signed by ”One time key” from user X, and thanks to the verification of ”Key image”, the Monero network will be able to confirm that sent to Y, they were not issued before. RingCT, is an algorithm by which the value of each ”output” is encrypted and saved in the transaction. Only the recipient can decode the value. Encryption is done by the sender using the private transaction key. This information is provided in the ”ecdhInfo” section. The private transaction key is created by combining the private ”view key” of the recipient and the public transaction key.

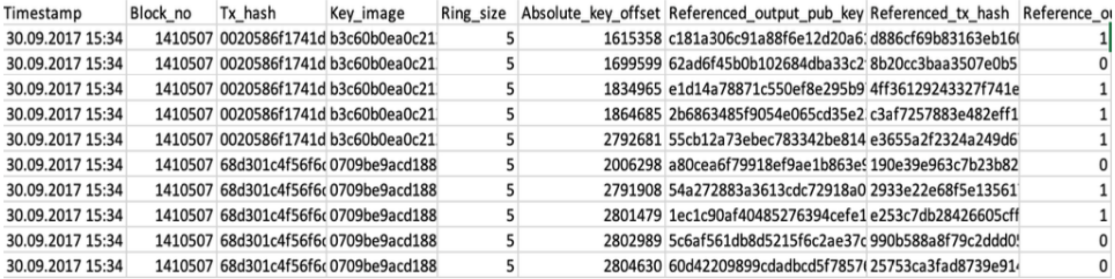
## 1.2 Related Work

As presented in the research paper ”An Empirical Analysis of Tracebility in the Monero Blockchain”, Authors: Malte Möser, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Shashvat Srivastava, Kyle Hogan, Jason Hennessey, Andrew Miller, Arvind Narayanan and Nicolas Christin, the Monero software allows you to configure users with many variables(Moser et al., 2018). At the beginning of the existence of Monero, it was not determined what is the minimum number of additional ”outputs” required, called ”mixins”. According to research, about 64% of transactions did not have them at all, they are 0-mixin transactions. The reason for this behavior could have been lower fees for transactions due to its size. This creates a problem not only for these operations, but also for future ones that will use them, because the ”output” X, which is the only one in transaction A, and for example one of two (X and Y) in transaction B, makes it unambiguously we can determine that Y is the correct ”output” for transaction B.

The above-mentioned research focused on several periods related to network updates in terms of the policy of adding ”mixins” to the transaction and analyzed the data from Blockchain to block 1288774, until April 15, 2017:

- before January 1, 2016: ”mixins” selected evenly, all had to have the same value, older ones selected more often than new ones,
- after January 1, 2016, version 0.9.0: the minimum number of ”mixins” is two, and favoring newer ones,
- after September 19, 2016, version 0.10.0: Introduction of the ”CT Ring”, which was finally available from January 10, 2017,
- after December 13, 2016, version 0.10.1: matching ”mixins”, min. 25% of the last 5 days.

To conduct the research, an iterative algorithm was used, which in each operation on a set of transaction data retrieved from Blockchain, selects all ”mixins” which can not be the correct ”output” because they were issued earlier(Kumar et al., 2017). The results show that in the first version of Monero, for the transaction ”0-mixins”, about 89% of the relevant ”inputs”



| Timestamp | Block_no | Tx_hash | Key_image | Ring_size | Absolute_key_offset | Referenced_output_pub_key | Referenced_tx_hash | Reference_o |
|---|---|---|---|---|---|---|---|---|
| 30.09.2017 15:34 | 1410507 | 0020586f1741d | b3c60b0ea0c21 | 5 | 1615358 | c181a306c91a88f6e12d20a6 | d886cf69b83163eb16 | 1 |
| 30.09.2017 15:34 | 1410507 | 0020586f1741d | b3c60b0ea0c21 | 5 | 1699599 | 62ad6f45b0b102684dba33c2 | 8b20cc3baa3507e0b5 | 0 |
| 30.09.2017 15:34 | 1410507 | 0020586f1741d | b3c60b0ea0c21 | 5 | 1834965 | e1d14a78871c550ef8e295b9 | 4ff36129243327f741e | 1 |
| 30.09.2017 15:34 | 1410507 | 0020586f1741d | b3c60b0ea0c21 | 5 | 1864685 | 2b6863485f9054e065cd35e2 | c3af7257883e482eff1 | 1 |
| 30.09.2017 15:34 | 1410507 | 0020586f1741d | b3c60b0ea0c21 | 5 | 2792681 | 55cb12a73ebec783342be814 | e3655a2f2324a249d6 | 1 |
| 30.09.2017 15:34 | 1410507 | 68d301c4f56f6 | 0709be9acd188 | 5 | 2006298 | a80cea6f79918ef9ae1b863e | 190e39e963c7b23b82 | 0 |
| 30.09.2017 15:34 | 1410507 | 68d301c4f56f6 | 0709be9acd188 | 5 | 2791908 | 54a272883a3613cdc72918a0 | 2933e22e68f5e13561 | 1 |
| 30.09.2017 15:34 | 1410507 | 68d301c4f56f6 | 0709be9acd188 | 5 | 2801479 | 1ec1c90af40485276394cefe1 | e253c7db28426605cff | 1 |
| 30.09.2017 15:34 | 1410507 | 68d301c4f56f6 | 0709be9acd188 | 5 | 2802989 | 5c6af561db8d5215f6c2ae37c | 990b588a8f79c2ddd0 | 0 |
| 30.09.2017 15:34 | 1410507 | 68d301c4f56f6 | 0709be9acd188 | 5 | 2804630 | 60d42209899cdadbcd5f7857 | 25753ca3fad8739e91 | 0 |

Figure 1: An Exemplary Structure of the Exported Transaction History from Monero Blockchain.

could have been identified, for all 2 053 328 transactions, about 77%. In version 0.9.0, where the minimum number was two, for "2-mixins", about 64%, for all, 3 156 248, about 62%. Between version 0.10.1 and April 15 2017, about 42% for "2-mixins" and about 40% for 1 046 028 transactions. It can also be concluded that in addition to the first version, "2- mixins" was the most commonly used, i.e. the smallest value required, and the least often between seven and nine. After September 16, 2017, the Monero version 0.11.0.0, the next network update took place on April 6, 2018. Version 0.12.0.0 introduced some interesting upgrades. The minimum ring signature size has been increased from five to seven, the Proof-of-Work algorithm has also been changed to prevent DoS attacks by ASICs and added sorting. On October 18, 2018, version 0.13.0.0 was released. Updated PoW algorithm to CNv2. 'Bulletproofs' was enabled to reduce the size of the transaction and the size of the ring signature was set to eleven globally, the maximum transaction size was set to half the size of the block(Wijaya et al., 2018).

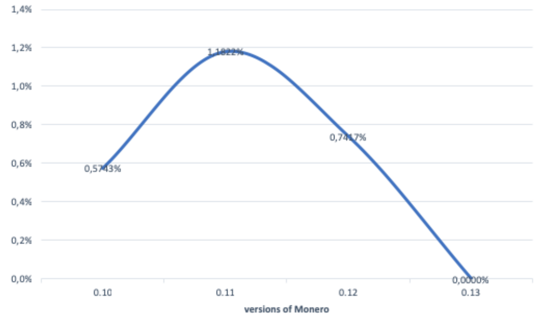


Figure 2: Percentage of Traceable "inputs" According to the Monero Network Version.

The use of three main technologies in Monero providing privacy: addresses "stealth", "Ring Signature" and "RingCT", resulted in an increase in the size of the transaction and Blockchain itself. This limited the possibility of increasing the minimum amount of mixins, because the "Range proof" algorithm significantly increased the transaction size and its fee. In response to this from the beginning of 2018, the "Bulletproofs" technology was started, which was finally implemented in version 0.13.0.0 on October 18, 2018. In contrast to the "Range proofs" algorithm, where the number of operations increases linearly to the number of "outputs" and bits within reach, the "Bulletproofs" grows only logarithmically. This allows two types of applications: "single output" and "multiple output". Thanks to the implementation of this technology, the transaction fee decreased, and the size of the sample transaction was reduced by approximately 80%. The average transaction fee in January 2018 was even 13.5 $. During the year, it decreased due to the decline in cryptocurrency prices and a smaller number of trade-oriented transactions to the level of 0.5 $ - 1.0 $. After the introduction of the "Bulletproofs" technology, the fee fell from the level of 0.6 $ to 0.02 $, which is a very large improvement of the transaction and the cryptocurrency itself. This allowed to set the minimum number of "mixins" to eleven, which makes it impossible to track transactions based on "inputs". This will be presented later in the paper.

## 2 MONERO BLOCKCHAIN ANALYSIS

Conducting the experiment required three main steps. The first was to install the Monero wallet and synchronize with the network to download the local Blockchain node. The next step was to use the transaction export tool to export the transaction history for different periods from the local Blockchain database. Finally, it was necessary to use a cloud computing in order to implement the iterative algorithm and generate results. The wallet has been synchronized in the Linux system, because the tools used to export data from Blockchain are dedicated to this system. In the background, the "Daemon" Monero worked, which was supposed to synchronize with the network and scan whether our system is intended for transactions and enable sending them. Blockchain Monero is stored locally in the LMDB database in the data.mdb file. The LMDB database is a transactional database in the form of a key - value, offering very high efficiency both in terms of speed and space. It is recommended to use SSDs for synchronizing the local node, because the data structure even for fast HDDs is very difficult, and thus synchronization can take up to several days.

The transaction export tool which was available on the GitHub platform by Martin Matak was used to export the history of the transaction from Blockchain. It allows you to export to a csv file, transaction details stored in Blockchain. After compilation and showing the path to our Monero together with the local Blockchain node, we can run the program for one of the selected parameters. For the experiment, the option to export all ”key images” with associated public keys ”outputs” was used, starting with the specified block. The generated csv file consists of nine columns: timestamp, block number, transaction hash address, key image, ring size, key offset, key public associated with ”key image”, address of hash transaction associated with public the ”output” key, which is also one of the ”stealth” addresses of this transaction. On the xmrchain.net portal you can verify the received export. For each block number, it is possible to display transaction details and the associated ”Key image” together with the ”Ring Signature” participants. You can read information about the block number, confirmation number, transaction size, fee, exact date and ”stealth” addresses.

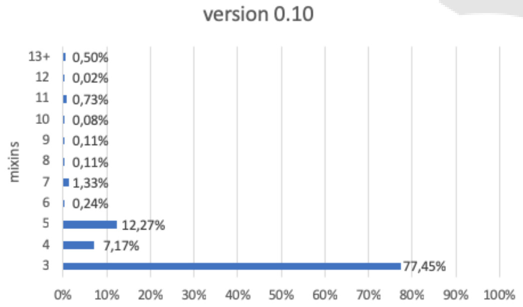


Figure 3: Percentage of the Use of a given Number of ”mixins” in Transactions, 15/04 - 3/05/2017.

The first step is to export test data from Blockchain to be able to load it into a cluster. In order to implement the algorithm on a large number of data, the Google platform was used. It is a cloud service that offers many interesting solutions, including Google App Engine, Google Cloud Storage, Google Cloud SQL, Google Cloud Compute, Google Big Query. For the purpose of the research, Google Cloud Storage was used to store selected exports and instances of Google Cloud Compute virtual machines as computing power. Three machine instances were used for the calculations, the main one with four processors and 15 GB of virtual memory, and two with one processor and 3.75 GB of virtual memory. Then, the data had to be sent to the server, the project was built locally and a calculation command sent to the virtual machines. After correctly performed iterations, we get a percentage result of the possible ”merged” transactions in a given set of data.

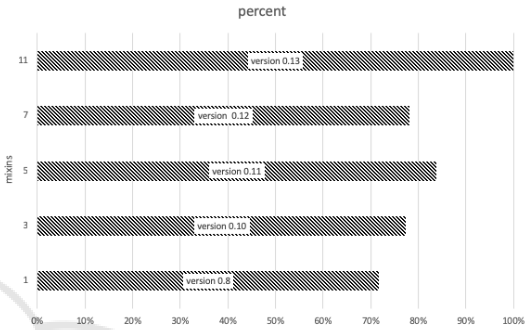


Figure 4: The Most Popular Sizes of ”Ring Signature” Depending on the Version of the Monero Network.

Transaction histories stored in Blockchain occupy a lot of space, and their export and the iterative algorithm executed on them requires significant computing resources and fast SSDs, therefore the test data has been divided into relevant parts related to changes in the Monero network. The initial interval is April 15, 2017, until May 30, 2017, the first not covered by research in the previously presented research work, to verify the impact of subsequent network updates on the ability to track transactions based on the elimination of their ”inputs” in historical operations.

Next, data samples were exported for selected months of 2017, and for March 2018, one month before the update to version 0.12.0.0, where the minimum size of the ring was set to seven. After the update, selected weeks from April 2018. From May 3, 2018 to July 23, 2018, and from August 30, 2018 to October 12, 2018, before the update 0.13.0.0 of October 19, 2018 introducing technology reducing the transaction size, and thus its payment: ”Bulletproofs”, and increasing the required ring size to eleven. The last ranges are data from October 20, 2018 to December 7, 2018, that is transactions were carried out on the latest version of the network. In order to verify the obtained results, a trial simulation was also carried out for data from the period from June 23, 2015 to July 13, 2015.

Table 1: The Obtained Results of the Iterative Algorithm for Selected Time Intervals.

| Time interval | Key images | Inputs | % |
|---|---|---|---|
| 23.06 - 13.07.2015 | 204 103 | 156 950 | 76,8974% |
| 15.04 - 30.05.2017 | 437 229 | 2132 | 0,4876% |
| 30.05 - 09.06 2017 | 135 852 | 683 | 0,5028% |
| 30.06 - 11.07.2017 | 117 650 | 689 | 0,5856% |
| 11.07 - 20.07.2017 | 86 758 | 961 | 1,1077% |
| 15.10 - 01.11.2017 | 146 026 | 2649 | 1,8141% |
| 07.11 - 13.11.2017 | 106 172 | 868 | 0,8175% |
| 11.12 - 22.12.2017 | 197 022 | 2748 | 1,3948% |
| 01.03 - 29.03.2018 | 228 186 | 1743 | 0,7639% |
| 03.05 - 23.07.2018 | 821 380 | 7155 | 0,8711% |
| 30.08 - 12.10.2018 | 425 962 | 2096 | 0,4921% |
| 20.10 - 14.11.2018 | 472 666 | 0 | 0,0000% |
| 14.11 - 07.12.2018 | 279 707 | 0 | 0,0000% |

## 2.1 Experiment Results

After completing the iterative algorithm on virtual machines, the following results were obtained: In the Table 1, in order to verify the results obtained, data from 2015 was presented. For this data sample, the number of transactions ”0-mixins” was as much as 71.8%, which is the main reason that as much as 76.9% ”inputs” it could be combined with the right transaction.

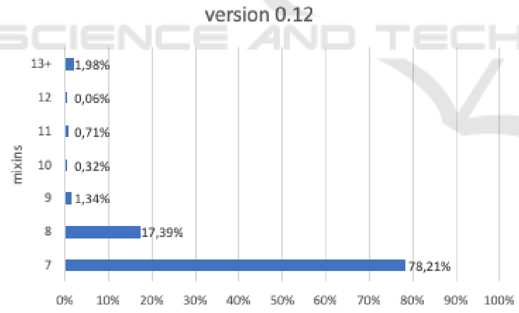


Figure 5: Percentage of the Use of a given Number of ”mixins” in Transactions, 03/05 - 14/05/2018.

The data show the time intervals for which the algorithm was performed. The number of all ”Key images” for transactions from a given period of time. The number of possible ”inputs” and their percentage. Current data from April 15, 2017, which focused on research shows that with subsequent updates and changes to the network and the increasing number of transactions with new settings, the ability to combine the relevant ”inputs” has decreased to an acceptable and safe level for transactions, which was presented in the Figure 4.

The chart shows that for transactions from April 15, 2017 to July 20, 2017, you could combine from 0.49% to 1.11% ”inputs”. This is the time when the minimum ”Rign Signature” size was three, and normal transactions were allowed and the encrypted RingCT value. Due to a significant reduction in the share of ”inputs” in the 0-mixin transaction from the beginning of Monero existence, a maximum of only 1.11% of transactions may be at risk. Transactions from October 15, 2017 to March 29, 2018 were made on the Monero version 0.11 network, which increased the size of ”Ring Signature” to five and introduced the ”RingCT” transaction requirement. This solution requires that all ”inputs” also come from ”RingCT”. This could affect the fluctuation from 1.11% to 1.81%, which is the highest value observed during the tests. Then the percentage falls and oscillates between 0.82% and 1.39%, at the end of the period it reaches 0.76%. Version 0.12 introduced the sorting ”inputs” and set the minimum number of ”mixins” to seven. A downward trend is observed from 0.87% to 0.49%. Along with October 19, 2018 and the current version of 0.13 of the Monero network, the ”Bulletproofs” technology was implemented, reducing the volume of transactions, which allowed to determine the number of ”mixins” at eleven, without the increase of transaction fees. As results from the conducted research, it is impossible to combine potential ”inputs” with current transactions performed after updating the network to version 0.13. The results obtained prove that from October 19, 2018, the problem of potentially traceable ”inputs” of the transaction has been eliminated and transactions in Monero’s cryptoval question can be considered anonymous and secure. The chart in Figure 2 presents a summary of results according to the year of collected data. Both in the range from 2017 and 2018,

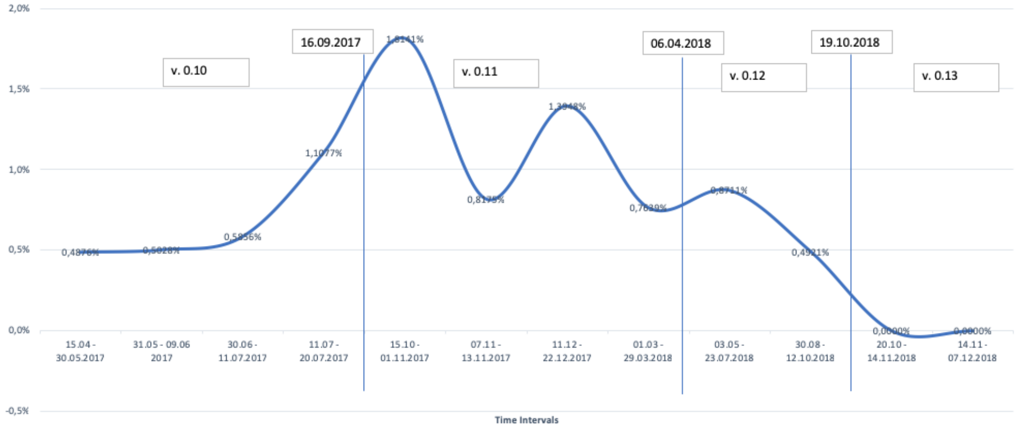


Figure 6: Percentage of Traced ’inputs’ in the Time Periods.

the possibility of combining ”inputs” with the transaction is less than 1%. For the data collected from 2018, the result is only 0.49%, compared to 0.87% from the previous year. It is mainly influenced by the Monero network upgrade from October 19, 2018, solving the problem under investigation.

Analyzing the obtained results according to the Monero network version, please note that version 0.10 introduced the possibility of using the ”RingCT” transaction, which requires that the size of ”RingSignature” be greater than 1. As shown in the research paper ”A Traceability Analysis of Monero’s Blockchain,” Amrit Kumar, Clement Fischer, Shruti Tople, and Prateek Saxena, already after about a month from the introduction of this version, almost 90% of transactions took place using this technology. This has the main impact on the decrease in traceable ”inputs” to the level of 0.57%. Subsequent versions of the network introduced the obligation to use the ”RingCT” technology, and increased the size of the ”Ring Signature” to levels five and seven. Percentage of traceable inputs depending on Monero version can be see in Figure 1.

The research shows that implementing version 0.11 did not eliminate the completely analyzed problem, there was still the possibility of connection between 1.18% in version 0.11 and 0.74% of ”inputs” in version 0.12. The results for version 0.13 were breakthrough, in which for the collected data, it is not possible to combine the ”inputs” with the transaction

## 2.2 Ring Signature Size Analysis

By exporting transaction details from Blockchain Monero for selected time periods, subsequent versions of the network, it was possible to analyze the number of ”mixins” used by users in transactions. Network updates introduced restrictions on the minimum number of ”mixins”, which is visible in the results obtained. The Figure 2 shows that 77.45% of transactions took place with the size of ”Ring Signature” set to three. Then ”Ring Signature” size five and four were used. It is worth noting that six transactions had a ring size value of more than a thousand, and one transaction for four thousand five hundred one.

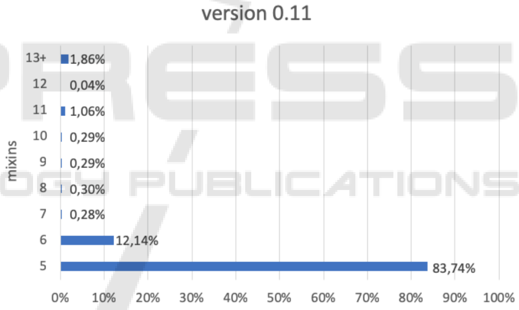


Figure 7: Percentage of the Use of the given Number of ”mixins” in Transactions, 15/10 - 01/11/2017.

For the data from version 0.11, similarly to the previous results, the minimum required value for this version was used, that is five, 84.74% of all transactions. The largest size of the ring was one hundred, used in two transactions.

The results from May 3, 2018 to May 14, 2018 show that 78.21% of the transactions were set to ”mixins” at level seven. The highest set value was nine hundred and ninety-nine in one transaction.

After the introduction of the ”Bulletproofs” technology, the ”Ring Signature” size was standardized for transactions up to eleven. The results obtained confirm that all transactions from November 14, 2018 to November 22, 2018, have a fixed value and no anomalies occur. On the Figure 3, in order to compare the distribution of occurrence of ”mixins” in transactions with current data, situations from the time in-

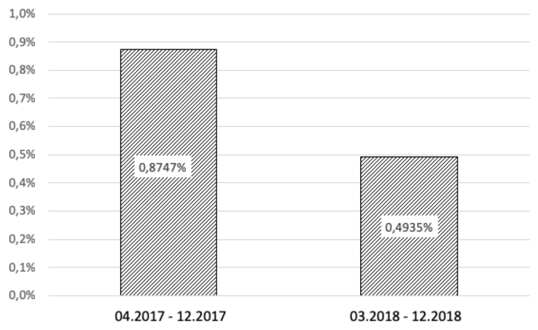


Figure 8: Percentage of Traceable "inputs" Acc. Years.

terval from June 23 to July 13, 2015 were presented, in which there were no restrictions as to the minimum number. It follows that almost 72% of transactions took place without the participation of "mixins", which in principle makes it possible to trace them. This state of affairs was dictated by the desire to reduce transaction fees. It was unacceptable because the transactions in Monero should be anonymous in principle. As can be seen in the Figure 5, the largest percentage of transactions is with the minimum number of "mixins" for a given version of the Monero network. It can be deduced from this that users used standard settings and were afraid of higher fees, as the increase in the number of "mixins" increases the size of the transaction and increases the fee.

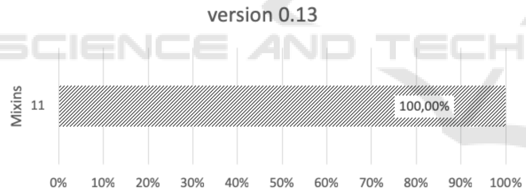


Figure 9: Percentage of the Use of a given Number of "mixins" in Transactions, November 14 - November 22, 2018.

Version 0.13 introduced the unification of the number of "mixins" for transactions up to eleven. The conducted research confirmed this implementation (see Figure 6). There are currently no transactions with different sizes of "Ring Signature". Thanks to this, individual transactions with a very large number of "mixins" are not observed, as in older versions, e.g. four thousand five hundred one in version 0.10, which cause a high load for the block and require a lot of time to be confirmed by the network. There are also no transactions with a minimum number of "mixins", which resulted in lower security and traceability.

# 3 CONCLUSIONS

The presented work analyzes the security of Monero Blockchain on the basis of the possibility of combining the appropriate input transactions and examined how the share of a particular number of "mixins" in the transactions is distributed. The main assumptions of Monero cryptocurrencies were described and the principle of operation of implemented technologies aimed at ensuring security and privacy of transactions was presented. The results of available research on the possibilities of combining "inputs" of transactions, based on the analysis of data recorded in Blockchain, where presented. An analysis of the share of a particular number of mixins in transactions was also conducted. In order to verify the changes introduced thanks to subsequent updates and checking whether currently transactions in Monero are free from the problem of combining "inputs" based on the analysis of transaction history, studies have been carried out that between April 15, 2017 and October 12, 2018, it was tracked between 0.49% and 1.81% of "inputs" in the transaction. It follows that the initial problems caused by the large share of the "0-mixins" transaction were offset by subsequent updates and the minimum size requirements of the "Ring Signature". Summing up, after the latest network update, research has shown that you can not combine "inputs" with transactions, i.e. the problem is resolved and Monero transactions can be considered safe and impossible to track down using this issue. The analysis of the existing sizes of "Ring Signature" in transactions in subsequent versions of the Monero network has proven that the minimum required size for a given version is most often used, and individual transactions with rare values, can potentially lead to the creation of a user profile, and this means identifying his transaction, e.g. based on the time it was made. The conducted analysis showed that the latest update unified the size of the "Ring Signature".

# ACKNOWLEDGEMENTS

This work was partially supported by the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No. 691152 (RENOIR) and the Polish Ministry of Science and Higher Education fund for supporting internationally co-financed projects in 2016-2019 (agreement no. 3628/H2020/2016/2).

## REFERENCES

Alonso, K. M. (2018). Monero-privacy in the blockchain. Universitat Oberta de Catalunya.

Biryukov, A. and Pustogarov, I. (2015). Bitcoin over tor isn't a good idea. In *2015 IEEE Symposium on Security and Privacy*. IEEE.

Courtois, N. T. (2016). Stealth address, ring signatures, monero. University College London, UK.

Kedziora, M., Kozlowski, P., Szczepanik, M., and Jozwiak, P. (2019). Analysis of blockchain selfish mining attacks. In *International Conference on Information Systems Architecture and Technology*, pages 231–240. Springer.

Kumar, A. et al. (2017). A traceability analysis of monero's blockchain. In *European Symposium on Research in Computer Security. , Cham*.

Li, X. et al. (2017). *A survey on the security of blockchain systems*. Future Generation Computer Systems.

Maurer, F. K. (2016). A survey on approaches to anonymity in bitcoin and other cryptocurrencies. *Informatik*, 2016.

Mell, P. (2018). Managed blockchain based cryptocurrencies with consensus enforced rules and transparency. In *the IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE*, volume 2018, page 17.

Mercer, R. (2016). Privacy on the blockchain: Unique ring signatures. preprint, arXiv.

Moser, M. et al. (2018). An empirical analysis of traceability in the monero blockchain. *Proceedings on Privacy Enhancing Technologies*, 2018(3):143–163.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. www.cryptovest.co.uk.

Noether, S. (2014). *Review of CryptoNote white paper*. HYPERLINK" cc/downloads/whitepaper_review. pdf".

Noether, S. and Noether, S. (2014). Monero is not that mysterious. Technical report, Monero Research Lab.

Noether, S., Noether, S., and Mackenzie, A. (2014). A note on chain reactions in traceability in cryptonote 2.0. *Research Bulletin MRL-000*, 1:1–8.

Van Saberhagen, N. (2013). Cryptonote v 2.0. Whitepaper.

Wijaya, D. A. et al. (2016). Anonymizing bitcoin transaction. In *International Conference on Information Security Practice and Experience. , Cham*.

Wijaya, D. A. et al. (2018). Monero ring attack: Recreating zero mixin transaction effect. In *IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE*, volume 2018, page 17.