Anonymization of Transactions in Distributed Ledger Technologies

Robert Werner, Sebastian Lawrenz, Andreas Rausch
Clausthal University of Technology, Institute for Software and Systems Engineering
Arnold-Sommerfeldstraße 1
Clausthal-Zellerfeld, Germany
email: { robert.werner | sebastian.lawrenz | andreas.rausch}@tu-clausthal.de

Abstract—**Increasing acceptance of transparent cryptocurrencies is leading to more and more publicly traceable financial transactions. This is a problem for civil society due to a lack of privacy, as well as for companies because of public financial data. It could even endanger entire states due to a transparent economy. To solve this problem, private, decentralized currencies have been created, but these prevent prosecution and thus undermine the accountability of citizens. In this paper, existing centralized techniques for ensuring privacy in distributed ledger technologies are presented and evaluated. On this basis, a software is presented which, through its semi-decentralized architecture, guarantees privacy for citizens and the economy when transacting on distributed ledger technologies without preventing state prosecution.**

Keywords—Distributed Ledger; Blockchain; Privacy; Blockchainanalysis; Cryptocurrency

I. INTRODUCTION

The idea of cryptocurrencies was introduced by the pseudonym Satoshi Nakamoto in 2008 with the Bitcoin Whitepaper [1]. Since then, cryptocurrencies have become increasingly popular, and both the transaction volume [2] on the Bitcoin blockchain and the trading volume [3] of Bitcoin has increased almost steadily. Besides, many new cryptocurrencies - so-called "altcoins" (alternative coins) - have been created and further developed, which also enjoy increasing usage and forming a new kind of a (software) ecosystem. Just like a natural ecosystem, a software ecosystem describes the relation and balance between organisms and their environment. The Bitcoin ecosystem for example is characterized by the blockchain itself, miners, the market, developers, and applications running on top of Bitcoin. The bitcoin price is influenced by this ecosystem, the market supply, and demand, as well as other external conditions, such as the dollar price [4] . In line with this is the definition of a software ecosystem, which is defined as the interaction of a set of actors on top of a common technological platform that results in several software solutions or services [5].

The usage of cryptocurrencies has also increased rapidly in the Darknet and has reached a new peak in 2019 with a monthly transaction volume of 8-14 million USD in bitcoin (BTC). Overall, illegal transaction volumes in 2019 accounted for approximately 1.1% of all transparent cryptocurrencies [6]. Furthermore, the blockchain hype that occurred in 2017 has also spread to governments and commercial companies. For example, the EU envisages great potential for the blockchain with international financial institutions and supply chains [7]. The blockchain for securing digital identity is seen as another great potential of this technology [8]. Facebook has also set itself the goal of launching a global currency based on the blockchain [9]. From the Bitcoin hype onward, many new cryptocurrencies and innovations in the area of blockchain have come forth and the ecosystem of cryptocurrencies is in continual change and adapting to new user requirements.

In the early years of cryptocurrencies in particular it was assumed that transactions on the blockchain are anonymous since people neither have to register nor have to enter a real name before transacting. As a matter of fact, it has been shown that the blockchain provides a good basis to break the supposed anonymity through data analysis. This results in observers being able to infer from people to their activities or inversely from activities to the participating people with little information from outside of the blockchain. With cryptocurrencies, transparency in our digital world reaches a new level. Financial data is one of the most sensitive pieces of information as it allows conclusions to be drawn about the whereabouts of people, their social environment, buying habits, state of health, and much more. In addition, many users are unaware of the public accessibility of this data. Due to the pseudonymity of many cryptocurrencies, users are often lulled into a false sense of security.

Further far-reaching cuts in the private sphere could severely endanger the basic human right to the free development of one's personality, and thus also the people themselves. The public availability of financial data can not only be threatening for the individual, but also poses a problem for companies as it would be possible for competitors to find out about their revenue, origin of revenue, and partnerships. Likewise, states cannot have any interest in making their own economy and national budget publicly available to the world and thus do the work of hostile intelligence services.

On the other hand, online crime is posing a challenge and is aggravated by new decentralized cryptocurrencies with a focus on privacy. These so-called "privacy coins" conceal transactions and prevent the investigation of crimes financed by such money. The German Federal Ministry of Finance sees privacy coins like Monero as "particularly susceptible to money laundering" and is concerned about "increasing acceptance in the darknet", although they allegedly do not pose a real threat yet [10].

New cryptocurrencies and technologies have emerged not only with a focus on privacy but also with an emphasis on scalability. Networks based on Directed Acyclic Graph (DAG) ledgers promise to scale far beyond bitcoin's limit of seven transactions per second [11] by adding transactions asynchronously to the ledger.

What is needed is an efficient payment system that works reliably, offers users privacy, but still enables state authorities to bring criminals to justice by analyzing their financial flows. At the same time, it must be prevented that this system can be abused, even by the operator herself.

A. Objective

The aim of this paper is to find a balance between anonymization and the preservation of law enforcement. Therefor, concepts for anonymization in decentralized and censorship-resistant Distributed Ledger Technologies (DLT) that safeguard criminal prosecution will be evaluated. As part of this, a semi-decentralized anonymization tool for a transparent DAG-based cryptocurrency is proposed. The goal is to provide users of this cryptocurrency with optional privacy via a second layer without obstructing law enforcement. Furthermore, we present a concept of how our tool can be integrated into the modern constitutional state and how it can be protected against abuse.

B. Outline

The rest of the paper is structured as follows: Section II presents relevant fundamentals, context, and related work. In Section III we present our software by outlining its requirements, introducing the concept, and giving implementation details. In Section IV we evaluate the limitations of our solution and propose further enhancements to combat these. Finally, we conclude the paper in Section V.

II. Background and Related Work

In the following section, the basics of different DLTs are discussed and blockchain analysis of transparent cryptocurrencies is introduced. Decentralization and centralization in the context of privacy are discussed and general attacks for deanonymizing transactions in DLTs are described. Furthermore, we present related projects.

A. Distributed Ledger Technologies

DLT is a technique for managing a decentralized transaction database. This database is stored redundantly by any number of equal participants. Each participant has the same copy of the transaction database, which is continuously synchronized peer-to-peer with all participants. The most prominent DLT is the blockchain technology, which can be implemented in different ways. Some newer DLTs use a DAG, and can also be implemented in different ways. In this paper, the focus of DAGs is on the implementation of the "block-lattice", which was introduced by the cryptocurrency "Nano" [12].

B. Block-Lattice vs Blockchain

In contrast to the traditional blockchain, on the DAG-based block-lattice, there is no single blockchain synchronized by all network participants to which new blocks, and thus transactions, are sequentially added by, e.g., miners. Instead, every user exclusively manages her own account-chain, to which only that same user may attach new blocks.

The account balance is stored in stateful blocks. This is in contrast to most blockchain-based cryptocurrencies (including Bitcoin [1] and Ethereum [13]), where the state of an account is not stored on the ledger itself, but has to be derived from it. To find out the balance of an account in Nano, only the last block of this account ("frontier", or "head block") must be considered. In the future, this feature could allow nodes to store only the frontiers by "pruning" the ledger, thus drastically reducing the size of the ledger since the transaction history is no longer being stored.

Unlike the blockchain, a block in the block-lattice contains only one transaction, thus only one state update for one account. Since only the account owner is allowed to attach blocks to her account and can thereby update the account state, the account owner has to create a block for each outgoing and incoming transaction to update her balance. Consequently, there are two basic actions that the blocks can represent: Send and receive. Each fully completed transaction consists of two blocks [12].

C. Blockchain Analysis

The first intrinsic contribution to privacy in DLTs lies in the pseudonymity of addresses. A pseudonym is an alias that by itself does not allow conclusions to be drawn about the actual person or entity behind it, but is nevertheless closely connected to it. In contrast to anonymity, i.e., complete namelessness, actions can be assigned to a pseudonym and vice versa. In the case of cryptocurrencies, addresses serve as pseudonyms for a user. Pseudonyms are tied to the user since only the user has access to the coins stored on these addresses. These addresses are automatically generated when a wallet is created. Their pseudonymity is broken as soon as a user receives money from someone or sends money to someone who knows their true identity. This is the case, for example, when a person receives coins from a friend or service with Know Your Customer (KYC) compliance or sends money to a friend, exchange, or online shop.

So far, the identity can only be linked to an address by those involved. However, it is even possible for third parties to obtain this information. This is because DLTs' transactions contain not only the sender and receiver addresses but also the value and time of the transaction. If, for example, a customer pays in a shop with a cryptocurrency, the customer automatically knows the address of the shop. If the customer now wants to find out the address of the person who stood in line after her, all the customer has to do is look at the ledger and check the incoming transaction after her own in the transaction history of the address of the shop. The address of the other customer is then displayed there as the transaction origin. This shows how easy it is, even for private individuals, to break peoples' pseudonymity as a third party. For states, interested companies, or consortia that can benefit from such information and have more data and resources available, this should pose a little hurdle.

Nakamoto,[1] has already known that a global currency needs privacy and has made some suggestions for improving it beyond pseudonymity. One of these suggestions is the use of multiple addresses per person. This way the wallet generates a new receiving address each time coins are requested. Multiple addresses make the scenario described in the previous paragraph much more difficult because the store would generate a new receiving address for each customer, who then would not easily be able to find other customers' addresses.

At first glance, this measure of using multiple addresses per user appears to be very powerful at protecting against prying eyes, but in reality, is far less effective. If funds are spread across multiple addresses and the balance of one is no longer sufficient, a transaction that combines these funds must take place. Consequently, tools exist that are able to find multiple addresses belonging to the same user and other addresses the user has interacted with [14].

D. *Decentralization*

An important aspect of evaluating DLTs is the degree of decentralization. Decentralization is not a binary state but can be classified on a spectrum from centralized to decentralized in different areas. By definition, all DLTs can be considered "decentralized" because the ledger is stored on several computers. This ensures greater accessibility and reliability compared to centralized alternatives and more resistance to technical failure and DoS attacks against individual actors.

However, decentralization is not only applicable to the way transactions are stored, but also to the creation or authorization of transactions, i.e., the consensus. This is important because a monetary system with guaranteed availability cannot be considered decentralized if only one single party decides which transactions are permitted and which are not. This type of centralization however is desired, especially for permissioned and private blockchains. Projects that focus more on performance and scalability also tend to have a more centralized consensus. For example, the EOSIO blockchain is an open blockchain, but with 21 alternating block producers, it has relatively few consensus creators at a point in time [15].

Another aspect of decentralization is the development of a DLT, because the ongoing development of a project determines its scope, features, and security. For example, centralized development could use software updates to change the inflation rate, disable privacy features [16], or even reverse transactions [17] in the blockchain otherwise known for its immutability.

Availability, security against manipulation, and development - these areas of decentralization influence the permanence, autonomy, and agility of projects. All three are of vital importance when it comes to privacy and thus possibly also to the well-being of people.

E. *Attacks against Privacy*

Although a definite value is usually desired when evaluating privacy, implementations show that there are various anonymization procedures that differ in the level of privacy they provide. In some cases, it is not yet clear how effective some approaches really are, so that they cannot be evaluated and compared well at this time. In addition, new methods of deanonymization are constantly being researched [18], which makes a final evaluation of different approaches impossible.

A basic principle of anonymization in DLTs is to make transactions indistinguishable to an observer, so that only a set of transactions is visible, which can no longer be assigned to exactly one sending and receiving address. It is important how large this set of indistinguishable transactions, the so-called "anonymity set", is since it is an important indicator for the degree of anonymity. For example, if there are only two sender addresses and two indistinguishable transactions, the anonymity set amounts to only two and the transactions can be attributed with a 50 percent probability. How an anonymity set is constructed depends on the method used and varies greatly between different projects, some of which are introduced in the next subsection.

Attacks designed to deanonymize aim to reduce this anonymity set so that in the end a transaction can be assigned to an address, i.e., a user, with high probability. Anonymization methods try to make the anonymity set as large as possible and at the same time prevent possibilities for reducing this set. In this context, two side-channel attacks play a special role: the "timing attack" and the "value attack".

The timing attack utilizes the behavior of users who act predictably. For example, this is ideally the case when a customer pays for a coffee every morning at exactly 8 o'clock. Even if the addresses are not known to outsiders, they can be assigned to the user through this predictable transaction.

The value attack focuses on the value of transactions. This attack also goes beyond the DLT. For example, if someone sends 121.27€ in BTC to exchange and later withdraws 121.27€ (minus fees) in Ether (ETH), it is easy to associate these two transactions. This way one has created a connection between two addresses on two different networks without the transaction history of a single network indicating this.

Both attacks can be combined to further reduce the anonymity set in case of doubt. Furthermore, there are also attacks carried out off-chain, that is, based on data that does not appear on the ledger. This includes methods to find out the IP address that was used to initially propagate a transaction.

F. *Related Work*

To create privacy on DLTs there are already many different projects with different properties. Some are centralized, building on top of a DLT, others are decentralized and have privacy built directly into the protocol, at the first layer.

Centralized projects usually require the trust of the user that they are actually protecting the users’ privacy and not stealing coins. They are also susceptible to external factors, such as cyberattacks and regulations. They are at the second layer because they build on top of existing transparent DLTs, of which the ledger and circulating supply is verifiable and the transaction history is always observable.

Decentralized projects are often linked to a cryptocurrency or are one themselves. Some projects use mechanisms that no longer store any transaction history and/or in which the circulating supply can no longer be checked.

This paper only covers central methods of anonymization because of their optional property to deanonymize transactions and similarity to the proposed solution. A very simple form of anonymization is to send coins to a central exchange and receive them at a later time from a newly generated address. This can be effective because an exchange serves many users, who make many incoming and outgoing transactions. Therefore the anonymity set is relatively large. However, the anonymity set can be reduced to one with a systematic value attack if used improperly. Figure 1 depicts transactions (TX) made to or from an exchange within a certain period of time. Since TX 3 and TX 4 have the same value, it can be assumed that addresses C and D belong to the same person.

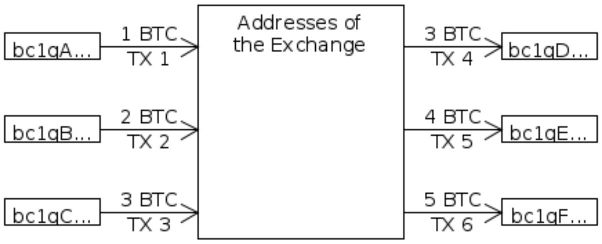

Figure 1. The concept of mixing coins on an exchange.

Another inherent disadvantage of exchanges is that they are a popular target for cyberattacks because they manage a large number of coins. The number of attacks on exchanges has increased almost steadily over the last few years. A total of USD 875 million was stolen by hackers in 2018 [6]. This not only has the consequence that coins may be insecure, but along with the high complexity of exchanges, it also repeatedly causes deposits and withdrawals to be temporarily disabled. Furthermore, there is a risk that the exchange will steal the coins or share the transaction history of its users.

Similar to exchanges are so-called CoinMixers, which are also based on the idea that a large number of users send them coins. The mixer then sends coins back to the user, which have a different history than the user's previously sent in coins. In order to prevent deposits and withdrawals from being associated by the same value, withdrawals can be split up into several transactions of which each is sent to a different address of the user. The mixer can create payouts with uniform values so that the case shown in Figure 1 does not occur. The latter two methods have already been implemented in Dash's PrivateSend protocol in a decentralized manner [19].

The mixer must be trusted, just as with the exchange, to return the coins and not to log and share data of the mixing process [20]. Due to its centralized structure, it is just as susceptible to cyberattacks or DoS attacks, albeit giving hackers a smaller incentive since it is not permanently storing user funds. With dedicated coin mixers, there is the additional risk that the mixed coins will be highly contaminated if they are being used primarily for money laundering.

III. Solution

This section covers our solution that provides privacy in decentralized and censorship-resistant DLTs while maintaining law enforcement. We state the requirements and present a corresponding concept. Based on that concept we present our prototypical implementation.

A. Requirements

Due to their decentralized architecture, DLTs offer the possibility to quickly transfer values without registration and intermediaries. Since DLTs are non-discriminatory, participants are basically on an equal footing in creating and monitoring transactions. If, for example, it is possible for governmental agencies to track financial data, anyone else can also track the data, thus undermining any privacy.

The centralized privacy enhancement concepts introduced in the last section are highly vulnerable to cyberattacks and technical failure. Furthermore, access to deanonymizing data cannot be controlled from the outside, which means that they have a high potential for abuse. Completely centralized anonymization tools are therefore unsuitable for safely and reliably protecting the privacy of companies and citizens.

Another aspect is scalability, which must be taken into consideration in case of possible increasing acceptance of cryptocurrencies. Privacy must not be costly or accessible to only a fraction of users due to technical limitations.

The solution must be able to be built on top of decentralized DLTs and sufficiently protect the privacy of the population. It is also necessary that the executive authority can break this privacy with relatively little effort. This effort must nevertheless be high enough and access must be transparent to prevent mass surveillance and allow only targeted observations.

To solve this problem, a concept is presented below, which was implemented on top of the cryptocurrency Nano. Nano is perfectly suited because it has high scalability due to its block-lattice, transactions do not cost any fees and are confirmed within milliseconds. Nano is exclusively transparent and has no possibility of a decentralized implementation of privacy. So far, there are also no effective anonymization tools for this cryptocurrency. The concept can be applied to other DLTs to a large extent. The implementation, however, is specific to this type of ledger and cannot be adopted by a blockchain.

B. Concept

The anonymization of transactions is carried out via a cluster of centrally administered coinmixers, each of which functions similarly to coinmixers of other cryptocurrencies. To ensure that the mixers are under state regulation, they can be operated by existing banks, for example. Banks are subject to strict banking secrecy, which may only be lifted by the state under certain circumstances. At the same time, banks are relatively trustworthy and can be closely monitored through the transparent ledger, so they cannot effectively steal customer funds.

A high-level overview of the concept is given in the following Figure 2.

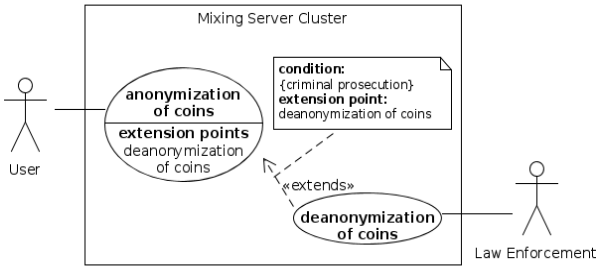

Figure 2. The user and law enforcement interact with the mixing service.

The coinmixers receive NANO from users of a predetermined denomination. After a time specified by the user, which should be as random as possible, the mixer sends back NANO of the same value to another address specified by the user. Because several users go through this process simultaneously, there is an overlap between deposits and withdrawals so that withdrawals can no longer be assigned to a single deposit. This successfully counters the value attack. The process is depicted in Figure 3 below. The coinmixer receives three incoming transactions of the same value from three different users within a certain period of time. The server later sends the coins back to the users to another address. It is no longer traceable which of the new addresses belong to which user.

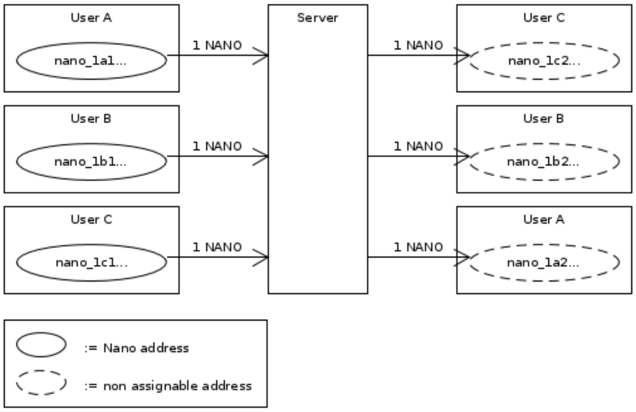

Figure 3. The concept of mixing transactions of the same value.

How large the anonymity set is, i.e., with how many other users a new payout address can be mistaken, depends on the number of deposits into the coinmixer within a common time period before the payout. This time period cannot be determined exactly and depends on the usual time chosen by the user until the Mixer returns the Coins. This consequently makes the timing attack less effective. Figure 4 visualizes the anonymity set of users in different scenarios. User A has an anonymity set of two since two deposits were made before her withdrawal. C has one of three and B and D both have an anonymity set of four since the same number of deposits took place within a common time period before. E only has an anonymity set of 2, as there were only two deposits within a typical time period.

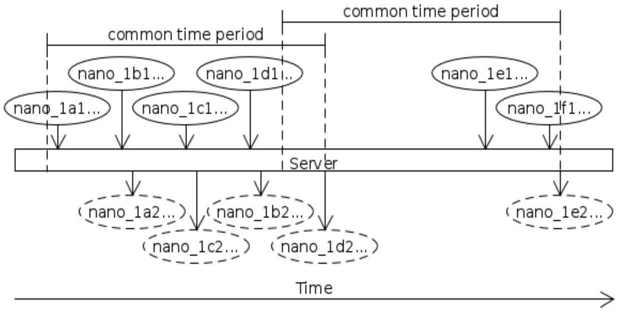

Figure 4. Multiple users deposit and withdraw from the coinmixer over time. The total number of users and their timing affect their anonymity set.

To increase the anonymity set significantly, it is alternatively possible to receive a private key to a "reserved address" from the server instead of being sent back coins. This key is transmitted off-chain, which changes the owner of the reserved address without this transaction being published. The reserved address contains the appropriate number of coins corresponding to the denomination selected by the client. The transaction that initially sent money to this address was made in advance, unrelated to a specific request, by the server. This gives the user the option to spend these coins at any time, as the user does not have to wait for the mixing process. The longer the user waits, the more her anonymity set increases. This is illustrated by the following Figure 5 in which NANO is sent to address d2 in the beginning. However, the associated private key is only transmitted to user D later on. Because D only uses this address after user E has made a deposit, e1 also falls into its anonymity set, which is equivalent to five in this figure. At the same time, e2 cannot be clearly assigned to e1, since e2 could also be a reserved address.

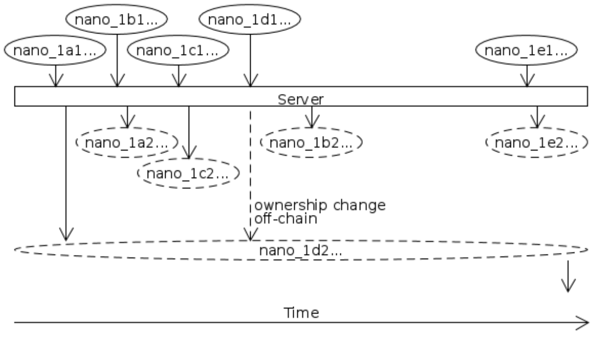

Figure 5. Transmitting ownership of coins off-chain greatly increases the anonymity set.

Since the server coordinates the received payment with a respective payout, it can document all mixing processes and thus remove the anonymity of desired users. This can be used if, for example, the flow of money beyond the mixer has to be tracked in the context of a criminal case. At the same time, however, this logging can also endanger the privacy of the users. To prevent this, several mixing servers are used. A user can now use these mixers sequentially so that her privacy is protected by each individual mixer. Figure 6 shows that by using three mixers for a mixing process, the privacy of user A is not broken even if two of these mixers are compromised.

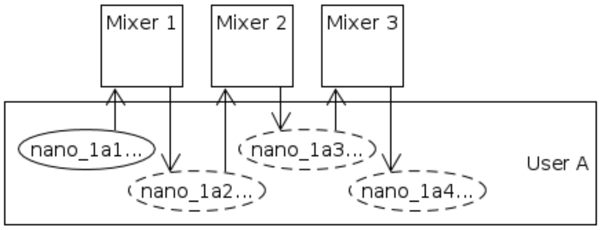

Figure 6. Using multiple mixers sequentially protects against maliciously tracking mixers and further increases the anonymity set.

Due to the sequential use of mixers, the number of required transactions, and the required time increases linearly. Therefore, for less privacy-critical transactions it is possible to use only one mixer per anonymization. This mixer is selected randomly so that all available mixers are used equally. This ensures basic privacy and a malicious mixer only has insight into a small subset of all private transactions taking place on the network.

To ensure sufficient liquidity of the mixer and thus a high anonymity set, it is necessary to promote the use of mixers by integrating them into the crypto ecosystem, such as wallets and enabling them by default. In that way, the coins of used addresses are regularly mixed. The privacy that is thereby strongly promoted serves to protect the general population and economy, even if they would not value privacy themselves. This way, the characteristic of cash to be anonymous by default is inherited.

C. Implementation

Within the scope of this work, the server software was implemented according to the use case shown in Figure 4. The code for this prototype is publicly available [21]. The server must be able to accept mixing orders, which can be placed either via a programming interface or a graphical user interface. In either case, the client sends the server the payout address, the number of coins to be mixed, and the time of the desired payout. The server then assigns the client a unique, newly generated deposit address, to which the client now sends the agreed-upon amount. As soon as this address contains sufficient coins, the funds are forwarded to a central address where they are combined with the coins of other users. As soon as the time for payout is reached, the respective number of coins will be sent from this mixing address to the specified payout address.

This is visualized in Figure 7. Client A and B send an equal amount of NANO to the mixer. Using an address generated for each of them, the mixer can confirm the payment and forward the coins to the mixing address. From there the payout takes place and it is not possible to trace which of these payout addresses belong to A or B.

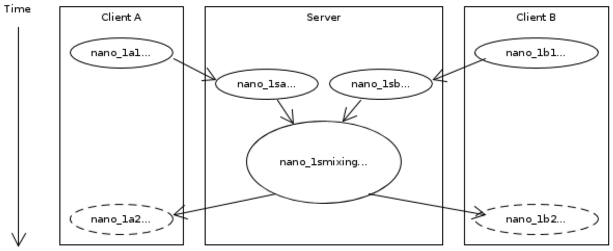

Figure 7. The mixing process of two clients in detail.

A relational database consisting of a single table is used for coordination. For each incoming order, a new row is created, which also reflects the status of the order. A row has the following eleven columns:

	name of row: variable type
1.	order_id: int(11)
2.	account: varchar(65)
3.	denomination: decimal(39,0)
4.	submission_epoch: int(10)
5.	fully_received_epoch: int(10)
6.	mixer_tx: varchar(64)
7.	mixer_epoch: int(10)
8.	fulfillment_account: varchar(65)
9.	fulfillment_tx: varchar(64)
10.	fulfillment_epoch: int(10)
11.	fulfillment_deadline_epoch: int(10)

Figure 8. A row in the database table for a single mixing request.

The column "account" corresponds to the deposit address and is unique. At the time of order creation, only columns 1, 2, 3, 4, 8, and 11 have a value. When the deposit is complete, column 5 is assigned and the mixing is initiated, which sets columns 6 and 7. Finally, when the payment is complete, columns 9 and 10 are filled. The columns ending in "_epoch" each store the corresponding timestamp in Unix time. The columns ending on "_tx" contain the ID of the respective transaction created by the server. Under "fulfillment_account" the payout address of the user is stored. A regularly executed script checks for incoming transactions and due payouts and updates the database accordingly.

IV. EVALUATION

The software is working correctly, as can be verified by the block explorer when examining the mixing address [22]. Nonetheless, it’s effectiveness depends on actual usage. Without frequent usage of these coinmixers, they do not offer any privacy advantage over exchanges as exchanges are also regulated and have to document all transactions. On the contrary, low usage could lead to an anonymity set of one and thus offer no additional privacy at all. In contrast to exchanges, mixers do not manage large amounts of money at any given time and are far less complex. This makes them more reliable, easier to maintain, and unattractive as a target of a cyberattack. However, mixers are also not given any incentive to process transactions. This jeopardizes the concept that is based on having as many reliable mixers available as possible.

Compared to non-transparent cryptocurrencies, this anonymization does not conceal the transaction values and, due to the transparent underlying cryptocurrency, allows attackers, even with extensive use of the mixers, to perform blockchain analysis and apply the timing and value attack or to observe the merging of addresses.

This can compromise anonymity if the user handles the mixer incorrectly. This is the case, for example, when a user spends the funds of a reserved address immediately after receiving it and thus becomes vulnerable to the timing attack. Such attacks through data analysis can become increasingly sophisticated as soon as statistics on user behavior are available or algorithms can recognize patterns with the help of artificial intelligence.

Equally dangerous can be the combination of remaining funds (change) on an account after an outgoing transaction. This is particularly critical if these funds cannot be further mixed because it is less than the smallest denomination.

The concept of using the exchange of private keys as value transfer is currently difficult to integrate into the existing wallet ecosystem as this type of transaction is not intended and would require new wallet backups by the client with every mixing transaction. Furthermore copying private keys and thus sharing them between multiple people is not reconcilable with the idea of trustless private keys which require a one-to-one relationship between key and user.

Another possible weakness is the constitutional state that the central authority is part of. If for some reason the central authority was no longer subjected to jurisdiction, its access would become uncontrollable and thus the tool meant to bring privacy to the masses could be turned into a tool for mass surveillance. This is not a novel problem and equally applies to current digital money transfer. This mixing concept will not protect users' privacy in an authoritarian regime but instead relies on a stable constitutional state.

If a good integration into the user wallets is achieved, it can be guaranteed that the tool is used correctly and thus offers strong privacy, which can only be lifted by the state in legally justified cases. This privacy is achieved without experimental and computationally expensive encryption. The greatly increased transaction volume resulting from mixing and the resulting growth of the ledger can be compensated for by modern cryptocurrencies that support ledger pruning. Expensive transaction fees and high latencies of transaction confirmations are also eliminated by cryptocurrencies like Nano.

A. *Possible Enhancements*

The anonymization tool can be improved in efficiency as well as functionality to further enhance privacy. Potential attack vectors can be closed and the user experience improved.

The transactions required by the server for the mixing process can be reduced from two to one by additionally requesting the source address from the client when creating an order and sending its coins directly to the mixing address. This worsens the user experience when used manually but hardly represents any additional effort when mixing in an automated way. In this case, the server checks the receipt of payment by filtering incoming payments to the mixing address according to the specified source address. This feature can coexist with the current system.

To prevent users from having their coins frozen after they have started a mixing order with a long mixing duration, it is possible to request an immediate payout. To do this, the user sends a request to the server with her order ID, whereupon the server ignores the originally set payout time and initiates the immediate payout. This would reduce the anonymity set in that specific case, but gives an incentive to initially specify a longer mixing time, since immediate payout is guaranteed, and thus increase the average anonymity set.

To make use of change without combining it with other addresses, it is possible to create an order with several deposit addresses. The user can then send the remaining coins of each account to one of those deposit addresses until they reach the value of the smallest denomination. To prevent a value attack, this deposit process should be spread over a longer period of time and overpaid. An overpayment not only enables untraceability but also creates a monetary incentive to operate a mixer. The concept of overpayment is illustrated by the following Figure 9 in which one NANO is assumed to be the smallest denomination of the mixer. Client A makes two payments with change to two different addresses of the mixer. Since A is overpaying, it is difficult for attackers to link her two addresses.

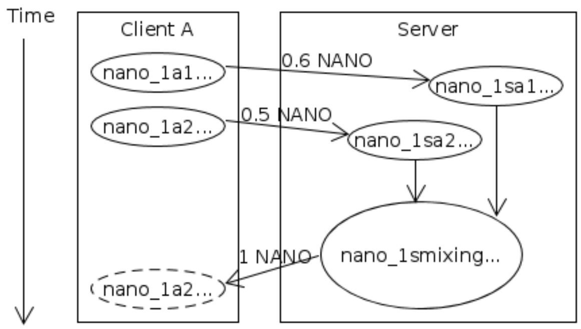

Figure 9. To utilize change without compromising privacy, the mixer supports multiple input addresses per order.

In addition to mixing, the mixer can offer a service requiring registration to manage user coins. The mixer manages all funds of a customer and makes the desired payments directly from the mixing address. This is very similar to a bank account or exchange account and can therefore be very attractive for many users, as they can hand over the responsibility for managing the coins to the bank.

The current implementation is decentralized in terms of anonymization, but still requires trust in the mixers for managing the coins. To decentralize control over the coins, it is possible to split the administration among several parties. Using so-called "multisignature" wallets, it would only be possible to carry out transactions if the majority agrees on them [23]. This prevents a single party from stealing coins. However, it also requires more reliable participants and a more complex system, which tends to work slower and is more prone to failures.

V. Conclusion and Outlook

The spread of DLTs as a means of payment is bringing with it new challenges. Some cryptocurrencies do not provide sufficient privacy, while others by contrast create complete anonymity at the expense of government authority.

In this paper, a concept for the anonymization of transactions on DAG-based cryptocurrencies was presented. A plan is proposed for integrating this concept into the modern constitutional state so that selective deanonymization maintains the possibility of criminal prosecution without being susceptible to abuse. Within the framework of the presented concept, the developed software enables the anonymization of transactions in a decentralized and censorship-resistant DLT while safeguarding criminal prosecution. How well it works in the real-world depends largely on its adoption and integration into the ever-changing crypto ecosystem. It provides a basis to promote and monitor decentralized transparent cryptocurrencies and make them suitable for society.

Semi-decentralized anonymization tools of the kind presented manage the balancing act between crypto-anarchism and state control. They allow states to have insight in decentralized cryptocurrencies without having to suppress them. It also gives them the possibility to introduce their own (complimentary) currencies based on DLTs and to control the use of transparency and anonymity purposefully in selected areas.

The development of such software is far from complete. With new technologies, there will always be new possibilities and limitations for existing implementations to reliably protect privacy. As the analysis of such transparent anonymization tools will progress, existing systems will be challenged again and again. Since DLTs are still in their infancy, there will continue to be a lot of potential in the area of trustless, centrally monitored anonymization in the foreseeable future.

Acknowledgment

This paper evolved from the research project “Recycling 4.0” (digitalization as the key to the Advanced Circular Economy using the example of innovative vehicle systems) which is funded by the European Regional Development Fund (EFRE | ZW 6-85017297) and managed by the Project Management Agency NBank.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. https://bitcoin.org/bitcoin.pdf (accessed Sep. 19, 2020).

[2] “Bitcoin Sent in USD Chart,” 2020. https://bitinfocharts.com/comparison/bitcoin-sentinusd.html#log (accessed Sep. 19, 2020).

[3] “Bitcoin price today, BTC marketcap, chart, and info | CoinMarketCap,” 2020. https://coinmarketcap.com/currencies/bitcoin/ (accessed Sep. 19, 2020).

[4] P. Ciaian, M. Rajcaniova, and d’Artis Kancs, “The economics of BitCoin price formation,” *Appl. Econ.*, vol. 48, no. 19, pp. 1799–1815, 2016, doi: 10.1080/00036846.2015.1109038.

[5] K. Manikas and K. M. Hansen, “Software ecosystems-A systematic literature review,” *J. Syst. Softw.*, vol. 86, no. 5, pp. 1294–1306, 2013, doi: 10.1016/j.jss.2012.12.026.

[6] Chainalysis, “The 2020 State of Crypto Crime,” no. January, 2020.

[7] E. Davradakis and R. Santos, “Blockchain, FinTechs and their relevance for international financial institutions,” *Econ. - Work. Pap. 2019/01*, 2019, doi: 10.2867/11329.

[8] T. Lyons, L. Courcelas, and K. Timsit, “Blockchain and digital identity,” p. 27, 2019, [Online]. Available: https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf (accessed Sep. 19, 2020).

[9] E. Kühl and M. Laaff, “Einmal mit Facebook zahlen, bitte! [Just pay with Facebook please!],” *Zeit online*, 2019.

[10] Bundesministerium der Finanzen, “Erste Nationale Risikoanalyse Bekämpfung von Geldwäsche und Terrorismusfinanzierung [First National Risk Analysis Combating money laundering and terrorist financing],” 2019.

[11] S. Elnaj, “The Problems With Bitcoin And The Future Of Blockchain,” 2018. [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2018/03/29/the-problems-with-bitcoin-and-the-future-of-blockchain/#1a05067f68dc (accessed Sep. 19, 2020).

[12] C. Lemahieu, “Nano: A Feeless Distributed Cryptocurrency Network,” *White Pap.*, p. 8, 2018.

[13] G. Wood et al., “Ethereum: A secure decentralised generalised transaction ledger,” 2019. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf (accessed Sep. 19, 2020).

[14] R. Werner, S. Lawrenz, and A. Rausch, “Blockchain Analysis Tool of a Cryptocurrency,” *ACM Int. Conf. Proceeding Ser.*, pp. 80–84, 2020, doi: 10.1145/3390566.3391671.

[15] “Consensus Protocol | EOSIO Developer Docs,” 2020. https://developers.eos.io/welcome/v2.0/protocol/consensus_protocol (accessed Sep. 19, 2020).

[16] Furszy and Random.Zebra, “Report: ‘Wrapped Serials’ Attack,” 2019. https://medium.com/@dev.pivx/report-wrapped-serials-attack-5f4bf7b51701 (accessed Sep. 19, 2020).

[17] V. Buterin, “Hard Fork Completed,” 2016. [Online]. Available: https://blog.ethereum.org/2016/07/20/hard-fork-completed/ (accessed Sep. 19, 2020).

[18] T. de Balthasar and J. Hernandez-Castro, “An Analysis of Bitcoin Laundry Services,” 2017, pp. 297–312.

[19] E. Duffield and D. Diaz, “Dash: A Payments-Focused Cryptocurrency,” 2014. [Online]. Available: https://github.com/dashpay/dash/wiki/Whitepaper (accessed Sep. 19, 2020).

[20] J. Bonneau, et al., “Mixcoin: Anonymity for bitcoin with accountable mixes,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8437, pp. 486–504, 2014, doi: 10.1007/978-3-662-45472-5_31.

[21] “rw501/nanonymity,” 2020. https://github.com/rw501/nanonymity (accessed Oct. 20, 2020).

[22] “Account – nano_3ikhg5yxkcpjcsrj7zyepzntpqzebe6qt6b8wy5k967wf49y7eei1cjtygg8,” 2020. https://nanocrawler.cc/explorer/account/nano_3ikhg5yxkcpjcsrj7zyepzntpqzebe6qt6b8wy5k967wf49y7eei1cjtygg8/history (accessed Sep. 19, 2020).

[23] V. Buterin, “Bitcoin Multisig Wallet: The Future of Bitcoin,” *Bitcoin Magazine*, 2014.