How to design a compliant, privacy-preserving fiat stablecoin via zero-knowledge proofs

etonec
for the Token Economy

Mina Foundation

uni.lu | SnT

HAUCK
AUFHÄUSER
LAMPE

Executive Summary

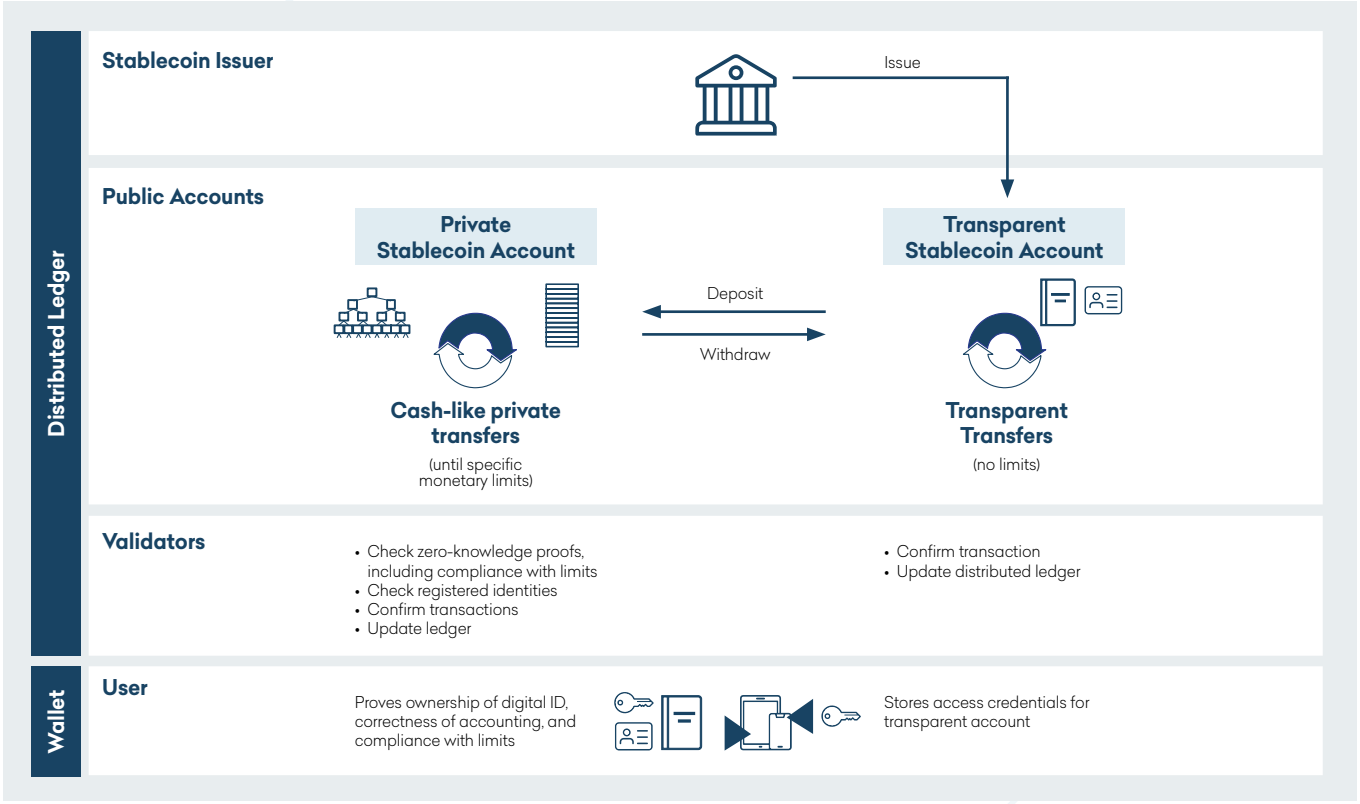
This proposal applies previous work by Gross, Sedlmeir, Babel, Bechtel, and Schellinger, who designed a central bank digital currency (CBDC) system that supports cash-like private, compliant payments using zero-knowledge proofs and digital identities (Gross et al., 2021). We explore the feasibility of a (fiat) stablecoin that provides cash-like privacy while enforcing compliance with anti-money laundering (AML) and countering the financing of terrorism (CFT) regulation. Such a privacy-oriented stablecoin solution does not exist today. We demonstrate, based on concepts developed in Gross et al. (2021) in the context of a CBDC, how users can exchange small amounts of value with a (fiat) stablecoin within pre-assigned limits outside the view of third parties, such as banks, central banks, crypto exchanges, regulators, or other parties, in a regulatorily compliant way. Put differently: this study uses the key concepts developed in Gross et al. (2021) to demonstrate the feasibility of a privacy-preserving and compliant stablecoin. The contribution of this paper is to show how the privacy and compliance concepts for a centralized CBDC can be **applied to a decentralized stablecoin**. In particular, we discuss the changes that result from replacing a central validator, i.e., the central bank in the context of a CBDC, with a decentralized transaction validation based on a distributed ledger. Further, we sketch how the Mina Protocol can be the basis for a privacy-preserving and compliant stablecoin system.

The proposed system enables cash-like private digital stablecoin transactions up to specific monetary limits. If these monetary limits are reached, transactions are conducted in a less private way, e.g., fully transparently on a blockchain or by including third parties that approve the transaction. The concept allows us to implement a wide range of different limits, including transaction limits, balance limits, and (e.g., monthly) turnover limits, depending on the legal requirements in the respective jurisdiction. In contrast to existing approaches beyond the realm of stablecoins, such as the mixer Tornado Cash, this allows us to comply with AML and CFT regulation requirements, e.g. around identification of the transaction parties and the origin of funds. High privacy guarantees and compliance with limits are, as in Gross et al. (2021), ensured in a trustless way via the use of cryptographic zero-knowledge proofs, in particular, zk-SNARKs. From an abstract perspective, a payment system that provides cash-like privacy in a centralized setting (CBDC) also provides cash-like privacy in a decentralized (blockchain-based) system where transactions are recorded on a public ledger, such as a stablecoin. As a result, the full technical solution by Gross et al. (2021) can be readily replicated, with the key difference being decentralized, smart contract-based verification of payments based on a distributed ledger instead of central bank-based verification of transactions.

To effectively implement turnover limits, the system follows the idea to rely on the availability of a unique digital ID (Gross et al., 2021) available to all participants of the stablecoin system. Payments by one person can then be mapped to one ID (or rather a hash of the information included in the ID) and summed up. This summing up is necessary to ensure that a participant can only open one private stablecoin account. Yet, only the owner of a unique digital ID and the corresponding account, i.e., the individual, can do this mapping - it will not be transparent to any third party. While in this context a digital government-issued ID is a desirable solution, we observe that the availability of such a digital ID will take time. Due to this fact and in contrast to Gross et al. (2021), for this new stablecoin approach, we consider a digital ID that is issued by the stablecoin issuer or contracted third parties in an outsourcing relationship instead of the government.

A cash-like private stablecoin transaction between Alice and Bob works as follows. Alice and Bob bilaterally agree on a payment, e.g. Alice wants to send Bob 50 euros privately via stablecoins. Both Alice and Bob create a ZKP on their computer or mobile phone. Alice proves that she owns sufficient funds to send to Bob, that she does not create new money out of thin air, and that the transaction complies with the regulatory limits on her account. Bob creates a similar proof. Subsequently, Alice and Bob send these proofs to the network. No confidential information about the transaction parties or the transaction amount is shared with any of the participants in the network. After submitting the transaction to the network, validators verify the ZKPs and, after the successful verification, append the transaction to the distributed ledger. This entry does not contain any confidential information, thereby allowing cash-like private payments.

Figure 1: System architecture of privacy-preserving stablecoin system



Source: based on Gross et al. (2021); applied to a decentralized stablecoin system.

1. Introduction

Privacy constitutes a fundamental civil right, e.g., stated in the United Nations Declaration of Human Rights and the Convention for the Protection of Human Rights and Fundamental Freedoms (Gross et al., 2021). In Europe, privacy of payments is heavily demanded by users (ECB, 2021). To date, in the context of payments, and in particular in the context of fiat currencies, cash is the only form of money that provides a high degree of privacy for transactional data (Gross et al., 2021). For cash payments, only the sender and receiver know the parties involved and the amount. On the other hand, digital payment methods such as bank transfers or mobile payment solutions, collect confidential payment data, thereby negatively impacting privacy. While central bank digital currencies (CBDC) can be used to improve the privacy of payments (Gross et al., 2021), also stablecoins have the potential to improve privacy of digital transactions for users, while building on the stability of fiat currencies. To the best of our knowledge, there is no stablecoin on the market that provides privacy features similar to those of cash today. All of today's stablecoin transactions are recorded on the respective permissionless blockchains, and their pseudonymised data can be observed publicly, which arguably gives individuals that conduct stablecoin-based transactions worse privacy guarantees than bank-based payments. The conflict of public blockchains with publicly available and perfectly traceable data and the requirements of privacy-preserving digital cash is obvious. Given the importance of privacy and the stability of stablecoins, we believe a privacy-preserving stablecoin has great potential.

In this paper, we use the concepts from Gross et al. (2021) and show how a privacy-preserving, yet regulatorily compliant, fiat stablecoin can be designed and how privacy-preserving transactions can be executed. The key contribution of this paper is to show how the privacy and compliance concept for a centralized CBDC (Gross et al., 2021) can be applied to a decentralized stablecoin. In particular, we discuss the changes that result from replacing a central validator, i.e., the central bank in the context of a CBDC, with a decentralized transaction validation based on a distributed ledger. Further, we sketch how the Mina Protocol can be the basis for a privacy-preserving and compliant stablecoin system. Cash-like privacy for stablecoin payments can be ensured by cryptographic zero-knowledge proofs (ZKPs) without the need to trust third parties such as banks or central banks for preserving privacy (trustless privacy).

For such cash-like private transactions, transaction details are kept confidential between the two transaction parties involved just as it is the case with physical cash. Third parties cannot access transaction details for payments until specific monetary limits are met. These thresholds can include balance, turnover, or per transaction limits. If the limits are exceeded, the transaction partners can conduct additional transactions only when they are identified to comply with regulation and impede illicit activities. These features already go beyond the possibilities of physical cash. Without third parties that can conduct compliance checks, users prove their compliance via ZKPs. The verifiers then verify the ZKPs. Amongst others, they verify that the specific requirements for payments implemented through the stablecoin design, including the defined transaction limits, are met.

In essence, our goal is to create a stablecoin that provides similar privacy guarantees as the privacy coin Zcash or the mixer Tornado Cash by using ZKPs and digital identities, yet without the corresponding regulatory challenges with respect to money laundering and terrorism financing (as in Gross et al. (2021) for a CBDC). These challenges led to the U.S. Treasury sanctioning Tornado Cash in August 2022. Similar to the wide adoption of public key cryptography in spite of initial strong opposition from governments we believe it will be challenging to suppress legitimate privacy needs in the context of financial transactions in the long run. Even within the digital euro project by the European Central Bank the need for privacy provision was already discussed at a very early project stage. Our goal is to sketch a private sector form of money alternative that addresses users' enhanced privacy needs, while complying with regulatory requirements by design.

This paper is similarly structured as Gross et al. (2021): In Chapter 2 we discuss key concepts used in this paper. In particular, we introduce the notion of stablecoins and ZKPs. Chapter 3 illustrates the system architecture of the stablecoin design and explains how a cash-like private stablecoin transaction is conducted. In particular, we elaborate on which entities can see which transaction data. Further, we sketch how the Mina Protocol can be the basis for a privacy-preserving and compliant stablecoin system. In Chapter 4 we discuss further considerations and future extensions of our concept. Chapter 5 concludes the paper.

2. Background concepts

2.1 Stablecoins

Stablecoins are payment instruments based on distributed ledger technologies (DLTs) that address the high volatility of traditional crypto assets, such as Bitcoin and Ether, by establishing a fixed exchange rate to some reference asset(s). It can be distinguished between license-backed, fiat-backed, asset-backed, and algorithmic stablecoins that differ in the underlying backing. In this paper, we focus on fiat stablecoins, i.e. DLT-based payment instruments that are referenced to fiat currencies such as the euro or the US dollar. These fiat stablecoins aim to maintain a 1:1 peg to the respective fiat currency and can be understood as fiat currencies "on chain". The most prominent examples for (something that comes close to) fiat stablecoins are USDT and USDC. USDT is a US dollar-backed stablecoin issued by Tether Limited, and USDC, a US dollar-backed stablecoin issued by the Centre Consortium, consisting of Circle and Coinbase. In October 2022, these two stablecoins had a joint market capitalization of 115 Billion US dollars. Their market capitalization accounted for approx. 12% of all cryptocurrencies (own calculations based on Coinmarketcap, 2022). Fiat stablecoins are somehow similar to conventional digital forms of money: Bank deposits are transacted when paying via bank transfers, credit cards, or mobile devices. The main difference to traditional digital forms of money is that stablecoins are based on DLTs. The respective decentralization provides novel opportunities related to addressing inefficiencies in global payments as well as enable novel use cases. As an example, due to the elimination of intermediaries, micro-/nano-payments can be conducted with marginal costs. On conventional payment infrastructures, these payments cannot be implemented in an economically efficient way. Additionally, streaming payment applications are enabled, for which one pays on a pay-per-use basis instead of a one-time payment. The streaming of money is a completely new use case that is today hard to grasp while examples from other industries can show how this might fundamentally change the industry: just imagine what streaming did to the music or video industry, money streaming could do the same to banking. Further, stablecoins can be an integral part of blockchain-based ecosystems, e.g. around decentralized finance (DeFi) or non-fungible tokens (NFTs).

2.2 Privacy of existing means of payments

Existing means of payment differ in terms of privacy. Cash is the most private means of payment. Third parties cannot access transaction details. Only the sender and receiver of cash payments know transaction details. To fight illicit activities, such as money laundering and terrorist financing, regulators introduced limits on private cash payments (Gross et al., 2021). If a specific monetary threshold is exceeded, identification information of the sender must be collected. For traditional payments via bank deposits, transaction data is shared with commercial banks and payment service providers (PSPs) and – if instructed – with supervisory and other regulatory authorities. Privacy is remarkably lower for such payments.

The degree of privacy is even lower for most of today's crypto assets: For the most common crypto assets such as Bitcoin, transaction details are publicly accessible on their respective public blockchains. The transaction data is observable for the general public, however, stored in pseudonymized form instead of personal data. Both academic research (e.g., Biryukov & Tikhomirov, 2019) and recent cases, such as the seizure of more than 500 Bitcoins connected to the darknet platform Hydra (Yahoo Finance, 2022), demonstrate that the identification of owners of pseudonymous Bitcoin addresses is feasible. Privacy aspects are even worse on account-based systems such as Ethereum and the corresponding smart contracts, which includes Ethereum-based stablecoins: Once a party interacts with a pseudonymous address and learns the individual or organization that owns the address, they can directly observe all transactions that this account is involved in.

To improve privacy for DLT-based digital payments, privacy-preserving crypto assets, so called "privacy coins", were created. The most prominent examples are Zcash and Monero. These privacy coins use cryptographic methods, such as ring signatures and ZKPs, to hide transaction details, thereby substantially improving users' privacy. However, privacy coins are highly volatile. From January until October 2022, Zcash and Monero lost 40–60% of its price (own calculations based on Coinmarketcap, 2022). They fail the promise to serve as a stable coin and the reason to exist is questionable. In this context, stablecoins that deserve their name can play an

important role. In today's stablecoin design, transaction data is recorded in pseudonymous form similar to Bitcoin and Ether. In the future, stablecoins could also leverage cryptographic privacy-preserving technologies, such as ZKPs, to provide cash-like privacy. This design could build on the stability of fiat currencies and – via the use of limits – also ensure regulatory compliance. To the best of our knowledge, such a privacy-oriented stablecoin does not exist today.

2.3 Zero-knowledge proofs

Blockchain-based infrastructures have various benefits over centralized systems. These benefits include the elimination of counterparty risk for payments, high availability, and strong integrity guarantees (Sandner et al., 2020; Butijn et al., 2020). Nonetheless, there are also significant challenges, both from a scalability and privacy perspective. These limitations typically result in congestion and relatively high transaction costs on the one side, and organizational or regulatory issues related to the excessive disclosure of sensitive information on the other side (Sedlmeir et al., 2022). Both challenges are inherently connected to the replicated processing of transactions on a blockchain: To make sure that all rules of a blockchain, or smart contracts that run on it, are followed, every node needs to do the same computations in the context of a transaction. A node modifies its state – a running aggregate of the history of blockchain transactions that is maintained for efficiency reasons – according to the transaction. For instance, the new balance is computed from the previous balance and the transaction amount. This implies that every node can see all input values, intermediate steps, and results of computation and can accordingly observe balances, turnover, business relationships, etc. It also means that the computational resources need to be provided on every node.

ZKPs are one of the most promising ways to address both issues in DLT scalability and privacy simultaneously. The core idea is the following: To verify that the result of a computation is correct, it is not necessary to replicate the full computation and know all of its inputs. Instead, another party can do the computation and create a short cryptographic proof that the result of the computation is correct. Consequently, it suffices to verify the ZKP instead of redoing the full computation. ZKPs are such proofs of computational integrity, with the additional property that they reveal no information beyond the correctness of the computation under consideration. More formally, ZKPs satisfy the properties of completeness, soundness, and zero-knowledge. Completeness means that an honest prover can convince the verifier about true statements. Soundness means a malicious prover can convince the verifier about a false statement only with small probability. Zero knowledge means that the verifier does not learn anything meaningful but the truth of the statement (Maurer, 2009). Importantly, for zk-SNARKs, proofs can be verified fast as they do not contain a lot of information.

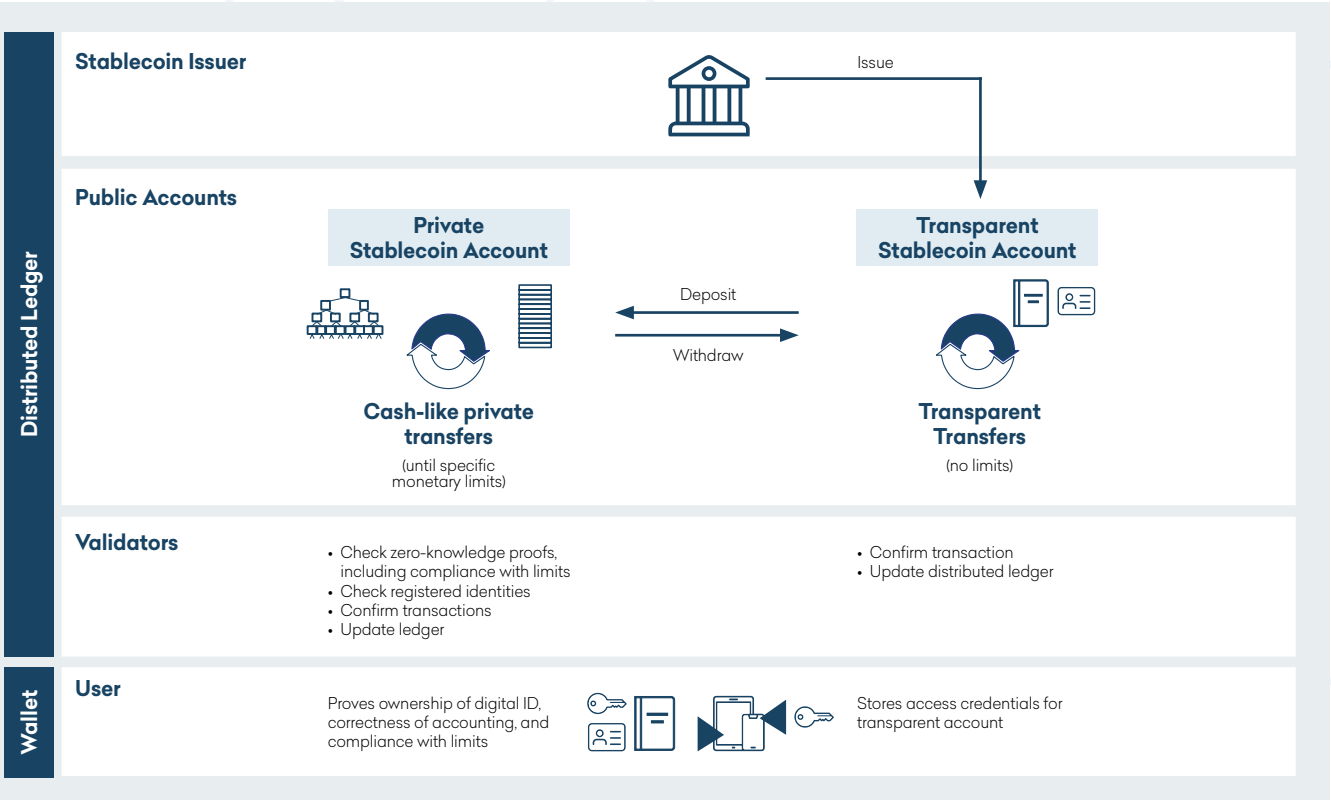
ZKPs for specific statements have been around for many years. For instance, consider the context of cryptographic key pairs: The digital signature, i.e., the proof that somebody knows a private key associated with a public key without revealing the private key, is essentially a ZKP. ZKPs for special cases were also already used in the 2000s to create anonymous credential systems. Anonymous credentials are a special form of digital certificates, i.e., digitally signed attestations that include a holder's attributes, as in an ID card or a driver's license. The digital signature makes these attestations tamper-proof and machine-verifiable. For the verification of the digital signature, usually the holder needs to send the full digital certificate to the verifier. This implies that the verifier will not only see all the attributes in the digital certificate but also uniquely identifying data like the digital signature itself. In contrast, anonymous credentials do not need to be sent to the verifier entirely and can, therefore, minimize the data that the verifier sees without hampering verifiability. This, for instance, allows one to prove that one holds an ID card that attests an age older than 18 (signed by a public key that is revealed during the process to identify the issuing authority), yet without disclosing any other personal information or the public key to which the digital certificate is bound. ZKPs for more generic statements have only become practical in the mid-2010s, presumably also because of increased interest for its use in blockchain applications. In fact, any statement that is in some sense efficiently checkable allows for a ZKP (Goldreich et al., 1986). This includes, for instance, proving knowledge of solutions to Sudokus, mathematical equations, or hash-puzzles, without revealing the solution itself.[1]

[1] More generally, ZKPs can attest the correctness of a privately executed computation: Given a public algorithm F and private inputs x, one can prove that a public result y satisfies F(x)=y. For instance, when F is the hashing algorithm SHA256 and y is a publicly known hash value, one can prove that one knows x such that SHA256(x)=F(x)=y. In this context, one calls x the "private input(s)" and y the "public output" of F(x)=y. Note that parts of the private inputs can always be made public if desired.

A prominent application of such ZKPs is the privacy coin Zcash. It uses ZKPs to hide both the sender's and receiver's identities/addresses as well as the transaction amount. More precisely, the sender proves using a ZKP that they have previously received (so far) unspent funds that they can use for a transaction with the same amount. Consequently, the sender does not explicitly point to the previous funds or leave any other correlatable information that would allow to link the transaction to the previous transaction and, thus, potentially de-anonymize the transaction party.

General-purpose ZKPs can also be used to replicate and extend the capabilities of anonymous credentials. In this paper and as in Gross et al. (2021), we combine ZKPs for proving the correctness of private payments associated with a private account with the ability to prove properties about an underlying identity credential that is also (hiddenly) connected to this account. Our ZKP-based approach allows us to ensure that specific transaction and turnover limits on private payments imposed by regulators are not exceeded – all without the sender or receiver leaving sensitive or even personally identifiable information. One of the core prerequisites of our system is that the credential that is necessary for users to conduct cash-like private transactions cannot be shared with third parties easily. Otherwise, the system could turn into a "money-mule" because criminals could collect access to many individuals' private payment accounts via hacking, blackmailing, or purchase on black markets. Making it difficult to get access to the identity credential via cyberattacks can be implemented through hardware-binding. Here, the cryptographic key that is needed to use the identity credential is stored on a mobile phone's or laptop's "secure element". The physical transfer of the device is required for transferring access to the identity credential and, ultimately, the private payment rail. Yet, hardware-binding does not address the threat of blackmailing and particularly voluntary sales of the identity credential sufficiently. The core problem is that an "isolated" system – one in which the identity credential is only used for giving a user access to the private accounts – may not have enough value for users to efficiently inhibit voluntary release. Consequently, the proposal ultimately relies on "all-or-nothing transferability": The identity credential should be required in a lot of other domains, such as opening bank accounts, accessing government services, applying for a job, etc. Only if the identity credential has sufficient value for every user – not only the ones that want to use cash-like private digital payments – identity credential passing and, ultimately, money mules can be avoided.

Figure 1: System architecture of privacy-preserving stablecoin system



Source: based on Gross et al. (2021); applied to a decentralized stablecoin system.

3. Our high-level proposal for a privacy-preserving and compliant stablecoin

3.1 System architecture and core components

Our privacy-preserving stablecoin system is illustrated in Figure 1 and can be implemented in various blockchain systems, such as the Mina Protocol. The Mina Protocol, in addition to its native deployment of ZKP technology, also provides a high degree of programmability which is paramount for such a system. When a user deposits money or receives a creditline with the stablecoin issuer, stablecoin tokens are provided in return. This implies that every stablecoin is fully backed by an equal amount of fiat reserves off-chain. The stablecoin issuer issues the stablecoin tokens on a blockchain network in – following the terminology in Gross et al. (2021) – so-called transparent stablecoin accounts, i.e., tokens are issued in the blockchain account address of the user. Via these transparent accounts, users can exchange funds on a peer-to-peer basis. This is very similar to today's stablecoin payments, and does not provide privacy improvements.

Higher privacy for stablecoin payments is ensured by a second stablecoin payment rail - again following the terminology in Gross et al. (2021) -, so-called private stablecoin accounts. Transactions conducted within private stablecoin accounts are cash-like private: Transaction data is only accessible to the two transaction parties involved. There is no way for third parties to access confidential transaction details. To conduct cash-like private payments, money must first be transferred from a user's transparent stablecoin account to a user's private stablecoin account. Note that, as in Gross et al. (2021), we implement limits on cash-like private stablecoin payments (see below on how this works technically). These limits are necessary to ensure that the stablecoin is not used for illicit activities on a large-scale. Otherwise, money laundering and terrorist financing could be enabled as – by design – there are no AML/CFT checks in the private stablecoin accounts possible. This is because information on the transaction sender, receiver, and amount are not available to third parties, such as monitoring agencies and regulators.

Different forms of limits can be implemented, e.g., (per-) transaction limits, balance limits (maximum account balance), and turnover limits (maximum monthly turnover), and can flexibly be modified depending on the needs of the regulator in the respective jurisdiction.

For an effective implementation and enforcement of the limits, it must be ensured that a user can only open one private account (Gross et al., 2021). Otherwise, the limits would be diluted. We ensure this via the use of verifiable credentials. In contrast to Gross et al. (2021), we consider verifiable credentials that are provided by the stablecoin issuer or another third party, instead of the government. As part of the onboarding process, the stablecoin issuer (or another regulated/authorized entity) conducts know-your-customer (KYC) measures and issues a digital certificate to the user, a digital representation of the information contained in their physical ID card. If a user seeks to open a private stablecoin account they must prove to validators, i.e., selected entities that are part of the consensus process and confirm transactions, that they possess a respective digital certificate issued by the stablecoin issuer. Note that only the hash of the digital certificate and a ZKP and no personal information is shared with the validators. Validators check if the user has already registered a private stablecoin account, i.e., if the hash of the digital credential is included in a list of hashes of all registered users. If not, validators initiate an account for the user, so that, subsequently, the user can transact privately within the private stablecoin account.

The technical setup and components for our stablecoin system are the same as in Gross et al (2021); amongst others, we also use zk-SNARKs to enable cash-like private payments. From an abstract perspective, a payment system that provides cash-like privacy in the centralized setting of a CBDC (Gross et al., 2021) also provides cash-like privacy in a decentralized (blockchain-based) system, as mentioned in the conclusion of the aforementioned paper. Consequently, the full technical solution by Gross et al. (2021) can be readily replicated in a stablecoin setting, with the main difference being decentralized, smart contract-based verification of payments (including ZKPs)

[2] For more details on the onboarding process of such a verifiable credentials-based system, see Gross et al. (2021).

instead of central bank-based verification. In particular, we also build on the concept of commitments and nullifiers used in Zcash. A cryptographic commitment corresponds to a one-way obfuscation and compression of data, typically using a hash function. Outside the context of ZKPs, cryptographic commitments are typically used to "commit to" information, i.e., to publish a short statement that does not allow to infer the underlying information but which is tied to the inputs. At a later stage, the commitment can be "opened" by the party that created the commitment. Thus, the information underlying the commitment is revealed, and the receiver of the information can use the commitment to verify that the information has not been changed since the commitment was created. In other words, cryptographic commitments correspond to 'sealed envelopes': The prover can hide information and reveal it only at a later stage, so the verifier can make sure that the information revealed is the one that was initially hidden. With ZKPs, one can keep the underlying information confidential (not open the commitment and reveal all the underlying information) but still prove selected properties of the underlying information. For instance, the underlying information could be a transaction including a sender and receiver address and a transaction amount. ZKPs can be used to prove that the amount of the transaction corresponding to a commitment is lower than a specific amount, e.g., 1000 euros (Gross et al., 2021). In Zcash, transactions are not published showing information on the sender, receiver, and amount in plain text on a public blockchain ledger and marking them spent on use. This would be the case in the original unspent transaction output (UTXO) model used, for instance, in Bitcoin. In contrast, Zcash only publishes commitments to transactions (UTXOs) and proves with a ZKP the authorization to spend and that no more money is spent than was previously received. Moreover, ZKPs are used to prevent double-spending without the need to explicitly point to a previously received UTXO that has not been spent before. This is necessary because the unlinkability of transactions is a prerequisite for anonymity. In essence, double-spending is prevented by creating and publishing a second commitment (a "nullifier") that is deterministically derived from the UTXO underlying the commitment that is to be spent. The commitment that is to be spent is not referred to directly but only inclusion in the structured database of all previous commitments in the state is proved, again with a ZKP.

Our approach uses some of the previously described concepts, yet with a substantial change: In our approach, we do not prove statements about (commitments to) previous transactions. While ZKPs allow for a proof that a transaction amount is below a specific threshold, a UTXO-based approach cannot enforce turnover or balance limits. In a UTXO-based system, a user can receive and send an unlimited number of transactions. These transactions are not linked to the user. Following Gross et al. (2021), we rely on an account-based model. Account-based models, such as what is available through the Mina Protocol, are better suited for this type of deployment also due to storage optionality, zero-knowledge smart contracts (zkApps), and fungibility. As a consequence, users publish commitments to their entire accounts. These accounts include the history of previous transactions. A transaction corresponds to two users invalidating ("spending") their previous account states and committing to a new account state. Both users create a ZKP that proves individually that the transition from their old to their new account state is legitimate (for details, see Gross et al., 2021). In this context, it is proven that balance and turnover limits are adhered to and that the users own a digital credential that is neither expired nor revoked. The two ZKPs from sender and receiver are linked: One can easily verify that the amount by which the one account balance is increased is exactly the same as the amount by which the other account's balance is decreased by comparing the respective (salted) hashes. Additional statements can easily be added, such as proofs that both IDs are not included on a specific sanctions list (Gross et al., 2021).

Through the use of commitments and nullifiers, and relying on a digital certificate for ID information, we can use the benefits of an account-based approach, such as the control of balance and turnover limits as well as certain identity-related requirements (Gross et al., 2021) without negative implications for privacy. At all times, confidential transaction data is kept in the user's local wallet. The local wallet records the transactions and knows the transaction history of the user. This confidential data is not shared with any third party.

3.2 The process of cash-like private transactions

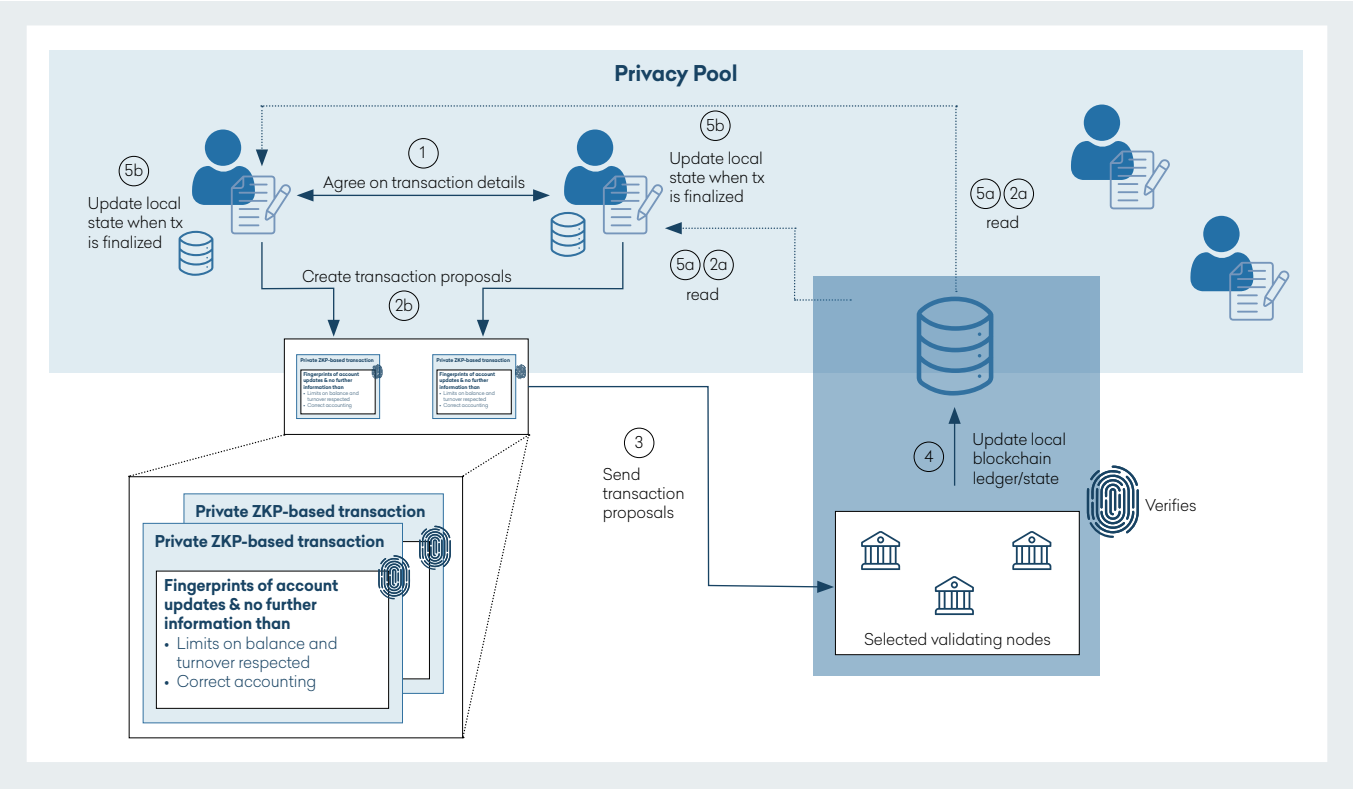
The transaction process works similarly as in Gross et al. (2021), but varies with respect to the (decentralized) validation and record-keeping on a DLT. To send money privately, the sender and receiver agree on the transaction amount and update their accounts on their local wallet. Then, both send a ZKP to the network/ validators. The sender proves that they own sufficient funds. Both prove that all limits are respected, and that no new money is created. After verifying the proof, the verifier adds the new transaction to the public ledger. The process is illustrated in Figure 2.

In detail, the following steps are executed:

1. Sender and receiver agree on a transaction amount and a random nonce. The nonce ensures that any relevant intermediary can check later that the ZKPs of the sender and receiver relate to the same transaction. In practice, the sender could propose a payment of amount x to the intended receiver. Their device subsequently generates the random nonce and puts this information in a QR code or message that the receiver can then scan or receive to proceed.
2. The sender's and receiver's wallet app automatically creates transaction proposals. These proposals correspond to tentative updates of their account balance and running turnover in their local wallet. They also compute the ZKP that proves the statements that the validators need to check. The ZKPs include proof of access to the digital identity credential that is neither expired nor revoked, sufficient funds available, and compliance with the limits. The ZKPs also prove that the corresponding public outputs, such as commitment to new account, nullifier for old account, transaction amount link, and validity of digital credential are computed out of their private inputs, namely old account state, digital ID credential and corresponding cryptographic key pair, and tentative new account state. To create the ZKP, they may need to retrieve the blockchain's state as they need to prove that the commitment to the old account state has previously been included in a block.
3. Both the sender and receiver send the public outputs and ZKPs from step (2) to the network (mempool) and wait until the validators include the (bundled) transaction in a block.[3]
4. The network selects block producer (winning validator), who includes the transaction, given it is valid. The validity check involves verifying the two ZKPs from step (2). If the two ZKPs are valid and their connection (same transaction amount link, which is the commitment to the transaction amount and a nonce that sender and receiver agreed on prior to the transaction) is legitimate, the new commitment and nullifier are added to the blockchain.
5. A message that the transaction is successful is emitted and can be realized by the client wallet app. The local ledger in the wallet app is then modified accordingly and the transaction is tagged successful by both sender and receiver.

[3] If the DLT does not provide absolute finality but only probabilistic finality (like PoW-Ethereum), they may wait until the probability of the transaction being reverted is lower than a user-defined threshold, e.g., wait for 20 additional blocks.

Figure 2: High level visualization for cash-like private stablecoin payment



3.3 Utilizing the Mina Protocol for privacy and compliant payments

One way of implementing the described stablecoin design is utilizing the Mina Protocol, a novel DLT that natively includes zero-knowledge capabilities. The Mina Protocol can be used to build sophisticated applications that are based on ZKPs, so-called zkApps. In the following, we briefly sketch out how the Mina Protocol can be used to implement such a solution. A general proof-of-concept will be made available in the upcoming months on etonec's GitHub page.

If Alice wants to send money to Bob, she can indicate in her browser application whether she would like to send the money in a private way to Bob or not. To date, depending on the jurisdiction there are regulatory limits on private payments imposed by local regulators (Gross et al., 2021). If AML regulations require a transaction-level threshold for private payments, Alice has to make sure that her transferred amount is below this threshold, if she wants to send money privately. If the payment amount exceeds the threshold, payment service providers have to capture personal identity information to process the payment. In this case, the application will ask Alice to provide a proof of identification. Note that this does not mean that Alice needs to reveal her personally identifiable details, such as name, address, or date of birth. Instead, Alice only needs to prove that she is in possession of a valid credential that has been issued by a trustworthy institution and it was checked that she is not listed on a sanction list or if she is a politically exposed person. Thus, no personal data is shared with the protocol, but only a proof instead. After proof of identification and proof of the payment amount, the amount will be transferred to her counterpart.

As mentioned above, payment amounts below the regulatory required threshold can be made with cash-like privacy implemented through a privacy pool (Gross et al., 2021). The previously described setup of using nullifiers and commitments will be explored at a later stage; at a high-level the pool works as follows: If Alice wants to send money privately that exceeds the regulatory or compliance limit for private payments, Alice needs to provide a proof of identification. If the amount lies below the limit, no proof of identification is necessary. Then, she is authorized to pay money into the privacy pool. The pool intermediates the transfer, so from an outside perspective, amounts that fall below regulatory thresholds can be transferred with cash-like privacy which is also dependent upon the number of participants in the privacy pool. As the money stems from a pool to which various parties contributed, the origin of funds remains private. As all parties that want to transact an amount higher than the threshold need to provide a proof of their identity, it is guaranteed that the main share of the money comes from a KYC-ed entity. As a result, this setup enables private payments, while guaranteeing that the entity that sent the payment has conducted sufficient KYC measures if required legally.

4. Future improvements and considerations

Our future research activities will focus on several topics, including the integration of digital identities and the corresponding integration of our cash-like private stablecoin with regulated environments and technical improvements regarding transaction costs, performance, and scalability, also resulting from the decentralized validation.

Regarding the integration of digital IDs, there are several choices on who could issue the digital ID needed for onboarding and interacting with our cash-like private stablecoin. For the start, we consider the stablecoin issuer a suitable entity, but in the medium and long term we aim to integrate countries' national ID cards. Particularly in Europe, we consider connecting to the eIDAS middleware or interacting directly with digital wallets a promising approach in order to connect societally recognized and verifiable forms of unique identities with the digital environment, in which one interacts with the proposed form of stablecoins. Yet, many technical details of the revision of eIDAS are not yet settled, and certification processes could be required for interacting with the corresponding systems or wallets (for instance, this is the case for the eID in Germany).

The use of digital identities and ZKPs could also be valuable for stablecoins beyond giving end users strong privacy guarantees: For instance, with certified institutions such as auditors, proofs of deposits could be verified efficiently through a smart contract and, therefore, increase trust that the stablecoin is indeed backed by a sufficient amount of funds. Further questions that need to be addressed concern the handling of identity revocation on-chain, the frequency of corresponding updates, and – arguably more complex – the maintenance of sanctions lists, which need to be provided through an Oracle reliably. Compared to a more centralized design (e.g. a CBDC), there are also several challenges related to the need for updating smart contracts and activities, such as periodically clearing the privacy pool (see Gross et al., 2021) or reverting transactions in a legal dispute. In a centralized ledger, such changes can be implemented if the need occurs. In contrast, in a smart contract-based design on a decentralized ledger, any changes that may need to be made retrospectively need to be prepared for. For instance, this could comprise the need for specifying the authorization policies in a way that makes them practicable but not easy to abuse for an attacker, and that allows to do necessary updates to the smart contract code without compromising the initial guarantees related to privacy characteristics.

From a technical perspective, the creation of ZKPs is still computationally intensive, which is particularly problematic for digital wallets on mobile phones. Moreover, the verification of ZKPs still adds overhead compared to simple payments on an already highly resource-constrained blockchain. We hence want to explore various opportunities for technical optimizations that would save proving time and transaction costs when interacting with cash-like privacy. This includes improvements regarding the complexity of creating and verifying ZKP-based transactions as well as maintaining and updating the state of the privacy pool, where optimizations are essential owing to the replicated execution and storage of transactions. We will investigate novel techniques for polynomial commitments in the context of Merkle trees and ZKPs like Caulk (Zapico et al., 2022), batching techniques for ZKPs like SnarkPack (Gailly et al., 2021) as an alternative to the proof recursion that is currently implemented in the Mina Protocol, as well as improvements similar to those employed in the implementation of the private CBDCs Platypus (Wüst et al., 2021), PEReDi (Kiayias et al., 2022) and UTT (Tomescu et al., 2022), which focused on a DLT-based deployment of an anonymized account-based CBDC system.

5. Conclusion

In this paper, we applied and extended the concepts from Gross et al. (2021) to discuss how a stablecoin system can be designed to ensure cash-like private transactions, i.e., transactions that are as private as cash transactions today. The contribution of this paper is to show how the privacy and compliance concept for a centralized CBDC (Gross et al., 2021) can be applied to a decentralized stablecoin. In particular, we have illustrated how a distributed ledger with its decentralized transaction validation, digital credentials, and ZKPs can be used jointly to provide high privacy guarantees for stablecoin payments leveraging an account-based infrastructure, yet taking legal requirements into account. While a privacy-preserving stablecoin constitutes a market gap today, it is technologically feasible. A ZKP-based stablecoin may face high user demand as it provides high privacy guarantees, regulatory certainty, and can be seamlessly integrated into blockchain ecosystems, e.g. DeFi or digital assets. For stablecoin issuers, positive returns from the underlying reserve can be expected. Amongst others, these two factors make a privacy-preserving stablecoin an excellent business opportunity.

About the authors

Dr. Jonas Gross
eTonec GmbH

e: Jonas@etonec.com
m: +49 160 98758776
w: www.etonec.com

Dr. Jonas Gross is Head of Digital Assets and Currencies at etonec and Chairman of the Digital Euro Association (DEA). Jonas holds a PhD in Economics from the University of Bayreuth, Germany. His main fields of interest are central bank digital currencies, stablecoins, cryptocurrencies, and monetary policy. Further, Jonas is co-host of the German podcast "Bitcoin, Fiat, & Rock'n' Roll" and member of the expert panel of the European Blockchain Observatory and Forum.

Johannes Sedlmeir
SnT, University of Luxembourg

e: Johannes.Sedlmeir@uni.lu
m: +49 157 51618033
w: wwwfr.uni.lu/snt/research/finatrax

Johannes Sedlmeir is a research associate at the Interdisciplinary Center for Security, Reliability and Trust (SnT), University of Luxembourg. He focuses on identifying challenges of blockchain (DLT) adoption in organizations, e.g., regarding energy consumption, performance, and the handling of sensitive information, and designing, implementing, or evaluating solution approaches. He also applies novel cryptographic technologies like zero-knowledge proofs for scalability and privacy enhancements in these areas, as well as in related topics like digital identity (SSI) and payment (CBDC) infrastructures.

Simon Seiter
Hauck Aufhäuser Lampe Privatbank AG

e: Simon.Seiter@hal-privatbank.com
m: +49 69 21611183
w: www.hal-privatbank.com/en/asset-servicing/digital-assets

Simon Seiter is heading the newly created Digital Assets division at Hauck Aufhäuser Lampe and responsible for the development of all digital asset initiatives and products. Previously, he was in the same role as Head of Digital Assets at Deutsche Börse AG, before that at Commerzbank. For years, he has also been advising a number of international blockchain committees, including the World Economic Forum, the German Banking Association and Global Digital Finance.

About etonec

etonec builds blockchain-based payment solutions at the intersection of payments, banking, and digital assets. What makes etonec unique is that it combines decades of global experience in payments and traditional finance, e.g., from working for PayPal, with insights in emerging technologies and concepts gleaned from working for leading crypto projects, such as the Libra/Diem Association. The etonec team is comprised of leading experts in digital currencies, stablecoins, central bank digital currencies (CBDCs), cryptocurrencies, self-sovereign identity (SSI), and in further innovative topics, such as the Bitcoin Lightning Network, Zero-Knowledge Proof Technologies, and Crypto-Backed Lending - topics that will heavily impact the future of payments. Etonec makes use of a global network of high-quality experts to help leading global brands leverage blockchain-based payment solutions and digital assets.

About Hauck Aufhäuser Lampe

HAUCK AUFHÄUSER LAMPE (HAL) can look back on 226 years of tradition. The bank emerged from the merger of three private banks rich in tradition: Georg Hauck & Sohn Bankiers in Frankfurt am Main, founded in 1796, Bankhaus Lampe, founded in Bielefeld in 1852, and Bankhaus H. Aufhäuser, on the market in Munich since 1870. The two houses Georg Hauck and Bankhaus H. Aufhäuser merged in 1998, Bankhaus Lampe was added in 2021. HAUCK AUFHÄUSER LAMPE sees itself as a traditional and at the same time modern private bank.

The private bank focuses on the four core business areas of private and corporate banking, asset management, asset servicing and investment banking. The focus of its business activities is on comprehensive advisory services and asset management for private and corporate clients, asset management for institutional investors, comprehensive fund services for financial and real assets in Germany, Luxembourg and Ireland. In addition, Hauck Aufhäuser Lampe offers research, sales and trading activities specializing in small and mid-cap companies in German-speaking countries as well as individual services for IPOs and capital increases.

About Mina Foundation

The Mina Foundation is a public benefit corporation serving the Mina Protocol, the world's lightest blockchain. The Foundation supports the protocol and its community by issuing grants to third parties that make significant contributions and by maintaining & managing community and network health. Board members include Former Executive Director at ZCash Foundation Josh Cincinnati, Harvard Business School Finance Professor and Coinbase Advisory board member Marco Di Maggio, VP of Engineering at Interchain GmbH and Tendermint developer Tess Rinearson, Mina Foundation General Counsel Joon Kim, and Mina Foundation CEO Evan Shapiro.

About SnT, University of Luxembourg

The Interdisciplinary Centre for Security, Reliability and Trust of the University of Luxembourg conducts research in information and communication technology with high practical relevance to create socio-economic impact. In addition to long-term, foundational research, SnT engages in demand driven collaborative projects with industry and the public sector. For instance, within the FINATRAX research group, these activities include topics in applied cryptography and blockchain, the digital transformation in the financial and energy industry, and general management information systems.

The authors thank Kurt Hemecker, Philipp Kant, Jonathan Knoll and Brian McKenna for their great feedback that were essential for this research.

References

Biryukov, A., & Tikhomirov, S. (2019). Deanonymization and linkability of cryptocurrency transactions based on network analysis. In *European Symposium on Security and Privacy* (pp. 172-184). IEEE.

Butijn, B. J., Tamburri, D. A., & Heuvel, W. J. V. D. (2020). Blockchains: a systematic multivocal literature review. *ACM Computing Surveys* (CSUR), 53(3).

Coinmarketcap (2022). Today's cryptocurrency prices by market cap, *https://coinmarketcap.com/* (access: September 10, 2022).

ECB (2021). ECB digital euro consultation ends with record level of public feedback, *https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210113~ec9929f446.en.html* (access: September 10, 2022)

Gailly, N., Maller, M., & Nitulescu, A. (2021). SnarkPack: Practical SNARK aggregation. *https://eprint.iacr.org/2021/529.*

Gross, J., Sedlmeir, J., Babel, M., Bechtel, A., & Schellinger, B. (2021). Designing a central bank digital currency with support for cash-like privacy. *https://ssrn.com/abstract=3891121* (access: September 10, 2022).

Goldreich, O., Micali, S., & Wigderson, A. (1986). How to prove all NP statements in zero-knowledge and a methodology of cryptographic protocol design. In *Conference on the Theory and Application of Cryptographic Techniques* (pp. 171-185). Springer.

Kiayias, A., Kohlweiss, M., & Sarencheh, A. (2022). PEReDi: Privacy-enhanced, regulated and distributed central bank digital currencies. *https://eprint.iacr.org/2022/974* (access: September 10, 2022).

Maurer, U. (2009). Unifying zero-knowledge proofs of knowledge. In *International Conference on Cryptology in Africa* (pp. 272-286). Springer.

Sandner, P., Gross, J., Drozdov, I. (2020). Will blockchain replace clearinghouses? A case of DVP post-trade settlement. *https://www.forbes.com/sites/philippsandner/2020/12/02/will-blockchain-replace-clearinghouses-a-case-of-dvp-post-trade-settlement/* (access: September 10, 2022).

Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets.*

Tomescu, A., Bhat, A., Applebaum, B., Abraham, I., Gueta, G., Pinkas, B., & Yanai, A. (2022). UTT: Decentralized ecash with accountable privacy. *https://eprint.iacr.org/2022/452* (access: September 10, 2022).

Wüst, K., Kostiainen, K., Delius, N., & Capkun, S. (2021). Platypus: A central bank digital currency with unlinkable transactions and privacy preserving regulation. *https://eprint.iacr.org/2021/1443* (access: September 10, 2022).

Yahoo Finance (2022). German authorities shut down darknet marketplace Hydra, seize 500 BTC, *https://financeyahoo.com/news/german-authorities-shut-down-darknet-090444781.html* (access: September 10, 2022).

Zapico, A., Buterin, V., Khovratovich, D., Maller, M., Nitulescu, A., & Simkin, M. (2022). Caulk: Lookup arguments in sublinear time. *https://eprint.iacr.org/2022/621* (access: September 10, 2022).