SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal
of Cryptocurrency Research

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Blockchain Privacy and Self-Regulatory Compliance: Methods and Applications

Vladimir Popov[1*], Andrew Gross[2], Mike Krupin[3] and Georgi Koreli[4]

[1]240 Richmond St W, Toronto, Ontario Toronto, Canada. E-mail: zkbob@proton.me
[2]240 Richmond St W, Toronto, Ontario Toronto, Canada. E-mail: zkbob@proton.me
[3]240 Richmond St W, Toronto, Ontario Toronto, Canada. E-mail: zkbob@proton.me
[4]240 Richmond St W, Toronto, Ontario Toronto, Canada. E-mail: g@hinkal.pro

Article Info

Volume 4, Issue 1, June 2024
Received : 24 January 2024
Accepted : 16 May 2024
Published : 05 June 2024
doi: 10.51483/IJCCR.4.1.2024.64-78

Abstract

New advancements in zero-knowledge proof construction, including improvements in user experience, have made blockchain-based privacy applications more accessible than ever. However, additional measures are required to balance the needs of regulators, the basic privacy rights of users, and the constant threat of bad actors. To address these issues, privacy protocols can introduce features designed to increase transparency, encourage compliance, and prevent illicit use. In this paper, current privacy-preserving methods (privacy pools) are explained along with compliance measures designed to prevent illicit usage. These measures are divided into three broad categories: general restrictions, such as transaction limits, deposit quarantine, and geoblocking; selective disclosure, such as privacy-preserving KYC, proof of innocence, and opt-in reporting; and threat identification and prevention, including AML wallet screening. Each of these methods are described in detail along with examples of three privacy-preserving protocols (Hinkal, RAILGUN, and zkBob) which utilize varying combinations of these methodologies to achieve privacy informed by self-regulatory compliance.

Keywords: *Blockchain, Privacy protocols, Transaction limits, Hinkal, RAILGUN, zkBob*

1. Introduction

Since the inception of the first blockchain-based payment protocols, the main value proposition has been the idea of self-sovereign currency. Privacy, and specifically confidentiality, has typically been treated as a secondary feature. The original Bitcoin paper (Satoshi Nakamoto, 2008) suggested that using one-off anonymous addresses was sufficient for any use case. However, using Bitcoin addresses for confidential purposes is very hard to implement in practice since it requires additional communication between parties prior to any transaction.

[*] *Corresponding author: Vladimir Popov, 240 Richmond St W, Toronto, Ontario Toronto, Canada. E-mail: zkbob@proton.me*

Researchers, developers and blockchain users acknowledge that a lack of basic privacy is a problem (Buterin *et al.*, 2023), and significant progress has been made in recent years to promote privacy applications on the blockchain. New applications have combined private token transfers with a convenient user experience to make privacy easier for regular users. Rapid advancements in the field of zero-knowledge proof construction (Miers *et al.*, 2013) have made these applications more convenient and effective.

However, privacy enhancing features still require additional steps during onboarding, resulting in longer waiting times, poor mobile performance, and other difficulties. Furthermore privacy-enhanced application use is discouraged by government agencies like FinCen (Financial Crimes Enforcement Network, 2023) and amplified by a few additional factors:

- Most current financial services that require privacy (see GLBA (Federal Trade Commission, n.d.), SOX (U.S. Government Publishing Office, 2001), PCI DSS (PCI Security Standards Council, n.d.)) have never been deployed to decentralized networks despite all of the expectations and efforts. Some leaders in the traditional fiat payments business have attempted to create hybrid products that present themselves as crypto-friendly, but in fact they are essentially merchants receiving crypto payments (Visa, 2022).
- Most current users are satisfied with the level of privacy in blockchain networks due to the fact that their address is not linked to their real-life identity (Authentic8, 2022).

These additional hurdles, combined with a popular fallacy about a lawful user having nothing to hide, have discouraged privacy protocol adoption by a wider audience. As a result, the current user base is mostly made up of either developers, privacy enthusiasts, or users who indeed deliberately try to hide the source or the destination of funds for unlawful reasons.

The latter group of users, despite being relatively small, pose a substantial risk not only for the privacy-enhanced DApps and their developers and community but potentially to all crypto currencies and tokenized assets in circulation (Berwick and Talley, 2022).

To promote more widespread usage of privacy-enabled protocols, viable solutions are required that can resolve contradictions between regulations (Shlomit Azgad-Tromer *et al.*, 2023), the basic need for privacy, and the constant threat of bad actors. Measures which address these issues include:

1. Increasing transparency.
2. Enabling opt-in reporting and selective disclosure within private applications.
3. Making it more difficult for bad actors to use privacy protocols.

In this paper we explore specific features implemented by several web3 privacy protocols and investigate how these features affect both attractiveness of the application for end-users and their efficacy to prevent illicit usage.

2. Background

The primary distinctive feature of decentralized protocols based on blockchain technology is the verifiability of state transitions. Anyone can independently verify that changes in the state of the system have occurred correctly and according to the rules of the protocol. This ability has enabled new ways of coordination between entities and is particularly well suited for modeling financial relationships (Schaer, 2021). Through its short history we have seen the rise of peer-to-peer payments, lending, and tokenized assets usage among other innovations.

Unfortunately, early usage was largely driven by low levels of control compared to traditional financial services, resulting in the rise of several illegal applications (see Silk Road (Jones, 2016), BTC-E (Europol, 2021) and others). However, as is the case with most neutral technologies that can be used in multiple contexts, growing attention from both bad actors and regulators has led to broader engagement and the emergence of more valid and legal use-cases, such as Visa making settlements in USDC (Visa, 2023).

The verifiability and immutability of blockchain has been both a blessing and a curse. Whereas for some financial activities privacy may not seem like a critical requirement, in other cases a completely public financial history poses certain risks including:

1. Tracking and illegal extortion of digital assets from wealthy individuals due to easy detection of wallets containing large amounts of funds and a low chance of the stolen funds being retrieved after robbery (Browne, 2021; NL Times, 2020).
2. Unauthorized access to salary information or payments made as part of contractual agreements can be used for adversarial behavior by competitors.
3. Leaking details of a trading deal enables front-running and other adversarial techniques (Eskandari *et al.*, 2019).
4. Unwarranted access to private information including transaction history is protected even from the government itself in some countries (Belonick, 2020).
5. Public access to financial data is a potential breach of data protection policies such as GDPR.

Traditional financial services including banks, payment providers and investment brokers are required to keep their clients' data secure from adversaries (see PCI DSS, GLBA). The mere idea of some centralized entity being solely responsible for owning and securing PII has its obvious flaws which has been proved by multiple private data leaks (Federal Trade Commission, 2022).

It could be argued that the shift from traditional financial services to decentralized services for a broader audience is nearly impossible unless the same level of data protection or better is guaranteed.

2.1. Privacy-Preserving Technological Advancements

Recent technological advancement in decentralized applications allow users to forgo unnecessary trust in service providers: not only can the value transfer occur in a permissionless manner, but the data about both balances and transactions history now can be owned solely by the individuals involved in the transaction (Zero Coin, n.d.; Jedusor, 2016).

Properties inherent in the blockchain don't allow transactions to be hidden natively. Several approaches have been adopted to obfuscate or hide information that may lead to linking a particular transaction to an individual or to group the transaction by involved parties:

- Transactions from different parties are aggregated before posting to blockchain with their sources and destination shuffled (Bitcoin Wiki, n.d.);
- The transaction originator can be hidden by utilizing a special type of electronic signature that allows adding a limited set of decoys, providing plausible deniability (Bitcoin Wiki, n.d.);
- The transaction destination, asset type and amount can be hidden using asymmetric encryption or one-way hash functions;
- All balances in the system can be described as an opaque commitment to the global state using a one-way hash function and the only publicly available transaction data are the proof of valid state transition and a one-off nullifier that prevents a double spend.

The latter approach, powered by zero knowledge proofs (Parno *et al.*, 2013), has become increasingly popular due to its inherent composability with smart contracts, low requirements for interactivity between participants, and extendability. An instance of this approach is often called a "pool", because all the funds from deposits are pooled together so that a withdrawal is not connected with any particular deposit transaction, thus breaking a logical link between the source and destination of the funds.

2.2. How Private Pools Work

On-chain privacy is difficult to achieve on the blockchain as state transitions must be publicly verifiable. Verification is of utmost importance and it must be non-interactive, lightweight, and as optimized as possible for verifiers to keep up without relying on excessive computational resources. Considering these requirements, the most popular current solution involves using zero-knowledge proofs (ZKPs) to prove a transaction has occurred without disclosing specific information about that transaction.

In general, ZKPs allow trustless outsourcing of some computational tasks to a third party. In this context, a blockchain node verifying transactions "outsources" resource-heavy tasks or those requiring access to sensitive data. With private pool data, computations are performed locally by the transaction initiator. During this process, an additional metadata object is generated. This additional metadata is called a proof, and it can be used to verify the integrity of the performed operations alongside the designated public arguments (sometimes including calculations output). All intermediary values and secret inputs are never disclosed, and cheating is computationally hard.

In a typical blockchain transaction, a simple token transfer has the following constraints:

1. The source of funds is one or more outputs which exist among all of the unspent outputs.
2. The sum of the created outputs balance is less than or equal to the sum of source outputs.

To create a private pool instead of a public list of unspent outputs, we model a tree-like structure where the leafs are transaction data hashes stored off-chain. These hashes are grouped together and recursively hashed using a cryptographically secure hash function until there's a single value left—the root. This allows checking the inclusion of a note indirectly—by verifying that there indeed exists a path in the tree which contains only hashes and lead from the specified leaf to the root. At the same time all of the values are opaque for the verifier and there is no way to deduce anything about a specific leaf.

This improvement alone doesn't create privacy, as correctness of hashing can only be checked using the plain text data. By using ZPKs, the individual can perform hashing, check the tree path, generate a new root and even verify a signature locally on their own device without leaking any sensitive information like the secret key, notes spent, and notes created. This way the verifier (blockchain node) can be assured that the transaction is indeed valid, authorized by the funds owner and that the new root is also correct.

Another aspect of this process is that every owner's own state must be nullified each time a transaction is made to prevent multiple usage of the same funds. This is done by publishing a special deterministic nullifier that corresponds to the current state of the owner's balances. This is also somewhat useful for selective disclosure since the data reported by the owner can be checked against the nullifiers (see Opt-in reporting 3.2.1).

An additional privacy safeguard for transaction handling is the use of a relayer, which helps users to avoid direct interactions with blockchain nodes. Direct interactions require a fee (gas) which can consequently link different transactions by the same user. The relayer serves as an intermediary, sending transaction data and processing gas fees in an anonymous way. Theoretically relayers are able to enforce individual policies, for example preventing transactions containing suspicious deposits from being processed (Proof of Innocence 3.2.3).

2.2.1. Stealth Addresses

To prevent different transfers to the same entity, which insinuates a connection between transfers, an additional feature such as randomized addresses (or stealth addresses) is implemented in most private pools. This feature allows users to create multiple addresses that look completely random but in fact correspond to a single private key. To extend the usability of stealth addresses, a user can register a single canonical address and new addresses can be generated by a sender for each transaction.

2.3. Illicit Usage Ramifications

One of the most prominent applications to utilize privacy-preserving technology is Tornado Cash, where thousands of transactions were processed each month despite comparatively high fees. Unfortunately, Tornado was also used by a well known hacker group (U.S. Department of the Treasury, 2022) to hide the source of the stolen funds. On one hand this proves that the technology is indeed neutral and permissionless and its effectiveness as a privacy tool is in line with expectations. On the other hand, these funds obtained through illicit activities contaminated the pool by mixing with other users' funds in an irreversible way. As a result the hackers gained plausible deniability by sharing the responsibility with law-abiding users.

Similar incidents have happened across multiple projects, tarnishing the reputation of the crypto currency industry and resulting in a response from different U.S. agencies. FinCEN's proposal for extended reporting (Financial Crimes Enforcement Network, 2023) recounts several known cases of money laundering and also recognizes how difficult it is to assess the share of legitimate usage.

To thwart potential criminal activity, the FinCEN proposal recommends that financial institutions such as banks or other money service providers collect a thorough report for every transaction. This report should contain an individual's IP address, full name, ID, tax ID and narrative (presumably proving the licit nature of source of the funds).

Implementing these types of measures is costly and would radically impact current applications. Estimates in the same document suggest this legislation would impact tens of thousands of entities just in the U.S. and cost hundreds of millions of dollars to enact. This would also likely lead to eventual censorship by regulated entities, and threaten efforts to create decentralized financial applications for regular users.

New approaches are required to support privacy and responsible use of blockchain-based financial applications.

3. Self-Regulatory Compliance Methodologies

Blockchain technologies allow for the possibility of a self-regulated and proactive approach to creating and using financial applications. To protect users, "private by default" is a necessary feature (just as with a traditional bank account). However, measures are also needed to prevent use and abuse by bad actors. The following methods offer different ways to protect privacy and the integrity of the protocol, and may be combined in various ways to suit different use cases.

We classify potential self-regulatory measures in the following way:

1. General restrictions: transactional limits, deposit quarantine, geo-blocking.
2. Selective disclosure: privacy preserving KYC, opt-in reporting, proof of innocence.
3. Threat identification and prevention: AML wallet screening.

3.1. General Restrictions

General restrictions may be introduced for all users to influence broad-level usage and proactively prevent misuse. These mechanisms are designed to discourage illicit usage by making certain operations difficult within the context of transfer amounts or based on geographic location. They do not tend to limit legitimate use cases though they can make some processes more inconvenient for regular users.

3.1.1. Transaction Limits

Exchanges and other applications which hold crypto currency funds are enticing targets for hackers. In 2022 alone, "a staggering $3.9 billion was looted from DeFi platforms" (Berkovitz and Pattnaik, 2023) resulting in substantial losses for protocols and individual users.

Once funds are stolen, hackers attempt to obfuscate or withdraw as quickly as possible, before funds can be earmarked as stolen or frozen by various applications or services. Hackers will often attempt to offload large sums (in the millions of dollars) into privacy applications to try and quickly mix their stolen funds with other funds contained in the privacy protocol.

Institutional policies in the financial sector can be used as a general guide for enacting limits. Most institutions in different jurisdictions have implemented risk-based AML practices focused on transaction amounts. For example, following the regulations by the U.S. Treasury, any suspicious transaction above $2,000, or any transaction above $5,000, must be reported (Electronic Code of Federal Regulations, n.d.).

In the context of digital assets these countermeasures often include banning certain addresses and freezing funds, then attempting to identify devices and individuals involved in the illegal activities. In these cases the bad actor has a natural competitive edge which comes from lagging response from developers, users and agencies.

Diminishing this lag time should be one of the goals for any financial application. A simple prevention technique is the introduction of transaction limits on deposits to privacy-enhancing applications. For example, the zkBob privacy application follows the Bank Secrecy Act (BSA) guidelines which require reporting of more than $10,000 USD for individual daily deposits (Office of the Comptroller of the Currency, n.d.). zkBob simply prevents any individual transitions over $10,000 USD to comply with this guideline. In addition, daily limits are enforced for the entire protocol ($300,000 USD per 24 hours) to prevent bad actors from splitting funds into many different wallets and depositing smaller amounts from each.

Universal limits are simple to enact but can limit the utility of the application. A progressive limits scale that raises limits for known users (such as using some form of KYC clearance or address whitelisting) may also be explored as a more nuanced approach to transaction limits.

3.1.1.1. Deposit Quarantine

In addition to limits, a protocol may quarantine inbound deposits for a period of time sufficient to determine whether these funds were derived from illegal activities. Since hacked funds are often moved to privacy protocols immediately following a hack, the wallets involved may not yet be identified through any threat detection services (3.3).

This measure on its own doesn't prevent processing of a bad deposit; rather it should be implemented alongside Proof Of Innocence (3.2.3) so that despite the inbound transaction being held up in process, other legitimate users are able to decouple their funds from this particular deposit.

3.1.2. Geoblocking

Geoblocking restricts access to online content based on the user's geographical location (Yu, 2019). Geoblocking techniques are employed by many blockchain applications to discourage usage (DeMichele, 2019) of certain tokens or products and comply with regulators' requirements related to a specific region.

When a user visits a Geoblocked application using an IP address from a restricted area, the user is typically presented with a message informing them that they are not allowed to access the app from their region. While a savvy user can circumvent this restriction rather easily, they do so in an informed way. This shifts the burden of responsibility to the user, who makes an informed choice to violate the application's terms and conditions and proceed with usage (similar to someone who chooses to trespass on property where there is a clear 'no trespassing' sign). Depending on the jurisdiction, usage of the site may or may not be deemed illegal by the authorities.

Geoblocking is generally not effective as a primary means of deterrence, and is often maligned in the community as antithetical to an open-access financial system. However, it is a tool for informing users of their risks and providing up-to-date compliance policies to users based on their region.

3.2. Selective Disclosure

Selective disclosure allows users to share essential information without providing any unnecessary or compromising details. For example, it may be sufficient to provide proof that a user has passed KYC requirements without providing the details themselves. There are several different ways to implement selective disclosure within privacy-preserving applications.

3.2.1. Opt-in Reporting

Users are given the option to provide some information about their transaction history and account balance in an ad-hoc manner. A report with intrinsic verifiability can be created and the integrity of the report is protected by the protocol itself. The report can take different forms:

- A short proof that a particular user has never interacted with a tainted deposit (Chainway Labs, 2023).
- A long form report that gives information about user deposits, withdrawals, transfers and current accounts.

An advantage of the short form is that it can be checked during transaction processing. With the RAILGUN protocol, this has evolved into a transaction checking constraint, so if a user is unable to produce a proof that their deposit is not in a black list, then there is no additional privacy granted from using the application, since "bad" and "good" deposits are bifurcated and consequently the "bad" withdrawals become also distinguishable on the contract level (RAILGUN Project, 2023).

While this may be adequate for most use cases, a long form report may still be required considering the current regulatory environment. One way to tackle this is to let users share a viewing key, which is used in asymmetric key exchange between sender and receiver, during a transaction flow (RAILGUN, n.d.).

Alternatively the protocol can provide a dedicated viewing key (Electric Coin Company, 2020) which is used to hide all of the information while allowing a trusted party to decrypt and check everything.

The main downside of viewing keys is the lack of flexibility, i.e., after the user has shared it, all future transactions for this account can also be decrypted. This perpetual access contradicts the "private by default" ethos. Rather than direct key sharing there are ways to disclose the plain text data for a limited period of past time along with a proof of it's integrity which proves that:

1. There were no omitted records.
2. The final balance is indeed the result of summation of all of the transactions in the report.

Processing this type of report uses information from the Merkle tree(s) to verify accuracy. The current standard for private transfer application state implies storing all of the accounts and transactions in a single or multiple Merkle Trees (1988) where the root of the tree authenticates the node that is used as a source of transaction. This is done in a zero-knowledge fashion, meaning a particular node is not known to anyone, yet it can be verified that the source of the transaction is indeed in the tree.

To check a report, the sender can publish a nullifier which is a result of hashing of some source-related data. A verifying party is able to link the opaque on-chain nullifiers with the plain text data and check that the report is indeed genuine.

As a general rule, compliance reports can be generated for users within privacy applications to include their private transfers and metadata associated with these transfers. It then becomes their responsibility to share this report with the appropriate authorities to ensure legal operations and submit tax information while following reporting framework guidelines (OECD, 2022) relative to their jurisdictions.

3.2.2. KYC

KYC, or "Know Your Customer," denotes the responsibility of a financial service to conduct specific identity and background verifications on its clients before granting them access to its products or platforms. KYC practices can be traced back to the Money Laundering Control Act of 1986 (Cornell Law School Legal Information Institute, 1986). Since then, KYC has undergone substantial expansion through successive regulations, including those enacted in 1988, 1992, 1994, 1998, 2001, and 2004 in the USA. This continuous evolution reflects a concerted effort to prevent both money laundering and the financing of terrorist activities.

KYC practices are common throughout the financial and investment industries in order to determine and mitigate different risks. This process includes customer identification using government-issued ID, sometimes accompanied with a photo, and some document confirming the customer's address of residence. The ubiquity of this policy is due to the conflicting incentive of bad actors to avoid revealing their true identity and physical location to prevent legal repercussions.

In the context of privacy enhanced protocols for token transfers, using KYC in a traditional manner defeats the purpose of the protocol. But there are some hybrid solutions that allow users to transact privately and at the same time make some guarantees about their identity. The main challenge is the lack of standardization and the gap between existing solutions and what is needed for on-chain applications.

The most popular current method is to delegate KYC to a third party who is responsible for storing and securing Personal Identifiable Information (PII). During a transaction, the service provides proof that KYC has been passed; no additional information is shared.

KYC can also be implemented using soul-bound tokens (SBT). Soul-bound tokens are non-transferable, non-fungible assets that contain certain credentials (Ohlhaver *et al.*, 2022). A SBT can be issued by a trusted authority for a specific address as a result of successfully passing the KYC process. The token can be checked to determine whether this customer is eligible for a certain transaction limit or able to make a transaction at all. The downside of this solution is that SBTs are inherently linked with native addresses and can be practically checked only during deposits and withdrawals, not during internal transfers.

3.2.2.1. Privacy Preserving KYC

A more advanced approach entails using "verifiable credentials" that can be issued for a specific pool account and associated with a specific key pair. A verifiable credential might be stored locally on a customer's device or might be an extension of an SBT stored on-chain where the issued token includes an identifier associated with the customer's account (e.g., a hash of a stealth canonical public key or something similar) and a provider's signature that attests to a successful KYC procedure. This credential can be later checked during any outbound transaction in a privacy preserving manner; the customer can provide proof that she knows a certified KYC provider's signature for the account being used without disclosing their address at all. Overall, this solution provides more complete privacy at the cost of additional complexity within the solution itself and additional actions for users.

3.2.3. Proof of Innocence

Proof of innocence relates to the aforementioned proof that a particular user has never interacted with a tainted deposit. It is possible to choose an arbitrary subset of all transactions by a user that contain only those deposits checked for licit source and create an additional proof of association.

Such proofs are blinded in the same way as regular transaction integrity proofs and do not reveal additional user or transaction data, but allow counterparties to gain additional assurance without requiring a full viewing key. Using specialized software which can publish proofs off-chain, counterparties can also check the proof of any funds received.

As malicious on-chain activity is publicly visible, lists of undesirable activity or actors can be constructed as input data to prove against. Input data can be arbitrary and tied to users' jurisdictions. For example, addresses on the Office of Foreign Assets Control Specially Designated Nationals List (2024) can be used to filter deposits made from blocked addresses.

Furthermore independent wallet providers can make the filter condition more strict and add any other list as a default list for all users shielding funds to prove against, effectively bifurcating out the anonymity set. This means that without a valid proof, any malicious actors receive no privacy benefit from using the system. List providers can be maintained by anyone and can accompany forensic data or even community maintained data from blockchain security experts.

This solution is recognized by the developer community (Buterin *et al.*, 2023) as one of the most promising although it has few downsides that should be addressed:

- This approach must be recognized as effective by government agencies and businesses. This is difficult to achieve because of its complexity and lack of incentive for regulators. This issue could be resolved if either broad adoption occurs (which is unlikely due to the same regulation) or a corresponding standard is created by the developer community which can be later used in negotiations with regulators.
- A new role of association set provider is introduced that is entitled to broadcast the current recommendations for the association set identifier and it is unclear whether the association set provider takes any responsibility for the service quality and availability.
- It is very unlikely that regular users would review the actual association sets and hence could be misled.

3.3. Threat Identification and Prevention

Screening methods are important to proactively prevent illicit funds from ever entering a protocol. The primary method used today involves AML checks from established providers and agencies.

3.3.1. AML Checks

Wallet screening checks stand as a crucial compliance measure, playing a pivotal role in restricting access to the protocol for malicious actors and effectively preventing the ingress of illicit funds. Diverse data providers extend such services to assist decentralized finance (DeFi) protocols in combating fraud, money laundering, and financial crime. The screening tool functions as a preventive measure, averting interactions with illicit crypto assets by scrutinizing wallets against various sanctioned lists from entities such as the OFAC, EBA, FCA, FINTRAC, OCC, and others. Given the heightened regulatory scrutiny of private protocols, especially in the aftermath of the Tornado Cash incident (U.S. Department of the Treasury, 2022), it is imperative to remain abreast of the latest changes to sanctions lists, with a particular focus on updates from the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). This vigilance is crucial for ensuring ongoing compliance within the evolving regulatory landscape.

Popular service providers for on-chain intelligence and forensics currently include Elliptic, TRM Labs, Chainalysis, Crystal Blockchain, BitRank, CipherTrace.

The mechanics of these services are quite similar; they index on-chain data and allow customers to query chosen wallet risk levels based on its counterparties, history, external markup sources, community feedback, etc. It works quite well in most cases but has a few downsides:

- Indexing takes time, so the attacker has a chance of making a deposit while the information about their wallet has not been yet added to the database (could be mitigated by introducing limits and delays for deposits and withdrawals 3.1.1 Transaction Limits).
- Sophisticated attackers try to obfuscate their trace by using multiple cross-chain bridge transactions which makes it much harder to untangle. At the time of writing cross-chain indices are very rare and not effective enough.
- Centralized services do not fit very well with decentralized protocols because they impose additional censorship risks and prevent decentralizing crucial architectural components.

4. Privacy Protocols Overview

Several active blockchain privacy protocols are using these methods to protect user privacy while providing compliance features for users and regulators. The three protocols below each take a different approach, using a combination of the methods described above within their solutions.

4.1. Hinkal

4.1.1. Overview

Hinkal is a zk-protocol enabling the execution of end-to-end strategies in decentralized finance (DeFi) with complete on-chain privacy. Hinkal allows institutional and retail users to make confidential transactions on popular decentralized applications, allowing the originator wallet and asset values to remain hidden. One of the primary use cases for Hinkal is copy trading prevention, so that no one can trace user wallets and assets. This allows users to swap, stake, and provide liquidity in a fully private environment. The application also allows private liquidations and token accumulation where users can import any token and liquidate privately without going to the OTC desk. The technology can be customized for each fund, integrating the specific applications they use for strategies. Hinkal is in production on 6 chains and currently offers 6 highest volume/ tvl apps.

4.1.2. Compliance Mechanisms

4.1.2.1. Privacy Preserving KYC(B)

Hinkal accepts KYC and KYB attestations from various providers including Coinbase and Binance (KYC 3.2.2). If the user has already passed KYC(B) with any of these solutions, they can directly mint an access token and use the protocol. Otherwise, they can pass verification by choosing any of the solutions accepted. The user provides required documents such as government issued ID, photo and others in accordance to local legislations and the provider's requirements. A special identifier, associated with the pool account, is specified automatically (Privacy Preserving KYC 3.2.2.1). The user can deposit and use funds only after providing a KYC(B) attestation. Proving and verifying KYC(B) attestation ownership requires some additional technical steps that are fully automated and do not lead to degraded performance.

4.1.2.2. AML

Hinkal uses real-time protection and wallet screening from Hexagate (AML Checks 3.3.1).

4.2. RAILGUN

4.2.1. Overview

RAILGUN is a privacy tool on Ethereum, BSC, Polygon, and Arbitrum. Apart from asset transfer it allows different DeFi integrations. Users receive a private '0zk' address that is generated from an Ethereum private key to which they can send funds and use to interact with the chain.

The main use-cases are protected trading, private payroll, censorship resistance and countermeasures against services that use on-chain data to compromise user's identity (Arkham, Nansen). The RAILGUN tech stack allows the community to run their own relayers so that users make a choice based on fees or other preferences.

4.2.2. Compliance Mechanisms

4.2.2.1. Proof of Innocence

(3.2.3 Proof of Innocence) RAILGUN has a live implementation of Proof of Innocence. Currently, all independent RAILGUN integrated wallets use the OFAC SDN list as input data, meaning addresses on and connected to that list are unable to enter the anonymity set. Data providers for Proof of Innocence will expand over time to cover additional scenarios.

4.2.2.2. OFAC Screening

The OFAC SDN list is the default data input for all wallets using the RAILGUN Proof of Innocence implementation.

4.2.2.3. Viewing Keys

RAILGUN supports viewing keys such that users can reveal their whole transaction graph to a third party. For example, if a CEX compliance team, regulatory entity, or any other counterparty wants to gain insight into a user's RAILGUN transactions, a viewing key can be shared that decrypts information.

4.2.3. Performance Analysis Regarding Self-Compliant Measures

RAILGUN Proof of Innocence went live in November 2023 and since then has generated tens of thousands of proofs. There has been no noticeable impact on performance of RAILGUN in terms of resources and transaction throughput. There is a 60 minute window after shielding where a user's only available action is unshielding back to the original public address, and this has not impacted performance in any way.

Contributors are working on an explorer for Proof of Innocence such that users can see the blinded proofs being generated using a frontend. This explorer displays what lists a transaction has been proved against but does not contain any special insight into the transaction and privacy is maintained throughout.

4.3. zkBob

4.3.1. Overview

zkBob is a privacy-centric application focused on anonymous payments and transfers. Use cases include payroll, donations, and small payment transfers between individual users. The DApp allows users to interact with the pool contract and make interactive deposits into their own accounts, withdrawals and transfers between accounts. Additionally a user or any external contract can initiate a deposit into a specific account through a dedicated smart contract. The protocol follows the aforementioned privacy pool architecture (2.2 How private pools work).

zkBob pools are deployed on different chains and every pool has a single supported token: Polygon (USDC), Optimism (USDC and ETH pools) and Tron (USDT) chains. Metrics such as the pool size and transaction amounts are available at Dune Analytics dashboard (Dune Analytics, n.d.).

4.3.2. Compliance Mechanisms

4.3.2.1. Daily Limits

Mutitiered limits system (3.1.1 Transaction Limits) constrain both individual users and the protocol in general to make it impossible to move large amounts of funds unless KYC is passed. The registration process is permissionless so anyone can create an account and receive an incoming transfer or make a deposit within a specified default limit. A user may create multiple accounts but there are also limits that constrain the pool size and turnover.

The limits are mainly tailored to accommodate payroll use cases, where known businesses (KYB) can unlock higher limits.

Table 1: Limits for zkBob USDC Pools on Polygon, Optimism (Denominated in USDC)

	Default Tier	KYC Tier	KYB Tier
Single deposit	10,000	20,000	100,000
Daily user deposit	10,000	20,000	100,000
Daily deposit sum	300,000	300,000	300,000
Daily withdrawal	300,000	300,000	300,000
Pool size	2,000,000	2,000	2,000,000
Single direct deposit	1,000	1,000	1,000
Daily direct deposit	10,000	10,000	10,000

Table 2: Limits for zkBob Ether Pool on Optimism (Denominated in Ether)

	Default Tier	KYC Tier	KYB Tier
Single deposit	5	10	50
Daily user deposit	5	10	50
Daily deposit sum	150	150	150
Daily withdrawal	150	150	150
Pool size	1000	1000	1000
Single direct deposit	5	10	50
Daily direct deposit	5	10	50

4.3.2.2. Optional KYC

Optional KYC is based on Soul Bound Tokens that are issued for customers' addresses by a third party (KnowYourCat) on the grounds of successful KYC on the Binance exchange (Binance Account Bound Token). Transaction limits are automatically increased for addresses that own a corresponding KYC token.

4.3.2.3. EOA Wallet Screening (AML Checks)

All wallets involved both in deposits and withdrawals are screened using TRM Labs wallet screening service (3.3.1 AML Checks). TRM Labs allows customers to fine-tune their own risk engine that categorizes risk level based on a specific flag of a wallet and whether this particular wallet:

- Was marked as a first-hand participant in illicit or suspicious activities ("ownership" risk).
- Has had direct interaction with a wallet with a specific risk level ("counterparty" risk).
- Has had an interaction with a wallet with a specific risk level through several transactional hops ("indirect" risk).

The current configuration restricts protocol access for all externally owned account (EOA) wallets marked as involved in sanctions, terrorist financing, human trafficking, CSAM, special measures, sexual exploitation or those who are marked as a counterparty to a wallet involved in a previous list. This strategic approach not only discourages undesirable actors but also serves as a preventive measure against the inflow of illicit funds into zkBob.

All interactions with the TRM wallet screening API are exclusively channeled through the zkBob sequencer for two primary purposes:

1. Mitigating the risk of TRM API key abuse.
2. Safeguarding against users attempting to disable TRM wallet screening on the UI side.

Additionally, customers can generate a voluntary account compliance report that discloses transactions for a selected period of time and also has intrinsic integrity protection (3.2.1 Opt-in Reporting).

5. Conclusion

The permissionless nature of blockchain networks allows for a wide variety of uses, spanning both licit and illicit activities depending on the jurisdiction. In the absence of the ability to distinguish one from the other, regulators sometimes find it necessary to ban a network or application completely (U.S. Department of the Treasury, 2022) or isolate it from regular users (Peterson, 2023) to prevent continued illegal usage, even if only by a small number of bad actors.

To create privacy applications that serve most users, who do not have illicit intentions, developers must leverage knowledge of behavioral patterns, transaction characteristics, and forensics tools so that hiding illicit activities using privacy-enhanced applications is either close to impossible or results in identity disclosure. At the same time, it is important not to encumber the user experience too much as this drives away legitimate use cases such as payroll, private swaps, payments and others.

It's no surprise that the dilemma around private asset transfers strongly resembles debates in regards to end-to-end encryption (Thakkar, 2021), as demonstrated by the zCash quote "if Bitcoin is http for money, zCash is https" (Zcash, n.d.). We see exactly the same arguments from both sides and somewhat similar incidents throughout the last few decades where inherently neutral platforms and services were used by bad actors. This is not a coincidence since tokenized assets and crypto currencies are essentially a new form of typed information that is processed by online services. An important historical difference (at least in the U.S.) is that unlike blockchain based financial services recognized as accountable for money laundering and other bad practices, general purpose web services such as social networks and messaging applications were granted immunity from being held responsible for user's content (Legal Information Institute, n.d.). Most recently, the bipartisan EARN IT Act (Congress.gov, 2023) obliges tech companies to implement some predefined practices to prevent bad behavior, or at least some reasonable measures defined by the companies themselves, but it obviously aims at e2e encryption.

This multi-decade long struggle between communication providers and regulators gives us a good idea about what kind of regulations should be expected down the road regarding on-chain privacy and what could be a viable proactive approach for the community to resolve these conflicts:

1. Comparing internet traffic to general financial transactions could be relatively easier analyzed in a privacy preserving manner and is worth further research.
2. Some standardization and oversight are required for such a complex issue to be resolved, and they will be either created internally by the industry in coordination with regulatory agencies or imposed from above as we've seen with FinCEN's NPRM, EARN IT Act and others similar.

In the meantime, standalone applications will continue to fill in the gaps while attempting to bridge the divide between privacy and compliance. By enacting self-regulatory measures, these protocols are taking proactive steps to provide privacy to legitimate users who want and need it.

References

Authentic8 (2022). The Fallacy of Anonymity in Cryptocurrency. Retrieved from https://www.authentic8.com/blog/fallacy-anonymity-cryptocurrency

Belonick, M. (2020). Transparency is the New Privacy: Blockchain's Challenge for the Fourth Amendment. *Stanford Law School*, Stanford University. Retrieved from https://law.stanford.edu/wp-content/uploads/2020/03/2020-03-22_Belonick_Final.pdf

Berkovitz, D.M. and Pattnaik M. (2023). Measuring the Regulatory Gaps for Digital Assets and the Use of Technology to Bridge the Gap. Retrieved from https://blog.merklescience.com/general/measuring-the-regulatory-gaps-for-digital-assets-and-the-use-of-technology-to-bridge-the-gap

Berwick, A. and Talley, I. (2022). Hamas Militants Behind Israel Attack Raised Millions in Crypto. *The Wall Street Journal*. Retrieved from https://www.wsj.com/world/middle-east/militants-behind-israel-attack-raised-millions-in-crypto-b9134b7a

Bitcoin Wiki (n.d.). CoinJoin. Retrieved from https://en.bitcoin.it/wiki/CoinJoin

BitcoinWiki (n.d.). CryptoNote. Retrieved from https://bitcoinwiki.org/wiki/cryptonote

Browne, E. (2021). Bitcoin Millionaire Zaryn Dentzel Beaten, Fortune Stolen in Masked Robbery for Cryptocurrency. Retrieved from https://www.newsweek.com/bitcoin-millionaire-zaryn-dentzel-beaten-fortune-stolen-masked-robbery-cryptocurrency-1645550

Buterin, V., Illum, J., Nadler, M., Schär, F. and Soleimani, A. (2023). Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium. Available at SSRN: https://ssrn.com/abstract=4563364 or http://dx.doi.org/10.2139/ssrn.4563364

Chainway Labs (2023). Introducing Proof of Innocence: Built on Tornado.cash. Retrieved from https://medium.com/@chainway_xyz/introducing-proof-of-innocence-built-on-tornado-cash-7336d185cda6

Congress.gov (2023). S.1207 - EARN IT Act of 2023. *Congress.gov*. https://www.congress.gov/bill/118th-congress/senate-bill/1207/text

Cornell Law School Legal Information Institute (1986). Money Laundering Control Act of 1986. Retrieved from https://www.law.cornell.edu/topn/money_laundering_control_act_of_1986

DeMichele, T. (2019). The US Is Essentially Being Geoblocked from Every Coin That Had an ICO by Exchanges. *Cryptocurrency Facts*. Retrieved from https://cryptocurrencyfacts.com/2019/06/17/the-us-is-essentially-being-geoblocked-from-every-coin-that-had-an-ico-by-exchanges/

Dune Analytics (n.d.). zkBob Dune Analytics Dashboard. https://dune.com/zkbob/zkbob

Electric Coin Company. (2020). Explaining Viewing Keys. *ECC Blog*. Retrieved from https://electriccoin.co/blog/explaining-viewing-keys/

Electronic Code of Federal Regulations (n.d.). 31 CFR § 1022.320 - Reports by money services businesses of suspicious transactions.. Retrieved from https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1022/subpart-C/section-1022.320

Eskandari, S., Moosavi, S. and Clark, J. (2019). SoK: Transparent Dishonesty: Front-Running Attacks on Blockchain. arXiv:1902.05164. Retrieved from https://arxiv.org/abs/1902.05164

Europol (2021). Cryptocurrencies - Tracing the Evolution of Criminal Finances, Europol Spotlight Report Series, Publications Office of the European Union, Luxembourg. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

Federal Trade Commission (2022). Equifax Data Breach Settlement. Retrieved from https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement

Federal Trade Commission (n.d.). Gramm-Leach-Bliley Act. Retrieved from https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

Financial Crimes Enforcement Network (2023). Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern. Retrieved from https://www.fincen.gov/sites/default/files/federal_register_notices/2023-10-19/FinCEN_311MixingNPRM_FINAL.pdf

Jedusor, T.E. (2016). Mimblewimble. Retrieved from https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.txt

Jones, B.L. (2016). The 21st Century DarkNet Market: Lessons from the Fall of Silk Road. *International Journal of Cyber Criminology*, 10(1), 40-61. DOI: 10.5281/zenodo.58521 Retrieved from https://www.researchgate.net/publication/306255981_The_21st_Century_DarkNet_Market_Lessons_from_the_Fall_of_Silk_Road

Legal Information Institute (n.d.). 47 U.S. Code § 230 - Protection for Private Blocking and Screening of Offensive Material. *Cornell Law School*. Retrieved from https://www.law.cornell.edu/uscode/text/47/230

Merkle Trees, R.C. (1988). A Digital Signature Based on a Conventional Encryption Function. In: Pomerance, C. (Eds.), *Advances in Cryptology — CRYPTO '87*. CRYPTO 1987. Lecture Notes in Computer Science, Vol. 293. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48184-2_32

Miers, I., Garman, C., Green, M. and Rubin, A.D. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin. *2013 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, pp. 397-411. doi: 10.1109/SP.2013.34.

NL Times (2020). Violent Robbery of Bitcoin Trader Included Water-Boarding, Power Drill. Retrieved from https://nltimes.nl/2020/02/02/violent-robbery-bitcoin-trader-included-water-boarding-power-drill

OECD (2022). Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard. Retrieved from https://www.oecd.org/tax/exchange-of-tax-information/crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.htm

Office of Foreign Assets Control (2024). Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists. Retrieved from https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists

Office of the Comptroller of the Currency (n.d.). Bank Secrecy Act (BSA) and Related Regulations. Retrieved from https://www.occ.treas.gov/topics/supervision-and-examination/bsa/bsa-related-regulations/index-bsa-and-related-regulations.html

Ohlhaver, P., Weyl, E.G. and Buterin, V. (2022, May 10). Decentralized Society: Finding Web3's Soul. Available at SSRN: https://ssrn.com/abstract=4105763 or http://dx.doi.org/10.2139/ssrn.4105763

Parno, B., Howell, J., Gentry, C. and Raykova, M. (2013). Pinocchio: Nearly Practical Verifiable Computation. *2013 IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, pp. 238-252. doi: 10.1109/SP.2013.47.

PCI Security Standards Council (n.d.). PCI Security Standards Council. Retrieved from https://www.pcisecuritystandards.org/

Peterson, M. (2023). Privacy Coins Zcash and Monero Face Delisting by Crypto Exchanges. *Blockworks*. https://blockworks.co/news/crypto-exchanges-delisting-privacy-coins

RAILGUN Project (2023). Having Your Privacy & Eating it Too: Railgun Proof of Innocence. Retrieved from https://medium.com/@Railgun_Project/having-your-privacy-eating-it-too-railgun-proof-of-innocence-efcba557aac4

RAILGUN (n.d.). Wallets and Keys: Viewing Keys. Railgun Documentation. Retrieved from https://docs.railgun.org/wiki/learn/wallets-and-keys#viewing-keys

Satoshi Nakamoto (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

Schaer, F. (2021). Decentralized Finance on Blockchain and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review*, 103(1), 97-116. Retrieved from https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets

Shlomit Azgad-Tromer, S., Garcia, J. and Tromer, E. (2023). The Case for On-Chain Privacy and Compliance. *Stanford Journal of Blockchain Law & Policy*. Retrieved from https://stanford-jblp.pubpub.org/pub/onchain-privacy-compliance

Thakkar, J. (2021). End-to-End Encryption: The Good, the Bad, and the Politics. *SSL Store*. https://www.thesslstore.com/blog/end-to-end-encryption-the-good-the-bad-and-the-politics/

U.S. Department of the Treasury (2022). U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash. Retrieved from https://home.treasury.gov/news/press-releases/jy0916

U.S. Government Publishing Office (2001). Public Law 107-204: Sarbanes-Oxley Act of 2002. Retrieved from https://www.govinfo.gov/content/pkg/PLAW-107publ204/html/PLAW-107publ204.htm

Visa (2022). Visa B2B Connect: Enabling Use of Crypto for Payments. Retrieved from https://usa.visa.com/content/dam/VCOM/regional/na/us/Solutions/documents/b2b-crypto-one-pager-april-22-ada.pdf

Visa (2023). By Settling in USDC, Crypto.com is Setting a New Course. Retrieved from https://usa.visa.com/content/dam/VCOM/regional/na/us/Solutions/documents/visa-crypto.com-usdc-case-study.pdf

Yu, P.K. (2019). A Hater's Guide to Geoblocking, *25 B.U. J. Sci. & Tech. L.* 503. Available at: https://scholarship.law.tamu.edu/facscholar/1339.

Zcash (n.d.). Bitcoin is HTTP for Money, Zcash is HTTPS. *Zcash Blog*. https://z.cash/bitcoin-is-http-for-money-zcash-is-https/

ZeroCoin (n.d.). ZeroCoin. Retrieved from https://zerocoin.org/

Cite this article as: Vladimir Popov, Andrew Gross, Mike Krupin and Georgi Koreli (2024). Blockchain Privacy and Self-Regulatory Compliance: Methods and Applications. *International Journal of Cryptocurrency Research*, 4(1), 64-78. doi: 10.51483/IJCCR.4.1.2024.64-78.