TARI

Executive Summary

Tari is a new kind of blockchain with new methods to support compliance. Its transactions are private by default, and yet counterparties can share full transaction histories. Its users are anonymous by default, and yet counterparties can share personally identifying information with each other. Compliance obligations are no longer insurmountable obstacles. With Tari, questions of compliance now have answers.

The bedrocks of compliance support lie in Tari's base layer, wallet layer, and sidechain layer. Within each layer, counterparties have toolsets to permit the voluntary sharing of select information with each other, and to prove ownership and control of specific network addresses. These features mean companies can easily comply with transaction monitoring, recordkeeping and reporting, global sanctions, anti-money laundering ("**AML**"), and know your customer ("**KYC**") requirements.

Tari designed these tools to facilitate such compliance with global sanctions laws, AML/KYC regulations, FATF's Travel Rule, and MiCA's forthcoming restrictions on token listing. Examples of these tools include:

- **TariScript.** Scripts can create basic conditions on transactions, to encourage storage of transaction details, provision of view keys, or to restrict transfers.
- **Base Layer Messaging.** Users can utilize Tari's base layer message feature to voluntarily send up to 64 bytes with their transactions. Exchanges can use this feature to comply with the Travel Rule and other obligations.
- **Interactive Transactions.** Using interactive transactions, parties can return funds to a sender where insufficient information has been provided or for any reason even though the sender's network address is hidden by default.
- **Wallet-Level Compliance.** Wallet users can choose to store a local, encrypted version of their transaction history within their local device to preserve an audit trail. This can be sent to a counterparty on request. Wallets may also automatically disable their send functionality for users in jurisdictions subject to comprehensive sanctions.
- **Wallet as API.** The official Tari wallet will be implemented as an API, allowing for more simple, automated compliance.

Tari lets companies implement versatile and complex tooling to help meet compliance obligations. Tari will provide free SDKs, guides such as this FAQ, and additional assistance to help the industry take full advantage of these features.

Blockchain Basics

What is Tari and how does it support compliance?

Tari is a revolutionary blockchain protocol that provides strong confidentiality guarantees to its end-users and gives virtual asset service providers ("**VASPs**"), including cryptocurrency exchanges ("**Exchanges**"), powerful tools to comply with applicable sanctions, recordkeeping, and reporting laws around the world.

Tari's development efforts support compliance in three ways.

First, the base layer of the blockchain will be launched with features that strike a balance between preserving privacy and permitting voluntary sharing of identifying information with exchanges. Tari will provide regulated entities with software development kits and tooling specifically designed to help them take full advantage of these features.

Second, the official Tari Wallet will contain features designed to help counterparties, including Exchanges, reveal their identity and audit trails with each other.

Third, a sidechain layer will enhance regulated Exchanges' tools to monitor certain sets of transaction outputs.

The compliance features of Tari's blockchain will be compatible with the monitoring architecture of most regulated entities. While Tari's native token is designed to operate like real money, it is also designed to help companies to fulfill their regulatory obligations. Thus, while Tari is private by default, all counterparties in the Tari network will have the ability to share private information with each other to support compliance.

What information is visible for each transaction?

Tari is private by default. An exchange receiving funds can only – initially – view any **output**, **number of confirmations,** and the **size** (in bytes). **Fees** may be viewed separately from outputs.

Notwithstanding the private nature of Tari's blockchain, all key transaction information, including the **network addresses** of the user and recipient and the **amounts** (both inputs and outputs) may be viewed by anyone chosen by a sender. Users can also include additional information up to 64 bytes with each output, which can only be viewed by the sender and recipient.

Exchange Compliance Considerations

What does applicable law typically require of Exchanges?

Several major frameworks impose compliance obligations on Exchanges. Member states of the Financial Action Task Force ("**FATF**") and the European Union have imposed or will impose rules specific to Exchanges. These include FATF recommendations and – as an example of an emerging framework – the European Union's Crypto Assets Regulations ("**MiCA**"), which go into full force in December 2024. Additionally, global sanctions laws, and each country's AML/KYC requirements require recordkeeping and reporting from Exchanges in some regard.

Global Sanctions Laws

Economic sanctions are restrictions on financial or trade-related activities with a specific person, country, region, or government. They can be comprehensive or targeted, and differ in each jurisdiction, but all typically require collection of the same subset of data to comply with these laws. That is, Exchanges must be able to identify counterparties by their **full name**, must know the counterparty's **geographic location**, and must know the counterparty's blockchain **network address**.

Anti-Money Laundering Laws

Money laundering involves disguising financial assets so they can be used without detection of the illegal activity that produced them. Criminals launder money to transforms the proceeds of criminal activity into funds that appear to stem from a legitimate source. FATF recommendations and MiCA require Exchanges (i) to undertake customer due diligence measures where transaction amounts exceed USD/EUR 1,000; (ii) to monitor transactions; (iii) to keep records of transactions and customer due diligence records; (iv) to comply with the Travel Rule (discussed below); and (v) to file reports of suspicious transactions.

In addition to the above, MiCA, once it is in full effect, will require Exchanges to not list crypto assets that have an "inbuilt anonymization function" unless the Exchange (or "competent authorities") can obtain both (i) the **identity** of the holders of the asset and (ii) the **transaction history** of the holder.

Travel Rule, Verification, and Recordkeeping

FATF's Travel Rule requires VASPs sending or receiving customer funds to or from another VASP to collect user data and transaction data.

"User Data" consists of the user's **full name**, **physical address**, **national ID number**, **customer ID number**, **date and place of birth**, and **source of funds**. This data is typically collected in a VASP's onboarding or KYC process.

"Transaction Data" consists of the **network address** for each counterparty, **nature and date** of the transaction, **amount** transferred, auditable **transaction history**, and any **other addresses or accounts** involved. This data is typically collected as a matter of course for transactions involving public, pseudonymous blockchains.

In addition to obtaining such data, the Travel Rule requires the sending VASP to verify sender's information is accurate and the receiving VASP to verify recipient's information is accurate. Verification can be straightforward for user data: a VASP may request documents

from the user to verify the user is who they say they are. For transaction data, verification requires sender and recipient to prove to their respective VASPs they own the network addresses linked to their own accounts.

Verification

Outside of the Travel Rule, for transactions that involve a VASP and an individual user, the VASP may need to verify ownership of the address used to deposit funds, or ownership of the withdrawal address.

Typically, any technology or software solution is acceptable to comply with the Travel Rule, so long as VASPs can fulfill their other obligations compliance obligations. FATF states "the information [required by the Travel Rule] can be submitted either directly or indirectly. It is not necessary for this information to be attached directly to the virtual asset transfers." This allows Travel Rule required information to be sent separately from the transaction itself.

Recordkeeping Obligations

FATF recordkeeping requirements state that VASPs maintain all records of transactions and customer due diligence measures for at least five years.

Native Blockchain Support for Exchanges

Which of Tari's unique features can be used to support Exchange compliance?

Tari's compliance features provide support at three levels: the base layer, the wallet software, and, once launched, the sidechain layer.

Tari's base layer has a range of features built into the native protocol, some of may be used by sophisticated Exchanges to enhance their transaction monitoring, recordkeeping, and reporting requirements:

- **TariScript.** Users can voluntarily decide to create basic scripts via the base layer's scripting language, TariScript. Similar to smart contracts, TariScript lets users create conditions to spending funds.
    - For example, Users can make use of scripts to automatically store output details within their wallet; or to automatically store specific information with every output, such as a unique identifier, a reference number, their PII, or information sufficient to reconstruct an audit trail. Users may also embed arbitrary data into scripts, which may require separate communication between spender and receiver to view.
- **Proof of Output Ownership.** Users can verifiably prove they own the output of a UTXO by providing knowledge of the spend key and script key. This can be done by signing using a commitment and public key signature ("**CAPK**") protocol.
- **Proof of Involvement.** Users can verifiably prove they were involved in a particular transaction by providing knowledge of the spend key which can be achieved by signing a message using the CAPK protocol.
- **Proof of Receipt.** Users can verifiably prove they received funds as well.
- **Multisignature Capabilities.** Users can voluntarily engage in transactions involving multiple signatories. This feature allows for basic escrow arrangements to be created, where funds only release once predefined parameters have been met. Exchanges can choose to set parameters would be set by one of the signatories, and the Exchanges themselves can be signatories.
- **Messages.** Users can voluntarily send information up to 64 bytes with each base layer output. Messages can be used to send information useful for compliance teams at any Exchange.
- **Return to Sender (Only Interactive Transactions).** Interactive transactions in Tari involve two parties and involve a message that can include secret data. With Interactive Transactions, an Exchange with Interactive Transactions enabled may be able to return funds to a sender even though the sender's network address is hidden by default.

Tari's Wallet software will contain certain compliance features by default, and will provide Exchanges with powerful, application-layer functionalities should they choose to make use of them. That said, all wallets will be able to implement the features below, if desired by their developers:

- **Mandatory Scripting.** Wallets may require automatic use of scripts to send funds, which allows a wallet to implement specific compliance functions. Exchanges may even submit requests to improve these functions through channels for open source development. Updates to a wallet should not require changes to the base layer to function properly.
- **Geoblocking.** A wallet (whether web or mobile) may be able to disable spend functionality for users located in a jurisdiction subject to comprehensive sanctions. Wallets would need to be able to identify IP addresses to implement this.
- **Proof of Transaction Initiation.** Wallet users can verifiably prove they initiated a particular output.
- **Transaction History Preservation.** Wallet users can choose to store a local, encrypted version of their transaction history automatically within their device. This would preserve an audit trail for each output made using that wallet.
- **Transaction History Sharing.** Wallet users can share their preserved transaction history with any counterparty they choose, including Exchanges, either (i) through the Messages feature of the base layer, or (ii) by exporting the information from the wallet and sending it off-chain to an Exchange.
- **Sharing of PII.** Wallet users can share their personally identifying information with any counterparty they choose, including Exchanges, either (i) through the Messages feature of the base layer, or (ii) by exporting the information from the wallet and sending it off-chain to an Exchange.
- **Wallet-Level KYC**. Wallet users may be able to, with the support of a third-party KYC provider, undergo a sanctions check and/or verify their PII, and record proof of successful KYC ("**KYC Token**") within the Wallet itself. This token could be sent on-chain, using Messages, or off-chain, by exporting the data and sending directly to an Exchange. An Exchange can verify the validity of the KYC Token with the third-party KYC provider that performed the KYC and generated the KYC Token.

Tari's sidechain layer, once launched, will contain additional tools Exchanges can make use of to monitor transactions involving second-layer assets, such as stablecoins, launched on Tari. The issuers of these second-layer assets can provide Exchanges with special view privileges not available to the public. These protections will be covered in a separate Compliance FAQ specifically regarding Tari's second-layer assets.

How can an Exchange comply with its various obligations using Tari's compliance features?

Every compliance regime is concerned with (i) collecting (and sometimes verifying) personally identifying information ("**PII**") to satisfy KYC requirements; (ii) obtaining and keeping a record of audit trails; (iii) keeping records of PII and other key information such as trading history; (iv) reporting suspicious activity to regulators; and (v) preventing the financing of illicit activity. Examples below illustrate how Tari provides versatility for Exchanges to comply with their various legal and regulatory obligations.

Global Sanctions Laws

To comply with global sanctions laws, an Exchange must know a sender and recipient's full name, geographic location, and network address.

Exchanges always obtain name and geographic location during their standard onboarding process. What Exchanges lack here is twofold: (i) the network address, and (ii) proof that funds received belong to a KYC'd customer.

To obtain a sender's network address, an Exchange can explicitly request the address from its depositors. To obtain proof that funds belonged to a KYC'd customer of the Exchange, one can also request verification of ownership using methods set out below.

Tari's base layer has tools to let senders and recipients to prove: (i) user owns an output; (ii) user was involved in a specific output; (iii) user received funds; and (iv) within the Tari Wallet, the user initiated a specific output (collectively, the "**Proofs of Ownership**").

> ***Example 1: Proofs of Ownership***
>
> *Exchange onboards User A. Exchange receives Tari funds into the address associated with User A. Exchange wishes to verify ownership of User A's sending address, and asks User A to prove ownership using a tool available within their wallet. They can prove knowledge of a spend and/or script key through their wallet, and Exchange can keep a record of that proof. Exchange only attributes funds associated with User A to User A after verification of ownership, and effectively freezes all other funds received from unverified senders.*

An Exchange may also decide to implement the Return to Sender feature by requiring all deposits be made via interactive transactions.[1]

Tari's messaging capacity gives Exchanges the option to request arbitrary data be sent to the Exchange with every deposit ("**Deposit Messaging**"). Exchanges can, on their own, decide not to credit any transaction that does not have this arbitrary data, effectively freezing funds.

> ***Example 2: Deposit Messaging***
>
> *Exchange receives a deposit from a Tari address. User B, a longstanding customer, claims the deposit came from her, but Exchange cannot verify this. Nor can the Exchange verify funds did not come from a sanctioned wallet address.*
>
> *Exchange can request User B send another deposit and include specific, arbitrary data with the deposit using Messages. Once the Exchange receives the deposit and verifies the message matches the arbitrary data, Exchange will be able to verify User B is the owner of that Tari Wallet address and can credit the user's transaction.*

[1] This may not permit full compliance in jurisdictions that require immediate freezing of funds associated with terrorist financing or illicit activity.

Customer Identification

To comply with customer identification requirements and collection of user data, Exchanges must obtain PII from their users. The collection of PII occurs during standard onboarding and does not need to occur via the Tari blockchain. Further, source of funds inquiries typically do not occur on a blockchain.

Tari can support an Exchange's compliance obligations via methods already discussed. The Proofs of Ownership and Deposit Messaging techniques may be used to verify funds are sourced from a network address owned by a user.

> ***Example 3: Script Whitelist / Return to Sender***
>
> *An Exchange may create a whitelist that contains addresses associated only with Users who have proven ownership of whitelisted addresses using a Proof of Ownership. Also, an Exchange with interactive transactions turned on can enable Return to Sender, which may be designed to send back User funds automatically if they come from an address not on the Exchange's whitelist.*

Transaction Monitoring

To comply with requirements to collect transaction data and auditable transaction histories, Exchanges can make use of compliance features embedded within a user's wallet.

According to FATF, VASPs should obtain the nature and date of a transaction, amount transferred, the user's network address, and an auditable transaction history. VASPs typically ask users for details regarding the nature of the transaction outside of the blockchain. VASPs also know the amount transferred to and from the VASP as a matter of course.

A VASP will need to obtain, for Tari transactions, the user's network address and an auditable transaction history. To do so, VASPs can make use of the Tari Wallet or other compliance-focused wallets. Within the Tari Wallet, all relevant transaction data may be stored, including network address, date of the transaction, amounts, and transaction history. VASPs can request users send this information to the VASP.

> ***Example 4: Wallet View Key***
>
> *Users may share a copy of their wallet-level view key with an Exchange. Exchanges can make crediting an account contingent on sharing of a wallet-level view key. In this way, Exchanges can pressure any potential user to use Tari wallets with compliance features in order to deposit funds.*

Travel Rule

For Tari transactions between VASP-custodial wallets, compliance with the Travel Rule is straightforward. Since regulated VASPs already perform know-your-customer (KYC) procedures on their users, they only need to share the sender or recipient information with the corresponding VASP.

For transactions to unhosted wallets, a VASP can require the use of interactive transactions to share secret data with the recipient to comply with the Travel Rule. For non-interactive transactions, a VASP may employ a "penny test" or other means (Proofs of Ownership) to prove the user owns the network address.

Example 5: Penny Tests

- ***Withdrawal From an Exchange-hosted Wallet to a User's Unhosted Wallet***

  Step 1: Exchange asks User for a withdrawal address.

  Step 2: Exchange asks User for PII and verifies it. Exchange checks any applicable sanction lists and decides it can go ahead with the withdrawal.

  Step 3: Exchange sends a random amount of microminotari (0.0000001 minotari) to the withdrawal address using a non-interactive transaction. Only the owner of this address will be able to know the amount sent. The exchange asks the user to input the amount, which is a random number between 0 and 99999. The user has a short time to enter this amount and has a limited number of retries (e.g., 3 attempts).

  Step 4: User waits for the transaction to appear in their wallet and uses it as a PIN to verify ownership of the wallet.

- ***Deposits From an Unhosted Wallet to an Exchange-hosted Wallet***

  The process can be used exactly as above, or alternatively can be done as follows:

  Step 1: User states the amount they will be depositing.

  Step 2: Exchange sends a secret penny test to the address User provides.

  Step 3: User sends funds to the Exchange using the original deposit amount plus the additional amount in the penny test.

  These examples demonstrate how Exchanges can comply with the Travel Rule in Tari transactions involving unhosted wallets. By implementing appropriate verification methods, Exchanges can ensure compliance while maintaining privacy and security.