REBEL REGULATORY & COMPLIANCE BRIEF

JULY 2022

This document is designed to give regulators, policymakers, and compliance experts an overview of REBEL.

REBEL is an open-source, decentralized virtual currency similar to Bitcoin. It protects users' privacy by using a cryptographic method based on zero-knowledge proofs.

REBEL is not a security and through its blockchain offers the public and exchanges greater transparency and less risk than Bitcoin with regards to privacy.

REBEL is fully compliant with the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) requirements set out in the June 2019 FATF Recommendations. Information about the sender and recipient can be added directly to shielded REBEL transactions, which makes it easier to meet Travel Rule requirements.

Under the ticker "RBL," REBEL is traded on many of the world's biggest virtual currency exchanges.

Privacy and confidentiality

Many things about a person may be gleaned from their personal financial records, including how much money they make, where they buy, what publications and websites they read, what they like to do for fun, and what charities they contribute to.

The governments of the world's largest economies have passed laws to protect people's financial privacy because they know how important it is. Data protection laws and regulations vary from country to country, but examples include the Gramm-Leach-Bliley Act in the United States as well as EU's General Data Protection laws and Japan's Protection of Personal Information Act. The public's understanding of how important it is to have strong privacy safeguards has increased as a direct result of the rising danger posed by cybercriminals and identity thieves, as well as high-profile cases like the data breach that occurred at Experian.

According to Gramm-Leach-Bliley Act Sec. 6801(a):

> It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ non-public personal information.

First-generation blockchain technology (as used in Bitcoin) needs the sender's and recipient's identities to be verified. The blockchain reveals the recipient's payment addresses as well as the amount being sent.

Anyone with access to a Bitcoin user's payment address may thus view all of the transactions that are sent and received by that address.

By offering users the option to shield their funds and conduct transactions privately, REBEL addresses this problem. To do this, REBEL has two kinds of transactions: transparent and shielded.

Transactions between transparent addresses are similar to Bitcoin transactions in that the blockchain shows the transparent addresses of both the sender and the receiver as well as the amount being sent.

REBEL has re-used the Bitcoin protocol for its transparent addresses and transparent transactions. As a result, it is simple and straightforward to add support for REBEL to already existing transaction monitoring systems.

If a user chooses to transact privately, s/he can shield the funds by using a shield address. Shielded funds kept in a shielded address are no longer visible on the public blockchain and can be transferred to another shielded address using a shielded transaction, which protects both the privacy of the Sender and the Recipient as well as the amount transferred.

Shielded funds can be unshielded again by moving them to a transparent address, which discloses them to the public blockchain.

The use of shielded addresses is totally discretionary. Virtual asset service providers (VASPs), which include exchanges and payment processors, have the option of employing either transparent or shielded transactions when accepting deposits, making payments, or allowing withdrawals. This choice may be made independently or in conjunction with one another.

Anti-Money Laundering and Terrorist Financing

AML/CFT measures, such as customer due diligence, record-keeping, reporting suspicious transactions, and providing required originator and beneficiary information for virtual asset transfers between VASPs (commonly referred to as the "Travel Rule"), have been built into REBEL as part of the platform's design.

Additionally, REBEL is compliant with the standards imposed by the Fifth Money Laundering Directive of the European Union and the Anti-Money Laundering rules of the United States.

D**ue Diligence for Customers (CDD)**

When establishing a business relationship, VASPs are obligated to conduct due diligence in accordance with the recommendations provided by the FATF. The fact that a VASP supports REBEL or that a customer plans to trade REBEL has no bearing on the VASP's capacity to perform CDD checks.

REBEL is similar to Bitcoin and Ethereum in this regard, and VASPs can use the same CDD processes.

Transaction monitoring

REBEL's privacy-preserving technology does not prevent a VASP from monitoring a customer's transactions with that VASP (e.g. deposits, withdrawals, trades), and comparing transaction patterns and volumes with expected behavior, based on the VASP's understanding of the customer's or their business nature (as determined during the CDD checks).

A VASP has access to the specifics of its customers' REBEL transactions since it is a party to those transactions (either as a recipient in the case of deposits or as a sender in the case of withdrawals, depending on the nature of the transaction). This enables the VASP to recognize transaction patterns that differ from the expected behavior of that customer and investigate further to evaluate whether the unexpected behavior is suspicious.

All transactions in REBEL must utilize payment addresses. This enables VASPs to provide a unique deposit address to each individual customer, making it possible for REBEL deposits to be indisputably ascribed to a particular customer user. Customers must also give a payment address in order to accept withdrawals from REBEL, allowing VASPs to undertake sanctions screening or limit transactions to whitelisted addresses.

In this way, REBEL is similar to other virtual currencies whilst the same tools and methods can be used to keep track of transactions.

Blockchain Analytic

Transactions set between transparent addresses are visible on the REBEL blockchain because REBEL re-uses the Bitcoin protocol for transparent transactions.

Record-keeping

VASPs are able to monitor and preserve the records of a customer's REBEL transactions in the same manner as they can keep transaction records for other virtual currencies.

For deposits, VASPs can record the customer's name, the amount of REBEL deposited, the destination address (the deposit address produced by the VASP for that customer), the source address (where the consumer deposits funds from a transparent address) and the transaction ID.

For withdrawals, VASPs can record the customer's name, the amount of REBEL withdrawn, the source address (the VASPs' address from which the coins are delivered), the destination address (whether it is a transparent address or a shielded address) and the transaction ID.

Importantly, the VASP always knows the payment address to which a REBEL withdrawal is sent.

In terms of the information accessible to be recorded by the VASP, the sole difference between REBEL and other virtual currencies is that if the consumer deposits from a shielded address, the

VASP will not immediately have visibility of the source address. If the VASP so desires, it may require that the customer give the source address for the VASP's records. This is not, however, required by the FATF Recommendations.

Reports of Suspicious Transactions

With the ability to monitor transactions, a VASP can find out if any of its customers are doing anything suspicious. The capacity of the VASP to keep records of the transactions carried out by its clients means that it is in possession of sufficient information to report potentially suspicious transactions when the situation calls for it.

The Travel Rule

The Travel Rule was taken into consideration throughout the development of REBEL. Using the encrypted memo field, the relevant originator and beneficiary information may be attached directly to a protected transaction. When the transaction is added to the blockchain, the contents of this field are encrypted. This protects the personal information from being disclosed in an inappropriate manner or without authorization.

The AML / CFT Risk

Recent research conducted by the RAND Corporation revealed that while the majority of virtual currencies are legitimate, Bitcoin is "widely documented to be the most dominant cryptocurrency on the dark web." RAND found that more than 90% of virtual currency addresses posted on dark web markets or forums were Bitcoin addresses.

Despite the obvious advantages of privacy coins for illicit or criminal transactions, REBEL has a negligible presence on dark web markets, whereas the less private Bitcoin is the most popular cryptocurrency on the dark web.

Sharing information about shielded transactions with third parties

It's possible that there will be times when one shall need to disclose confidential transaction details with third parties. The REBEL protocol was designed to support two features that make it possible to reveal information about transactions that have been shielded.

(1) Viewing Keys - The person who has a shielded address has the ability to generate a Viewing Key, which they may subsequently provide to a third party. Anyone with the Viewing Key for the shielded address can view all transactions sent to or from that shielded address. Key viewing functionality is supported in its entirety.

(2) Payment Disclosure – this allows for the disclosure of transaction information that has been shielded. This functionality is very similar in nature to that of Viewing Keys; however, rather than offering visibility of all transactions issued and received by a shielded address, it allows visibility of a single transaction. A payment disclosure key can be generated by either the sender or the receiver of a shielded transaction. This key enables a third party to view some aspects of the transaction, notably the recipient's shielded address and the contents of the Encrypted Memo Field.

The use of these features will make it possible for VASPs to share visibility of shielded transactions and shielded addresses in a private and secure manner with the relevant authorities or auditors. VASPs and statutory regulators may also use these features to facilitate market surveillance and the identification of suspicious transactions.

Conclusion

REBEL was created with the goal of safeguarding users' financial privacy whilst remaining compliant with international AML / CFT standards, such as the FATF Recommendations that were implemented in June 2019, the EU's Fifth Money-Laundering Directive and US anti-money laundering laws.

REBEL's privacy does not impede regulated organizations from meeting their regulatory duties, which is an important consideration.

REBEL does not have a significant presence on the dark web markets.

REBEL works with policymakers and regulators in a proactive, productive and cooperative manner. In an effort to inform and promote a risk-based approach to regulation, we strive to offer accurate and impartial data. We would be happy to discuss any concerns one may have regarding regulatory or compliance issues, as well as answer any questions one may have regarding how REBEL operates and the implications this has for AML and CFT compliance.

Please contact us (support@rebelstation.org) to address any of the problems raised in this message.