MimbleWimbleCoin's

Regulatory & Compliance Brief

17th of July 2020

Introduction

This note is intended to provide an overview of MimbleWimbleCoin for regulators, policy-makers, and compliance professionals.

MimbleWimbleCoin, also referred to as "MWC", is an open-source, decentralized virtual currency, similar in nature to Bitcoin, which protects users privacy through the use of an innovative cryptographic technique based on zero-knowledge proofs.

Despite this MWC is fully compliant with AML and CFT requirements set forth in the FATF Recommendations adopted in June 2019[1] Required originator and beneficiary information can be attached directly to MWC transactions facilitating compliance with the "Travel Rule" requirements. In this document we elaborate on this.

[1] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

Confidentiality & Privacy

Personal financial information can reveal a huge amount of information about the subject, including how much they earn, where they shop, what newspapers, magazines and websites they subscribe to, their interests and hobbies, how much they have saved up and what causes they may have donated to.

Governments of the world's largest economies have recognised the importance of personal financial privacy, and have enacted legislation to protect it. Examples include the Gramm-Leach-Bliley Act in the United States, the EU's General Data Protection Regulation and Japan’s Act on the Protection of Personal Information.

The growing threat from cyber-criminals and identity thieves, and high profile incidents such as the Experian data breach have raised public awareness of the importance of robust privacy protections and MWC is another form of such protection.

> 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’ nonpublic personal information. (Gramm-Leach-Bliley Act)

Unlike traditional Blockchain technology like Bitcoin MimbleWimbleCoin *does not* require the addresses of sender and recipient and the transacted amount to be revealed on the blockchain. As a Result a third-party observer cannot see transactions done by another party by simply observing a known address.

MWC uses Three main properties to increase the privacy of their Users.
All Transactions on the base layer are CoinJoined with Confidential Transactions and signature aggregation. Consequently there are no addresses, transaction amounts or intermediary inputs and outputs in blocks and all transactions are indistinguishable from one another. Unless you are a transaction participant then all inputs and outputs look like random pieces of data on the blockchain

Anti-Money Laundering & Terrorist Financing

MWC is by Design compatible with the AML / CFT measures recommended by the Financial Action Task Force on Money Laundering (FATF), including customer due diligence, record-keeping, reporting suspicious transactions, and providing required originator and beneficiary information for virtual asset transfers between VASPs (often referred to as the “Travel Rule”).

Customer Due Diligence (CDD)

Under the FATF recommendations, VASPs are required to undertake CDD measures when establishing a business relationship. The fact that a VASP supports MWC or that a customer intends to trade MWC does not impact the VASP’s ability to carry out CDD checks. In this respect, MWC is no different from other virtual currencies such as Bitcoin or Ethereum, and VASPs can apply the same CDD processes they are already familiar with.

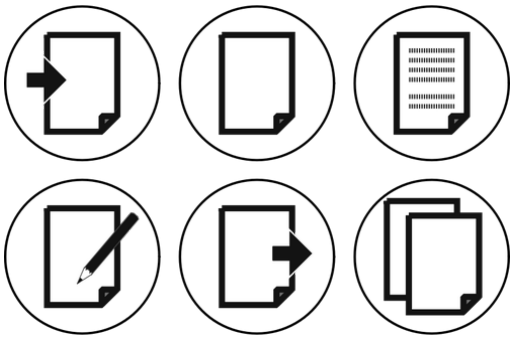
Transaction monitoring

MWC's privacy-preserving technology does not prevent a VASP from being able to monitor a customer's transactions with that VASP (e.g. deposits, withdrawals, trades), and comparing transaction patterns and volumes with the expected behaviour, based on the VASP's understanding of the nature of the customer or their business (as determined during the CDD checks). As a party to its customers' MWC transactions (either as a recipient, in the case of deposits, or a sender, in the case of withdrawals), a VASP has visibility of the transaction details. This allows the VASP to detect transaction patterns that do not match that customer's expected behaviour, and investigate further to determine whether the unexpected behaviour is suspicious.

Although MWC technically isn't bound to traditional addresses a VASP still needs to provide a way to deposit for example through an HTTP reverse proxy omitting the userid which can be seen as the address. This allows VASPs to issue a unique deposit address to each customer, thus allowing MWC deposits to be unequivocally attributed to a specific customer.
MWC also requires that customers provide a payment address in order to receive withdrawals, allowing VASPs to conduct sanctions screening, or restrict withdrawals to whitelisted addresses. In this respect, MWC is no different from other virtual currencies, and the same tools and procedures for transaction monitoring can be applied to MWC.

Record-keeping

In the same way that VASPs can monitor a customer's transactions, they can also keep records of those transactions. For deposits, VASPs can record the customer's identity, the amount of that was deposited, the destination address (i.e. the deposit address the VASP created for that customer), the source address (where the customer deposits funds from), and the transaction ID. For withdrawals, VASPs can record the



customer's identity, the amount that was withdrawn, the source address (i.e. the VASPs's address from which the coins are being sent), destination address and the transaction ID. It is important to note that the VASP always knows the payment address that a withdrawal is sent to.

The only difference between MWC and other virtual currencies in terms of the information available to be recorded by the VASP is that if the customer makes a deposit, the VASP will not automatically have visibility of the source address. If it wishes to do so, the VASP can request that the customer provide the source address for the VASP's records. However, this is not a requirement under the FATF Recommendations.

Suspicious Transaction Reports

The ability to carry out transaction monitoring ensures that a VASP is able to detect any suspicious activity on the part of its customers. The ability to maintain records of its customers' transactions ensures that the VASP possesses adequate information to make suspicious transactions reports where appropriate.

Travel Rule

MWC was designed to be compliant with the Travel Rule. The required originator and beneficiary information can be attached directly to a transaction using the encrypted "message" parameter. (`-g, --message <message>`)

As the name implies, the contents of this field are encrypted when the transaction is added to the blockchain, thus preventing inappropriate or unauthorised disclosure of personal information.

Sharing Visibility of Shielded Transactions with Third Parties

On occasion it may be necessary to share transaction information with third parties. The protocol has been designed to support two features that enable the disclosure of shielded transaction information. The first is known as Payment Disclosure. This allows either party to a shielded transaction to generate a key which they can provide to a third party, thereby allowing them to view the details of the transaction (including the contents of the Encrypted "message" parameter), while ensuring that it remains shielded from the world at large. This feature will allow VASPs to share visibility of transactions with appropriate authorities or auditors in a confidential manner. We also anticipate that they may be leveraged as part of information sharing arrangements amongst VASPs, as part of information-sharing efforts, or between VASPs and statutory regulators, to facilitate market surveillance and the identification of suspicious transactions.

Development

The MWC project was announced in February 2019 and it's mainnet launched in November 2019. The Team behind MWC consists of highly skilled and experienced professional Silicon Valley developers.

The MWC team provides technical coordination and leadership, and a point of contact for both users and regulators. Importantly, the MWC team investigates and responds to issues, bugs and problems, and provides information and resources support to MWC's users through a number of online channels, including GitHub, Discord, Telegram and Email.

Conclusion

MWC was designed to protect consumers' financial privacy while retaining compatibility with global AML / CFT standards, including the FATF Recommendations that were adopted in June 2019. Importantly, the privacy provided by MWC does not prevent regulated entities from fulfilling their regulatory obligations. The Developers of MWC aim to provide accurate and objective information regarding regulation.