# MobileCoin

A crypto-currency delivering best user experience in blockchain world

November 13, 2017

# 1. Motivation

Applications that make use of crypto-currency and blockchain technology are often difficult to deploy in practice, particularly in mobile environments. Implementors currently face deployment challenges around device resource constraints, transaction times, and key management, all of which often contribute to a negative user experience. Mobile applications don't have the ability to synchronize an entire multi-gigabyte blockchain, minutes-long transaction times are unacceptable for typical use cases, and end users are not equipped to reliably maintain secret keys over a long period of time.

As a result, most attempts at building a compelling crypto-currency user experience unfortunately resort to trusting a third party service to manage keys and validate transactions. This largely sacrifices the primary benefits offered by crypto-currency to begin with.

MobileCoin is an effort to develop a fast, private, and easy-to-use cryptocurrency that can be deployed in resource constrained environments to users who aren't equipped to reliably maintain secret keys over a long period of time, all without giving up control of funds to a payment processing service.

# 2. Experience

The technical design of MobileCoin is entered around a target user experience for integrating crypto-currency into mobile messaging apps like WhatsApp or Signal. A user should be able to install the app, enter a 4 digit PIN, and send receive funds to from other users addressed by their phone number or user identifier. Transactions should take less than a second, funds should immediately be available for use, and neither the messaging service nor any other third party should learn anything about a user's account balance or transaction history (such as who is paying who). At any point, a user should be able to reinstall the app or get a new phone and regain secure access to their funds simply by entering a 4-digit PIN. Payments should also be possible across apps and networks.

# 3. Design

MobileCoin starts by recognizing that not all clients are capable of participating in a P2P network, and proposes a federated approach instead. The MobileCoin network is made up of nodes, and each node is designed to serve users.

Nodes do the heavy lifting of tasks that are ill-suited for user clients, such as maintaining an expansive ledger and processing high-throughput low-latency transactions, but are designed such that a node operator does not have access to their users' funds and does not learn anything about their users' balances and transaction history.

This is accomplished via a layered approach, combining several levels of protection for defense-in-depth and forward-secrecy.

## 3.1 SGX

All MobileCoin nodes run in an SGX secure enclave. An SGX enclave is isolated from the host OS in hardware-encrypted RAM, which prevents the node operator from being able to "see" into the enclave, although care must be taken to avoid information leaks through memory access patterns. SGX also supports a feature known as remote attestation, which allows a remote client to determine that a server is running a specific piece of software inside an SGX enclave over a network. By doing remote attestation before establishing encrypted communication channels between nodes, the entire MobileCoin ledger always remains sealed within SGX enclaves across the entire network, which means that the ledger, while "public" and distributed to all MobileCoin nodes, can never be accessed or viewed by humans (even the operators of the MobileCoin nodes) so long as SGX and the MobileCoin software remains secure.

## 3.2 Transaction Privacy

MobileCoin does not rely solely on SGX for maintaining transaction privacy. Transactions employ CryptoNote[1] one-time addresses and one-time ring signatures, so MobileCoin still maintains transaction privacy through unlinkable addresses if an attacker is able to defeat SGX and view transactions on the network.

## 3.3 Consensus

Owing to its federated nature, MobileCoin nodes use the Stellar Consensus Protocol[2] to synchronize a ledger, which allows for sub-second transactions under normal circumstances, along with decentralized control and flexible trust. This also allows nodes to avoid storing a full blockchain of transaction history, since it is only necessary to maintain a ledger of address → value mappings, as well as the list of used key images to prevent double spending.

This provides a certain measure of forward secrecy[3] . Even though one-time ring signatures hide the source of a transaction among a large set of possible candidates, using SCP means that information can be discarded entirely after a transaction completes, rather than being maintained in a block chain forever.

## 3.4 Key Management

Running MobileCoin in an SGX enclave allows nodes to securely manage keys for users. A client can perform remote attestation to its MobileCoin node before transmitting its keys into the remote enclave along with a short recovery PIN. The MobileCoin node can then rate limit authenticated access to the keys, while the enclave prevents the node operator or anyone who compromises the node from circumventing the software and attempting to brute force access to the keys directly. In this way, user keys can reside safely in a node and survive across application reinstalls or lost devices, without having to trust the node operator or the security of the node computer, and without having to memorize or safely store extremely long recovery passphrases.

---

[1] https://cryptonote.org/whitepaper.pdf

[2] https://www.stellar.org/papers/stellar-consensus-protocol.pdf

[3] https://en.wikipedia.org/wiki/Forward_secrecy

# 4. Life of a MobileCoin Transaction

1. At install time, Alice's client generates a MobileCoin keypair and short recovery PIN.
2. At install time, Alice's client performs remote attestation with its MobileCoin node, establishes a secure communication channel into the remote enclave, and transmits its keypair along with its recovery PIN.
3. To send Bob a payment, Alice's client looks up Bob's public key.
4. Alice's client generates a CryptoNote one-time public key for Bob.
5. Alice's client generates a CryptoNote one-time ring signature for the transaction.
6. Alice's client transmits the pending transaction to its MobileCoin node.
7. The node synchronizes the transaction to the network using Stellar Consensus Protocol. The MobileCoin ledger is updated to reflect the transaction's output values, as well as the key image generated as part of the one-time ring signature in order to prevent double spending. Everything else is discarded.
8. Bob's MobileCoin node uses Bob's CryptoNote tracking key to recognize the one-time public key.
9. Bob's MobileCoin node sends Bob's client a message, which can then calculate the private key that corresponds to the generated one-time public key.
10. Bob has now successfully received a payment.

The transaction completes in less than a few seconds, all transaction and balance information is kept private within SGX enclaves across the network such that the transaction itself is never visible, transaction privacy is further protected with CryptoNote one-time addresses and one-time ring signatures if an attacker is able to forge SGX remote attestation in order to connect to the network with modified software. The node operator or attackers who compromise a node never have access to user keys or user data, and users can switch phones or reinstall the app and maintain access to their funds simply by entering a 4-6 digit PIN.

# 5. MobileCoin Wallet

MobileCoin is designed so that a mobile messaging application like WhatsApp or Signal can serve as a MobileCoin wallet. The messaging application can securely recover the information it needs in order to construct and validate transactions from its MobileCoin node on install or reinstall, and receive updates from its MobileCoin node without having to maintain persistent network connectivity. A MobileCoin wallet integrated into a messaging app like WhatsApp or Signal can also look up payment destination public keys based on username, and transmit an encrypted message with a deniable signature to the recipient of a transaction in order to prove where the payment originated.

# 6. Team

## Joshua Goldbard - CEO

Joshua is a high school dropout who thinks deeply about narratives and information systems. Working in Telecom for much of his adult life, Joshua developed, managed, and implemented networks of significant complexity. His expertise on mobile systems as well as his passion for cryptocurrency as an information network governing systems of value help him lead this project.

## Moxie Marlinspike - CTO

Moxie is a cryptographer with a passion for secure communications. As the lead developer of Open Whisper Systems, Moxie is responsible for the entirety of Signal (with over 10M users), and the cryptographic protocols governing Whatsapp (with over 1.3 billion users), both world-leading cryptographic messaging systems. Moxie is also responsible for the development of SSL certificate pinning while helping to lead security at Twitter. Moxie loves adventure and travels the world by land, sea, or air.

## Shane Glynn - General Counsel

Shane is a lawyer with a passion for adrenaline and logical consistency. In his work at Google, Shane has helped bring many products to life including those from the Android teams. Shane delights in understanding novel problems in relation to the law and imbibes the current state of cryptocurrency regulation with zeal. As an accomplished sky diver, Shane enjoys falling from the sky almost as much as reading SEC case law.

## Advisors

### Li Xiaolai

One of the largest holders of Bitcoin in the world, early investor in EOS, Sia, Zcash, and Yunbi.com.

### Eric Meltzer

Partner, INB. Advisor to Basecoin and Stream.

### Dax Hansen

Partner, Perkins Coie. One of the premier crypto focused lawyers in the world.

### Todd Huffman

Founder and CEO, 3scan, co-founder of the BIL conference.

# 7. Private Presale FAQ

### How many MOB tokens will be issued?

250 million. This supply is fixed at issuance and can never increase.

### How many tokens will be sold in the presale?

37.5 million tokens.

### How much is being raised?

$30M.

## How much will the tokens cost in presale?

0.80 cents per MOB.

## Are there any volume discounts, or special discounts offered?

No. 0.80 cents per MOB is the fixed and only price at which MOB tokens are being offered.

## When is the presale closing?

Soft commitments are due Dec 12.

## Is there a lockup period?

No lockup for supporters, the teams tokens are locked for 1 year and vest for the next 4 years.

## When will the token be listed on exchanges?

MOB has a hard commit from one exchange for listing at the end of December, and will likely get listed on other exchanges in Q1-Q2 2018.

## When will the ERC20 token be converted to the live network token?

The team intends to ship MobileCoin within 6 months of the completion of the presale. That being said, software projects, particularly those using new technical systems are hard and we will always prioritize shipping something safe over shipping quickly.

## Why have an ERC20 token in advance of the MOB network going live?

The conversion event from ERC20 to the live token is a unique opportunity to force 100% of users to undergo a "tumbling" process that renders the initial MOB network token allocations extremely anonymous. Other anonymous cryptocurrencies suffer from an easily de-anonymized initial transaction set, something which we aim to avoid with this technique. Second, allowing a period

of exchange will increase the number of addresses in the ledger, which improves the effectiveness of Cryptonote's privacy.

## What is a secure enclave?

Secure Enclaves are hardened computer systems that exist inside some modern computers. With the right technical implementation, these enclaves can provide zero-knowledge computing environments allowing nodes to operate without knowing what code is running.

## What is a secure key management system?

By using a simple technical system involving the secure enclave, users can recover their crypto assets using a 4-6 digit pin, even on a new device. This pin is also used, in combination with other identity heuristics, to authorize transactions.

## How will the token sale proceeds be used?

100% of the proceeds will be used to develop open-source software, and tools and infrastructure to support the Mobilecoin protocol and ecosystem.