# MobileCoin: Defense in Depth

Joshua Goldbard
j@mobilecoin.com
mobilecoin.com

## Introduction

MobileCoin was built to enable mobile applications like **Signal** to send digital payments without compromising on user security. Transactions complete in just a few seconds, and all transaction information is kept encrypted end-to-end between the parties involved.

This article covers our security strategy for building a safe and secure digital currency. We will discuss why decentralization is important, how Bitcoin offers digital gold, and why digital gold is not the digital cash needed for payments. Next, we'll discuss what CryptoNote offers for distributed ledgers, how the MobileCoin ledger further protects users, and how remote attestation can help prove that servers you don't control are running the right software.

MobileCoin's software is composed of 7 defensive layers, each providing increased security:

- Layer 1: Open-Source
- Layer 2: Decentralized Governance
- Layer 3: CryptoNote
- Layer 4: Confidential Transactions
- Layer 5: MobileCoin Ledger
- Layer 6: MobileCoin Consensus Protocol
- Layer 7: Secure Enclaves and Remote Attestation

## Layer 1: Open-Source Code

Open-source technology is publicly auditable. To build trusted systems, we must start with making our code public. In doing so, we support the community in verifying that the intention of our design matches our implementation. We can build secure software in a world where anyone can audit our technology, which is why we are committed to keeping our payments protocol open-source, now and forever.

## Layer 2: Decentralized Governance

Commerce on the Internet has come to rely almost exclusively on centralized financial institutions serving as trusted third parties to process electronic payments.[1] Centralized payment networks are convenient, but they offer few data protection guarantees, meaning that users are exposed to security risks and abuse by intermediaries.

With the introduction of the bitcoin whitepaper by Satoshi Nakamoto in 2009, the world got its first taste of an peer-to-peer electronic payment system with decentralized governance. Satoshi's vision for Bitcoin was "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."

Using physical cash is one way to allow payments between two people in person without a centralized third party. Cash is by-and-large anonymous, but it's impossible to use over the Internet. It is difficult to offer the safety of cash over the internet, but we approach this level of safety using a well-designed decentralized payment network.

The reason that decentralized payment networks can provide better consumer protections is simple: In a decentralized payment network, the only person who controls your money is you. When you use Visa or PayPal or even the ACH debit network, you give up control of your money as soon as you use the network. Centralized payment networks carefully monitor all financial traffic to collect a trove of transaction information that can be sold to the highest bidder.

In a decentralized payment system, there is no controlling authority who stands to profit by reducing user security at the protocol level. Decentralized governance is a baseline prerequisite for a payments system that values security over profit.

When a user initiates their first transaction with Bitcoin, a unique pair of a public key and a private key is created. Each of the keys consists of a long string of alphanumeric characters that help to keep a user's holdings secure in the digital ecosystem. The private key is required to initiate a transfer; as long as you never share your private key, your funds are safe.

Bitcoin transactions are stored in a public record, backed up and recorded on thousands of servers on the internet. All of this data is available to anyone using block explorers, websites that allow you to search the ledger for a transaction. Users can choose between many

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

different versions of block explorers, This makes it easy for anyone to verify a payment without trusting a third party. No single organization or government has control over what data is available to the public. This level of public access to the public ledger was revolutionary in 2009.

Block explorers can do more than just search for a transaction - they are also used to search for your wallet and your history of transactions. This includes your entire history of payments sent and received, the amount, the date and time, and more. In order for the Bitcoin ledger to be publicly verifiable and visible to everyone, all of the transaction data and metadata is stored unencrypted.

The tradeoff of using the public ledger, is your personal financial history, all of your transactions, are viewable to anyone. When it comes to protecting personal financial data, Bitcoin offers no encryption or protection from snooping. With a complete copy of all transaction history, money can be watched as it flows from one bitcoin address to another, allowing anyone to connect the dots between addresses that are known to belong to particular individuals or organizations.[2] There are several companies who have already analyzed the publicly available data and linked the bitcoin addresses to identities. Anyone with access to the right tools can access your personal financial history, and sell their reports to the highest bidder.

Bitcoin has widely been called “digital gold." Considering Bitcoin's alchemical combination of mathematics and computer science, this is an apt analogy. Bitcoin is better than gold because it is divisible and digital. Like counting gold, bitcoin takes time to verify a transaction, 10-60 minutes to complete a transaction. At 10 transactions per second, Bitcoin was not designed for fast payments. Digital gold like the elemental metal gold is not instantaneous for payments and that’s okay. There's value in having a slow moving digital asset, but it's probably not how you're going to pay for a cup of coffee.

## Layer 3: CryptoNote

[2] Simon Barber. Bitter to Better - How to Make Bitcoin a Better Currency. http://elaineshi.com/docs/bitcoin.pdf

In 2012, Nicolas van Saberhagen, an unknown anonymous author, published the **CryptoNote whitepaper** describing a new distributed ledger protocol called CryptoNote. At its core, CryptoNote is an attempt to improve on the design of Bitcoin to create an encrypted ledger.

CryptoNote introduced two innovations: ring signatures and one-time addresses. Ring signatures make it harder to statistically analyze the network by changing the direct links between buyers and sellers used in Bitcoin into probabilistic links between sets of possible buyers and sellers. Every transaction has a set of possible ancestors which makes tracking payments in the public ledger much more difficult.

CryptoNote's one-time addresses allow payments to be received using numerical aliases that are indistinguishable from random numbers for everyone except the intended recipient. Essentially, every transaction in Bitcoin publicly shares the recipient's pseudonymous address, while CryptoNote ledgers publish the recipient's address in an encrypted format that protects user data.

## Layer 4: Confidential Transactions

CryptoNote ledgers are significantly more secure than Bitcoin, but they still leave the amount of each transaction in plain sight. One potential solution was published in 2016 by Shen Noether, called **Ring Confidential Transactions** (RingCT). RingCT protects the amount exchanged in each transaction using cryptography. Rather than publish the value that is exchanged, RingCT transactions include a mathematical proof that the transaction is balanced, meaning that the recipient didn't receive more money than the sender spent. This originally required a computationally intensive proof, but a more efficient algorithmic approach called Bulletproofs was introduced by Bünz et al. in 2017 that has greatly improved performance. It is now possible to use transactions with protected amounts without reducing the throughput of the payments network.

## Layer 5: MobileCoin Ledger

MobileCoin Ledger takes transactions built with CryptoNote signatures and RingCT and adds two new improvements: membership proofs for transaction inputs and redacted transaction records.

When a transaction is prepared by a user, it contains a ring signature with a double-spend proof. What's a double-spend proof? One of the many ground-breaking elements of Satoshi's

Bitcoin electronic payment system was that it solved the long-standing "double-spend" problem that plagued cashless spending. Through the implementation of time-stamped transactions that are unanimously verified by a distributed network of validators, it was no longer possible for a person to spend the same funds twice.

In addition to the double-spend proof, the MobileCoin Ledger's ring signature also contains the proofs-of-membership for transaction inputs. Membership proofs allow the transaction to be validated without requiring disk access to the corresponding entries in the ledger. This closes a potential access-pattern side channel that could allow a malicious actor to observe the particular set of inputs used to construct the transaction. When a valid transaction is ready to be published in the MobileCoin ledger, the membership proofs are ***deleted*** and only the double-spend proof and the new transaction output are added to the public record. These "redacted transactions" make it difficult to link and deanonymize users through analysis of the public blockchain.

Redacted transactions also necessarily imply that the public blockchain entries do not contain enough information for the complete transaction history to be revalidated in an audit. Our solution is to provide two separate mechanisms for audit support. All blocks are signed as they are published by the code that performs the validation and redaction for publication.

## Layer 6: Consensus Protocol

The redacted transactions that are written to the public MobileCoin  hide the probabilistic links between buyers and sellers that are used in CryptoNote, but the complete transactions still need to be validated and checked for attempted double spending and counterfeiting.

All cryptocurrencies rely on a distributed network of equivalent nodes to cooperatively agree on the validity and ordering of transactions. MobileCoin has developed a high-performance, byzantine fault tolerant protocol for distributed agreement called the MobileCoin Consensus Protocol (MCP), based on the **"federated byzantine agreement" described by David Mazieres**. MCP adds an additional security enhancement.

Rather than agreeing on sets of transactions, validator nodes agree on the cryptographic hash of encrypted sets of transactions. This allows the consensus algorithm to operate independently of the MobileCoin Ledger protocol validation code so that the potential attack surface is minimized.

A key feature of federated byzantine agreement protocols like MCP is that each node operator independently controls the configuration of a trusted set of peers, called a quorum. Sensitive data, even in an encrypted form, is never shared beyond the web of trust defined by these quorums.

## Layer 7: Secure Enclaves and Remote Attestation

At least some of the code running on the nodes that participate in MCP must be able to view the complete transactions. However, the operators of these nodes don't need to see this data themselves. The final layer of the MobileCoin system confines the sensitive transaction data and all of the code that operates on it in a "secure enclave", bringing the latest advancements in confidential computing to cryptocurrency.

A secure enclave provides strong guarantees about the confidentiality and integrity of the software actions being performed inside. Using a secure enclave, we can conceal the complete transactions even from the operators of the nodes that participate in MCP.

MobileCoin implements secure enclaves using **Intel's Software Guard eXtensions (SGX)** technology. SGX additionally offers a "remote attestation" system that can be used to prove that code that claims to be running in a secure enclave is running in a secure enclave (and on real hardware rather than a simulator as well!). Put simply, remote attestation gives us more confidence that a remote computer is running the right software, right now. This makes it much harder for operators to cheat in our system, and basically impossible for an operator to deny responsibility if they are ever caught cheating.

In short, the MobileCoin network becomes a network of blind oracles who simply agree on a set of encrypted strings. No information about who is transacting with whom, or for how much is revealed, even to the operators of the nodes that validate the transactions.

## Bringing it All Together

MobileCoin's defense-in-depth for protecting user data starts by establishing a very high baseline using established technologies like ring signatures, one-time addresses, and RingCT.

On top of this foundation we've added secure enclaves and careful information management to securely delete the last traces of identifying information left behind by Cryptonote in our redacted public .

Node operators or malicious attackers who compromise a node can't access user keys or user data.

MobileCoin was built to restore security without compromising on convenience. We are excited to see what the world does with the technology we've built. Here's to a brighter, safer future.