MobileCoin: Defense in Depth

Secure, Privacy-Protecting Payments that Scale

MobileCoin is a new privacy-preserving payments network designed for use in chat apps.

We have developed a number of open source software components that work together to deliver a high quality user experience without compromising on privacy. Our goal is to make payments software you'd feel safe using in apps like Facebook Messenger, WhatsApp, and Signal.

This article introduces our "defense in depth" strategy for building a digital currency that works online like cash works in the real world.

Broadly, MobileCoin's software is composed of many defensive layers, each providing increased privacy protection:

- 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

We will discuss why decentralization is important, how Bitcoin offers digital gold, and why digital gold doesn't work for payments. Next, we'll discuss what CryptoNote offers for distributed ledgers, how MobileCoin's ledger further protects users, and how remote attestation can help prove that servers you don't control are running the right software, right now.

Layer 1: Open-Source

Open-source technology is auditable; closed-source technology is not. To build trusted systems, we have to start with making our code public and supporting the community in verifying that the intention of our design matches our implementation. We can only 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

Presently, most payments are made using physical currency or centralized payment networks. Physical currency is by-and-large privacy protecting, but it's impossible to use over the Internet. Centralized payment networks are convenient, but they offer few privacy guarantees, exposing users to security risks and abuse by intermediaries. It is difficult to offer the privacy of cash over the internet, but we can get very close with 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 the second you use the network. Any of these operators can stop or reverse a transfer or lock up your funds. When you use a centralized payment network, your money isn't yours anymore. 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 privacy at the protocol level. Decentralized governance is a baseline prerequisite for a payments system that values privacy over profit.

When Satoshi Nakamoto introduced Bitcoin in 2009, the world got its first taste of a decentralized payment system that offered a practical solution for the problem of double-spending. When you use Bitcoin, you have a set of keys which allow you to transfer your money. The only person who can initiate a transfer is you - as long as you keep your keys safe! Bitcoin transactions are stored in a public record on the internet, so anyone can verify a payment. This is great when you're sending payments across the Internet, but it's not necessarily the best idea if you want financial privacy. The only privacy protection included in Bitcoin's design is pseudonymous addresses for receiving payments.

The problem with having a history of all transactions viewable in public is that, well, all of your payments are public! Now instead of just the people routing the payments being able to sell your information to the highest bidder, anyone who looks at the Bitcoin transaction history has the ability to get your information for free. With a complete copy of all transaction history, money can be watched as it flows from one pseudonymous recipient address to another, allowing anyone to connect the dots between addresses that are known to belong to particular individuals or organizations.

Not only is Bitcoin not private, but it's also slow, unscalable, and difficult to use. Bitcoin takes a minimum of ten minutes to complete a transaction (sometimes up to sixty minutes) and can only process about ten transactions a second. It also requires about as much energy as the entire nation of Ireland to operate.

Many have proclaimed Bitcoin to be “digital gold.” Considering Bitcoin’s alchemical combination of mathematics and computer science, this isn’t a bad analogy. Gold, the elemental metal, is also slow and difficult to use for payments. After all, you can only process transactions as fast as you can count the weight. 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

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

Layer 4: Confidential Transactions

CryptoNote ledgers are significantly more private than Bitcoin, but they still leave the amount of each transaction in plain sight. A 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

What if we could create a public blockchain that avoids publishing even the probabilistic links between buyers and sellers from CryptoNote?

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 constructed with a set of Merkle proofs-of-membership, and a double-spend proof. The membership proofs allow the transaction to be validated without requiring disk access to the corresponding entries in the blockchain. This closes an 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 blockchain, 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 impossible 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. On a longer timescale, zero-knowledge arguments are constructed that unambiguously demonstrate that all calculations were performed correctly.

Layer 6: MobileCoin Consensus Protocol

The redacted transactions that are written to the public MobileCoin blockchain 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 privacy-protecting enhancement. Rather than agreeing on sets of transactions, nodes instead 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 trusted 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 is designed so that mobile messaging applications like WhatsApp, Facebook Messenger, or Signal can easily offer digital payments without compromising on user privacy. Using an integrated wallet, a messaging application on a mobile phone can send MobileCoin transactions without having to maintain a complete copy of the blockchain and without ever needing to share the keys with a remote server.

Transactions complete in just a few seconds, and all transaction information is kept private between the parties involved. MobileCoin's defense-in-depth for protecting user privacy 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 blockchain. Node operators or malicious attackers who compromise a node can never access user keys or user data.

We designed MobileCoin to restore the privacy we have all given up for convenience, all without compromising on either. We are excited to see what the world does with the technology we've built. Here's to a brighter, privacy-protecting future.

Thank you to Moxie Marlinspike, David Mazieres, and Dan Boneh for their specific contributions to this project. We are pleased to also acknowledge the countless researchers on whose shoulders we stand. MobileCoin is the accumulation of decades of work into cryptographic systems and would not be possible without that effort.