

Monero Quick Facts



Overview

Recently, the threat group behind Sodinokibi ransomware publicly announced the switch from Bitcoin to accepting only Monero payments. The switch was motivated largely by the fact that Monero is inherently more difficult for law enforcement to track payments as well as the groups desire to remain anonymous; something Bitcoin doesn't offer to the extent of Monero. When a Bitcoin transaction is made the Bitcoin address and the transaction history are publicly recorded on the Bitcoin blockchain (referred to as the ledger). The public ledger is what allows you to associate the real world identity back to a Bitcoin address. With Monero the balance and transaction history are 100% private and not recorded on a public blockchain thus providing another layer of privacy.

Quick Facts

Arete has established accounts with leading Over the Counter (OTC) trading centers for digital assets, including Bitcoin (BTC) and Monero (XMR). As with all cryptocurrency transactions, Arete will perform due diligence on the wallet provided by the Threat Actor and provide an OFAC attestation prior to performing a transaction.

Monero transactions are performed by Arete staff and are on-demand to provide competitive and current market rates. Below is the current Monero fee structure:

- USD to XMR - cost plus 5% acquisition/transaction fee



Bitcoin	Monero
All Bitcoin transactions are posted to a public blockchain known (aka "ledger") along with information about the sender and recipient addresses and the amount of BTC transacted	Monero hides ALL transaction data to protect the sender/recipient privacy
Bitcoin is not completely anonymous. Wallet balances can be checked with freely available tools like blockchainexplorer.com.	Monero hides ALL transaction data to protect the sender/recipient privacy
Users have a "single" wallet ID. Bitcoin is received and sent from the same wallet ID.	Monero uses multiple different privacy technologies that hide the amount of money, along with the sender and recipient.
Bitcoin is considered "Digital Gold" as it's considered the most secure crypto currency	Developed with privacy and anonymity as central tenants. Monero uses Ring Confidential Transactions (RingCT) a form of BTC Mixing services where transactions are signed by a group of randomly chosen Monero owners with the same amount of XMR coins. The result of the transaction is complete anonymity where no one can tell who was involved. Wallet balances cannot be tracked publicly
Bitcoin is easily obtainable through sites like coinbase and coincafe. There are even some ATMs that can convert fiat currency to Bitcoin.	Monero offers "out of the box" anonymity with using stealth wallets, Ring Confidential Transactions (RingCT), and Kovri.