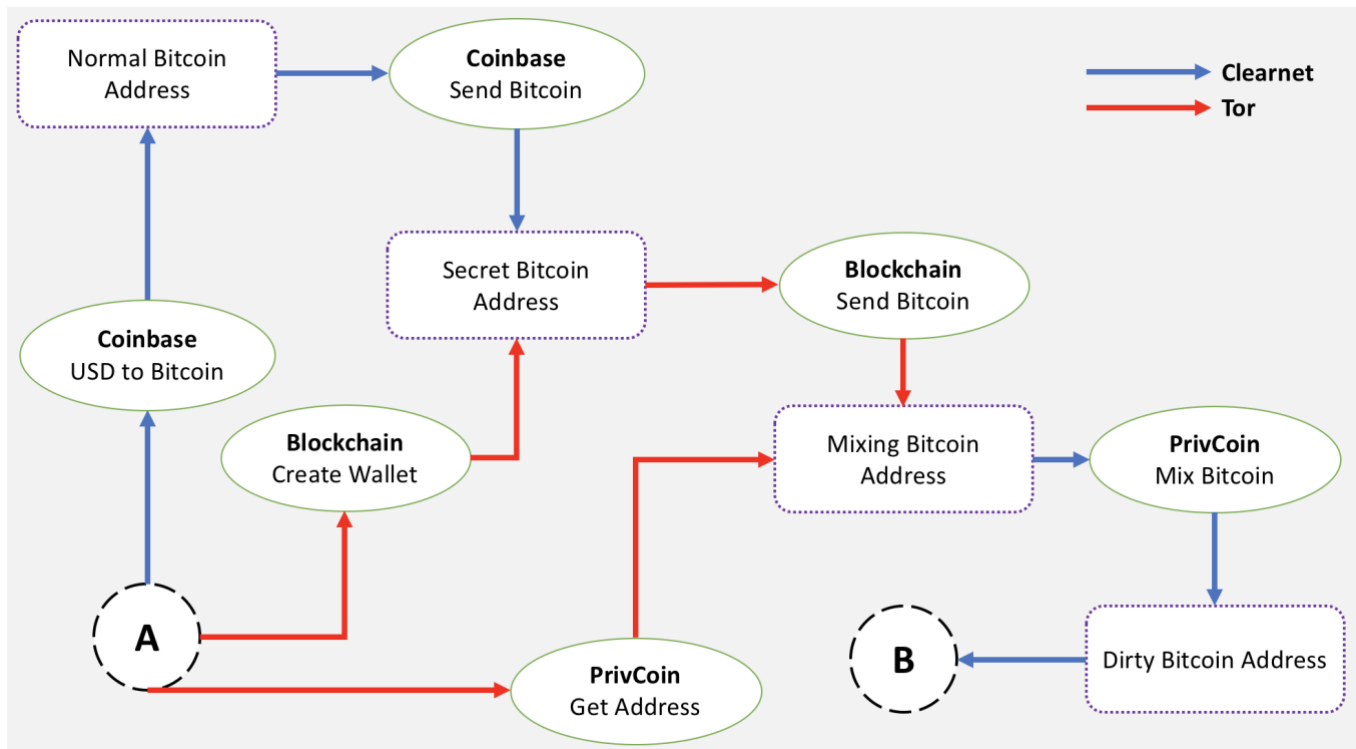


Laundering with Bitcoin

HingOn Miu
hmiu@andrew.cmu.edu



Say A wants to send B money, exactly A_money US dollars, and A knows B's bitcoin address as B_address. Assume B_address is public knowledge, or known by law enforcement to be dirty. Anyways, A wants to pay B secretly.

First, A should use secret_wallet.py to create secret wallet S with no IP trace via blockchain.info and Tor. A now has information of the secret wallet S, such as wallet identifier S_guid, wallet password S_password and bitcoin address of secret wallet S_address. S_address is not tied to A since network traffic is encrypted and IP is disguised.

Next, A should use btc_purchase.py to buy bitcoin with A_money via coinbase.com. A now owns bitcoin address A_address with address balance of A_bitcoin. A_address is tied to A since A's payment info is exposed to coinbase.com. And A should use btc_purchase.py to send A_bitcoin from A_address to S_address normally via coinbase.com. This particular transaction can be explained as normal daily payment since the identity of owner of

wallet S remains unknown. This transaction is tied to A since bitcoin transaction history of A_address is public.

Then, A should use secret_mixing.py to get a mixing address M_address with no IP trace via privcoin.io and Tor. A should set B_address as the forward address of M_address so that bitcoin transaction between M_address and B_address is mixed. M_address is not tied to A since network traffic is encrypted and IP is disguised.

Afterwards, A should use secret_transaction.py to send A_bitcoin from S_address to M_address with no IP trace via blockchain.info and Tor. The mixing service begins as A_bitcoin is received by M_address. This transaction between S_address and M_address is not tied to A since both addresses are not tied to A while network traffic is encrypted and IP is disguised. Finally, A_bitcoin is sent to B_address, which means A_money US dollars equivalent amount is deposited secretly to B with no tie to A.