United States: An Untraceable Currency? Bitcoin Privacy Concerns[1]

Bitcoin is often portrayed as an untraceable method of payment that facilitates illicit activities by enabling criminals to make and receive payments without being tracked. This depiction implies that users transacting in bitcoin can do so completely anonymously — that their identities will not be exposed. However, that is not necessarily the case. While bitcoin offers increased privacy compared to traditional payment methods involving a third-party intermediary such as a credit card provider, it is still not as anonymous as a cash transaction. In fact, there are many ways a person's identity could potentially be exposed in bitcoin transactions.

An Overview of the Blockchain

Bitcoin is not anonymous. As we explain below, it is pseudonymous — an important distinction. It is also a decentralized, peer-to-peer digital currency, having no third-party intermediary (for instance, a credit card issuer, merchant processor or bank) that is involved to verify a transaction between a buyer and seller. Since there is no third party, there must be another way to verify a transaction between two users and avoid the "double-spending" problem (i.e., a way of ensuring that a user does not spend bitcoin they have previously transferred).

This is where the blockchain, the truly revolutionary aspect of cryptocurrencies such as bitcoin, comes into play. A blockchain is a public, distributed ledger, in which every transaction is recorded. Unlike traditional payment systems in which the ledger is maintained by a single third party, a blockchain ledger is distributed across a group of computers (thousands of them), each with its own copy of the blockchain transactions. Each block of transactions in a blockchain is confirmed by users in the peer-to-peer network, called "miners," who compete to solve a complex computational problem. The first successful miner to validate the transaction broadcasts it to the network, which then checks the results. Once checked, the new transactions are added as a new block to the blockchain. In the case of bitcoin, the miner who first successfully verified this transaction gets rewarded by the network with newly created bitcoins. As of July 2016, the reward was reduced from 25 to 12.5 bitcoins, and it is expected that the reward will be further reduced to 6.25 bitcoins in 2021.

Anonymity vs. Pseudonymity

Because the bitcoin blockchain is a permanent public record of all transactions accessible by anyone at any time, it is not anonymous. Instead, the transactions in the blockchain are encrypted with public key cryptography that masks the real identities of the individuals behind the transactions. This makes bitcoin pseudonymous. In each bitcoin transaction, each user is assigned two digital keys: (1) a public key or address — the address is actually a hash derived from the public key, but for purposes of this article, we use these terms interchangeably — which everyone can see and is published on the

[1] Fenwick & West LLP, Article by Tyler G. Newby and Ana Razmazma 9 April 2018

VATANDOUST
Level 23, 52 Martin Place, Sydney NSW 2000 Telephone +61 2 9220 5138 | Facsimile +61 2 9220 5001
Email mail@vatandoust.com.au | Web www.vatandoust.com.au

bitcoin blockchain, and (2) a private key, which is only known to the user and is the user's "signature." The private key is used by others to verify that the transaction was in fact signed by that user. The bitcoin blockchain will only show that a transaction has taken place between two public keys (an identifier of 34 random alphanumeric characters), indicating the time and amount of the transaction.

Tracing Bitcoins Back to Individuals

Encryption might create the impression that these transactions are viewable but unmatchable to specific individuals. However, bitcoin is not as untraceable as encryption may imply. Tying an encrypted transaction to an actual individual is possible — it is not a remote risk. There are several ways this could occur.

Users who rely on a bitcoin trading exchange (such as Bitfinex, Binance or Kraken) to exchange currency for bitcoin have to divulge their personal information to that exchange to create an account. The information collected by the exchange varies, but normally includes, at a minimum, a user's first and last name, and, possibly, a phone number. The exchange may also collect a user's IP address. If these exchanges were subject to a data security breach, a user's personal information could be exposed. In addition, some centralized exchanges offer to manage users' bitcoin funds and users' private keys on their behalf.

There are also online wallet service providers that manage users' wallets on their behalf. A wallet is a software program that stores a collection of a user's public and private key pairs. The storage of private keys makes these centralized exchanges, and online wallet service providers, prime targets for criminals because, as discussed above, anyone with access to a user's private key will be able to create a valid bitcoin transaction. A hacker who accesses a user's private key can send all of that user's bitcoins to him or herself, or to any intermediary of their choosing. There have been several high-profile breaches of exchanges in the past, including the February 2014 hack of Mt. Gox, once the world's largest bitcoin exchange. The Mt. Gox attack resulted in a loss of 850,000 bitcoins then valued at $450 million. Thus, hackers who gain control over a user's exchange or online wallet account not only gain access to a user's personal information and transaction history but also to a user's bitcoin funds.

Exchanges are also increasingly subject to regulatory requirements that could lead to government entities accessing a user's personal information. Bitcoin valuation plunged recently when the U.S. Securities and Exchange Commission released a statement warning that online platforms trading digital assets that meet the definition of "securities" would be considered exchanges under the securities laws and need to register with the SEC or show exemption from registration. Although the SEC has not taken any action to date, this means that cryptocurrency exchanges could be subject to the stringent securities regulations applicable to national securities exchanges. Similarly, South Korea announced greater regulation of bitcoin earlier this year. Under the new South Korean regulation, users will only be able to deposit into their exchange wallets if the name used on the exchange matches the name on the user's bank account. Exchanges are also already subject to certain legal

VATANDOUST
Level 23, 52 Martin Place, Sydney NSW 2000 Telephone +61 2 9220 5138 | Facsimile +61 2 9220 5001
Email mail@vatandoust.com.au | Web www.vatandoust.com.au

requirements, such as responding to subpoenas, which could require them to share personal information with governmental authorities if required by law. For instance, the U.S.-based exchange Coinbase was recently ordered by a court to turn over to the Internal Revenue Service information regarding approximately 14,000 of its customers. A brief review of several exchanges' online privacy policies indicates that exchanges will share a user's information as needed to comply with their legal and regulatory obligations.

Blockchain Analytics

It is also possible to identify users simply by analyzing transactions on the blockchain. Companies like Elliptic and Chainanalysis have built businesses based on blockchain forensics. These companies use analytics on the bitcoin blockchain to link bitcoin addresses to web entities and help their customers assess the risk of illegal activities. Their customers include exchanges but also government entities. In fact, it became public last year that the IRS is using Chainanalysis's software to track potential tax evaders.

Several studies have also shown that it is possible to use network analysis and other methods to observe and potentially tie back blockchain transactions to certain websites and individuals. Specifically, one 2013 study by researchers at the University of California, San Diego and George Mason University showed that it was possible to tag bitcoin addresses belonging to the same user by using clustering analysis of bitcoin addresses. A small number of private transactions with various services were used to identify major institutions (such as exchanges or large websites). From there, the researchers were able to get information on the structure of the bitcoin network, where transaction funds are going and which organizations are party to it. Another study by researchers at ETH Zurich and NEC Laboratories Europe that looked at bitcoin transactions in a small university sample found that using behavior-based clustering techniques could unveil in a typical university environment the profiles of up to 40 percent of the users.

How Bitcoin Users Can Enhance Their Privacy

Despite these privacy issues, bitcoin users need not despair — there are ways to enhance one's privacy on the bitcoin blockchain. First, a bitcoin user can use a new bitcoin address for each transaction and will thus receive a new public key for each transaction, making it more difficult to trace one specific individual's transactions to the same address. This is actually the approach that was envisioned by Satoshi Nakamoto, bitcoin's pseudonymous (and still unknown) founder, who recommended in the paper that first introduced bitcoin using "a new key pair ... for each transaction to keep them from being linked to a common owner." Second, a bitcoin user can take some additional precautions to minimize the risk of traceability on third-party exchanges. The user could use the anonymous Tor browser to access the exchange and create an account without including any real personal information; the user's IP address and personal information would not be exposed. Third, the user could avoid storing bitcoins in online third-party wallets, and only use offline desktop wallets; that reduces the exposure to exchange hacks. Fourth, bitcoin mixing algorithms, such as CoinJoin, link

VATANDOUST
Level 23, 52 Martin Place, Sydney NSW 2000 Telephone +61 2 9220 5138 | Facsimile +61 2 9220 5001
Email mail@vatandoust.com.au | Web www.vatandoust.com.au

users and allow them to pay together such that the bitcoins are mixed. This makes it harder to identify a particular user because only a group of transactions is published on the blockchain (although studies and research have shown that even CoinJoin presents weaknesses and could allow linking back to a particular individual).

The Monero Alternative

These privacy issues have not gone unnoticed and alternative cryptocurrencies with an increased privacy focus have emerged. Monero is the most prominent of these alternatives. Unlike the bitcoin blockchain, which, as we have noted, is based on a two-key (public and private key) cryptography, the Monero blockchain is based on unique one-time keys and ring signatures. With ring signature technology, the actual signer is pooled together with a group of possible signers, forming a "ring." This creates a distinctive signature that can authorize a transaction. When an individual initiates a Monero transaction, the verifier is able to establish that a transaction came from a group but is not able to determine the identity of the initiator whose private key was used to produce the signature. As a result, the Monero blockchain does not identify a specific sender, and the receivers' addresses and the transaction amounts are hidden. Monero has become the cryptocurrency of choice for privacy-focused users.

Although bitcoin is a decentralized and unregulated payment method, users should understand that this does not mean that their bitcoin transactions are anonymous and hidden from scrutiny. The public nature of the blockchain combined with the increasing threat of government regulation can lead to the identification of users engaged in transacting the currency.

VATANDOUST
Level 23, 52 Martin Place, Sydney NSW 2000 Telephone +61 2 9220 5138 | Facsimile +61 2 9220 5001
Email mail@vatandoust.com.au | Web www.vatandoust.com.au