Welcome to this lecture where we’re going to be discussing Monero, and explaining its three major anonymity methods with you.

Following Monero’s launch in April 2014, it has has progressed, slowly and steadily for the most part, to claim its place among the major cryptocurrencies. Monero has long played the tortoise rather than the hare, at least until Monero jumped up and started sprinting in August of 2016.

Now besides being accessible through darknet networks such as I2P and Tor, Monero integrates several sophisticated cryptographic techniques to achieve an impressive level of overall privacy. So let me go over the 3 major anonymity methods of Monero with you now.

1) Unlinkable Stealth Addresses

Address re-usage is one of the common privacy bugbears of Bitcoin. Receiving multiple payments to a single address allows anyone who knows your address to track its balance and all related incoming and outgoing transactions. What’s worse is that even separate addresses in your wallet may become linked due to the way Bitcoin handles change! For this reason, Bitcoin core developer Luke Dash Jr. said that, “only a fool would use Bitcoin as it is today for darknet.”

No such privacy issues exist in Monero. All destination addresses are obscured within its blockchain, such that only the sender and receiver can identify them. Analysis of the Monero blockchain will never reveal the destination address at which one receives XMR. Instead, only a cryptographic hash of the destination, unique to each and every transaction, is visible. Only the sender or receiver can decode this to reveal the actual address. These obscured addresses are known as “stealth addresses.”

Beyond the obvious privacy benefits, stealth addresses have a number of ramifications, such as making it impossible to determine the current XMR distribution among addresses.

You can verify this yourself by putting a publicized Monero address (which likely contains some XMR) into the Monero block explorer:

2) Indistinguishable Separated Transaction Units

If you were to send XMR to an “address,” in reality the encoded stealth address described above, it’d arrive as several discrete payment units. For example, if you were to send 18 XMR it would arrive in whole number units of 10, 5 and 3 XMR, totalling 18 XMR. Each unit would appear on the Monero blockchain as being transferred to it’s a unique and distinct stealth address.

This same process is applied to any change which is returned to the sender and any fees paid to miners. This property makes the task of tracking specific payment amounts vastly more complicated. As an example, an adversary who knows a vendor’s product costs an unusual amount – let’s say precisely 11.88101234 XMR – could conceivably monitor the blockchain (likely via some automated process) for that amount’s appearance and then focus their analytic techniques and resources on related transactions. By sorting all transactions into unremarkable units, the Monero system ensures otherwise-distinctive sums are “lost in the crowd” of un-differentiable whole units.

3) Untraceable Ring Signature Payments

There’s definite synergy between the way Monero handles addresses and payment amounts. This 3rd technique, Ring Signatures, is another neat piece of cryptographic engineering which makes it even harder for a Monero user to be identified. Ring Signatures are essentially an advanced, mandatory system for transaction mixing.

In order to understand Ring Signatures, it’s necessary to understand that, as in Bitcoin, a Monero “address” is essentially a specialized form of a cryptographic public key. Funds associated with that “address” may only be moved through the use of its paired private key.

To continue the earlier example: you send 18 XMR to a shop. This transmission then gets sub-divided into 10, 5 and 3 XMR streams, all of which flow to separate, stealth versions of the shop’s Monero address. Here is where Ring Signatures come into play…

From the point of view of an adversarial tracker, the private key which authorised any 10, 5 and 3 XMR sums ever sent across the Monero blockchain, since its 1st (“genesis”) block, becomes a possible signatory to the transaction. The number of possible signatories depends on the “mixing depth” you set; for example a depth of 4 implies that any 3 Monero keys which have been used are also potential signatories to your transaction… And as your transaction is split into units which all possibly derive from this “group signing” pool… Ring signatures ensure that transactions can’t be decisively traced back to specific computer’s IP address (or their Tor or I2P proxy address).

To sum it up – it’s pretty damn hard to identify Monero users

The combination of the elements mentioned makes Monero a veritable maze of mirrors for any adversarial tracker. No definite linkage can be determined, only the fuzzy possibility of linkage. To put it bluntly, the best blockchain forensic techniques which could feasibly be applied to a Monero transaction would likely prove inadmissible or at least unconvincing if presented as evidence in a court of law. Even Monero miners are unable to censor transactions. It’s far more likely that some element beyond the scope of Monero’s code would result in de-anonymizing its average user.

However everything has a price…

The anonymity methods mentioned, are expensive in terms of data requirements; there’s always a trade-off. Additionally, Monero’s blocksize grows with increasing demand (although a penalty fee is in place to prevent bloat). For this reason, Monero uses more system resources than Bitcoin and most other cryptocurrencies. This may become a serious obstacle to Monero’s future success.

So that’s everything for this episode on Monero, I hope you enjoyed it! See you in the next.