COS 597E **Charles Marsh (crmarsh@)**
Fall 2014 **Lecture 6: Bitcoin & Anonymity**

Defining Anonymity

People have different views on what it would mean for Bitcoin to be "anonymous." Some people say that Bitcoin is an anonymous digital currency (with no caveats), while others believe that you can be tied to your Bitcoin transactions in some way.

At a literal level, anonymity means "without a name." Bitcoin addresses are public key hashes rather than real identities (Computer scientists call this *pseudonymity*).

The distinction here is that with pseudonymity, you can link together transactions and identify them as belonging to the same user. In this sense, **anonymity is pseudonymity with unlinkability** (i.e., different interactions of the same user with the system aren't identifiable).

As a concrete example: with Reddit, you pick a long-term pseudonym, so your posts can be related back to the same ID even if it can't be linked back to you; with 4Chan, you make posts with no attribution whatsoever.

Why do we need unlinkability?

- Many Bitcoin services require real identity.
- Linked profiles can be de-anonymized by a variety of side channels (e.g., people posting on the Bitcoin forum requesting donations, so you can link one of their addresses to their identity on the forum).

Formalizing Anonymity

We could come up with several reasonable notions of unlinkability, e.g., unlinkability could mean that it's difficult to:

- Link different addresses of the same user.
- Link different transactions of the same user.
- Link sender of a payment to its recipient.

But we'd also like to be able to quantify anonymity. To do so, we can define an **anonymity set**, which is the crowd into which one attempts to blend. This is calculated as follows:

- Define an adversary model.
- Reason carefully about what the adversary knows, does not know, and *cannot* know.

Ethics of Anonymity

If you have a cryptocurrency that doesn't have anonymity built into it, you could have privacy properties that are much worse than traditional banking, because we need the entire blockchain to be public in order to rely on consensus, etc. So anonymity in this sense is definitely useful.

There's a legitimate worry, however, that anonymity can allow for money laundering, etc. That said, the main problem for criminals using Bitcoin for money laundering is that there's a large bottleneck in moving dollars in and out of the cryptocurrency.

It's very difficult to design a system that *only* gives you the good aspects and provides a technological guarantee against the bad. We can make an analogy to Tor, which provides an "anonymous communication network" such that the sender and receiver of a message are unlinkable. This is used by normal people and professionals, but also to disseminate malware and child pornography. Overall, we agree that the existence of Tor is better for the world than the nonexistence of Tor.

Anonymity and decentralization are in conflict. Interactive protocols with a bank are hard to decentralize, but decentralization is often achieved via public traceability (i.e., to enforce security).

Linking Transactions

Say Alice has three addresses with 5, 3, and 6 Bitcoins respectively, and she wants to buy a teapot for 8 BTC. Alice might want to combine the 5 and 3 into a single transaction, this would link those two addresses together, telling the system that the same owner owns both addresses. You can apply this reasoning transitively across the entire network.

Alternatively, if the teapot costs 8.5 BTC, then Alice might combine her 6 and 3, and send back 0.5 BTC to her change address. It's hard to tell which address is the change address, in this case (i.e., is the 8.5 BTC or the 0.5 BTC?). In A Fistful of Bitcoins, they propose the heuristic that each address is only used once as change (this is an idiom used in most wallet software).

If you look at cluster graphs, you'll find that there's a very high degree of centralization in service providers (e.g., exchanges). Most flows pass through one of these providers in a traceable way. But it's still very difficult to then relate these addresses to real-world identities, unless a government agent has subpoena power over a service that you've used.

In summary: if it's just a regular guy coming after you and you've been careful not to link any of your addresses to your digital identities (i.e., through forum posts with donation links), you're probably okay.

Network Layer De-anonymization

The first node to inform you of a transaction is probably a source of it. Therefore, when you hear about a transaction, you can do an IP lookup and then associate Bitoin and IP addresses.

The solution: **use Tor**. However, Tor is intended for low-latency activities like web browsing, so there's been some investigation into other approaches, like mix nets.

Intermediaries

To protect anonymity, you could also use an intermediary, like a dedicated mixing service. In effect, when you put money in, you get it out later at a different address. Online wallets already have this property (e.g., when you put money into a bank and withdraw it later, you aren't being given the same dollar bills)–do they provide anonymity? Actually, yes. It's hard to link what comes in with what comes out.

While dedicated mixing services promise not to keep records, online wallets are more reputable and often regulated. These typically require proof of identity to keep records (so you have no anonymity with respect to the wallet). Users often trust them with their Bitcoins and keep them for longer, which increases their anonymity set.

Principles of Mixing Services

These are mostly part of the Mixcoin proposal written by Arvind, Joe, and others.

1. Use a **series of mixes**, where mixes should implement a standard API to make them easy-to-use. *This could be a problem because you might put in a weirdly specific amount, which makes it easy to link your input to an output.*

2. **Uniform transactions**: all mixes agree on a standard chunk size such that they're all compatible with each other and input-output pairs cannot be matched based on the size of the transaction (i.e., because they're all the same).

3. Client-side software must be **automated**.

4. Fees should be **all-or-nothing**: to avoid taking fees at each step in the mix (and thus avoid the standardized chunk size at some step in the multi-mix), mixes should either take the entire transaction or take nothing, maybe with a 1% probability based on a public source of randomness (e.g., the blockchain itself).

There aren't any existing mixes that actually follow these principles.

Coinjoin

Why would we want decentralized mixing?

- It makes theft impossible.
- It could lead to better anonymity.
- It's more philosophically aligned with Bitcoin.

When you have a Bitcoin transaction with multiple inputs, these don't necessarily need to come from the same individual–that's just how Bitcoin is typically used, rather than a technical requirement.

This is the inspiration for **Coinjoin**: make a transaction with three inputs and three outputs, then execute a standard Bitcoin transaction. Each individual can generate a signature entirely separately (i.e., after they've checked that they'll be receiving the correct amount at a new address). We treat this operation as one mixing round and expect that you maintain the principles described before (e.g., series of mixes, standard transaction amount).

In the end, there's no way to discern which output address belongs to which input.

Problems

- How do you find peers?
- Your peers know the input-ouput mapping! In effect, to construct the transaction, we have to collect an input-ouput pair from each peer, and so the participants know the matching.

To solve the peer anonymity problem, a strawman solution would be to exchange inputs, disconnect and reconnect over Tor, then exchange their output addresses. That way, you can't tell which input is connected to which output.