bitcoin

CS1699: Blockchain Technology and Cryptocurrency

12. Anonymity

Bill Laboon

What Do We Mean By "Anonymity"?

- From the Greek - *an-* "without" + *onoma* "name"
- Is Bitcoin anonymous?
  - YES - If we mean, can be used without your real name
  - NO - If we mean, can you use no "name" at all

Bitcoin is Pseudonymous

- Also from the Greek: *pseudēs* "false" + *onuma* "name"
- Your name is your address/PK, so you do have a "pseudo-identity", even though you can generate more

What About Anonymity?

- The technical definition of anonymity:
- A pseudonymous system which also provides
- *unlinkability* (individual but distinct interactions should not be traceable to a single identity)

Why Do We Even Want Anonymity?

- Recall that every Bitcoin transaction that has ever taken place is recorded (directly or indirectly) on the blockchain
- Motivation One: Have the same level of privacy that you do when using a bank/credit card (where only some others have access to your transaction history)
- Motivation Two: Make it computationally infeasible for anyone to track the participants in a transaction

The Ethics of Anonymity

- Personal privacy - do you want your co-workers to know your salary?
- Business privacy - do you want your competitors to know who your suppliers are?
- Political privacy - do you want others to know to whom you send political contributions?

On The Other Hand…

- Truly anonymous currency can be used to evade taxes, launder money, participate in “dark markets”, gamble illegally, etc.
- Example: WikiLeaks

Squaring the Circle

- Potential idea: can technology be implemented such that users can reap the benefits of anonymity as long as they are doing good things with it?

- No! You have to take the good with the bad *if we want to be decentralized*. Otherwise, we would depend upon a central arbiter to determine the good/bad use cases.

- Particular "bad" and "good" use cases look the same from the point of view of the technology!

Crypto-anarchy

- Being able to communicate and exchange information with no way for others to monitor you weaks the power of the state
- With Bitcoin, money is now a form of communication
- https://www.activism.net/cypherpunk/crypto-anarchy.html

Is Pseudonymity Enough?

- Perhaps - but not if your goal is *privacy*!
- Blockchain is public - and if your real identity can be linked to your address, you can easily be de-anonymized
- Many, many, many ways to do this
- It is very difficult to avoid leaking information

Deanonymization Via Side-Channels

- Side channel = indirect (i.e. off-chain) leakages of information
- Examples:
  - Paying with Bitcoin at a coffee shop exposes your physical body to barista
  - Analysis of usage times can be used to determine time zone
  - Re-using or posting addresses
  - Special meaning behind vanity address?

Unlinkability

1. It should be hard to link together different addresses of the same user.
2. It should be hard to link together different transactions of the same user.
3. It should be hard to link the sender of the payment to its recipient.

Anonymity Set

- Turns out the third concept is rather difficult (since identity A needs to verify that they sent a certain amount to identity B, as does identity B - and we are vulnerable to traffic analysis)
- But what we can do is hide the transaction in with a bunch of others
- The *anonymity set* - the set of transactions an adversary cannot distinguish from your own transaction

Anonymity Set

- Adversaries may be able to know that you made a transaction, but they can't tell which one of some set
- The larger the number of possible transactions, the better able to hide you are
  - "Cicada strategy"
- Note that this is not one specific number! Different adversaries may have more motivation/skill/resources to minimize the anonymity set further than others

Anonymity Set

- To calculate, need to determine:
  - What the adversary DEFINITELY (trivially) knows
  - What the adversary PROBABLY DOESN'T know
  - What the adversary CANNOT know

Taint Analysis

- "How related are two Bitcoin identities?"
- If coins from *S* always end up in *R* even if they go through intermediaries *a*,*b*,*c*…, *S* and *R* are highly "tainted" (have a high taint score)
- Ameliorated by avoiding address re-use

Next Class..

- Improving the anonymity of Bitcoin
- Alternative cryptocurrencies which provide better / easier anonymity