UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

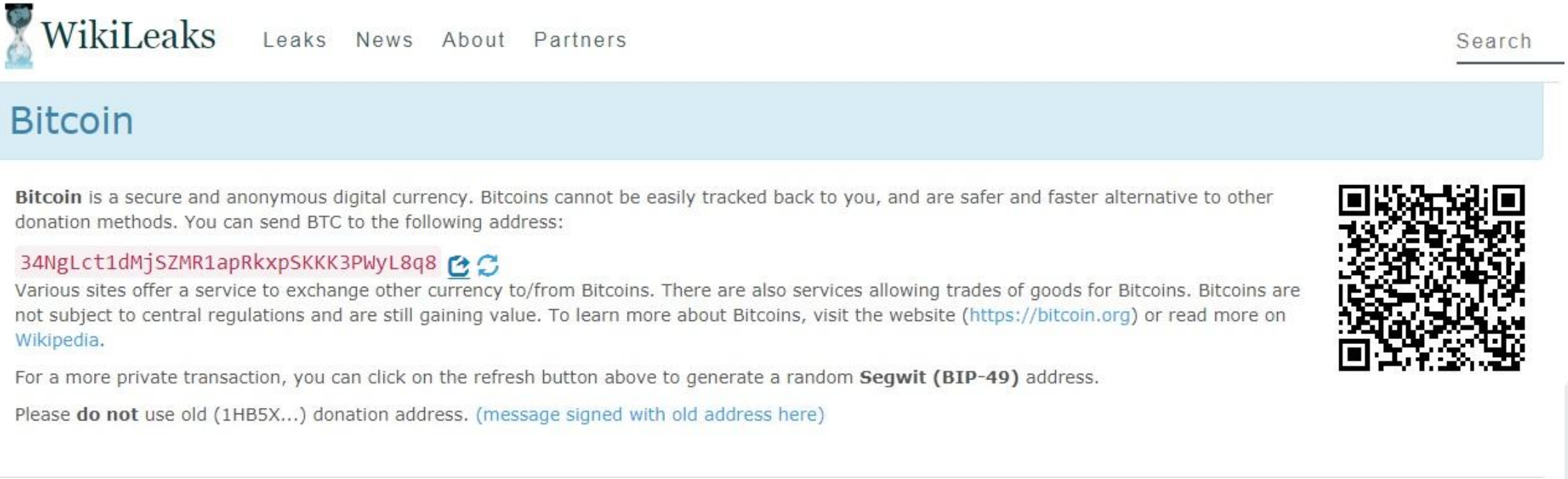
ciie
Centro de Investigación
e Innovación Educativa

Introducción

4.5 Anonimidad y servicios de mezcla

Algunos usuarios de Bitcoin dicen que es Anónimo

Página de donación de Wikileaks:



¿Qué significa Anónimo?

Definición de anónimo:

El anonimato es el carácter o la condición de anónimo, es decir, que la identidad de una persona o entidad es desconocida. Esto puede ser simplemente porque no se le haya pedido su identidad, como en un encuentro ocasional entre extraños, o porque la persona no puede o no quiere revelar su identidad.

Anónimo == Sin un nombre

Definición de seudónimo:

El seudónimo es un nombre que utiliza una persona de manera intencional para publicar sus obras o libros. El seudónimo conlleva un nombre y un apellido o, en ocasiones, sólo un sustantivo.

Seudónimo == con nombre identificatorio
(pero distinto del real)

Anonimidad en ciencia de la computación

Direcciones Bitcoin:

Las direcciones Bitcoin son claves públicas, pasadas por funciones hash en vez de identidades reales.
La blockchain contiene una lista de todas las transacciones realizadas en la red. Si una persona puede atar una dirección Bitcoin a una identidad real entonces tal vez puede obtener otras identidades que hicieron transacciones con la primera.

Anónimo == Seudónimo + irrastreable

Las diferentes interacciones del mismo usuario con el sistema no deben ser correlacionables entre sí.

Seudónimos vs. Anonimidad en redes

- Las redes de teléfono cuando queremos obtener sus servicios nos piden un documento que acredite una identidad y una factura de un servicio a nuestro nombre.

- Las redes sociales cuando nos registramos no nos piden ningún tipo de identificación para hacerlo ni para su uso.

¿Por qué es necesaria la irrastreabilidad?

1. Distintos servicios de Bitcoin requieren una identidad real. Por ejemplo: Las casas de intercambio nos van a pedir una foto de un DNI para el registro (para cumplir leyes de AML y KYC) y probablemente un recibo de ingresos para determinar el monto de BTC que nos podrán vender.
2. Los perfiles relacionados pueden ser de anonimizados de un varias maneras.

Definición de irrastreable en Bitcoin

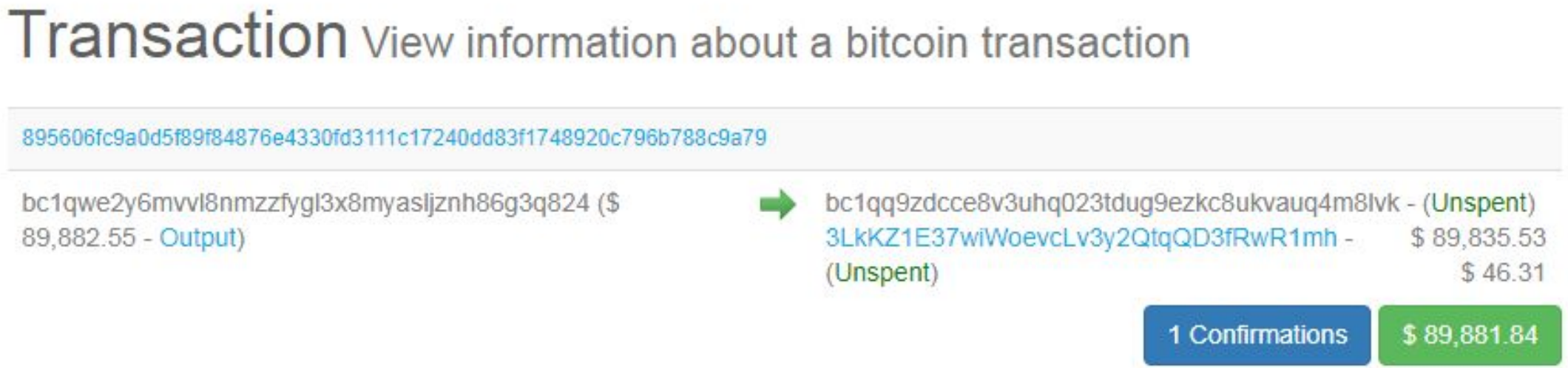
1. Tiene que ser difícil de poder relacionar distintas direcciones Bitcoin a un usuario en particular.

2. Tiene que ser difícil de poder relacionar transacciones Bitcoin a un mismo usuario.

3. Tiene que ser difícil relacionar al emisor y receptor de un pago realizado en Bitcoin.

Ejemplo de transacción Bitcoin

Una transacción Bitcoin:
895606fc9a0d5f89f84876e4330fd3111c17240dd83f1748920c796b788c9a79

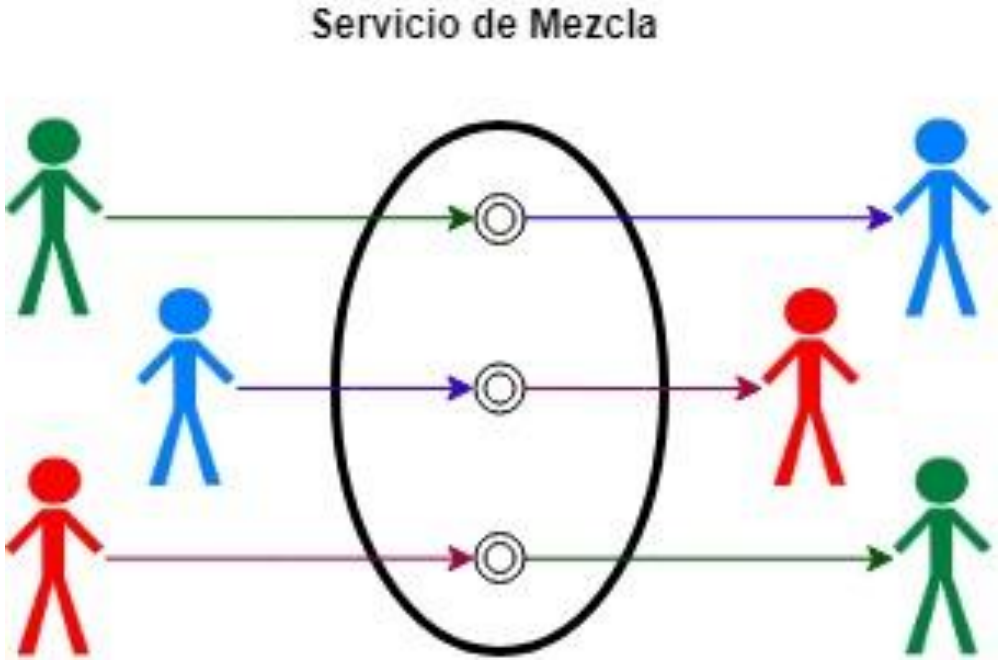


¿Por qué criptomonedas anónimas?

- Las criptomonedas basadas en una blockchain (registro de todas las transacciones), son públicos y abiertos, entonces cualquier persona puede realizar ingeniería para intentar de rastrear personas a transacciones.
- Sin anonimidad y privacidad para realizar transacciones (como el dinero en efectivo), Bitcoin sería peor que los sistemas bancarios tradicionales.
- Por suerte, este “problema” es sabido dentro de la comunidad y constantemente se trabaja en buscar soluciones y mejoras.

Para proteger nuestra anonimidad podemos usar un intermediario

Hay varios mecanismos que pueden hacer que el análisis de la blockchain sea menos efectivo. Una técnica es la mezcla de transacciones, y es muy simple de comprender: si se quiere anonimato, se utiliza un intermediario. Los usuarios envían BTC a un intermediario y recuperan las monedas que fueron depositadas por otros usuarios. Esto hace que sea más difícil rastrear las monedas de un usuario en la cadena de bloques



Servicio de Mezcla dedicados

- Deben ser 100% confiables en que no van a mantener un registro de las transacciones que mezclaron.

- No deben pedir un registro de identidad para su utilización.

- A veces tienen un costo para su utilización.
  - Para mantener la anonimidad, utilizan un % de una transacción variable, de forma que no pueda ser utilizado para rastrear transacciones.

Billeteras Online y casas de intercambio

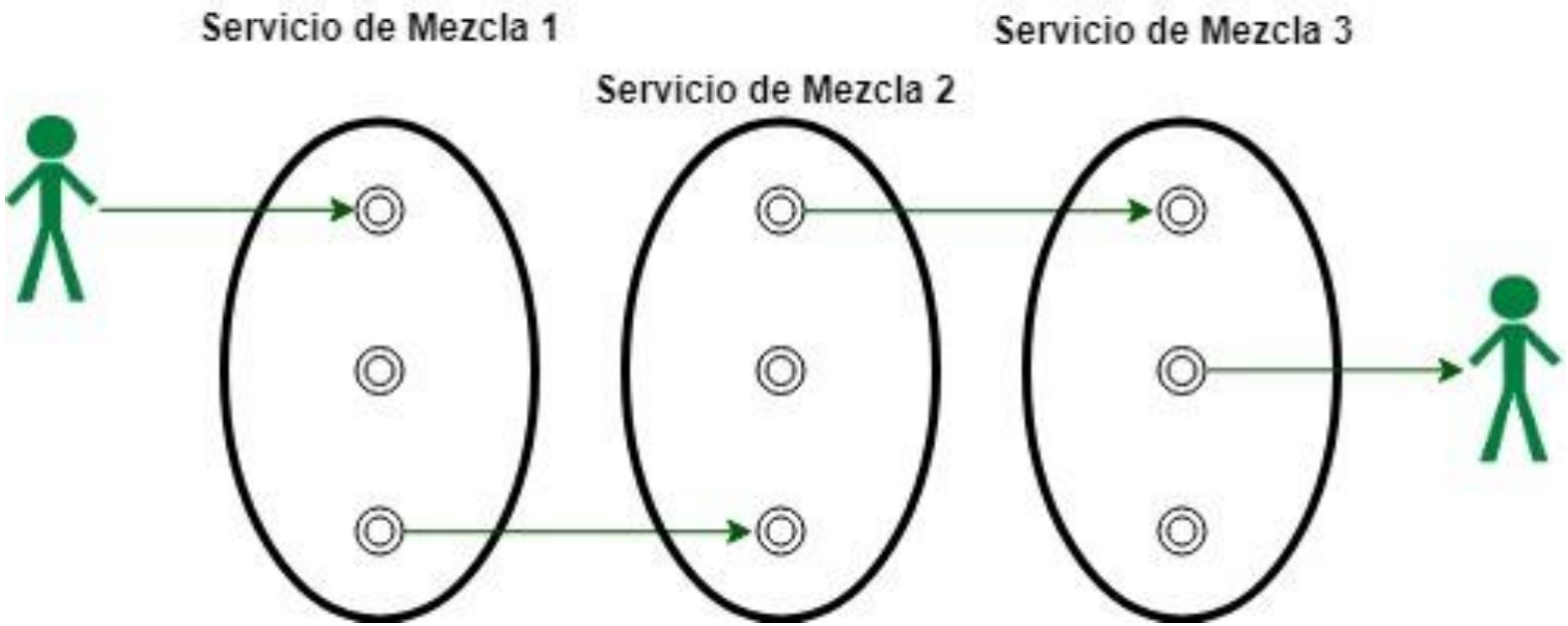
Son servicios en general regulados y con reputación generada a lo largo del tiempo:

- Típicamente requieren identidad y mantienen un registro de los usuarios y las transacciones que ellos realizan.

- Los usuarios confían en ellos para la custodia de Bitcoin
  - Recordemos que han sucedido infinidad de casos en donde han hackeado a estas casas de intercambio y los usuarios han perdido sus Bitcoin. El caso más emblemático es “MtGox (2014)”.

Funcionamiento de los servicios de Mezcla

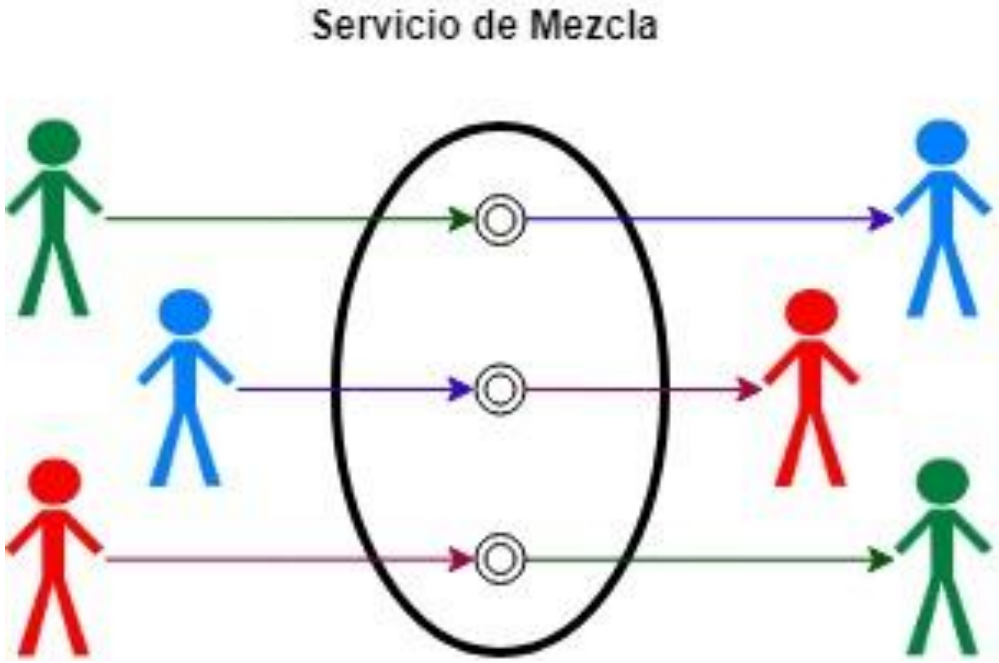
Comenzamos con un usuario tiene BTC en una dirección que asumimos que el adversario ha logrado vincular. El usuario envía la moneda a través de varios servicios, cada vez proporciona una dirección de salida recién generada al servicio. Siempre que al menos uno de estos servicios destruya sus registros de la entrada y salida, y que no haya fugas de información en un canal lateral, un adversario no podrá vincular los Bitcoin al usuario.



Funcionamiento de los servicios de Mezcla

Uniformidad de las transacciones:

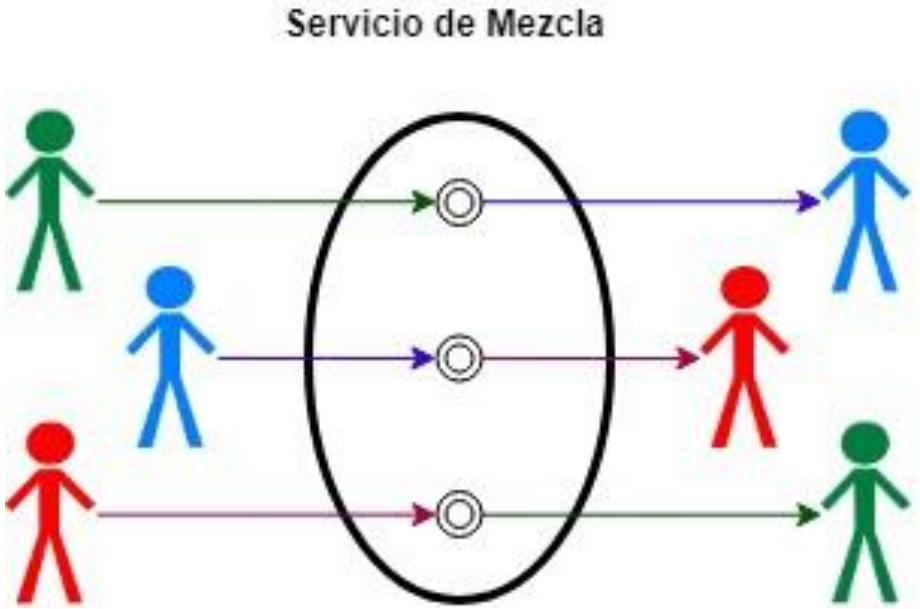
Si las transacciones enviadas al servicio de mezcla por diferentes usuarios tuvieran diferentes cantidades de bitcoin, entonces la mezcla no sería muy efectiva. Dado que el valor que entra en la mezcla y que sale debe conservarse, permitirá vincular las monedas de un usuario a medida que fluyen a través de la mezcla, o al menos disminuir en gran medida el anonimato.



Funcionamiento de los servicios de Mezcla

Las tarifas deben ser de todo o nada.

Las mezclas son negocios y esperan ganancias. Estos servicios pueden cobrar tarifas y para eso reducen una parte de cada transacción que envían los usuarios. Esto es problemático para el anonimato, porque las transacciones combinadas ya no pueden tener el tamaño estándar. (Si los usuarios intentan dividir y fusionar sus BTC ligeramente más pequeños de nuevo al tamaño del BTC original, se introducen riesgos de anonimato serios y difíciles de analizar debido a los nuevos vínculos entre las monedas que se introducen).



Funcionamiento de los servicios de mezcla

Servicios de mezcla en la realidad.

- Todavía en el 2019 no existe un ecosistema de mezcla funcional.
- Existen muchos servicios mixtos, pero tienen volúmenes bajos y, por lo tanto, poco anonimato. Peor aún, se ha informado que muchos servicios roban los BTC una vez enviados. Tal vez la dificultad de “generar" tal ecosistema es una de las razones por las que nunca ha funcionado.
- Dada la mala reputación de los servicios de mezcla, no mucha gente querrá usarlas. Cuantas más personas utilicen un servicio de anonimato, más anonimato se puede generar.
- Además, si no se gana mucho dinero prestando estos servicios, los operadores de estos servicios podrían verse tentados a robar fondos, perpetuando el ciclo de servicios de mezcla poco confiables.

Mezcla descentralizada - Coinjoin

Coinjoin.

Es una propuesta para la mezcla de BTC descentralizada. En este protocolo, diferentes usuarios crean conjuntamente una sola transacción de Bitcoin que combina todas sus entradas. El principio técnico clave que permite que Coinjoin funcione es el siguiente: cuando una transacción tiene múltiples entradas provenientes de diferentes direcciones, las firmas correspondientes a cada entrada son independientes entre sí. Así que estas diferentes direcciones podrían ser controladas por diferentes personas. No necesita una parte para recopilar todas las claves privadas.