Distributed Trust and Blockchains	Date: *21-10-2019*
Instructor: *Sujit Prakash Gujar*	Scribes: Anjul Gupta , Ramkishore S

Lecture 12: Bitcoin And Anonymity

1 Recap

Online Wallets

- An online wallet is similar to a local wallet, except the information is stored in some cloud owned by some company, and you can access it using an through computer application or an app on a smartphone.
- Advantage -
  - Some third party companies provide you the services, and provides easy to use and maintain interface.
- Drawback -
  - If organisation who manages the wallets are malicious, they can steal your bitcoins.

Bitcoin Exchanges

- Bitcoin exchanges works in a similar way to banks. They accept deposits of bitcoins and will promise to give them back on demand when asked by the customer. We can also transfer fiat currency like dollars into an exchange by transferring from your bank account along with Bitcoin payments.
- Advantage -
  - Exchanges connects the Bitcoin economy with the fiat currency economy, and hence it's easy to exchange them with one another.
- Drawback -
  1. Risk of a bank run.
  2. Owners of the banks may be crook and can run away with all your money.
  3. Most of these exchanges operate outside of any Government regulations. So, on one side there might be no support from the government while on the other, the government might deem the exchange itself illegal.
  4. Someone can penetrate the security of exchange.

Proof of reserve: Assures customer about the safety of the money they deposited.
Consists of proving two things. First is to prove how much reserve the exchange is holding. The second thing is to prove how many demand deposits it holds.

Currency Exchange Markets:

- Works on Supply and Demand.
- Formula for Price calculation :
  - T : The total transaction value mediated via Bitcoin by everyone participating in the market.

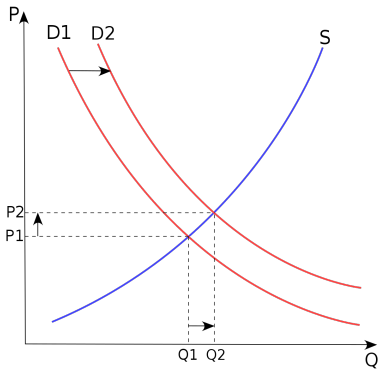

Figure 1: Supply Demand curve

- D : The duration of time that bitcoins need to be held out of circulation to mediate a transaction.
- S : The total supply of bitcoins available for this purchase which is equal to all of the hard currency bitcoins that exist minus those that are held by people as long-term investments.
- P : the price of a bitcoin, measured in dollars.

$$P = (T \times D)/S$$

2 Introduction

2.1 Anonymity

- Anonymity means no one knows real world identity. Anonymity refers to pseudonymity along with unlinkability.
- Pseudonymity means using public key hash as your identity.
- Unlinkability means that if a user interacts with the system repeatedly, adversary should not be able to be link one interaction to another. Properties that are required for Bitcoin activity to be unlinkable are :
  1. hard to link together different addresses of the same user.
  2. hard to link the sender of a payment to its recipient.
  3. hard to link together different transactions made by the same user.
- Bitcoin is pseudonymous. Bitcoin addresses are hashes of public keys. You don't need to use your real name to interact with the system, instead you use your public key hash as your identity.

Ethical Question: Can we design technology such that only the good uses of anonymity are allowed and avoid the misuse ?

2.2 Stealth Address

- Suppose Mohit wants to receive donation on some address. Mohit can make use of stealth addresses for this to achieve anonymity. Mohit can publicly post some static "permanent" address from which any sender Amit can derive new addresses, whom private key access is to Mohit only.
- Mohit can do so by using ECDSA public keys-

1. Mohit publishes public key g^x, where x is private key and address is $H(g^x)$.
2. Amit selects random number r, compute g^{xr} and sends money to this public key.
3. Amit communicates r securely to Mohit. Mohit can compute the correct private key xr to spend the money sent to (g^{xr}).

2.3 Possible attacks on Anonymity

2.3.1 Linking Addresses

- Suppose Mohit wants to buy a teapot that costs 8 BTC and his bitcoins are in three different addresses whose amounts are 3, 5, and 6 BTC, respectively. Mohit doesn't have an address with 8 BTC in any account, so he must combine two of his outputs as inputs to a single transaction and pay to seller.
- The transaction is published in the block chain, and anyone can see it and find out that the two inputs to the transaction belong to the same user.
- The adversary can repeat this process. If another address is linked to either one of Mohit's addresses in this manner, then the adversary knows that all three addresses belong to the same entity, and he can link all addresses in such way and can form a cluster of addresses belonging to Mohit.

2.3.2 Change Address

- Consider the same scenario as above. Mohit wants to buy a teapot costing 8 BTC and his bitcoins are in three different addresses whose amounts are 3, 5, and 6 BTC, respectively. Suppose now, the price of the teapot is 8.5 BTC. Mohit doesn't have the addresses with bitcoins that he can combine to produce the exact amount. So he create two outputs, one of the outputs is the seller's payment address and the other is a "change" address owned by Mohit himself.
- Transaction is recorded in the block chain, and adversary can infer that one of the output addresses also belongs to the same user.

2.3.3 Network Layer Attack

- It is based on the assumption that the first node to inform you of a transaction is the source of it with a high probability.
- When a node creates a transaction, it broadcasts the transaction to all the nodes connected to him. If many nodes on the network are run by a adversary, he can find the first node to broadcast the transaction. He can then link the transaction to the node's IP address and through it can find the real world identity of the person.

2.3.4 Taint Analysis

- Analysis to learn how two addresses are related. If transactions originating at suppose, address S, end up at address R, most of the time, than they have high taint score. Attackers can be able to link such addresses.
- Identifying of Individuals-
  1. Directly transacting : it is similar to tagging by transaction, where we can find out the receiver address by transacting with that receiver for eg. purchasing an item, storing bitcoins.
  2. Via service providers : service providers ask users for their identities.
  3. Carelessness : People often post their Bitcoin addresses in public forums.

2.4 Mixing

- Here, we can send our bitcoins to an address provided by the mix, and tell them a destination address to send bitcoins to. The mix will send them in your place.
- *Multilayer Mixing* :
  - Use a series of mixes, one after the other, instead of just a single mix, (similar to Tor which uses a series of routers for anonymous communication). As long as any one of the mixes in the series doesn't reveal the identity, we can expect that no one will be able to link our addresses.
- Challenges -
  1. Have to trust dedicated Mixes that they keep their promise and send back all our bitcoins.
  2. Mixes know our addresses.
  3. Fees - depends on them, they can take all or nothing.

2.5 Coin Join

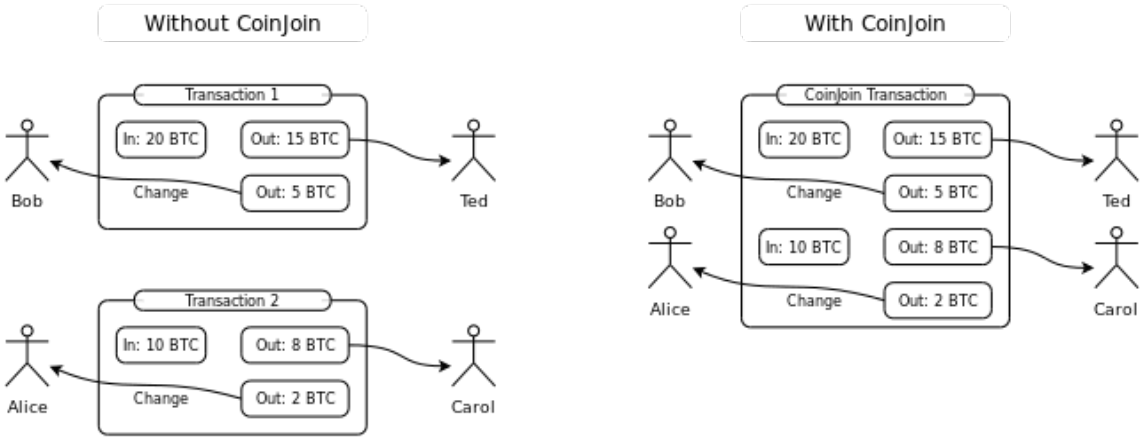

Figure 2: CoinJoin Transaction

- Decentralized mixing protocol.
- In this protocol, different users jointly create a single Bitcoin transaction that combines all their inputs.
- Steps in protocol -
  1. Find peers who want to mix.
  2. Exchange input/output addresses.
  3. Construct the transaction.
  4. Send the transaction around to each participant. Each peer signs after verifying their output is present.
  5. Broadcast the transaction.
- Challenges -
  1. How to find the appropriate peers.
  2. Peers know your input and output mapping.
  3. Denial of service. A peer could participate in the first phase of the protocol, providing its input and output addresses, but then refuse to sign in the second phase.

3 References

- Bitcoin and Cryptocurrency Technologies, Arvind Narayanan, Joseph Bonneau, Edward Felten,Andrew Miller, Steven Goldfeder
- https://hackernoon.com/blockchain-privacy-enhancing-technology-series-stealth-address-i-c8a3eb4e4e43
- https://en.bitcoin.it/wiki/CoinJoin
- https://en.wikipedia.org/wiki/Cryptocurrency_tumbler