Distributed Trust and Blockchains		Date:	*24 October 2019*
Instructor: *Sujit Prakash Gujar*		Scribes:	Aman Agrawal, Aditi Shrivastava

Lecture 13: Bitcoin and Anonymity, Zero Knowledge Proof, Local Coin

1 Recap

In Lecture 12 we discussed about Bitcoin Anonymity .

2 Introduction

Anonymity is one of the primary requirement of any crypto-currency. In bitcoins, payments are made either to public-key, public-key hash, script-hash, i.e. no real identity of neither sender nor of receiver gets revealed. But these addresses can be link to real identity of a person. It is called pseudo-anonymity. Anonymity refers to pseudo-anonymity together with unlinkability.

3 Bitcoin Anonymity

Bitcoin transactions are recorded on a block chain which is public, and anyone with a given address can look all its transactions. If someone can link that address to real world entity, then all transactions of that user can be linked back to his identity. i.e. In a coffee shop, if one transact using bitcoins and barista look up his transaction address, then barista knows a lot about user identity.

3.1 Pseudo-Anonymous

No real identity should be involved in any transaction. i.e. Bitcoin payments are not linked to a person or identity. A person's name, physical address, or email is found nowhere in the transaction.

3.2 Unlinkability

Unlinkability means that different interactions of the user with the system cannot be linked. i.e. different transactions of a user cannot be linked to one-another i.e.

- Hard to link two addresses are of same user.
- Hard to link two transactions pertaining to same user.
- Hard to link sender of payment to the receiver.

4 Ways To Achieve Anonymity in Bitcoin Transactions

4.1 Bitcoin Mixing

It is a process which tries to break the linkability or traceability by either creating temporary addresses or by swapping coins with other addresses of the same value. This makes the trail hard to follow on the blockchain.

4.2 Logless VPN

It is a virtual private network (VPN) in which network doesn't store the history of activities on their servers. It encrypts all of our Internet traffic and routes it through multiple servers of our choice at different locations before arriving at the final location.

For making it difficult to pinpoint and trace any person's identity, some logless VPNs also maintain a shared IP address for multiple users.

If we trust the VPN service provider that it will not log-on our activities,then we can use lossless VPNs to connect to our Bitcoin client as it is another way to improve the privacy of our Bitcoin transactions.

4.3 Tor- Onion Routing

In Tor network before transactions traffic reaches its final destination, Tor nodes encrypt and route our internet traffic to random computer nodes. Hence, it becomes extremely difficult to pinpoint the IP address or system from which the message or transaction was broadcasted.

4.4 Always use New Address for Transactions

We can generate any number of receiving address & hence use new address each time to send and receive bitcoins.

4.5 Buy/Sell Bitcoins in Cash

Doing face-to-face cash transactions is an anonymous way of doing bitcoin transaction. Services like LocalBitcoins provide this service.

4.6 JoinMarket

This is not a software or a service; rather, it's a market. In JoinMarket, market makers and takers come together to make special transactions called CoinJoin transactions. This market arranges the right amount of coins at the right time and the right place.

Takers of this market pay a nominal fee to the makers who are ready to mix their coins. The CoinJoin mechanism enables mixing without Escrow or centralized parties.

In this type of transaction, private keys are always under the control of the user. However, at present, the market is not so popular and there is not much traffic on it.

5 Steps to be taken to ensure anonymity in Local Bitcoins

- Use VPN or TOR

- Don't use your email or address or real name, instead use a fake name generator and burner email to register at LocalBitcoins
- Use public phones to coordinate meetings and arrange meetings at public place having facility of free wifi
- Reach the venue in public transport, transact, and wait for 2-3 confirmations. Private vehicle no. can reveal our identity.

6 Zero Knowledge Proof

In cryptography, it is a method by which one entity proves other entity that it knows some secret, without revealing that secret. i.e.
Prover (P) knows secret S
Verifier (V)

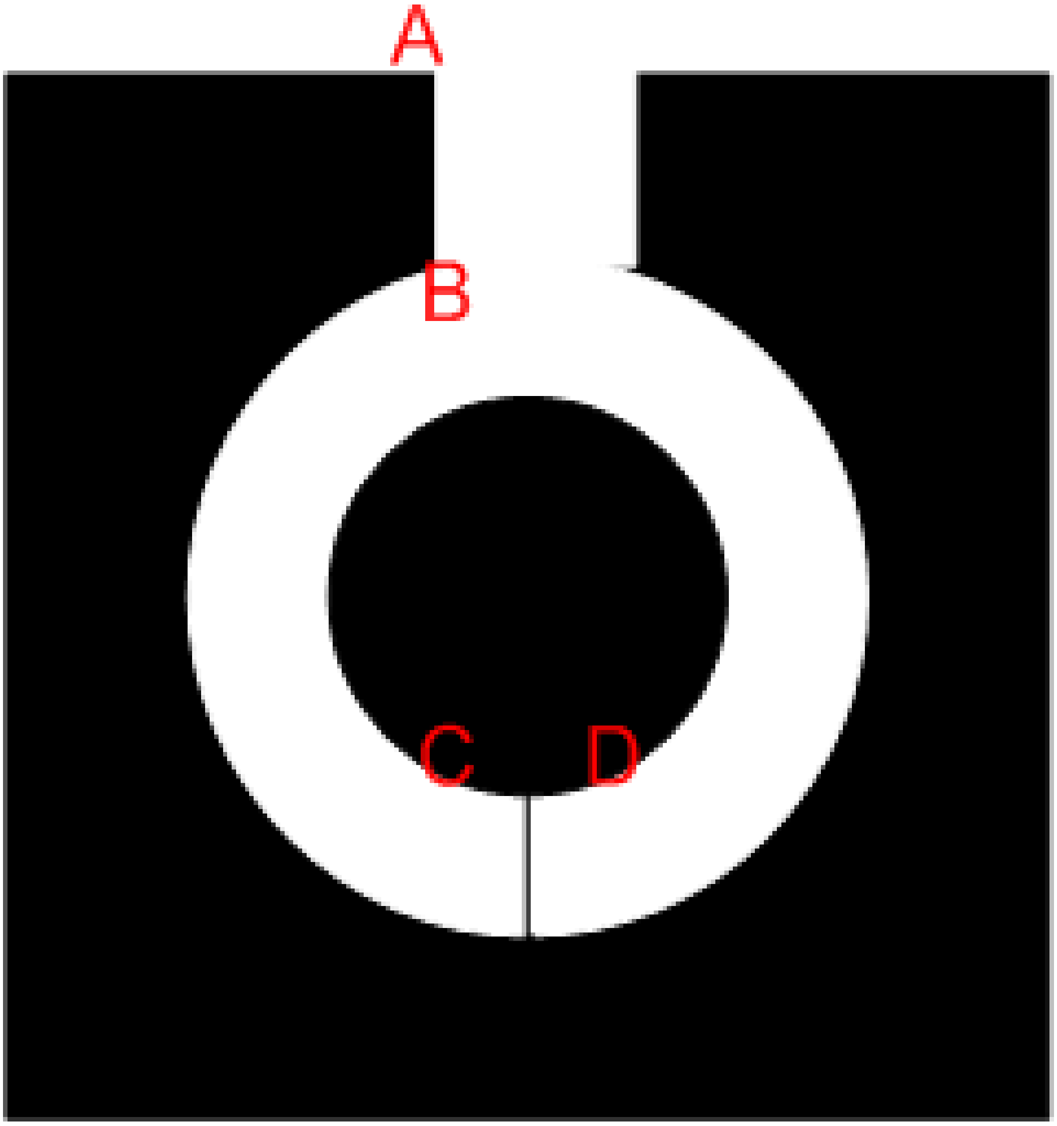
- P proves to V that it knows S
- V does not know S
- V cannot prove that P knows S

6.1 The simplest example is Cave and two people

P knows the password of the door, without revealing that password to V, it proves V that it knows the password:

- V is at point A.
- P goes all the way through the cave to the door or down the aisle C, or D. the aisle V does not see which way to go P.
- V moves to point B when P disappears in the cave
- V asks P, to come out from either left or right side of cave
- P using key of door comes out of the side he asked to do so.
- P and V repeat above steps couple of no. of times.

If P does not know the key of door, probability to escape from asked side is 50% in first attempt. Each time this probability gets halves and eventually after couple of steps it becomes negligible. Thus without knowing the secret key, it is very hard for P to succeed in each attempt. If V record a video of all this events, it is not required proof to convince third entity as P and V may agree on doing this so in advanced, also V can edit the video in such a way that only successful attempts are there in video. Thus it satisfy all above conditions, hence it is a zero knowledge proof.


A
B
C
D

6.2 Two different color balls and a blind man

Let A and B are two people. B is blind. A have two balls: one red and one green, but otherwise identical. For B, they are completely identical. A want to prove to B that they are different color balls and nothing else.

A gives the balls to B and asked him to either swap them or dont swap. Now A have to told whether B swappped or not by looking the balls. Since A know the order in which he gives balls to B, if same order comes, B didnt swapped, otherwise B swapped. If these balls were also identical in color, then A can correctly guess with 50% probability in his first attempt, and in each attempt probability of guessing correct reduced to half. Thus it becomes very hard for A to succeed in all steps. Thus A will only succeed in each step when balls are actually of different colors. By following these steps, B never learns which ball is green and which is red; indeed, he gains no knowledge about how to distinguish the balls.

7 ZK SNARK

ZK-SNARK stands for "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge."
It refers to a proof construction in which one entity knows a secret and without revealing that secret to other party, it proves that it knows that secret without any interaction between the prover and the verifier.

8 Cryptographic accumulator

A cryptographic accumulator is a one way membership function. A family of one-way accumulators is a family of one-way hash functions each of which is quasi-commutative. It tells whether a potential candidate is a member of a set without revealing the individual members of the set.

9 LocalCoin

- An Ad-hoc Payment Scheme for Areas with High Connectivity
- **Written by**: Dimitris Chatzopoulos, Sujit Gujar, Boi Faltings, and Pan Hu
- **Motivation**: Bitcoin and other cryptocurrencies demand high computational powered devices from their miners and also it's required that they must be interconnected via the internet.
- **Contribution**: LocalCoin has helped overcome the above mentioned difficulties as it doesn't require an Internet connection nor devices with high computational capabilities. However, since it is a location based, ad-hoc and peer-peer cryptocurrency, it is required that the there is high connectivity between users that opportunistically exchange messages.
- **Main Challanges**: The main challenges faced by Decentralised Cryptocurrencies are:
    1. **Proof of ownership-** Users have to prove their ownership,i.e. they have to prove that the amount of money they are claiming belongs to them.
    2. **Double spending avoidance -**Users should not be able to spend the same money more than once and fool others. This has been done to protect users and act as a defense mechanism to prevent double spending.

3. **Incentives -** Determining the appropriate incentives for the stakeholders.

- **Important Terms**:

    1. ***BS-*** *The size of each block is denoted by BS.*
    2. ***mVu* -** *A minimum number of users to verify each transaction.*
    3. ***mTr* -** *A minimum number of trusted users of the user's trusted network.*
    4. ***aVd* -** *The average distance between the users that will verify the creation of a new block should be more than aVd.*
    5. ***U* -** *A set of mobile users who are registered to the LocalCoin service.*

- **Double Spending Avoidance**: Bitcoin overcomes double spending in the following manner:

    - by using a proof-of-work mechanism that is based on the fact that cheating is improbable because verification of the transaction takes time and the malicious user has to compute faster than the other users.
    - In order to overcome this mechanism, the malicious user has to solve a hard problem fastly that takes much time for a brute force algorithm to solve.
    - Cheating in LocalCoin is very difficult because:
        - ∗ Every user in the LocalCoin protocol has its own set of trusted users by selected by him/ her.
        - ∗ Majority of a set of trusted users has to be misinformed by the malicious user.
    - Local Coin avoids double spending in the following manner:
        - ∗ The transaction will be accepted by the receiver if and only if the transaction received by the user is signed by at least some minimum number of trusted users of the user's trusted network, denoted by mTr. This creates a delay that spreads the transaction message to the more number of users . Thus the probability of one trusted user to detect the same input to another transaction increases.
        - ∗ Every participant keeps track of double spending attempts during the block creation process. Fake block creation attempts by a set of collaborative malicious users are avoided using LocalCoin. The average distance between users that will verify the creation of a new block should be more than aVd, as enforced by LocalCoin. This ensures that the block creation messages are scattered to as many users as possible.

- **Incentives**: Incentives are provided in the form of Block fees and Transaction. The users are motivated to store the maximum possible blocks from the distributed block chain by the Block fees, and, to forward messages by the transaction fees.

- **Settings**:

    - Let U be a set of mobile users who are registered to the LocalCoin service.
    - Each user $i \in U$ can utilise the service if she is inside the geographical area, $d_i \in D$, and can change d_i only by moving to another location and not by manipulating it.
    - Any user $i \in U$ is able to exchange LocalCoins with another user $j \in U$ by creating one transaction $t_{i \to j}$. User i needs to broadcast the transaction message that determines its characteristics.

Transaction Template		
Input	Output	Output Description
TNi	Oj	Oj is the amount that user j will receive
h(t→i(1))	Oi	Oi is the remaining amount goes to User i
h(t→i(2))	trfij	trfij is the transaction fee
h(t→i(3))	bfij	bfij is the balance fee
	bi	bi is the balance of user i

  - Any user j has a set of trusted users TN_j and this selection is based on social interaction between users as well as on other device to device interactions.
  - j decides TN_j, who are responsible for guaranteeing that any received transaction with j as a destination should be examined before being broadcasted.

- **Transacting Messages**:
  1. send(i, j, $t_{i\to j}$): Broadcasts $t_{i\to j}$ to all the nearby users (neighbors).
  2. receive($t_{i\to j}$):
     - If she is not familiar with either the sender or the receiver, she forwards the message hoping to collect the transaction fees.
     - If she is one of the trusted users of the receiver of the transaction, she signs the message if she is able to validate all of the input transactions.
     - If the message is received from a trusted user, she updates her transaction database according to the signed message.
  3. process($t_{i\to j}$, k).
     - If the same transaction is received again, she ignores the message unless it is now signed by another trusted user of j.
     - Once a transaction is received, j has to wait for at least mTr of her TN_j trusted users to sign and forward the transaction to her.
     - The amount of trf_{ij} will be received by the first user who forwards this message to j, regardless of being in j's trusted users, if the transaction is going to be accepted by j and verified by the network.
  4. ack(i, j, $t_{i\to j}$): On receving the message from mTr users of her trusted network TN_j, j broadcasts an acknowledgement message.

- **Block Creation**:
  1. build($\mathbf{BLK}(t_{i\to j}, t_{i'\to j'}, \ldots)$):
     - On collecting BS transactions (both send and ack), that are not yet verified, a user l tries to build a new block.
     - For that she needs to agree with $mVu - 1$ other users about the validity of the BS transactions in order to reach to a consensus.
     - Her signed message also contains her location, d_l and a current value of average distance vector d. The distance vector has BS entries and each entry has the average distance between the users who verified the transaction.

2. verify($\mathbf{BLK}^{'}(t_{i \to j}, t_{i' \to j'}, \ldots)$):
    - The block fees is shared by the first mVu users who verify all the transactions in the create message and have average distance between each other bigger that aVd.
    - Every user k who receives a verify message checks her database for unverified transactions and if she has any of the included transactions in the message she signs them and forwards the message.
    - User k updates the distance entries, which she has signed, before forwarding the message.
    - If a double spending attempt is detected by user k, she deletes her entry if it has a later time-stamp or she signs her entry and adds it into the message if it has an earlier time-stamp.
    - In case of double spending detection, user k sets the entry for the corresponding transaction to 0 and attaches and signs her detected pair with a newer time-stamp.
    - Whenever a user receives a verify message with the location of the user not being in her coverage radius.
        (a) she verifies any transaction she can verify,
        (b) she notes that the location of the receiver is not in her coverage radius and she marks the location entry as false, and, then
        (c) she broadcasts the message.

3. create($\mathbf{BLK}^{''}(t_{i \to j}, t_{i'' \to j''}, \ldots)$):
    - Users who receive a message with transactions that are verified mVu times and have average distance bigger than aVd, they also broadcast a create message that defines the users who will share the block fees.
    - Before broadcasting the create message, they examine if there is any entry of the mVu that has been marked by another user as false and in such case, these entries are not considered in the block creation.

- **Block Management**:

    1. delete(i, $t_{i* \to j}$):
        - A garbage collection functionality is proposed that deletes every transaction that is not useful.
        - The delete command is triggered after the create command in order to delete all the input transactions to the freshly verified ones since they can not be used any more.
        - The whole block is deleted after deleting all the transactions of one block.
        - This process is followed in order to keep the size of the distributed block chain as storage efficient as possible, because the mobile devices are not able to dedicate significant amount of storage for that.

    2. sync(t):
        - Sync function can be called by any user by giving only the time-stamp of her last update.
        - By doing so, any nearby trusted user will send the newly verified transactions as well as the hash of the ones that have been deleted.

10 References

- Bitcoin and Cryptocurrency Technologies, Arvind Narayanan, Joseph Bonneau, Edward Felten,Andrew Miller, Steven Goldfeder
- https://en.wikipedia.org/wiki/Zero-knowledge_proof
- http://cryptowiki.net/index.php?title=The_simplest_example_is_the_cave_of_Ali_Baba_(Ali_Baba)
- LocalCoin: An Ad-hoc Payment Scheme for Areas with High Connectivity- Dimitris Chatzopoulos, Sujit Gujar, Boi Faltings, and Pan Hui