Beaver and crowd sensing

NJIT CS SCI
Content

• Beaver system
  ➢ What is beaver system
  ➢ How does it work

• Crowd sensing
  ➢ Our goal in crowd sensing
  ➢ How do we borrow idea from beaver
  ➢ Some other possible solutions
Beaver

A decentralized anonymous marketplace with secure reputation
The Problem

• Centralized Marketplaces
  - Third party needs to be trusted for Privacy, Correctness, and Availability
  - Very weak privacy guarantee

• Decentralized Marketplaces
  - The marketplace system is not entrusted to a third party, but stored with each user (in a Blockchain)
    - See: Bitcoin
  - Open to Sybil attacks
    - Users spamming false information or reviews to damage others’ reputation
  - Presents inconsistent views of the network
  - Can leak critical information about users
The Problem

• Anonymous Marketplaces
  ➢ Centralized, must be trusted
    ▪ Especially for correctness
  ➢ Can fail to provide adequate level of trust
    ▪ See: Silk Road takedowns
  ➢ Vulnerable to exit scams

• Reputation Systems
  ➢ How do we know the user providing the review is a real consumer?
    ▪ Verify their identity with the vendor
  ➢ If the user is to be kept anonymous, how do we verify their identity?
    ▪ How can we protect their identity and validate their review at the same time?
Beaver’s Solution

- Decentralized Anonymous Marketplace (DAM)
  - Decentralized: transaction ledger is kept within a blockchain
    - Can be trusted for availability
  - Anonymous: buyer information is private
    - Since it is decentralized, can be trusted for security
- Beaver aims to provide a DAM with a secure Reputation system
  - Buyers can give feedback to vendors, Amazon or eBay
    - Establishes trust in the marketplace community
  - Provides means of verifying feedback while maintaining privacy for the users
    - Trustworthy, anonymous reviews
Blockchain

- A decentralized, cryptographically validated ledger of transactions
  - Used by popular cryptocurrencies, such as Bitcoin
  - Maintained by every member of the network; no centralized authority
- Transactions are grouped into “blocks” and then cryptographically verified
  - Ensures each transaction is valid and that the blockchain is unaltered
- Those who verify transactions are called “miners”
  - Often incentivised by providing cryptocurrency in exchange for their work
- Beaver utilizes this technology to maintain the ledger of transactions in the online marketplace
  - Collects taxes and fees to pay miners
Beaver’s Structure

• Beaver consists of multiple vendors, who each list their items by registering their public key to the ledger
  ➢ Fees associated with listing and updating items disincentivizes flooding the market with fraudulent listings, as well as relisting items with bad reviews

• The user can then view the items, along with any reviews associated with those items

• If the user wishes to purchase an item, they make a payment transaction for the item and the seller transfers the item to them
  ➢ Transaction tax disincentivizes vendors from purchasing large numbers of their own items to leave fraudulent reviews, while simultaneously collecting money to pay miners

• Afterwards, the user may optionally leave a review for the item
  ➢ Users can optionally link their reviews to each other
(a) Vendor registers the public key of item to the ledger.

(b) Customer retrieves item listings and their reviews, and makes a payment transaction for an item.

(c) Customer leaves a review for the item purchased (optional).
Managing Reputation in Beaver

• Because products are linked to a seller’s unique identity, and reviews are included in the blockchain, users can easily see how reputable a seller is
  ➢ Features of the Beaver marketplace, such as taxes and fees, disincentivize illicit reviews and keep feedback useful

• Conversely, user reviews themselves are anonymous and use a unique identity for each review
  ➢ Protects the anonymity of the reviewers
  ➢ Reviewers can optionally link their reviews to form a reputation as a buyer, while compromising anonymity
Concerns

• Less privacy for vendors than sellers
  • Number of transactions is made public - vendors may want to conceal their transaction volume

• Sybil resistant - but not Sybil-proof
  • Registration fees and other fees encourage proper behavior and maintenance of the marketplace
  • Does not protect against economically irrational adversaries
Crowd Sensing

Adapting the Beaver model to the collection of crowd sourced data
Our goal in crowd sensing

• Protect the providers’ privacy.
• The accuracy of the providers’ data.

⇒ let’s firstly make the problem easier

• Keep the providers’ privacy.
• the providers provide data to the client when the client pay money to the providers.
• The review that the client gave later help us know the accuracy of the data.
Three types of participants

• Client (school/company who wants data)
  ➢ Get data from the providers
  ➢ Pay money to providers
  ➢ Give a review to the provider which help us to build reputation for the providers (data’s quality)

• Provider(users who provide sensed data)
  ➢ Collect data and give data to the client without sacrificing privacy
  ➢ Receive payment from the client
  ➢ Maybe give a review to the client about task’s quality and if the client pay

• Miner(compete with miners and submit transactions to the public ledger)
  ➢ Mainly verify different transactions and submit them to the public ledger
High level idea

- The client first register themselves to the network by publishing their pseudonyms.
- The providers are then able to enumerate the list of client, and finish a task by making an anonymous transaction to the client.
- We can regard the process which the providers finish the task and get money from the client as the process which the provider pay data to the client and the client pay money to the providers.
- To leave a review, the client privately ties the review to the transaction she made earlier and submits the review to the network.
- The provider can give a review to the client too.
Work flow

- Make a review
- Make payment $t_{pk}$
- Get data from providers
- Receive task $t_{pk}$
- Provide data for $t_{pk}$
- Get money for $t_{pk}$

<table>
<thead>
<tr>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>prWCD9</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>$t_{pk}$</td>
</tr>
</tbody>
</table>
Registration transaction

• Client

1. Register the task

For each task, the client will generate a public-private key pair \((t_{pk}, t_{sk})\) and forms a registration transaction as follows.

\[ rt = (\text{REGISTRATION}, TXID, \text{TASKINFO}, t_{pk}) \]

After the client register the task, they will publish a list of public keys of different tasks. The provider who try to work with some tasks can search them.
Data Payment transaction

• Provider

2. Choose a task

When the providers want to finish a task, he will generate a public-private key pair \((p_{pk}, p_{sk})\) for the task. And the transaction about giving data is as follows.

\[ rt = (DATAPAY, TXID, p_{pk}, t_{pk}, PROVIDERINFO) \]

Here, the public key \(p_{pk}\) must hold enough data to send.
Payment transaction

• Client

3. Pay the provider for the task

In fact, this payment transaction is like beaver’s payment transaction.

It also looks similar to that of Bitcoin. The transaction is as follows.

\[ rt = (PAYMENT, TXID, c_{pk}, p_{pk}) \]
Review transaction

4. Give a review to the provider
   - The client has the option to give the review or not
   - Generate the review transaction: key pairs of task \((t_{pk}, t_{sk})\), public key for the data provider \(p_{pk}\), rating for the data \(\alpha_i\), short message for the review \(M\), set of reviews to link to \(r_i\)
   - After the reviews are generated, the miners will verify the reviews before adding them to the ledger
Review transaction

- Client

4. Give a review to the provider

A review transaction will be as follows.

\[ r = (\text{REVIEW}, \text{TXID}, a, M, t_{pk}, p_{pk}, r_i) \]
Problems and other possible solutions

1. The provider give data back, will these data still let the provider lose their privacy?
2. The reputation is weak which depend on the provider privately link all reviews he got. Is it possible to improve it?
3. Is privacy for the client important? They are like the vendor in the beaver system and lose some privacy.
Other papers

• Mayank Raikwar, *An efficient anonymous reputation system*, 2016
• Cristian Tanas etc, *An Integrated Reward and Reputation Mechanism for MCS Preserving Users’ Privacy*, 2016
• Johannes Blomer etc, *Anonymous and Publicly Linkable Reputation Systems*, 2015
• Xinlei Wang etc, *ARTSense: Anonymous Reputation and Trust in Participatory Sensing*, 2013