Decentralisation and Privacy: An Analysis of the Bisq Decentralised Exchange

Liam Hickey Martin Harrigan

June 19 2022

South East Technological University, Carlow, Rep. of Ireland

Outline

Introduction

Decentralisation in Bitcoin

Decentralisation is one of the primary driving forces behind the rapid growth of cryptocurrencies in recent years.

- Remove trusted third parties from financial transactions.
- No central point of failure.

However, to facilitate this decentralisation, transactions are published via a blockchain, allowing for broad-based analysis of blockchain activity.

Centralised Exchanges

Ports of entry can be problematic for decentralisation, this is most evident for centralised exchanges.

Though easy to use, centralised exchanges are flawed from both the perspectives of decentralistion and privacy.

- Identity checkpoints are often enforced in accordance with *Know Your Customer* (KYC) law.
- Centralised exchanges are a trusted third party.

The combination of identity checkpoints with blockchain-based analysis techniques is a well-known privacy risk.

Bisq

Bisq is a decentralised exchnage, or *DEX*, that addresses many of the issues surrouding centralised exchanges:

- Traders using Bisq trade with one another directly, no trusted thrid party.
- Identity checkpoints are not enforced.
- The project is entirely open source.

Decentralised Trading

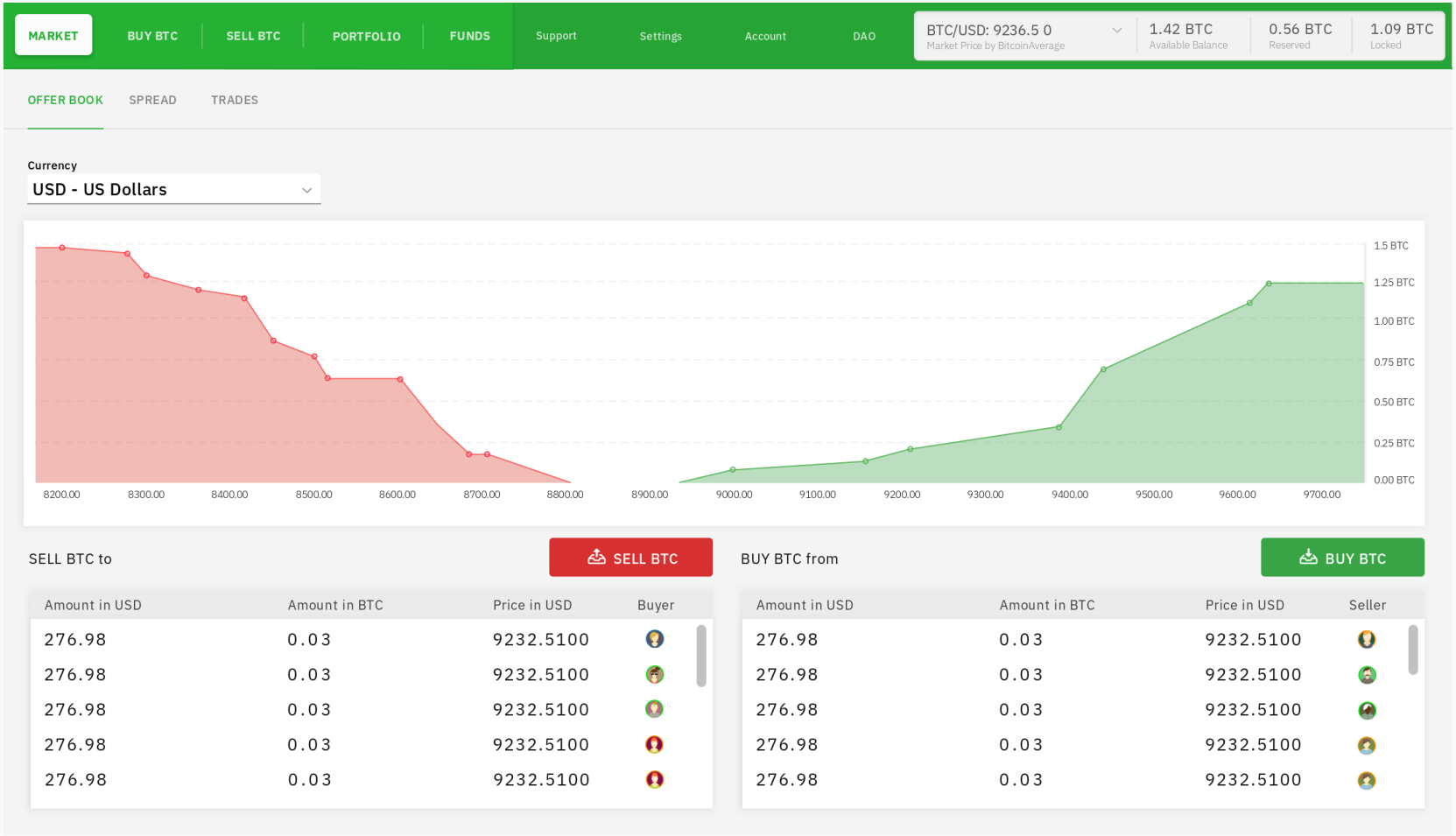
Bisq facilitates the exchange of both cryptocurrencies as well as fiat currencies by relying on the Bisq trade protocol.

Biq trades are:

- carried out without the involvement of a trusted third party.
- secured by relying on the Bitcoin blockchain and Bisq P2P network.
- managed using an distributed orderbook.

As of block height 670 026, over 90 000 trades have been completed using Bisq.

Bisq Software



Screenshot of Bisq software, taken from `https://bisq.network/`

Decentralised Governance

In addition to its trading functions, Bisq decentralises its governance functions through the Bisq DAO, or *Decentralised Autonomous Organisation*.

By participating in the DAO, Bisq users can:

- Make and vote upon proposals relating to Bisq.
- Be compensated for contributions towards the Bisq project.
- Assign Bisq related roles, such as trade mediator.
- List new assets that can be traded on on the exchange.

Our Analysis

- Bisq is effective in carrying out the trading, finance, and governance functions of the exchange.
- However, in doing so, both the Bisq trade protocol and Bisq DAO rely on the Bitcoin blockchain.
- In this presentation, we examine this reliance by applying blockchain analysis techniques to Bisq.
- We aim to highlight areas in which Bisq can be improved from a privacy persepctive.

Decentralised Trading

Trading Using Bisq

To trade, Bisq clients connect to the Bisq P2P network over Tor, traders can either create or accept offers to trade.

- Traders using Bisq can trade using a wide variety of both fiat currencies and altcoins.
- However, every trade must exchange Bitcoin in exchange for some other asset.
- The Bitcoin blockchain is used to provide security for both traders.
- The Bisq P2P network facilitates communication.

While the Bisq P2P network plays a role in the Bisq trade protocol, we focus on blockchain activity.

Trade Protocol

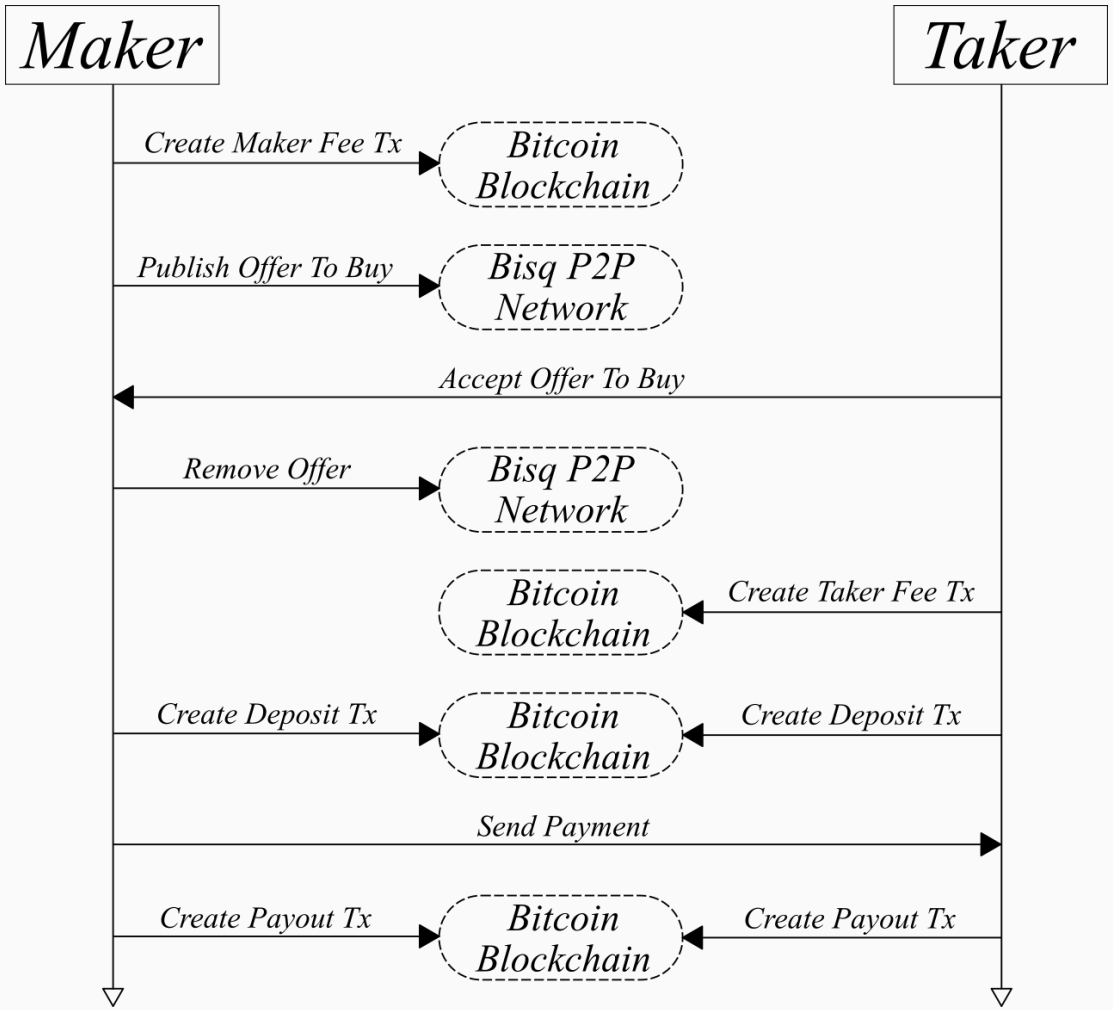
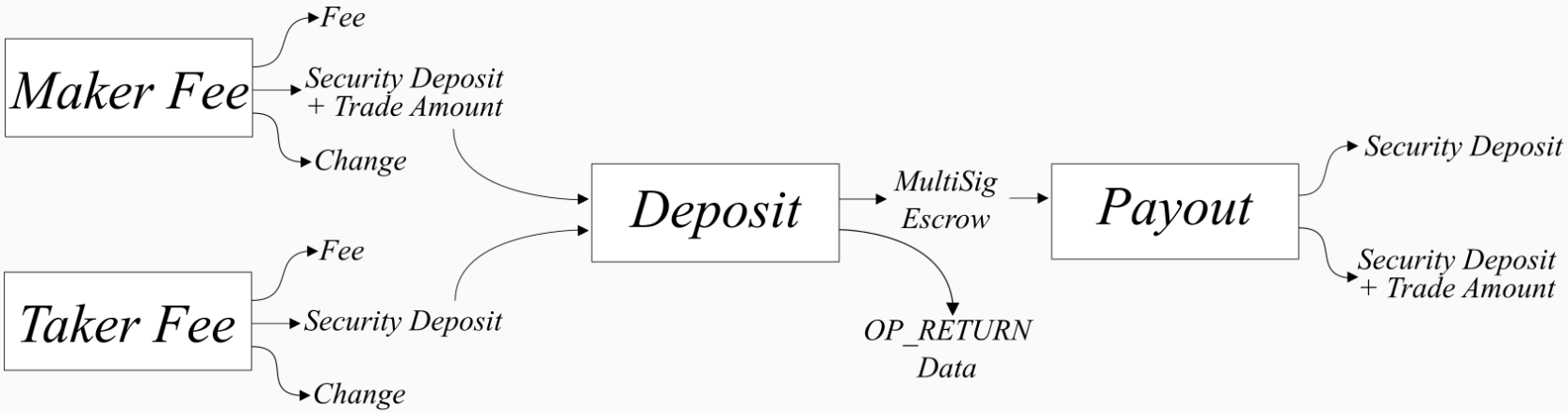


Figure illustrating the flow of a Bisq trade.

Trade Protocol



1. **Maker Fee Tx** - Extracts trade fee, security deposit, and trade amount from maker.
2. **Taker Fee Tx** - Extracts trade fee and security deposit from taker.
3. **Deposit Tx** - Secures deposits and trade amount in multi-signature output escrow until payment completes.
4. **Payout Tx** - Redistributes funds to the maker and taker.

Trade Protocol Analysis

Identifying Bisq Trades

The first step of our analysis is isolating Bisq trades, we identify a deposit transaction using the following criteria:

1. It must have at least two transaction inputs and two transaction outputs.
2. Both inputs must reference the second output of their previous transaction.
3. The first output must be a 2-of-2 or 2-of-3 `P2SH/P2WSH` multi-signature output.
4. The second output must be an `OP_RETURN` containing 32 bytes of data.

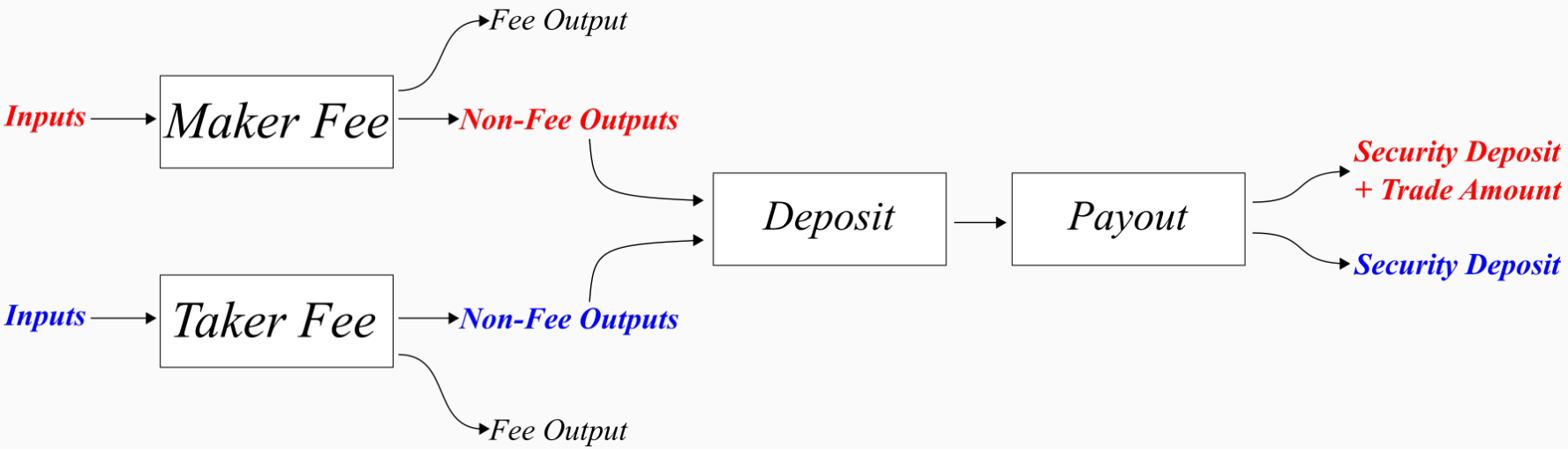
Once we identify the deposit transactions, retrieving the others is trivial. They are interlinked.

Address Clustering Heuristic

Once we have identified Bisq trades on the Bitcoin blockchain, we can perform a more in-depth analysis.

- We noticed that the inputs of the deposit transaction follow the same order as the outputs of the payout transaction, the first ordinal belonging to the buyer, and the second to the seller.
- We can add addresses referenced in fee transactions to clusters corresponding to the buyer and seller as well, the only exception being the fee output.

Address Clustering Heuristic



The Bisq trade protocol-specific address clustering heuristic can best be understand using a diagram. Red indicates addresses belonging to the buyer, while blue indicates addresses belonging to the seller.

Results

- As of block height 670 026, we identified 90 801 Bisq trades on the Bitcoin blockchain.
- After removing arbitrated and irregular trades, we applied the address clustering heuristic to 87 326 trades.
    - The pool of 87 326 trades reference 621 697 distinct addresses.
    - The clustering heuristic paritioned this pool into 40 801 clusters.
    - On average, each cluster contained 15.24 addresses.

Validation

The Bisq P2P network stores trade data in shared files, `TradeStatistics2`, which was deprecated for privacy concerns, and `TradeStatistics3`, which removes sensitive data.

`TradeStatistics2`:

- We failed to identify 18 trades.
- We identified 503 trades not present in `TradeStatistics2`.
- `TradeStatistics2` contained inaccuracies.

`TradeStatistics3`: counts 91 689 trades. Our heuristic falls short by 888 trades, identifying 90 801.

Decentralised Governance

The Bisq DAO

The Bisq DAO (*Decentralised Autonomous Organisation*) is the component of Bisq responsible for decentralising its governance finance functions.

- Bisq DAO participants make and vote upon proposals relating to Bisq.
- Voting takes place in approximately monthly cycles known as DAO cycles.
- Votes are counted using a stake based voting system.

BSQ Colored Coin

The Bisq DAO manages its operation by tracking the issuance and actions of a colored coin on the Bitcoin blockchain called BSQ. Participants must hold some BSQ in order to participate in the functions of the DAO.

BSQ Usage:

- Minted to reward contributors (contribution request transactions and the genesis transaction).
- Used to pay trade fees at a reduced rate (Trade Fee Transaction).
- Used to make and vote upon DAO proposals (All other transaction types).

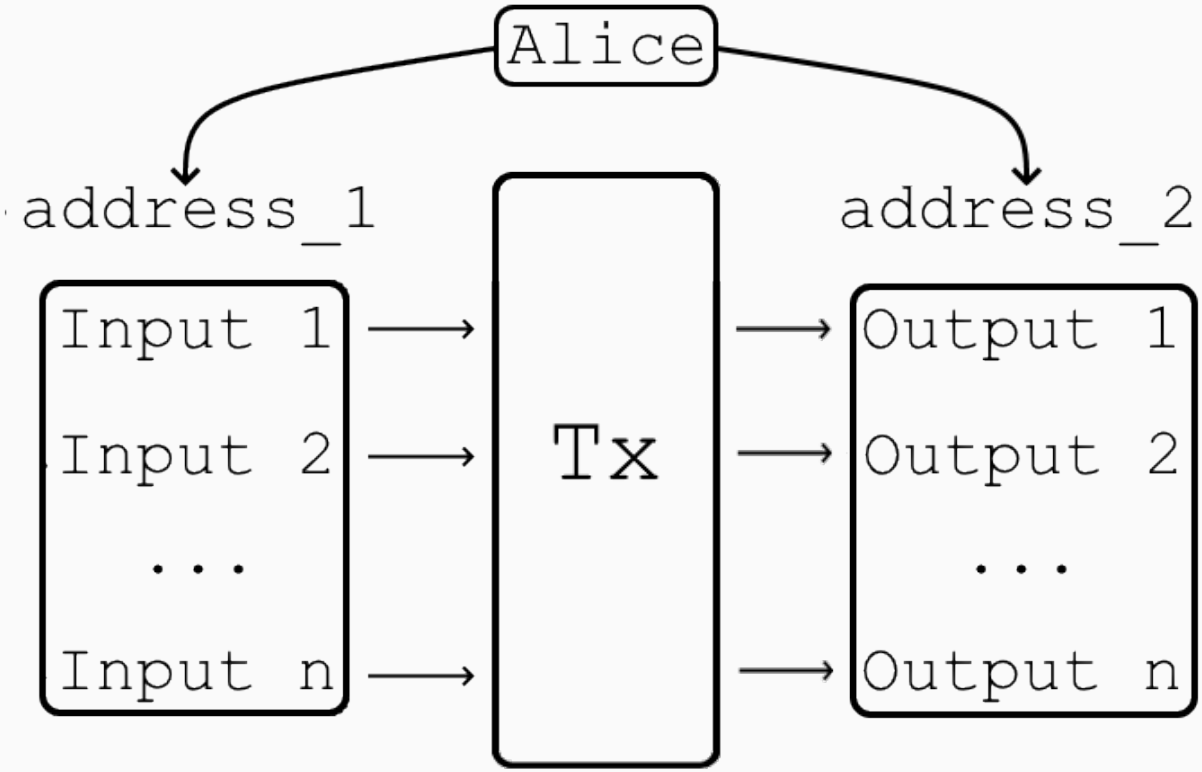
BSQ Transaction Types

BSQ Transaction Types:

- Trade Fee
- Transfer
- Compensation Request
- Reimbursement Request
- Proposal
- Blind Vote
- Vote Reveal
- Lockup
- Unlock
- Asset Listing Fee
- Proof of Burn
- Genesis Transaction

DAO Analysis

Self-Transfer Issue



Self-Transfer: A transaction in which all of the inputs and outputs belong to the same participant.

The majority of BSQ transactions are self-transfers.

Self-Transfer Transactions

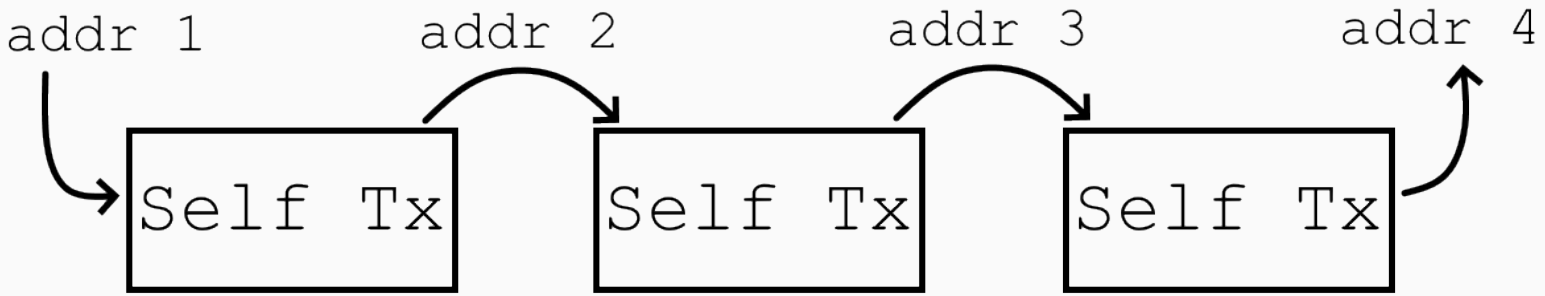
BSQ transaction types and whether or not they are self-transfers; green indicates a self-transfer, red indicates non-self-transfers:

- Trade Fee
- Transfer
- Compensation Request
- Reimbursement Request
- Proposal
- Blind Vote
- Vote Reveal
- Lockup
- Unlock
- Asset Listing Fee
- Proof of Burn
- Genesis Transaction

Clustering Heuristic

This leads us to our Bisq DAO specific clustering heuristic:

- Addresses at either side of a self-transfer transaction can be linked; they are owned by the same participant.
- If two self-transfers occur sequentially, we can assert all addresses belong to the same participant.
- Our clustering heuristic clusters BSQ/Bitcoin addresses based on sequential self-transfer transactions.



Results

The application of our DAO specific heuristic yielded the following results:

- At the time of our analysis, there were 56 775 BSQ transactions referencing 163 430 unique addresses.
- Our heuristic partitioned this set into 1532 address clusters.
- Address tagging further reduced this number to 1504 clusters.

Conclusion

Summary

Our analysis shows that while Bisq is effective in maintaining decentralisation at every level of its operation, its reliance on the Bitcoin blockchain comes at a privacy cost.

- Bisq trades are identifiable on the Bitcoin blockchain.
- Address clustering can be used to aggregate trader activity.
- BSQ self-transfer transactions allow for address clustering to be applied to BSQ transactions as well.

Improving User Privacy

There are various tactics that can be used to improve Bisq user privacy:

- Ambiguity: Each of the heuristics presented relies on the structure of Bisq trade and BSQ transactions; ambiguity in these transactions could lessen their effectiveness.
- Behaviour: Both address clustering heuristics aggregate user activity across multiple transactions/trades. More privacy conscious user behaviour would ameliorate this.
- False Positives: It is possible to create a set of transactions that mimic the structure of Bisq transactions.

Haveno

Haveno is a privacy focused fork of the Bisq project that relies on the Monero blockchain.

- Haveno's usage of Monero, a more privacy focused blockchain, makes the analyses we have described impossible.
- Haveno forgoes a DAO to decentralise governance, solely implementing a decentralised trade protocol.

Conclusion

Bisq is an innovative example of a decentralised exchange that maintains decentralisation at every level of its operation. However, to maintain this level of decentralisation, both the Bisq trade protocol and the Bisq DAO rely on the Bitcoin blockchain, placing both within the scope of blockchain analysis. We applied such analysis to identify the privacy concerns arising from Bisq's reliance on the Bitcoin blockchain and discussed ways in which the privacy of Bisq's users may be improved.