Research Report

A scheme of presumptive identification of sell, buy, swap, and shift transfers of crypto token

Mike Choi fleetpro@gmail.com

Abstract

The requirements of a Dapp project often call for the system to dissuade sell, buy, and pure transfers of token, by imposing them with their respective fees. As the three types of transfer should be able to have their individual fee rates, we need to be able to identify between them when they take place.

- A scheme of transfer categories is suggested: sell, buy, swap, and shift transfers.
- Independent, presumptive definitions of sell, buy, swap, shift are suggested in the middle level terms.
- The definitions are transformed to identification algorithms at the lowest, coding, level.

Throughout this report, we assume a fiction crypto token called the **TOKEN**, of which we discuss the identification of sell, buy, and pure transfers.

1. Challenges

- It is difficult to detect **standalone sell/buy operation**, where the constituent transfers are all included in a single transaction, because all we can detect are TOKEN transfers. *For example, a contract transfers TOKEN tokens from a person to another account, and, before or later in the same transaction, transfers 3rd-party tokens from the account to the parson. We can only detect the TOKEN transfer. Should the TOKEN transfer be a pure gift-sending transfer, or a sell transfer that sends TOKEN tokens in return for the 3rd-party tokens?*
- It is difficult to detect **distributed sell/buy operation**, where the constituent transfers like giving and taking are distributed over different transactions, because the transactions may not take place in serial.
- While we can keep track of our own TOKEN/- Dex pair installed on our own Dex, we can *not* directly detect that a TOKEN/- pair is installed on another Dex. Nor can we restrict other Dexes from being freely created. Challenges are when those external Dexes are used to attack our protocol.

2. Abbreviations, Definitions, and assumptions

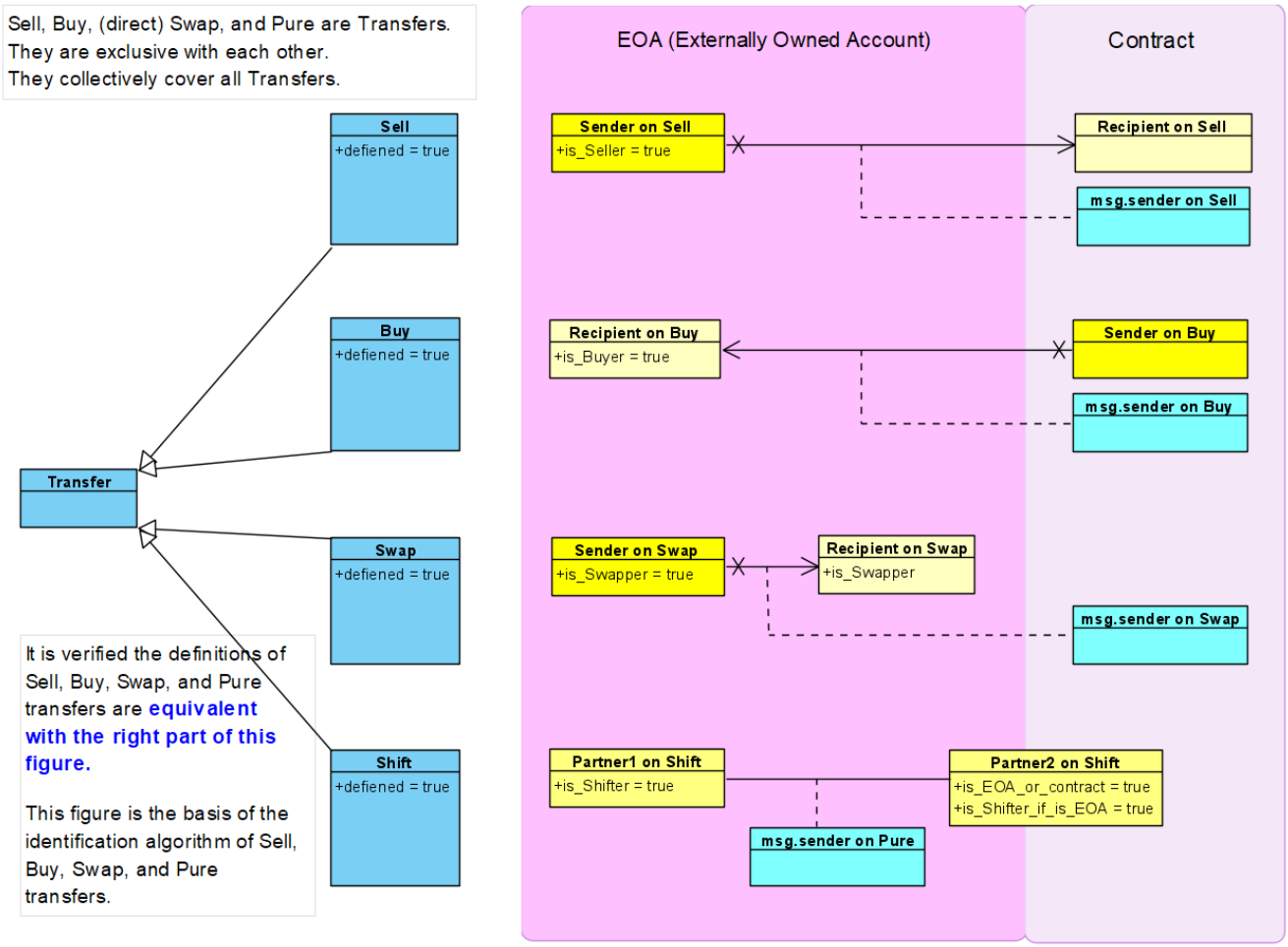
- EOA is the abbreviation of Externally Owned Account.
- A **move/transfer** of token is a call to the 'transfer', 'transferFrom', or other function, which debits the tokens from an account and credits other accounts with them. Move/transfer as a verb are in consistency with their noun meanings.
- A **trade chain** is a chain of one or more transfers taking place in serial to fulfil a trading event, like [transfer asset *from trader* to poolA, transfer assetA from poolA to poolB, transfer assetB from poolB to poolC, ..., transfer assetG from poolG *to trader*].
- A **trade path** is a list of assets that appear in a trade chain, like [asset to give, ..., asset to finally take].
- A **direct trade**, or a swap, has the shortest trade chain [transfer asset *from trader* to poolA, transfer assetA from poolA *to trader*].

- An **indirect trade** has a longer trade chain, with one or more intermediary transfer(s).

3. Suggested definitions of sell/buy/swap/shift transfers

- A **sell transfer** is an on-chain transfer event that moves TOKEN tokens from an EOA to a contract account, where the transfer *can be* integrated with another transfer that moves other assets to an account that the EOA selects, in the same on-chain transaction as the first transfer. The EOA is the Seller.
- A **buy transfer** is an on-chain transfer event that moves TOKEN tokens from a contract account to an EOA, where the transfer *can be* integrated with another transfer that moves other assets from an account that the EOA selects, in the same on-chain transaction. The EOA is called the Buyer.
- A **swap transfer** is an on-chain transfer event that moves TOKEN tokens from an EOA to another EOA, where the transfer *can be* integrated with another transfer that moves other assets in the opposite way. The first EOA is called the Seller, the second the Buyer.
- A **shift transfer** is an on-chain transfer event that moves TOKEN tokens between an EOA and another EOA or contract, where the transfer *can not be* integrated with another transfer that moves other assets in the opposite direction.

The definitions are going to turn out to be explained as shown in the below figure:



4. Discussion

- The definitions are in middle level terms.
- The definitions are independent of each other.
- Pure transfers are named the 'shift' transfer.
- The 'Swap' category is newly introduced for the purpose of the elegancy of classification and flexibility of production use. Sell can buy categories will overlap if we don't introduce a separate category of 'Swap'.
- A sell transfer is effectively a transfer that can **not be proven not to** be a part of an indirect selling transaction.** It is a *presumably* selling transfer. It turns out to be the first transfer of an indirect trade chain.
- A sell transfer is effectively a transfer that can **not be proven not to** be a part of an indirect buying transaction. It is a *presumably* buying transfer. It turns out to be the final transfer of an indirect trade chain.
- A swap transfer is effectively a transfer that can **not be proven not to** be a part of a direct swap (simultaneous selling and buying) transaction. It is a *presumably* swapping transfer. It turns out to be be any of the transfers of a direct trade chain.
- A shift transfer is **truly** a one-way transfer transaction. It is *not* a presumed transfer. It turns out not to appear in a trade chain.
- The above definitions leave open the possibility of users dodging transfer fees by distributing elements of their malicious sell/buy/transfer operation over multiple on-chain transactions.
- This can be justified, as identifying/monitoring multiple scattered transactions cooperating to form a malicious operation, will incur extensive research beyond this project scope.
- This is ALSO justified by the judgement that a distributed operation will need very strong, if not impossible, trust between the transactions over which the operation's element transfers are distributed. Only those accounts belonging to the same interest group can deserve this chain of transactions.

5. Known knowledge

- Lemma 1: For a transaction, which is a series of msg.senders, the 1st msg.sender and only that is an EOA. (Trivial.)

- Lemma 2: Note: Sell, buy, swap, and shift transfers, defined above, are exclusive with each other, and completely cover all TOKEN transfers. (See the above figure.)

6. Patterns of Sell, buy, swap, and shift transfers in general

All we, our code, can detect is a TOKEN transfer call, which may be part of a whole, invisible, transaction, and which has the following form:

transfer(Sender, Recipient, Amount)

The total attributes in terms of which we can think of a transfer call are listed below:

- Sender: the account that is debited.
- Recipient: the account that is expected to be credited. Note fee accounts are also credited.
- Amount: the amount to debit from the Sender, and to credit the Recipient with a portion of.
- msg.sender: the actor who directly called this transfer.

- tx.origin: the externally owned account/actor who initiated the whole transaction of which this transfer is an element action.
- fee accounts: the accounts that will intercept the Amount amount and get debited with a portion of the Amount amount.
- gasLeft can not be used to identify sell/buy/transfer, because it's not robust of the change of ordering.

Every actor, on-chain or off-chain, should, directly or indirectly, call this operation when they need to move TOKEN tokens from one account to another account, for whatever purpose.

We need to investigate transfer categories before we can build a formula identifying between them.

7. Sell transfers

Sells have the following pattern:

- (Sending) TOKEN tokens are moved from Seller EOA to some account (we CAN detect this transfer)
- (Receiving) and 3rd-party tokens are moved from the/another account to Seller EOA (we can NOT detect this transfer).
- all in the same transaction, by definition.

We don't know and care about which takes place first: giving or taking.

Lemma 3. If a transfer is a sell, then there exists a (group of) contract(s) that is not the TOKEN contract and that calls Sending. Proof:

- Assume a sell has no non-TOKEN contract that calls Sending.
- There is an EOA that initiates a transaction. (Lemma 1).
- The EOA only has a single chance of accessing contracts in the transaction. (Lemma 1.)
- The EOA accesses and lets the TOKEN contract call Sending, as its first and only action. (The assumption and above two).
- *The TOKEN contract will be designed to ensure the following:*
    - The EOA has no option but calling either the 'transfer' or 'transferFrom' function, to move TOKEN tokens.
    - The 'transfer' and 'transferFrom' provides a single transfer only, except for fee collection.
- So, there is no way for Receiving taking place.
- So, this is not a sell, negating the assumption.

The following conditions combined by AND, are necessary and sufficient for a sell transfer:

- **Sender == EOA**
- **Recipient == contract**
- **msg.sender == contract**

They are necessary conditions for a sell transfer (Proof skipped)

- key: If there can be another transfer called before or after a transfer, then the msg.sender for the 2nd transfer is not an EOA.

They are sufficient conditions for a sell transfer (Proof skipped)

- key: If msg.sender of a transfer call is a contract, then there can be another transfer called before or after the transfer by, at least, that contract.

Known cases, identified by the above rule

- If Sender is not an EOA, it is not a sell transfer.
- If an EOA transfers its own TOKEN tokens, it is not a sell transfer, because msg.sender == Sender == an EOA != a contract.
- If a contract transfers Sender EOA's TOKEN, it is a sell transfer.
- If an EOA account transfers Sender EOA 's TOKEN, and if the account is an EOA, it is not a sell transfer.
- If TOKEN is the 1st token in a swap path, and, so, a Dex router transfers TOKEN tokens from Sender to a Dex pair, it is a sell transfer.
- If TOKEN is in the middle of a swap path, and, so, a Dex pair transfers its reserve TOKEN tokens from itself to another account, it is not a sell transfer because the Sender pair is not an EOA.
- If TOKEN is the last token in a swap path, and, so, a pair transfers its reserve TOKEN tokens from itself to another account, it is not a sell transfer because the Sender pair is not an EOA.

8. Buy transfers

- (Sending) 3rd-party tokens transferred from Buyer to some actor (we can NOT detect this transfer)
- (Receiving) and TOKEN tokens transferred from the/another actor to Buyer (we CAN detect this transfer).
- all in the same transaction, by definition.

We don't know which takes place first: giving or taking.

For a buy, there exists a Dex or any contract that calls both Sending and Receiving in a single transaction.

(It is proven similarly as in the 'Sell transfers' section.)

The following conditions combined by AND, are necessary and sufficient for a buy transfer:

- **Recipient == EOA**
- **Sender == contract**
- **msg.sender == contract**

9. Swap transfer

- (Sending) TOKEN tokens are moved from Sender EOA to Recipient EOA (we CAN detect this transfer)
- (Receiving) and 3rd-party tokens are moved from Recipient EOA to Sender EOA (we can NOT detect this transfer).
- all in the same transaction, by definition.

Explanation

- While sell and buy transfers are also a swap transfer, we identify 'swap' transfer as a separate category.
- Swap transfer is a part of a *direct trade chain*, while sell and buy transfers are a part of an *indirect trade chain*.
- A swap transfer is both a selling swap transfer and a buying swap transfer, simultaneously.

- You can *not* aggregate swap transfers with sell or buy transfers without destroying the exclusivity between sell and buy transfers.
- That justifies introducing the 'swap' transfers as a separate category.

The following conditions combined by AND, are necessary and sufficient for a swap transfer:

- **Sender == EOA && Recipient == EOA**
- **msg.sender == contract**

10. Shift transfer

- Any of Sender and Recipient is an EOA and transfers to the other.
- The transfer is called by an EOA.

The following conditions combined by AND, are necessary and sufficient for a shift transfer:

- **Sender == EOA || Recipient == EOA**
- **msg.sender == EOA**

A shift transfer is the only transfer that has no more transfers before or after it. It is a single-transfer transaction. (Lemma 1.)

11. Presumptive formulae of transfer identification

So far, we got the following presumptive formulae of transfer identification:

- sell transfer:
  - **Sender == EOA**
  - **Recipient == contract**
  - **msg.sender == contract**
- buy transfer:
  - **Recipient == EOA**
  - **Sender == contract**
  - **msg.sender == contract**
- swap transfer:
  - **Sender == EOA && Recipient == EOA**
  - **msg.sender == contract**
- shift transfer:
  - **Sender == EOA || Recipient == EOA**
  - **msg.sender == EOA**

12 Identification Algorithm

- In practice, major TOKEN/- pairs, routers, and similar contracts on major Dexes are known, allowing us to reduce the rate of presumptive identification. We call them the Dex contracts.
- The list of known Dex contracts should be maintained independently from off-chain.
- If any of the contracts participating in the above presumptive formulae is found in the list of known Dex contracts, then the transfer is a verified sell, buy, or swap transfer.
- If not, then they are a presumptive sell, buy, or swap transfer.

13. Conclusion

- A scheme of transfer categories is suggested: sell, buy, swap, and shift transfers.
- Independent, presumptive definitions of sell, buy, swap, shift are suggested in the middle level terms.
- The definitions are transformed to identification algorithms at the lowest, coding, level.
- Swap transfers can *not* be aggregated with sell/buy transfers.
- There is no assumptions and restrictions imposed on any Dexes for the identification purpose.