A Preliminary Field Guide for Bitcoin Transaction Patterns

Danno Ferrin

Numisight
danno@numisight.com

Abstract—A collection of common transaction patterns found on the bitcoin blockchain is described. Real transactions are given as an example along with generic parameters for these patterns.

I. INTRODUCTION

After over 6 years, 350,000 blocks, and nearly 60 million transactions the bitcoin blockchain has the entire history of every public transaction of bitcoin. From Hal Finney’s first coins, to the first pizza pie purchase, to the Silk Road sales and seizures, and to iPhone micropayments and rewards, the blockchain contains the entire history of all coins spent. In the process many best practices (and worst practices) by the various wallets and services have been developed and from this patterns and signatures that can be identified and enumerated have emerged.

To date, most of the software and research focusing on analysing the information on the bitcoin blockchain have focused either on simply enumerating single transactions (block explorers like blockchain.info and Blocktrail), aggregating the data of the transactions (like Coinalytics or Coinometrics) or attempting to correlate the information to larger off-blockchain signals (such as ZeroBlock or the Winkdex).

In this paper we will take a more middle of the road approach in showing the patterns that can be observed in the blockchain data by examining the transactions recoded in context of each other. Instead of looking at individual breadcrumbs or the economy of the bakeries where the bread is made we will look at a loaf of bread and see where the breadcrumbs made from that loaf lead to and the paths that are exposed.

II. NOTATION GUIDE

The graphs that are presented here represent actual transactions from the bitcoin blockchain. They are represented as acyclic directed graphs with the implicit direction flowing down the page; no arrows will be used on the lines since the direction relative to the page is implicit.

The nodes of the graphs represent bitcoin transactions. These transactions are composed of a number of inputs and outputs that are represented as the lines. These lines represent the “coins” of bitcoin rather than the transactions, so the lines represent the actual value of the bitcoins.

Inside each node are multiple lines of test representing information about each node. In order to aid in the reconstruction of the sample transactions it is important that this information be integral to the graph itself. The first line is an elided form of the transaction id. The second line represents the total output value of the transaction. The third line is the time that the transaction was processed in its containing block on the block chain. The time zone will always be GMT. The fourth line shows the block number it was included in.

The fifth line shows the total number of transaction inputs and outputs for the transaction. This number may be higher than the number of edges entering the top of the node (for inputs) as well as the number of edges exiting the bottom of the node (for outputs). When a node has all input and output lines represented in the graph it is in, the color of the node is changed to yellow (or a lighter grey for grey scale printing). Partially expanded nodes (nodes where all the transaction inputs and outputs are not represented in the graph) are rendered in “bitcoin” orange.

The sixth line represents the fees paid to the block miner for the posted transaction. The sum of the processed output value and the fees matches the values for the inputs to the transaction.

When an unspent transaction output is expressed on the graph, it is represented both by the transaction line and a special green output node with more rounded corners then the transaction nodes, looking like an elongated oval. The first line is the address of the unspent output, or in the case of multi-sig addresses the first several lines represents the addresses and the required signers for the address. The second line shows the value stored in that specific unspent output.

The lines are labelled with the value of bitcoin for those transaction outputs. Occasionally the addresses of the transaction outputs and inputs will be relevant, in those cases the addresses are shown above the bitcoin value.

The horizontal axis of the graphs have no bearing on the meaning in this paper, neither do the ordering of the edges into or out of the nodes. The vertical axis is the relative time order of the transactions represented. The top of the graph represents earlier time and time becomes more current towards the bottom of the graph. Note that the ordering isn’t absolute, but relative to the other transactions. Hence a transaction that shares the same vertical alignment of another transaction may have occurred strictly earlier or later, but the two transactions do not share any coins that would have made one transaction dependant on the other.

The addresses and transaction IDs are elided when presented in the graphs. This is for ease of use and for better
user experience. The first six and last four digits and letters are used to form the elided IDs and addresses. For the shown transactions the root transaction ID can be found in the references section at the end of the paper. The related transactions in the graphs can easily be derived from a transaction whose full ID is listed in the references section.

III. SINGLE TRANSACTION PATTERNS

Some of the transactions observed in the blockchain can exist strictly on a single transaction. However to gain a better understanding of multiple transaction patterns it is first necessary to understand the implications of the patterns in single transactions.

A. Peel Transaction

Name: Peel
Also Known As: Spend and Change, Simple Spend
Number of Inputs: Any
Number of Outputs: 2
Sample Transaction: (See Figure 1)

```
4184fc596403b9d638783cf575c605f635f6bc913385309e9831e9e16
```

Figure 1 – A Simple Spend Transaction [1]

The most common style of transaction is the peel transaction or spending transaction. In this transaction any number of inputs are combined in a transaction and two outputs are created. In the cases where one of the outputs is directed at an outside party then the outside party receives the output designated as the “spend” and the other output is the “change” output of the transaction.

Wallets that generated these transactions will gather up as many unspent transaction outputs as are needed to create the value needed to create the spent part of the transaction. Because of the structure of a bitcoin transaction all of the value of an input must be accounted for. If a transaction is not fully spent then the miner collects the unspent portion as a “fee.” For small amounts this is deliberate, but for larger amounts the controller of the transaction will want to keep the unspent amounts, necessitating an extra output in the transactions.

This transaction pattern is not limited to multi party transactions where control of the bitcoins passes to an outside party. For example if the controller wishes to “peel” off portions of their unspent transactions to place in specific addresses then this is one type of transaction they may use to do that.

Typically when forming a classical spend transaction the wallets will only gather enough unspent transactions to just barely provide enough value for the spend side of the output. In such cases the change amount will be smaller than any of the input transactions, were that not so then the input transaction that was larger than the change output could be removed from the transaction. When attempting to identify change and spend outputs this property can be useful. However care should be taken because this property is not absolute.

The sample transaction show in Figure 1 is the first peel transaction on the bitcoin blockchain [1]. In this transaction Satoshi Nakamoto sent Hal Finney 10 bitcoins as a test of the transaction system.

B. Sweep Transaction

Name: Sweep
Also Known As: Consolidation
Number of Inputs: 2 or more
Number of Outputs: 1
Sample Transaction: (See Figure 2)

```
e9f01302beea8dceed0af450f9185ddf1
```

Figure 2 – A Sweep Transaction [2]

A sweep transaction exists when a transaction controller wants to combine multiple separate unspent transaction outputs into a single transaction output that is easier to process and control.

The motivations for this consolidation can be very wide ranging. The controller may be transferring the entire transaction to another party, so the transaction could be a payment. The controller may also be gathering balances into
a single address to aid public audits or visibility. In the theft of coins this transaction is also used for a speedy exit from the control of the coins from one set of compromised addresses to another address.

In some variants of this transaction there will be two outputs. This is usually because a sweep is attempted and the desired sweep amount was calculated incorrectly. In order to prevent the loss of value wallet software will create a change address and places the remaining amounts in the change address.

The sample transaction in Figure 2 shows a Mt. Gox related transaction that occurred after the exchange declared bankruptcy and went out of business [2]. In the process of winding down operations nearly 200,000 bitcoins were found in unused wallets. This transaction represents one of the early consolidations of these “found” bitcoins into a 180,000 bitcoin transaction output.

C. Distributions Transaction
Name: Distribution
Also Known As: Payout
Number of Inputs: Any
Number of Outputs: 3 or more
Sample Transaction: (See Figure 3)
9c888af52fa003849964227fa898178
a7254631cbf14b2a6f7d276386e3bce6a

A distribution transaction is most commonly associated with the payment of multiple parties from a single organization or entity. Typical examples are paying out mining pools or gambling rewards. It is also used in single party transaction for splitting out a larger transaction into smaller transactions for uses such as cold storage or parallel transaction processing.

Like a peel transaction a distribution transaction can have a change output, although identifying the change can be more difficult since many of the payouts may have less of a value than the smallest input transaction. Some mining pools, such as P2Pool, make it a point to payout the entire coin base of a block reward to its rewarded miners. For example, the coinbase transaction for block 309997 pays out transactions to 83 miners [4] (thus ruining the notion that a coinbase transaction has a single address).

D. Relay
Name: Relay
Also Know As: Pass-Through, Perfect Spend
Number of Inputs: 1
Number of Outputs: 1
Sample Transaction: (See Figure 4)
67ccdb7f19faceb150093286bcee6e4a45
eb9c032cc30af267f9b003ea50e30430

The relay transaction is a surprisingly popular transaction, ranking third in total volume of transactions (behind single input peels and double input peels) as of early 2015. Relay transaction can be used for many reasons. One use is to move bitcoins from one party to another party without leaving any extra information such as change outputs or combining inputs form other transactions. Another motivation may be to move bitcoins from one address to another where the control policies on the keys may differ.

In the sample transaction shown in Figure 4, bitcoins were moved from a simple public key address to a pay to script hash address, presumably a multiple signature address. With this transaction the bitcoins were moved to an address that requires a different redemption process while maintaining the privacy of the bitcoins by not combining them with other bitcoins or creating separate outputs that could later be correlated.

E. Self-Spending Transaction
Name: Self-Spending
Number of Inputs: Any
Number of Outputs: Any
Sample Transaction: 016baf4d70ace9bfa5b20b279b293b3141
c4ee6c371c4cf13dd5ae6ce8f206e130d
Self-spending transactions are not a transaction by itself, but rather a property observed in other transactions. A self-spending transaction has one or more input addresses that also show up in the output addresses of the transaction. There can be one or more self-spending addresses in the transaction.

When combined with a peel a self-spending transaction the self-spending address is most likely the change address. Notable exceptions are where both halves of the peel are represented as addresses in the inputs or when the same address is shared between both of the addresses.

When combined with a distribution a self-spending address would similarly indicate the strong likelihood that the shared address is the “change” address.

Combining a self spend with a relay transaction would serve little purpose on itself, and when examining one or more other factors should be considered such as off-chain meaning (an audit could require a transaction) or other factors such as the lock time field in the transaction.

F. Meta Transaction

Name: Meta Transaction
Also Known As: Proof of publication, meta-coin transaction
Number of Inputs: Any
Number of Outputs: Any

A Meta Transaction is any bitcoin transaction where external data is inserted into the transaction itself. This technique is used to allow other information to piggyback on the bitcoin blockchain’s ubiquity and stability. Typical uses are for placing messages in the blockchain (such as the original Satoshi Whitepaper [7][8]), for providing “proof of publication” by placing hashes of documents as data, and as a layered protocol for conducting transactions for other financial systems such as Counterparty or Mastercoin.

Like the self-spending transaction pattern this pattern can be layered on top of other patterns. The only distinguishing characteristic is that it contains an output that encodes the data. Typically relay or peel transaction are the layered transactions.

When layering the data inside of a bitcoin transaction there are currently two models in common use. The first is naked multi-sig and the second is the use of the OP_RETURN script instruction in the output script.

1) Naked Multi-sig Transactions:

Sample Transaction: (See Figure 6)

<table>
<thead>
<tr>
<th>9bdcee_c71d</th>
<th>B 0.14648396</th>
<th>14-09-11 11:04</th>
<th>Block # 320134</th>
<th>1 in 2 out 0 unspent</th>
<th>Fee: B 0.0001</th>
</tr>
</thead>
<tbody>
<tr>
<td>1PcCGV_WxX6</td>
<td>B 0.12541315</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>016bf...130d</th>
<th>B 0.12531315</th>
<th>14-09-11 11:06</th>
<th>Block # 320136</th>
<th>1 in 2 out 0 unspent</th>
<th>Fee: B 0.0001</th>
</tr>
</thead>
<tbody>
<tr>
<td>1PcCGV_WxX6</td>
<td>B 0.10424234</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>03a965...d716</th>
<th>B 0.0273708</th>
<th>14-09-11 11:20</th>
<th>Block # 320140</th>
<th>2 in 2 out 0 unspent</th>
<th>Fee: B 0.0001</th>
</tr>
</thead>
<tbody>
<tr>
<td>ab80d...dc25</td>
<td>B 0.10414234</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>46534...cede</th>
<th>B 0.0019993</th>
<th>15-02-09 01:44</th>
<th>Block # 342630</th>
<th>1 in 3 out 0 unspent</th>
<th>Fee: B 0.000035</th>
</tr>
</thead>
<tbody>
<tr>
<td>1NDaWk_rec</td>
<td>B 0.0019743</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9c692...b817</th>
<th>B 0.0019333</th>
<th>15-02-09 01:44</th>
<th>Block # 342630</th>
<th>1 in 3 out 0 unspent</th>
<th>Fee: B 0.000035</th>
</tr>
</thead>
<tbody>
<tr>
<td>1NDaWk_rec</td>
<td>B 0.0019143</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9c692...b817</th>
<th>B 0.0019333</th>
<th>15-02-09 01:44</th>
<th>Block # 342630</th>
<th>1 in 3 out 0 unspent</th>
<th>Fee: B 0.000035</th>
</tr>
</thead>
<tbody>
<tr>
<td>1NDaWk_rec</td>
<td>B 0.0019143</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The first method used to encode data into the bitcoin blockchain is to use the addresses in the output script to encode the data. Fake addresses are created to encode the needed for the information. Typically one or more multi-signature transactions are used because of the compactness in the script encoding.

This style is called naked multi-sig because the addresses are encoded directly instead of via the more modern pay-to-script-hash (P2SH) methods. P2SH methods are inappropriate because the addresses that make up the script are not encoded in the output of the script but are instead presented by the redemption script.

Some implementations of naked multi-sig cause the bitcoin used to encode the value to be “burned” because the addresses are essentially gibberish and are not derived from known public/private keys. Other protocols allow for some of the addresses to be known addresses.

In the sample transaction a counterparty token is being sent to the 1BsVGP address, while the 1NDaVK address is engaged in both a self-spend transaction and a meta-
transaction. The last address in the multi-sig address is the same 1NDaVK address used to initiate this transaction.

2) **OP\_RETURN Transactions:**

Sample Transaction: (See Figure 7)

```
1654912d8a11a666718856f39b745f83
 eighth8e...6951
 B 0.0399
 14-11-01 22:49
 Block # 328903
 1 in 203 out 37 unspent
 Fee: B 0.0001
```

```
bbae8e...6951
 B 0.0399
 14-11-01 22:49
 Block # 328903
 1 in 203 out 37 unspent
 Fee: B 0.0001
```

```
bbae8e...6951
 B 0.0399
 14-11-01 22:49
 Block # 328903
 1 in 203 out 37 unspent
 Fee: B 0.0001
```

The second standard method to encode data is via the use of the OP\_RETURN operation in the output script. The core bitcoin clients were changed in mid 2014 to allow for a small amount of data to be added after an OP\_RETURN operation (although the preferred size of the data is the subject of much debate). Using this method data can be directly added clearly as data and not encoded as addresses, which is beneficial to bitcoin nodes that only maintain the currently spendable transaction output because they can ignore the data since it is not spendable.

In the sample show in Figure 7 the entirety of the value of the input transaction is consumed by the transaction fees, leaving no value in the unspent transaction.

**Figure 7 – A Meta Transaction using OP\_RETURN to encode data [10]**

The single biggest implication in a joint transaction is that the presumptions about correlations between the input addresses by virtue of their participation in the transaction are irrelevant when a joint transaction is encountered. In some large joint transactions the number of input and output transactions regularly exceeds 20 or more, which can result in over 51 trillion possible arrangements of transaction parties. And that is on only one side of the transaction. For a large joint transaction the combinatorial explosion makes casual analysis fruitless.

Wise choices for input and output values can also make picking apart the layered transactions more difficult. In the sample transaction shown in Figure 8 all of the input and output values are identical, making the majority of possible arrangements of layered transactions valid.

**Figure 8 – A Joint Transaction [11]**

**IV. MULTIPLE TRANSACTION PATTERNS**

More interesting transactional patterns can be found in the interaction of multiple transactions, not just in the transactions themselves. A few of the more interesting transactions will be listed here.

**A. Peeling Chains**

Name: Peeling Chain

Also Known As: Peel Chain, Long Chain Transactions

Defining Characteristic: Consecutive Peel transactions.

Constituent Transaction Patterns: Peel, and occasionally Sweep and Relay transactions.

Attribution: “A Fistful of Bitcoins: Characterizing Payments Among Men with No Names” by S. Meiklojhn, et al [12].

Sample Transactions: (See Figure 9)

```
012c509a06ca9146e58fE001a4bb1551
 5eae19e9d1fc35275ae40ce5e9c459
```

Joint transactions are the result of layering multiple transactions into a single, larger transaction. There are multiple methods, both trusted and trustless, to generate a joint transaction. The participants in these transactions do not need to be known to each other, and it is most common that they are not. Also, no single entity needs to control the transaction because some of the protocols allow for a group consensus to form.
A peeling transaction consists mostly of peel transactions where the change transaction is used as the input to a subsequent peel transaction. The most typical configuration is a chain of single input peeling transactions, but as the change amounts approach zero the remaining change amount can be combined with other small change amounts in another peel transaction to continue the chain. In some circumstances several peeling chains can be combined into a single surviving peel chain.

When reconstructing a peeling chain the identification of the change address is a critical task. Sometimes the spend side of a peel transaction will wind up as input to another sequence of peeling transactions from another party or entity who is not responsible for the peeling of the transactions. Identification of the change transactions is trivial if the “ground truth” of the actual addresses controlled by the entity are available. However other transactional cues can be used to tease out the likely change addresses. Repeated patterns such as the same fee payment strategy, “round numbers” for spent amounts, occasionally the ordering of the transaction outputs (although this alone is not a good indication), and later combining of the spend side of the transaction provide evidence as to what sides of the transaction belong to the spend and the change amounts.

One of the advantages that the controller of the peeling chain has is they do not need to worry about double spends of the change address from a peel transaction. So occasionally long peeling chains can be seen within the same block.

In the sample peeling transaction shown in Figure 9 the peel chain exists entirely within the same block, and the peeling transactions all paid the same fee, as well as peeling off the same round sum of bitcoins. It is presumed that this is a Mt. Gox controlled peel chain because two transactions below the 29a3ef transaction is the famous 180,000 “pyramid” transaction [2].

B. Green Address

Name: Green Address

Defining Characteristic: All bitcoin value passing through a single, publicly known address.

Constituent Transaction Patterns: Sweep, Relay, Peel, and Distribution Transactions.

Sample Transaction: (See Figure 10)  
11f1f528327c0da401dgdce7f7baa2c6 
c15f17cd397b328e2190e1300a1bedd2 
and  
d3bdc1164f5b2a6ved00bd1d7029022331 
89eala061c3593c575def77780d05cd34
A Green Address is an older exchange pattern [17] that is still used by some exchange despite its deprecated status. Originally intended as a means to reduce the double spend risk of a transaction by having the well-known output addresses of exchanges and other Bitcoin service providers known to the miners. However because of the structure the green address was at least one transaction removed from the unspent transaction output. This imposed an extra logic and memory requirement that made it less palatable for fast and lean block assembly code.

The green address pattern typically involved two transactions. The first transaction usually consisted of a consolidation or a relay transaction, with the output address of the first transaction is the ‘green address’ desired. The second transaction uses a relay, peel, or distribution transaction to pay the bitcoins out to the customers involved. In the sample transaction shown in Figure 10 the green address is 1LNWw6...WG7q [17] which was the Mt. Gox Green address [18]. The customer account for this transaction was not publicly known when this paper was written.

Despite the problems associated with double spend protections, green addresses are still useful for exchanges and customers as a clear maker address that the bitcoins involved in a transaction were processed at one point by the Bitcoin service provider. That would provide a clear and public line of transfer of ownership in subsequent audits, at the expense of some level of anonymity for both the service provider and the customer.

C. Mixing Clouds

Name: Mixing Cloud
Also Known As: Tumblers, Mixing Pools, Washers
Defining Characteristic: Multiple interconnected joint transactions.

Constituent Transactions: Any at the edges of the cloud, but primarily joint transactions that form large sweeps and distributions in the core of the mixing cloud.

Sample Transaction: (See Figure 11)

C. Mixing Clouds

Name: Mixing Cloud
Also Known As: Tumblers, Mixing Pools, Washers
Defining Characteristic: Multiple interconnected joint transactions.

Constituent Transactions: Any at the edges of the cloud, but primarily joint transactions that form large sweeps and distributions in the core of the mixing cloud.

Sample Transaction: (See Figure 11)
A Mixing cloud is the typical configuration of the holy grail of bitcoin privacy advocates: a series of transactions where it is difficult if not impossible for the casual or trained observer to determine where the controller of the transaction inputs intended for the outputs to be sent. Users of these services typically include multiple transactions before arriving at their intended destination. Some users will split the inputs and the outputs into multiple transactions and even add them and remove them from the cloud at different times.

The core enabling transaction for a mixing cloud is the joint transaction, often through the coinjoin protocol. Chaining and meshing the transactions created by a coinjoin transaction creates a very complicated graph of transaction outputs and transactions. Some of these transactions serve as inputs and outputs to the cloud and are where the real transactions of value take place, the rest of the transactions serve as obfuscation for the connection between the transactions.

In the sample transaction shown in Figure 11 only one of the joint transactions is shown, but the interconnected nature of the cloud can be seen in the output transactions and their connection with each other and (in one case) in a transaction that provided an input to the sample transaction. A few candidate input and output transactions can also be identified by the number of inputs and outputs from those connected transactions.

D. Tunnelling

Name: Tunnelling
Also Known As: Hawala, Induced Transaction
Defining Characteristic: Connections and influence outside of the analysed blockchains. At least two related transactions have no immediate or close relationship.

Constituent Transactions: Any transactions Sample Transactions: (See Figure 12)
\[ \text{dc3169e180261d89d895c437a48f2c19} \]
\[ \text{c18df7aadd6fa44e35f5910fa56300} \]
\[ \text{8cbb2da0df87a09330532089de74ebca} \]
\[ \text{296c221954566d8f8ea41379096f74ea} \]

In enumerating some of the transaction patterns both individually and as groups the emergent phenomena of a transaction network was observed. All of the patterns described in multi-transaction patterns section are a transaction network of some size.

A. Definition

A transaction network is a collection of two or more transactions that share a similar theme or aspect that influences the shape and structure of the transaction network.

The connected transactions do not need to be directly connected on the blockchain ledger although they usually are. The theme or aspect may be something concrete like an individual or a corporation, or it may be more abstract such as an emergent coinjoin network or a social construct such as tipping.

A transaction and the associated transaction outputs and inputs may belong to multiple transaction networks, such as green address and a peeling chain. Some transaction networks may also contain other transaction networks within itself, such as a peeling chain inside of a personal wallet.

B. Anatomy

To describe the parts of a transaction network, we will look at a partial and expanded version of the sample shown in the mixing cloud [20] with an additional transaction shown on the output [24]. The sample transaction is show in Figure 13.

A tunnelling transaction is one or more transactions that are not immediately connected to each other by transaction history but are still related in some fashion. Typically the value transmitted in the transaction is the same; when they differ the differences usually represent a transaction fee from the service provider or a reward, finders fee, or gambling payment to the receiver.

In the sample transaction shown in Figure 12 one tenth of a bitcoin was sent to a well known bitcoin service provider, and then over four months later the same amount of bitcoins were removed from the service. Because of the particulars of the operation of the service provider (they maintain an operational “hot” wallets and “cold” storage wallets) the output of the transaction that was used to deposit the bitcoin was not available at the time the withdrawal was requested.

This is also a technique advertised in some bitcoin services providers that are providing transaction-obscuring facilities. The claim is that they maintain multiple wallets and will immediately pay you out of a different wallet than you deposited into. However, some services advertising this claim have failed to fulfill the promised tunnelling transaction [23].

This is also an emergent phenomenon from personal use wallet software, so observance this pattern is not in and of itself evidence of intent. Some wallets prioritize the use of older unspent transaction outputs in an effort to maximize their likelihood that the transaction will get a higher priority for inclusion into a bitcoin block. Possibly an individual who serves as a short-term holder of bitcoin value for something like an escrow functionary or as a bond holder, the transaction output being returned may not be connected to the transaction outputs that were initially provided.

V. TRANSACTION NETWORKS

A Mixing cloud is the typical configuration of the holy grail of bitcoin privacy advocates: a series of transactions where it is difficult if not impossible for the casual or trained observer to determine where the controller of the transaction inputs intended for the outputs to be sent. Users of these services typically include multiple transactions before arriving at their intended destination. Some users will split the inputs and the outputs into multiple transactions and even add them and remove them from the cloud at different times.

The core enabling transaction for a mixing cloud is the joint transaction, often through the coinjoin protocol. Chaining and meshing the transactions created by a coinjoin transaction creates a very complicated graph of transaction outputs and transactions. Some of these transactions serve as inputs and outputs to the cloud and are where the real transactions of value take place, the rest of the transactions serve as obfuscation for the connection between the transactions.

In the sample transaction shown in Figure 11 only one of the joint transactions is shown, but the interconnected nature of the cloud can be seen in the output transactions and their connection with each other and (in one case) in a transaction that provided an input to the sample transaction. A few candidate input and output transactions can also be identified by the number of inputs and outputs from those connected transactions.

D. Tunnelling

Name: Tunnelling
Also Know As: Hawala, Induced Transaction
Defining Characteristic: Connections and influence outside of the analysed blockchains. At least two related transactions have no immediate or close relationship.

Constituent Transactions: Any transactions Sample Transactions: (See Figure 12)
\[ \text{dc3169e180261d89d895c437a48f2c19} \]
\[ \text{c18df7aadd6fa44e35f5910fa56300} \]
\[ \text{8cbb2da0df87a09330532089de74ebca} \]
\[ \text{296c221954566d8f8ea41379096f74ea} \]

In enumerating some of the transaction patterns both individually and as groups the emergent phenomena of a transaction network was observed. All of the patterns described in multi-transaction patterns section are a transaction network of some size.

A. Definition

A transaction network is a collection of two or more transactions that share a similar theme or aspect that influences the shape and structure of the transaction network.

The connected transactions do not need to be directly connected on the blockchain ledger although they usually are. The theme or aspect may be something concrete like an individual or a corporation, or it may be more abstract such as an emergent coinjoin network or a social construct such as tipping.

A transaction and the associated transaction outputs and inputs may belong to multiple transaction networks, such as green address and a peeling chain. Some transaction networks may also contain other transaction networks within itself, such as a peeling chain inside of a personal wallet.

B. Anatomy

To describe the parts of a transaction network, we will look at a partial and expanded version of the sample shown in the mixing cloud [20] with an additional transaction shown on the output [24]. The sample transaction is show in Figure 13.

A tunnelling transaction is one or more transactions that are not immediately connected to each other by transaction history but are still related in some fashion. Typically the value transmitted in the transaction is the same; when they differ the differences usually represent a transaction fee from the service provider or a reward, finders fee, or gambling payment to the receiver.

In the sample transaction shown in Figure 12 one tenth of a bitcoin was sent to a well known bitcoin service provider, and then over four months later the same amount of bitcoins were removed from the service. Because of the particulars of the operation of the service provider (they maintain an operational “hot” wallets and “cold” storage wallets) the output of the transaction that was used to deposit the bitcoin was not available at the time the withdrawal was requested.

This is also a technique advertised in some bitcoin services providers that are providing transaction-obscuring facilities. The claim is that they maintain multiple wallets and will immediately pay you out of a different wallet than you deposited into. However, some services advertising this claim have failed to fulfill the promised tunnelling transaction [23].

This is also an emergent phenomenon from personal use wallet software, so observance this pattern is not in and of itself evidence of intent. Some wallets prioritize the use of older unspent transaction outputs in an effort to maximize their likelihood that the transaction will get a higher priority for inclusion into a bitcoin block. Possibly an individual who serves as a short-term holder of bitcoin value for something like an escrow functionary or as a bond holder, the transaction output being returned may not be connected to the transaction outputs that were initially provided.

V. TRANSACTION NETWORKS

A Mixing cloud is the typical configuration of the holy grail of bitcoin privacy advocates: a series of transactions where it is difficult if not impossible for the casual or trained observer to determine where the controller of the transaction inputs intended for the outputs to be sent. Users of these services typically include multiple transactions before arriving at their intended destination. Some users will split the inputs and the outputs into multiple transactions and even add them and remove them from the cloud at different times.

The core enabling transaction for a mixing cloud is the joint transaction, often through the coinjoin protocol. Chaining and meshing the transactions created by a coinjoin transaction creates a very complicated graph of transaction outputs and transactions. Some of these transactions serve as inputs and outputs to the cloud and are where the real transactions of value take place, the rest of the transactions serve as obfuscation for the connection between the transactions.

In the sample transaction shown in Figure 11 only one of the joint transactions is shown, but the interconnected nature of the cloud can be seen in the output transactions and their connection with each other and (in one case) in a transaction that provided an input to the sample transaction. A few candidate input and output transactions can also be identified by the number of inputs and outputs from those connected transactions.

D. Tunnelling

Name: Tunnelling
Also Know As: Hawala, Induced Transaction
Defining Characteristic: Connections and influence outside of the analysed blockchains. At least two related transactions that have no immediate or close relationship.

Constituent Transactions: Any transactions Sample Transactions: (See Figure 12)
\[ \text{dc3169e180261d89d895c437a48f2c19} \]
\[ \text{c18df7aadd6fa44e35f5910fa56300} \]
\[ \text{8cbb2da0df87a09330532089de74ebca} \]
\[ \text{296c221954566d8f8ea41379096f74ea} \]

In enumerating some of the transaction patterns both individually and as groups the emergent phenomena of a transaction network was observed. All of the patterns described in multi-transaction patterns section are a transaction network of some size.

A. Definition

A transaction network is a collection of two or more transactions that share a similar theme or aspect that influences the shape and structure of the transaction network.

The connected transactions do not need to be directly connected on the blockchain ledger although they usually are. The theme or aspect may be something concrete like an individual or a corporation, or it may be more abstract such as an emergent coinjoin network or a social construct such as tipping.

A transaction and the associated transaction outputs and inputs may belong to multiple transaction networks, such as green address and a peeling chain. Some transaction networks may also contain other transaction networks within itself, such as a peeling chain inside of a personal wallet.

B. Anatomy

To describe the parts of a transaction network, we will look at a partial and expanded version of the sample shown in the mixing cloud [20] with an additional transaction shown on the output [24]. The sample transaction is show in Figure 13.
A transaction network is best analysed by the transaction inputs and the transaction outputs rather than attempting to assign roles to a transaction. Because of the layering properties of a joint transaction a transaction can serve possibly all of the needed functions of a transaction network in a single transaction.

In this anatomy the transaction inputs and outputs will be referred to as coins. This brings the analogue of bitcoins closer to the terminology than “unspent transaction outputs” and the ungainly initialism UTXO.

Occasionally the term address may be used, but this usage is correct only if the address associated with the coins is only ever intentionally used in the role described. It is entirely possible that a single address can be used in all three roles.

1) **Entry Coins**: An entry coin is a coin that existed outside of the transaction network prior to its entry. It then participated in a transaction that is a part of the networks unifying theme or aspect. It represents a transition in control (such as from a customer to a bitcoin service provider) or in role (such as from an operational wallet into a storage wallet).

2) **Exit Coins**: An exit coin is a coin that originated from a transaction that had other coins participating in the transaction network and it is either an unspent coin or it participated in a transaction that is not part of the transaction network it came from. It similarly represents a transition on control or role like an entry coin does. It is common for an exit coin from one transaction network to become the entry coin to another transaction network.

3) **Interior Coins**: An interior coin is a transaction output and input that spans between two transactions that are in the same transaction network. The coin principally maintains the same control or role defining the transaction network between the output from one transaction to the input of the next transaction.

4) **Phantom Coins**: A phantom coin is a coin that does not exist as a proper transaction input or output of a transaction but is needed to explain the connectedness of the transaction network. Some examples are off-chain transactions at bitcoin exchanges and sidechain transactions.

C. **Common Types of Transaction Networks**

The following are some of the more common transaction networks that have been observed. A more firmal examination of these networks is outside the scope of this paper.

1) **Wallets**: The original transaction network was the bitcoin wallet. The user’s unspent transaction outputs form the core of the network, as well as change addresses automatically created by the wallet software. Entry coins map to payments received, outputs coins map to payments sent, and interior coins consist of the aforementioned change outputs.

2) **Exchange Operational Wallet**: The exchange operational wallet, sometimes called the “hot” wallet because of the immediate availability of the coins to customers, is an example of a transaction network defined both by control and purpose. In addition to entry and exit coins provided by customers this transaction network also commonly has entry and exit coins that go to or from the storage wallet for the exchange. Operational wallets also exhibit a larger amount of “churn” where a coin exists for a very short amount of time (sometimes only within one block), lower value of transactions, and a higher frequency of transactions.

3) **Exchange Storage Wallet**: An exchange storage or “cold” wallet is a wallet with some degree of separation from the operational side of the exchange. While controlled by the exchange like a hot wallet the storage wallets usually have distinctive control features such as a separate functionary in the organization responsible for access or multiple signature address, and in many cases storage of the private keys in offline storage devices or on paper printouts, and these are sometime kept in actual bank vaults or at the very least more secured physical. Storage wallets exhibit a longer lifespan of their related coins and tend to have fewer and higher value transactions.

4) **Mixer Clouds**: A mixer cloud is an example of a transaction network not unified by control but unified by a theme or purpose. Individual coins participating in a mixer...
cloud that exhibit a change in control usually transfer ownership at entry or exit to another party. In some odd cases an exit coin may become an entry coin back into the same cloud. Without solid ground truth such coins are indistinguishable from internal coins in the mixer cloud. The sharing of control inside the mixing cloud is usually accomplished via a coinjoin transaction or some variant of it.

VI. CONCLUSION

With the bitcoin blockchain recording every transaction that is, ever was, and ever will be recognized by the various bitcoin miners a rich treasure trove of information about financial practices is now available unlike we have never seen before. Because of the public nature of the transactions a simple million-dollar theft can get the kind of front-page news that a billion-dollar theft won’t get because of the cloak of bank secrecy. Therefore it is important to gain a better understanding of the structure of these transactions.

The patterns presented in this paper are not a complete enumeration of the patterns. Some useful patterns may have not been discovered yet and some may exist as closely held trade secrets by others. There is still more research to be done in this area, in particular the observation of the various known and unknown transaction networks. It is hoped that by sharing and formalizing this information that more discussion and research in this area will be conducted to further enumerate the patterns used on the bitcoin blockchain, as well as any other virtual or real currencies that use a publicly available ledger.

ACKNOWLEDGMENT

I would like to thank the Texas Bitcoin Conference for the call for papers. Without it I may never have been motivated to formalize my observations.

REFERENCES

[1] Bitcoin, Transaction ID f4184fc5 96403b9d 638738cf 57adeaf4c 75e605fb 356f6be9 335830e9 831e9e16, Block 341638, 2 Feb 2015
[2] Bitcoin, Transaction ID 4ae897f7 b2d84a85 d5f11d52 604fd8db e9f01302 beca8ddde 8ea450f9 9185dfb1, Block 289321, 7 Mar 2014
[3] Bitcoin, Transaction ID 9ce888af6 5260038 49964227 6a891878 a7254631 cbf14b2a 67fd2763 6e83be6a, Block 340475, 25 Jan 2015
[4] Bitcoin, Transaction ID 18ce4cf2 4ca3922e f8f335e3 95f9d9f4 5c26e226 ad8ccad0 1ca35a66 c8c3d24b, Block 309997, 9 Jul 2014
[5] Bitcoin, Transaction ID ebc940fc 20729063 7b6iac86 c6efced0c 5bf3d91 b5bf92078a7a3ace0 ac225882, Block 343620, 15 Feb 2015
[6] Bitcoin, Transaction ID 04160af0 70ac9bfa 5b20b27b 293b3141 c4e6ec37 1ec4b3d5 d36a6cf8 20fe130d, Block 320136, 11 Sep 2014
[7] Bitcoin, Transaction ID 54e48e5f 5e65b626 c3bca14a 8e95a58 3d07ebe8 4dce3b7d d4a78f4e 4188e713, Block 2300096, April 2013
[9] Bitcoin, Transaction ID 9e929888 182809f3 55bddec0 516dec34 e191d251 27b39ef4 576c6f73 22108f17, Block 342630, 9 Feb 2015
[10] Bitcoin, Transaction ID 1654912d 8af1ae66 718856ef 9745f83 e1cd7bb1f 588fcb80 3153e3bd fa97999b, Block 341070, 29 Jan 2015
[11] Bitcoin, Transaction ID 9256332b 9ea5252c b66f5729 d6f8982d 8a3f37d4 696bb4c10 e9f69b3d a0e6df38, Block 254450, 27 Aug 2013
[13] Bitcoin, Transaction ID 012c50a9 06ca6914e 6e5f86f0 e1af8f881 05eaa19e a9df1f35 275a4e0c e5e8e459, Block 142742, 27 Aug 2011
[14] Bitcoin, Transaction ID e3624514 4421135b 943765a6 0fff5f55fa0b00e0 c0d2f657 6b0c9255 e7f42665, Block 142742, 27 Aug 2011
[15] Bitcoin, Transaction ID 11f15283 27c01da4 01dexc0e f78a2c26 c15f17d7 397b328e 2190e130c e8f1ed2d, Block 259315, 22 Sep 2013
[16] Bitcoin, Transaction ID d3bdc116 4f5b2a6e d00b1dd7 09202231 89ea1061 c3593c57 5dc7778d 0d05c0d4, Block 259319, 22 Sep 2013
[18] Bitcoin, Address 1LNW6vyCakUmkhArb2N2fPMw6vG7sfWG7q
[20] Bitcoin, Transaction ID ef1995d 170e97bf0 017e23e1 737b45d5 2a71930f 4dl1bade 36b8e0e7 e778737c, Block 338077, 28 Jan 2015
[21] Bitcoin, Transaction ID dc316f9c 8026d1a89 d895e4c15 a8f2f2c19 c186d7a7 ddb6f44 e354f591 04aa5300, Block 322524, 25 Sep 2014
[22] Bitcoin, Transaction ID 201936b0 d0f7a9d3 30532089 dc74e6ca 296c2219 5456bd8f 8ea41379 096f74, Block 334073, 11 Feb 2015
[24] Bitcoin, Transaction ID 06268097a 8a59e047 1e1956d7 2bbed7f92 e965802e c30b1aa2 1e6667bc e8c5f6b9, Block 338103, 8 Jan 2015