# Decentralised Bitcoin Exchanges. The digital crumbs revealing your identity. Why financial privacy matters in the blockchain age and how to calculate privacy

Marco Gauer
University of Nicosia

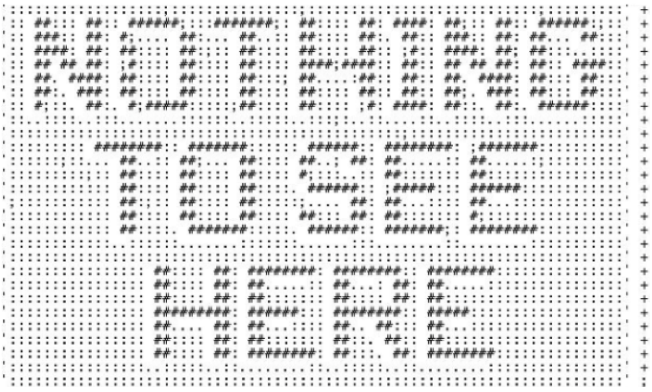
# Decentralised Bitcoin Exchanges. The digital crumbs revealing your identity

Why financial privacy matters in the blockchain age and how to calculate privacy

## Table of contents

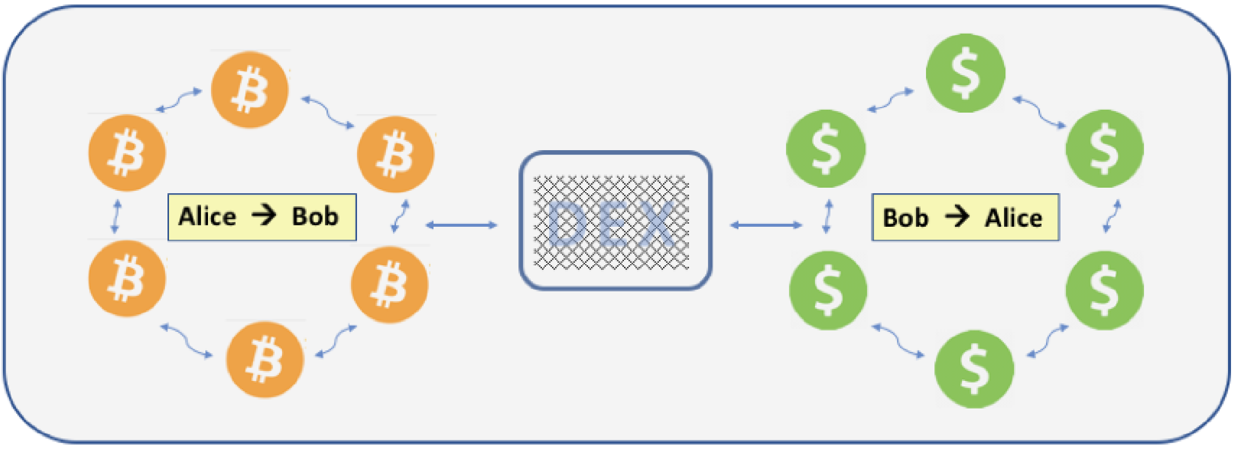
email: marco.gauer@gmail.com

## 1. Abstract



Exchanging one crypto currency for another or for national currencies, requires crypto exchanges unless the exchange happens via a personal contact or via an ATM. Most exchanges are centralized, however, given the many security problems(M1) and privacy breaches(M2) in the past, more and more decentralized, peer to peer exchanges (DEX) are emerging(M3).

As of May 2018, four out of more than 200 DEXs (Bisq(M24), Hawala, Openledger and Waves) support the exchange between Bitcoin and traditional currencies, with Bisq being most effective at protecting one's privacy. Data protection is no small feat. In chapter 2, this paper examines why and for whom privacy is important when using public blockchains via exchanges and how existing flaws can be fixed at Bisq.



Exchanging Bitcoin for national currencies or vice versa connects two currency networks, the Bitcoin network and the traditional national currency payment network. With a DEX deal, for example, a bitcoin amount moves from Alice to Bob and a dollar amount from Bob to Alice. In both systems, these transactions are put on the books (except for cash payments). They may, at first glance, have nothing to do with each other. However, the Exchange stores the link between these two transactions in a few pieces of data. Privacy for these cross-system swaps must be guaranteed on both sides, in both payment networks. If one side has a leak, the publicly accessible data of the DEX will build a bridge to the other side. In chapter 3, we take a detailed look at privacy on the national currencies side at decentralised crypto exchanges. Little has been written about this topic so far. A lot of research has already been done on the cryptocurrency side, the most important points are summarized in chapter 4.

The paper will examine whether privacy can be calculated and whether it can be improved at all.

## 2. Importance of financial privacy

Privacy isn't just for criminals, we all need privacy in financial matters. We don't want to receive advertising based on yesterday's shopping, we don't want to become a victim of a crime just because we're wealthy(M23). Especially in the volatile cryptocurrency area, a past trade of insignificant value can have, later on, great consequences. We don't want to explain ourselves because we bought something in particular. We don't want competitors and the rest of the world to know our income, turnover and profit. We don't want the complete history stored because it could be misused in case of current or future totalitarian regimes(M4).
We don't want to justify ourselves or be banned as payee, because fortuitously there is a link to criminals (e.g. a criminal buys from us a car). Or we could lose money because our crypto coins are, not by our own efforts, contaminated to a certain degree. They may have been mixed in the past with blacklisted coins (see company Chainalysis(M18) and others like http://taintchain.org). Nowadays, one gets the impression that all unhacked data is at high risk of being hacked at some point. This data can then be bought and abused by companies (e.g.: Did you buy cigarettes for a friend? Your new health insurance company hesitates to sign a contract with you). More than 8,000 data breaches have been made public since 2005, more than 10 billion records were stolen(M5). The number of unreported cases is likely to be much higher, as companies have not always an interest in reporting such problems or they may not even notice them. Misuse of data is now even suspected of influencing elections and thus harming our democracies(M6). The prospect of extensive and enduring data storage that can be made public or misused has the effect of silencing those who have nothing to hide. Thus influencing or reducing in a practical way freedom of speech and freedom of action(M9)(M10).
Only a fifth of the UK public trusts companies and organisations to store their personal data(M22). One can assume that the level of confidence is not significantly higher in other countries.
Member states of the European Union are committed to applying the principle of data minimisation(M7)(M8), Art. 5, (1) c) of the new data protection rules (GDPR): *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');"* There is a good reason for this.

This is all the more important when using public pseudo-anonymous blockchains like Bitcoin. What is the difference with traditional financial transfers of national currencies? Only few have access to your data (selected bank employees, if necessary state authorities or sometimes a hacker). Bitcoin, however is an open ledger. Everybody has access to it, anyone with Internet access and some expertise or anyone who is able to use database analysis software or an online explorer. Thousands will scan and analyse your footprint in the new decentralised public financial world. Although the sender and recipient of bitcoin transactions are protected by nameless use of numbered accounts (bitcoin addresses), if there is only a single link, a bridge to the outside (now or sometime in the future), then clustering techniques de-anonymize an avalanche of crypto financial transactions: The house of cards collapses. The financial actor's identity becomes like an open book. This does not change completely if you use a new bitcoin address for each transaction. In almost all cryptocurrency transactions there is some amount of change (the amount of Bitcoin used is larger than the transaction amount), such small amounts (we call 'change') are later mixed together and finally unite many Bitcoin addresses into an interrelated unit.

The following method and formulas are particularly important for oppressed organisations(M27) and private individuals living or operating under repressive regimes. According to Freedom House Reports(M20)(A1) about a quarter of all people live in non-free countries. However everyone else should also be aware of this problem. Seemingly harmless data collected today (in a democracy) can be used tomorrow by another (perhaps repressive) regime. History gives us the example of the democratic Weimar Republic, where homosexuals were largely tolerated for some time. Only harmless 'pink lists' with their names were kept. Later these list of names were used by subsequent dictatorship to arrest 100,000 men, many of whom ultimately perished in concentration camps.

### 3. Privacy on the fiat side

Anyone who exchanges fiat (national currencies) on a DEX such as bisq cannot, of course, prevent bookings on the blockchain or on their national bank account, but, as we will see, it is possible to make the link between the two very difficult. For this purpose, so-called 'discreet numbers' and 'discreet factors' are introduced, which are later very helpful for specific assessments or calculations of privacy.

### 3.a. Method for discreet numbers

In the summer of 1943, German air defence operators over Hamburg could no longer locate any aircrafts, because their radar units showed aircrafts everywhere. British pilots had airdropped millions of tinfoil strips which appeared as airplanes on the radar. The same strategy is recommended for privacy reasons when exchanging local currencies for crypto: if you can't hide a transaction, make sure it looks exactly like thousands of others.

Bisq is a public decentralised censorship resistant peer-2-peer exchange where everybody can trade on bitcoin main net Bitcoins against other cryptocurrencies or national currencies. Bisq is not a company, it's a budding 'Decentralized Autonomous Organisation' (DAO)(M25). The protocol works without any server or other single attack point. Trades are secured with 2-of-3 multisig escrow via the Bitcoin blockchain, distributed hash tables are used to temporarily store the data decentrally and flooding algorithms ensure messaging. Data is encrypted en route through hidden TOR nodes (no exit nodes). Bisq supports Tor bridges(M26) to enable use of the TOR network in case access is technically blocked in your country.

Bisq stores the history of all transactions in all nodes, including the timestamp, fiat amount (transfer amount in national currency), currency (e.g. USD,EUR,CHF, VUV, SAR,…, XMR, LTC ...), Bitcoin amount and payment method (e.g. bank transfer). Offers and agreed trades must be known to all Bisq nodes in order to manage this reliably on a decentralized basis. This data is pseudo-anonymous, it cannot be directly associated with a person. However, if authorized bankers, state authorities, hackers or a corrupt bank employee access data(M11)(M12), digital forensic time/value analyses could often reveal the identity years from now and the privacy of the crypto buyer or seller could be violated. How can Bisq users protect their privacy when exchanging national currencies? How can one hide the numbers among many others, like a needle in a haystack, so that attempting to personalize them is fruitless?

The strategy is to use unobtrusive amounts in trading, which are used at the same time by many other people in financial transactions. A data abuser then has no chance or at least a reduced chance of associating the trade on the exchange with your identity. The prerequisite, of course, is that such discreet and inconspicuous amounts do exist, which we will show below. The results are highly significant. Bank transfers are not directly controlled by bisq, only safeguarded with a 2-of-3 multisig escrow transaction in the Bitcoin blockchain (this is a simple form of a smart contract). The bank transfer purpose field in the bisq procedure is always filled in with a neutral code, which looks like an invoice number or the ordering code from any internet shop. If we use as data basis all bank transfers within a currency zone starting at the bisq transaction’s timestamp and 24h later, then one of those transfers relates to our bisq deal. Of course a bank transfer always appears on two accounts, once as a debit and once as a credit, we count this as one transfer.

### 3.b. Definition: discreet factor d(x,t*)

The discreet factor d(x,t*) represents how often a transfer amount x is used on a day t* in the same currency area compared to the average.

A more precise formal definition:
Let b be the smallest amount of money in a currency area so that 99% of all transfer amounts (used in a 12-month fixed reference period T from the near past) are less than b. In this currency area, we consider a transfer amount x with 0<x<b (two decimal places) on a certain day t*. This exact amount x would appear n(x,t*) times for bank transfers in the currency area on day t* (credit and debit are only counted once). Let a be the average of the 365*100*b possible n(x,t*) with 0<x<b and t*∈T. We define the discreet factor d(x,t*)

$$\mathbf{d(x,t^*) :=}\ \frac{n(x,t*)}{a}$$

The higher the factor (functional value) d(x,t*), the better. Better in the sense that frequently occurring transfer amounts cannot be assigned to one person, but transfer amounts occurring rarely can. A factor d(x,t*)=1 means, we have an average occurrence of that amount. A factor of 0.1 means, this exact amount occurs only 10%

as often compared to the average. d(x,t*)=2 means the amount x occurs twice as often than average on day t* in the currency area.
You may wonder why we need the 99% barrier b here. This is to stay in the realm of finite possibilities. Without these you could not calculate average frequencies of amounts, because it would be 0. The basis is what has been transferred not what amount could theoretically be transferred.

### 3.c. Example of a discreet factor

A transfer amount x in Swiss francs (a smaller 99% barrier b) occurs on average about 1.61 times on the same day t* among all transfers. If after applying one or more associated steps d(x,t*) = 39, one can expect that the new amount will occur on average 1.61 * 39 ≅ 63 times on the same day as the transfer amount. As we will see below, this essential difference can already be achieved by changing the decimal places.

Below are the 5 steps with intermediate factors d1,...,d5 to find a good transfer amount x and a good date t*, so that the product d(x,t*)=d1*d2*...*d5 becomes as high as possible.
The steps are unknown to Bisq traders or at least not used, as you can see in the public Bisq history. All these steps should be carried out in the order indicated to protect the privacy on the fiat side, which is the gateway to privacy on the linked crypto side. The factors d1,...,d5 are designed to be 1 for an average trade each.

### 3.d. Five steps towards privacy

#### 3.d.i. Step 1: Wise trade time / discreet factor $d_1$ = 0.3-5.4

On an average day, approximately 100%/30 = 3.3% of all monthly transfers take place. On the first banking day, however, the average is 5.4 times as many[M16]. Compared to the weakest days (after the 6th day of a month with exception 15th of a month) it is even about 18 times as many transfers. The recommendation is to make such trades on the first banking day of the month if possible (if the first day of the month falls on a weekend or a bank holiday, the effect is even greater) and at least not after the 6th of the month (with the exception of the 15th day).

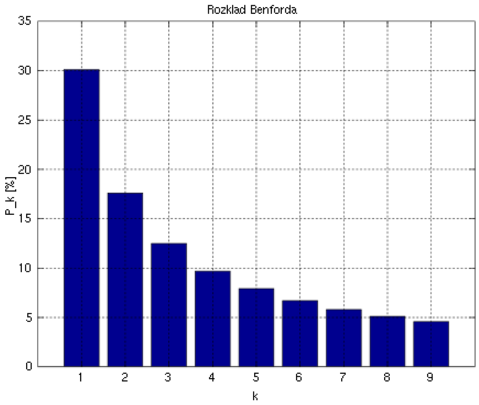
#### 3.d.ii. Step 2: Currency selection / discreet factor $d_2$ = 0.0000864553-1.5

The bigger the currency area and the lower the exchange rate to Bitcoin, the better. If you can make bank transactions with different currencies, so if you have a choice, always use the currency with the largest currency area and lowest exchange rate.
To compare two currencies in terms of privacy, the following rule of thumb may apply:
Exchange rate Currency1 to 1 Bitcoin: e1
Exchange rate Currency2 to 1 Bitcoin: e2
Number of transfers Currency1 per day: n1
Number of transfers Currency2 per day: n2
Now calculate the quotients n1/e1 and n2/e2, wherever the larger number comes out, this is the more suitable currency.
The exchange rate is important, because a high exchange rate increases the number range in the local currency below the 99% barrier b.

For example, if you are in Saudi Arabia and have the chance to transfer in US-dollars, you move your trade into a 70 times bigger currency area with a better exchange rate of factor 3.75 (better in the sense that a country with smaller amounts uses fewer amounts overall and therefore each individual transfer can be better obfuscated). Without touching the other steps you can expect that your trade amount occurs about 262 times more often in the currency area. Citizens of the South Pacific island state of Vanuatu also trade on bisq their currency Vaduz (VUV) against Bitcoin. With only 90,000 local bank transfers estimated per day (0.333 per citizen) and an exchange rate of about 1BTC = 1Mio VUV, anonymization is extremely weak, this is ‘discreet numbers’ technologies nightmare. A suggestion to the inhabitants would be to have a club where everyone makes the same transfers. As a realistic value we assume that the currency area effect can be improved on average by factor 1.5 (weighted analysis of currencies used in bisq and assumed opportunities for improvement).

### 3.d.iii. Step 3: Fiat amount to start with low digit / discreet factor $d_3 = 0.31\text{-}3.74$

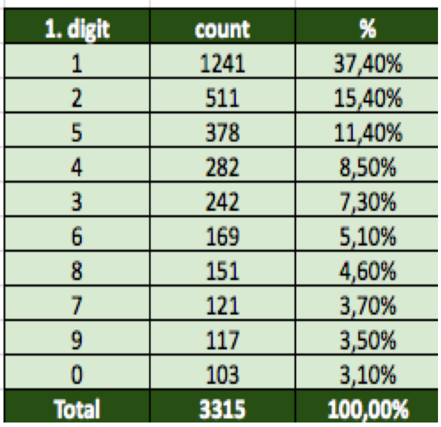
Financial data sets (amounts) usually obey Benford’s law(M13)(M14)(M15). Benford found out nearly 80 years ago that financial amounts start much more often with small digits than with large ones. This is the usual logarithmic distribution, the 1 occurs e.g. more than six times as frequently as the 9:



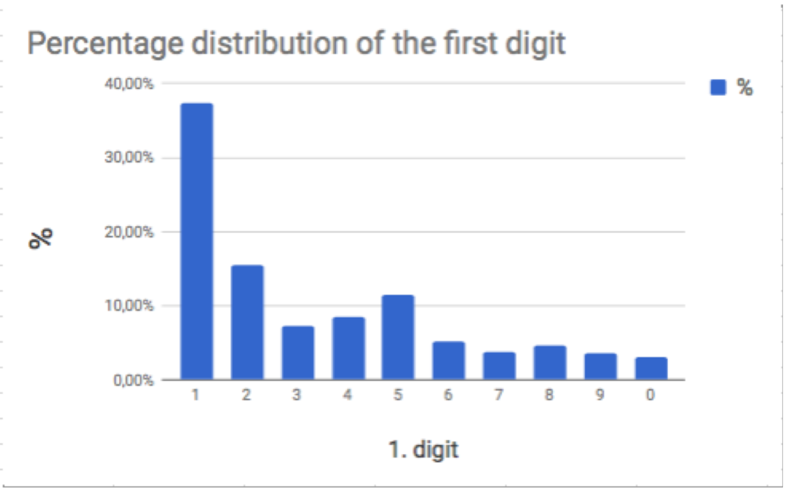
(M13)

This was compared with real bank data by analyzing 3315 transactions, the result confirms the more frequent occurrence of amounts starting with small numbers (although it is not an ideal Benford curve)(M16).

The amounts start more than 10 times more often with a 1 (37.4%) than with a 9 (3.5%).



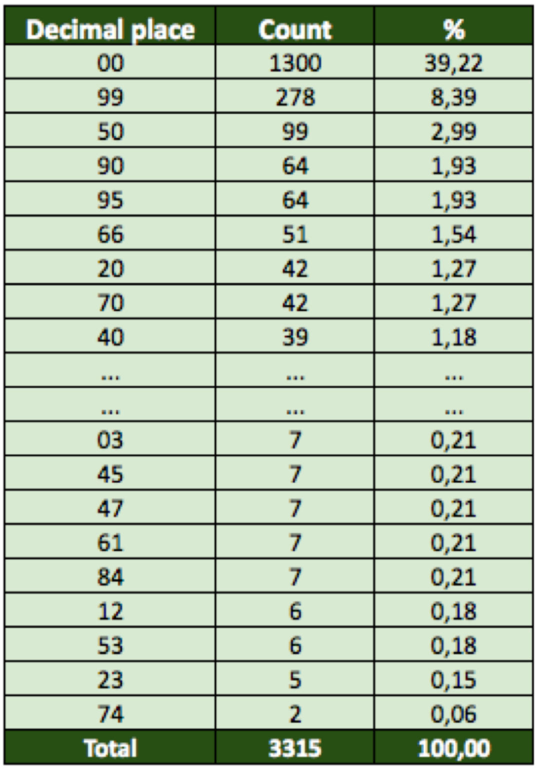
| 1. digit | count | % |
|---|---|---|
| 1 | 1241 | 37,40% |
| 2 | 511 | 15,40% |
| 5 | 378 | 11,40% |
| 4 | 282 | 8,50% |
| 3 | 242 | 7,30% |
| 6 | 169 | 5,10% |
| 8 | 151 | 4,60% |
| 7 | 121 | 3,70% |
| 9 | 117 | 3,50% |
| 0 | 103 | 3,10% |
| Total | 3315 | 100,00% |



Of course we can use this to our advantage when trading. Better to make a deal with 1000€ than with 790€ or 980.78€.

### 3.d.iv. Step 4: Fiat amount rounded to full amount X.00 / discreet factor $d_4$ = 0.06-39.2

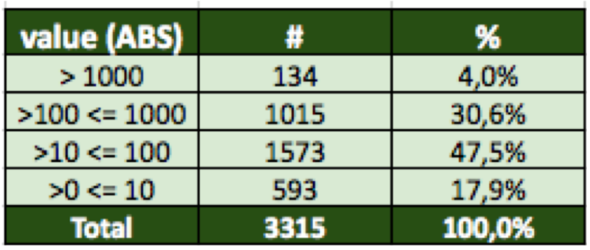
There are 100 different possibilities for the Mantissa ( https://math.stackexchange.com/questions/64042/what-are-the-numbers-before-and-after-the-decimal-point-referred-to-in-mathemati ). At first glance, one might think that each of these options should occur with a 1% frequency in a normal bank account. However, this is by no means the case. In the 3315 transactions studied, all 100 possibilities were available, but the most common were 0 cents, the second most 99 cents. It is recommended to take only the .00 or may be sometimes the .99. The .00 is 39.2 times more often used than the average and e.g. 218 times more frequent than .53. The values at the end of the table are not exact numbers due to the low occurrence, but this does not change the recommendations made. Only the upper 1-3 values should be used. Step 4 is our most powerful instrument.



| Decimal place | Count | % |
|---|---|---|
| 00 | 1300 | 39,22 |
| 99 | 278 | 8,39 |
| 50 | 99 | 2,99 |
| 90 | 64 | 1,93 |
| 95 | 64 | 1,93 |
| 66 | 51 | 1,54 |
| 20 | 42 | 1,27 |
| 70 | 42 | 1,27 |
| 40 | 39 | 1,18 |
| ... | ... | ... |
| ... | ... | ... |
| 03 | 7 | 0,21 |
| 45 | 7 | 0,21 |
| 47 | 7 | 0,21 |
| 61 | 7 | 0,21 |
| 84 | 7 | 0,21 |
| 12 | 6 | 0,18 |
| 53 | 6 | 0,18 |
| 23 | 5 | 0,15 |
| 74 | 2 | 0,06 |
| Total | 3315 | 100,00 |

### 3.d.v. Step 5: Low amounts / discreet factor $d_5$ = 0.33-3

The transfer amount should not be too high. In our sample, 96% of all amounts were below 1000€. If necessary, simply make several transfers out of one deal. In our data there were usually between 2-10 times as many amounts in the same range when the amount was halved (i.e. divided into two transfers). A division into three partial amounts also appears appropriate (especially in combination with a small 1st digit). Since not all two or three partial amounts have to be of the same size, there are a very large number of possible combinations here. The available data basis is not sufficient for precise statements. Taking into account that splitting transfer amounts also has a slightly opposite effect, it’s conservatively estimated that a realistic possible factor is about 3.



| value (ABS) | # | % |
|---|---|---|
| > 1000 | 134 | 4,0% |
| >100 <= 1000 | 1015 | 30,6% |
| >10 <= 100 | 1573 | 47,5% |
| >0 <= 10 | 593 | 17,9% |
| Total | 3315 | 100,0% |

### 3.e. Discreet Factor formula

Discreet factor (multiplicative comparison of a good choice x,t with an average choice)

**$d(x,t) = d_1(x,t) * d_2(x,t) * d_3(x,t) * d_4(x,t) * d_5(x,t)$**

That means on average we can improve our privacy for a given (x,t*) by applying steps 1-5 by a factor of d(x,t*) = 5.4 * 1.5 * 3.74 * 39.2 * 3 = 3562.6

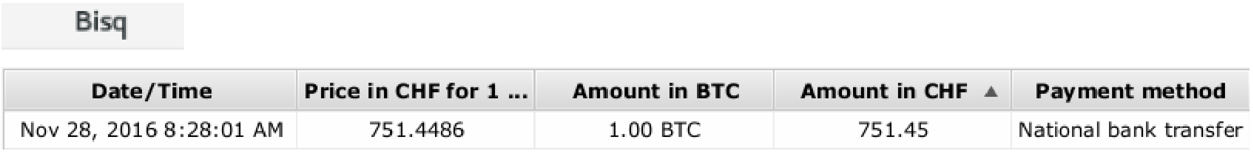
Maximum impact factor (comparison of the best and the worst choice)

**$d_{max\_impact}$ =** (5.4/0.3) * (1.5/0.0000864553) * (3.74/0.31) * (39.2/0.06) * (3/0.33) **= 65.7 billion**

### 3.f. Examples

**3.f.i Example 1** (real existing trade at bisq exchanging 1 Bitcoin (BTC) against 751.45 swiss francs (CHF)

**Bad choice for discreet number selection**



| Date/Time | Price in CHF for 1 ... | Amount in BTC | Amount in CHF ▲ | Payment method |
|---|---|---|---|---|
| Nov 28, 2016 8:28:01 AM | 751.4486 | 1.00 BTC | 751.45 | National bank transfer |

$d_1$ = 1.07 (calculated from the analysis carried out)
$d_2$ = 0.01868 (exchange rate is similar, but smaller currency area than US/EU)
$d_3$ = 3.7%/10% = 0.37 (first digit is a 7, 10% would be factor 1)
$d_4$ = 0.21 (decimal amount is 45)
$d_5$ = 2 (it looks like in bisq that the trader split the amount in half due to the maximum allowed BTC-amount - assumption)

=> **d(CHF 751.45 , 11.28.2016) =** 1.07 * 0.01868 * 0.37 * 0.21 * 2 **= 0.0031**

This is quite a bad discreet factor which nearly guarantees, that the amount of CHF 751.45 is unique. Under the assumption that the trader cannot change the currency the situation could have been much better by carrying out three CHF 250.00 trades three days later on Dec 1, 2016 with the following results:

$d_1$ = 5.4 (good trade time)
$d_2$ = 0.01868 (no change, assumption is the trader cannot switch to EUR/USD)
$d_3$ = 1.54 (first trade amount digit improved from 7 to 2)
$d_4$ = 39.2 (decimal place = 0, which is easy to make happen and brings a huge gain for our discreet factor)

$d_5$ = 3 (splitted into three trades)

=> **d(CHF 250.00 , 12.01.2016) =** 5.4 * 0.01868 * 1.54 * 39.2 * 3 **= 18.27**

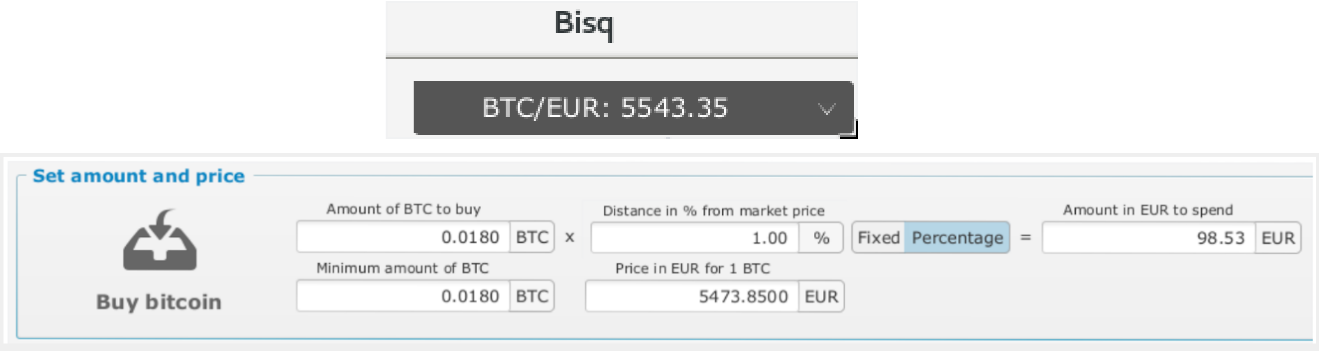
which is a nearly 5900 times better discreet factor than the real one from the bisq history and makes it very likely that your trade stays private.

There are around 1.95 million private credit transfers per day in Swiss francs(M19) (this number requires halving, as each amount appears on one account as a debit, on another as a credit). Neglecting the rare transfer amounts over the 99% barrier b = CHF 12,000 (estimation for b, don't use this amount with every currency), there are 1.2 million different amounts possible between CHF 0.01 and CHF 12,000, so on average each amount occurs 1.61 times daily. With a well-chosen discreet score the amount will occur thousands of times. Having a bad discreet score by ignoring this or by bad luck might result in you being the only one using that amount on that day. The time/amount factor is a potential attack vector, the digital crumbs will reveal your identity and your Bitcoin ownership!

### 3.f.ii. Example 2

### Bad choice for discreet number selection

In this example, we simulate buying bitcoins with euro in order to test whether the large currency area alone creates inconspicuousness. An amount that is not privacy friendly is set (starting with a high digit 9) and not rounded to whole euros (53 cents). As for timing, we assume the 17th of the month.



Bisq

BTC/EUR: 5543.35

Set amount and price

Buy bitcoin

Amount of BTC to buy: 0.0180 BTC

×

Distance in % from market price: 1.00 %

Fixed | Percentage

=

Amount in EUR to spend: 98.53 EUR

Minimum amount of BTC: 0.0180 BTC

Price in EUR for 1 BTC: 5473.8500 EUR

Lets calculate the discreet factor:

$d_1$ = 0.5 (unfavourable date according to the data collected)

$d_2$ = 1.5 (large currency area)

$d_3$ = 3.5%/10% = 0.35 (first digit is a 9)

$d_4$ = 0.18 (digital place 53)

$d_5$ = 3

=> d(€98.53 , day 17) = 0.5 * 1.5 * 0.35 * 0.18 * 3 = 0.14175

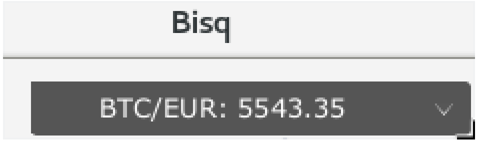
How many clone friends does a € transfer actually have in a 24h window? This can be estimated. According to the European Central banks(M17) latest statistics there are 30.5 billion credit transfers by Non-banks per year in the EU. This means in a 24h window we have on average 83.562 million. Global Finance statistics(M19) suggest that there are about twice as many, so I conclude that each amount was counted twice (on the sender account as debit and on the recipient account as credit). We assume the 99% barrier as b = €10,000.

With 1 million possibilities between €0 and €10,000 an average amount can be seen slightly less than 83 times per day. With the above discreet factor we can assume, that our €98.53 appears 83 * 0.14175 = 11-12 times. This is not much, especially because those calculations aren't exact, only estimates that are volatile. So a selection with such a small d(..) in even in a large currency area like EU or US is a risk.

### 3.f.iii. Example 3

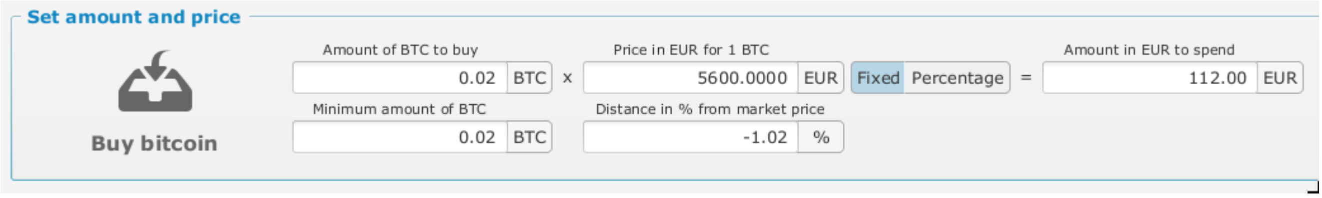
**Good choice according discreet number selection**

In this example one should post new trade offers in the exchange (in this case buying 20mBTC with euros). The amount starts with the small digit 1 and there are whole euros, no cents. The price is fixed. To achieve this, the exchange rate was adjusted slightly unfavourably, there is no free lunch.



Bisq

BTC/EUR: 5543.35



Set amount and price

Buy bitcoin

Amount of BTC to buy: 0.02 BTC × Price in EUR for 1 BTC: 5600.0000 EUR [Fixed] Percentage = Amount in EUR to spend: 112.00 EUR

Minimum amount of BTC: 0.02 BTC

Distance in % from market price: -1.02 %

Assuming the trade date is the first day of a month, the discreet numbers factors are:

| | |
|---|---|
| $d_1 = 5.4$ | (optimal date according to the data collected) |
| $d_2 = 1.5$ | (large currency area) |
| $d_3 = 3.7$ | (first digit is a 1) |
| $d_4 = 39.2$ | (digital place 00) |
| $d_5 = 3$ | (a split of low amounts is not helping) |

=> d(€112 , day 1) = 5.4 * 1.5 * 3.74 * 39.2 * 3 = 3562.6

That means we can expect about 83 * 3562.6 = 295,696 identical amounts on the same day. This is a 25,133 times better value than on the example before, so a success from a privacy point of view.

By using all five steps of the discreet numbers methodology we can assume that there are on average 5.4 * 1.5 * 3.74 * 39.2 * 3 = 3562.6 times more clones available with the same amount. This makes you a stealth trader, at least if you acted as wisely on the crypto side. A privacy breach based on a time/value attack on the fiat side is therefore nearly impossible. Obviously this can also be applied to other financial transactions, it is not reduced to Bisq.

The proposed changes to obtain discreet amounts can be implemented immediately by users without requiring a change to the program code or to the agreement with the trading partner. In the long run, however, it would make sense to support this in code (e.g. allow more decimal places on the bitcoin side, split deals into 100 + 200 euros as they are better than 300 euros, suggest sensible amounts and ensure high liquidity through cooperations / atomic swaps or advertising).

You won't always get exactly the same values in your own analyses with your own basic data, some elements were subject to estimates or would slightly change by analysing a larger data set. Nevertheless, a similar result would be obtained and the conclusion would remain the same.

### 3.g. Calculating privacy and the likelihood that an immutable past trade was a stealth trade

Let *e*' be the exchange rate for 1 Euro from the traded currency (at a specific date) and n be the average number of daily transactions in the currency area. A trade is deemed private if at least p=100 people have transferred the same amount on the same day. We define p=p(x,t) as the *privacy* of (x,t), the higher p (numerous people doing the same), the more private a trade is. It is now necessary to calculate the share of trades this applies to.
First we need to calculate the 99% barrier. For the Euro currency area, our assumption was b=10,000€, for another currency it's b=10,000*e' (for countries with low GDP the real 99% barrier might be lower)

3.g.i. Specific trade (x,t)

You can calculate the privacy by calculating/estimating the *discreet number* factors $d_{1,}$ $d_{2,}$ $d_{3,}$ $d_4$ and $d_5$ as explained above. With d(x,t) = $d_1 * d_2 * d_3 * d_4 * d_5$ and b=10,000*e' we obtain the

**Privacy formula**

$$\mathbf{p(x,t)} = \frac{0.99 * n}{b * 100} * \mathrm{d(x,t)} = \frac{0.99 * n}{10{,}000 * e' * 100} * \mathrm{d(x,t)}$$

$$= \frac{0.99 * n}{1{,}000{,}000 * e'} * \mathrm{d(x,t)} = \mathbf{0.00000099} * \frac{n}{e'} * \mathbf{d(x,t)}$$

3.g.ii. Generally

This needs to be considered for each currency area. Below are examples for some countries. With f=0.00000099*n/e' we have p(x,t) = f * d(x,t).

3.g.iii.1. The minimum privacy is f * 0 = 0
[0% of all (x,t) have a worse privacy figure]

3.g.iii.2. The average privacy is f * 1 = f
[appr.* 50% of all (x,t) have a worse privacy] *appr. because 50% is the median

3.g.iii.3. The privacy level we're interested in is f * (100/f) = 100
[**h%** of all (x,t) have a worse privacy figure / h to be calculated]

3.g.iii.4. The maximum level of privacy is f * $d'_{max}$ (= f * $d_{1\,max}$ * 1 * $d_{3\,max}$ * $d_{4\,max}$ * $d_{5\,max}$ )
[100% of all (x,t) have a worse privacy level. $d_{2\,max}$ is ignored here because the currency is predetermined]

Using logarithms we can calculate approximately the percentage of all (x,t) which are below a privacy of 100, the

***Privacy100-Percentage h***:

**h = 50% [1 + max(-1,min(1,** $\frac{ln(100/f)}{ln(d'max)}$ **))]**

3.g.iii. Now we can apply the formula to a few currency areas.

3.g.iii.1. Switzerland CHF

n = 1.95 million

e' = 1.2 (May 2018, replace it with latest figures)

=> f = 1.61

With $d'_{max}$ = 2375.1 we obtain for the Privacy100-percentage

h = 50%[1 + max(-1,min(1, $\frac{ln(100/1.61)}{ln(2375.1)}$ ))] = 50% * (1 + 0.5312) = 76.6%

So approximately 76.6% of all possible (x,t) have a privacy < 100 (which is not wanted), about 23.4% have a privacy > 100. If you have only a handful of trades, it is of course difficult to extrapolate this, it is advisable to determine the individual privacy values under 1.

3.g.iii.2. European Union EUR

n = 83.562 million

e' = 1

=> f = 82.73

With $d'_{max}$ = 2375.1 we obtain for the Privacy100-percentage

h = 50%[1 + max(-1,min(1, $\frac{ln(100/82.73)}{ln(2375.1)}$ ))] = 50% * (1 + 0.0244) = 51.2%

Approximately 51.2% of all possible (x,t) have a privacy < 100 (which is not wanted), about 48.8% have a privacy > 100.

3.g.iii.3. Vanuatu VUV

n = 90,000

e' = 132.262 (May 2018 value!)

=> f = 0.000673663

With $d'_{max}$ = 2375.1 we obtain for the Privacy100-percentage

h = 50%[1 + max(-1,min(1, $\frac{ln(100/0.000673663)}{ln(2375.1)}$ ))] = 50% * (1 + 1) =

100%

About 100% of all possible (x,t) have a privacy < 100 (which is not wanted),

about 0% have a privacy > 100. Probably all of your past bisq trades have a

privacy < 100.

In these extreme marginal areas you have to be very careful with the results. Even if the calculated Privacy value is 100%, there will always be social phenomena or exceptions making reality look different.

Let's suppose a local custom has it that on May 5 all uncles and aunts transfer 1000 VUV to their nieces and nephews and you make a bisq deal for 1000 VUV on the same day, then the statistical considerations do not apply in this case. Likewise, if you'd found a Vanuatu 999-club and convince everyone to transfer 999 VUV to someone else on the 7th of the month, obviously you'd be able to go undetected under this cover.

3.g.iii.4. Saudi Arabia SAR

$n = 2.21$ million
$e' = 4.4867$ (May 2018 value!)
$\Rightarrow f = 0.4876$
With $d'_{max} = 2375.1$ we obtain for the Privacy100-percentage

$$h = 50\%[1 + \max(-1,\min(1, \frac{ln(100/0.4876)}{ln(2375.1)}))] = 50\% * (1 + 0.6849) = 84.25\%$$

So approximately 82.59% of all possible (x,t) have a privacy < 100, about 15.75% have a privacy > 100.

## 4. Privacy on the crypto side

Bisq has already a high standard. What recommendations could be made, on the cryptocurrency side, to decentralized exchanges and their users ?

a. Monero & Co

Bitcoin is an open book which is not optimal for securing user privacy. Either there will be updates to increase the privacy (e.g. Coinjoin), or Bitcoin's fungibility will disappear sooner or later. That means that the exchange values for one Bitcoin won't be the same as for another Bitcoin (almost all coins will be contaminated to a minor degree at some point, a lower contamination then means a higher value). It's only a question of time before all central exchanges filter each affected coin against black and white lists. This is partly the case today. If the Bitcoin community fails to solve this issue then it is recommended to use coins supporting a certain level of privacy (Monero, zCash, Dash and others).
What has privacy to do with value and fungibility? The problem bears a resemblance to the following fictional story:

Imagine that after using a banknote, the banknote number is always reported to a central database, including information about who handed over the banknote to whom. The database isn't 100% accurate, but gives a good picture of how the money flows. If there is any doubt about the legality of a transaction, the number on each affected banknote is placed on a central black list. Today you go to a store and when paying the seller compares the number of your 50 dollars banknote with the black list and finds that the number was added yesterday, because two years ago it was used by a criminal. He won't accept your 50 dollars as a means of payment. The banknote has already changed owners dozens of times in the last two years and you have nothing to do with the illegal business, but nobody wants a banknote like this anymore. You can throw it away or trade it on the black market for a clean 10 euro banknote.

The value of your 50 dollars is at best 10 euros not because you did anything wrong but just because there was no privacy.
Since several small 'banknotes' can become one large 'banknote' with Bitcoin, a Bitcoin amount has usually a proportionate contamination, e.g. 0.17%.
http://taintchain.org (and others) are going to maintain and publish black lists.

b. Own full Bitcoin node
Either integrated into the DEX software or started in parallel by the user (Bisq automatically prefers a local full Bitcoin node if available). Otherwise the connection to the Bitcoin network goes via bitcoinj to external nodes. There is a severe privacy leak in the broken bitcoinj bloom filters (an external spying node can link all addresses of the DEX client to each other). Alternatively, if you know one or more 100% trusted nodes you can connect to them with program parameter -btcNodes=[IPadress1,IPadress2,...]

c. Use fresh coins to fill your trade wallet
If you use coins mixed with coins having a trail to you, then you generate a trail as well from the new coins of the DEX. This can be avoided by using services like xmr.to or shapeshift.io via VPN.

d. Don’t mix coins after moving it out of the DEX wallet
After transferring new coins out of the DEX environment you shouldn’t mix them with other coins.

e. Address change. Change your bisq onion address from time to time. Do this if no trade is open and you withdrew your funds. You can start a fresh account by adding parameter ‘-appName=Bisq2’ when starting. You can run as well parallel instances of bisq this way.

f. No reuse of Bitcoin addresses
Changing the bitcoin address on each trade is useful to increase the privacy.

g. Operating system
Keep your system safe and use a fresh environment without running other programs in parallel[M21] (e.g. booting from a live linux distribution via usb stick). Qubes is an operating system supporting security at a very high standard. Applications run in (temporary) containers and cannot access other containers. Malicious Trojans have no chance.

It would be ideal from this viewpoint if every cryptocurrency entering the DEX door already brings a high degree of privacy (such as ring signatures, stealth addresses, ZkSNARKS,...). Alternatively users need to manage this which is a bit tricky for non tech people.
Another ideal approach from a privacy point of view would be that a cryptocurrency prevails worldwide and largely replaces fiat currencies. This would eliminate entry and

exit points and even pseudo-anonymous currencies would be much more difficult to abuse from a data protection perspective.

## 5 Conclusion

In times of data scandals or the resale of customer data, in times when a quarter of humanity cannot really enjoy freedom, in times when over a billion people are economically restricted because they do not have access to banking services like a normal account, more and more people tend to gain their financial freedom with digital peer to peer money like Bitcoin and exchange it in DEXs. It has been shown that the secure, supposedly private trading of Bitcoin against national currencies on decentralized exchanges creates digital footprints and endangers privacy.
The combination of the exchange amount and the exchange date will reveal the identity of the exchange partners sooner or later. This is mainly caused by the constantly changing ‘random’ exchange rate. Explanations were given on how to avoid this problem.

To improve privacy by a factor of 3500, a 5-step method was presented. The most effective method is the fourth, which improves privacy by a factor of 39 by simply changing the decimal places of an exchange amount. This is done by calculating the new so-called discreet numbers and discreet factors. A privacy formula was presented that allows the calculation of the privacy on the national currencies side for any Bisq trades. Furthermore, a formula was developed (Privacy100-Percentage) allowing to compare privacy levels between different currency areas. Indeed, there are very large differences depending on the national currency used. The individual results were explained using several examples.

If there is an increased need for privacy (e.g. for organisations under repressive regimes or for data privacy enthusiasts), the new methods and formulas can be used to ensure that trades with national currencies resist time/amount attacks. All this is even more useful if no other gate is opened on the crypto side. The most important factors in this regard were explained.

## 6. Acknowledgement

Thanks to David Boveington-Fauran for editorial and stylistic modifications and to the University of Nicosia staff and students for inspiration.

## 7. Conflict of interests declaration

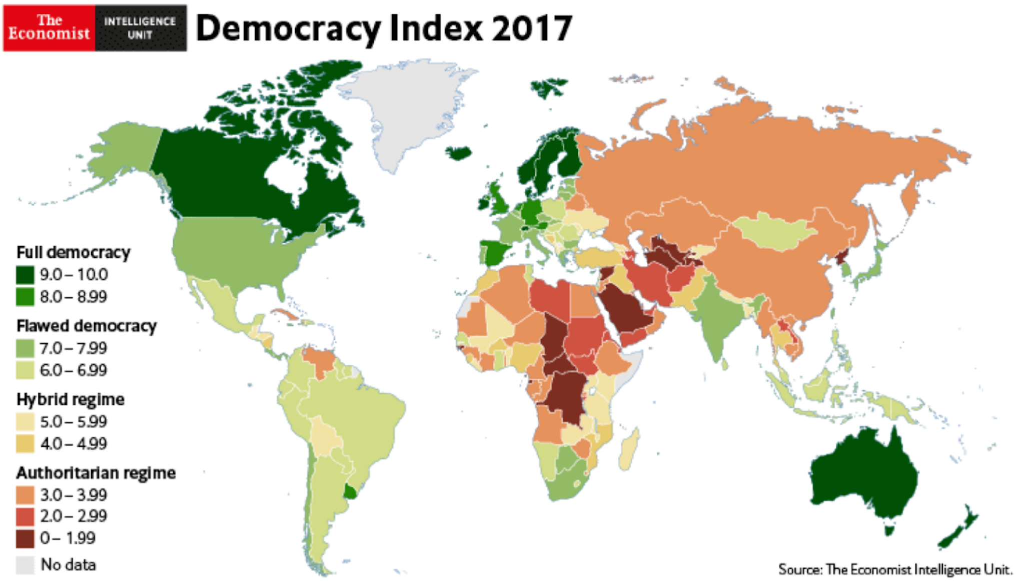
The author declares that there is no conflict of interest

## 8. Post scriptum

If someone has a large number (> 10,000) of reliable and anonymous bank transfer data from current century (incl. value, currency and if possible date specifications), the author asks for an e-mail including the reasons why the data is authentic. Please no data with additional information (data minimisation). The more data available as a basis, the more accurate calculations can be made for discreet numbers and privacy. Thank you!

## 9. Appendix

(A1) The Economists Intelligency Unit Dempcracy Index, https://www.eiu.com/topic/democracy-index



Source: The Economist Intelligence Unit.

## 10. References

(M1) TOP 5 CRYPTO EXCHANGES HACKS IN THE HISTORY

http://www.vizzwebsolutions.com/top-5-crypto-exchanges-hacks-in-the-history/

(M2) All Major Korean Cryptocurrency Exchanges Fail Privacy Tests – 30 Days to Improve https://news.bitcoin.com/korean-cryptocurrency-exchanges-privacy-tests/

(M3) Github list of all DEX
https://github.com/distribuyed/index

(M4) List of totalitarian regimes
https://en.wikipedia.org/wiki/List_of_totalitarian_regimes

(M5) Privacy Rights Clearinghouse: More than 8000 data breaches made public since 2005
https://www.privacyrights.org/data-breaches

(M6) Cambridge Analytica used data from Facebook and Politico to help Trump
https://www.theguardian.com/technology/2017/oct/26/cambridge-analytica-used-data-from-facebook-and-politico-to-help-trump

(M7) European Union, The principle of "data minimization"
Art. 5, (1) c) "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');"
https://edps.europa.eu/data-protection/data-protection/glossary/d_en
https://gdpr-info.eu/art-5-gdpr/

(M8) Forbes: Why data minimisation is an important concept in the age of big data
https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#7c820d2c1da4

(M9) Mass surveillance silences minority opinions, according to study
**Under Surveillance:** Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring
https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/?utm_term=.3e8fffa8e6e9
http://journals.sagepub.com/stoken/rbtfl/1jxrYu4cQPtA6/full

(M10) Why Privacy is important even though you have nothing to hide
https://medium.com/meet-lima/why-privacy-is-important-even-though-you-have-nothing-to-hide-ee93c27ab26f

(M11) The New York Times - Feb 1, 2016
Bank Tellers, With Access to Accounts, Pose a Rising Security Risk
https://www.nytimes.com/2016/02/02/nyregion/bank-tellers-with-access-to-accounts-pose-a-rising-security-risk.html

(M12) Express - July 27, 2017
Italy's largest bank HACKED in major security breach as data from 400,000 accounts stolen
https://www.express.co.uk/finance/city/833440/italy-unicredit-bank-hacked-cyberattack-italian-banking-major-security-breach

(M13) Benford's Law
https://en.wikipedia.org/wiki/Benford%27s_law

(M14) The Effective use of Benford's Law to Assist in Detecting Fraud in Accounting Data
http://faculty.usfsp.edu/gkearns/Articles_Fraud/Benford%20Analysis%20Article.pdf

(M15) Price Developments After a Nominal Shock: Benford's Law and Psychological Pricing After the Euro Introduction
https://www.researchgate.net/publication/222708069_Price_Developments_After_a_Nominal_Shock_Benford%27s_Law_and_Psychological_Pricing_After_the_Euro_Introduction

(M16) Analysis of 9 bank accounts (7 private accounts and 2 business accounts), overall 3315 bank transfers. Marco Gauer, 2018
http://these_data_will_not_revealed_here.com

(M17) European Central bank press release- 2017, Sep 15
Payments statistics for 2016
https://www.ecb.europa.eu/press/pdf/pis/pis2016.pdf?be9989f6bd72483ebe27d8dfae1f0362

(M18) Chainalysis: “PREVENT, DETECT AND INVESTIGATE CRYPTOCURRENCY MONEY LAUNDERING, FRAUD AND COMPLIANCE VIOLATIONS.”
https://www.chainalysis.com

(M19) Global Finance. Payments Volumes Worldwide. Payment Transactions by Non-Banks
https://www.gfmag.com/global-data/economic-data/26gzj8-payments-volumes-worldwide

(M20) Freedom House reports
https://freedomhouse.org/report/special-reports/worst-worst-2012-worlds-most-repressive-societies

(M21) On Gui isolation. Joanna Rutkowska
https://blog.invisiblethings.org/2011/04/23/linux-security-circus-on-gui-isolation.html

(M22) INFORMATION COMMISSIONER’S OFFICE – TRUST AND CONFIDENCE IN DATA
http://www.comresglobal.com/wp-content/uploads/2017/11/ICO_trust-and-confidence-in-data_2017-1.pdf

(M23) Cointelegraph apr 10, 2018: “Extorted 200 BTC From Businessman”
https://cointelegraph.com/news/india-police-officers-beat-exhorted-200-btc-from-businessman-local-sources-say

(M24) Bisq - the P2P exchange network
https://bisq.network

(M25) Wikipedia: Decentralized Autonomous Organization
https://en.wikipedia.org/wiki/Decentralized_autonomous_organization

(M26) Tor Documentation: Bridges
https://www.torproject.org/docs/bridges

(M27) The Guardian: Civil rights groups face global crackdown ‘not seen in a generation’
https://www.theguardian.com/law/2015/aug/26/ngos-face-restrictions-laws-human-rights-generation