Bachelor Degree Project

An Evaluation of User Attitudes Towards Anonymity in Bitcoin

Bachelor Degree Project in Informatics
Level ECTS
Spring Term 2017

Mihkel Pajunen

Supervisor: Dennis Modig
Examiner: Jianguo Ding

Abstract

Bitcoin has emerged as the leading cryptographic currency since its inception in 2009 and at the time of writing holds a market capitalization of $28.4 billion. This ever-increasing figure has attracted adopters seeking to advance their investments, often leaving purely technical aspects on the sidelines. As is the case with any innovative technology, misconceptions are plentiful and information is not always conclusive. The research effort presented in this paper consists of a quantitative study seeking to address the subject of user anonymity in the Bitcoin network by employing an online survey on one of the most prominent Bitcoin forums. This includes 50 eligible participants, whose motivation is derived through the application of *temporal motivation theory*. The survey seeks to form an understanding of user attitudes towards the aspect of anonymity by following a methodological approach for exploring common tendencies among the representatives and will serve as the underlying data set from which conclusions can be drawn. Furthermore, this paper will present a literary study of the actual state of anonymity in this peer-to-peer technology by reviewing current findings highlighted in the area, thus presenting a comprehensive view of anonymity in the Bitcoin network, which will contrast the user study.

Keywords: Bitcoin, cryptographic currency, pseudo-anonymity, peer-to-peer

Contents

1 Introduction

Bitcoin is a decentralized cryptographic currency proposed in a 2008 white paper authored by Satoshi Nakamoto, a likely pseudonym (Nakamoto, 2008). Bitcoin builds on public-key cryptography, allowing individuals to engage in peer-to-peer transactions over the Internet by referencing the address of the receiver. This address consists of a sequence of alphanumeric characters and is known as a Bitcoin address. This means that Bitcoin does not take into account any information pertaining to someone's actual identity, effectively allowing parties to become pseudo-anonymous in the Bitcoin network. However, it may still be possible to derive ownership of a Bitcoin address. Research suggests that by analyzing real-time transaction relay traffic, researchers were able to associate Bitcoin addresses with IP addresses, likely owned by the same individual (Koshy, et al., 2014). Past studies have also discussed the implications of cluster analysis on the Bitcoin block chain. Using appropriate network representation, researchers were able to associate several Bitcoin addresses with each other, and by conducting a passive analysis on external information, were able to resolve IP addresses belonging to the same user (Reid & Harrigan, 2012).

Despite there being several methods for reducing user anonymity in the Bitcoin network, researchers have considered practices that allow users to maintain their anonymity. A common solution for upholding anonymity is to only use a Bitcoin address once, which means that the user generates a new Bitcoin address each time they receive a payment, as is outlined in the original white paper (Nakamoto, 2008). Another practice is to employ the use of mixing services, a procedure that reduces traceability, hence obscuring the relation between the input and output values in a transaction (Herrera-Joancomartí, 2015). This does however require the user to place trust in a third party, as the funds have to be funneled through an external holder. It is worth mentioning that the third party is still capable of producing the relation between the source and the destination.

Considering the solutions that allow a user to remain anonymous, how many are actually motivated to uphold their anonymity in the Bitcoin network? This study seeks to understand user behavior in Bitcoin, focusing on the aspect of anonymity. The paper is structured as follows: Section 2 provides a basic understanding as to what Bitcoin is. Section 3 outlines related work. Section 4 presents the problem formulation. Section 5 describes the motivation behind this study. Section 6 highlights the research objectives. Section 7 establishes the limitations of this research effort. Section 8 introduces the methodology. Section 9 discusses expected results. Section 10 outlines thoughts concerning validity. Section 11 presents the findings of the study. Section 12 discusses the results. Section 13 outlines future work. Section 14 discusses ethical aspects of the study. Section 15 outlines the potential value of this study. Section 16 provides a discussion in regards to system and network administration. Section 17 draws parallels to related work. Section 18 concludes this research effort.

2 Background

Bitcoin is a cryptographic currency, released as open-source software, meaning that anyone can review the source code. It is decentralized by design, meaning that individuals are able to directly engage in transactions over the Internet, without the involvement of a third-party. Within the confines of the Bitcoin network, both the sender and the receiver are anonymous, allowing their identities to remain unknown to the rest of the network, with the only identifying attribute being a Bitcoin address, which is employed by the receiver. This address consists of a sequence of alphanumeric characters and represents the destination of a transaction.

2.1 Bitcoin Addresses

A Bitcoin address is a single-use token and is not intended to be used more than once, as is described in the original white paper (Nakamoto, 2008). A user can generate a unique address for each transaction, allowing for increased privacy by breaking the flow of information. It is important to note that Bitcoin addresses are used to receive funds, but not to send them: The concept of a "sender address" does not exist within Bitcoin. This is possible because every new transaction is referencing payments from previous transactions. In essence, you are implying ownership of past transactions, which are then used to fund any new transactions, discarding the "sender address" from the equation.

2.2 Block chain

Every Bitcoin transaction is recorded in a public ledger, which is shared by all the nodes in the Bitcoin network. This ledger is known as a block chain because transaction data is stored in units called blocks. Each block contains a hash of the previous block, forming a chain of blocks that span all the way back to the genesis block. This allows the block chain to become immutable, as data cannot be altered retroactively. The Bitcoin block chain can be downloaded and viewed by anyone and at the time of writing contains 124GB of transaction data, going back to early 2009 when the first ever Bitcoin transaction was conducted.

2.3 The Bitcoin Network

The Bitcoin system propagates various kinds of information, more precisely: individual transactions and blocks. This data is distributed over the Internet using a distributed peer-to-peer network. This network is constructed in a dynamic way, meaning that each peer is a computer running the software of a Bitcoin network node, which is included by default in full-client wallets, but is not usually incorporated in light wallet versions, most commonly used in mobile devices. This is an important distinction, as network analysis could ignore such nodes since they would not be identified by the scanning techniques imposed on the full-client nodes in the network (Herrera-Joancomartí, 2015).

2.4 Bitcoin Anonymity

Bitcoin achieves anonymity due to users being able to generate any number of Bitcoin addresses, which they then reference in a transaction. Although a fair starting point for achieving anonymity, transactions still leverage the Internet as a carrier of information, which does not incorporate anonymity in its infrastructure. This, coupled with the exposure of the blockchain poses a threat to Bitcoin anonymity since network traffic can be analyzed, as well as cross-referenced to the public ledger.

3 Related Work

Prior research has focused on associating Bitcoin addresses directly to IP addresses in an attempt to de-anonymize users in the Bitcoin network. The researchers propose a novel approach for creating and evaluating such mappings solely using real-time transaction traffic collected over a period of five months. By leveraging anomalous relaying behavior, the researchers were able to accumulate nearly 1,000 Bitcoin addresses which could be mapped to their likely owner (Koshy, et al., 2014). In their research, the researchers construct a custom Bitcoin client which they name "CoinSeer". Using this client, the researchers were able to establish connections to all listening peers in the Bitcoin network, actively collecting data that was being relayed over the network. The collected data was then prepared for offline processing. By applying an algorithmic approach, the researchers were able to derive between 252 and 1,162 Bitcoin address to IP address pairings from the data set.

A similar research effort suggests that it is not only possible to reveal public IP addresses, meaning addresses that have been mapped using NAT (Network Address Translation), but to also reveal internal addresses behind this address space. This is an important finding, since a vast majority of client nodes are located behind address translation, where they allow 8 outgoing connections to a server node, which are Bitcoin nodes that hold a public IP address. The researchers propose a method for uniquely identifying Bitcoin user by targeting the nodes that they connect to, also known as entry nodes. By pairing connections to entry nodes, the researchers were able to reveal IP address information of clients located behind address translation with an accuracy of $11 - 60\%$, pairing an otherwise anonymous Bitcoin address with an internal IP address (Biryukow, et al., 2014).

Other relevant research has focused on user experience concerning integral aspects of the Bitcoin ecosystem in terms of security, privacy, and anonymity. Here the researchers survey 990 Bitcoin users in order to determine how users confront the challenges proposed not only by Bitcoin, but also by other users, as there are many common misconceptions surrounding the subject (Krombholz, et al., 2017). By employing an online survey, the researchers were able to capture self-reported Bitcoin management behavior and risk perception, and together with qualitative interviews develop a deeper understanding concerning key usability issues of Bitcoin. The research highlighted major challenges reported by the users, which primarily stem from insufficient security measures and a lack of backups. The researchers found that 22,5% of participants had already experienced security breaches that resulted in the loss of funds, half of which were self-induced, highlighting the difficulties of managing their assets in a secure and reliable manner.

4 Problem

By considering prior research, this study seeks to explore how users of Bitcoin view anonymity. In order to derive any conclusions from the participants, it is essential to explore the user's mindset pertaining to the aspect of anonymity, which requires an understanding of their perceived value. It is false to assume that users by default value anonymity as an axiom regarding the strengths of Bitcoin, since it is possible for a user to disregard both the value of anonymity and reflect that mindset in practice. Consequently, one would expect users who value their anonymity to also expend more effort into maintaining it. This research seeks to understand if users who value their anonymity in the Bitcoin network possess the competence to maintain it, but also if users who disregard the aspect anonymity do so by their own volition and not as a result of incompetence.

4.1 Research Questions

The proposed research includes several research questions that seek to explore anonymity in the Bitcoin network, focusing on the user perspective. By placing the user in the spotlight, this research is able to assess whether or not the end user is mindful of their anonymity, as well as exploring any common tendencies among users who compare similarly in terms of age and frequency of use. Therefore, the following research questions were developed:

1. *To what extent do users value their anonymity in the Bitcoin network?*
2. *How much effort are users willing to extend into maintaining their anonymity?*
3. *Do users possess the competence required to maintain their anonymity?*
4. *Does frequency of use affect the user's mindset concerning anonymity?*

4.2 Hypotheses

The hypotheses assumed for this study are derived from observing prior research efforts, which indicates that theory is ahead of practice, as described in an influential large-scale study of Bitcoin users (Krombholz, et al., 2017).

1. *A majority of users value their anonymity in the Bitcoin network.*
2. *The aspect of anonymity is more of a concern when sending Bitcoins, compared to receiving Bitcoins.*
3. *Users put significant effort into assuring their anonymity when sending Bitcoins.*
4. *Users do not possess the competence required to maintain their anonymity.*

5 Motivation

Bitcoin has seen widespread adoption among individuals, small businesses, as well as large retailers. Bitcoin is a technology that provides an even playing ground; essentially making everyone an end user, with the only differences being external to the technology. As with any technology of money, it is vital to obscure one's identity, reducing the likelihood for being the victim of a targeted attack. Using Bitcoin, individuals and businesses alike seek to transact with each other over a common medium that ensures that everyone involved is in fact following the same rule set. This ensures the validity of any-and-all transactions, but it does not ensure much else. This is the case with anonymity in the Bitcoin network, despite it being regarded as a given benefit of the technology. It is true that Bitcoin does allow for an end user to become anonymous, at least to a great extent, but this is not something that is guaranteed by the technology itself. It is up to each end user to make decisions concerning their state of anonymity, which does require self-study and varying degrees of effort. Since not all users are computer scientists, or security experts for that matter, one can come to expect varying degrees of self-study and effort to be extended. At the same time, there are also users who do not concern themselves with the aspect of anonymity, at all. This research effort seeks to form an understanding concerning the general mindset of anonymity in the Bitcoin network, which in turn can allow developers of both client-side software and web-based applications to build their services with a greater understanding of their clientele. Additionally, this research can prove useful in purely educational purposes, as blockchain technologies become more widespread and find their way to individuals who are not technology enthusiasts.

6 Objectives

This research effort outlines several objectives in chronological order. These objectives serve to produce relevant background literature, quantifiable research data, and validated conclusions.

1. *Perform a literary study concerning the current state of anonymity in the Bitcoin network.*
2. *Formulate relevant research questions that include a null-hypothesis, but at the same time also allow for distinctive claims to be made.*
3. *Implement a methodology for achieving meaningful results.*
4. *Adopt a framework for dealing with threats concerning validity.*
5. *Construct an end user survey in order to form an understanding of Bitcoin users and their mindset concerning anonymity in the Bitcoin network.*
6. *Launch the web-survey and promote its existence to relevant forums.*
7. *Outline the quantitative data for structural analysis of its underlying characteristics.*
8. *Formulate statistically validated conclusions from the research data.*

7 Delimitation

Bitcoin is a broad subject that encompasses multiple fields of expertise, which is why this research effort exclusively targets individuals who are already familiar with the technology. It is not necessary for the participant to understand Bitcoin, however, there is a precondition to have performed a transaction in the Bitcoin network, whether it be transferring funds, receiving funds, or both. This research effort builds upon self-reported user data concerning the perceived value of anonymity in the Bitcoin network. It does mention aspects other than anonymity, but the primary interest lies in understanding how the end user views anonymity, measuring factors such as: competence, perceived value, extended effort, and frequency of use.

8 Method

The proposed user survey is to be constructed using *temporal motivation theory*, which integrates four central components in order to address an individual's aspiration for a particular outcome. The theory was adopted since it can be used to evaluate an individual's competence, perceived value, time sensitivity, and perhaps most importantly, the cost associated with the activity, which is measured in time before realization. Other theories, such as *expectancy theory*, which is a component of *temporal motivation theory*, does not incorporate time sensitivity in this evaluation, which causes difficulties in assessing the relationship between sensitivity to time as a valuable resource and time as a cost concerning a specific activity. The chosen theory builds upon prior theories in order to incorporate four relevant components that are to be used in conjunction with this study. In its most simple form, the theory states that an individual's motivation can be derived using the formula:

$$motivation = \frac{expectancy \times value}{1 + impulsiveness \times delay}$$

where *expectancy* is the probability of success, *value* being the reward associated with the outcome, *impulsiveness* being the individual's sensitivity to delay, and *delay* being the time to realization (Steel & König, 2006).

The theory is to be employed in the construction of the end user survey, which requires the discovery of relevant activities, in which the end user chooses to engage in. This research effort outlines two specific activities relevant to the use of Bitcoin concerning the aspect of anonymity, namely the activity of *sending Bitcoins*, as well as the activity of *receiving Bitcoins*. These activities make up the sum total of actions that an end user is allowed to perform as a client node in the Bitcoin network. Of course, this is a simplification of the actual state of the technology, as transactions can become rather complex, including multiple signatures, time constraints, and even programmable features in the form scripts. Although, from the aspect of anonymity, these factors do not amount much relevance, as transactions are bound by the same core rule set, regardless of their complexity. Following the implementation of the theory, it is essential that all four components are present in each of the two activities. It is also crucial that the proposed measurements adhere to a comparable scale. The scale itself may be arbitrarily chosen, often to satisfy a purpose external to the main theory, but it is essential that all components utilize the same proposed measurement for an appropriate comparison.

A scale ranging from 1 – 10 was chosen as the quantifier, where 1 represents a low assessment and 10 represents a high assessment. This range of positive integers was chosen primarily for capturing a broad range of evaluations among the participants, but also for avoiding intermediate values, which forces the participant to take a stand on each question.

8.1 Introduction

In order for the survey to yield accurate results, several complementary sections have to be added, allowing for an increase in quality; the primary addition being the exclusion of web-based wallet solutions. The reason for this being the possibility for a lack of understanding concerning this specific user study, as web-based wallet solutions tend to shift the aspect of anonymity from the end user to the service provider. Because this study seeks participants who face this challenge head on, it is imperative that the participants understand how the technology functions outside the parameters of an external service provider. This issue is to be addressed through the addition of an introductory section, which defines the context of the survey, but also outlines the understanding of Bitcoin client software as a prerequisite.

8.2 Demographics

Following the introduction, the survey will also implement a section concerning user demographics. Within this section, participants will be able to provide information pertaining to their gender and age, but also report on their frequency of use. While not a directly contributing factor to the research effort, this data provides a greater understanding of the individuals who participate. Besides the informational value, the frequency of use section also serves to eliminate participants who report to never have used a software client.

8.3 General Mindset

An important consideration when dealing with specific activities is the mindset of a user barring any constraints. For the purpose of comparative measurements, the survey will implement a section that seeks to encapsulate the participant's perspective concerning Bitcoin anonymity in its general sense. Once again, *temporal motivation theory* is employed in order to construct questions pertaining to the aim of maintaining one's anonymity, or the lack thereof. It is not assumed that participants seek to maintain their anonymity, which is why such implementations are necessary, as it allows for the disclosure of potential discrepancies between a participant's general mindset and their mindset concerning a particular action.

8.4 Closing Questions

As a final addition to the end user survey, a section is to be implemented that allows participants to provide their public key. This public key serves two purposes in the context of this survey. One, the participants are eligible to claim a small reward in the form of Bitcoins, which incentivizes participation. Two, the participants provide evidence that suggests their use of the technology, which adds to the validity of the study.

Considering the nature of this survey, participants should be able to submit their public key whilst also upholding their anonymity, which is why the survey is to implement encryption. The encryption method chosen for this purpose is *Pretty Good Privacy*, or more precisely OpenPGP, which is to implement a dual RSA (Ron Rivest, Adi Shamir, Leonard Adleman) format. This structure consists of a primary key of 4096bits, as well as a sub-key of the same length, allowing participants to encrypt their Bitcoin public key during transit. The submitted keys are then to be stored and decrypted locally, where they are to serve their stated purpose, before being destroyed.

9 Expected Results

It is expected that the survey results should suffice to answer the previously outlined research questions, using quantitative metrics to distinguish between correlation and contradiction. Additionally, the application of *temporal motivation theory* is expected to assist in the discovery of potential discrepancies concerning perceived value and pursued action. Another interesting factor is that of demographics, meaning differences in attitudes towards anonymity pertaining to certain age groups or gender. It would come as no surprise that variation exists between demographics, but exploring the degree of variation, as well as shared tendencies between classifications could prove interesting, as the methodology allows for these comparisons to be made.

10 Validity Threats

The aspect of validity is managed by adopting the works of Wohlin (Wohlin, et al., 1999), where the authors define a framework for recognizing validity threats. This framework consists of four primary categories, namely *internal validity*, *external validity*, *conclusion validity*, and *construct validity*. The purpose of this implementation is to avoid threats that could invalidate this research effort. Alternatively, managing threats that cannot be avoided, reducing their impact on the study.

10.1 Internal Validity

Threats to internal validity stem from influences affecting the independent variable; meaning that treatment and outcome have a causal relationship. Internal validity includes three subcomponents, namely *single group threats*, *multiple group threats*, and *social threats*. The only relevant out of the three being *single group threats*, as the proposed research effort includes a single group of participants, meaning there is no alternative outcome. It is therefore possible that other forums would produce different results than the one chosen for this research effort.

Another relevant component to consider is *history*; meaning the passage of time. It is important to recognize that alterations to the treatment can manifest different results, as circumstances were not identical to the extent that was necessary. A more concrete example would be to alter the contents of the user survey during its deployment, which could be something as miniscule as different ordering of items. Therefore, it is imperative that the survey remains unaltered throughout its course.

It is also possible for *maturation* to affect the results of this research effort, as subjects undergoing the treatment can react differently as time proceeds. This may include factors such as the subject's state of mind during the survey. This is a factor to be recognized and managed, as it is impossible to control. By removing any time restrictions, participants are allowed to undergo the treatment on their terms, meaning that participants are allowed to take the survey during any time of day, as well as being able to take as much time as they deem necessary before submitting. This allows for a reduction in negative outcomes associated with stress and boredom, as the participants are allowed to pause the survey and continue at another time, before finally submitting their results.
A final consideration of internal validity threats is that of *selection*. In the case of an online survey, volunteers may skew the results, as the individuals undergoing the treatment may fail to represent any larger group. It is possible that volunteers may possess traits that make them more motivated to partake in the survey compared to a larger body, which may force a biased outcome. This factor is somewhat diminished as there is a reward associated with the survey, but the threat remains as a whole.

10.2 External Validity

Threats to external validity stem from conditions that inhibit generalization of results. This includes three types of interactions with the treatment, namely people, place, and time. First and foremost, there is *interaction of selection and treatment*, which is a component of external validity. This is the effect of including subjects that are not representative of the population that the research seeks to study. This is a possible threat to the proposed research, as the treatment is made available for anyone that can access the hyperlink. Although the survey is to be exclusively publicized to a forum for users of the technology, it could still be the case that participants outside this target group gain access to the survey. This threat cannot be avoided, as it would limit participation, perhaps to the degree that no conclusions could be drawn. Instead, the survey implements three components for dealing with the issue. One, the participant is always greeted with an introductory section concerning the nature of the survey. Two, the participant has to report on their use of the technology; meaning their frequency of use. A submission indicating no use of the technology would be discarded. Three, participants are incentivized to submit their Bitcoin public key, which confirms their use of the technology. Although they may never have sent or received any funds, it still proves that the participant understands what a public key is in the context of Bitcoin. Note that simply including a proper public key is not enough. The participant still has to report a use of the technology in order to not be discarded. There is also *interaction of setting and treatment*; meaning that the treatment lives up to the expectations of the participant. Since this research effort seeks to understand how the end user perceives anonymity, it would be expected that the treatment allows for means to remain anonymous. This is managed by allowing the participant to encrypt their public key, although they still have to place trust in the research effort.

10.3 Conclusion Validity

This component incorporates threats concerning the difficulty to outline a valid conclusion of the relationship between treatment and outcome. This includes *low statistical power*, which stems from the inability to reveal a true pattern in the data set. A low statistical power suggests a high risk for erroneous conclusions, especially in small sample sizes. This can be managed to a certain degree if the sample size is large enough to filter out any misrepresentations. Although, it is still possible to misinterpret the data in analysis, outlining the importance of rejecting the null hypothesis, as statistical power is a general function of distribution across a data set. Another relevant component is *fishing and error rate*. There are two factors to look out for when dealing with this issue. Primarily, there is *fishing*, which is to actively pursue a specific outcome, undermining the validity of the research effort. This can be avoided by adopting a methodology that accurately evaluates the participant, leaving no response open for subjective interpretation. The second factor has to do with *error rate* concerning the distribution in a data set. This can be managed by conducting multiple analysis on a data set in order to avoid invalid conclusions further on.

A final component worthy of mention is *reliability of measures*. The validity of a data set is highly dependent on measures being reliable in the context of the research effort. Factors such as poor wording and improper instrumentation can cause artifacts in a data set, which could lead to improper conclusions. This threat can be managed with the implementation of a proper methodology, bringing structure and coherence to a treatment, thus reducing the likelihood of unreliable measures.

10.4 Construct Validity

The fourth category deals with generalization of the outcome, or more specifically preparation of the treatment. If a treatment is designed in a way that allows for multiple interpretations, it could be difficult or impossible to derive any valid conclusion, seeing as there is an inconsistency between that which is studied and that which is measured. This category includes several components, of which three are of relevance to this study. The first component is named *inadequate preoperational explication of constructs*, which implies that constructs related to the research effort have not been sufficiently defined. It is imperative that measurements coincide with the theory, which is why this research effort builds on a validated methodology for measuring motivation. The second component is *mono-method bias*, which implies that a single treatment could result in measurement bias. This could damage the validity of the outcome, as the measurement does not include any form of comparison. In the context of this study, two comparisons are made, namely comparing the activity of *sending Bitcoins* to the activity of *receiving Bitcoins*, as well as comparing general motivation to that of specific activities. The third component relevant to this study is named *confounding constructs and levels of constructs*, which stems from the difficulty of evaluating binary constructs. This is avoided by employing a quantifiable scale, allowing the participant to more accurately evaluate their aptitude to succeed at a task.

11 Results

In total, 52 participants conducted the end user survey, out of which two people reported to never have used the technology, leaving 50 participants for the analysis. The survey was constructed using Google Forms, which is a web-based tool for collecting information from users via a personalized survey, see appendix A – G. The survey was then publicized on Reddit, a discussion website where members can submit content, such as text posts or direct links. Since Reddit includes countless discussion forums, each very different from the next, a specific subsection, or "subreddit" had to be chosen. The largest subreddit for discussions concerning Bitcoin is named /r/bitcoin, including over 300,000 readers, which is where the survey was finally made available with the help of a few moderators. This forum was chosen since /r/bitcoin is discussion forum for Bitcoin in general, meaning that users come from various backgrounds, unlike other forums that target enthusiasts or experts, leaving out users who are just becoming familiar with the technology.

The results of this survey are divided into five sections, each dealing with a specific component of the survey. The resulting metric of *temporal motivation theory* is compared in connection with two distinct categories, namely age and frequency of use. Both categories are not all that relevant, considering the distribution of participants, which results in generalization becoming rather difficult. Although there were some challenges, the results are outlined for both categories.

11.1 Section One

In the first section of the end user survey, participants were given the option to report on their background. The section included three questions, out of which two were optional. The first question asked the participant to provide their gender. This question was implemented in order to understand gender distribution across the data set. Out of the 50 qualified participants, 46 (92%) reported to be male, 2 (4%) reported to be female, and 2 (4%) chose not to answer. The original thought behind this implementation was to compare motivational factors between the sexes, unfortunately this cannot be done, since the only represented group are males, making it impossible to conduct a valid comparison.

The second question asked the participants to report on their age. Here, 47 (94%) participants chose to disclose this information, while another 3 (6%) chose not to answer. The participants who chose to answer are distributed across five age categories. Four participants (8%) reported to be between the ages of 15 – 19, another 24 (48%) reported to be between the ages of 20 – 29, 14 participants (28%) reported to be between the ages of 30 – 39, followed by 3 participants (6%) reporting to be between the ages of 40 – 49, and finally, there were 2 participants (4%) between the ages of 60 - 69. Note that no participants reported to be between the ages 50 – 59, which is why this age category is excluded from the following figures. A full summary of the age categories represented in this study can be seen in the figure below.

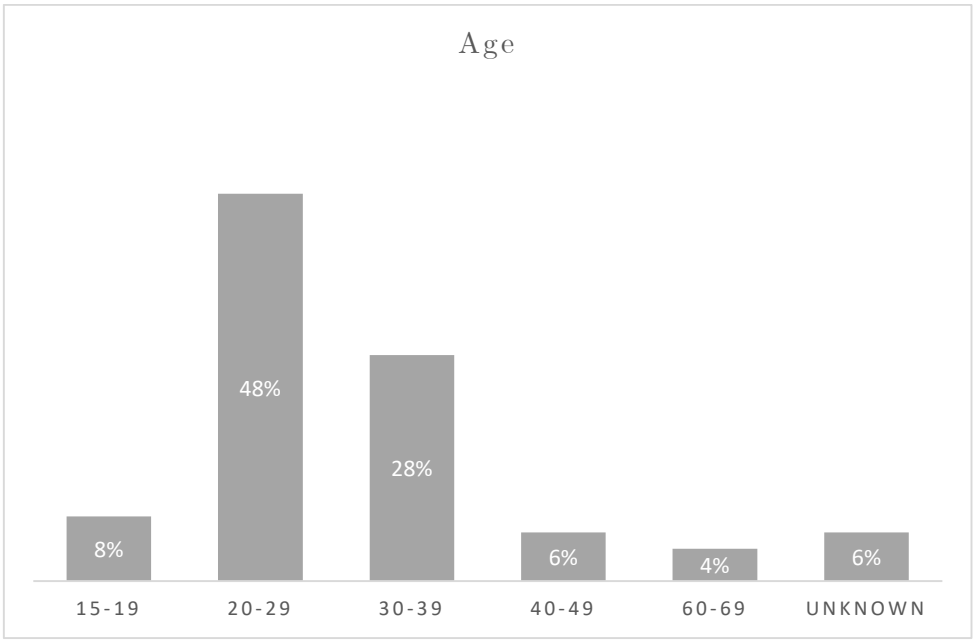

Figure 1 – Age distribution

The third and final question of this section allowed the participants to report on their frequency of use, meaning how often they make use of the technology, if at all. Unlike the previous questions of this section, this question could not be left unanswered for reasons discussed in the validity chapter. Out of the 50 participants, 11 (22%) report to conduct one or more Bitcoin transactions every day, another 19 (38%) conduct one or more transactions on a weekly basis, while 17 (34%) conduct one or more transactions each month, leaving 3 (6%) of participants conducting one or more transactions on an annual basis. A more comprehensible representation can be found in the figure below.

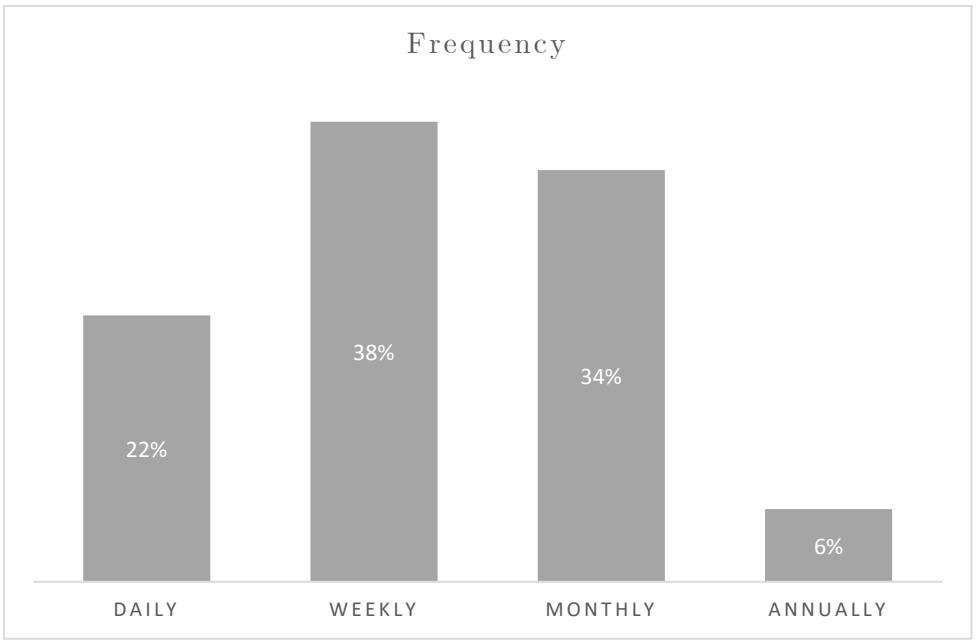

Figure 2 – Frequency distribution

11.2 Section Two

This section presents the first metric for evaluating motivation. It features four distinct questions, each representing a component in *temporal motivation theory*. As mentioned earlier, each of the four questions follow a quantitative scale of 1 – 10, where 1 represents a low assessment and 10 represents a high assessment. This section seeks to understand the general mindset of each participant in contrast to particular activities.

1. *How competent are you in maintaining your anonymity in the Bitcoin network?*
2. *How much do you value your anonymity in the Bitcoin network?*
3. *How much effort do you put into maintaining your anonymity in the Bitcoin network?*
4. *How often do you research new methods for maintain your anonymity in the Bitcoin network?*

These questions translate into *Expectancy*, *Value*, *Impulsiveness*, and *Delay* following the order in which they are listed. Questions 1 and 2 translate directly into a useable metric, but questions 3 and 4 have to undergo additional treatment. Since *Impulsiveness* and *Delay* are both denominators, it would not make sense having a positive assessment cause a negative impact on motivation. These components have to be reversed in order for motivation to hold any meaning. The metrics are reversed using the following equation, substituting the subtrahend for *Impulsiveness* and *Delay*, independently. Using this equation, one would substitute x for the value of *Impulsiveness* and *Delay* for a particular user, which would result in y becoming the reversed assessment. Note that this is done for both components separately. Applying the equation on only one of the two components would not be sufficient.

$$y = 10 - x$$

This can result in *Impulsiveness* and *Delay* now becoming zero values, which is why 1 is added to the denominator of the main equation proposed by *temporal motivation theory*. This solves the division by zero problem, but there is yet another issue with the equation. It is still possible for *temporal motivation theory* to yield values below 1. Since any assessment below 1 is still considered low, there is little meaning in preserving values below this threshold. A ceiling function is used to produce a minimum value of 1, as can be seen in the equation below. Here, the variable x is substituted with an individual's assessments of motivation. Note that this equation is only employed for participants reporting a motivation below 1.

$$Ceiling(x) = \lceil 1 \rceil$$

This results in a proper assessment of motivation, where the minimum value is 1 and the maximum value is 100, although distribution is not linear. The following list illustrates the treatment of the results:

1. Users provide an assessment of *Expectancy*, *Value*, *Impulsiveness*, and *Delay*.
2. The components *Impulsiveness* and *Delay* are reversed as described previously.
3. Motivation is then derived using *temporal motivation theory* with the survey data.
4. If the resulting motivation falls below 1, it is rounded to 1 as the nearest integer.
5. The final assessment of motivation places the individual somewhere between 1 – 100.

The individuals are then categorized by age and frequency of use, where the motivation of all participants is summed and divided by the number of participants in the category. The same method is applied to the remaining categories, where the resulting value is the average among all participants in the specific category and is defined as *Motivation* in figures 3 – 8. The horizontal line spanning the graphical element is the average motivation of all participants in the specific figure. Here, the sum total of assessments is summed and divided by the number of participants in the study and is defined as *Average* in figures 3 – 8. Note that both values represent motivation, where *Motivation* is the average motivation for participants in a specific category and *Average* is the average motivation for all participants.

The first category of participants aged 15 – 19 held a motivation of 3,81, the second category aged 20 – 29 held a motivation of 12,39, the third category aged 30 – 39 held a motivation of 8,79, followed by those aged 40 – 49 that held a motivation of 2,00, and lastly, the category aged 60 – 69 held a motivation of 43,15. These figures do not adhere to a linear scale, meaning that direct comparisons are challenging. Instead, what is interesting is the differences and similarities between age groups. The figure below illustrates the average motivation for each age category, as well as the general average for all participants, which is 10,94. Note that the figure follows a logarithmic scale.

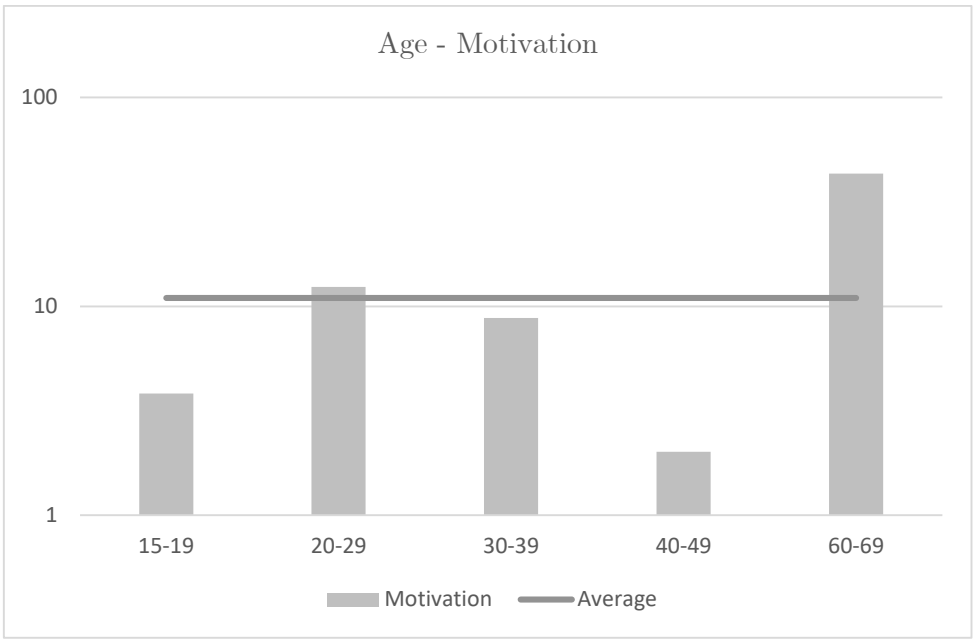

Figure 3 – Motivation across age categories

To start off with, it is clear that the age category of 60 – 69 causes difficulties for comparisons of age categories, as well as the average of all participants and the reason is two folded. First, the category consists of two participants, both reporting an exceedingly high evaluation of motivation, which is evident by the illustration. Second, these participants provided a high assessment of *Value*, meaning that anonymity is of great importance to these two participants. This is also supported by their assessments of both *Impulsiveness* and *Delay*, meaning that the participants are willing to extend a great deal of effort in order to maintain that status.

The age categories 15 – 19, 20 – 29, 30 – 39, and 40 – 49 show an interesting trend, where motivation is low among participants aged 15 – 19, then dramatically increases for participants aged 20 – 29, as well as those aged 30 – 39, showing similarities in both categories. This is also evident in their mindset, as these two categories reported high assessments of both *Expectancy* and *Value*, but not in *Impulsiveness* and *Delay*, meaning that the participants value their anonymity, but not to the degree where they are willing extend significant effort. The age category 40 – 49 does not share this evaluation, and is more similar to the age category of 15 – 19, both being somewhat equally represented.

Another factor to consider is frequency of use, meaning how often a participant engages in a Bitcoin transaction. The four categories outlined are: daily, weekly, monthly, and annually. Participants conducting transactions on a daily, weekly, and monthly basis show distinct similarities concerning their motivation to maintain their anonymity. The first category of participants (daily transactions) held a motivation of 9,28, the second category of participants (weekly transactions) held a motivation of 11,45, the third category (monthly transactions) held a motivation of 14,09, and lastly, the fourth category (annual transactions) held a motivation of 2,72. An interesting trend can be seen among the first three categories, where participants share similarities in regards to motivation, which is also supported in their assessment of the four components in *temporal motivation theory*. This is however not the case for participants conducting transactions on an annual basis. These participants report high assessments in *Expectancy* and *Value*, but are very much against the idea of extending any significant effort in order to maintain their anonymity in the Bitcoin network.

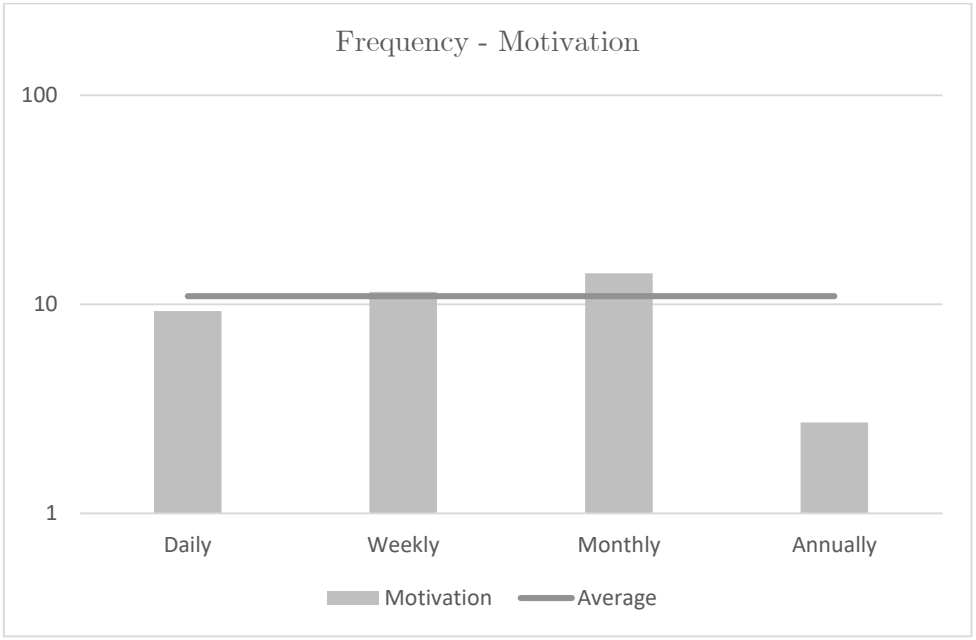

Figure 4 – Motivation across frequency categories

11.3 Section Three

This section presents the second metric for evaluating motivation, more specifically, motivation concerning the activity of *sending Bitcoins*. Just like the first section, this section implements the four components of *temporal motivation theory*, as it seeks to understand the mindset of a participant when presented with a specific activity.

1. *How competent are you in maintaining your anonymity when sending Bitcoins?*
2. *How much do you value your anonymity when sending Bitcoins?*
3. *How much effort do you put into confirming your maintained anonymity before sending Bitcoins?*
4. *How much do you allow the aspect of anonymity to affect the activity of sending Bitcoins?*

Just as in the previous section, these four questions translate into *Expectancy*, *Value*, *Impulsiveness*, and *Delay* following the order in which they are listed. The resulting evaluation has undergone the same treatment as outlined in section two.

The first category of participants aged 15 – 19 held a motivation of 27,34, the second category aged 20 – 29 held a motivation of 9,92, the third category aged 30 – 39 held a motivation of 7,79, followed by those aged 40 – 49 that held a motivation of 2,51, and lastly, the category aged 60 – 69 held a motivation of 20,84. This is illustrated in figure 5, once again implementing a logarithmic scale.

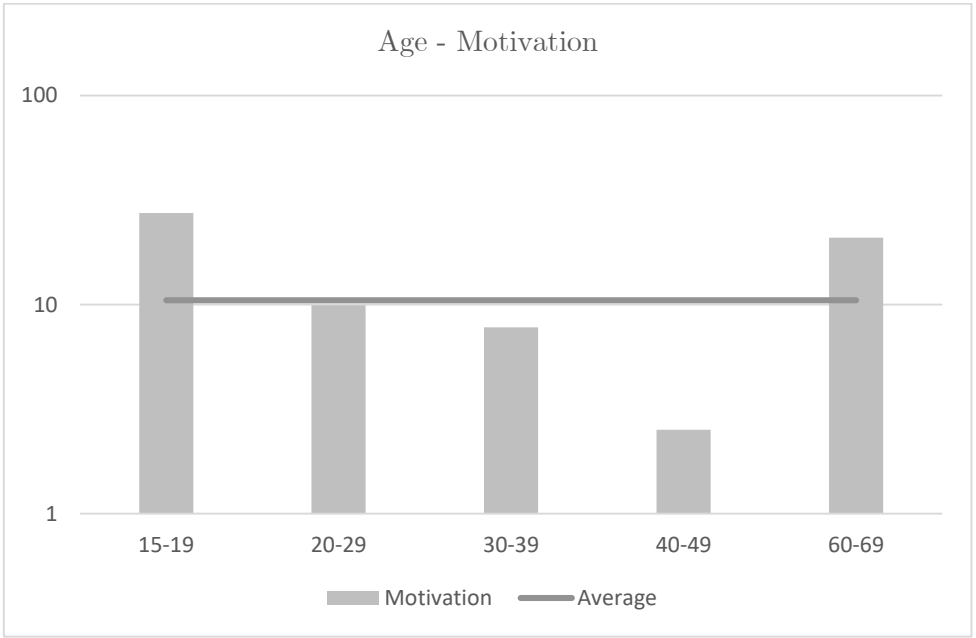

Figure 5 – Motivation across age categories

Here, the categories 20 – 29, 30 – 39, and 40 – 49 fare well in regards to consistency, although categories 15 – 19 and 60 – 69 show noticeable differences. The category 15 – 19 went from 3,81 in the previous section, to now reporting 27,34 in motivation. This may come across like a massive increase, but keep in mind that the scale is not linear, although it is an increase and a quite significant one at that. The category 60 – 69 went from 43,15 in the previous section, to now reporting 20,84 in motivation. Both these categories suffer in validity, seeing as there are only a handful of participants in each of them, making any generalizations rather difficult.

Then there is frequency of use which shows a similar trend as seen in the previous section, where daily, as well as weekly use reaches close to the general average, with monthly use showing a higher evaluation of motivation, and annual use falling off the trend, as was the case in the previous section concerning general mindset.

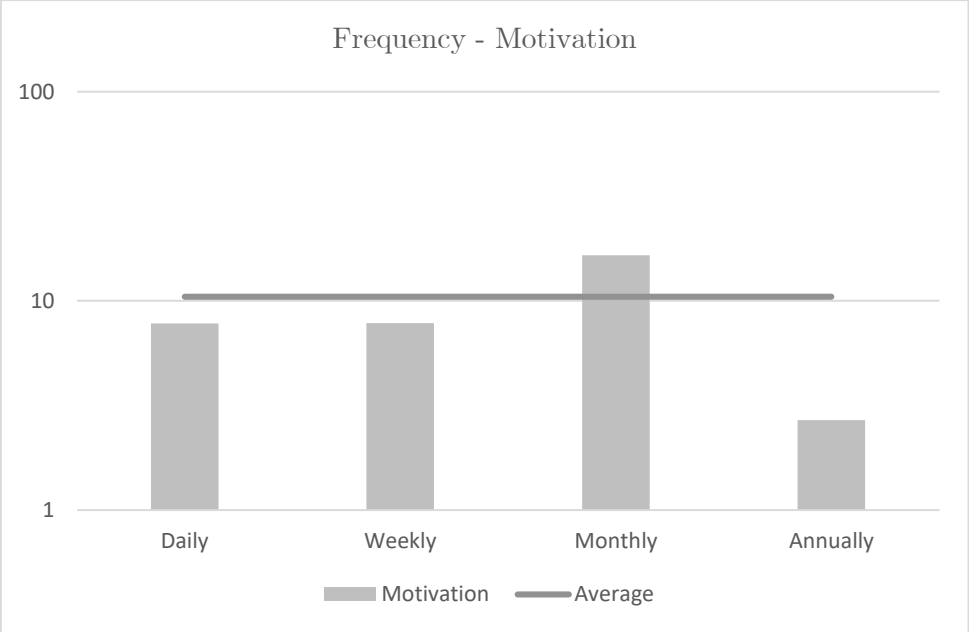

Figure 6 – Motivation across frequency categories

An interesting observation is that users who reported to conduct transactions on an annual basis actual did value their anonymity. The reason for why annual use fell off the trend has to do with *Impulsiveness* and *Delay*, rather than *Expectancy* and *Value*, which actually evaluate higher than the general average.

11.4 Section Four

This section presents the third metric for evaluating motivation, more specifically, motivation concerning the activity of *receiving Bitcoins* and is the final section of the end user survey that deals with *temporal motivation theory*. Just like the previous two sections, this section implements the four components of the theory, as it seeks to understand the mindset of a participant when presented with this specific activity.

1. *How competent are you in maintaining your anonymity when receiving Bitcoins?*
2. *How much do you value your anonymity when receiving Bitcoins?*
3. *How much effort do you put into confirming your maintained anonymity before receiving Bitcoins?*
4. *How much do you allow the aspect of anonymity to affect the activity of receiving Bitcoins?*

Just as in the previous two sections, these four questions translate into *Expectancy*, *Value*, *Impulsiveness*, and *Delay* following the order in which they are listed. The resulting evaluating has undergone the same treatment as outlined in section two.

The first category of participants aged 15 – 19 held a motivation of 35,50, the second category aged 20 – 29 held a motivation of 11,35, the third category aged 30 – 39 held a motivation of 14,13, followed by those aged 40 – 49 that held a motivation of 8,33, and lastly, the category aged 60 – 69 held a motivation of 20,50. This is illustrated in figure 7 where the categories are outlined next to a logarithmic scale.

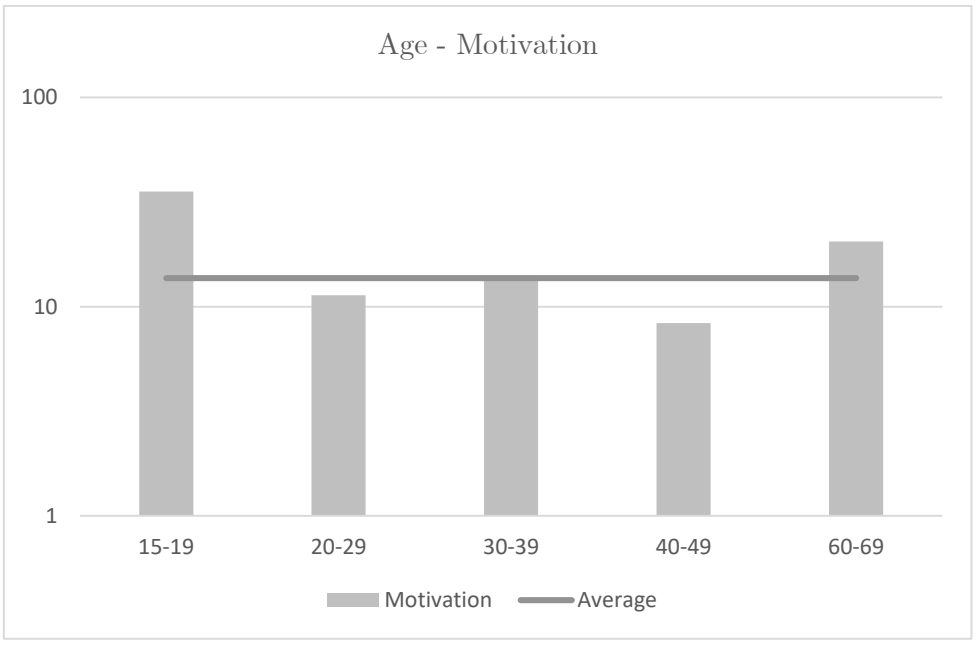

Figure 7 – Motivation across age categories

The results of this section are similar to those presented in section two, showing noticeable increases in motivation compared to section one. The categories 20 – 29 and 30 – 39 hold a consistent evaluation, which in part is due to their large representation of participants. The category of participants aged 15 – 19 show motivation extending well beyond the average, which is due to low representation, causing dramatic shifts in evaluation. Although, *Expectancy* and *Value* compare similarly to the other categories in this data set, *Delay* is what causes the uptick among participants aged 15 – 19, meaning that they allow more time to pass before realization.

When looking at frequency of use, however, there is a slight change compared to section two. Here it seems that weekly and monthly activity have traded places in regards to motivation, although they fare somewhat equally. This is illustrated in figure 8.

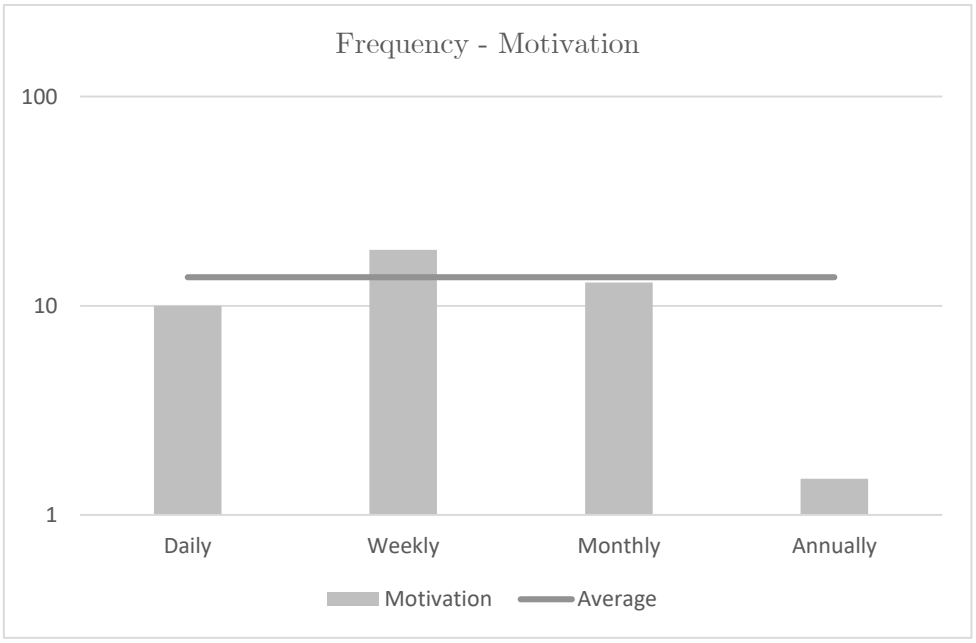

Figure 8 – Motivation across frequency categories

Here, one can observe that participants conducting transactions on a monthly basis fall short of the average, which was not the case in the previous sections. However, one can also notice that participants conducting transactions on a weekly basis exceed the average motivation for the whole data set, which is due to high assessments in *Expectancy* and in *Value*. Once more, the participants conducting transactions on an annual basis fall short of the average, which is caused by low assessments in both *Impulsiveness* and *Delay*.

11.5 Section Five

In the final section of the end user survey, participants were asked to answer the following question:

1. *How often do you review and/or improve your methodology for maintaining your anonymity in the Bitcoin network?*

Out of 50 qualified participants, 2 (4%) reported to be reviewing and improving their methodology for maintaining their anonymity on a daily basis, 3 (6%) reported to do this on a weekly basis, 18 (36%) reported to do this on a monthly basis, another 16 (32%) reported to do this on an annual basis, and lastly, 11 (22%) of the participants reported that they never review or change their methodology.

Additionally, participants were able to claim a small reward for participating in the survey, which meant that they had to submit a valid Bitcoin address. Out of the 50 qualified participants, 33 (66%) chose to include a Bitcoin address, with all addresses being valid. Out of those 33 submissions, 2 (6%) submitted their Bitcoin address in an encrypted format.

12 Discussion

The purpose of this end user study was to reveal differences, as well as similarities among participants. The participants were divided into categories based on age and frequency of use, given as these factors are what most definitively differentiate individuals involved in Bitcoin. This turned out to be rather difficult, as the data set heavily clusters between the ages 20 – 29 and 30 – 39, making up 76% of participants. However, frequency of use shows a more even distribution, which suggests that this category may be a better indicator for motivation.

When it comes to age, one can notice that the categories 15 – 19, 40 – 49 and 60 – 69 include a noticeable degree of variance across the three measurements, which can be explained by the low representation among these categories, making up only 18% of participants. Therefore, making generalizations impossible. However, categories 20 – 29 and 30 – 39 show more or less consistent evaluations of motivation across all three measurements, with participants aged 20 – 29 holding the highest evaluation out of the two. Participants aged 20 – 29 average a motivation of 11,20, while participants aged 30 – 39 average 10,23 across the three measurements, which hardly constitutes a difference, given the non-linear scale. In conclusion, it can be stated that age has minimal impact on motivation, at least for participants aged 20 – 29 and 30 – 39, which comprises a difference of 19 years in age. However, when looking at all categories, differences become noticeable, but this is once again explained by the low representation, as outliers heavily skew the results.

As for frequency of use, one can notice a consistent trend across all three measurements, with slight variations in weekly and monthly activity. These categories are somewhat evenly distributed, with the only exception being users who transact on an annual basis, making up only 6% of the participants. Participants conducting transactions on a daily basis hold an average motivation of 9,00, which falls below the general average for all participants. Then there are participants who conduct transactions on a weekly and monthly basis, where both categories compare similarly in regards to their general mindset, as well as in the activity of *sending Bitcoins*, holding motivations of 12,59 and 14,50 across the three measurements. However, in the activity of receiving Bitcoins, these two categories trade places, with weekly activity now surpassing the general average, and monthly activity falling below the line. This is due to an increase in both *Impulsiveness* and *Delay* among participants conducting transactions on a monthly basis. As for participants conducting transactions on an annual basis, there is not really much to discuss, because of the low representation. However, it is clear that these participants value their anonymity, which is suggested by both *Expectancy* and *Value*, but once again, *Impulsiveness* and *Delay* decreases the overall motivation for this category, significantly below the general average. However, what is interesting about frequency of use, is the measured consistency among the categories, where motivation peaks at weekly and monthly activity. This suggest that daily users are somewhat less motivation compared to weekly and monthly users, with users transacting on an annual basis being significantly less motivated to maintain their anonymity compared to all other categories.

In summary, it can be argued that frequency of use is a more valuable metric for evaluating motivation, compared to age. Since Bitcoin is a fairly recent implementation, it can be difficult to conduct comparisons using age, given the distinct falloff, as seen in this study. This does not however imply that age is not an interesting factor. It is more the case that age is limited in its application, resulting in statistics having severe limitations. This also concurs with a prior large-scale study, where the median age was 28,67, being right at the edge of the two categories most central to this research effort (Krombholz, et al., 2017).

When it comes to motivation, things become even more difficult. The three sections implemented in the survey show that participants do value their anonymity, which is supported by the average assessment of *Value* being 6,62 across all three sections, showing no discernible difference between *sending Bitcoins* and *receiving Bitcoins*. This is also the case for *Expectancy*, where participants report an average *Expectancy* of 6,52 across all three sections, again, showing no discernible difference between the activities. This means that participants value their maintained anonymity, while also possessing the knowledge required to succeed. However, what participants value along with their anonymity, is their time and effort. This is evident by participants reporting an average *Impulsiveness* of 5,04, and *Delay* of 4,98, which significantly decreases their motivation, according to *temporal motivation theory*. This is somewhat ambiguous, as the results can be interpreted differently. It could be the case that participants leave the aspect of anonymity to Bitcoin, hoping that the technology will ensure their anonymity by default. It could also be the case that the costs outweigh the benefits, meaning that participants simply cannot be bothered to maintain their anonymity. Whatever the case may be, it is beyond this research effort and requires an approach that incorporates this element.

There is also the section concerning improvement, where 36% of participants reported to be reviewing or improving their methodology for upholding anonymity on a weekly basis, and another 32% on a monthly basis. This also coincides with *Expectancy*, as participants report to possess the knowledge necessary to succeed. However, merely 6% of participants encrypted their Bitcoin address before submitting, supporting the notion that the costs outweigh the benefits.

In conclusion, it can be stated that it is not a question of whether or not participants value their maintained anonymity, because the results show that they do. It is more a question of how to strike a balance between costs and benefits, as participants do allow for some leeway when it comes to *Impulsiveness* and *Delay*, but it is not significant.

13 Future Work

There are some ways of improving this research effort. One such way would be to include a larger collection of participants. This would allow for a more comprehensive comparison, as each distribution, whether it be age, frequency, or another metric altogether, would incorporate enough participants to counteract significant deviations from the mean. Another option would be to implement a methodology that more accurately encapsulates the underlying reason for why participants value their anonymity, or more interestingly, to what extent. Although this research effort sought to answer the second question, there is still room for improvement, more precisely when it comes to distribution across a given metric, as the distribution in this research effort clusters heavily in both age and frequency. If one were to discover a determining factor for both high and low evaluations, it would be more apparent why some participants fare well in terms of *Motivation* and *Value*, but also in *Impulsiveness* and *Delay*, resulting in motivation that is significantly above the general average.

14 Ethical Aspects

A consideration to be had when discussing the aspect of ethics is the vulnerability of participants in the survey. Since there was an incentive to submit a Bitcoin address, participants were likely to do so. However, it would be possible to use these Bitcoin addresses for malicious purposes. This research effort is merely concerned with academic purposes, meaning that the addresses have a single purpose, as discussed previously. These addresses were confidential to the study and have not been made available to external actors.

15 Research Value

The results of this research effort are relevant to software developers and security experts engaged in Bitcoin. This study shows that anonymity is an aspect to consider when dealing with transactions in the Bitcoin network, which is supported by the evaluation of the participants. It can be argued that anonymity should be a feature in any trading platform involved in Bitcoin, whether dealing with stock exchanges, e-commerce, or local businesses, ensuring anonymity throughout the chain of transaction. This position could attract users to such platforms, given their high regard for anonymity.

16 Relevance of the Study

From a network and system administration point of view, this study can become quite confusing, as it deals with a technology that is still in its infancy. However, it would not be false to assume that blockchain technologies are to play a significant role in future payment systems, as they benefit the individual in terms of security and anonymity, while also providing a scalable and reliable solution for a business. Many businesses have already adopted Bitcoin, even if through an intermediary service, which increases the need for security experts that understand PKI (Public Key Infrastructure). It would not be far-fetched to think that this responsibility would fall on system administrators, as they are the ones responsible for managing Internet-facing services. Blockchain technologies, such as Bitcoin, would just become another service in the application stack, where the administrator would be responsible for configuring and managing the service. From the system administrator's perspective, this would include management of Bitcoin wallets, where some wallets must be tied to a public transaction service, and others would be stored outside the reach of any potential attackers. Since prior research has revealed that it is possible to link Bitcoin addresses to IP addresses, as disclosed in the work of Koshy, et al., 2014, the network and system administrator would also be responsible for dealing with denial-of-service attacks targeting the transaction server. If the objective of an attacker is to obstruct a service, it would not be any different for a server running a Bitcoin API (Application Program Interface), as the attacker would employ the same techniques for achieving their results as they would when for example targeting a web server.

This study shows that users of Bitcoin value their anonymity, which is something that network and system administrators should be mindful of when deploying any transaction services, as anonymity has to be ensured throughout the chain of transaction, meaning that their configuration should allow for users of Bitcoin to maintain their anonymity. One way of achieving this would be to implement a mixing service, where transaction links are broken by funneling the funds in a way that reduces traceability (Herrera-Joancomartí, 2015).

It is difficult to tell how blockchain technologies, such as Bitcoin, are to unfold in the future, but it is necessary to understand how they would be implemented and maintained, as these technologies are directly tied valuable assets. Although there are many technical challenges to blockchain technologies, this study aims to understand the user perspective. In order to fulfill the expectations of Bitcoin users, one has to understand how users perceive aspects relevant to the technology. Anonymity is one such aspect and should be incorporated in any system dealing with Bitcoin, which is why this research is relevant to network and system administrators, as they are the ones responsible for configuring and maintaining services dealing with users of this kind. There have already been instances where improper implementations caused the loss of funds or enabled attackers to disclose user information, both in private and corporate scenarios, which is why information concerning blockchain technologies has to become more widespread.

17 Previous Research

It is difficult to compare this study to previous publications, given the uniqueness of this research effort. However, there is an interesting parallel to be made, where a large-scale study of Bitcoin users revealed that security is a major challenge to Bitcoin users. The researchers discovered that many participants were not even aware of the security features provide by their wallet-solution, meaning the platform which they transact on (Krombholz, et al., 2017). This goes in stark contrast to what the participants of this study reported, as the average *Expectancy* was quite significant, showing an understanding of potential security measures.

18 Conclusion

This research effort presents an end user survey of 50 Bitcoin users, examining their motivation to uphold their anonymity in the Bitcoin network. By implementing *temporal motivation theory*, this study is able to measure the four components: *Expectancy*, *Value*, *Impulsiveness*, *Delay*, each translating into a behavioral attribute. The results are compared in conjunction with two secondary metrics, more precisely, age and frequency. These metrics serve to highlight differences and similarities among participants by categorizing their age and engagement in the technology. The results show that age is an ineffective metric, since participants heavily cluster between the ages of $20 - 29$ and $30 - 39$, making comparisons a challenge. The second metric, namely frequency, shows a more even distribution of participants, although somewhat deficient when it comes to annual engagement in the technology. The results show that frequency is a more reliable metric for evaluating motivation, which is a consequence of distribution, as the measurements more accurately coincide with each other. The research also reveals that the motivation is evenly balanced between the activities of *sending Bitcoins* and *receiving Bitcoins*, showing no discernible difference. However, it is worth mentioning that the activity of *receiving Bitcoins* is fairly different from *sending Bitcoins*. When it comes to *sending Bitcoins*, attacks on anonymity would originate from externalities, such as personal information tied to a purchase in Bitcoin. When *receiving Bitcoins*, that transaction is stored in the blockchain, together with all other transactions, where cluster analysis could potentially disclose links between sender and receiver.

The results of this research effort show that users do value their maintained anonymity, which is perhaps the most interesting finding of the study. This is supported by the fact that an overwhelming majority of participants report high assessments in both *Expectancy* and *Value*. However, motivation declines as participants constrain their *Impulsiveness* and *Delay*, meaning effort and time. This quantitative study cannot reveal the reason for why users put constraints on these factors, but it does affirm that users recognize the value of anonymity, which suggests that anonymity is an integral part of Bitcoin, at least from an end user perspective.

References

Biryukow, A., Khovratovich, D., & Pustogarov, I. (2014). *Deanonymisation of Clients in Bitcoin P2P Network.* ACM New York, NY, USA. doi:http://dx.doi.org/10.1145/2660267.2660379

Herrera-Joancomartí, J. (2015). *Research and Challenges on Bitcoin Anonymity.* Springer, Cham. doi:http://dx.doi.org/10.1007/978-3-319-17016-9_1

Koshy, P., Koshy, D., & McDaniel, P. (2014). *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic.* Springer, Cham. doi:https://dx.doi.org/10.1007/978-3-662-45472-5_30

Krombholz, K., Judmayer, A., Gusenbauer, M., & Weippl, E. (2017). *The Other Side of the Coin: User Experience with Bitcoin Security and Privacy.* Springer, Berlin, Heidelberg. doi:https://dx.doi.org/10.1007/978-3-662-54970-4_33

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from https://bitcoin.org/bitcoin.pdf

Reid, F., & Harrigan, M. (2012). *An Analysis of Anonymity in the Bitcoin System.* Springer, New York, NY. doi:https://dx.doi.org/10.1007/978-1-4614-4139-7_10

Steel, P., & König, C. (2006). *Integrating Theories of Motivation.* doi:http://dx.doi.org/10.5465/AMR.2006.22527462

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M., Regnell, B., & Wesslén, A. (1999). *Experimentation in Software Engineering.* Springer Berlin Heidelberg.

Appendix A Survey Introduction

As part of my final-year project at University, I have constructed a short survey of user competence concerning anonymity in the Bitcoin network. I seek participation from individuals that at some point have used a Bitcoin client (examples: Bitcoin Core, Armory, Electrum), which they have installed on their system in order to send and receive Bitcoins. This does not include any web-based solutions, where the technical challenges are of no concern to the end user. It is important that you have experienced the process of sending and receiving Bitcoins in order for your input to be valuable in my study, so please do not participate if you do not understand what this implies.

Appendix B Survey Background

Bitcoin builds on public-key cryptography, allowing individuals to engage in peer-to-peer transactions over the Internet by referencing the address of the receiver. This address consists of a sequence of alphanumeric characters and is known as a Bitcoin address. This means that Bitcoin does not take into account any information pertaining to someone's actual identity, effectively allowing parties to become pseudo-anonymous in the Bitcoin network.

Research suggests that it is in fact possible to pair Bitcoin addresses to IP addresses by observing transaction relay traffic and together with external data, such as forum posts, reveal information about users in the Bitcoin network. Although anonymity is an integral part of Bitcoin, it is often overshadowed by the economic benefits that the technology provides. This survey seeks to grasp an understanding of what anonymity means to the end user by implementing a series of questions, each measuring the user's readiness to succeed.

Appendix C Introductory Questions

This section seeks to understand the demographics behind this survey, but it is possible to ignore the first two questions, should you feel that they are too intrusive on your identity. Although an understandable choice, it does undermine the purpose of this survey to an extent, but your participation is still valued. The third question requires an answer in order for you to proceed.

Question 1: What is your gender?

- *Male*
- *Female*
- *Prefer not to answer*

Question 2: What is your age?

- *14 years of age or younger*
- *15 – 19*
- *20 – 29*
- *30 – 39*
- *40 – 49*
- *50 – 59*
- *60 – 69*
- *70 – 79*
- *80 years of age or older*

Question 3: How often do you send and/or receive Bitcoins?

- *Daily*
- *Weekly*
- *Monthly*
- *Annually*
- *Never*

Appendix D Mindset Regarding Anonymity

This section seeks to understand the user's attitude towards anonymity concerning Bitcoin in its entirety. This includes choices made outside of the actual technology, such as sharing your Bitcoin address on forums and message boards.

Question 1: How competent are you in maintaining your anonymity in the Bitcoin network?

- *Choose a number from 1 – 10, where 1 represents a low evaluation and 10 represents a high evaluation.*

Question 2: How much do you value your anonymity in the Bitcoin network?

- *Choose a number from 1 – 10, where 1 represents a low evaluation and 10 represents a high evaluation.*

Question 3: How much effort do you put into maintaining your anonymity in the Bitcoin network?

- *Choose a number from 1 – 10, where 1 represents a low evaluation and 10 represents a high evaluation.*

Question 4: How often do you research new methods for maintaining your anonymity in the bitcoin network?

- *Choose a number from 1 – 10, where 1 represents a low evaluation and 10 represents a high evaluation.*

Appendix E Sending Bitcoins

This section seeks to understand the user's mindfulness regarding the aspect of anonymity when sending Bitcoins, as well as how much the user allows this to affect their primary objective, which is to engage in a transaction.

Question 1: How competent are you in maintaining your anonymity when sending Bitcoins?

- *Choose a number from 1 – 10, where 1 represents a low evaluation and 10 represents a high evaluation.*

Question 2: How much do you value your anonymity when sending Bitcoins?

- *Choose a number from 1 – 10, where 1 represents a low evaluation and 10 represents a high evaluation.*

Question 3: How much effort do you put into confirming your maintained anonymity before sending Bitcoins?

- *Choose a number from 1 – 10, where 1 represents a low evaluation and 10 represents a high evaluation.*

Question 4: How much do you allow the aspect of anonymity to affect the activity of sending Bitcoins?

- *Choose a number from 1 – 10, where 1 represents a low evaluation and 10 represents a high evaluation.*

Appendix F Receiving Bitcoins

This section seeks to understand the user's mindfulness regarding the aspect of anonymity when receiving Bitcoins, as well as how much the user allows this to affect their primary objective, which is to engage in a transaction.

Question 1: How competent are you in maintaining your anonymity when receiving Bitcoins?

- *Choose a number from 1 – 10, where 1 represents a low evaluation and 10 represents a high evaluation.*

Question 2: How much do you value your anonymity when receiving Bitcoins?

- *Choose a number from 1 – 10, where 1 represents a low evaluation and 10 represents a high evaluation.*

Question 3: How much effort do you put into confirming your maintained anonymity before receiving Bitcoins?

- *Choose a number from 1 – 10, where 1 represents a low evaluation and 10 represents a high evaluation.*

Question 4: How much do you allow the aspect of anonymity to affect the activity of receiving Bitcoins?

- *Choose a number from 1 – 10, where 1 represents a low evaluation and 10 represents a high evaluation.*

Appendix G Closing Question

Question: How often do you review and/or improve your methodology for maintaining your anonymity in the Bitcoin network?

- *Daily*
- *Weekly*
- *Monthly*
- *Annually*
- *Never*