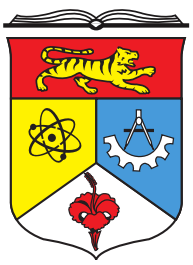
De-anonymization of Bitcoin Transactions in Decentralized, Trustless Payment Channel Networks

Gijs van Dam P95677

Research proposal

2018, Semester I

Supervised by:
Prof. Dato' Dr. Halimah Badioze Zaman F.A.Sc
Dr. Rabiah Abdul Kadir
Dr. Puteri Nor Ellyza Nohuddin
Institute of Visual Informatics



Universiti Kebangsaan Malaysia
National University of Malaysia

The National University of Malaysia

Date: 2018-12-21
Revision: v1.0-40-g7989ae6

Table of Contents

1 | Executive summary

The success of Bitcoin, the world's first distributed cryptocurrency, has shed light on its shortcomings. One of these shortcomings is the low throughput of 3 to 7 transactions per second. To make Bitcoin a feasible candidate for a global payment network, these numbers have to increase dramatically.

To achieve this, solutions have been proposed that run on top of Bitcoin, in a sort of second layer. The majority of transactions now occurring in the Bitcoin blockchain could theoretically be offloaded into this second layer, thereby improving the throughput to levels that rival current centralized global payment networks like VISA. The Lightning Network has emerged as the first real contender of being such a network.

These networks have the additional property of improving the anonymity and privacy of the participants. Privacy and anonymity on the level of the native Bitcoin blockchain, the first layer, so to speak, is a well-studied subject. But this body of knowledge is still lacking when it comes to the Payment Channel Networks proposed for the second layer.

The goal of this study is to formally analyze privacy in the context of second layer payment channel networks that run on top of the Bitcoin Blockchain.

The results should provide more transparency in the use of cryptocurrencies in transactions done on a Payment Channel Networks. It seeks to increase the awareness of the risks involved in dealing with cryptocurrencies. Lastly, the techniques developed in this research should be beneficial in due-diligence of reporting institutions by scrutinizing and screening blockchain and PCN transactions.

2 | Introduction

Bitcoin is the cryptocurrency with the largest market capitalization. In the beginning of 2018 Bitcoin hit its highest market cap of 835 billion US Dollar. Although this number has dwindled since then, it's still by far the most popular cryptocurrency. With this popularity some of its flaws have also risen to the surface, scalability being one of them. Several solutions have been proposed to solve these scalability issues, but only one of them has been implemented so far: the Lightning Network. This network runs on top of the Bitcoin blockchain and has the theoretical property of increasing the throughput of transactions dramatically. These solutions have the added benefit of increasing the level of anonymity of the participants. Until now the privacy of the participants in Lightning Network and other networks alike hasn't been formally analyzed. This study seeks to analyze and measure the privacy that can be obtained by participants in the Lightning Network.

3 | Research background

Bitcoin is a fully decentralized cryptocurrency that can operate in a trustless environment. Bitcoin was the first cryptocurrency that solved the Byzantine Generals Problem (Lamport et al. 1982) in the *specific context* of cryptocurrency, by incentivizing the nodes in a network to behave honest, and by embracing randomness. The latter meaning that there's a Bayesian approach to the confirmation of a transaction, meaning that the certainty of a transaction approaches 100% asymptotically over time. Because a decentralized cryptocurrency operates without a trusted, central party, participants need to have a way to trust the protocol without relying on another party. This is primarily achieved by broadcasting *all* transactions transparently on to the blockchain. This gives

participants in the Bitcoin network the opportunity to download the entire blockchain to verify that transactions are valid, and that the sender of a payment of which they are the receiver isn't trying to double spend their coins.

The transparency of all transactions means that privacy and anonymity can only be achieved by separating the transaction of the identities of the participants performing the transaction. This separation of transaction and identity is obtained by asymmetric encryption where the hash of the public key acts as an account number or address. These addresses act as pseudonyms for the participant. The anonymity that is achieved by this separation knows its limits, and a lot of research has been done to show those limits (Meiklejohn et al. 2013), (Garcia-Alfaro et al. 2015), (Langenheldt et al. 2018).

These limitations in turn provided the incentive for privacy improvement proposals. These proposals can be categorized into three different categories: - Alt-coins, new cryptocurrencies that are completely separate from Bitcoin - Protocol improvements, improvements to the Bitcoin protocol itself - Second layer improvements, overlays that run on top of the Bitcoin blockchain and don't require any or only small modifications to the Bitcoin protocol

Apart from being used as a solution for stronger privacy, the second layer is also the domain of Payment Channel Networks. These PCN's are proposed as a solution for Bitcoins scalability problem. Bitcoin is designed to handle on average 3 to 7 transactions per second. These numbers are dwarfed by centralized global payment networks like VISA, who claim to be able to process up to 24.000 transactions per second. PCN's achieve higher throughput by keeping transactions off-chain, meaning they don't get broadcasted unto the blockchain. This is made possible by opening up payment channels between participants, and keep private off-chain balances of transactions between any two participants. Upon closing of a payment channel the final balance is broadcasted to the Bitcoin blockchain. This way the amount of transactions that need to be broadcasted is drastically reduced. Theoretically this could lead to throughputs of the PCN that rival those of VISA and other global payment networks.

The improved anonymity of these PCN's is almost somewhat of a byproduct, but it is comparable to the anonymity achieved by second layer improvements that have the specific goal to increase anonymity, like Mixcoin, Blindcoin and TumbleBit (Conti et al. 2018). The lack of a rigorous definition of the PCN protocols, the absence of a threat model, and the ambivalent interpretations of the concept of anonymity have hindered formal analysis of privacy in the context of PCN's (Malavolta et al. 2017). # Problem statement

The level of anonymity to be attained in Bitcoin transactions is well studied, but the

amount of anonymity to be attained in Payment Channel Networks running on top of Bitcoin, has yet to be determined through formal privacy analysis. This study quantifies the achievable anonymity of participants in Payment Channel Networks under attack of both passive and active adversaries. It does so by using a formal threat model and using taint resistance as the quantity to measure anonymity. With PCN's being touted as *the* solution for Bitcoin's scalability problem, a proper assessment of the anonymity risks of those PCNs is of great importance.

4 | Research Objectives

This research has the following objectives:

1. To Find predictors for activity on PCN's within the blockchain
2. To Develop new heuristics for de-anonymization in PCN's
3. To uncover anonymity in PCN's using Supervised Machine Learning Algorithms

5 | Research scope

The scope of this study will be Trustless, Distributed Payment Channel Networks, running on the Bitcoin blockchain. The heuristics that are to be developed will use information

obtained through both passive and active adversaries.

6 | Hypotheses

1. The number of Unilaterally closed payment channels broadcasted to the Bitcoin blockchain in a specific period of time is a predictor for the number of Txs in the PCN.

    a) There is an effect modification of the average transaction fee calculated over the same period
    b) There is an effect modification of the average exchange rate against the US Dollar calculated over the same period
    c) There is an effect modification of the topological average connectedness of the PCN calculated over the same period

2. The fact that contracts belonging to the same Txs in a PCN encode the same condition, is a valid and practical heuristic for significantly reducing anonymity, measured as taint resistance of the coins involved in the Txs.

    a) A passive adversary cannot obtain the information needed to implement this heuristic.
    b) An active adversary can obtain the information needed to implement this heuristic.

3. Anonymity of yet-unidentified entities, measured as taint resistance of the coins involved, in a PCN can accurately be reduced by Supervised Machine Learning algorithms using training set data with linked senders and receivers.

7 | Literature Review

7.1 Bitcoin

At its core a distributed ledger like the Bitcoin blockchain is an asset database that is shared across multiple sites (Walport 2015). The entities or nodes involved in the ledger have a replicated version of the ledger available to them. Changes to the ledger are synchronized to all replicas by means of a peer-to-peer network. To ensure consistent replication across all nodes in a distributed ledger, a consensus algorithm is put in place. The peer-to-peer network in combination with the consensus algorithm enables the distributed ledger to exist without a central administrator or centralized storage.

7.2 Privacy and anonymity

The nature of a distributed ledger, without a central trusted party, requires that all transactions are transparent and broadcasted to the nodes in the network. As a result, privacy can only be obtained by making it impossible to link transactions to identities (Yli-Huumo et al. 2016). The separation of transaction and identity is obtained by an asymmetric encryption system in which the hash of the public key acts as an account number or address. These addresses should be interpreted as pseudonyms for the account holder (Moser et al. 2013). Account ownership is established by owning the corresponding private key, thus making it possible for the account holder to claim ownership of an address without revealing its identity. Whether this can be considered anonymous depends on your definition of anonymity. Since the advent of bitcoin several alternatives (alt-coins) have been proposed that commit to stronger privacy requirements and as such adhere to a stricter definition of anonymity. E.g. Zerocoin uses a definition that stays true to the cryptographic notion of unlinkability, resulting in a system where one coin can never be distinguished from another. (Miers et al. 2013) Strong anonymity a proposed by Zerocoin was never a design goal of the Bitcoin system (Reid & Harrigan 2013), and the resulting protocol leaks information that can be used to de-anonymize participants. The

underlaying, non-anonymous infrastructure of the internet and the inherent transparency of all transactions in the blockchain make this possible (Garcia-Alfaro et al. 2015).

7.3 Taint resistance

Taking the original design of Bitcoin as a given, one can arrive at a different notion of anonymity, coined *taint resistance* (Meiklejohn & Orlandi 2015). Taint resistance embraces the fact that a coin and its spending history are inseparable and as such focusses on obscuring the ownership of a coin at each point in its spending history. Taint resistance is a quantifiable measure of anonymity. It is a property of the transaction and can be applied to each transaction of a coin in its spending history. Taint resistance has a value ranging from 0 to 1, where 1 means an adversary can't achieve any accuracy in identifying the inputs of the Tx that tainted the output (also called the *taint set*) and 0 means that an adversary can identify the exact set of Txs that tainted the output. The latter means an adversary has exact knowledge of the taint set.

7.4 Account clustering

Account clustering is one of the techniques being used to reveal participants. In a longitudinal analysis of the flow of coins through the Bitcoin network, properties of transactions in the blockchain can be used to deduce statements about the entities performing the transactions. E.g. if two ore more addresses are inputs to a single transaction, one can assume that the addresses are controlled by the same entity (Ron & Shamir 2013). Additionally, one can assume that a one-time change address is controlled by the same entity that controls the input addresses (Meiklejohn et al. 2013). These heuristics enable clustering of addresses and linking them to entities. More recently Supervised Machine Learning techniques have been proven to be successful in uncovering anonymity by using training set data consisting of 200 million transactions that had previously been clustered and whose participants had been identified (Langenheldt et al. 2018).

7.5 Overlays and the Second layer

Overlays are Bitcoin improvements, proposed as solutions that run on top of the Bitcoin blockchain and don't require modifying the Bitcoin protocol. In some case small adjustments are needed to the Bitcoin protocol to make these overlays possible, which tend to

be achieved via BIPs. Overlays are sometimes jointly described as Bitcoin's Second Layer and should be distinguished from initiatives that seek improvements by introducing new virtual currencies altogether.

7.6 Active or passive adversaries

Using the definition of taint resistance to measure anonymity, one can measure this in two ways. Using only passive adversaries or using active adversaries. A passive adversary can only use the blockchain to get information on the taint set of a specific output. This means that information that is available in the second layer, but doesn't reach the blockchain is unavailable to a passive adversary. An active adversary on the other hand can participate in the second layer and can use this extra information to his or her advantage to identify the taint set.

7.7 Trustless Payment channels

Micropayment channels or Payment channels are a class of techniques designed to make it possible to make Bitcoin transactions that aren't committed to the blockchain. In a typical setting of a payment channel, 2 or more participants keep an off-chain ledger amongst themselves that keeps track of the outstanding balances between the participants. Upon closing of the payment channel, the final balance is broadcasted to the blockchain.

The first proposal for a payment channel was made by Satoshi Nakamoto, but this proposal wasn't secure ("Payment Channels" n.d.). Since then different designs have been proposed but most of them were susceptible to transaction malleability and aren't considered secure and as such can't operate in a trustless environment.

The scalability issues that now face Bitcoin have renewed the interest in payment channels as a possible solution for this problem. *Decker-Wattenhofer duplex payment channels* was the first solution proposed to combat these scaling issues, that didn't sacrifice the property of being able to operate in a trustless environment (Decker & Wattenhofer 2015).

Poon-Dryja payment channels was the second in this new class of trustless payment channels (Poon & Dryja 2016). Poon-Dryja payment channels form the foundation of the Lightning Network. The Lightning Network has emerged as the most prominent PCN to date (Malavolta et al. 2017).

The most recent addition to the trustless PCN's is *Decker-Russell-Osuntokun eltoo Channels* (Decker & Russell 2018). The Eltoo PCN tries to improve several aspects of its two

predecessors, e.g. the absence of a punishment branch and simplifying watchtower design.

7.8 PCN Privacy Threat Model

For a formal analysis of privacy in the setting of trustless PCN's a privacy threat model is a necessity. We use the threat model proposed by Malavolta (Malavolta et al. 2017). This threat model describes four notions of interest:

- Balance security: Participants don't run the risk of losing coins to a malevolent adversary.
- Serializability: Executions of a PCN are serializable as understood in concurrency control of transaction processing, i.e. for every concurrent processing of payments there exists an equivalent sequential execution.
- (Off-path) Value Privacy: Malevolent passive adversaries
- (On-path) Relationship Anonymity: Given at least on honest intermediary, corrupted intermediaries cannot determine the sender and the receiver of a transaction better than just by guessing.

8 | Research Methodology

We will run a Bitcoin node with a Lightning Network node on top of it, running both in the cloud. We will run both nodes for a period of two months. During that period the following data will be collected:

- Bitcoin exchange rate against the US Dollar
- Topological connectedness of the PCN

The gathered information together with the data available in the blockchain itself, e.g. transaction fees, will be used to predict the activities on the PCN.

Secondly, the information obtained during those two months can be used to test the taint resistance of transactions performed on the PCN in the context of a passive adversary.

This also allows for developing an PCN attack model in the context of an active adversary. Following this model we will set up one to multiple Lightning nodes to allow for a second round of data gathering. During this second round we will test multiple active adversary heuristics, and measure the resulting taint resistance of transactions performed on the PCN.

Thirdly, using Supervised Machine Learning algorithms and a training set data gathered in the previous phase, we will produce an inferred function which can be used to decrease the taint resistance of yet to be identified transactions.

9 | Significance of study

> "Promoting greater transparency in the use of digital currencies serves to protect the integrity of the financial system and strengthen incentives to prevent their abuse for illegal activities"
>
> "Members of the public are therefore advised to undertake the necessary due diligence and assessment of risks involved in dealing in digital currencies or with entities providing services associated with digital currencies."

Source: Bank Negara - Policy document on Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) – Digital Currencies (Sector 6)

The above quotes from Bank Negara give a backdrop to the significance of this study. The results should provide more transparency in the use of digital currencies by supplying new techniques for analyzing the blockchain and PCN especially. Assess the risks involved in dealing with digital currencies through these newly implemented second layer solutions. Lastly, the results of this study could be beneficial in due-diligence of reporting

institutions by scrutinizing and screening blockchain and PCN transactions.

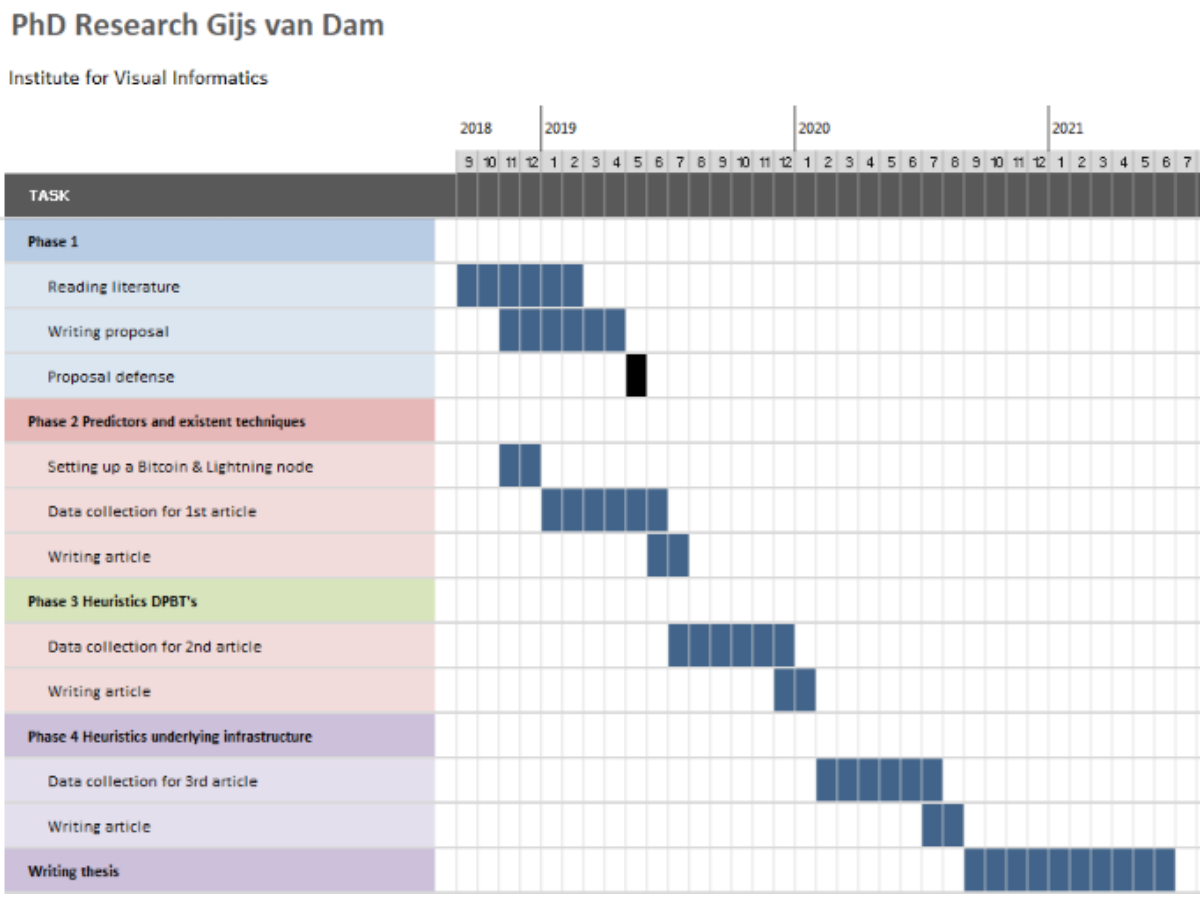
10 | Summary

Scalability solutions for Bitcoin take the form of overlays on to the Bitcoin Blockchain, that offload a significant percentage of the transactions into this overlay, dubbed the second layer. These solutions, called Payment Channel Networks have recently found ways to make this work in a trustless environment, making them a feasible solution for extending and improving upon the success of Bitcoin. Because these solutions take transactions, and thus information, off-chain, they have the added benefit of improving the level of privacy and anonymity that can be obtained while performing transactions through these networks.

These privacy improvements are as of yet mostly theoretical, and formal research into the actual, obtainable privacy has been sparse to non-existent. This study seeks to analyze and measure the privacy that can be obtained by participants in those second layer networks. It does so by running both Bitcoin and Lightning nodes, and collecting data to determine the predictors of activity on the Lightning Network. Furthermore, this study will use inherent properties of payment channel networks to develop heuristics that can be used in the context of either passive or active adversaries to decrease the level of anonymity, measured as taint resistance.

Upon developing those heuristics we will use Supervised Machine Learning to produce an inferred function which can be used to decrease the taint resistance of yet to be identified transactions.

Appendix 1: Gantt chart



Appendix 2: Abbreviations

PCN	**P**ayment **C**hannel **N**etwork
Tx(s)	**T**ransaction(s)
BIP	**B**itcoin **I**mprovement **P**roposal

References

Conti, M., E, S.K., Lal, C. & Ruj, S. 2018. A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys and Tutorials* 20(4): 3416–3452.

Decker, C. & Russell, R. 2018. eltoo : A Simple Layer2 Protocol for Bitcoin: 1–24.

Decker, C. & Wattenhofer, R. 2015. A fast and scalable payment network with bitcoin duplex micropayment channels. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 9212: 3–18.

Garcia-Alfaro, J., Herrera-Joancomartí, J., Lupu, E., Posegga, J., Aldini, A., Martinelli, F. & Suri, N. 2015. Data privacy management, autonomous spontaneous security, and security assurance.

Lamport, L., Shostak, R. & Pease, M. 1982. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems* 4(3): 382–401.

Langenheldt, C., Harlev, M.A., Hua, H., Yin, S., Mukkamala, R.R. & Vatrapu, R. 2018. Breaking Bad : De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learninghlm. 3497–3506.

Malavolta, G., Moreno-Sanchez, P., Kate, A., Maffei, M. & Ravi, S. 2017. Concurrency and Privacy with Payment-Channel Networks. *Proceedings of the 2017 acm sigsac conference on computer and communications security - ccs '17*, hlm. 455–471. ACM Press, New York, New York, USA.

Meiklejohn, S. & Orlandi, C. 2015. Privacy-enhancing overlays in bitcoin. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).*

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. & Savage, S. 2013. A fistful of Bitcoins: Characterizing Payments Among Men with No Names. *Communications of the ACM* 59(4): 86–93.

Miers, I., Garman, C., Green, M. & Rubin, A.D. 2013. Zerocoin: Anonymous distributed e-cash from bitcoin. *Proceedings - ieee symposium on security and privacy*, hlm..

Moser, M., Bohme, R. & Breuker, D. 2013. An inquiry into money laundering tools in the Bitcoin ecosystem. *eCrime Researchers Summit, eCrime.*

Payment Channels. (n.d.)..

Poon, J. & Dryja, T. 2016. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.

Reid, F. & Harrigan, M. 2013. An Analysis of Anonymity in the Bitcoin System. Dlm. *Security and*

privacy in social networks, hlm. 197–223. Springer New York, New York, NY.

Ron, D. & Shamir, A. 2013. Quantitative analysis of the full Bitcoin transaction graph. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 7859 LNCS: 6–24.

Walport, M. 2015. Distributed ledger technology: Beyond block chain. hlm. 1–88.

Yli-Huumo, J., Ko, D., Choi, S., Park, S. & Smolander, K. 2016. Where is current research on Blockchain technology? - A systematic review. *PLoS ONE* 11(10): 1–27.