Obfuscation in Bitcoin: Techniques and Politics[1]

Arvind Narayanan & Malte Möser
Princeton University

Abstract. In the cryptographic currency Bitcoin, all transactions are recorded in the blockchain — a public, global, and immutable ledger. Because transactions are public, Bitcoin and its users employ obfuscation to maintain a degree of financial privacy. Critically, and in contrast to typical uses of obfuscation, in Bitcoin obfuscation is not aimed against the system designer but is instead enabled by design. We map sixteen proposed privacy-preserving techniques for Bitcoin on an obfuscation-vs.-cryptography axis, and find that those that are used in practice tend toward obfuscation. We argue that this has led to a balance between privacy and regulatory acceptance.

Obfuscation Techniques

Bitcoin's design is centered around a widely distributed, global database which stores all transactions that have ever taken place in the system. Thus, there is no avenue for redress if a user wishes to retrospectively hide a transaction. Further, nothing in the ledger is encrypted, and digital signatures are mandatory, ensuring cryptographic attribution of activities to users. On the other hand, account identifiers in Bitcoin take the form of cryptographic public keys, which are pseudonymous. Anyone can use Bitcoin "wallet" software to trivially generate a new public key and use it as a pseudonym to send or receive payments without registering or providing personal information. However, pseudonymity alone provides little privacy, and there are many ways in which identities could be linked to these pseudonyms (Narayanan et al., 2016).

To counter this, Bitcoin and its users employ a variety of obfuscation techniques to increase their financial privacy. We visualize a representative selection of these techniques in Figure 1 based on their time of invention/creation and our assessment of their similarity to obfuscation vs cryptography. We make several observations. First, techniques used in Bitcoin predominantly fall into obfuscation, with stronger techniques being used exclusively in alternative cryptocurrencies (altcoins). Second, there is a trend towards stronger techniques over time, perhaps due to a growing interest in privacy and to the greater difficulty of developing cryptographic techniques. Third, obfuscation techniques proposed at later points in time are seeing less adoption, arguably a result of their increased complexity and need for coordination among participants (Möser & Böhme 2017).

[1] Presented at the *International Workshop on Obfuscation: Science, Technology, and Theory*, New York University, April 7-8, 2017.

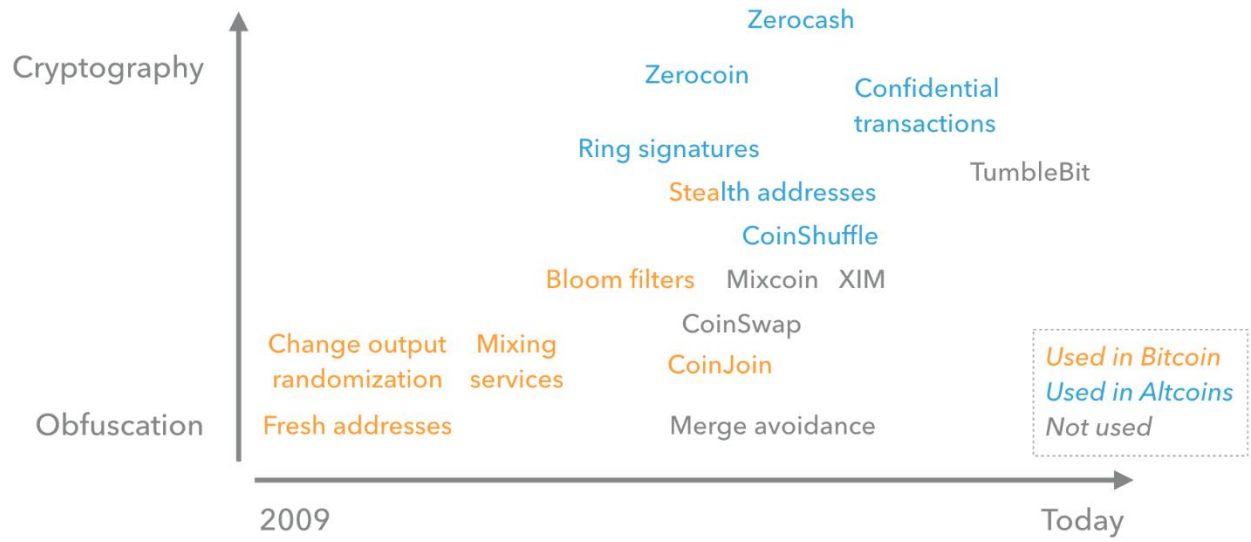

Figure 1: Privacy-Enhancing Technologies for Bitcoin. The X-axis is the date of invention and the Y-axis is an informal measure that combines the sophistication of the technique and the strength of the privacy guarantee. See Appendix 1 for references and dates.[2]

Among the techniques used in Bitcoin, the most prevalent can be characterized as "ambiguating obfuscation" (Brunton & Nissenbaum 2015): effectively reducing the information an adversary is able to extract from a particular transaction. Examples include using a new pseudonym for every new transaction and randomizing the structure of transactions to make the spend to the "true" recipient indistinguishable from "change" going back to the sender.

A second type of obfuscation, namely "cooperative obfuscation", has risen in popularity over the last years. For example, users can send their money to a service that will "mix" their funds with those of other users, thereby obfuscating the flow of payments (cf. Möser, Böhme & Breuker 2013). A similar technique called CoinJoin works in a peer-to-peer fashion and doesn't require a trusted intermediary is CoinJoin. Due to the need for these users to find and transact with each other, markets for anonymity have arisen that bring together providers and receivers of anonymity (Möser & Böhme 2016).

The Case for Obfuscation

Critically, none of the techniques discussed provide provable privacy guarantees through cryptography. While these do exist and have been deployed (e.g., Zcash), they are far from being adopted by the Bitcoin community, for both technical and political reasons. On the technical side, Bitcoin's decentralization already incurs a severe performance penalty compared to centralized payment systems such as Paypal. Achieving cryptographic privacy would further degrade performance. Obfuscation also has a lighter impact on the

[2] In a previous draft of this paper, the X-positions of some of the techniques in the figure were slightly off due to an image editing error. We have fixed those, and report the dates in Appendix 1.

usefulness of the blockchain for non-currency applications. The current design allows selectively employing obfuscation, leaving room for other uses that prioritize different goals, such as Colored Coins (Rosenfeld 2012), a protocol for representing assets on top of the Bitcoin blockchain.

On the political side, providing stronger privacy through cryptography might make Bitcoin even more attractive for activities such as money laundering, ransomware, or terrorism financing, and thereby tempt a government crackdown. Much of the Bitcoin community is invested in its mainstream adoption, and therefore keen to avoid such an outcome. When Bitcoin began to be noticed by the press, members of the community went to work explaining it to policy makers. They framed the technology as neutral and unthreatening, and the Bitcoin ecosystem as subject to existing regulations and amenable to new ones (cf. Brito 2013, Brito & Castillo 2013, Lee 2013, Murck 2013, Hattem 2014).

The use of obfuscation in Bitcoin may have achieved a balancing act between the financial privacy of its users and the investigatory needs of law enforcement and regulators. Law enforcement agencies have two important advantages over everyday adversaries: the budget for specialized Bitcoin tracking tools and services (Cox 2017), and subpoena power. The latter allows deanonymizing selected actors by obtaining user records from exchanges and cross-referencing them with the results of blockchain analysis (Meiklejohn et al. 2013). Since only a few governmental actors possess these powers, users still enjoy a measure of financial privacy. Thus, the imperfect privacy protection in Bitcoin may be one of the keys to its success.

References

Bissias, G., Ozisik, A. P., Levine, B. N., & Liberatore, M. (2014). Sybil-Resistant Mixing for Bitcoin. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society* (pp. 149-158). ACM.

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J. A., & Felten, E. W. (2014). Mixcoin: Anonymity for Bitcoin with Accountable Mixes. In *International Conference on Financial Cryptography and Data Security* (pp. 486-504). Springer Berlin Heidelberg.

Brito, J., & Castillo, A. (2013). Bitcoin: A Primer for Policymakers. Mercatus Center at George Mason University.

Brito, J. (2013). Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies. Testimony to the Senate Committee on Homeland Security and Governmental Affairs. Available online at https://www.mercatus.org/system/files/Brito_BeyondSilkRoadBitcoin_testimony_111313.pdf (retrieved on 2017-06-02).

Brunton, F., & Nissenbaum, H. (2015). Obfuscation: A User's Guide for Privacy and Protest. MIT Press.

Cox, J. (2017). US Law Enforcement Have Spent Hundreds of Thousands on Bitcoin Tracking Tools. *Motherboard.* Available online at https://motherboard.vice.com/en_us/article/us-law-enforcement-have-spent-hundreds-of-thousands-on-bitcoin-tracking-tools (retrieved on 2017-06-02).

Hattem, J. (2014). Bitcoin Gets a Lobbyist. *The Hill.* Available online at http://thehill.com/policy/technology/207085-bitcoin-investors-register-lobbyist (retrieved on 2017-06-02).

Hearn, M., & Corallo, M. (2012). BIP 37: Connection Bloom Filtering. Available online at https://github.com/bitcoin/bips/blob/master/bip-0037.mediawiki (retrieved on 2017-06-02).

Hearn, M. (2013). Merge Avoidance. Available online at https://medium.com/@octskyward/merge-avoidance-7f95a386692f (retrieved on 2017-06-02).

Heilman, E., Baldimtsi, F., Alshenibr, L., Scafuro, A., & Goldberg, S. (2017). TumbleBit: An Untrusted Tumbler for Bitcoin-Compatible Anonymous Payments. In *Network and Distributed System Security Symposium (NDSS)*.

Lee, T. B. (2013). Here's How Bitcoin Charmed Washington. *The Washington Post.* Available online at https://www.washingtonpost.com/news/the-switch/wp/2013/11/21/heres-how-bitcoin-charmed-washington (retrieved on 2017-06-02).

Maxwell, G. (2013a). CoinJoin: Bitcoin Privacy for the Real World. Available online at https://bitcointalk.org/index.php?topic=279249.0 (retrieved on 2017-06-02).

Maxwell, G. (2013b). CoinSwap: Transaction Graph Disjoint Trustless Trading. Available online at https://bitcointalk.org/index.php?topic=321228 (retrieved on 2017-06-02).

Maxwell, G. (2015). Confidential Transactions, the Initial Investigation. Available online at https://www.elementsproject.org/elements/confidential-transactions/investigation.html (retrieved on 2017-06-02).

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. In *Proceedings of the 2013 Conference on Internet Measurement* (pp. 127-140). ACM.

Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In *2013 IEEE Symposium on Security and Privacy (S&P)* (pp. 397-411). IEEE.

Möser, M., Böhme, R., & Breuker, D. (2013). An Inquiry Into Money Laundering Tools in the Bitcoin Ecosystem. In *eCrime Researchers Summit, 2013* (pp. 1-14). IEEE.

Möser, M., & Böhme, R. (2016). Join Me on a Market for Anonymity. In *Workshop on the Economics of Information Security (WEIS)*.

Möser, M., & Böhme, R. (2017). Anonymous Alone? Measuring Bitcoin's Second-Generation Anonymization Techniques. In *IEEE Security & Privacy on the Blockchain (IEEE S&B)*. IEEE.

Murck, P. (2013). Testimony of Patrick Murck General Counsel, the Bitcoin Foundation to the Senate Committee on Homeland Security and Governmental Affairs "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies". Available online at

https://www.hsgac.senate.gov/download/?id=4CD1FF12-312D-429F-AA41-1D77034EC5A8 (retrieved on 2017-06-02).

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

Rosenfeld, M. (2012). Overview of Colored Coins. Available online at https://bitcoil.co.il/BitcoinX.pdf (retrieved on 2017-06-02).

Ruffing, T., Moreno-Sanchez, P., & Kate, A. (2014). CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin. In *European Symposium on Research in Computer Security* (pp. 345-364). Springer International Publishing.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy (S&P)* (pp. 459-474). IEEE.

Todd, P. (2014). Stealth Addresses. Available online at https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2014-January/004020.html (retrieved on 2017-06-02).

Van Saberhagen, N. (2012). CryptoNote v 1.0. Available online at https://cryptonote.org/whitepaper_v1.pdf (retrieved on 2017-06-02).

Appendix 1: References for Privacy-Enhancing Techniques for Cryptocurrencies

Name	Reference	Approx. Date[3]
Bitcoin mixers	*cf.* Möser, Böhme & Breuker 2013	2011
Bloom filter	Hearn & Corallo 2012	October 2012
CoinJoin	Maxwell 2013a	August 2013
CoinShuffle	Ruffing 2014	April 2014
CoinSwap	Maxwell 2013b	October 2013
Confidential transactions	Maxwell 2015	June 2015
Merge avoidance	Hearn 2013	December 2013
Mixcoin	Bonneau et al. 2014	February 2014
Ring signatures	Van Saberhagen 2012	December 2012
Stealth addresses	Todd 2014	January 2014
TumbleBit	Heilman et al. 2017	June 2016
XIM	Bissias et al. 2014	November 2014
Zerocash	Sasson et al. 2014	May 2014
Zerocoin	Miers et al. 2013	May 2013

[3] The dates represent the earliest public proposals of the respective techniques that we could find. For the latest version of this table, see https://github.com/maltemoeser/bitcoin-anonymity/blob/master/obfuscation-techniques.md

Appendix 2: The Lifecycle of Obfuscation

The success of obfuscation in Bitcoin motivates studying the adoption of obfuscation in sociotechnical systems more generally. To this end, we present a simplified model of the adoption of obfuscation, visualized in Figure 2.

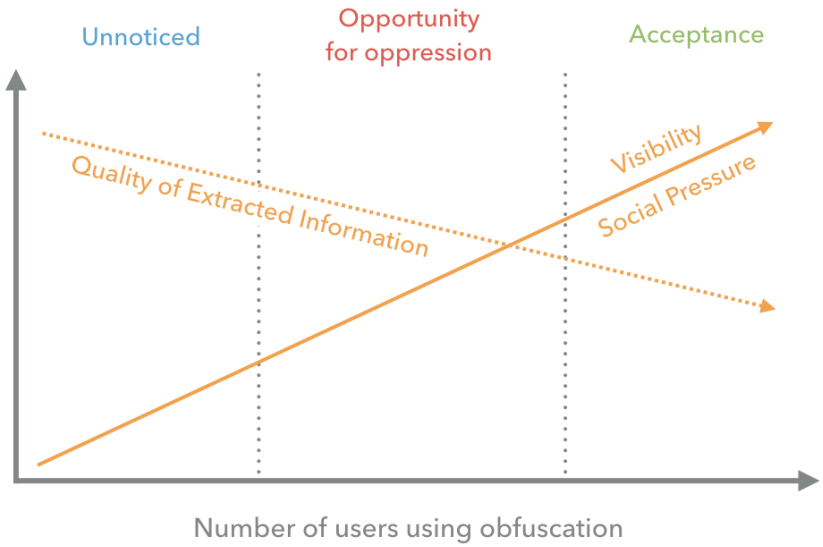

Figure 2: Lifecycle of Obfuscation

We conjecture that as the number of users of obfuscation grows, the visibility of the use of obfuscation increases as well. It also reduces the quality of the information that can be extracted from the system. We argue that initially, the use of obfuscation is mostly unnoticed as the user base and its impact is small. On the other hand, once obfuscation has reached a critical mass, social pressure helps against the platform owner's (or government's) wish to oppress obfuscation, leading to general acceptance. A good example is "Nymwars", i.e. Google's (and other companies) attempt to forbid the use of pseudonyms on social networks. Due to a large, negative public reaction Google had to reverse its decision to ban the use of pseudonyms. This suggests a critical phase in between these two, where there is opportunity for oppression by the platform owner or government. For those who aim to establish obfuscation as a means of defense against a system, this suggests two related strategies to minimize the window of oppression. The first is to hide the use of obfuscation for as long as possible through both social and technical means. The second is to maximize the visibility of obfuscation and campaign for its acceptance once it can no longer remain unnoticed.