Chair of Strategy and Organization
TUM School of Management
Technical University of Munich

Executive Summary - Analysis of lost coins on the Bitcoin blockchain

How many bitcoins will never come back into circulation due to either technical failure, human failure, or intentional destruction?

Jakob Wandschneider

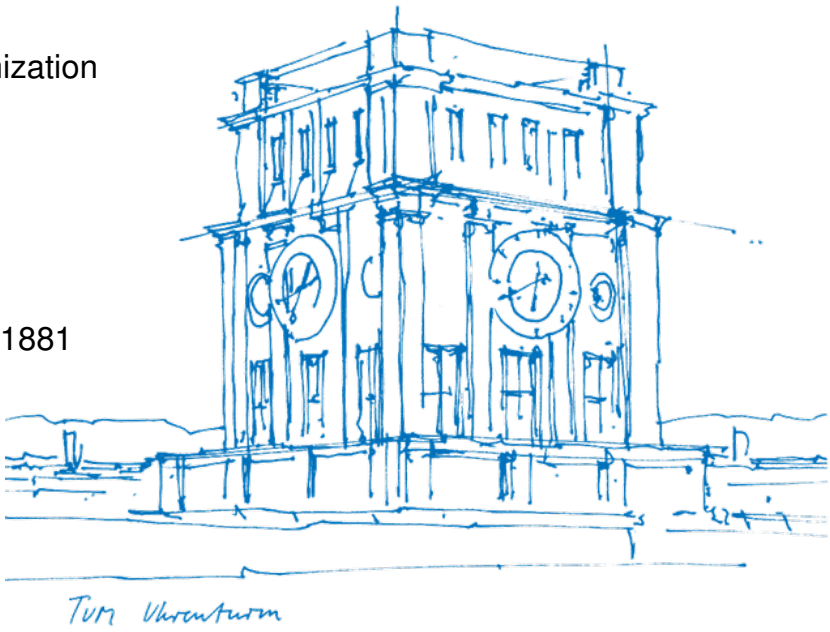
Thesis for the Attainment of the Degree
Master of Science
at TUM School of Management of the Technical University of Munich

Examiner
Prof. Dr. Isabell M. Welpe
Chair of Strategy and Organization

Supervised by
Dr. Ulrich Gallersdörfer

Submitted by
Jakob Wandschneider
Matriculation Number: 03681881

Submitted on
15.06.2022



Contents

Introduction **3**

Methods **4**

Results and Discussion **4**

Conclusion **6**

List of Tables

1 Overview of lost bitcoins listed by category and methods. 5

List of Figures

1 Comparison of currently mined bitcoins and the number of bitcoins lost resulting in the real estimated bitcoin supply. 5

Analysis of lost coins on the bitcoin blockchain

Bitcoin was the first blockchain, and today, after 13 years, it is still the market leader in market capitalization (Coinmarketcap, 2022). The special feature of Bitcoin is that it is a limited asset. The blockchain was programmed to have a maximum of 21 million bitcoins (Nakamoto, 2008). However, with Bitcoin, no institution can help users if something goes wrong with the assets. So if a user loses the private key, the bitcoins are lost, and no one else can access these bitcoins. It can be assumed that there will never be 21 million bitcoins in circulation.

Currently, all financial KPIs and studies about the environmental impact of bitcoins are based on either the maximum supply of 21 million bitcoins or the total number of currently mined bitcoins, which is around 19 million bitcoins at the moment. Nevertheless, these KPIs should be based only on bitcoins that are accessible because lost coins do not add any value to the network. Unfortunately, the actual number of bitcoins in circulation that users can access is currently unavailable. This thesis aims to provide a holistic view of how many bitcoins are accessible by users and how many bitcoins are lost and will never be accessible again.

Six possibilities in three categories were identified to quantify the number of lost bitcoins. The first category, called *Human Failure* includes lost private keys and address typos. Bitcoin assets can only be spent with the correct private key. If the key is lost, the bitcoins are lost (Antonopoulos, 2017). Accidentally including a spelling mistake in the receiving bitcoin address can lock the coin forever in an address that nobody uses (LiteForex, 2019). The second category called *Intentional Destruction* includes OP_Return transactions and burn addresses. OP_Return writes a message on the bitcoin blockchain but makes any bitcoins included in the transaction unspendable forever (Bartoletti and Pompianu, 2017). Burn addresses do not have a private key, and any bitcoins sent to

burn addresses are locked to the specific burn address forever (Karantias, Kiayias, and Zindros, 2020). The third category, called *Technical Failure* looks into failed coinbase transactions and bitcoin dust. Miners receive bitcoins for discovering a new block. Sometimes miners fail to claim the full block reward (StackExchange, 2012). Small bitcoin values worth less than transaction costs are called dust and are uneconomical to move. These bitcoins are also lost (Delgado-Segura, Perez-Sola, Navarro-Arribas, and Herrera-Joancomart, 2018).

Methods

The analysis was performed with python code. Every data set was pulled directly from the bitcoin node running on the same server (Bitcoin.org, n.d.). Burn addresses, OP_Return transactions, and coinbase transactions were analyzed using block data from the node. Bitcoin dust and address typos were detected using the UTXO set at block 724,018. The lost private key method used both data sources in a combination. The complete information on the code can be found in the GitHub Repository: https://github.com/CarbonRatings/lostCoins.

Results and Discussion

The main finding is that, in total, approximately 4.2 million bitcoins are lost. Currently, 19.0 million bitcoins have been mined and should be in circulation. However, due to the 4.2 million bitcoins that are lost, as analyzed by the six methods, only 14.8 million bitcoins are actually in circulation. Currently, miners are still about 2 million bitcoins away from the maximum 21 million bitcoins meaning that in the future, there can only be a maximum of 16.8 million bitcoins in circulation (Figure 1).

The second most important result is the realization that the lost private key is the most significant reason for lost bitcoins. Table 1 gives an insight into the exact number

Figure 1

Comparison of currently mined bitcoins and the number of bitcoins lost resulting in the real estimated bitcoin supply.

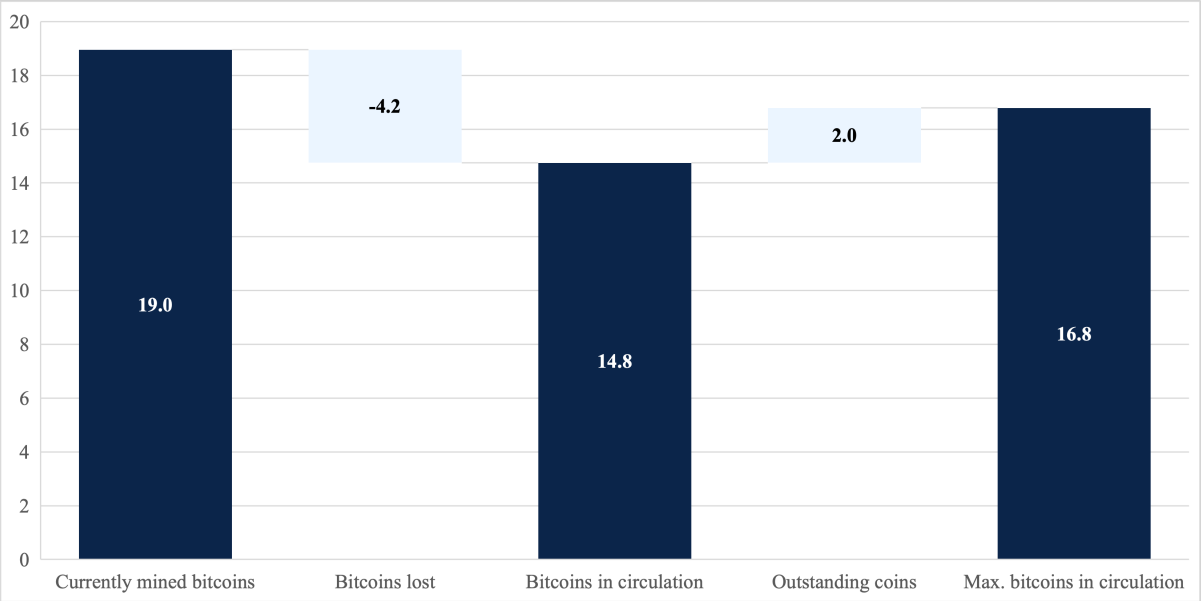


Table 1

Overview of lost bitcoins listed by category and methods.

Category	Method	Number of lost bitcoins	% of lost bitcoins
Human Failure	Lost Private Key	4,204,090.00	22.17%
	Address Typo	0.01	0.00%
Intentional Destruction	OP_Return	27.25	0.00%
	Burn Address	2,951.78	0.02%
Technical Failure	Coinbase Trasaction	28.96	0.00%
	BTC Dust	1,064.34	0.01%
Total coins lost		4,208,162.34	22.19%

of lost coins grouped by category and method. Approximately 4.2 million bitcoins are lost due to private key losses. In comparison, all other methods combined only caused approximately 4,072 lost bitcoins. Only 0.01 bitcoins were lost due to spelling the address wrong. Burn addresses were responsible for 2,951.78 bitcoins lost and OP_-Return transactions locked in 27.25 bitcoins forever. The smallest amount of bitcoins were lost due to *technical failure*. The dust problem makes up 1,064.34 bitcoins, and coinbase transactions are only 28.96 bitcoins. This table shows that lost private keys are the biggest lost coins problem, and the other methods can almost be neglected.

Conclusion

More than 22% of currently mined bitcoins are lost, and more than 99.9% of these lost bitcoins are lost due to private key problems. Humans are thus the weak point in the Bitcoin network. The private key must be stored extremely securely and secretly. As a result, it is lost, and users lose access to their assets. All other possibilities to lose bitcoins, such as *intentional destruction* or due to *technical errors*, are almost negligible for the topic of lost coins.

Based on these results, the analysis of bitcoins lost due to users losing their private keys should be repeated regularly to understand if the number increases, stagnates, or maybe even decreases. This future research would help understand the effect of lost private keys on the usability of Bitcoin one day.

Bibliography

Antonopoulos, A. M. (2017). *Mastering Bitcoin: programming the Open Blockchain*. O'Reilly Media, Inc.

Bartoletti, M. & Pompianu, L. (2017). An analysis of bitcoin op_return metadata. arXiv. doi:10.48550/ARXIV.1702.01024

Bitcoin.org. (n.d.). Running a full node. Retrieved on 2022-04-18. Retrieved from https://bitcoin.org/en/full-node

Coinmarketcap. (2022). Today's cryptocurrency prices by market cap. Retrieved on 2022-05-17. Retrieved from https://coinmarketcap.com

Delgado-Segura, S., Perez-Sola, C., Navarro-Arribas, G., & Herrera-Joancomart, J. (2018). *Analysis of the Bitcoin UTXO Set*. Department of Information Engineering and Communications, Universitat Autonoma de Barcelona, CYBERCAT-Center for Cybersecurity Research of Catalonia, Barcelona, Spain.

Karantias, K., Kiayias, A., & Zindros, D. (2020). Proof-of-Burn. *Financial Cryptography and Data Security*, *24*, 523–540.

LiteForex. (2019). What if i enter the wrong address of a bitcoin wallet? Retrieved on 2022-04-26. Retrieved from https://medium.com/@LiteForex/what-if-i-enter-the-wrong-address-of-a-bitcoin-wallet-86f0d910cefc

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

StackExchange. (2012). What happens when a miner does not claim all fees/generated coins? Retrieved on 2022-04-27. Retrieved from https://bitcoin.stackexchange.com/questions/4573/what-happens-when-a-miner-does-not-claim-all-fees-generated-coins

Declaration of Academic Integrity

I hereby declare that the thesis submitted is my own unaided work. All direct or indirect sources used are acknowledged as references.

I am aware that the thesis in digital form can be examined for the use of unauthorized aid and in order to determine whether the thesis as a whole or parts incorporated in it may be deemed as plagiarism. For the comparison of my work with existing sources I agree that it shall be entered in a database where it shall also remain after examination, to enable comparison with future theses submitted. Further rights of reproduction and usage, however, are not granted here.

This paper was not previously presented to another examination board and has not been published.

Munich, 15.06.2022 Jakob Wandschneider