Demo: Visualizing the Bitcoin's OP_RETURN operator

Johannes Mols
johannes.mols@gmail.com
Aalborg University

Emmanouil Vasilomanolakis
emv@es.aau.dk
Aalborg University

ABSTRACT

Bitcoin is undoubtedly the most used distributed ledger technology nowadays. Bitcoin's OP_RETURN operator allows for saving arbitrary data on the blockchain. This comes as an extension of Bitcoin's core usage (i.e. cryptocurrency) and opens up a multitude of use cases. These range from benign applications (e.g. ownership of a digital/physical asset) to illegal/malicious scenarios (e.g. blockchain-based botnets). In this paper, we present a system that provides advanced analytic and visual capabilities with regard to the OP_RETURN operator. Furthermore, we showcase a quantitative and qualitative analysis of the OP_RETURN along with a number of interesting findings.

CCS CONCEPTS

• **Security and privacy** → *Network security*; • **Networks** → *Network experimentation*.

KEYWORDS

Bitcoin, OP_RETURN, Blockchain, Visualization, Distributed Ledgers

ACM Reference Format:
Johannes Mols and Emmanouil Vasilomanolakis. 2020. Demo: Visualizing the Bitcoin's OP_RETURN operator. In *The Twenty-first ACM International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing (Mobihoc '20), October 11–14, 2020, Boston, MA, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3397166.3415278

1 INTRODUCTION

Bitcoin was the first blockchain to be conceptualized in 2009 and has since surged in popularity. With a total value of ~167 billion USD[1], it has become a widely popular and well-researched technology.

Bitcoin users have been searching for different ways of embedding non-financial data in transactions. The idea here is that one can exploit the blockchain's properties (resilience, transparency, etc.) for applications that are beyond the cryptocurrency context. Examples include but are not limited to ownership of assets, document notary and digital copyrights [2]. These type of transactions are unspendable and forever kept in the unspent transaction output (UTXO). As a compromise, the Bitcoin Script received a new operator called OP_RETURN in v0.9.0 which allows users to store up to 83 bytes of arbitrary data in transactions and mark them as unspendable.

Since its introduction, the OP_RETURN operator has been utilized and has been exploited in a plethora of ways. On the one hand, Bartoletti and Pompianu [2] performed an empirical study on the (benign) usage of OP_RETURN by various protocols. On the other hand, Faisal et al. [4] and Matzutt et al. [5] provided an analysis of the operator with an emphasis on potentially illegal content and hidden files. Furthermore, Böck et al. [3], following the steps of [1], provided an assessment of the threat of blockchain-based botnets.

This paper further investigates the usage of OP_RETURN since its introduction, both quantitatively and qualitatively. We present a service that collects and analyzes all OP_RETURN transactions. Moreover, we created a web application that visualizes the data and allows users to perform advanced searches for specific transactions.

2 VISUALIZING AND ANALYZING THE OP_RETURN UTILIZATION

This Section presents quantitative and qualitative results with regard to the OP_RETURN utilization.

2.1 Quantitative Analysis

The web application is capable of displaying four different charts: the daily usage of OP_RETURN compared to other transaction types, the daily average output size of OP_RETURN transactions (see Figure 1), the daily protocol usage for each protocol, and a pie chart for the distribution of protocols over a fixed range of time (see Figure 2).

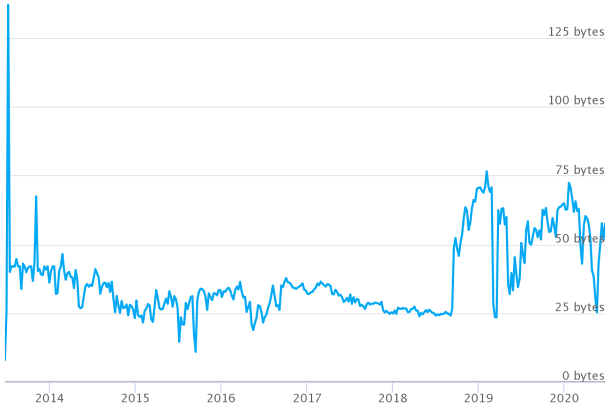

Figure 1: Daily average size of OP_RETURN transactions

Since its introduction in 2013, the usage of the operator has steadily increased. At the end of 2018, the *VeriBlock*[2] service was

[1] https://coinmarketcap.com/currencies/bitcoin/ (accessed 2020-06-29)

[2] https://www.veriblock.org/ (accessed 2020-06-29)

Mobihoc '20, October 11–14, 2020, Boston, MA, USA
© 2020 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-8015-7/20/10.
https://doi.org/10.1145/3397166.3415278

introduced. This created a significant spike in the usage of the operator, with a peak of 192,818 daily OP_RETURN transactions on 2019-04-21, 20.77% of all Bitcoin outputs of that day.

Our analysis shows that VeriBlock is responsible for ∼50% of all OP_RETURN transactions, closely followed by another protocol called *Omni*[3] at ∼39.8%. The remaining ∼10.2% can be partially attributed to other protocols.

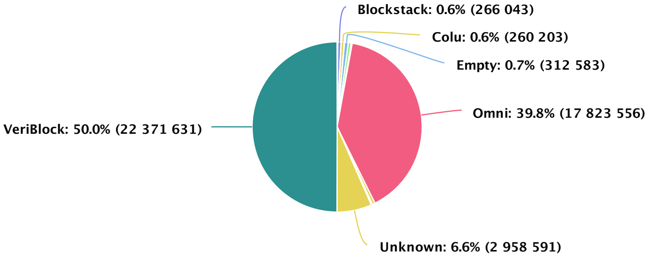

Figure 2: Distribution of protocols using OP_RETURN

Besides the large amount of VeriBlock transactions, the protocol also has a significant impact on the average size of OP_RETURN transactions. Before it was introduced, the average size was between 25 – 40 bytes, and has then jumped to 50 – 70 bytes. We estimate that VeriBlock is responsible for ∼77.5% of all data stored using the operator due to its average size of 82 bytes per transaction.

2.2 Qualitative Analysis

Besides the charts, our web application allows users to search for specific transactions based on various filters including the date range, content, protocols, and file headers. This opens up the possibility of analyzing the contents of the transactions more closely.

While most transactions are not stored in plain text, the ones that are can be decoded by the application and displayed to the user. The text-based search function allows users to search for such content. Our analysis revealed many interesting examples including *marriage proposals, birthday wishes, poems*, etc.

By manually reviewing transactions that cannot be attributed to a known protocol (c.f. [2, 6]), we were able to identify 16 additional new protocol patterns; these are depicted in Table 1. We argue that many more can be potentially discovered with our system.

The system is also capable of recognizing the file headers of the most common file types. Hence, by manually inspecting the results, we were able to identify related transactions that contained the remaining parts of the files. In total, we were able to reconstruct four images: 1 PNG, 1 JPG, and 2 GIF's (see Figure 3), by identifying the various transactions that they were split into (due to the operator's size limitations) and concatenating the hex data in a reverse order.

Identifier	Total Out.	Potential Source
VX	16,783	Unknown
POET	13,987	po.et
ChainX	10,705	chainx.org
RSKBLOCK	10,555	rsk.co
Safex1, Safex2	7,090	safex.io
DC-L5	3,142	Unknown
PEIRMOBILE.COM	1,442	peirmobile.com
PHOTECTOR.COM	1,225	photector.com
POTX	1,042	Unknown
BERNSTEIN	974	bernstein.io
POR	858	Unknown
euklid-orders	807	euklid.uk.com
btt	661	Unknown
J_	371	Unknown
CRED	205	mycred.io
CERT	57	Unknown
Total	**69,904**	-

Table 1: Newly detected OP_RETURN protocols

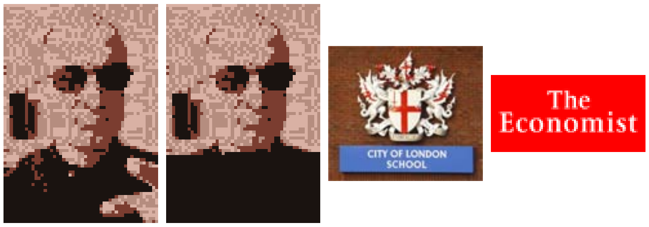

Figure 3: Images identified in the OP_RETURN operator

3 CONCLUSION

The OP_RETURN Bitcoin operator can be exploited for various malicious (and benign) purposes. In this paper, we present a system that analyzes and visualizes the usage of the operator. In addition, our system provides the user with advanced searching capabilities that can assist for the identification of protocols using (misusing) the operator (see Table 1). We welcome the reader to explore the Bitcoin's OP_RETURN operator via our proof of concept website[4] or make use of the open-source code for their own deployment[5].

REFERENCES

[1] Syed Taha Ali, Patrick McCorry, Peter Hyun-Jeen Lee, and Feng Hao. 2018. ZombieCoin 2.0: managing next-generation botnets using Bitcoin. *International Journal of Information Security* 17, 4 (2018), 411–422.

[2] Massimo Bartoletti and Livio Pompianu. 2017. An analysis of Bitcoin OP_RETURN metadata. In *International Conference on Financial Cryptography and Data Security*. Springer, 218–230.

[3] L. Böck, N. Alexopoulos, E. Saracoglu, M. Mühlhäuser, and E. Vasilomanolakis. 2019. Assessing the Threat of Blockchain-based Botnets. In *2019 APWG Symposium on Electronic Crime Research (eCrime)*. 1–11.

[4] Tooba Faisal, Nicolas Courtois, and Antoaneta Serguieva. 2018. The Evolution of Embedding Metadata in Blockchain Transactions. In *Proceedings of the International Joint Conference on Neural Networks*. https://doi.org/10.1109/IJCNN.2018.8489377 arXiv:1806.06738

[5] Roman Matzutt, Jens Hiller, Martin Henze, Jan Henrik Ziegeldorf, Dirk Müllmann, Oliver Hohlfeld, and Klaus Wehrle. 2018. A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin. In *Lecture Notes in Computer Science*. https://doi.org/10.1007/978-3-662-58387-6_23

[6] Elias Strehle and Fred Steinmetz. 2020. Dominating OP Returns: The Impact of Omni and Veriblock on Bitcoin. Blockchain Research Lab.

[3] https://www.omnilayer.org/ (accessed 2020-06-29)

[4] https://op-return.net/ (accessed 2020-06-30)

[5] The source code of the various components used in this project can be found on GitHub: https://github.com/Bitcoin-OP-RETURN (accessed 2020-06-30)