International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Framework for Realtime Bitcoin Transaction

Ramesh G[1], Srivatsan R P[2], Ranjith Kumar R[3] , Sakthi Balan J R[4]

[1]*Professor, Dept. of Information Technology, K.L.N. College of Engineering, Tamil Nadu, India*
[2,3,4]*Student, Dept. of Information Technology, K.L.N. College of Engineering, Tamil Nadu, India*

Abstract - *Bitcoin has emerged as the most successful crypto currency since its appearance back in 2009. A Blockchain, originally block chain, is a growing list of records, called blocks, that are linked using cryptography. Receiving live bitcoin transaction data from web socket and streaming the transaction log to kafka. Analyze the transactions in realtime and count the rate of transactions on a given minute, save this in redis. Consume the transactions from a kafka consumer and persisting(Data Analytics) only the transactions made in the last 3 hours.*

Key Words: **Bitcoin, Blockchain, Bitcoin Live Transaction, Transaction Graph, Transaction Analysis, Kafka, Redis.**

1. INTRODUCTION

Bitcoin is a cryptocurrency. It is a decentralized digital currency without a central bank or single administrator that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.

Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain. Bitcoin was invented in 2008 by an unknown person or group of people using the name Satoshi Nakamoto and started in 2009. When its source code was released as open-source software. Bitcoins are created as a reward for a process known as mining. They can be exchanged for other currencies, products, and services. Research produced by University of Cambridge estimates that in 2017, there were 2.9 to 5.8 million unique users using a cryptocurrency wallet, most of them using bitcoin.

Bitcoin has been criticized for its use in illegal transactions, its high electricity consumption, price volatility, and thefts from exchanges. Some economists, including several Nobel laureates, have characterized it as a speculative bubble. Bitcoin has also been used as an investment, although several regulatory agencies have issued investor alerts about bitcoin.

2. The Bitcoin system

In this section, we point out the main ideas that allow to understand the basic functionality of the bitcoin virtual currency. Such background is needed to understand the meaning of the research performed so far. However, the complexity of bitcoins makes impossible to provide a fully description of the system in this review, so interested readers can refer to for a detailed and more extended explanation on the bitcoin system.

Bitcoin is a cryptocurrency based on accounting entries. For that reason, it is not correct to look at bitcoins as digital tokens since bitcoins are represented as a balance in a bitcoin account. A bitcoin account is defined by an Elliptic Curve Cryptography key pair. The bitcoin account is publicly identified by its bitcoin address, obtained from its public key using an unidirectional function. Using this public information users can send bitcoins to that address[3]. Then, the corresponding private key is needed to spend the bitcoins of the account. Regarding this definition, it is easy to understand that any user can create any number of bitcoin addresses (generating the key pair) either using any standard cryptosoftware or self purpose created programs, like bitcoin wallets. Notice that if the user creates such bitcoin accounts in a private manner then, a priori, nobody can link the identity of the user with the value of a bitcoin address.

3. Bitcoin Anonymity

Anonymity is probably one of the properties that has been key for the success of the currency deployment. Anonymity in the bitcoin network is based on the fact that users can create any number of anonymous bitcoin addresses that will be used in their bitcoin transactions. This basic approach is a good starting point, but the underlaying non anonymous Internet infrastructure, together with the availability of all bitcoin transactions in the blockchain, has proven to be an anonymity threat. In order to review the papers published on bitcoin anonymity, we group them in three different categories: those papers that exploit mainly data obtained from the blockchain to derive some information from users or more general properties like usage patterns; papers that use bitcoin network

information to identify users; and papers that propose mixing techniques to protect users anonymity.

3.1.Blockchain Analysis

A direct approach to analyze the anonymity offered by the bitcoin system is to dig information out of the blockchain. Since the blockchain includes all transactions performed by the system, a simple analysis provides information from which bitcoin addresses the money comes and to which bitcoin addresses it goes. However, since users in the bitcoin system can create any number of addresses, the main goal is to cluster all addresses in the blockchain that belong to the same user. As we will see, authors apply different techniques to perform such clustering.

The first research article on Bitcoins was published by Reid and Harrigan , a first version of which appeared in arXiv in July 2011. From the blockchain information, authors construct the transaction network and the user network. The former represents the flow of bitcoins between transactions, where each vertex represents a transaction and each directed edge indicates whether or not there is an input/output address that links the transactions. The latter represents the flow of bitcoin users over the time. To construct the user network, authors cluster addresses of the same user assuming that all input addresses of a transaction belong to the same user. Then, external information on bitcoin addresses is obtained from different Internet resources (like twitter posts, forums, specialized bitcoin applications -like bitcoin faucet-) to help the clustering process and to identify the users behind such clusters.

3.2.Traffic Analysis

As we already mentioned, the anonymity degree of users in the bitcoin system is also bounded by the underlying technologies used. Transactions in the bitcoin system are transmitted through a P2P network, so, as it was first pointed out in [2], the TCP/IP information obtained from that network can be used to reduce the anonymity of the system. Although it is true that most wallets are able to work over anonymous networks a high number of bitcoin users do not use such services, and then, there is still room for network analysis.

Koshy *et alter* [12] perform an anonymity study based on real-time transaction traffic collected during 5 month. For that purpose, authors develop CoinSeer, a bitcoin client designed exclusively for data collection. For more than 5 million transactions, they collected information on the IP address from where the CoinSeer received such transaction and, in the general case, they assigned as the IP corresponding to the transaction the one that broadcast the transaction for the first time. In order to perform a pure network analysis, authors do not apply any address clustering process, so only single input transactions (almost four million) are taken into account in the analyzed data set. Then, to match an IP with a bitcoin address, they consider a vote on the link between IP_i and $address_j$ if a transaction first broadcasted form an IP_i contains the bitcoin $address_j$ as input address. Authors also perform a similar analysis for output addresses and model the problem as an evaluation of association rules, identifying the corresponding confidence scores and the support counts for the rule. After their analysis, authors conclude that it is difficult to map IP addresses with bitcoin addresses by performing traffic analysis if bitcoin peers act properly, since the bindings authors could obtain between IP addresses and bitcoin addresses mainly come from anomalous transactions patterns. Furthermore, authors also indicate that some network configuration, like mixing services or e-Wallets, might conduct to erroneous assumptions when linking IP and bitcoin addresses.

In contrast to blockchain analysis, traffic analysis has received less attention from the researches probably due to the fact that the blockchain is ready available for analysis and network data has to be gathered. In fact, bitcoin network analysis is a hard topic due to the dynamism and size of such P2P network. The anonymity analysis performed by Koshy *et alter* seems to show that no information can be derived with this technique, but it is difficult to completely discard such approach since in their work authors do not provide any estimation regarding which part of the bitcoin P2P network represent the 2,678 peers they were able to monitor, and for the period of the analysis, no data of the size of the network is available from other sources. So, with only one work performed, whether or not network analysis can reveal private information from bitcoin users still remains an open problem. Furthermore, network analysis can be performed to identify not only the owner of an address but also the identity of other actors in the bitcoin community.

Proposed System

The proposed system will recieve live bitcoin transaction data from web socket and streaming the transaction log to kafka(Data pipeline). Analyze the transactions in realtime and count the rate of transactions according to needs, and store in database(Redis). Consume the transactions from a kafka consumer and persisting(Data Analytics) only the transactions made in the last 3

hours.Displaying the output in Python Flask(Framework) with tools that enable research, analysis, monitoring and order execution.

Restful API Configuration

A **RESTful API** is an application program interface (**API**) that uses HTTP requests to GET, PUT, POST and DELETE data. An **API** for a website is code that allows two software programs to communicate with each another .The websocket connection for bitcoin streaming is taken from **wss://ws.blockchain.info/inv**.Receive new transactions for a specific bitcoin address.

```
{"op":"addr_sub", "addr":"$bitcoin_address"}
```

API Execution

Display latest 100 transactions

http://127.0.0.1:5000/transactions

Display number of transactions per minute for the last hour http://127.0.0.1:5000/count_per_minute

4. CONCLUSIONS

Bitcoin is a payment system based on a decentralized architecture that provides a mechanism to obtain multiple anonymous credentials, bitcoin addresses, that can be used to perform and receive payments.

Furthermore, if one of the addresses of the cluster can be mapped to a real identity, then the payment history of the entire cluster may disclose relevant information of that user. Although interesting research has been performed in this topic, the dynamism of the bitcoin ecosystem that constantly modifies and enhances the bitcoin usage implies that some of the hypotheses assumed for those blockchain analysis may not completely hold and, for that reason, blockchain analysis still presents interesting open questions.

Apart form the blockchain analysis, anonymity of the bitcoin system can be analyzed by gathering information from the P2P network used for payment communication. Since the P2P network uses the TCP/IP protocol, traffic analysis may reveal private information from users. However, such analysis is much more difficult to perform than the blockchain analysis since the bitcoin P2P network is highly dynamic.

Finally, it is worth mention that research in the bitcoin ecosystem can be performed in other topics than anonymity, like for instance cryptography, network security or P2P network to name a few. On the other hand, besides the research lines that can be performed directly on the study of the bitcoin system itself, other approaches perform research using the bitcoin system as a tool.

Acknowledgements

This work was partially supported by the Spanish Ministerio de Ciencia y Tecnologia (MCYT) funds under grants TIN2010-15764 “N-KHRONOUS” and TIN201127076-C03 “CO-PRIVACY.

REFERENCE

[1] Giancarlo Giudici1,Alistair Milne,Dmitri Vinogradov, Cryptocurrencies: market analysis and perspective https://doi.org/10.1007/s40812-019-001386 Published online: 17 September 2019 .

[2] WEF. (2018). Trade Tech—A new age for trade and supply chain finance, The World Economic Forum in collaboration with Bain & Company. World Economic Forum, January 2018. http://www3.wefor um.org/docs/White_Paper_Trade_Tech_report_201 8. pdf. Accessed 14 Sept 2019.

[3] Adhami, S. & Guegan, D. (2020). Crypto assets: the role of ICO tokens within a well-diversified portfolio. Journal of Industrial & Business Economics **(forthcoming)**.

[4] Goldstein, I., Wei Jiang, W., & Karolyi, G. A. (2019). To FinTech and Beyond. The Review of Financial Studies, 32(5), 1647–1661. https://doi.org/10.1093/rfs/hhz025.

[5] Baliga, A. (2017). Understanding Blockchain Consensus Models. Persistent White paper. https://pdfs. semanticscholar.org/da8a/37b10bc1521a4d3de925d 7eb c44bb606d740.pdf. Accessed 14 Sept 2019.

[6] Bessembinder, H., & Seguin, P. J. (1993). Price volatility, trading volume, and market depth: Evidence from futures markets. Journal of financial and Quantitative Analysis, 28(1), 21–39.

[7] Cukierman, A. (2019) Welfare and political economy aspects of a central bank digital currency. Centre for Economic Policy Research, discussion paper DP13728, May 2019.

[8] Glaser, F., Zimmermann, K., Haferkorn, M., Weber, M. C., & Siering, M. (2014). Bitcoin-asset or currency? revealing users' hidden intentions. Revealing Users' Hidden Intentions (April15, 2014).ECIS.

[9] Milne, A. K. L. (2018) Argument by False analogy: The mistaken classification of Bitcoin as token money (November25, 2018). https://ssrn.com/abstract=3290325.

[10] Richter, C., Kraus, S., & Bouncken, R. C. (2015). Virtual currencies like Bitcoin as a paradigm shift in the field of transactions. International Business & Economics Research Journal, 14(4), 575–586.

[11] Akyildirim, E., Corbet, S., Katsiampa, P., Kellard, N., & Sensoy, A. (2019). The development of Bitcoin futures: Exploring the interactions between cryptocurrency derivatives. Finance Research Letters. https://doi.org/10.1016/j.frl.2019.07.007.**(in press)**.

BIOGRAPHIES

Mr.Srivatsan R P is a final year student of Department of Information Technology, K.L.N College of Engineering, Sivaganga.

Mr.Ranjith Kumar R is a final year student of Department of Information Technology, K.L.N College of Engineering, Sivaganga.

Mr.Sakthi Balan J R is a final year student of Department of Information Technology, K.L.N College of Engineering, Sivaganga.

Dr.G.Ramesh is working as professor in Department of Information Technology, K.L.N College of Engineering, Sivaganga.