WalletRank Final Report

Team 105: Rizki Wicaksono, Mani Narasimhan, Jennifer Evans, Siddharth Seth

# 1. Introduction

## 1.1 Motivation

The anonymity of bitcoin offers positive benefits, but can attract fraudulent or even illegal activities. Governments are beginning to regulate financial institutions’ bitcoin involvement. “Know Your Customer”, “Anti Money Laundering”, and “Counter Terrorism Financing” are some common regulations that financial institutions have to comply with when using bitcoin. Unfortunately, the anonymity of bitcoin makes regulatory compliance and enforcement difficult. We propose a Bitcoin Wallet “Credit Score” called WalletRank to measure risk of doing business with a wallet-holder. Similar to the credit score used to measure creditworthiness, WalletRank can measure risk before conducting a bitcoin transaction.

## 1.2 Problem Definition

Given a graph G = (V,E), find a score between [0,1] for every vertex in set V. Lower scores have less risk, higher scores have more risk. This will be mapped to a user-friendly number scale on par with Consumer Credit score.

# 2. Literature Survey

## 2.1 Origination: Bitcoin and Ethereum Whitepapers

**Bitcoin Whitepaper**

On October 31, 2008 anonymous author Satoshi Nakamoto published the “Bitcoin Whitepaper” describing Bitcoin: a peer-to-peer cashless electronic payment system based on a new cryptographically secure, non-repudiable consensus protocol, called Blockchain.[1] We extend this work providing a meta-analysis of bitcoin transactions.

**Etherium Whitepaper**

In 2014, Vitalik Buterin, wrote “Etherium Whitepaper” describing decentralized applications and smart contracts built using a Turing-complete programming language on a new blockchain protocol: Etherium.[2] This concept foreshadows the direction of our project: We provide an application auditing Bitcoin via a meta-analysis of Bitcoin transactions.

**Ripple: Competition**

Newer blockchain-based protocol, Ripple, was introduced in a 2014 paper. It’s a direct competitor to Bitcoin because its global distributed payments system has low convergence latency, allowing a broader set of transactions.[3] This paper provides impetus for expanding the proposed WalletRank beyond Bitcoin if proven successful.

## 2.2 Security and Privacy Using Blockchain

**Decentralizing privacy: Using blockchain to protect personal data**

Inspired by increases in user data privacy breaches, the paper implements a new automated access control manager using a blockchain ledger. Our project can use the ledger thought process and implementation as inspiration. [4]

**Blockchain for IoT security and privacy: The case study of a smart home.**

IoT devices don’t have strong computational power and traditional blockchain concepts won't work. The paper proposes a smart home system without the Proof-of-Work concept, introducing unique uses of blockchain our project could analyze. [5]

**Hawk: The blockchain model of cryptography and privacy-preserving smart contracts.**

The blockchain ledger records pseudonyms and transactions amounts, making the system not completely financially anonymous. Hawk attempts solving the financial transparency problem by implementing a private smart contract system using a cryptographic protocol to maintain anonymity. [6]

## 2.3 Fundamentals, Sustainability and Fraud Detection

**Sustainability of Bitcoins**

This paper addresses sustainability of bitcoins from different perspectives: Environmental, Social and Economic. The energy requirements (KWh) and environmental impact for Bitcoin mining is valid for our research because it raises questions of Bitcoin sustainability. [7]

**Bitcoin: Technical Background and Data Analysis**

This paper covers the fundamentals of Bitcoin technology providing results on usage, value, volume and velocity of Bitcoins. It would be good to validate the usage pattern of Bitcoins with current data and explore the products or services bought using bitcoins. [8]

**Fraud detections for online businesses**

This paper discusses how Blockchain technology can eliminate objective fraud such as loan application fraud while mitigating subjective or other types of rating fraud. The authors address the privacy concerns of users due to the possibility of retaliation. This is relevant because it provides a broader perspective on the technology. [9]

## 2.4 Anomalous and Suspicious transaction detections

**Quantitative Analysis of the Full Bitcoin Transaction Graph**

This paper discovered interesting transaction graph structures. Some structures they discovered would be useful in our project to develop algorithms for discovering suspicious transactions. This paper is a bit dated, we hope to see more interesting results in our project. [10]

**Anomaly Detection in Bitcoin Network Using Unsupervised Learning Methods**

This paper uses unsupervised learning like k-means clustering to discover anomalous bitcoin transactions. This is useful for our project to discover anomalous transactions. This paper only has 30 known cases, we hope to find more in our project. [11]

**Detecting suspicious behavior in the Bitcoin network**

This paper analyzed bitcoin network to find suspicious behavior using Markov logic network that might be useful in our project. The authors analyzed a subset of the bitcoin network due to huge search space; we will attempt to analyze full bitcoin network.[12]

## 2.5 Guilt-by-Association and PageRank

**Data Mining Meets HCI: Making Sense of Large Graphs**

Prof. Polo Chau’s thesis is relevant to our problem as it describes the application of belief propagation networks in various situations, especially malware detection. We believe this solution may be applied to find malicious actors in the blockchain ecosystem. [13]

**Combating Web Spam with TrustRank**

This paper gave us the idea to use a similar algorithm, Personalized PageRank (PPR), based on the concept that a set of good sites influence neighboring sites or “trust-by-association”. We decided to use PPR for WalletRank, with guilt-by-association rather than trust-by-association. [14]

**Unifying Guilt-by-Association Approaches: Theorems and Fast Algorithms**

This paper reviews the guilt-by-association algorithms class, which all have the same basic idea: a node in a graph may be influenced by neighboring nodes. For example: a friend of a thief might also be a thief. This concept is directly applied to the problem of labeling a bitcoin wallet as bad or good based on their neighbors. [15]

# 3. Proposed Method

**Intuition:**

Currently, the mechanism for identifying bad actors within the Bitcoin community is to rely on manual reporting by people who have experienced a problem with a particular wallet (end-user). These are listed on bitcoinabuse.com for people to check before doing business with a particular wallet. The list includes those wallets used to collect money from Ransomware, extortion schemes and other criminal activity. There is an API to both report automatically, and to check if a wallet is on the reported list. However, even though an API exists, this process still requires an actual effort to identify and report a wallet, or to check if someone has reported. It does not “predict” potentially bad wallets, nor does it produce a risk score for them.

**Description of Approach, Algorithm and UI:**

This project is about assessing transaction risk with particular wallet addresses in a quantitative way. In other words, we are trying to quantify risk for each bitcoin wallet address such that a user would be able to gauge the risk of doing business before sending bitcoin to the wallet. We propose using PPR algorithm to find vertices of interest and those nearby vertices of interest. We label known “bad” vertices with a score of 1.0 and allow PPR to “taint” nearby vertices with their bad reputation.

When the algorithm achieves a measure of stability, we have a majority of the vertices which are good near 0.0, those that are bad at 1.0 and those which are suspect somewhere above 0.2. Once we learn the PPR score for each wallet, we can calculate a risk score based on PPR and other features (age, number of transactions, average transacted amount) from historical data pertaining to this particular address. Figure 1 shows the WalletRank calculation.

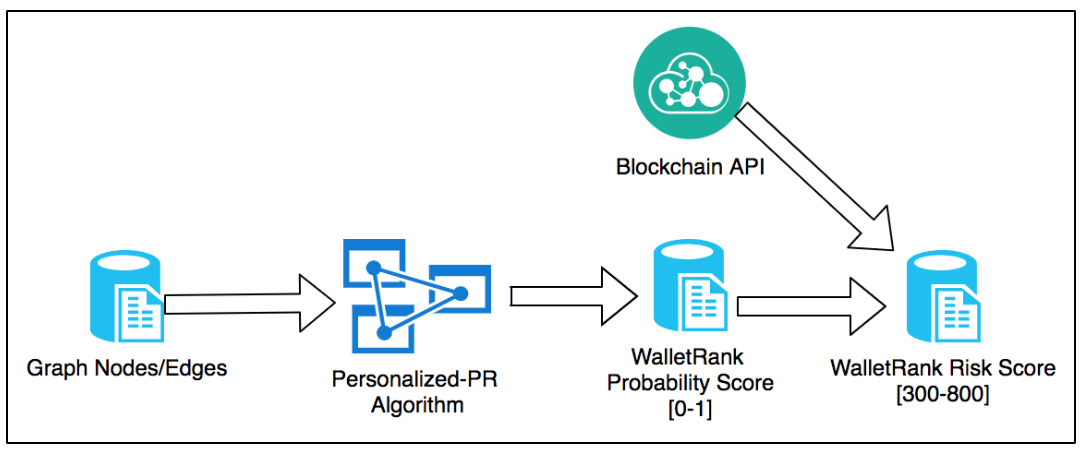
****

Figure 1: WalletRank analytics process

**Our Innovation and Contribution**

* Intuitive and user friendly risk score even for novice users
* Automated way to quantify risk of every bitcoin wallet address based mainly on personalized PageRank algorithm
* Interactive visualization of bitcoin transactions allows user to inspect interesting wallets and transactions

**Data Acquisition and Preparation**

As shown in Figure 2, data acquisition and preparation procedures begin with public BigQuery bitcoin transactions tables followed by series of transformations and preparations to make an edge file usable by memory-mapped pagerank algorithms.

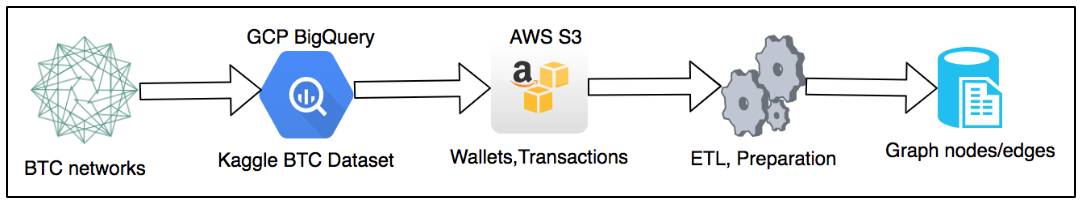
****

Figure 2: Data acquisition and preparation flow

We also exported the list of known (reported) malicious wallets from bitcoinabuse.com to use for seeding our PPR algorithm with wallets of “interest”. We also did data transformations and preparations to make wallets list usable by pagerank algorithm.

Full details of data acquisition and transformation for both bitcoin transaction graph and known bad wallets are detailed in this markdown document: <https://gist.github.com/rzwck/caee8c74ffa20b1e076a8913d18ac349>.

Transformed data is available on the public S3 folder: <https://s3.console.aws.amazon.com/s3/object/team105/>

|  |  |  |
| --- | --- | --- |
| S3 Filename | Description | Link to File |
| id\_address\_pairs.csv | Graph nodes containing mapping of ID (integer) and wallet addresses (string) | s3://team105/id\_address\_pairs.csv |
| bad\_addresses.csv | List of wallet ID (integer) manually reported as malicious on bitcoinabuse.com | s3://team105/bad\_addresses.csv |
| srcid\_dstid\_pairs\_sortby\_srcid.csv.gz | Graph edges containing pairs of integer source\_id and integer destination\_id sorted by source\_id. | s3://team105/srcid\_dstid\_pairs\_sortby\_srcid.csv.gz |
| srcid\_dstid\_pairs\_sortby\_srcid.bin.gz | Graph edges in little-endian binary format (gzipped) | s3://team105/wallet-pagerank/srcid\_dstid\_pairs\_sortby\_srcid.bin.gz |
| srcid\_dstid\_pairs\_sortby\_srcid.idx.gz | Nodes degrees in big-endian binary format (gzipped) | s3://team105/wallet-pagerank/srcid\_dstid\_pairs\_sortby\_srcid.idx.gz |
| srcid\_dstid\_pairs\_sortby\_srcid.json | Details about graph binary files | s3://team105/wallet-pagerank/srcid\_dstid\_pairs\_sortby\_srcid.json |

**User Interface Design**

WalletRank is available through an online application that visualizes the data and allows users to interact with it. The application is based on ReactJS and uses D3 for visualization. We deployed the application here: <http://ec2-54-67-52-170.us-west-1.compute.amazonaws.com/>

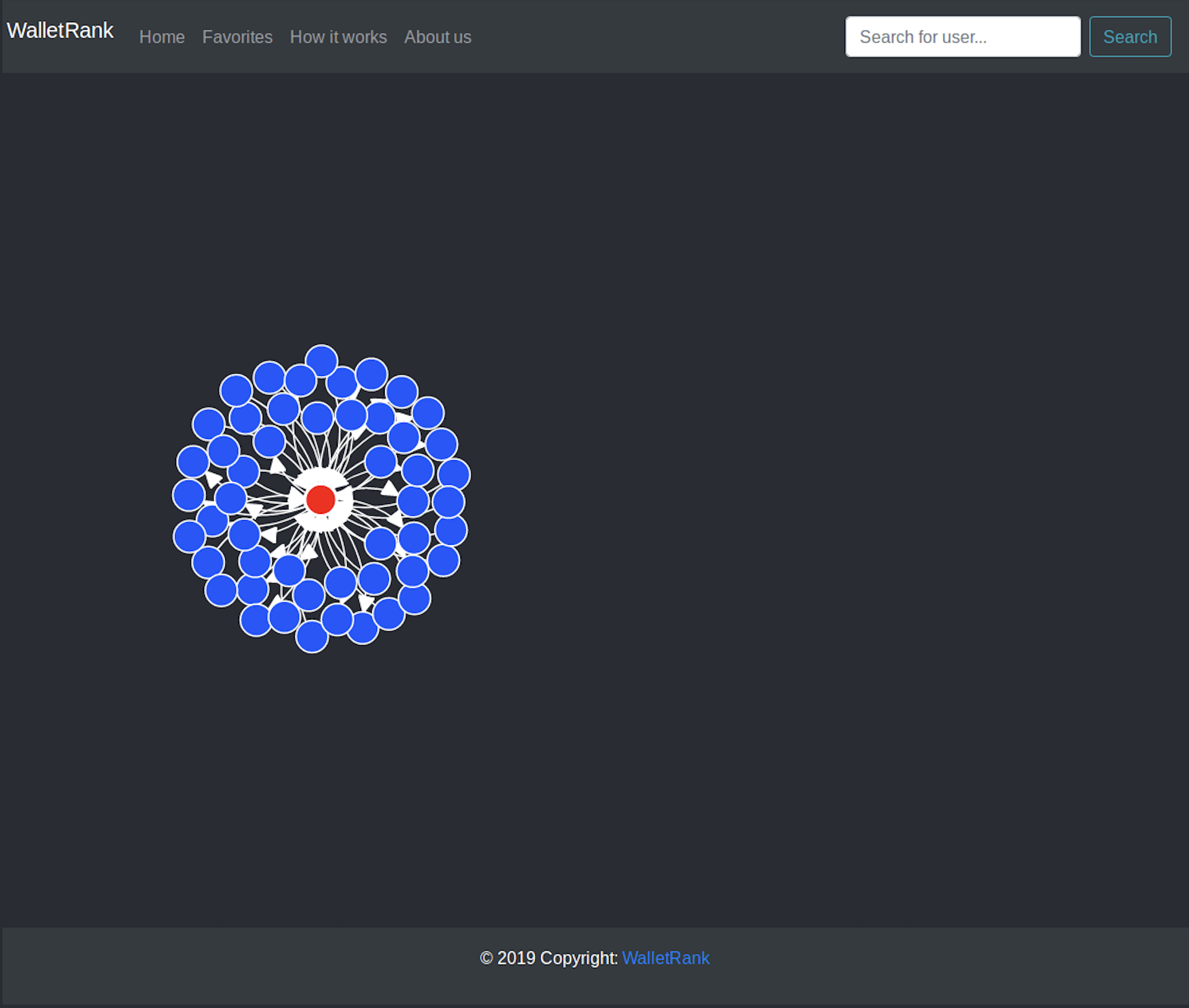


Figure 3. UI of WalletRank application

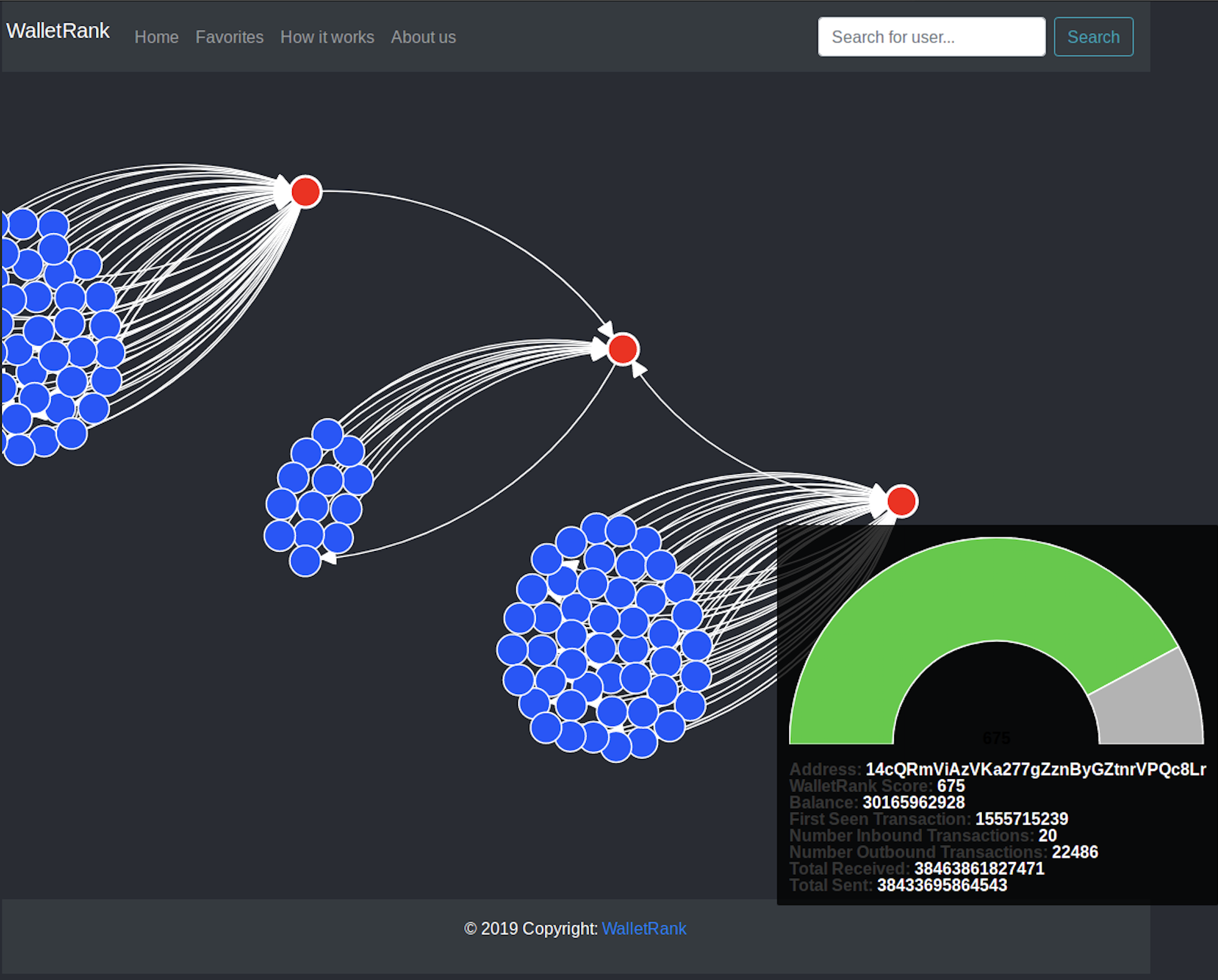


Figure 4. Viewing Wallet Score in WalletRank

The application shows a graph of the wallet nodes the have been analyzed. These nodes can be visualized based on their wallet score and transactions history. In addition, users can search for a specific wallet to learn more about its transactions and history. Code to replicate this UI is available on Github here: <https://github.com/siddharthseth/wallet-rank>

# 4. Experiment Design

**Testbed: What are we attempting to discover?**

If we label bad actors on certain vertices which are known to have caused problems, we wish to understand how the flow of that negative reputation will propagate through the network. In particular, we suspect nearly neighbors will be highly affected (2-3 hops away from bad actor vertices). But it is less clear what will happen 20-30 hops away? How far will the negative reputation propagate? Can we actually discover new, unreported wallets controlled by people with malicious intent?

**Details of the experiments; observations:**

We have collected the raw data, processed and cleaned it, and we have a full-scale run of Personalized PageRank (PPR) on the full bitcoin dataset. We fed the data for known malicious wallets from BicoinAbuse.com-reported wallets into the algorithm to “tag” the wallets of interest. We also fed the full dataset of all wallets and transactions for the year including Sep 2017 - Sep 2018. These wallets can be considered nodes, and transactions can be considered edges, forming a directed graph. This directed graph and the list of malicious wallets, supplied to the PPR algorithm produces a score for each node in the graph between [0, 1]. This successfully worked when we ran the full algorithm and each node was identified with a score. Scores for known bad (reported) wallets were set to 1, and we looked at the top 25 wallets that were predicted bad by the algorithm.

Previously unreported malicious/potentially malicious wallets were found by investigating a number of other sites which were of ill repute and also mentioned these wallets (common bitcoin scammer websites such as bitcoindoubler.com). We found among these 8 previously unknown (not reported on Bitcoinabuse.com) malicious wallets, and 11 previously unknown potentially malicious wallets. Only 5 were found not to be malicious. It seems the PPR algorithm is, in fact, able to predict new bad actors based on association with the known ones, confirming our major hypothesis.

This method and result appears to be state of the art versus the manual ad-hoc after-the-fact reporting methods that exist today. Malicious wallet prediction is now possible.

Observations include the findings for the top 25 highest scoring PPA wallets (i.e. most likely to be malicious) in Table 1 below:

Table 1: New Findings from WalletRank (PPA) analysis of Bitcoin Data and Known Bad Actors

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Wallet Address** | **WalletRank** | **Findings** | **Types** | **New** |
| 1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s | 300 | Malicious | Blackmail | No |
| 12cgpFdJViXbwHbhrA3TuW1EGnL25Zqc3P | 300 | Not Malicious | - | - |
| 1KSuWHN6Hc36tJmYtk4RyAbkKDtNjACRX9 | 300 | Malicious | Scam | Yes |
| 1FoWyxwPXuj4C6abqwhjDWdz6D4PZgYRjA | 300 | Malicious | Scam | Yes |
| 1JUToCyRL5UwgeucjnFAagKs4v1YqhjT1d | 300 | Potentially Malicious | Anomalous | Yes |
| 1DUb2YYbQA1jjaNYzVXLZ7ZioEhLXtbUru | 300 | Malicious | Scam | Yes |
| 1Fu3iBR2EMQWeYGi3XvrPmcPUkne8ZWj9h | 300 | Malicious | Hacked | No |
| 1LhWMukxP6QGhW6TMEZRcqEUW2bFMA4Rwx | 300 | Potentially Malicious | Anomalous | Yes |
| 1G47mSr3oANXMafVrR8UC4pzV7FEAzo3r9 | 300 | Malicious | Scam | Yes |
| 1LCAJF94Yxin9eWNx19b5BZnrnBSVstV1g | 300 | Potentially Malicious | Scam | Yes |
| 1Po1oWkD2LmodfkBYiAktwh76vkF93LKnh | 300 | Malicious | Scam | Yes |
| 392LK4ZQD3gixWg5xJRTv1a24N3YDgCbwP | 300 | Malicious | Scam | Yes |
| 1L6zTihRVecCjisYkn6BuXKrwvg8hJFC4f | 300 | Malicious | Scam | Yes |
| 1H6q83MQr9k8c6VezSU8x5oKasABjF4btN | 300 | Potentially malicious | Anomalous | Yes |
| 3QorgsdWKX2CvaMDPH5PvRchoz8s9GM2by | 300 | Not Malicious | - | - |
| 39f5XZ1vRB3Lm187psnrwSikLy8Xmm3DCu | 300 | Potentially malicious | Anomalous | Yes |
| 1PAxSJnxGRWTNSa4NgRbNiQahEMY9KjGJ3 | 300 | Potentially malicious | Anomalous | Yes |
| 3AW42uyi9u4euRKRrcuMzxnUzjSKpJvij4 | 300 | Potentially malicious | Anomalous | Yes |
| 1Kr6QSydW9bFQG1mXiPNNu6WpJGmUa9i1g | 300 | Potentially malicious | Anomalous | Yes |
| 1DcKsGnjpD38bfj6RMxz945YwohZUTVLby | 300 | Malicious | Scam | Yes |
| 1CE5T4P6WmFUQvQFwvedgTEc5Z7BSVJLVN | 300 | Malicious | Hacked | Yes |
| 1ASSo159nbriTnyjPeTicJeW27D9pNSwas | 300 | Potentially malicious | Anomalous | Yes |
| 336xGpGweq1wtY4kRTuA4w6d7yDkBU9czU | 300 | Not Malicious | - | - |
| 3LQxUzikM2rWBhUFrLFNiuWPbPLLJn84DB | 300 | Malicious | Scam | Yes |
| 14V38fi6XLQR78j9ivE561s8VkRXqczs7b | 300 | Potentially malicious | Anomalous | Yes |

Also, we computed the distribution of consumer-friendly wallet rank scores among the population of all wallet IDs. The chart with the distribution is below.

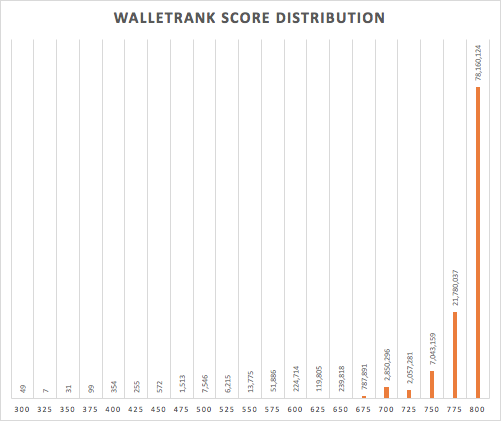


Figure 4. WalletRank “Consumer-Friendly” Score Distribution - All Wallet IDs

# 5. Conclusion and discussion

Overall, we have framed our problem statement as a directed graph where the bitcoin wallet sender and wallet receiver address in a transaction are treated as nodes and the transaction between each node is treated as an edge. We identified that bitcoin transaction data spanning one year would be a reasonable timeframe to glean some insights and have collected data from September 2017 to September 2018. We leveraged the list of known bad actor wallets listed on bitcoinabuse.com to seed the nodes of interest for the Personalized PageRank (PPR) Algorithm. We have applied the PPR algorithm on this dataset to derive the risk score for each address. We have also used the findings from the algorithm to accurately predict unreported bad actor wallets that were previously unknown, due to their association (transactions with) known bad actors. We have converted the PPR score, which is in the range [0,1] to a “user-friendly” score from [300,800] similar to the consumer credit score and have associated the score to each Bitcoin wallet. The data is made available for interaction via an online portal walletrank.com, and individual wallets may be queried and viewed, along with their neighbors.

# 6. Team Efforts

All team members have contributed a similar amount of effort.

# 7. References

[1] Nakamoto, S. (2008, May). Bitcoin: A Peer-to-Peer Electronic Cash System, <https://bitcoin.org/bitcoin.pdf>

[2] Buterin, V. (2014, Oct). A Next-Generation Smart Contract and Decentralized Application Platform, <https://github.com/ethereum/wiki/wiki/White-Paper>

[3] Schwartz, D., Youngs, N., Britto, A. (2014). The Ripple Protocol Consensus Algorithm. Ripple Labs, Inc. <https://ripple.com/consensus-whitepaper/>

[4] Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE* (pp. 180-184). IEEE.

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163223>

[5] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on* (pp. 618-623). IEEE. <https://allquantor.at/blockchainbib/pdf/dorri2017blockchain.pdf>

[6] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016, May). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)* (pp. 839-858). IEEE. <https://www.computer.org/csdl/proceedings/sp/2016/0824/00/0824a839.pdf>

[7] Pasquale Giungato, Roberto Rana, Angela Tarabella and Caterina Tricase: Current Trends in Sustainability of Bitcoins and Related Blockchain Technology. *Sustainability* 2017, *9*(12), 2214.

<https://doi.org/10.3390/su9122214>

[8] Badev, Anton I. and Chen, Matthew, Bitcoin: Technical Background and Data Analysis (October 7, 2014). FEDS Working Paper No. 2014-104. Available at SSRN:

<https://ssrn.com/abstract=2544331>or [http://dx.doi.org/10.2139/ssrn.2544331](https://dx.doi.org/10.2139/ssrn.2544331)

[9] Yuanfeng Cai, Dan Zhu: Fraud detections for online businesses: a perspective from blockchain technology. Financial Innovation (2016) 2: 20.

<https://doi.org/10.1186/s40854-016-0039-4>

[10] Ron, Dorit & Shamir, Adi. (2012). Quantitative Analysis of the Full Bitcoin Transaction Graph. 10.1007/978-3-642-39884-1\_2.

[11] Phillip Thai Pham, Steven Lee, *Anomaly detection in bitcoin network using unsupervised learning methods.*

[12] Jobse, Frank. Detecting suspicious behavior in the Bitcoin network. Tilburg University, 2017

[13] Horng, D.J. (2012). Data mining meets hci: making sense of large graphs.

[14] Gyongyi, Zoltan and Garcia-Molina, Hector and Pedersen, Jan (2004) *Combating Web Spam with TrustRank.* In: 30th International Conference on Very Large Data Bases (VLDB 2004), August 29 - September 3, 2004 , Toronto, Canada .

[15] Koutra D., Ke TY., Kang U., Chau D.H.., Pao HK.K., Faloutsos C. (2011) Unifying Guilt-by-Association Approaches: Theorems and Fast Algorithms. In: Gunopulos D., Hofmann T., Malerba D., Vazirgiannis M. (eds) Machine Learning and Knowledge Discovery in Databases. ECML PKDD 2011. Lecture Notes in Computer Science, vol 6912. Springer, Berlin, Heidelberg