ROBOCALLS 2.0

Whitepaper

Jan 16, 2019

Version 2.0

Table of Contents

1. Overview

Spam calls are automatically programmed calls, designed to deliver an already recorded message to, most often, a large group of people. They have been applied for different purposes which include a simple application of information dissemination, network promotions and other functionalities like huge political and telemarketing phone campaigns. Most of these calls are not solicited by the call recipients and are usually undesirable. With the increased volume of calls in recent times, over 147 million per day in the United States, spam calls have grossly increased exponentially.

Several solutions have been designed to curb this menace in the communications industry but have been ineffective or failed entirely, either due to legal problems, hackability and caller ID spoofing, especially when it comes to previously proposed solutions such as Whitelisting/Blacklisting, Captcha and Crowdsourcing. An advanced method proposed to resolve this endemic challenge is to use intelligent real-time analysis techniques coupled with trusted big data to detect and apprehend these spam calls despite their complex change of identities.

This is in fact what Robocalls.io aims to do by coupling the capabilities of the Artificial Intelligence and Blockchain technology. Robocalls.io will use its unique AI algorithm to scan through its user-established and blockchain-secured spam call ID database, to predict unwanted calls based on inbound dialing patterns. Its structure relies on the Ethereum blockchain to validate, notify and block this activity, leveraging this powerful technology, our Algorithm will create the biggest predicted black list database of unwanted and scam numbers in the blockchain.

1.1 Communications Market Overview

Verbal communication is the strongest means of human communication and the most comprehensive and impacting, emotionally. For this sole reason, many have argued that the telephone is one of the greatest communication inventions, although some still argue otherwise. The telephone allows for this verbal communication between parties over unimaginable distances with just a little loss of emotional transfer or impact. This is because from a party's voice in a conversation, the listening party can discern anger, sarcasm and even contract the laughter from the speaking party. With little observation, we notice that when a caller speaks, he usually make gesticulations as if the listener could see him.

Digital marketers have realised this fact and have weaponized it to increase their conversion rates. To reduce stress and increase efficiency, automate some of these tasks, savvy marketers have turned to using bots to deliver pre-recorded messages to their large customer base.

The reduced cost of manufacturing verbal communication devices, in addition to this digital marketer's leverage of spam calls in their marketing tasks has grossly increased the volume of calls globally. The United States alone records over 147 million calls per day. In the United Kingdom, the number of mobile calls increased from 127 billion (in minutes) as at 2009 to 157 billion as at 2017. Statistics reveals that the annual retail revenue from mobile telephony in the United Kingdom in the year 2017 was 15.6 billion GBP approximately.

Unfortunately, spammers, scammers and spoofers are like a cancerous growth in the body of this industry, posing in different forms, even in form of digital marketers. With the use of spam calls, they've managed to constantly sound their campaigns in the ears of phone users, without permission - utterly pestering them. The Federal Communications commission has reported that they receive about 500,000 complaints a month about these spam calls and it's still on the rise. The Federal Trades Commission's Ian Barlow, who oversees the "Do Not Call" registry, recently reported that spam call complaints are the highest received complaints at the commission. In 2018 alone, a robocall watchdog, YouMail, has reported over 16.3 billion spam calls in America.

2. Previous Attempts to Eliminate Spam Calls That Failed

There have been attempts over the years to curb this endemic challenge of spam calls. Unfortunately, the proposed solutions all saw a dead end as the issue prevailed till the time of this report. Some of the previous proposed solutions are discussed below:

2.1 Do Not Call Lists

This is a government maintained database containing phone numbers of individuals and families who do not wish to be called, for any reason by telemarketers. This was meant to remove some select users from the general pool of contacts available to these spammers. Although this has led to some percentage reduction on telemarketing calls, this did not stop digital marketers

from sourcing for numbers to carry out their telemarketing or even violating the "Do Not Call" request.

2.2 Whitelisting/Blacklisting

This method of suppressing spam calls involves users creating their personal database of phone numbers allowed to call them. The software, which may be in the form of a mobile app or a built-in function of a smartphone device, prevents or ends future calls from numbers that have been blacklisted. All numbers before blacklisting are initially on the whitelist for that particular user. The inefficiencies of this method arise from the limited database created by the user, as spam callers can easily change their IDs when they detect any campaign blockages on the previous IDs.

The crowdsourcing model is meant to consolidate this weakness, by sourcing from blacklisted caller IDs from a crowd-sourced database, in order to make the blacklists of users more comprehensive and updated. Truecaller, a mobile app, applies this model. It stores the mustered whitelist/blacklist database of several users. This makes the gathered user-generated whitelist/blacklist available to other users, making it very difficult for these spammers to use the same call ID twice.

Such a model has one primary flaw and that is, centralization of database. Not only does this cause valuable data to be shut behind closed doors of some select spam calls blocking service providers, hoarding it from their competition who could have provided better services with a different and more innovative method, it makes the database an easy target for hackers. Hackers that may have been hired by telemarketers or are telemarketers themselves, to get genuine call IDs so they can spoof with them. 2013 proves true this point, as Truecaller reported that its database was hacked.

2.3 Captcha

A Captcha is a computer program that helps differentiate between a human input and a machine's in order to reduce spam or automation in the selected niche used. They are commonly found in websites during logins, either as poorly written

letters which needs to be rewritten by the user or as multiple images that requires users to identify images containing a particular object or place out of the entire image matrix.

This mechanism was applied to spam calls, to validate calls from already suspected numbers. It challenges them to go through a verbal verification process which may involve saying some different words or the caller's Identification. When it involves the callers ID, the recording will be played for the recipient, who could decide to accept, decline or even report the call. This mechanism however failed due to the long protocol and the undesirable process it makes real callers to pass through.

2.4 A VoIP Validation & Authentication System

The FCC proposes that the complete solution to these spam calls is a framework that involves a network level validation system of all calls over the internet and also signing in of all calls made over the internet, to allow Network carriers identify spam calls. A validation system on calls over in the internet would, make sure that no call is initiated unnoticed and such calls would get to the customer only with the network's carrier's permission and say a user reports a spam call, it can easily be traced back to the source.

Compliance of the industry to this FCC proposal has been quite slow. The proposal was made in 2015, targeted at being fully achieved by 2017. It is still yet to be achieved. Precisely November 6, 2018, the FCC wrote letters to voice providers to remind and encourage them to raise their "Traceback" efforts which would combat spam calls. An interesting part of this letter report is the part which mentions that the government needs the industry to fight these spam calls. However, the industry is not yet responsive to this call, leaving the truckload of the spam calls problem on the shoulders of the government.

3. The Robocalls 2.0 Solution

Robocalls.io implements all the strengths of the previous solutions coupled with that of the future propositions to produce an almost perfect spam calls combating solution. It is the summation of Blacklisting/Whitelisting, Crowdsourcing, VoIP validation system and Real-time Intelligent analysis to combat spam calls.

By coupling the capabilities of artificial intelligence (AI) and blockchain technology, Robocalls 2.0 will use its unique AI algorithm to scan through its user established and blockchain secured spam call ID database, to predict unwanted calls based on inbound dialing patterns. The structure relies on the Ethereum blockchain to validate, notify, and block this activity. Leveraging this powerful technology, our algorithm will create the biggest predicted black list database of unwanted and scam numbers in the blockchain.

3.1 Real-time Analysis

Until full compliance with the FCC proposal, Artificial intelligence remains the best method to stop the spam calls. This would involve fetching out the call behavior patterns buried in a big data sample of call IDs, predicting the next one and stopping them even before it gets to the next victim. This call blocking method basically uses complex AI algorithms to understand call behavior patterns and fights the spammers, from its wealth of database. This is therefore one of the tools Robocalls.io proposes to integrate into the system in order to tackle spam calls.

3.2 Robocalls 2.0 and the Blockchain Technology

The blockchain technology is the brainchild of the anonymous Satoshi Nakamoto. It was birthed in Oct 31 2009. The birth of this technology made possible true Peer to Peer (P2P) transactions by eliminating any centralized authority that was previously involved. The technology creates a trusted network that validates value transactions between peers via consensus protocols, where key nodes agree on the truth of time-stamped transactions. The credibility of the network also arises from its time proven solid security. To hack the blockchain, one needs to have a mining power greater than the mining power of all the nodes combined which is practically impossible as it is cost inhibitive. This is because altering a

blockchain recorded transaction would involve changing all others before it, since its beginning, because they are all hashed together.

Robocalls 2.0 will use this trust machine, as the blockchain has been popularly dubbed to created unique identities of callers which cannot be altered. Caller IDs attached to a particular phone stays that way, forever and if a call recipient bans a particular caller ID via Robocalls.io, it stays that way, it would be impossible for the spam or scam or both ID to reach that customer by spoofing a new ID.

Unlike the central database storage of Truecaller which was hacked, utilizing the decentralised nature of the Blockchain, Robocalls.io makes it practically impossible for a successful hack. Data sharding, which involves splitting data, encrypting and storing pieces of it at different locations have proved to be a much secured form of storing information. Projects like Storj, IPFS, have already proved this. When required, the data pieces are assembled back together, decrypted and accessed via private keys, which are only known to the database owners. In other words, Users have complete control of their spam and scam robocallers database with Robocalls.io and can trade it to Robocalls.io for the Robocalls 2.0 tokens (RC20).

From a slightly different perspective, Robocalls 2.0 creates a data sharing economy with the blockchain technology. Centralized mountains of data will be in the past with Robocalls.io. The protection this creates for data is just a minor benefit when compared with the benefit of data flow that it will create. The ecosystem of Robocalls.io will allow companies with mountains of data, Like Truecaller, Nomorobo or Robokiller, secure their data and also build a business model around it as they can trade or rent this data for RC20. By enabling this, we can see that with blockchain technology, Robocalls 2.0 creates an ecosystem where spam and scam calls database are secure and fluid, enabling channels for Customer to Buyer (C2B) and Buyer to Buyer (B2B) exchange, a more effective means or model or crowdsourcing blacklists/whitelists.

With the severity of these spam calls of late, Robocalls 2.0 will be an effective tool for the government to incentivize the industry and encourage their participation. Also, the validation and authentication system proposed by the FCC have a larger chance of being implemented through Robocalls 2.0, as it will actualize a trustworthy validation system on the Ethereum network.

3.3 Robocalls.io and Artificial Intelligence

Artificial intelligence (AI) is used to refer to thinking machines. Machines being capable of understanding data input and producing data output, in the form of predictions. AI is much like how humans are trained to think by teachers by providing them with necessary information and become disciplined to solve problems which they've never encountered. Machine Learning is a niche of Artificial Intelligence which involves training this machines with a large data set input to make accurate predictions in the future problems.

Inheriting this ability of AI to predict without human supervision, Robocalls 2.0 aims to intelligently populate its database to create the largest spam and scam robocalls blacklist/whitelist on the blockchain. Considering the volume of calls made per day, this is a huge data exercise, but then it creates an opportunity for the AI algorithm to get more data input to improve its accuracy in predicting and ending spam calls. Based on the Ethereum blockchain which will in no distant future attain scalability, handling the volume of calls, which will be tagged as transactions on the blockchain network will not be a problem.

4. Robocalls 2.0 Products

4.1 The Application

Robocalls 2.0 client app will be available for IOS and Android devices. Once installed in a user's device, it syncs with the Robocalls.io mainnet and downloads the secured spam and scam blacklist, into the device's phone book, with which it would confirm a caller's ID is not blacklisted before allowing call to come through. The application holds the database of the blocked calls and gives the description as to why it's blocked in case users get selective and would like calls from some telemarketers to come through. The database is retrieved daily from the Mainnet, which would contain numbers reported to be spam or/and scam calls and numbers populated the Robocalls 2.0 unique AI algorithm.

4.2 The Wallet

This would serve to store the ERC-20 Robocalls 2.0 tokens (RC20). To keep the application services active, users just need send some tokens from this wallet to a

smart contract address. This wallet may be built into the application or outside of it. P2P value transactions are also easily enabled via the wallet.

4.3 The MainNet

The MainNet will hold a fresh copy of the blacklist ready to respond the validation request from the phone and saving the numbers reported from the mobile client. This database copy will be retrieve from the blockchain in a daily basis and it will contain all the numbers sent by the users.

5. Benefits of using Robocalls 2.0

- ✓ Manage multiple phones and protect them all with a single account.
- ✓ No subscription required, No monthly payment, just a free app.
- ✓ Users will have the benefit of gain free tokens, when they reported scam numbers in our Algorithm.

6. Roadmap Overview

The Roadmap will be updated in the next review of the whitepaper. Stay tuned for further announcements.

Meet The Team!

Jose Ortiz

CEO CoFounder

Prince Nchiba

Project Manager

James Tylee

Advisor / Angel Investor

Maariz Tamminen

Social Media Manager

Shanshann Inocencio

Social Media Lead

Jose Vazquez

Social Regional and International Relations

Grace Isidro

Social Media

Kingsley Bello

Telegram Moderator

Partners!

For More Information Please Visit:

Telegram Group: ***https://t.me/httprc20token***
Announcement Channel: ***https://t.me/robocalls20news***
Twitter: ***https://twitter.com/robocallsio***
Website: ***https://www.robocalls.io***
Facebook: ***https://www.facebook.com/NoSpam2.0***
Instagram: ***https://www.instagram.com/robocalls2.0***
Discord: ***https://www.discord.gg/sCp48fN***
Reddit: ***https://www.reddit.com/user/Xay912***