NOTGIVING.ETH

WhitePaper

Abstract

NOTGIVING.ETH is an approach to proactively as well as reactively protect the interest of the crypto innocent in the ecosystem and help in building goodwill and faster adoption.

AMIT BORUNDIYA | ANURAG DASHPUTRE | NITIN GURBANI

This document is first draft of the project NOTGIVING.ETH and is created to get views and comments from the industry and community. The information contained in the document is not final and is subjected to change with or without prior information. We welcome your honest comments and critique as this will help this idea to evolve into feasible product.

INTRODUCTION

THE PROBLEM

Scams in the cryptocurrency world run rampant.[1] Reported scams on tracking site EtherscamDB total more than 38,179 ETH (~$23 million) which have been taken from users. And this is only what we can trace!

- Fake MyEtherWallets/MyCryptos: $7.57 million
- Fake ICOs: $4.5 million
- The word “give”: $1.48 million
- Punycode lookalike domains: $507,000
- Fake exchanges: $502,000
- The word “gift”: $459,000
- Elon Musk scams: $32,000
- TOTAL: $23 million

[1] *This article was originally written by Brandon Arvanaghi of Bloom*

The severity of this problem is such that even who's who of the crypto world have their status marked in social networking sites "Not Giving Away ETH" or others Vitalik Non-giver of Ether

There are many aspects of the scams, one is where the hackers' exploits certain vulnerability of the smart contract on the other hand there are many who pose as imposter for a well-recognized celebrity and run a campaign as "Give Away ETH".

Exploiting the Smart Contract vulnerability indeed is a high value but they are not in numbers and many diligence services have come up who can audit the smart contract and inform the potential threat eg: ConsenSys Diligence. Also, recently from the ConsenSys a TCR for smart contract is been conceptualize called Panvala, which in our opinion will further help to detect the safer contracts to deal with.

Also, there are certain attempts to maintain the scam Dbs eg: EtherScamDB, where the knowledgeable user can go and verify if the certain URL is potential scam or not.

All the approach mentioned above are mostly reactive, where the preventive actions happens once the fraud is initiated or is occurred. The approach in almost all mechanism it to get certification of being safe from trusted bodies or group of bodies.

There has been little or no effort to protect the common users who are affected by the "Give Away" scams. The users are not completely technological savvy to understand all the risks and effect of certain action and hence are the most vulnerable.

A close look at the "Give Away" scams will reveal that it mostly initiated in off-chain world via twitter or any other social media. The common user are enticed to make quick bugs are trapped into and they lose their hard earned ETH.

Let's take a scenario, Alice is crypto Innocent and a diehard of celebrity Elan. She has been contemplating to make quick money through the wave of cryptocurrency.

Bob on the other hand is a Crypto Greedy and has been in this domain for a while to understand the ecosystem and vulnerabilities of the crypto innocent people.

When an ecosystem has innocent and knowledgeable greedy, it is conducive environment for frauds.

Bob knows this and sends a tweet as an imposter of Elan. Alice is excited to read the tweet and send requested ETH to the address mentioned in the tweet with the hope to receive promised ETH from celebrity i.e Elan.

Alice doesn't get any ETH plus lost whatever was sent to the address. This experience makes Alice's confidence lower on the crypto ecosystem and she is sharing this with all acquaintances potentially dissuading them to be part of the ecosystem. The larger implication of this is slowing the faster adoption.

There are certain scammers who use the on-chain mechanism, to send transaction with 0ETH and in the data field request the ETH.

Thus the menace of "Give Away Scam" is omnipresent and the users once they lose their ETH are helpless.

To overcome these challenges we suggest **Deal Only** with **Trusted Sources (DOTS)** approach for ON-CHAIN and **Artificial Intelligence Driven Engine (AIDE)** using of state-of-the art AI/ML approaches in OFF-CHAIN to proactively act against the potential scam.

VALUE PROPOSITION

- On-Chain
    - The victim by participating in identifying the potential scammer will be able to recover some of the lost ETH by selling the White Dots accumulated as a reward to identify the true scammer (the scammer address will be market with Black Dots).
    - The Victims are incentivized to spot the potential spam address makes this mechanism self-sustaining and will help curtail the on-chain spread of bad actors.
    - The scammer is provided an opportunity to neutralize his Black Dots through buying of white dots only from victims from the open market. This mechanism penalizes scammers for the bad act done.
- Off-Chain
    - Using various Machine Learning and Natural Language Processing (NLP) algorithms we will be able to spot and build a database of potential scammer's addresses.
    - Many software clients like MetaMask, myEtherWallet and exchanges can use this service, to alert the user before a transaction is initiated.
- Ecosystem
    - This will assist in improving the trust and the confidence about using the ecosystem and help to increase the adoption rate.
    - Facilitates collaboration within the ecosystem

NOTGIVING.ETH approach of securing the users is complementing the existing approaches to maintain the TCR of the URLs and TCR of the smart contract, thus in a way completes the security layer off and on chain for most of the known vulnerabilities.

In summary, NOTGIVING.ETH is an attempt to proactively as well as reactively protect the interest of the crypto innocent and help in building goodwill and faster adoption.

Our Vision:

To protect interest of Technology Innocents in Crypto-World

Our Mission:

To create a system that align incentives of duped strangers to cooperate against potential fraudster and proactively dissuade the potential scammers

APPROACH

As mentioned the menace of the Give Away Scam is not only monetary but has a wider impact on the evolution and adoption of the ecosystem. The present approach to create the awareness among the users and educated them with Do's and Don'ts will not suffice. The users who are fortunate to come across this advises or who have undergone such experiences are the ones who will benefit leaving the masses out. Thus an approach which is seamless and provide feedback to the common user with better user experience is needed.

NOTGIVING.ETH is an attempt to make this as simplistic as possible for the users without getting into the nuances of the technology behind it.

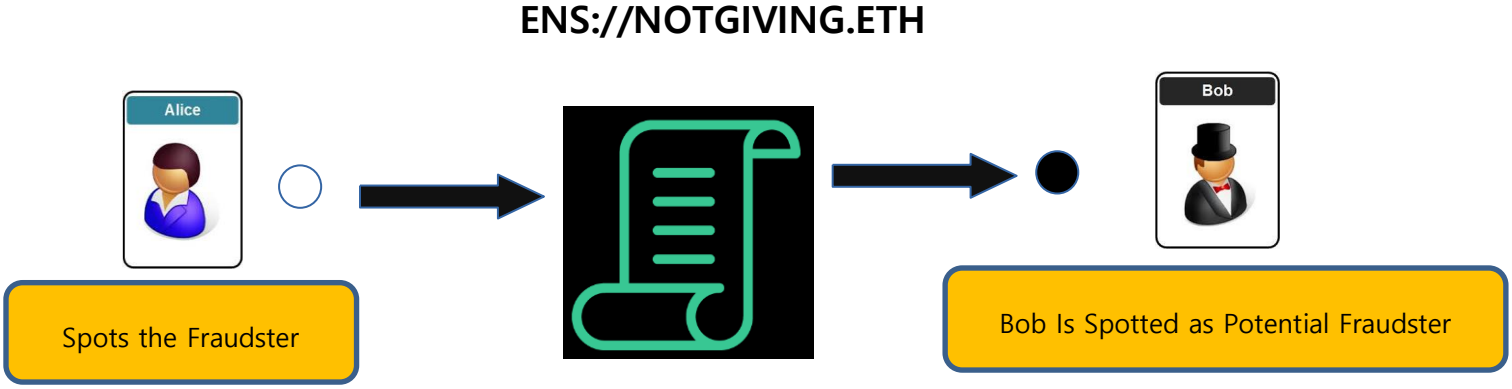
ON CHAIN APPROACH

We propose a dual token system called **Deal Only** with **Trusted Source (DOTS)** consisting of white and black dots.

MECHANISM

- The victim claims a particular address as a the potential fraudster to contract hosted at ens domain **notgiving.eth**
- On verifying the transaction and basic checks, the potential address is given Black Dots and Victim is rewarded with White Dots equivalence of the amount of fraud claimed[2]. At this stage both the Black and White Dots are in lock state and cannot be traded
- Once the consensus is reached on the claim, following steps occur
  - IF Found True : The lock on Victim and Potential Scammer are removed and they are free to trade them
  - IF Found False : The victim is penalized by issuing black coin of the equivalent amount and if there are White Coins available with the victim they are destroyed of the equivalent amount.

[2] This step is not completely full proof, but after long deliberation and consultation we believe this is appropriate approach as this will be able to curtail the fraud's spread when it is happening rather than waiting for consensus. The approach can be misused but with the disincentive mechanism in place the bad actor will be identified eventually.



Alice now knows that there is a mechanism that she can help spot the fraudster by just sending a transaction to smart contract located at NOTGIVING.ETH.

The smart contract checks its database to see if the address is being marked fraud previously, if yes it send the Black Dots to fraudulent address and White Dots to Victim address of the equivalent of the fraud amount

If the fraudulent address is new, still contract sends the respective Black and White dots but with the caveat that they are in locked state until the consensus is reached that the address is indeed fraud.

If the consensus is otherwise the victim is penalized by issuing the Black Dots as well as destroying White Dots of equivalent amount. The potential address is given clean chit and Black Dots is destroyed.

The amount of Black and White Dots are equivalent to amount of ETH which have been transferred by the victim.

CONSENSUS MECHANISM FOR THE SIGNERS

Our ultimate goal is to make the system a truly decentralized. We understand this is not possible from the beginning and hence we propose the signers mechanism which can be extended further to have self-sustaining mechanism

Signers Assignment

- Trusted signers will be nominated
- Various wallet service providers can also be assigned as signers, as their interest is also to protect the users and will help to improve their reputation

NOTE: The number of Signers will be moderated so that there are qualified signers in the ecosystem.

Consensus Mechanism

- Victim claims certain address as Fraudulent
- Signers are notified
- Period is open to participate in the voting (Time based or Quorum of 5 is achieved)
- The participating signers stakes is 10% of the fraud amount in White Dots
- Voting Commences and Completed
    - During the Voting period the Signers can access the twitter and social media analysis of the address through NOTGIVING.ETH UI
    - For the fair voting it is expected that the signers will also look at the additional materials and data to make a judicious call
- Majority of Votes makes the decision either the claim of victim is True or False
- 10% of the staked amount from the signers who voted against the majority is distributed equally among those who voted in accordance to majority

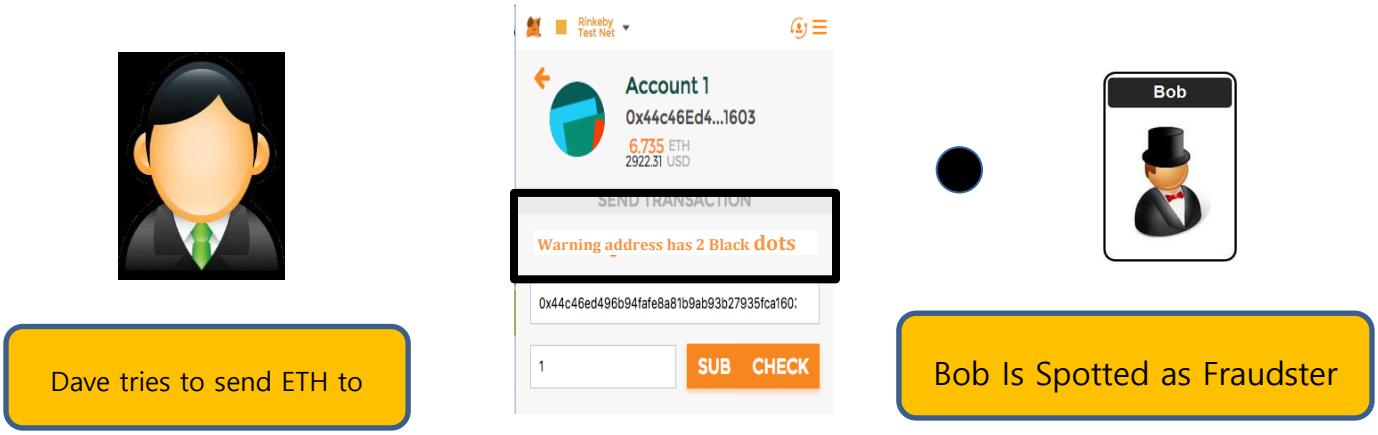
INCENTIVE MECHANISM FOR SIGNERS

The system is transparent and selective to choose the signers. Also, the signers will be able to accumulate the White Dots by participating honestly in the consensus and in alignment with others.

Since the system allows the fraudster to neutralize their Black Dots, this is an opportunity for signers to gain for their honest efforts for keeping the ecosystem clean.

Let's see scenario once the potential address is marked spam, many of the software clients like Metamask can use this information to alert the user who are vulnerable to such activities.

Assume Dave is also one such victim and he falls in the trap like Alice and is initiating a transfer of ETH to the Bob, now when he copies the address of the fraudster in the address bar, there can be a warning message displayed in the software client.



Thus, Dave can instantly know the transaction has a risk and will be alert before he commits the transaction.

NOTE: The above screenshot is from forked version of Metamask as a POC for this approach.

This way the Bob's attempt to trap many crypto innocents is curtailed.

INCENTIVE MECHANISM

Fraudster eg. Bob can neutralize his Black Dots by buying the equivalent White Dots from the victims through Open Market. This mechanism will give a chance for the victims to recover some or more of their lost ETH depending upon the value of White Dots.

In the worst case scenario, if Bob doesn't neutralize the Black Dots but changes his address, this is beneficial for ecosystem and we successfully manage to curtail his further attempts.

This also will work as a deterrent and Bob needs to do all the efforts OFF Chain and ON Chain to trap potentials victims which is a barrier in itself.

For the Victims, it is incentive to mark as many fraudster as possible to accumulate the White Dots. Apart from the opportunity to recover the ETH this also can be viewed as a positive contribution to make the ecosystem more secure and enable social balance in the system.

Deliberate attempts to mark someone as Fraud will require to send actual ETH and raise the claim that the address is potential fraud. This has to be approved by the signers. This is two steps process. Plus if the claim is rejected the sender will be penalized by equivalent Black Dots. This mechanism act as high barrier for someone to deliberately mark someone as fraud.

The receiver of such deliberate attempt on the other hand, gets free actual ETH and he can keep it if signers reject the claim or in worst case if signers make an error in judgement he can utilize those actual ETH to neutralize Black Dots by buying the White Dots from other victims from open market. He is only to gain from this kind of deliberate attempt.

OFF CHAIN APPROACH

The “Give Away Scam” majorly originates in the Off-Chain world and as per the trends it is mostly with the twitter and lately we see it is also penetrated in telegram and other social media platform. Such messages usually take advantage of users curiosity, fear or sense of urgency.

One way to proactively curtail the spread of the scam is to spot in Off-Chain world and sync with the on-chain world so that flag is raised at the right time. This approach will also act as deterrent for the fraudulent guys.

We suggest to build **Artificial Intelligence Driven Engine (AIDE)** to aide in curtailing such spams proactively. We will utilize the existing state of the art techniques in Natural Language Processing, text mining and machine learning to build AIDE.

Most of the ML approach requires a data set and this is one of the most important task in the developing and validating the algorithms.

- With the limited amount of the data available about the scam we will use the existing text mining algorithms analysis tools to do sentiment analysis on the Twitter feeds to score or ranks the sentiments on each tweets as +1 Positive; 0 Neutral; -1 Negative. This will kick start the activities with certain degree of accuracy.

- We will use text mining techniques to collate the right data not only from the tweets but also from other sources for machine learning to build relevant and appropriate corpus.

- Once the corpus collection is complete, we will build customize Neural Network based model to identify potential fraud tweets or message.

- Lately we have observed that instead of the mentioning the addresses in the message, URLs are been used. We are conversant with this problem and in parallel we will work on to leverage ML and Language processing technique to curtail this menace.

One of the challenge for building AI/ML algorithms would be the data collation and this in our opinion will be crucial. Here we can leverage the ConsenSys ecosystem to build the corpus in shortest time to enable the model to deliver the results.

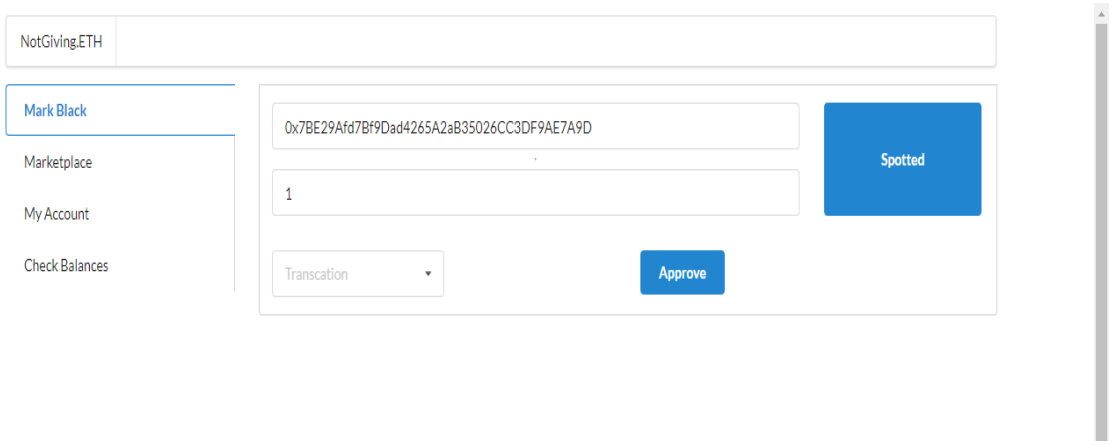
One important point as with any other cyber security firm the Off-chain activity is continuously ongoing and will evolve based on the technique the scammer used.

USER INTERFACE

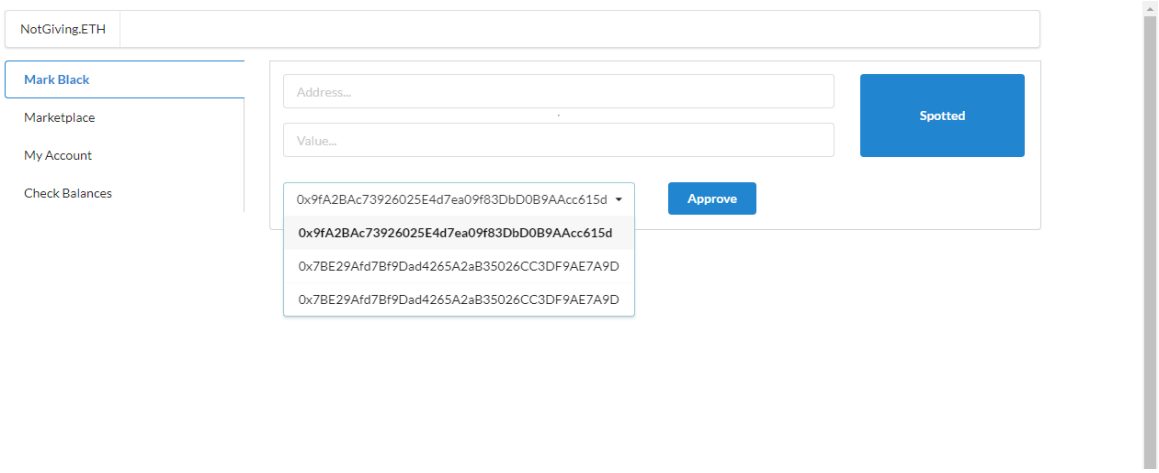
We intent to provide a UX based interface for the users for easy access and transact on NOTGIVING.ETH platform.

Few of the sample wireframe are illustrated below, this is just for illustration purpose

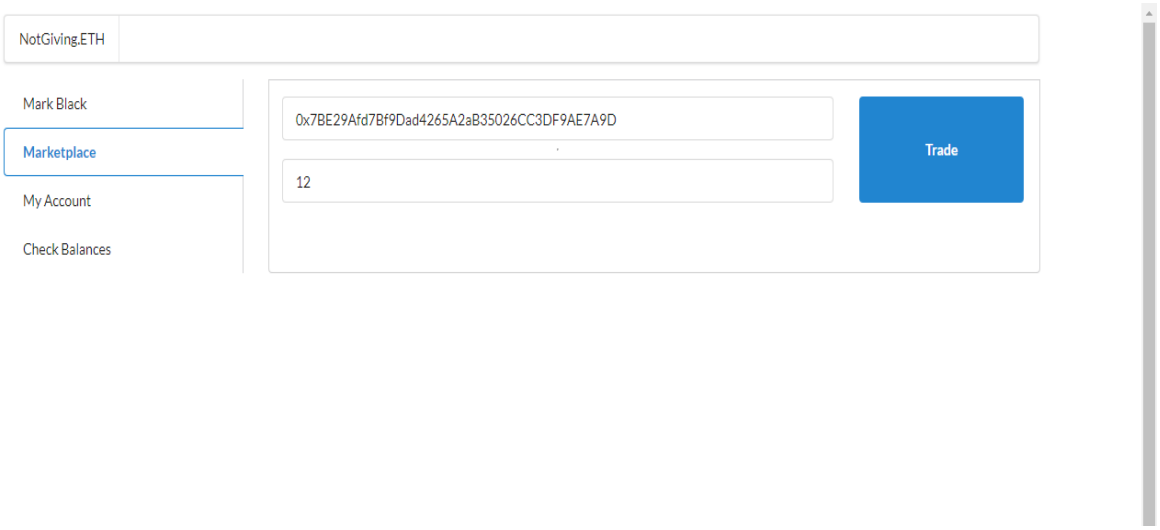
Screen 1: Interface for Victim to Spot the Potential Spam Address



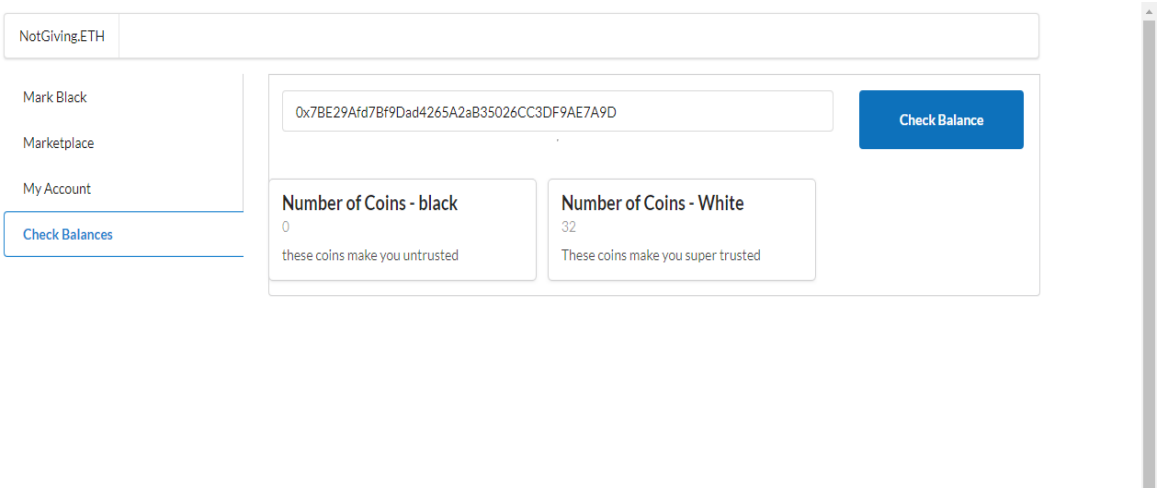
Screen 2: Signer Screen to approve or Reject the claim from the Victim



Screen 3: Market Place for Neutralizing the Black Dots



Screen 4: Option to check the Balance of White and Black Dots for a given address



These are not the final UI and will change based on the feedback and comments from the industry and community.

We also intend to use identity solution for signers and provide them mechanism to vote through their hand held devices. Eg: Uport

CONCLUSION:

To overcome the menace of the “Give Away Scam” we propose two prong approach for On and Off chain world

Deal Only with Trusted Source (DOTS) is a self-sustainable on-chain mechanism based on the incentive and disincentive principals where the victim collaborate to identify potential scammer in the ecosystem. With our research and experience this is FIRST TIME A CONCEPT OF DUAL TOKEN is experimented in the Ethereum ecosystem

Artificial Intelligence Driven Engine (AIDE) will utilize the state-of-the-art AI/ML and Natural Language Processing algorithm to proactively identify the scams and create an alert mechanism. We aim to develop custom algorithms once the data collation is completed to improve the predictability of the engine

We strongly believe the approach will secure the overall ecosystem ON as well as OFF chain and is complementary to the existing approaches to secure smart contract etc.

TEAM CONTRIBUTORS ALPHABETICALLY

Amit Borundiya

Anurag Dashputre

Nitin Gurbani