CryptoAds - A decentralized advertising system that allow users to own and profit from their data

Raul Maldoando

raul@kicl-smart.com

Living in the information era and being bombarded in a day to day basis by all different kinds of mediums, advertisers had embraced an adversarial role in society where users of different platforms are encouraged to upgrade their subscriptions in order to avoid advertisement. Such is the case of big platforms like Spotify and Youtube. Thus the effects of un-targeted advertising may even be detrimental for a brand in terms of its public image, it running the risk of being labeled as intrusive and annoying. This among many other factors has created an increasing value on personal data which, in the past, users were eager to give away in order to connect with their friends and family, giving an increasing power to social networks. This resulted in the user losing power over their data which is now being centralized by social networks who become the owners and the ones selecting whom to share it with. The present paper presents a system where users are able to own their data while allowing advertisers to reach their desired audience in a cooperative way without the need for a middleman.

INTRODUCTION

It is of common knowledge that the economy is driven by the consumer and that most of this consumerism is driven by advertising. By its definition, advertising implies inviting the consumer to buy something that they would not otherwise buy, hence its fundamental role in the economic flow. It is estimated that in the golden ages of the television an ad on one of the big three networks could reach up to 70 percent of the viewing audience[1], however, since those days, the efficacy of the ads has been going down and the frequency with which the consumers are exposed to ads has increased dramatically going from an estimate of 500 ads a day in 1970, to an estimate of 5,000 ads a day in 2006[1].

The conditions under which a consumer tends to be sceptical of an ad vary widely but overall several studies have found a correlation between the concentration that a consumer is placing on a given task before the ad is shown, the congruence between the task and the theme and topic of the ad, the originality of the add, and several other factors[2],[3]. An example of ads generally labeled as annoying and intrusive are the Pop up adds due to its perceived annoyance and intrusiveness, the later which can be defined as the interruption of editorial content. This statement describes most of the forms of modern advertising, whether it is on magazines, televisions, computers, etc., the advertising abstracts the consumers from their reality in order to introduce this new idea they were not aware of before. Modern consumers were born in the era of advertising, hence, they know when an ad is trying to persuade them to buy something. The Persuasion Knowledge Model[3] was born under the premise that the consumer has learned, throughout the years of exposure to ads, to identify when someone is trying to sell something to him and react in accordance, often feeling manipulated or in the try of being manipulated.

This phenomenon has put the consumer and the advertiser on adversarial roles, making the consumer look for new techniques to avoid ads, hence the popularity of software such as Adblock, and the advertisers invest ever more capital studying and implementing new techniques of advertising just to see the consumers become "immune" to these techniques faster each time.

In response to the issue, a new sector of the market flourished the social networks. Throughout the years the social networks had accumulated the personal data of the user with Facebook being the biggest social network with over 2.9 billion monthly active users. This data has allowed them to become the middleman between consumers and advertisers given their knowledge of intimate data of the consumers and the ability to use this data freely. It is estimated that only in Q3 of 2017 the revenue of Facebook reached $10.3 billion USD, 98% of which was from advertising[4]. Not only is it economically detrimental for the user since they receive nothing from the use of this data, but the loss of control of this intrinsically powerful data has allowed malicious organizations to apply this knowledge to suit their political agenda[5].

It is important not to underestimate the power of the media and advertising, being able to shape and indulge values in the consumers, hence the need for conscious advertising is of utmost importance[6]. Over the years, advertising has shown, if badly motivated, to foment some of the lowest aspects of the human being such as addictions, and consumerism, with widely studied cases where consumers become dependent of

a product that is detrimental to their well being. Moreover, international advertising may fail to address the local situation and the needs of the consumers they serve. It is estimated that alcohol and cigarettes, which are legal products of frequent advertising, with alcohol drinks advertising having an estimated investment on advertising of 200 million pounds in the UK, each cause more yearly deaths than all illegal drugs combined[7].

Cryptography and its recent applications in the new ongoing technology known as blockchain, has enabled a new kind of leaderless, borderless and autonomous organizations that are able to solve problems of trust among their participants and also increase the privacy in some applications that so they require[8],[9]. Particularly, Ethereum takes special importance due to the versatile Turing complete language called solidity which has enabled developers to code and implements smart transactions and operations and has them run in a distributed in-mutable ledger. This technology has allowed several applications to emerge and propose a solution amid the numerous flaws of the advertising system, most of them although proposing Nobel solutions of incentivizing the users creating a platform token and ICOs and reputation systems where users and publishers can qualify each other[10],[11],[12],[13],[14], fail to address the lack of trust generated by ICOs and the reduced market adoption that would result in the creation of yet another token[15],[16].

TECHNOLOGIES

CryptoAds was selected to live in the Ethereum blockchain, firstly, to ensure immutability of the reputation system and openness of the participants in the advertising ecosystem. by establishing a clear reputation system that rules the way ads are displayed to the consumers, CryptoAds strives to create a community of cooperation where the need of the participants is served accordingly.

Ethereum was selected in particular given a variety of reasons:

- A Touring complete language for programming smart contracts.

- It is the most advanced platform for the development of decentralized applications.

- Ethereum has one of the biggest communities and hence the active development of the crypto world.

CRYPTOADS DESIGN

CryptoAds is a decentralized ecosystem that allows users to regain power over their information usage and facilitates publishers and brands to reach their users in a more effective and non-adversarial manner. The system focuses on market adoption and ease of use.

The system consists of two main parties that will interact will openly interact with each other on a and off the blockchain, those will be referred to as Advertisers and consumers. In order for these two parties to communicate with eachother, two communication channels will be opened: the organic advertisements and the paid advertisements.

Both parties will come together in a web 3.0 platform whose only objective will be to allow the communication between the user and the advertisers as clean and non-intrusive as possible. The platforms main page will have no advertising whatsoever and will allow the consumer to use a search engine to browse the registered advertisers and will allow the advertisers to upload any given product. The ads will only be displayed to the user in accordance with the 2 interaction rules established.

Finally, in order to incentivize the continuous use of the platform, the system will make use of reputation scores depending on how much they contribute to the platform which will be measured in terms of how much they buy from the advertisers. this reputation score will be described in further sections.

Registration

In order for a consumer to become a registered consumer according to the platform, it is necessary for him to create a consumer address and store it in the ledger. This can be accomplished by sending a fixed amount of ether to the contract, and a public address to which he owns the private keys. This address will be stored together with an empty score and a date of creation.

To become a recognized advertiser, its necessary to send a fixed amount of money to the contract, a public address, and a domain name that will be stored in the public ledger together with an empty score and a date of creation

Interactions

As described above the interactions will work in two different ways as depicted in Figure 1.

The first kind of interactions, the organic advertising, will be the interactions where the user manually searches for a given product. he will not be asked by any party nor will he be suggested to search for a given brand of product, the user will search for a product on his own out of necessity or curiosity this will happen on the browser that is located in the main page of the platform. as the consumer searches for a product, the add will come up in the order of the reputation that a given advertiser is registered to have. Each product will consist of one image and a short description and will redirect the consumer to the domain that the advertiser registered in the blockchain with a given extension, the consumer will be informed about this domain and will be advised not to trust the site if the domain does not match.
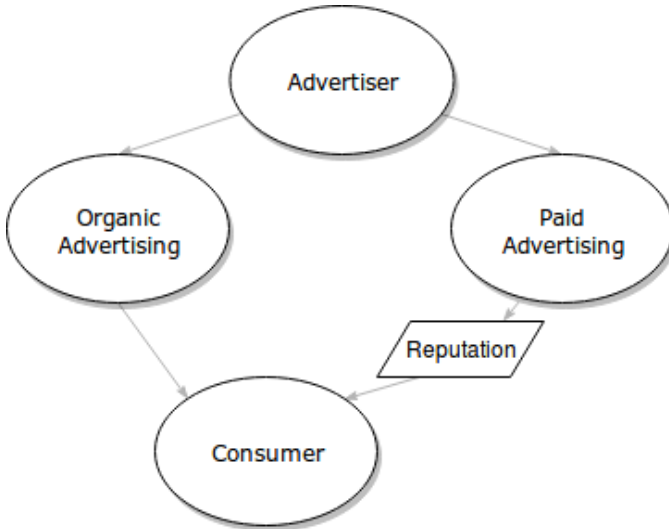
Figure 1. Advertiser-Consumer flow.

On the other hand, the paid interactions consist of the advertiser paying a given set of users to watch a given ad or product. This mechanics will be ruled by 3 main stages:

- Placing a bounty for the consumers

- Filtering the consumers

- Establishing the conditions to claim the bounty

The Bounty. This stage is as simple as it sounds. The advertisers will select a certain amount to be paid and a maximum number of participants to be paid to. The result of the amount times the maximum number of participants will be stored in the smart contract and when the given condition is satisfied, the money will be paid to the participants of the paid advertising campaign.

The Filtering. The advertiser is allowed to specify the number of filters as to whom the campaign will be directed to. the filters will specify which addresses will be able to claim the bounty once the given condition is satisfied. The filters will be related to information that is in the block-chain and will be publicly available to all the participants.

The filters can be as simple as just targeting a given campaign to the user that have a score higher than a fixed threshold, or as complex as filtering those users who're buying history is limited to a certain category in a given range of time.

The Bounty Claim. The creator of the campaign will be the person in charge of selecting the event needed for a bounty to be claimed. This condition will be publicly available and stored in the blockchain for everyone to see. In order to facilitate communication and reduce storage costs, the actual content of the ad will be hosted by the owner of the advertising campaign and the consumer will be directed to the content through the CryptoAds platform if he satisfies the

conditions — once again the consumer will be notified of the domain that the advertiser has registered in the blockchain.

Since the actual interaction with the advertisement will happen off-chain, The completion of a given condition will be verified in the contract with ECDSA signatures generated by the owner of the Advertising campaign:

```
function getOriginAddress(bytes32 signedMsg,
                          uint8 v,
                          bytes32 r,
                          bytes32 s)
         constant returns(address) {
  bytes memory prefix =
        "\x19Ethereum Signed Message:\n32";
  bytes32 prefixedHash =
        keccak256(prefix, signedMsg);
  return ecrecover(prefixedHash, v, r, s);
}
```

Once the agreement has been verified, the contract will transfer the corresponding amount to the consumer and the transaction will be registered to the public. The address of the consumer will be eliminated from the filtering list to avoid the consumer claiming the bounty several times. Also, the signed message will be stored to avoid several consumers claiming the bounty using it more than once.

The Reputation system

Reputation is the pinnacle of the complete system, it will encourage consumers to continue contributing to the platform by making them the focus of paid advertising campaign in which they can earn money, as well as allows the advertisers to identify quality consumers without them having to give away sensitive information, creating a cooperative environment where everybody gets benefited. On the other hand, the reputation system incentives the advertisers to create paid advertising campaigns and give back to the community of consumers. consequently, the reputation system works differently for the consumers than for the advertisers.

To ensure that the trust to maintain an equilibrium in the system, it will be calculated using the trust and profit formula[17]:

$$T(t) = \frac{r_g C_G}{r_g C_G + r_b C_B + \delta + Z * e^{-r_g C_G t}} \quad (1)$$

Where:

$$Z = \frac{r_g C_G}{T(0) + \pi} - (r_g C_G + r_b C_B + \delta) \quad (2)$$

This formula will allow the system to penalize advertisers which campaigns are not claimed by any consumer which would imply a fraudulent deception and will incentivize the

Table 1
Trust and profit parameters

Param.	Description	Default Value
C	Contributive capacity	1
C_G	Good contributions	C
C_B	Bad Contributions	C - C_G
r_g	factor for C_G	0.2
r_b	factor for C_B	0.99
T(0)	Starting trust value	0
δ	Decay Factor	0.01
π	Trust constant	0.01

users to participate actively in the network due to the constant decay of the trust over time.

The Contributive capacity of a given advertiser will be given as a function of the number of different consumers they successfully interacted with.

Consumers reputation. Likewise, the consumer's reputation will be calculated utilizing equation (1) to promote good interactions however the parameters will be adjusted to suit the necessities of the environment. In this case, the parameter C will be defined by the owners of the contract as a function of the different number of advertisers they have successfully purchased a product from, and the reputation of those advertisers. Furthermore, the only detrimental factor in the consumer's trust will be the Trust constant since C_B will be equal to 0 for consumers.

FUTURE WORK

Since CryptoAds strives to become an open self-governed platform, it is of utmost importance to establish the rules on which some of the parameters will be modified such as those that the contract owner can manipulate freely, this not to incur in trust issues from the community towards the administrators. Furthermore, market adoption shall be thoroughly tested in an attempt to promote the ideals of the platform and also to test the suitability of companies changing the conventional advertising schemas to a more convenient one like the one this white paper is promoting.

ACKNOWLEDGMENTS

References

[1] Caitlin Johnson, *"Cutting Through Advertising Clutter"*. https://www.cbsnews.com/news/cutting-through-advertising-clutter. September 17 , 2006.

[2] M. Edwards, Hairong Li, and Joo-Hyun, *"Forcced Exposure and Psychological Reactance: Antecedents and Consequences of the Perceived Intrusiveness of Pop-Up Ad"*. Journal of Advertising. 2002.

[3] Marian Friestad,Peter Wrigh, *"The Persuasion Knowledge Model: How people cope with persuasion attemps"*. Journal of Consumer Research. 1994.

[4] *"Q3 Financial Report Illustrations of Facebook in 2017"*. http://tech.qq.com/a/20171102/007691.htm?qqcom$_p$gv$_f$rom = aio.2017.

[5] *"How Donald Trump campaign used data scraped from Facebook to win presidency"*. https://www.independent.co.uk/news/world/americas/facebook-scandal-latest-donald-trump-campaign-presidential-election-cambridge-analytica-steve-bannon-a8269706.html. 2018.

[6] Hye-Jin Paek, Zhongdang Pan *"Spreading Global Consumerism: Effects of Mass Media and Advertising on Consumerist Values in China"*. 2004.

[7] Silvia A. Law *"Addiction, Autonomy, and Advertising"*. 1991.

[8] Satoshi Nakamoto *"Bitcoin: A Peer-to-Peer Electronic Cash System"*. http://bitcoin.org/bitcoin.pdf 2009.

[9] Vitalik Buterin *"A NEXT GENERATION SMART CONTRACT DECENTRALIZED APPLICATION PLATFORM"*. https://github.com/ethereum/wiki/wiki/White-Paper. 2011.

[10] Papyrus *"Papyrus, Decentralyzd advertising ecosystem"*. https://papyrus.global/static/whitepaper.pdf.

[11] The Leadchain Foundation *"Kind Ads, A Decentralized Trust Protocol for Domains Publishers"*. https://kindads.io/Content/kind-ads-whitepaper.pdf.

[12] ONO *"ONO white paper"*. https://medium.com/ono-social-network/ono-white-paper-e33102d3aad5.

[13] Foreground *"Foreground, A Decentralized Affiliate Marketing and Advertising Solution"*. https://foreground.io/whitepapers/foreground-whitepaper.pdf.

[14] Sheneni Tukura, Pishikeni Tukura *"WebAd, Decentralized social media to reward businesses"*. https://webercoin.io/wp-content/uploads/2018/02/Webercoin-Whitepaper.pdf.

[15] Tom Jackson *"Is this the next financial scandal waiting to happen?"*. https://www.bbc.com/news/business-40704306.

[16] *"China bans initial coin offerings calling them 'illegal fundraising"*. https://www.bbc.com/news/business-41157249. 2017.