

Online Advertising Fraud

By: [Nir Kshetri](#) and Jeffrey Voas

Kshetri, Nir and Voas, J. (2019)." Online Advertising Fraud ", *IEEE Computer*, 52(1), 58-61.

Made available courtesy of IEEE: <https://doi.org/10.1109/MC.2018.2887322>

© 2019 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Abstract:

Fraud is a trust issue. Online fraud is a cybertrust issue. Juniper Research estimated that advertising frauds cost online advertisers US\$19 billion worldwide in 2018. A recent survey found that 78% of respondents were concerned about ad fraud and bot traffic.

Keywords: advertising | blockchain | computer security | computer crime | trust management

Article:

Currently, it is difficult for advertisers, demand-side platforms (DSPs), and others to find or locate the perpetrators of advertising fraud. Most of this fraud is associated with illegitimate clicks on pay-per-click (PPC) advertisements (ads). Advertisers have accused PPC ad providers such as Google and Facebook of 1) using secretive techniques to detect invalid clicks and 2) only providing aggregated statistics about clicks. It is believed that PPC providers directly benefit from fraudulent ad clicks and have a vested interest in labeling more clicks as valid than really are. Because of this, an independent, third-party method that measures accurate online advertising delivery is warranted.¹

Blockchain startups have been working to ensure a higher level of transparency in PPC advertising. Some advertisers have obtained visible results by employing blockchain—one company reportedly saved US\$1 million by using a blockchain-based solution (<https://tinyurl.com/ydbcvjs9>).

Blockchain's impact on advertising has inspired industry groups to respond. The online advertising industry trade group Interactive Advertising Bureau (<https://www.iab.com/our-story/>), whose members include more than 650 media and technology companies, formed a blockchain working group to address this problem (<https://iabtechlab.com/working-groups/blockchain-working-group/>).

By using a distributed ledger model, data related to deliveries of ads on user screens (known as *impressions*), clicks, and information about the audience are stored in a blockchain. This model

shows an ad's delivery status as well as who saw it; the data are then shared among cooperating participants. The relevant data are encrypted and broadcast to each participant, and relevant participants approve the data contained in each block. As a result, the block becomes part of a permanent distributed ledger, and the data can be audited and verified.

CURRENT STATE OF AFFAIRS

The World Federation of Advertisers estimates that worldwide advertising fraud could amount to as much as US\$50 billion by 2027.² Advertising campaigns associated with automated technology are more likely to suffer from fraud: a 2016 study found that 29% of online advertisers who used automated technology experienced ad fraud.³ The study also found that 12% of online ad spending using nonprogrammatic methods (i.e., advertising bought directly from publishers) was affected by fraud.

Although humans and technology can initiate invalid clicks to generate revenue, unethical publishers can also click on their own websites' ads. Clicks on Internet ads often come from people who are paid to do so, and automated click-generating programs are becoming more pervasive.¹

Click fraud is among the most lucrative activities for botnet operators. One recent estimate suggests that a "botmaster" with a network of 30,000 bots can make profits of US\$26,000 per month by launching distributed denial-of-service attacks, more than US\$18 million per month by engaging in bank fraud, and more than US\$20 million a month by using bots to perpetrate click-fraud schemes.⁴

The roots of this online advertising fraud problem lie partly in the opaque nature of the advertising supply chains, and players in the digital advertising ecosystem often benefit from this lack of transparency. Middlemen such as DSPs, ad exchanges, and ad networks profit from ads that run through their systems even if the ads are not viewed by real people or contain malware.

Advertisers and search providers differ widely in their assessment of the percentage of clicks that are fake. As mentioned previously, such clicks on ads distributed by a PPC provider are human or machine generated. PPC providers such as Google assert that invalid clicks not proactively detected account for less than 0.02% of total clicks (<https://tinyurl.com/r76pb4>). However, advertisers such as Cars.com, Expedia, LendingTree, PepsiCo, Hewlett-Packard, and Kimberly-Clark believe that the percentage of undetected fraudulent clicks is higher and argue that PPC providers' secretive techniques for detecting invalid clicks hold advertisers as "financial hostages." Google, e.g., provides advertisers with aggregated statistics. Advertisers, however, are not provided with information about whether a specific click was valid or invalid.¹

BLOCKCHAIN'S POTENTIAL

Table 1 shows how blockchain could affect various actors in an advertising chain. Blockchain's transparency helps identify fraudulent traffic and improves the advertising delivery process. Advertisers can combine data about ads with data provided by ad viewers and wireless providers

related to smartphone ownership to increase the effectiveness of their advertising campaigns.⁵ As a result, it is possible to know who did what and when.

Table 1. Blockchain’s potential impact on various players in an advertising ecosystem

| Player | Potential Impact | Remarks/mechanisms |
|---|--|--|
| Advertisers | Blockchain reduces waste in ad budgets and increases the effectiveness of ad campaigns. | Advertisers can identify the players in the ad supply chain, their roles, and who is paid. They can collect consumer response data and, it can be hoped, use it securely. |
| Consumers | Ad viewers can be incentivized to provide personal information. They will have more control over their data. | Smart contracts can be used to negotiate deals between advertisers and ad viewers. The amount paid to an ad viewer depends on the details and value of information shared with the advertiser. |
| PPC providers (e.g., Google and Facebook) | The current dominance of a few big PPC service providers in the advertising industry may decrease. | Blockchain may challenge the secretive nature with which advertisers currently treat information related to ad transactions. |
| Ad publishing websites | A positive reputation will be important for attracting more ads. | A website’s reputation may be determined by democratic voting. |
| Intermediaries (e.g., subdistributors) | Roles will decline over time. | Blockchain’s decentralized nature may make it possible for advertisers to more directly connect to future ad viewers. |

As mentioned previously, advertisers are typically provided only aggregated statistics about clicks. A blockchain-based solution, on the other hand, allows media buyers to look at all details of individual transactions.⁶

Recent efforts have been directed toward eliminating intermediaries. IBM’s digital marketing wing, IBM iX, teamed up with software firm Mediaocean to launch a tracker for transactions in digital media (<https://tinyurl.com/yaag4ev6>). This tracker aims to remove intermediaries from among advertisers, publishers, and consumers and prevent payments from being disbursed to the wrong parties. Blockchain’s transparency allows advertisers to identify the various players in the advertising supply chain, their roles, and how the advertising dollars travel from one place to another.

Blockchain-based advertising delivery models can be implemented to collect consumer response data and use it efficiently and more securely⁷ as well as to provide details about an ad campaign’s efficiency and effectiveness.⁸

The importance of click statistics is particularly interesting. Ad viewers may be paid in cryptocurrencies for participating in this process and providing relevant information. For instance, ad-blocking browser Brave’s blockchain-based digital advertising platform uses Ethereum-based Basic Attention Tokens (BATs). Internet users who opt to view advertising are paid in BATs. Brave’s browser claims to monitor ad viewers without violating privacy rights (<https://www.cnet.com/news/privacy-browser-brave-tor-trump/>).

When consumers are offered something of value in exchange for their participation, it is believed that they may be more willing to share their data with the companies with which they do business.⁹ However, the main reason consumers may be reluctant to share information with firms is that they are concerned about the inappropriate usage or leakage of their data. These concerns

have been heightened following recent high-profile cases of data mishandling, such as Facebook's Cambridge Analytica controversy and the credit rating agency Equifax's data breach.

Blockchain's decentralized nature and transparency features allow consumers to know how their data are being handled and for what purpose. Blockchain may also give consumers more control over how their data are used. If this model works as expected, companies should be able to build greater trust with consumers (<https://hbr.org/2018/05/what-blockchain-could-mean-for-marketing>).

Smart contracts are also used to connect ad viewers, advertisers, and other parties to facilitate trust. For instance, verifying that an ad viewer is the true owner of a smartphone requires that the advertiser have access to the viewer's subscriber identity module card to confirm ownership information with a wireless provider. The advertiser may also want to know the ad viewer's location.² However, it is important that verification of ad delivery and personalization are done without breaching privacy laws.

CHALLENGES FOR APPLYING BLOCKCHAIN

Despite blockchain's potential to reduce online advertising fraud, challenges exist. The most prominent one is that blockchain has not yet been widely adopted and seriously tested to address this problem. A related issue is that blockchain's distributed and decentralized nature requires that each block receive some form of approval before its inclusion in a chain. Additionally, blockchains may not be able to process real-time advertising transactions quickly enough. It is reported that 10 to 30 s are needed to validate a transaction before a new block is added to a public ledger (<https://tinyurl.com/yd7xv6r7>). This processing speed is too slow to accommodate the current operation of programmatic ad-buying and ad-selling platforms.

Consider real-time bidding in an ad exchange, where ad impressions are bought and sold in an auction-like setting. A bid request contains information about potential ad viewers such as demographic data, location information, and browser history. Then, an ad exchange submits the bid requests to a list of potential advertisers. The ad, product, or service that wins the auction is placed on the website. The entire process, including receiving the bid request and serving the ad, takes no longer than 100 ms (<https://tinyurl.com/yc659d77>).

Currently, this level of performance cannot be reached for blockchain advertising delivery. Because of blockchain's relatively slow response times, it may not be feasible for it to be used to prevent frauds and validate transactions on a real-time basis. Therefore, some companies may only use distributed ledger technology following an ad campaign to validate and authenticate transactions.

It is also believed that the main barrier to introducing blockchain has been educational rather than technical (<https://tinyurl.com/ybywu926>). Studies have shown that the lack of awareness among key stakeholders and the lack of availability of skilled professionals are key impediments to blockchain deployment. For instance, a study conducted in December 2017 by the World Federation of Advertisers and dataxu found that only 3% of advertisers understood blockchain's potential for reducing advertising fraud.⁶

Finally, for a blockchain ad-tracking system to work effectively, all parties must be willing to participate. They must use blockchain to track transactions and provide the relevant information. Securing the cooperation of diverse players, however, may prove difficult.⁶

Blockchain has the potential to transform the way online advertising is paid for, sold, and measured. Blockchain makes it possible for advertisers to see whether their ads are being delivered and reaching the appropriate customers. Advertisers can track who opened an ad and where that potential customer is located. Moreover, they can assess a promotional campaign's conversion rates, i.e., ads that result in a sale.

Because of the pervasiveness of click fraud, a compelling need exists for new intermediaries that track online advertising. Intermediaries that provide third-party measurement approaches capable of increasing trust may reduce some of the concern; however, these intermediaries are not yet established. Blockchain's immutability and transparency features provide methods for auditing and verifying details related to online advertising; however, blockchain performance remains a concern.

ACKNOWLEDGMENT

The authors are completely responsible for the content in this article. The opinions expressed here are completely their own.

REFERENCES

1. N. Kshetri, "The economics of click fraud," *IEEE Security Privacy*, vol. 8, no. 3, pp. 45–53, 2010.
2. K. Gallagher, "Ad fraud estimates doubled," *Business Insider*, Mar. 16, 2017. [Online]. Available: <http://www.businessinsider.com/ad-fraud-estimates-doubled-2017-3>
3. L. Handley, "Businesses could lose \$16.4 billion to online advertising fraud in 2017: Report," *CNBC*, Mar. 17, 2017. [Online]. Available: <http://www.cnbc.com/2017/03/15/businesses-could-lose-164-billion-to-online-advert-fraud-in-2017.html>
4. MIT Technology Review, Inside the business model for botnets. 2018. [Online]. Available: arxiv.org/abs/1804.10848
5. WARC, "Blockchain ripples media," 2017. [Online]. Available: https://www.warc.com/LatestNews/News/Blockchain_ripples_media_waters.news?ID=38272
6. N. Perrin, "How blockchain can stop digital ad fraud: Some marketers are prioritizing the technology in 2018," *eMarketer*, Mar. 26, 2018. [Online]. Available: <https://www.emarketer.com/content/how-blockchain-can-stop-digital-ad-fraud>

7. J. D. Neuburger, "The cross-industry promise of blockchain," *The National Law Review*, Mar. 15, 2017. [Online]. Available: <http://www.natlawreview.com/article/cross-industry-promise-blockchain>
8. G. Sloane, "Digital TV players eye blockchain to block Facebook, Google," *AdAge*, Feb. 27, 2017. [Online]. Available: <http://adage.com/article/digital/digital-tv-players-eye-blockchain-block-facebook-google/308090/>
9. R. Kurzer, "Report: Gen Z, millennials more willing to give up personal data in exchange for personalized experiences," Sept. 11, 2018. [Online]. Available: <https://martechtoday.com/report-gen-z-millennials-more-willing-to-give-up-personal-data-in-exchange-for-personalized-experiences-223985>
10. C. Tan and E. T. K. Lim, "Blockchain could help advertisers lock up our attention," *Which-50*, Mar. 20, 2017. [Online]. Available: <https://which-50.com/blockchain-help-advertisers-lock-attention/>