CrowdLED: Towards Crowd-Empowered and Privacy-Preserving Data Sharing Using Smart Contracts

Constantinos Pouyioukka, Thanassis Giannetsos, Weizhi Meng

CrowdLED: Towards Crowd-Empowered & Privacy-Preserving Data Sharing using Smart Contracts

Constantinos Pouyioukka*, Thanassis Giannetsos‡, Weizhi Meng‡

* *Research Fellow*,
‡ Cyber Security, Department of Applied Mathematics and Computer Science,
Technical University of Denmark
Email: {cp00296@surrey.ac.uk, atgi@dtu.dk, weme@dtu.dk}

Abstract. In this research paper, we explore how Blockchain technologies and Smart Contracts can be used to fairly reward users for the data they share with advertising networks without compromising anonymity and user privacy. The novelty of using Blockchains alongside such systems is to understand and investigate how a proper and fair exchange of data can ensure that participating users can be kept secure and eliminate aggressive data collection by ad libraries; libraries that are embedded inside the code of smart-phones and web applications for monetization. There are a lot of privacy issues regarding mobile and online advertising: Advertising networks mostly rely on data collection, similar to a crowdsensing system, but in most cases, neither consent has been granted by the user for the data collection nor a reward has been given to the user as compensation. Making a comparison between the problems identified in mobile and online advertising and the positives of the approach of using Blockchain, we propose "CrowdLED", a holistic system to address the security and privacy issues discussed throughout the paper.

Keywords: Blockchains, Online Advertising, Smart Contracts, Security, Privacy, Fairness, Crowd-Sourcing

1 Introduction

Internet of Things and subsequently its applications and systems are mostly based on a cloud-centric approach. To ensure proper security and smooth operation of processes that are involved in such paradigms, several authors explored the possibility of integrating Blockchain technologies in IoT operations [1].

Advertising Networks (ANs) work by relying on a mass scale data collection from participating users, leveraging smartphone applications, web applications, online services and internet browsing history. Data collection is achieved through advertising libraries that are embedded into the services and software. The collected data is then used to deliver specific ads, according to a user's online activity, ethnographic background and other information. In most cases, advertising networks aggressively collect user data without the necessary consent which in turn raises a number of questions regarding user anonymity and privacy [2].

ANs and subsequently their systems can be separated in *online* and *mobile* advertising. For setting the fundamentals of the research, we will explore online advertising as a whole; with mobile advertising as the core extend of that.

Advertisers in general, rely on ANs to efficiently deliver ads to customers [3, 4]. This is achieved through the use of smartphones, as such devices, contain rich information that are needed by the advertising network. Services and mobile applications that are offered free of charge, utilize such networks for monetization, via the equivalent advertising schemes in place.

When referring to ad delivery and targeted ad placement, we are not only referring to smartphones, smart homes or smart appliances but to the wider spectrum of IoT applications; e.g., Intelligent Transportation Systems [5, 6]. Such smart vehicles and respectively their drivers, will be part of such aggressive data collection methods being utilized by advertising networks. As drivers and passengers consume a large portion of their daily lives commuting, these systems can be susceptible to location specific advertising [7]. This might be considered an alternative to static billboards. These systems require to communicate with the backend infrastructure and, thus, will also have to share data between them. Providing incentives in a transparent and fair way for users to participate, even in these services is of paramount importance.

Contributions: By taking all the information into consideration, this paper follows on to identify the main issues and share a brief insight on privacy-related solutions towards preventing aggressive data collection in the online and mobile advertising spectrum. Following, with an explanation of why blockchain technologies can be the solution and how they can be leveraged in such systems. Then we proceed with presenting the key challenges in designing and developing a viable solution coupled with the requirements that such systems need to fulfill as criteria, and an overview of the proposed architecture. This research paper finalizes with critiques of such an approach and how it can be enhanced further. Final thoughts and discussions are presented alongside our conclusions.

2 The Existing Problem in Web and Mobile Advertising

In websites, web applications and mobile applications, developers embed advertising libraries in their source code. This is a common way among companies to monetize their services, offering them for free instead of opting for a fee from their users. Those advertising libraries can then deliver targeted ads according to the specific online profile of a user. These libraries collect user data so that they can offer a more targeted approach when referring to ads.

This approach though comes with one major flaw; *the uncontrolled mass collection of user data risking privacy.* Technology giants in the likes of Google and Facebook offer their services for free, taking advantage of the advertising platforms they have developed over the years. In turn they act as brokers selling those advertising data to clients, to place targeted ads on their platforms. Clients/advertisers create campaigns on such platforms to promote their services or products. The advertisers can then request (through those platforms) where their ads will be placed, for how long and which specific groups of people will target, i.e.,: "People that make use of a smart-phone device, from the European Union aged between 25-40, who have an interest in football". This generic approach, mentioned as an example, can then be narrowed down even further with

specific keywords provided by the advertising framework. Concluding that such techniques can be a major privacy issue, as developers implementing advertising libraries in their web or mobile applications, can collect personal data as an individual third party. Each platform and broker have their own payment systems in place, but the general approach is to pay according to the 'number of impressions' or 'how many times a link has been clicked' followed to the client's service. The more functional a platform is, the more revenue a broker can make from user data and in return their clients that use those platforms.

Although a straightforward process, data collection is happening aggressively without the user's consent especially in mobile applications. The most valuable asset of users, their data are given for free. When a service provider or an advertiser gets the revenue, a user doesn't get a share of that revenue.

Another important issue with advertising is the use of advertising libraries for malicious acts. Ads containing malicious code or misleading audiovisual content, with the sole purpose of extracting user sensitive information. Or forcibly through an ad, install ad-ware on a user's system to collect information in the background. This method is commonly referred to as "Malvertising" (Malicious Advertising). This practice is commonly used by perpetrators, as the advertising libraries provide a solid platform for malware to flourish and be distributed due to the intrusive nature of ads. Advertising libraries being intrusive by nature can ensure that a product or a service can gain traction by attracting loads of users. But at the same time can be a double-edged sword as it compromises user security and privacy. As advertising is now a normal process of selling products or services on legitimate websites and social networks, attackers can directly advertise malicious code websites or applications masked behind a valid ad without compromising those legitimate websites.

In this paper we aim to introduce an incentivized and privacy enforced solution towards mitigating the following issues: (i) *The uncontrolled and aggressive data collection of users*, (ii) *The non-incentivisation of user data to compensate users for participating in the advertising model*, and (iii) *The possible distribution of Malware or offensive ads using an advertising library.*

3 Privacy Preserving Solutions towards Preventing Aggresive Data Collection

A lot of research has already been conducted towards ensuring that strict security and privacy mechanisms are clearly followed when collecting user data for ad placements [7]. Studies have mainly focused in measuring and identifying the security and privacy risks that are directly associated with the delivery of ads in web applications, websites and mobile applications. Results have identified that most advertising libraries abuse systematically the way they handle and gather data from host applications and their user base [2].

Pluto: ("Free for All! Assessing User Data Exposure to Advertising Libraries for Android") [2]. A framework notable for its usage in analyzing and detecting if an advertising library and by extension its host application is exposing targeted user data. Pluto is built in a novel way utilizing the power of language processing

and machine learning and the equivalent data mining models. This is done to identify what type of user data is exposed and what information, advertising networks can extract from a list of installed applications in a device. Pluto can estimate the risks associated when developers choose to implement advertising libraries in their applications.

AdSplit: ("AdSplit: Separating smartphone advertising from applications") [8]. An application embedded to the Android Operating System that allows an application and the advertising library associated with it to run as separate processes on the system kernel. Each process is assigned a separate user-id, thus, eliminating the need for the main application to request permission to mine data on behalf of the advertising library. AdSplit, guarantees privacy of users but does not solve the problem of aggressive data collection.

PiCoDa: ("PiCoDa: Privacy preserving Smart Coupon Delivery Architecture") [9]. A privacy preserving smart coupon delivery system, with its main purpose of protecting user data on the client side rather than on the service side. This framework guarantees that when an ad is placed, a user is being verified if it is eligible for a coupon. It also offers protection to the service/vendor by not revealing any information about the targeting strategy.

Privad: ("Privad: Practical Privacy in Online Advertising") [10]. An advertising system that provides a balance between user privacy and placements of ads across the web. Privad makes use of keywords, demographics and user interests for prioritizing those data according to the needs of an AN via online auctions. Privad improves a user's browsing experience, while maintaining low costs when we are referring to costs of infrastructure for an advertising network.

RePriv: ("RePriv: Re-Imagining Content Personalization and In-Browser Privacy") [11]. A browser add-on system, that has as its main purpose to enable privacy for participating users. RePriv only discovers data after getting an explicit user permission. It then mines relevant user interests and shares this information with third party ANs. As the authors and developers claim, this data mining is happening in-browser and no drawbacks are being reported when we are referring to, a user's online browsing experience and the performance drawback of producing results.

From a brief description of the above solutions, we can conclude that while some of them are focusing in delivering privacy as their ultimatum, others, by compromising privacy, provide a sense of fairness. None of them, however, guarantees and solves the initial problem as a whole: *Providing the privacy, fairness and security as their core characteristics.* When referring to fairness, we imply the compensation of users for providing their data to advertising networks.

4 Using Blockchain Technologies, Smart Contracts and Incentives to Close the Gap

Blockchains work in such a way that can provide a 'shared governance', thus, ensuring trust and anonymity. And with the use of smart contracts, involved parties can benefit from shared agreements as well as the fair exchange of data without the need of a third-party intermediary being in charge. Blockchains for the IoT

domain can be applicable in a plethora of applications and systems [12]. One field though that hasn't attracted much attention is the integration of blockchain technologies in advertising network applications.

The main challenge in such systems is **to fairly reward users while avoiding uncontrolled and aggressive data collection** of user's personal information and data. To overcome the issue of fair execution, an approach would be the use Smart Contracts. Using smart contracts, service providers can ensure that rewards provided by the service, and the data provided by users are exchanged simultaneously. This can be achieved because smart contract terms and conditions are strictly followed after they are agreed by the parties involved [13].

4.1 Advantages of using Blockchains in Online/Mobile Advertising

Transparency: Users will have control over which data can be shared but also can opt out from the data collection process at any given time. Also, with Blockchains, advertisers and advertising libraries can verify that a user engagement on an ad is genuine. Users can be confident that an ad placement is not coming from a fraudulent entity as, through smart contracts, the ad of a service can be verified and validated on the network, i.e., if an ad is placed for an Amazon product the user will know that the advertiser has created an ad campaign that was placed directly by Amazon and not another fraudulent entity.

Incentives: Users can still support the advertising business model but can also be given the option of exclusion. ANs can be incentivized to collect only the necessary and minimum amount of data required for their services, as they will have to 'pay' for gaining further access to user data. Rewards can either be, monetary or non-monetary [14–16]. Systems with monetary incentives, reward their participants with real money or virtual redeemable credit which is equivalent to the actual price in currency. Non-monetary incentives do not include any real money rewards but can include a plethora of options such as entertainment, social and service incentives [3]. This can vary according to the advertisement library and the agreements set at the programming of smart contracts.

Fairness: Fairness can exist if the parties involved mutually agree on the terms of the Smart Contract. Those terms will be upheld and followed strictly as any node connected inside the network can validate the status of the contracts ensuring absolute trust between the parties involved.

Privacy and Anonymity: Using Blockchains, we can ensure user privacy and anonymity, as security mechanisms are implemented by default. Although, such mechanisms exist, we still need to take appropriate actions to identify any leakage of personal user information.

No single point of failure: Data are distributed in such way where each node has an exact copy of the entire Blockchain since the genesis block. Even if nodes inside the network do fail, the network is still fully operational, and any workload is distributed to the other network nodes.

Open Source Software: Blockchain technologies are based on Open Source software, allowing a plethora of applications to be deployed. A huge community of developers is present that ensures the security and proper maintenance of

the source code. Advertising libraries and providers of advertising libraries can benefit from the openness of this technology.

Direct Communication between Advertisers and Users: Based on the current mode of operation, current advertising libraries introduce a middleman between users and advertisers. Those middlemen can be in the likes of large corporations who act as brokers. With the use of Blockchains, these middlemen can be eliminated or become less powerful in terms of controlling user data. Thus, they will be deemed irrelevant to the final transaction of the smart contract. When advertisers leverage this direct contact to the end users, more robust and effective ads can be delivered.

Less Intrusive - More Effective Ad Placements: At their current state ads are very intrusive. Especially in mobile applications where the majority ads can take the form of video overlays that cannot be closed until a specific time interval has concluded. A good example of a privacy related application is the web browser Brave, which offers an approach of Blockchain related advertising. Brave allows users to opt – in or out for receiving ads. Following a similar approach, in our system, advertisers can benefit from receiving the data they need, without compromising user privacy.

Less Malicious Code Exploits & Elimination of Malware: One issue with intrusive ads is the possibility of distributing malicious code and fraudulent ads to the end-users. A big portion of advertising libraries have less checks in place to validate the authenticity of ad campaigns or do not have checks at all to ensure what ads are being served. Although already mentioned, with transparency in mind, assurance and quality of ads derives directly from Blockchains. When a transaction is sent throughout the network, it is validated and then accessible to view by any valid user. If a malicious user tries to interact with the network, it can be traced back to the point it originated; thus, it can be deemed invalid and not safe for the entirety of a network.

Taking into consideration the benefits of Blockchain technologies, smart contracts and their characteristics, we aim to further expand on these technologies for finding the golden ration between advertisers, advertising networks and users. With the use of Blockchain technologies, the main problem of aggressive data collection can be remedied. As adopters of this system, can agree with their users, to receive specific data anonymously, in exchange of rewards. Users on their end can still support the advertising business model, by having the option to share (or not) their data. Advertising networks in turn can be incentivized to collect only the necessary data as they will have to 'pay' for the data they require. Thus, the problem of fairness can be solved as well. In the next section a more in-depth approach on the Blockchain underpinnings is conducted and we identify the key challenges in designing a system, like CrowdLED.

5 Key Challenges in Designing CrowdLED

As aofrementioned, Blockchains can be used to enhance the advertising platform for better delivery of ads and a fair exchange of data for the appropriate user incentivization while ensuring verification and enhanced user privacy. All these

objectives can be achieved by taking crucial measurements and identifying the key challenges that need answering before implementing CrowdLED.

From a "System Security" Perspective: *How can we ensure that users or mobile applications don't feed or spoof data to get a competitive advantage, or unfairly get compensated in a system? How can we ensure that the system proposed in its entirety is secure from user manipulation but also, how can we ensure users are secured from and by the system?* - This key challenge is very important in such systems to ensure their viability and properly compensate users according to their participation. By integrating Blockchain technologies and with the use of smart contracts, the security and privacy but also, the fairness aspects of the research questions can be solved.

From an "Economics Perspective": *How can a Smart Contract be implemented to accommodate the entities involved? What types of incentives can be offered as an acceptable form of compensation? What is the right amount of compensation for the right amount of data gathered?* – This key challenge is again important and needs to be addressed for properly incentivizing users according to the data they share. Compounding this issue, we need to implement metric mechanisms; using device metrics to quantify user privacy and data shared across parties.

From a "System Design" Perspective: *How is the data collected and shared, from user devices to advertising networks? Should there be a central system service that handles data requests, or an ad hoc mechanism handled by the device's operating system? Is the system secure by web-based attacks?* – Currently mobile and web applications offer ads, collect data and share them with an advertising network. Usually the data collection from such services is hidden from the host application, the operating system and the user itself. The decision on which approach needs to be taken into consideration for implementation, between a central system or an ad hoc mechanism, is solely based on examining the trade-offs of each approach. The solution should not be susceptible to tampering but also be efficient as not to impact the performance of a user's device or that of the system from delivering the ads.

From a "User Privacy" Perspective: *How can we ensure that proper user privacy practices are being followed? Is the system secure from social engineering attacks, with their main aim to identify users?* - As already mentioned, ANs rely on aggressive data collection to target specific ad placements to their users. This aggressive data collection extracts personal user information which users wouldn't share in the first place.

6 Closing the Gap between ANs and Users

CrowdLED will be a fully operational system combining Blockchain technologies and Smart Contracts for enabling privacy and fairness when advertising networks collect user data. By using incentives and rewards, we can ensure a fair exchange of data and credits between a user and an advertiser. But also, enable correct security practices that ensure: **Privacy and Anonymity**, to the users involved and **Fairness and Security**, to the users and the system providers.

6.1 Data Collection

Data Collection Characteristics: The type of information that is to be collected from the users, but also the possible use of sensors in a smartphone so that data can be extracted. This data can take the form of raw application data, or statistical values such as maximum, average or minimum [17, 14, 18, 19].

The frequency on which data is to be transmitted and time duration characteristics: This includes the periodic submission interval that data is to be submitted to the advertising network. Time intervals can vary in time, length but also in frequency. Those time intervals might also have specific requirements on the data that are to be submitted, i.e., every twenty (20) seconds for the time interval of two (2) minutes, submit the device's location where that location is above thirty (30) meters of sea level [17–19]. The duration of a task that users need to participate, and the time interval data sharing is live on the network, needs to be recorded [17].

Area of interest and incentive characteristics: The area of interest that the system will be deployed for delivering ads on a specific area. The area can be defined as the population of a geographical area. Dense geographic areas are more of interest to ensure maximum ad placement and delivery [17]. *Incentives:* The Incentive criteria, on which, the users will be rewarded according to the data they provide to the service.

Eligibility criteria to join: User devices must meet some pre-defined hardware or software specifications. Pre-defined eligibility criteria might fall in the category of specific user profiles or user groups. Examples might be software requirements like an Android or iOS operating system. Specific user profiling might include users who enjoy a specific outdoor activity to deliver ads based on environmental and user's activity data.

6.2 Security

Privacy Preserving and Fairness Mechanisms: Users participating, taking into consideration the time on a service and their contribution, should be rewarded *fairly* and *anonymously* [18, 19]. Any external or internal observers shouldn't be able to identify any users. If there is the need for collecting sensitive personal information, users can either opt out or enable access with the equivalent reward [18, 19].

Access Control and Authorization Mechanisms: Users participating, should only allowed to access areas of the system, according to the privileges provided to them by system administrators.

Confidentiality, Authentication and Integrity Mechanisms: The system must have specific mechanisms to ensure the proper authentication of participating users. Proper protection on their communications should be provided alongside strong confidentiality and integrity of the communication channels against unauthorized third parties with the purpose of causing harm to the system or its users [2, 20].

Accountability Mechanisms: Any entity that might be deemed as offensive to the system, including participating users, administrators or components

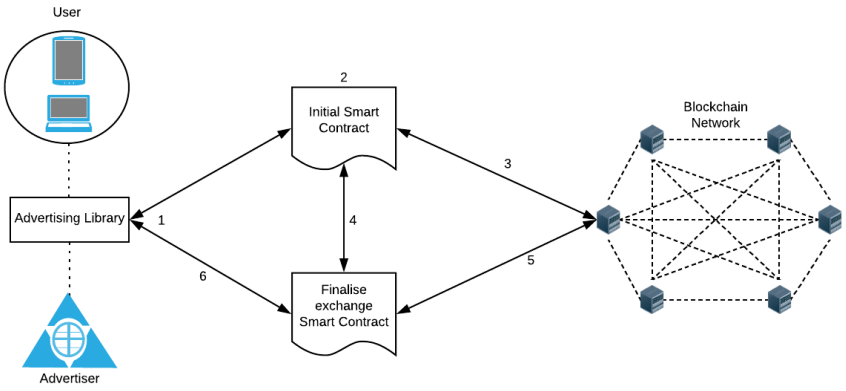

Fig. 1. : User & Advertiser Interaction with the Blockchain network - Overview

of the system's infrastructure should be 'disciplined' based on a set of rules pre-defined by the system.

Trustworthiness and Validity of Data Mechanisms: The system must have the necessary mechanisms to ensure the validity of data and their trustworthiness as submitted by the participating users. Also, ads must be delivered in such a way to not affect performance and should be as accurate as possible [21].

6.3 Incentives/User Compensation

Well-laid out incentive schemes must cover basic requirements, which include:

- The maximization of profits for both users and the system [22];
- Avoid any risks, relating to users and system, having a 'damaging' cause. Incentives must be adequate to outweigh any drawbacks while transmitting data. Drawbacks might include: battery drainage, excessive usage of device resources, and the time the service is running on the background;
- The system should be aware of the exact population of participating users on demand at any given time. Also known as a stochastic population. This ensures that proper incentive allocation is fairly distributed across users.

7 An Architectural Blueprint of CrowdLED

Figure 1 depicts how users and advertisers could interact with each other when using smart contracts. The system is equipped with a direct communication scheme in place, between an advertiser and a user. Rather than relying on a broker to handle user data for specific ad campaigns on behalf of an advertiser, the advertiser is now responsible for placing ads; by having direct access to user data after consent has been granted. This approach can make data brokers irrelevant to the relationship between users and advertisers.

7.1 High-level Overview

This approach follows a two-contract mandate between users and advertisers. The first contract will dictate the data that the user will share with the advertiser and the incentives the advertiser will issue as a compensation to the user. The second contract, directly issued by the first contract, will dictate what ad will be served to the user, according to the data transmitted on the first contract for a more effective ad placement. The first contract acts as a reference point of the initial transaction. The second contract will be issued automatically as the user has already approved and authorized the collection of data for delivering an ad. In respect to Figure 1 and its numbering we present the process flow as follows:

Advertisers request data from the users through a smart contract using the advertising library (Step 1). Users will decide if they will opt-in to engage in the smart contract providing their data, with the option to select what data to distribute, i.e., Location and Interests. Advertisers then, according to the agreed amount of data that they will receive, they issue the amount of incentives that the user will receive (Step 2). As already discussed, incentives can be of monetary or non-monetary format. This can be settled on a universal mandate by the network and its participants. If the user is not happy with the incentives that will be issued after the transaction has been finalized, the user can choose to opt-out without further commitment and user data and incentives are omitted.

If all has been decided by the user and the advertiser, the contract is then encrypted and represented as a block to be broad casted and mined from the validating users (miners) of the network. Once the block has been mined, validated and the network approves the transaction, the block is permanently added to the chain. This is the initial block that will create a reference for the next block and the smart contract of delivering the ad (Step 3).

The second contract is issued automatically by the first contract, but its validity can still be rejected by the network. The advertiser issues the ad campaign according to the received data, and the contract is encrypted and represented as a block and follows the same journey of validation by the network. If the contract is validated according to the standards of the network, the user receives in an automatic approach the ad placement. If now the contract is deemed as containing an anomaly or any malicious code, or the ad doesn't meet the advertisement criteria, both the contracts are voided and reversed, and the advertiser is issued a penalty according to the severity of the anomaly (Steps 4, 5, 6).

This approach of a two-contract based system can have the benefit of identifying fraudulent users trying to circumvent the initial contract. With the issue of a penalty, advertisers can always make sure that they follow the network procedures without risking financial loss. Also, it gives the opportunity to users to select which advertisers to trust based on a feedback system.

7.2 CrowdLED Implementation Details & Execution Flow

As a first prototype, the system is being developed as an Android application. For future iterations, the system will leverage both web and mobile frameworks towards a universal deployment. Currently the Blockchain network used

is Ethereum [10] Development branch with "CrowdLED token" being created as an incentive to compensate users. Geth [9] command line has been used to create a test bench for the development and for initializing a new Blockchain to test the communication between the Android application and the network. Open Source library Web3J [11] has been used to provide the necessary toolbox to enable the deployment of smart contracts from the Android application to the test Ethereum network. "CrowdLED token" has been created as part of the test network and has a fixed price. At the current stage of development, one token equals with sending one location packet to the service, for testing purposes. The location packet is making use of the sensing capabilities of the smartphone to send longitude and latitude in a string format.

Google Firebase acts as the equivalent of the advertising library (See Figure 1) and is being used as a medium to exchange the data from the user to the advertiser. The back-end infrastructure communicates with two different versions of the application. One version is for the hypothetical user and another is for the hypothetical advertiser. Both the advertiser and user have unique wallet addresses bind to each application for simplicity. Once the user commits to send data to the service, the service asks for a consent to transmit the data. Moving on, from the Android Application, the back-end is responsible for transmitting the user's location to the advertiser only if the first contract has been validated. The user is then rewarded for the data and the back-end sends the information for the ad. The ad in this early development stage is just an image, again for testing purposes. Pre-loaded tokens from the Advertiser's account wallet are subtracted, according to the data a user is sending and are added to the user's account wallet. Smart contracts are written in Solidity; an object-oriented high-level language with syntax similar to JavaScript. Web3J library acts as a wrapper to deploy the smart contracts from the Android Applications to the Blockchain test network.

At this stage of development, the two contracts behave as they should, assuming the user always accepts the binding agreement of the first contract and the network has validated that the ad placement on the user's application is following the advertisement criteria of the network.

As already mentioned, CrowdLED is a work in progress. Everything discussed in this section and the current development stage is to give an overview of the system to the reader. The current development stage is to test the system in a scenario where everything works as intended.

8 Discussion & Critique

With respect to the benefits of using Blockchains, mentioned in Section IV, and the requirements set in section VI, there are still some open issues that need further investigation as they can have a negative impact on the system functionality.

The system needs to present a fair incentive model. What do we mean with fair incentives? Who is responsible for deciding what is a fair compensation to users that provide their data? Can the community of participating users

decide what a fair compensation is? Or should the advertisers decide on what to compensate users according to the data they receive?

A simple approach is: 'a user sends an "X" amount of data to an advertiser for a fixed amount "Y" of compensating incentives.' Those compensating incentives can be unique for each advertiser, i.e., Amazon can offer discounts to its online marketplace or provide users with one month of premium shipping. There are a lot of approaches in the fairness model but also, algorithms that can be implemented to ensure that fairness can exist. Further research must be conducted to identify, design and implement a 'fair approach' algorithm.

The need for checking mechanisms to be implemented, to ensure that malicious ads or malware don't make their way to end users. Also, what other mechanisms can be implemented to ensure that any other form of attacks don't occur in such a system? As discussed in section VI, access control and accountability mechanisms need to be implemented in the final solution. Furthermore, research has been conducted towards ensuring security in the Blockchain. Security that it is not compromised by attacks. Such attacks can take many forms with most notable ones being Sybil and Eclipse attacks. These two attack vectors are the ones that need to be explored further as they can make the whole system and its validity of serving effective ads, ineffective. This danger is more prominent with Sybil attacks where in our case, a node in the network can act, as one with many identities, spamming the advertising libraries with repetitive data to 'win' more incentives.

When an advertiser has served a misleading or a 'fake' ad, with the purpose of extracting user sensitive information or misleading the end user, how is that advertiser penalized? Which entity inside the system is responsible for adjusting that penalty and what form of penalty is the most suitable one? Mechanisms need to be implemented to ensure that any type of mishap can be stopped and not occur again. A penalty system needs to be implemented in accordance to advertising policies.

When referring to ad validity, what types of ads can be deemed as misleading or fake? In order to address properly this issue, we need to follow Regulations, Policies and Laws set for Advertisers worldwide. Such examples include:

- The Advertising law from the Federal Trade Commission in the US;
- The Consumer Protection from Unfair Trading Regulations and the Business Protection from Misleading Marketing Regulations in the UK;
- EU's Audiovisual Media Services Directive for the EU.

One of the most notable open issues with such a system approach is the use of smart contracts and their security. How can we ensure security in smart contracts and in their entirety are not susceptible to attacks? When referring to the validity of the transactions in smart contract, it doesn't always mean that the security is not compromised. From further research it has been identified that, smart contracts can include bugs or critical security vulnerabilities, which in turn can make their way inside the Blockchain. The main reason such security vulnerabilities and bugs are present inside the smart contract code, is because

of the way a smart contract is programmed. Common problems with smart contracts can be logical errors, the failure to use or implement cryptographic protocols during the binding of the contract, misaligned incentives and the details of the implementation approach of the contracts are error-prone. An attacker can then manipulate those errors inside the smart contract to its advantage if appropriate security mechanisms are not in place.

9 Conclusions

Throughout this research paper, we aim to identify current issues in Mobile and Online advertisement networks. By using Blockchains and smart contracts, we aim to introduce a feasible approach to close the gap between advertising networks and users. Also, the main aspect outlined in this paper is to ensure that Security, Anonymity, Privacy, Transparency and Fairness will be implemented as core characteristics in the proposed system. Making a brief comparison between the problems and the positives of such an approach, "CrowdLED" is being introduced: A system that when deployed to its full extend, will be evaluated to ensure its validity and effectiveness by comparing it against initial objectives and requirements set. A more in-depth paper following the algorithms involved and a thorough system architecture and how the two-contract based approach will work with adequate testing, will be released at a later stage.

10 Acknowledgments

This work was supported by the European Commission, under the ASTRID and FutureTPM projects; Grant Agreements no. 786922 and 779391, respectively.

Special thanks to Dr. Soteris Demetriou, Assistant Professor at Imperial College London, for his insights in privacy and security for mobile and online advertising, and the valuable feedback at the initial stages of drafting this paper.

References

1. C. Catalini and J. S. Gans, "Some Simple Economics of the Blockchain," National Bureau of Economic Research, Inc, NBER Working Papers 22952, Dec. 2016.
2. W. Meng, R. Ding, S. P. Chung, S. Han, and W. Lee, "The price of free: Privacy leakage in personalized mobile in-apps ads," in *NDSS*. The Internet Society, 2016.
3. V. Rastogi, R. Shao, Y. Chen, X. Pan, S. Zou, and R. Riley, "Are these ads safe: Detecting hidden attacks through the mobile app-web interfaces," in *23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016*. The Internet Society, 2016.
4. S. Shekhar, M. Dietz, and D. S. Wallach, "Adsplit: Separating smartphone advertising from applications," in *Proceedings of the 21st USENIX Conference on Security Symposium*, ser. Security'12, 2012, pp. 28–28.
5. S. Gisdakis, M. Lagana, T. Giannetsos, and P. Papadimitratos, "SEROSA: service oriented security architecture for vehicular communications," in *VNC*. IEEE, 2013, pp. 111–118.

6. J. Whitefield, L. Chen, T. Giannetsos, S. Schneider, and H. Treharne, "Privacy-enhanced capabilities for vanets using direct anonymous attestation," in *2017 IEEE Vehicular Networking Conference (VNC)*, Nov 2017, pp. 123–130.
7. M. C. Grace, W. Zhou, X. Jiang, and A.-R. Sadeghi, "Unsafe exposure analysis of mobile in-app advertisements," in *5th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WISEC '12, 2012, pp. 101–112.
8. G. Einziger, C. Chiasserini, and F. Malandrino, "Scheduling advertisement delivery in vehicular networks," *CoRR*, vol. abs/1804.05183, 2018.
9. Geth, "Official Go Implementation of the Ethereum Protocol," [Available Online]: https://geth.ethereum.org/].
10. Ethereum, "A Decentralized Platform that runs Smart Contracts," [Available Online]: https://www.ethereum.org/].
11. W. . L. Web3j, "Where Jave meets the Blockchain," [Available Online]: https://web3j.io/].
12. L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16, 2016, pp. 254–269.
13. P. Papadopoulos, N. Kourtellis, P. R. Rodriguez, and N. Laoutaris, "If you are not paying for it, you are the product: How much do advertisers pay to reach you?" in *Proceedings of the 2017 Internet Measurement Conference*, ser. IMC '17, 2017, pp. 142–156.
14. I. Leontiadis, C. Efstratiou, M. Picone, and C. Mascolo, "Don't kill my ads!: Balancing privacy in an ad-supported mobile application market," in *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications*, ser. HotMobile '12, 2012, pp. 2:1–2:6.
15. S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "Shield: A data verification framework for participatory sensing systems," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec '15, 2015, pp. 16:1–16:12.
16. T. Dimitriou, T. Giannetsos, and L. Chen, "Rewards: Privacy-preserving rewarding and incentive schemes for the smart electricity grid and other loyalty systems," *Computer Communications*, vol. 137, pp. 1 – 14, 2019.
17. K. Delmolino, M. Arnett, A. E. Kosba, A. Miller, and E. Shi, "Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab," *IACR Cryptology ePrint Archive*, vol. 2015, p. 460, 2015. [Online]. Available: https://eprint.iacr.org/2015/460
18. P. Papadopoulos, N. Kourtellis, and E. P. Markatos, "The cost of digital advertisement: Comparing user and advertiser views," in *Proceedings of the 2018 World Wide Web Conference*, ser. WWW '18, 2018, pp. 1479–1489.
19. H. Haddadi, P. Hui, and I. Brown, "Mobiad: Private and scalable mobile advertising," in *Proceedings of the Fifth ACM International Workshop on Mobility in the Evolving Internet Architecture*, ser. MobiArch '10, 2010, pp. 33–38.
20. S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "Sppear: Security & privacy-preserving architecture for participatory-sensing applications," in *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks*, ser. WiSec '14, 2014, pp. 39–50.
21. C. F. Chiasserini, F. Malandrino, and M. Sereno, "Advertisement delivery and display in vehicular networks: Using v2v communications for targeted ads," *IEEE Vehicular Technology Magazine*, vol. 12, pp. 65–72, 2017.
22. G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," *CoRR*, vol. abs/1506.03471, 2015.