Targecy
The transparent and private advertising protocol

Author: Martin Grabina

Version 0.2 (Sep 2023)

martin@targecy.xyz

Abstract. A purely decentralized and non-custodial advertising protocol is now possible while still keeping users' data private by using novel cryptographic techniques. Issuers, such as marketplaces, generate digitally-signed credentials that are saved on the user's device (in exchange for rewards). Those are loaded while exploring publishers applications, such as social networks, in order to show corresponding advertisements and improve advertisers ROI. The entire flow is designed to preserve user's privacy and be compliant with regulations, by using an open source relayer, Zero-Knowledge Proofs[8] and Pedersen Hashes[9]. This whitepaper provides an in-depth look into the protocol's architecture, context on current advertising industry challenges, its approach to privacy and regulations compliance, and outlines future directions for enhancing on-chain anonymization, efficient tokenization, and OpenRTB[5] (traditional advertising network) interoperability.

1. Background

In the early 2000s, traditional advertising mediums like print, radio, and television were the dominant forces. Later, with the advent of the internet and digital technologies, a seismic shift was initiated. By 2021, digital advertising had overtaken its traditional counterparts, accounting for 65% ($522.5 billion[12]) of the total advertising spend.

While Web2 technologies brought about unprecedented reach and targeting capabilities, they also introduced significant challenges. Centralized platforms controlled by tech giants like Google, Facebook, and Amazon became the gatekeepers of digital advertising. In 2021, these three companies alone captured more than 60% of the global digital advertising market, and kept 25%-60% of each ad's revenue. This centralization led to issues such as lack of transparency, high fees, significant privacy concerns[11], and censorship.

In that context, regulations all over the world, such as the General Data Protection Regulation (GDPR)[10] in the European Union and the California Consumer Privacy Act (CCPA) in the United

States have imposed stringent rules on data collection and usage. While these regulations aim to protect consumer privacy, they have also increased compliance costs and limited the effectiveness of targeted advertising campaigns which of course impacts ROI for advertisers.

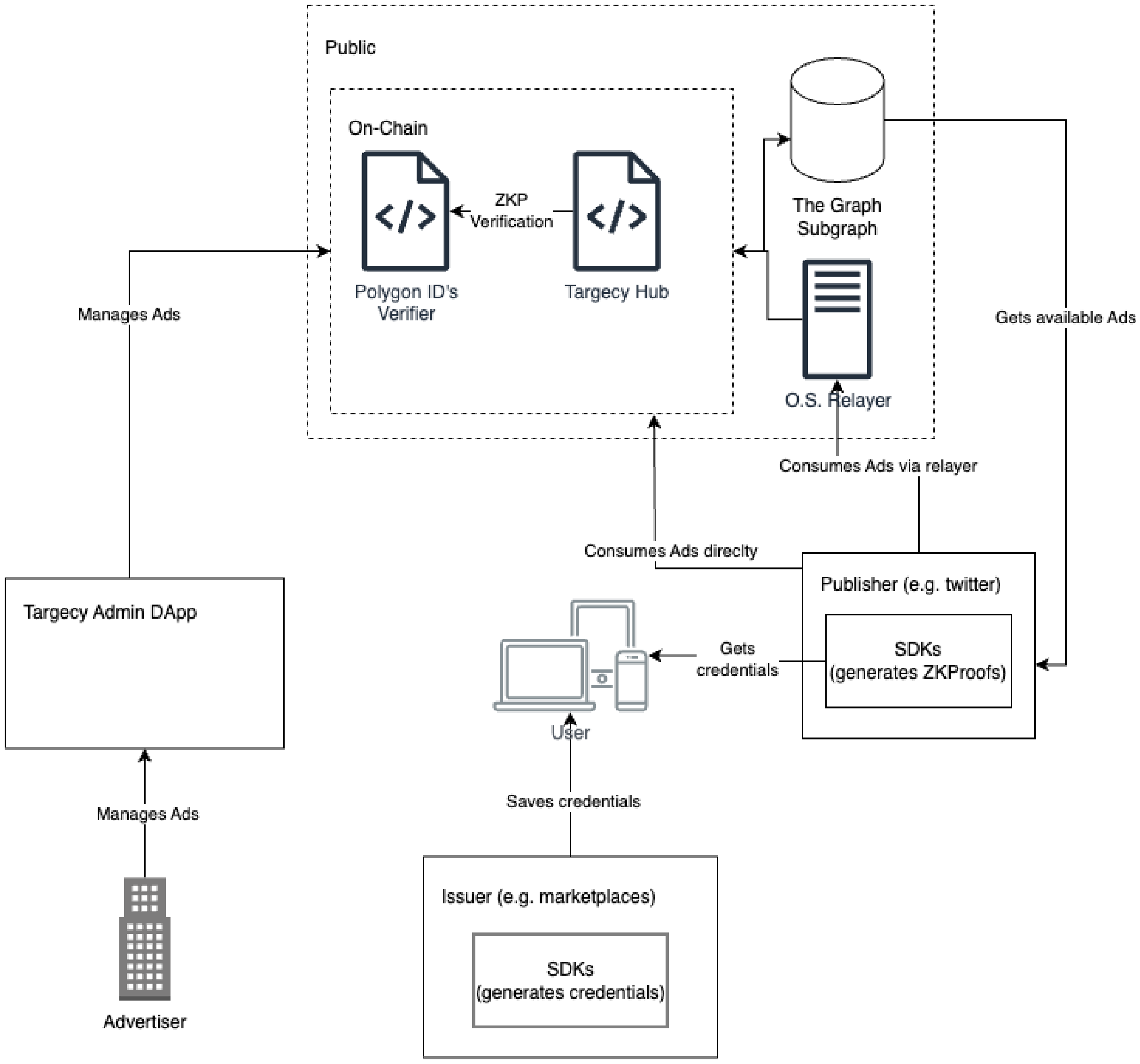
Web3, often dubbed as the third generation of the internet, promises a decentralized future. It aims to give individuals more control over their personal data and disrupt the centralized structures that have long dominated the digital world. Despite the rapid growth of the crypto and Web3 ecosystems, one critical element remains conspicuously absent: advertising as a source of funding. While traditional and digital advertising have been key funding mechanisms for content creators and platforms in the Web2 world, a similar model has yet to be established in the Web3 space, and at the same time, there isn't a clear way for users to find interesting protocols for them. The journey to establish advertising in the Web3 ecosystem is fraught with challenges, primarily centered around privacy and the immutable nature of blockchain. The very features that make blockchain secure and transparent also make it difficult to implement traditional advertising models that rely on data collection and user profiling[1]. These inherent challenges have deterred the development of a robust advertising model in the Web3 space.

While the challenges are significant, they also pave the way for groundbreaking opportunities. In essence, the adoption of a cryptographic-based advertising model has the potential to transform the industry: while decentralization and transparency leads to create a perfect market with lower fees, privacy leads to regulatory compliance and therefore to enhanced targeting and better ROIs for advertisers. This creates a win-win scenario for all stakeholders—regulators, users, publishers and advertisers.

2. Targecy Architecture

2.1. Overview

The architecture of our protocol was designed with the core principles of privacy, transparency, and interoperability in mind, the protocol leverages a combination of on-chain smart contracts, a public data indexing service, a dedicated web application for advertisers, an optional relayer, and specialized SDKs for publishers and issuers. Our aim is to enable all stakeholders to utilize the protocol either in a decentralized manner or through APIs for enhanced functionalities.



Overview of Targecy's Architecture

2.2. On-Chain Smart Contracts (Targecy Hub)

The backbone of our protocol lies in the smart contracts deployed on Polygon's blockchain, capitalizing on its low transaction fees and high throughput. This ensures a cost-effective and scalable solution. These contracts serve multiple functions, including holding the database of advertisements and their associated metadata, referencing target groups. Target groups are defined by attributes such as age, location, and interests and references zero-knowledge proof requests, ensuring that ad targeting is both effective and privacy-preserving. The zero-knowledge proofs and credentials are created using Polygon ID js-sdk[4] and verified using Polygon ID's[3] on-chain contracts, that are already audited and battle-tested.

Upon successful validation of these proofs, the ads are consumed, meaning they are displayed to the end-user in a manner that respects both privacy and relevance. Once the ad is consumed, the rewards are distributed correspondingly between the publisher, Targecy (fixed fee), and the users (if applicable).

The consumption of the ad itself does not only allow to distinguish between an impression and a click, as legacy platforms, but also we introduce a new acquisition model: actions. By leveraging the interoperability and atomicity of transactions on-chain, we can ensure the consumption of an ad in case a call to a dedicated contract was successful or not. As a user, just imagine exchanging tokens inside an ad or taking a loan, and as an advertiser, just imagine paying the ad proportionally to the revenue it created, by ensuring cryptographically the avoidance of today's frauds.

2.3. On-Chain Data Indexing

To retrieve on-chain data, we employ The Graph[7] for indexing. This enables quick and efficient data retrieval, a feature that is indispensable for real-time analytics and good UX. Advertisers can monitor campaign performance with ease, and publishers can fetch relevant ads without latency, thereby enhancing the user experience. Anyone can fetch the (public) data and create new subgraphs.

2.4. Web Application for Advertisers

For advertisers, we offer a DApp (decentralized app) that serves as a one-stop solution for managing ad campaigns. The application not only allows for the creation and modification of ads but also provides real-time metrics on ad performance. This includes key performance indicators such as impressions, clicks, and ROI, enabling advertisers to make data-driven decisions. Of course, this element of the system can grow as much as wanted and create new business opportunities (ad generators, analytic tools, etc).

2.5. SDKs for Publishers and Issuers

To ensure seamless integration and wider adoption, we provide Software Development Kits (SDKs) tailored for different stakeholders. Publishers can use our SDK to display ads on their platforms, while issuers can issue signed identity credentials (standardized W3C Credentials[14]) to users, for any custom behavior, which can create the Zero-Knowledge Proofs required for ad consumption. The first SDK will be compatible with React and Typescript (frontend frameworks used by majority of web3 apps), and other languages (including compatibility with mobile devices) will be developed on demand.

2.6. Relayer

To further enhance user privacy, our architecture includes an optional open-source relayer component. This relayer acts as an intermediary between the user and the smart contracts, allowing users to hide their interactions with the protocol. While the use of the relayer is optional, it offers an added layer of anonymity without compromising the core functionalities of the protocol. By routing interactions through the relayer, users can engage with the advertising ecosystem without directly exposing their blockchain addresses or other identifying information, thereby achieving a higher level of privacy. In addition to this, they doesn't need to pay for their transaction's gasses and can retrieve and delete its history of interactions (GDPR compliant) without deleting their private key (compliant alternative for the *'right to forget'*).

By combining these elements, our architecture offers a holistic, privacy-preserving, and efficient solution that aligns with the regulatory landscape and meets the needs of advertisers, publishers, and end-users alike.

3. Privacy On-Chain and Regulations

In the context of regulatory compliance, particularly with stringent laws like the General Data Protection Regulation (GDPR) in the European Union, the concept of anonymity is not black and white but exists in various shades of gray called pseudo-anonymity. Therefore, the goal in order to be compliant is to reduce as much as possible the linking between an user (represented by his on-chain address or any other type of ID), and his private data (characteristics, interests, apps usage, behaviors, etc.). This is opposed to how public blockchains work, where all data is publicly accessible: you would be able to deduce some characteristics of an user based on the ads he proved to deserve to see.

Regarding user consent, the sole action of transforming user's behavior into credentials (even if those never leave his device) requires user's consent in order to be GDPR compliant. Legacy platforms rely on "contextual behavior" [13], which is allowed without explicit consent, when the user hasn't allowed enhanced tracking. For us, it is going to work the same way: contextual behavior credentials when there is no explicit consent and enhanced behavior (as precise as possible) when consent has been granted. We will dig into the details to verify if we can reach more precision without consent compared to legacy systems, since we are never retrieving a user's data from his device, but because of the novelty of the solution, it falls in a gray area so it is something that has to be studied by the authorities for further decisions.

A possible solution to this problem would be to use one address for each transaction but this would require user's interaction, so we propose two options:

- For experienced web3 users that want to avoid any type of middleman, they can reach the contract directly, pay the needed gas and take full responsibility of what data they are exposing. They can manually use a fresh address for each transaction.
- As a default method, users will sign a message (for authentication) sent to the relayer (which will be open-source for transparency) and it will send the transaction to the contracts (including user's zero-knowledge proofs) to consume the corresponding ad. This removes the need for the users to pay for the needed gas and helps avoid needing to delete the private key as a way to comply with GDPR[10] on "right to delete data", since anyone would be able to get and delete their data from the relayer.

The use of ZKProofs[8] instead of plain data as traditional systems forces to reduce as much as possible the data exposed: in order to see +18 Ads a proof proving +18 years is created instead of exposing the entire user's identity. This concept is replicated for any type of data.

After all verifications, if the publisher has set to share rewards with the user, we can't send them directly because it would expose their characteristics as well, so we implemented a flow similar to Tornado Cash[2]. Based on Pedersen Hash[9] theory, the sender of the transaction creates two hashes (commitment and nullifier) that are related. The commitment hash is sent in the transaction and saved on-chain in a merkle-hash-tree to be easily searchable. The nullifier works as a certificate for the user to withdraw the funds in a separate transaction. If multiple ads rewards have the same amount, the user's reward is untraceable to the ad's target groups, and therefore the user's characteristics aren't unveiled.

This way, we are preserving user's private data from one end to the other, while ensuring effective targeting for ads. Privacy is still a hot topic being researched, and new techniques based on cryptography are being developed, further advancing the field and offering promising avenues for even more secure and compliant digital advertising solutions in the future. Please see the 'Future Opportunities' section for more information.

4. Competitors

The good news is that there are multiple companies and investors trying to solve the problems explained in Background by using different approaches. What's more, many of them already have some traction because most of the biggest players in the industry are already spending millions in marketing. But the industry is still finding the best way to do it:

- Some of them developed a new blockchain or other type of decentralized architectures a.k.a. "decentralized network of advertisements" (like adshares.net, or alkimi.org) providing a solution for web3 DSPs and SSPs by removing current multiple middlemens and therefore reducing the fees.
- A few of them present web3 alternatives for SSPs, but by only using public on-chain data (blockchain-ads.com) or private data given specifically by users on-demand (permission.io).
- Others are specific implementations like referral links using smart contracts (fuul.xyz), earn-by-giving-data-directly social networks (profila.com), web3 analytics (cookie3.co), among others.

Targecy's architecture provides a complete solution:

- The SDK works as SSP (Supply-Side-Platform), used by publishers
- The DApp works as DSP (Demand-Side-Platform), used by advertisers
- The contracts works as a decentralized & fully transparent exchange
- And Polygon's Blockchain ensures one of the most decentralized chains in industry and best interoperability available for CPA (Cost-Per-Action) acquisition models.

In this context, we believe that the key differentiator is to provide the best ROI (Return-On-Investment) for advertisers, and that the only way to do it is by having the best targeting solution, while keeping other elements such as fees and network size competitive as well. For that, our novel solution proposes to use signed certificates and Zero-Knowledge Proofs providing maximum precision and flexibility for targeting while preserving user's privacy.

5. Future Technical & Business Opportunities

5.1. On-Chain Anonymization Alternatives

As privacy continues to be a focal point in the digital advertising landscape, we are actively researching advanced techniques for on-chain anonymization that may make the flow more efficient. Future implementations may include ZKRollups, privacy-preserving transactions, the use of private chains for enhanced security, and stealth addresses to further anonymize user interactions. All these solutions are still being researched and not ready for production.

5.2. Token Business Model

While our current model operates using native tokens and keeping a fee for each operation, we are exploring the possibility of introducing a custom token to offer more specialized functionalities. This could include features like loyalty programs, governance, and a unique reward mechanism tailored to the advertising ecosystem which can provide a commissions-free protocol for everyone.

5.3. OpenRTB[5] Connection

To bridge the gap between Web2 and Web3 advertising models, we are studying on integrating us to the OpenRTB protocol. This will enable seamless interoperability with existing digital advertising platforms, expanding market reach and offering a more comprehensive advertising solution. This would allow not only fetch ads from legacy systems (and therefore bring funds from web2 to web3), but also push ads from web3 apps to current mainstream platforms.

5.4. Satellite applications

As in traditional ad-tech, there are a lot of solutions to be integrated to the barebone ad-network: ad creative generators, AI spellers, etc. It’s a matter of time that they start appearing in crypto as well.

5.5. Cross-Chain Acquisition

By using protocols like ZetaChain, it would be possible to capture cross-chain operations.

6. The Vision

We want to create the barebone platform for the future of advertising, which in addition to be more efficient for advertisers (by lowering fees, improving targeting in a compliant way and removing fraud), should respect user’s privacy and present a new ad revenue sharing model, that unblocks a new set of opportunities: we see everyday play2earn games without solid economic fundamentals, newer developments should, for example, allow people in poor countries to live off their favorite games or social networks in a sustainable and scalable way.

7. Summary

In summary, Targecy offers an approach to digital advertising in the Web3 space. It addresses the industry's pressing challenges, including centralization, unnecessary high fees, fraud, lack of transparency, censorship, and privacy concerns, by leveraging advanced cryptographic techniques and blockchain technology. With a focus on regulatory compliance and future scalability, our protocol is poised to redefine digital advertising, offering a win-win scenario for all stakeholders—regulators, users, publishers, and advertisers.

8. References

8.1. Blockchain and the General Data Protection Regulation (https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf)

8.2. Tornado Cash Whitepaper (https://berkeley-defi.github.io/assets/material/Tornado%20Cash%20Whitepaper.pdf)

8.3. Polygon ID Docs (https://0xpolygonid.github.io/tutorials/)

8.4. Polygon ID js-sdk (https://github.com/0xPolygonID/js-sdk)

8.5. OpenRTB (https://iabtechlab.com/wp-content/uploads/2022/04/OpenRTB-2-6_FINAL.pdf)

8.6. Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium (https://deliverypdf.ssrn.com/delivery.php?ID=249000000081123030125085120080088065040082022002039016066109027100116081109008116095122031018004012045098004017105113120105119051027045019081115104118086101006093126040046041080081071095117086113068064097085072029021008095018092068099029107089070067001&EXT=pdf&INDEX=TRUE)

8.7. The Graph Whitepaper (https://github.com/graphprotocol/research/blob/master/papers/whitepaper/the-graph-whitepaper.pdf)

8.8. Zero-Knowledge Proofs (https://ethereum.org/en/zero-knowledge-proofs/)

8.9. Pedersen Hash (https://iden3-docs.readthedocs.io/en/latest/iden3_repos/research/publications/zkproof-standards-workshop-2/pedersen-hash/pedersen.html)

8.10. GDPR (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679)

8.11. Privacy Concerns (https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/)

8.12. Digital Advertising Spending by Statista (https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/)

8.13. Contextual behavior (https://theappsolutions.com/blog/development/contextual-and-behavioral-targeting/)

8.14. W3 Verifiable Credentials (https://www.w3.org/TR/vc-data-model/)