FRACTAL

Valued users, trusted ads: Proposing an Open Source Protocol for the Advertisement Industry

WHITE PAPER
VERSION 2021-FEB-01

Table of Contents

Glossary

Ad Budget

The **Ad Budget** is the total amount that **Advertisers** are willing to spend in paying the **Bid Prices** due for verified **Ad Claims**.

Ad Buy

An **Ad Buy** is the information that **Advertisers** post in the Protocol and conveys the target audience that the Advertisers want to reach, the actions that Advertisers are willing to pay for, and how much Advertisers are willing to pay for such actions. An **Ad Buy** contains the following parameters: **Required Action**, **User Characteristics**, **Bid Price**, **Ad Budget**.

Ad Claim

An **Ad Claim** is the **User's** assertion to have performed a **Required Action**. **Ad Claims** are verified by Verifiers.

Ad Escrow

The **Ad Escrow** is the escrow where **Advertisers** deposit part of the **Ad Budget**.

Ad exchange

Where advertisers and publishers meet for price discovery. Most operate Real-Time Bidding ad auctions where prices are negotiated on a per-impression basis when a User visits a publisher's site.

Ad impression

The display of an Ad Unit and reporting thereof.

Ad network

Platform that aggregates publisher inventory supply and matches it to demand. The term is falling out of use in favor of "ad exchange".

Ad Market

Used as short for "online advertising market".

Ad request

An API call that publishers send to ad exchanges with information about the inventory for sale and the current user visiting their site

Ad tag

Fragment of code that a publisher adds to their website to signal and characterize available inventory. Will cause an ad unit to be rendered, and generate an ad impression, if any demand source matches this supply signal.

Ad unit

Rendered ad, e.g. a banner image, interstitial video, full-page takeover, etc.

Advertiser

The term "advertiser" is used to refer to the entity on the buying side of the online marketing ecosystem[1] (in which case the word is not capitalized) and to a role in the Protocol (in which case the word is capitalized). The **Advertiser**, in the sense of participant in the Protocol, is interested in having its ads reach **Users** and, for this, the Advertiser posts **Ad Requests** in the Protocol.

Arbitrage Escrow

The **Arbitrage Escrow** is the escrow where **Verifiers** (potentially with liquidity provided by **Insurers**) deposit amounts equivalent to the **bid price** of the **Ad Claims** they wish to verify.

Attester

The **Attester** is a participant in the Protocol. The Attester is responsible for verifying Users' **Data Claims** and issuing **Credentials**.

Bid price

The **Bid Price** is one of the parameters of the **Ad Request**. This is the price per verified **Ad Claim** the **Advertiser** is willing to pay.

Credential

A **Credential** is issued by an **Attester** to represent their attestation of the legitimacy of a **Data Claim** made by a **User**.

Demand Side Platform (DSP)

Tool for advertisers to manage their campaigns and buy ads from ad exchanges and other aggregators of inventory.

Data Claim

A **Data Claim** is an assertion made by a **User** to an **Attester** that certain data is true about themselves.

Data Management Platform (DMP)

Tool used to store and manage information. Used in combination with DSPs (to inform buying decisions) or SSPs (to augment the ad request with additional information the publisher knows about the current user).

FCL

The Fractal token - the native token of the Protocol.

Insurer

The **Insurer** is a participant in the Protocol. The Insurer provides liquidity to Verifiers (needed to fund the **Arbitrage Escrow**).

Publisher

A publisher provides the capability and inventory that allows advertisers to run ads in their websites.[2]

[1] https://www.adjust.com/glossary/advertiser/

[2] https://www.adjust.com/glossary/publisher/

Protocol The Fractal Protocol presented in this white paper.

Required action The **Required Action** is one of the parameters of the **Ad Request**. In the protocol, the **Required Action** is an advertising model category (e.g., CPM or CPA).

Supply Side Platform (SSP) Tool for publishers to manage their inventory and its conditions and make it available to advertisers. This happens most often with real time bidding through ad exchanges.

User The term "user" is used to refer to people that use internet services (in which case the word is not capitalized) and to a role in the Protocol technically performed by a browser plug in or data wallet (in which case the word is capitalized). The **User**, in the sense of participant in the Protocol, sees **Advertisers'** ads and post **Ad claims** and **Data Claims** in the Protocol.

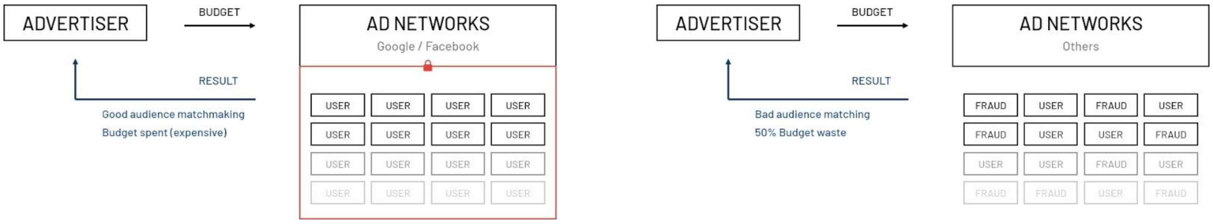
User characteristics **User Characteristics** is one of the parameters of the **Ad Request**. These are characteristics that the **User** needs to meet for the **Advertiser** to be willing to pay for the **Required Action**.

Verifier The **Verifier** is a participant in the Protocol. The Verifier is responsible for verifying the **Ad Claims** posted by Users. The Verifier verifies **Ad Claims** by putting the relevant **Bid Price** amount in the **Arbitrage Escrow**.

Abstract

This paper introduces the Fractal Protocol ("**Protocol**"), an open source protocol designed to replace the ad cookie to give users back control over their data. We want to create a data commons to enable fair competition against a market duopoly with valued users and trusted ads. The Protocol creates the market dynamics and the technical infrastructure needed to incentivize and enable a fairer distribution of value in the Ad Market.

1. Online Advertising Ecosystem



1.1. Online Advertising - A Livelihood for a Free Internet

Almost 30 years into the history of the web, online advertising remains the most viable monetization strategy for content creators and publishers. While some of the strongest global brands and an increasing number of niche publishers have seen some success with subscription models, the web at large remains devoid of alternatives[3].

Online advertising therefore remains the prime source of funding for most content on the Web. Hence, we do not believe that preventing online advertising is the best route to solve its issues (which are better detailed below in **Section 1.2.2** below). We prefer an approach that preserves monetization opportunities for content creators, protecting the prevalence of a free and open Web, while incentivising a realignment of the incentives in the Ad Market towards a better equilibrium.

1.2. The Current Dynamics

1.2.1. Overview

The Ad Market relies on the accurate targeting of potential consumers browsing the web. In turn, accurate targeting relies on the accumulation of accurate information about users. This makes users' data a valuable commodity on the internet.

In the current structure of the Ad Market, two main avenues are used to obtain users' data:

[3] Other attempts like micropayments for tipping lost their luster over time, as we have realized the extent to which users place a premium on frictionless consumption.

1. The users' behaviour is tracked throughout the web. Since the web is browsed anonymously, these tracking data are used to infer a demographic profile of users as their behaviour is observed (e.g., what sites they choose to visit or purchases they choose to make).
2. The largest advertising players, most relevantly Google and Facebook who dominate the digital advertising space by a combined market share of over 60% of the digital ad market[4], offer a sprawling collection of web products for "free", which enables them to gather user data and build accurate demographic profiles at an unprecedented scale.

The collected User data is then leveraged in the Ad Market. Although online advertising is one of the most complex digital ecosystems to date, we provide a simplified description of how online ads are sold and leveraged.

In the most common scenario, publishers use SSPs to sell ad space to advertisers via real-time auctions that happen in ad exchanges.

Publishers place ad tags on their sites' ad space. When a user visits their site, these ad tags send ad requests to ad exchanges, specifying the ad space properties (e.g. banner size) and ask price. The ad request can also include the data publishers have on the user visiting the site. Including quality user data in the ad request will increase the publisher's chances of selling the ad space at a higher price. This configuration is done through SSPs such as Google Ad Manager or Appnexus.

Advertisers configure their campaigns (collateral assets, budget, targeting) and buy ad space using DSPs like MediaMath. These DSPs plug into inventories from several ad exchanges and networks (e.g. Google Display Network). Ad exchanges make the bridge between SSPs and DSPs, and run very fast real-time auctions that match the advertisers' ads with the publishers' inventory and set the price at which publishers sell the ad space to advertisers.

1.2.2. Issues

The current Ad Market dynamics described in the previous section result in users' lacking control over their data, the sedimentation of a duopolistic and therefore inefficient market and rampant levels of fraud. This section provides insights on these issues, laying the grounds for an understanding of how the Protocol contributes to solving them.

1.2.2.1. Unconsented user data collection

As explained above, user data is an essential asset in the Ad Market and tracking users' behaviour throughout the web is one of the most common methods to obtain it. Users' behaviour is tracked using small text files placed on the users' devices as they browse - commonly known as "**cookies**". There are several types of cookies, but for the purposes of this paper the so-called marketing cookies are the most relevant: these cookies track users' online

[4] Facebook and Google are a duopoly with e.g. 60,7% market share in the US, 63% in the UK and 74,5% share in Germany. See eMarketer (2019) study "Facebook-Google Duopoly Won't Crack This Year", eMarketer (2019) study "Germany Digital Ad Spending 2019" and eMarketer (2019) study "Facebook and Google Control Ever-Greater Portion of UK Ad Market".

activity and share that information with other organizations or advertisers. These cookies are designed to be as persistent as possible - which means that they remain on the hard drive until erased by the user or by the browser at the end of the cookies' expiration date - and almost always placed by third party advertisers or analytic companies[5].

This tracking is pervasive, often unconsented[6] and opaque — and has been in decline. The decline of marketing cookies is attributed, on the one hand, to restrictions imposed by privacy regulators - for instance, the GDPR[7] and the ePrivacy Directive[8] prohibit the use of marketing cookies without free, specific, informed and unambiguous consent from the User (which is why we witness the proliferation of cookie banners); and, on the other hand, to the rise in popularity of ad blocking tech driven by a general annoyance at advertising and a growing mindshare of privacy concerns in the zeitgeist. Browser extensions such as Adblock Plus and uBlock Origin are used by hundreds of thousands of users, and browsers themselves have started making third-party tracking more difficult or even offering ad blocking as a feature.

Although the unconsented user data collection is an issue that needs a solution, these approaches, *per se,* fail to strike a good balance between privacy protection and the need for publishers to monetize their content, and actually also reinforce the duopolistic structure of the Ad Market (therefore undermining privacy protection).

1.2.2.2. Duopolistic market

Considering the multitude of products offered by the dupolists, some even considered "essential facilities" by antitrust regulators[9], the likelihood that the duopolists have relevant data on the user visiting the publishers' website is high (the user is likely to browse using Chrome, use Google search as their preferred search engine, have a Facebook or Instagram account, etc.). Google and Facebook's edge is that they enable publishers to leverage how much these giants know about their website visitors when competing to sell their ad space. The higher the quality and quantity of data publishers have on the users visiting their website, the higher the chances of being paid the most for their ad space.

The demise of third-party marketing cookies jeopardizes access to user data by other networks. To add to that, Google and Facebook silo user data because their business model depends on the exclusivity of these data sets. These factors further concentrate data access, reinforcing the duopolistic structure of the market.

[5] https://gdpr.eu/cookies/

[6] While the GDPR requires explicit consent to track users, the most common practice is to try to trick users into giving this consent through UI gimmicks, leaving users mostly unaware of what they have consented to.

[7] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[9] The qualification of digital platforms as essential facilities is explored in this article in the context of Google's appeal of the European Commission's abuse of dominance decision involving on-line comparison shopping services.

The concentration of power in the Ad Market is also fueled by the substantial network effects present in the duopolists' products (a social network that is not adopted by all your friends will not connect you; a search engine that is not used by everyone else will not deliver the best results). Network effects function as barriers against entry to anyone who proposes to challenge the duopolists' online empire.

1.2.2.2.1. Rent-seeking behaviour

As with any non-competitive market, no stakeholder benefits from the duopolistic structure of the Ad Market except for the duopolists themselves:

Any non-competitive market observes rent-seeking behaviour, and the Ad Market is no exception. Although the high prices practiced by Facebook and Google can in part be attributed to these platforms' capability of delivering better ad targeting (which is in itself a consequence of their market power), weak competition allows the duopolists to leverage their market power to earn higher prices than would be possible in a competitive market[10]. This increases the costs for advertisers, who are left with scarce alternatives to reliably reach users.

Publishers are left with a lower share of advertising revenues as they increasingly rely on third-party providers, most relevantly Facebook and Google, to increase the value of their ad inventory. Publishers also rely on the duopolists for traffic to their sites and content (a significant number of the Users that land on their websites clicked through a platform owned by Google or Facebook)[11]. Hence, there is an imbalance of bargaining power that results in publishers receiving low shares of the advertising revenues[12]. This decreases the publishers' ability to invest in free and independent content creation to the detriment of the broader society. As we will see below, the users themselves are entirely excluded from market participation — they are given limited agency over their data and its value.

1.2.2.2.2. Capped utility for Users

In addition to constituting a threat to a free-internet, the dupolistic structure of the Ad Market negatively impacts users by capping the utility available to them. The high switching costs, arising from the lock-in effects of social networks for Facebook and from the 86% market share of Google search[13], create an uneven playing field where users are not truly free to opt-out. Users, therefore, have no choice but to agree to share their data under the unfavorable terms imposed by Google and Facebook. The terms for data sharing are unfavourable to users

[10] In its market study final report on online platforms and digital advertising ("**Market Study**"), the Competition & Markets Authority highlights that *"in the UK, Google's revenue per search has roughly doubled since 2011, and our comparison of Google and Bing's search prices suggests that Google's prices are [30-40]% higher on desktop and on mobile when comparing like-for-like search terms. Facebook's average revenue per user has increased from under £5 in 2011 to more than £50 in 2019, and our comparison with other social media platforms suggests that it is now more than ten times higher than those competitors for which we have been able to obtain robust UK data."*

[11] Market Study, p. 318.

[12] In Market Study, p. 319, it is reported that *"intermediaries receive at least 35% of the value of advertising bought through the open display channel*".

[13] See Statista (2020) *"Worldwide desktop market share of leading search engines from January 2010 to July 2020"*

because they allow Google and Facebook to heavily monetize their data through digital advertising without offering adequate rewards. The value that these platforms provide to the user is capped at the utility value of their product, irrespective of the value of the data that the user provides in return - and, in a non-competitive market, even the incentive to maximise the utility value of their product is insufficient[14].

When given the opportunity to protect the privacy of their data (through the use of an adblock, for instance), this limits users' access to content since they are limiting the monetization opportunity for publishers. Users are left with an hobson's choice between data privacy and access to content and products.

1.2.2.3. Fraud and Attribution Uncertainties

Ad fraud and lack of data quality are also inefficiencies worth noting. "*Half the money I spend on advertising is wasted; the trouble is I don't know which half*" is a very telling advertising adage in this respect. Today, advertisers pay for bot interactions, irrelevant users and users they really want to target and cannot distinguish between them in advance.

Despite the ongoing consolidation, the sprawling ecosystem of vendors and tools has limited interoperability and this makes it hard for advertisers to understand how their budget is being split between the different adtech providers that sit between the advertisers and the publishers (e.g., marketing agencies, attribution partners, ad exchanges, fraud detection, data management platforms, etc.)[15]. The increasing technical sophistication of adtech solutions makes it harder for advertisers to confidently measure the performance of their digital campaigns. 74% of advertisers say they have little to no confidence in the data[16].

This lack of transparency helps ad fraud proliferate[17]. 56% of digital ad spend is served to the wrong audience, never actually displayed, or consumed by bots instead of humans[18]. With programmatic ad fraud rates between 10% and 30%[19] (which can go up to 80%[20] in heavily targeted campaigns), the industry has entered a technology arms race with fraudsters to detect fraudulent behaviour and resorted to accepting fraud and pricing it into their offerings.

[14] The Market Study, in p. 313, reports that "*these effects are already emerging. On Facebook, the average number of impressions served per hour has increased from [40-50] in 2016 to [50-60] in 2019. On Instagram, there were [60-70] impressions per hour in 2019, a more than 200% increase from 2016. This means that users of Facebook and Instagram are now seeing more ads than they were before. This increase in consumer attention devoted to ads can be expected to result in a reduction in the quality of the service for the user.*"

[15] https://www.iab.com/wp-content/uploads/2016/03/Programmatic-Value-Layers-March-2016-FINALv2.pdf

[16] https://resources.marketingeffectiveness.nielsen.com/blog/keeping-up-digital-advertising-challenges

[17] https://www.emarketer.com/content/digital-ad-fraud-2019

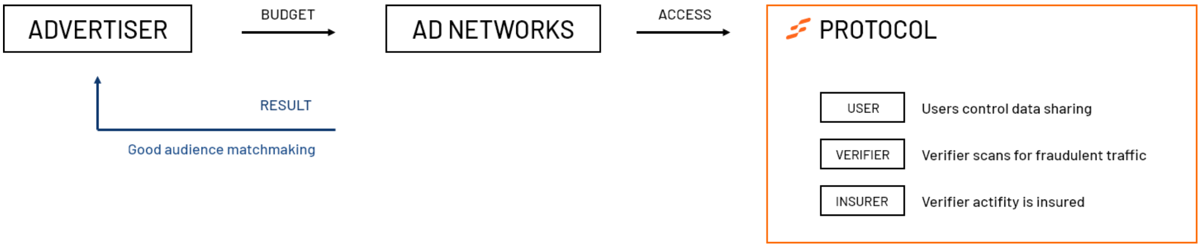
[18] https://resources.marketingeffectiveness.nielsen.com/blog/keeping-up-digital-advertising-challenges

[19] E.g. In Australia 30% of programmatic ads are fraudulent, while Japan (10%) and the U.S. (19%) showing lower rates. Data is based on Statista (2019).

[20] MarTech advisor's Michael Paxman reports that SDK spoofing can siphon off 80% of ad budgets.

Particularly, smaller advertisers lack the sophistication to target relevant users outside of the walled gardens of digital platforms without relying on expensive and opaque middlemen.

2. The Case for a Data Commons


ADVERTISER
BUDGET
AD NETWORKS
ACCESS
PROTOCOL
RESULT
Good audience matchmaking
USER
Users control data sharing
VERIFIER
Verifier scans for fraudulent traffic
INSURER
Verifier actifity is insured

The previous chapter establishes that, despite its continued growth trajectory, the digital advertising environment has not been working to the benefit of all its central stakeholders. Over the course of the past two decades, a plethora of middlemen have established themselves as facilitators in digital advertising, employing proprietary technology to create closed ecosystems, limit transparency, profiting off the obfuscation of performance metrics and annoying users.

Fractal argues that the tradeoff between the interests of users, advertisers and publishers does not need to be problematic, as long as each stakeholders' fundamental interests are protected at the protocol level. Users need to be empowered to control the data flows, free to switch between services, and fairly compensated for sharing their data. Advertisers need assurance that their budget is being spent on fraud-free traffic that satisfies their targeting criteria. Publishers need agency to lift up their inventory value through data and control how to fill their inventory. All participants in the digital advertising ecosystem stand to benefit from increased agency and transparency.

To achieve a new and improved equilibrium in digital advertising, we propose an incentive system for the sale and purchase of ad inventory built on transparent trustless infrastructure. This incentive system is enforced through the use of blockchain technology, delivering verifiable guarantees of said enforcement and a trustless public record allowing stakeholders to monitor each others' behaviour in a privacy preserving manner, which will in itself function as a disincentive to fraud. The Fractal Protocol fosters the transition to an accessible, competitive and fraud-free-by-design Ad Market.

3. The Fractal Protocol - A Data Commons

This chapter explains how the incentive system embedded in the Protocol tackles the inefficiencies of the incumbent Ad Market dynamics. It begins by describing the different roles interacting in the Protocol. Then, the chapter provides an overview of the different components of the Protocol. Finally, we summarize how these components work to incentivize a positive shift in the Ad Market.

3.1. Protocol Roles

The Protocol's goal is to connect Advertisers and Users, through a network of participants we call Verifiers, Insurers and Attesters. Below, we take a closer look at each role and how they interact with the Protocol.

3.1.1. Advertisers

Advertisers are entities looking to spread a message, for instance about their products or services. Advertisers are on the buying side of the Ad Market. Advertisers interact with the Protocol by posting Ad Buys. Advertisers pay for having their message reach their target audience and are reimbursed in case of perceived fraud.

3.1.2. Users

Users are people browsing the web. Users interact with the Protocol by submitting their data for verification by the Attesters, deciding whether or not to share it with Verifiers, and engaging with Advertiser's ads.

3.1.3. Verifiers

Verifiers connect Advertisers to Users. The role of Verifier can be performed by publishers, ad networks, ad exchanges and others. Verifiers interact with the Protocol by verifying Users' Ad Claims.

3.1.4. Insurers

Insurers provide liquidity to the Protocol and potentially receive staking rewards in return. Insurers provide liquidity to individual Verifiers (needed to verify users' Ad Claims) based on their reputation. Anyone with liquidity to provide could perform the role of Insurer.

3.1.5. Attesters

Attesters interact with the Protocol by issuing Credentials to attest Users' Data Claims. The Attester role could be performed by identity verification service providers or any entity that is able to confirm the veracity of a Data Claim.

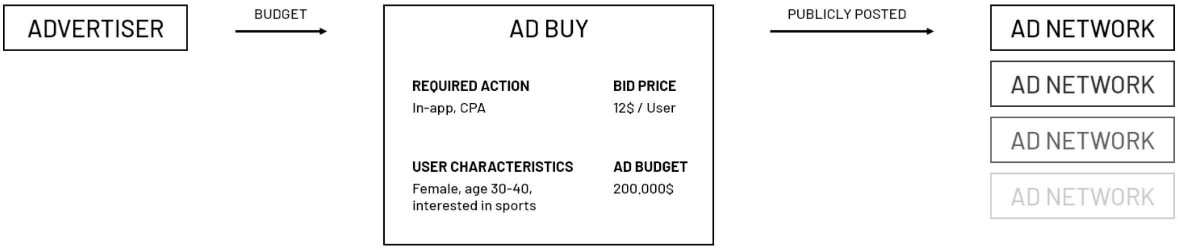
3.2. The Protocol Functionalities

The incentive system created by the Protocol relies on a set of functionalities that, together, enable a more efficient market for the sale and purchase of ad inventory. This section identifies and describes each of these functionalities.

3.2.1. Posting Ad Buys

An Ad Buy is a public sign of demand for a certain User action by an Advertiser. Ad Buys include the following parameters:

1. **Required action and action type** (e.g., CPA or CPM)
2. **User characteristics** (e.g. 30 - 40 years old or 'qualified investor')
3. **Bid price** (e.g. 40 USD equivalent / action)
4. **Ad Budget** (e.g. 4.000 USD equivalent in total)



Below we take a closer look into each parameter of an Ad Buy:

3.2.1.1. Required Action and action type

The **Required Action** is a descriptive indicator of the action Advertisers want Users to perform. Advertisers may want to optimize their campaigns for a broad range of results, from low-engagement to deeply-embedded behaviour. For instance, they might want to increase the number of users in their app, in which case they would optimize for number of downloads; or they can be looking to promote brand awareness, in which case they would optimize for impressions. Required Actions are categorized in different **action types** using advertising model categories: CPM, CPC, CPI, CPA[21]. This allows Ad Buys clustering, which in turn enables market comparability (see **Section 3.2.6** below on market price formation). Ideally, standards of action types that fully describe the Required Action will emerge. Verifiers confirm whether or not the Required Action was performed (see **Section 3.2.4** below).

3.2.1.2. User Characteristics

User characteristics define the audience the Advertiser wishes to target (e.g., 'Portuguese nationals', 'dog lovers'). The Advertisers' communication of the characteristics of their target audience and the Users' communication of their own characteristics would follow the same standard, so that accurate targeting is possible.

3.2.1.3. Bid Price

The **Bid Price** is the price per Required Action that the Advertiser is willing to pay. The Bid Price is potentially distributed between Verifiers, Insurers, Users and Attesters, as compensation for

[21] Cost-per-Mille (CPM) means the price that an advertiser is willing to pay for one thousand users to see an ad. Cost-per-Acquisition (CPA) is the price for one user completing a designated task (e.g., sign up for a service). Cost-per-Install (CPI) is the price for one user installing an app. Cost-per-Click (CPC) is the price for each ad click from a user.

verifying the Ad Claim, securing the Verifiers' activity, sharing data, and issuing Credentials to the User, respectively. The Protocol is agnostic to whether and how the Bid Price is distributed - the goal is to promote an efficient market that acts as a pricing discovery mechanism, where stakeholders are free to price their services.

The Bid Price is always paid in FCL, but can be denominated in stablecoin for cash flow predictability and stable prices. The Protocol will integrate an oracle functionality to make the exchange rate available throughout the network.

3.2.1.4. Ad Budget

The **Ad Budget** is the aggregate amount the Advertiser is willing to spend paying Bid Prices. The Ad Budget is set and deposited in FCL but, again, can be denominated in stablecoin using the oracle functionality.

To post an Ad Buy the Advertiser must put a certain percentage of the ad budget in escrow (the "**Ad Escrow**"). This mechanism prevents spam in the network, incentivizes Advertisers to remove ads that are not being picked up by Verifiers (or to adjust the Ad Buy parameters to the market) and secures payments.

The Ad Budget is deducted from a central address that is used to issue the Ad Buys. If the central address does not hold enough funds to pay the Bid Price, the Ad Escrow is used for payment. If the Ad Escrow is not sufficient, the Ad Buy is terminated.

3.2.2. Data Claims and Credentials

Users can share attestations of their characteristics and relying parties (in the protocol, Verifiers and Advertisers) can confirm such attestations exist and have not been revoked. Users make claims that certain data is true about themselves ("**Data Claim**") to Attesters (e.g., "I am a Portuguese citizen") and request Attesters to verify that such a Data Claim is truthful. The Attester performs the verification work according to certain criteria (e.g., requiring the submission of a Portuguese identity card). If the Attester determines that the Users' Data Claim is truthful, the Attester issues the User a "**Credential**". This Credential is transferred to the User's control (for example, stored in a browser plugin that functions as a data wallet) and from then on it can be shared with relying parties in a privacy preserving manner (ideally, the data flow would work in a way which enables relying parties to use the User's data without being able to access it). The credential issuance must be interoperable with the mechanism used by Advertisers to communicate the characteristics of their desired target audience, to allow for accurate matching.

3.2.3. Ad Claims

Empowered with Credentials, Users can decide to share data with Verifiers. When Users land on a website, the Verifier (which can be the website itself or a third party working with the website) makes an ad request enriched by the verified data the User potentially decided to share. The ad request communicates the ad inventory available and the characteristics of the

User visiting the website. The Verifiers' ad request will compete to win the Ad Buys posted by Advertisers. If the Verifier wins an Ad Buy, the relevant ad unit will be displayed to the User. Users' data wallets can claim that the User performed the Required Action specified in the Ad Buy ("**Ad Claim**"). Once an Ad Claim has been publicly posted, it is pending verification by the Verifier (see below **Section 3.2.4**). Siloing the Ad Claim and its verification in different actors (the User and the Verifier, respectively) increases transparency, therefore improving fraud monitoring (e.g. it allows for identification of Users with plenty of unverified Ad Claims regardless of Verifier, or Verifiers with plenty of fraudulent verifications regardless of User).

It should be noted that there is no on-chain mechanism that prevents Users from making Ad Claims without actually having performed a Required Action. It is the Verifier's role to confirm whether the User's Ad Claim is legitimate (see below **Section 3.2.4**).

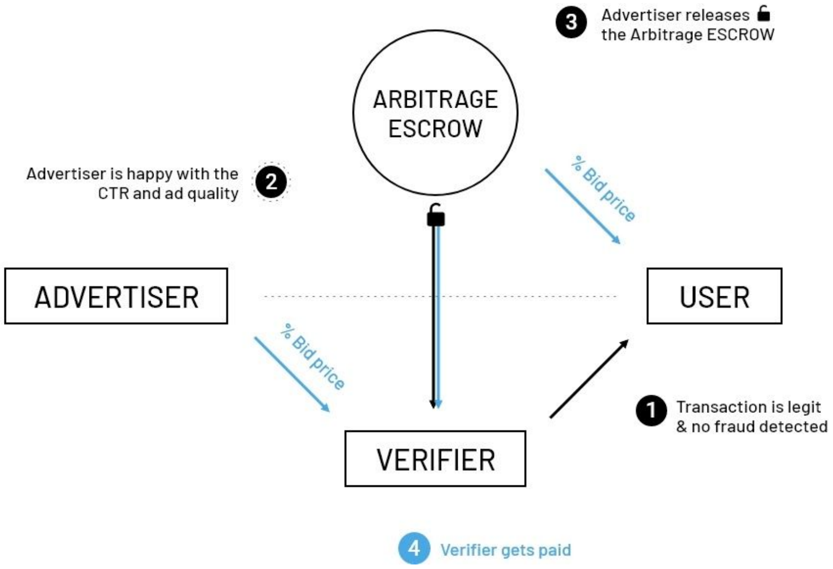
3.2.4. Verifying Ad Claims

Verifiers attest to whether Users' Ad Claims are truthful. This verification relies on signals not present on-chain and, therefore, the Protocol is agnostic to the criteria used by Verifiers to decide whether or not to attest Ad Claims. To confirm that an Ad Claim is legitimate, the Verifier puts the bid price amount in escrow (the "**Arbitrage Escrow**"). At this point two things happen:

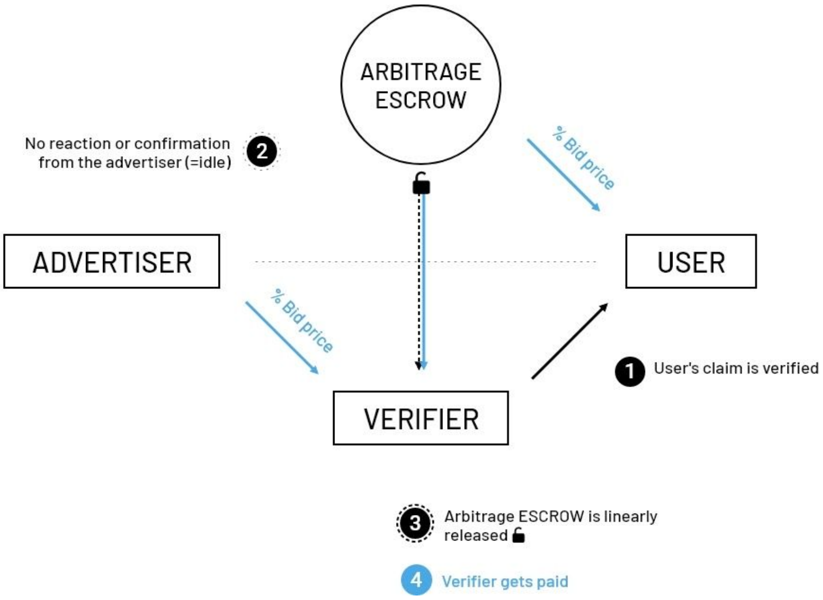
1. the share of the Bid Price that is due to the User, if any[22], is deducted from the amount in the Arbitrage Escrow and transferred to the User's wallet (eventually, this is distributed downstream to the Attestor);
2. the control over the Arbitrage Escrow account is transferred to the Advertiser. Three possible paths might follow:

    a) **The Advertiser releases the escrow back to the Verifier** (signaling that the Advertiser is happy with ad quality and thus the transaction is successfully finalized), in which case the Bid Price is also automatically transferred from the Advertiser's central address to the Verifier.

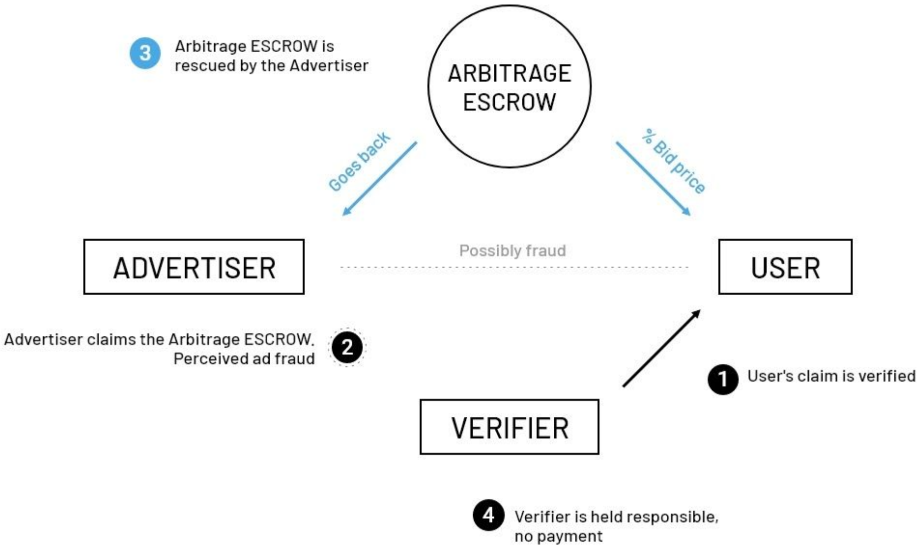
[22] The reward offered to the User for sharing data is not necessarily a share of the bid price. It can be, for instance, access to exclusive content on the publisher's website.


3 Advertiser releases the Arbitrage ESCROW
ARBITRAGE ESCROW
2 Advertiser is happy with the CTR and ad quality
% Bid price
ADVERTISER
USER
% Bid price
1 Transaction is legit & no fraud detected
VERIFIER
4 Verifier gets paid

b) **The Advertiser is idle**, in which case, after a certain time, the escrow and the Bid Price are linearly released to the Verifier.


ARBITRAGE ESCROW
No reaction or confirmation from the advertiser (=idle)
2
% Bid price
ADVERTISER
USER
% Bid price
1 User's claim is verified
VERIFIER
3 Arbitrage ESCROW is linearly released
4 Verifier gets paid

c) **The Advertiser rescues the amount in the arbitrage escrow** (signaling that the advertiser does not believe the Ad Claim to be truthful, contrary to what the Verifier attested), in which case Bid Price is not transferred to the Verifier.


3
Arbitrage ESCROW is rescued by the Advertiser
ARBITRAGE ESCROW
Goes back
% Bid price
ADVERTISER
Possibly fraud
USER
Advertiser claims the Arbitrage ESCROW. Perceived ad fraud
2
1
User's claim is verified
VERIFIER
4
Verifier is held responsible, no payment

There is no arbitration process for the Advertiser's decision on how to interact with the Arbitrage Escrow. Releasing or claiming the escrow is a final decision of the Advertiser and cannot be reversed. Although the Protocol does not require the Advertiser to prove that the Verifier was fraudulent in order to rescue the amounts in the Arbitrage Escrow, the transparent infrastructure of the Protocol provides a strong incentive for the Advertiser to appear honest (otherwise, the Ad Buys posted by Advertisers will be less attractive to other market participants).

3.2.5. Insurering the verification of Ad Claims

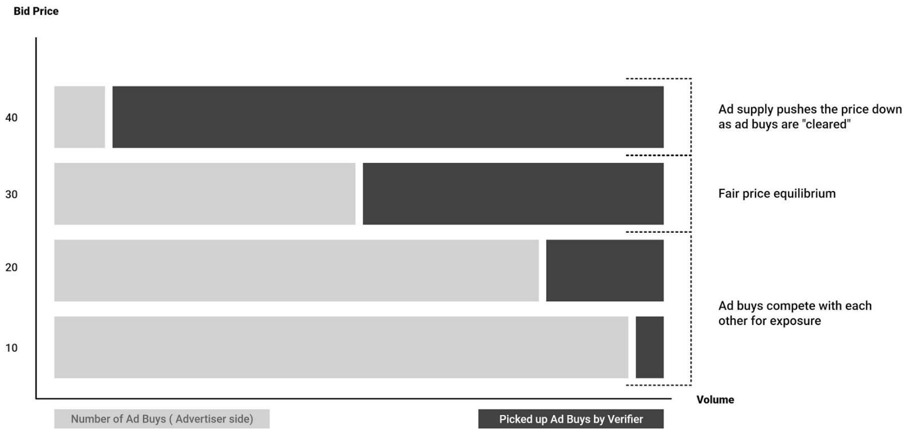
Insurers provide liquidity to the Arbitrage Escrow (see details about the escrow above in **Section 3.2.4**). Insurers can be anyone who wishes to lock-up funds (in FCL) in the Arbitrage Escrow with the goal of earning rewards.

Insurers stake FCL on Verifiers of their choice and, in return, receive a percentage of the payout that flows to those same Verifiers when an Ad Claim is verified and the Advertiser does not rescue the Arbitrage Escrow. The market acts as a pricing discovery mechanism for the percentage due to Insurers (e.g., Insurers should be able to command higher prices from non-reputed Verifiers). When Advertisers claim the Arbitrage Escrow, Insurers also participate in the loss. This creates a market dynamic where trustworthy Verifiers have more liquidity than fraudulent Verifiers. Because the liquidity Verifiers have in Arbitrage Escrows is directly related to the volume of Ad Claims they can verify, this results in more Ad Claims being verified by trustworthy Verifiers, therefore mitigating fraud within the Protocol.

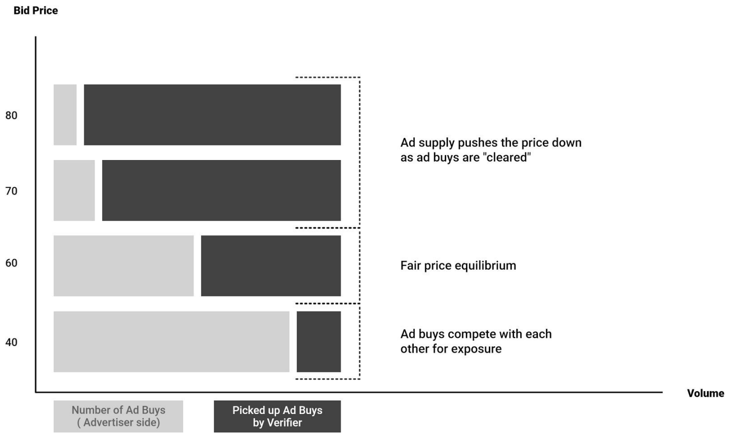
3.2.6. Market Price Formation

The combination between the elements of Advertisers' Ad Buys (required action, user characteristics, and bid price) and Verifiers' ad requests leads to evolving ad markets. Standardized communication of types of required actions and user characteristics enables a fair price-finding mechanism for different clusters. For instance, we could see demand and supply settling on an average bid price of €80 for 1000 impressions from North American Users aged between 18 and 21.

Segment 1 : "Male", CPA



Segment 4 : "North American", "Age 18-21", CPI



The market Bid Price resulting from the price formation described above will influence Users' price tolerance towards Verifiers, as well as the Attesters' willingness to verify the Users claims. How much revenue Verifiers' are willing to share with Users in exchange for their data and how much Users demand to receive will depend on the market price for the cluster at issue. Likewise, Attesters choose to verify User data only for Users who stand to generate a return on their investment.

3.3. The Achieved Equilibrium

The previous section already offers perspective as to how the Protocol enforces incentives for an accessible, competitive and fraud-free-by-design Ad Market. This chapter consolidates this knowledge by connecting the issues identified in **Section 1.2.2.** above to the solutions explained in the previous section.

3.3.1. Data Sovereignty

Today, the Ad Market mostly relies on user data that is collected through pervasive, unconsented and opaque tracking of users' behaviour online, or that is, often unconsciously[23], provided by Users in their almost unavoidable use of the products offered by Google and Facebook (most relevantly). The collected data is never in control of its true owner, the user, and only the third-parties collecting it can leverage it on the Ad Market.

The identity layer of the Protocol enables Users to take back control over their data. User data is not collected and appropriated by third-parties. Users can resort to a network of Attesters that are incentivized to verify their Data Claims. Users control the Credentials that are issued to them and can decide whether and how to share them with Verifiers.

3.3.2. Competition

The death of third-party cookies and the siloing of user data by Facebook and Google concentrate data access on these two players, sedimenting their Ad Market duopoly. High entry barriers and network effects make it unlikely that Google and Facebook's duopolistic control over the Ad Market will be disrupted by the emergence of new players that endanger their position.

Only the creation of a data commons, as proposed in the Protocol, can foster healthy competition, erode rent-seeking duopoly margins and increase the utility available to Users. The Protocol breaks data access exclusivity by creating incentives and infrastructure for Users to share verifiable data about themselves, which can in turn be leveraged by Verifiers to sell their ad inventory, and trusted by Advertisers when buying it. Increasing competition in the Ad Market lowers the rent-seeking margins kept by the incumbent dupolists and therefore improves advertisers' return on investment, increases the revenue potential for publishers and unlocks the utility that users can derive from sharing their data. The Protocol therefore strikes a better balance between data sovereignty and the need for publishers to monetize their content, essential to the survival of independent content creation and a free internet.

3.3.3. Fraud Arbitrage and Prevention

The lack of transparency and data quality in the Ad Market exposes advertisers to paying for undesired and fraudulent traffic. When fraud is detected post payment, advertisers need to engage in often long and opaque negotiations with networks to recover the unduly paid amounts.

[23] The Market Study reports, on pp. 14 and 15, that "*very few consumers read privacy policies when signing up to an online service and the evidence we have gathered confirms this: for example, in a recent 28-day period, the average visit to the Google privacy page was just 47 seconds, with 85% of visits lasting less than 10 seconds. The upshot of this is that users understandably simply agree to the default choices they are presented with. These are set by the platforms, and it is hard to be confident that they will adequately balance users' preferences about the use of their personal data against the substantial benefits to the platform.*"

The Protocol allows for standardized and interoperable communication of target audience characteristics. On the Protocol, Advertisers use a standard that is accepted and understood by Verifiers to communicate the characteristics of the desired traffic. This increases data quality and enables a straightforward understanding of whether the generated traffic is desired or undesired and, therefore, of whether or not payment is due. In another front, the arbitrage escrow mechanism enables advertisers to analyse their traffic before incurring the risk of paying for wrong or fraudulent attributions (therefore avoiding post payment discussions) and incentivizes the organic exclusion of fraudulent Verifiers, who would lack Insurers' vital support.

4. Implementing the Protocol in the Application Layer

This chapter describes the current plan for the technical implementation of the Protocol. We will build the Protocol using a staggered approach, where we will deliver small components that can add value on their own and plug them into the existing ad tech stack. In parallel, we continuously work towards building the whole Protocol, leveraging the learnings from those integrations and adapting to new market realities. Throughout this process, the technical proposal described in this chapter will evolve.

4.1. Web2 components - Protocol user stories

In **Section 3.2** above we described the functionalities of the Protocol and how its participants interact to form a market for the sale and purchase of ads. This section describes the web2 components that support those interactions.

4.1.1. Advertisers

4.1.1.1. Posting Ad Buys

Advertisers would use our web application or API to show an ad unit to a given audience. The web application or API would enable Advertisers to do the following:

1. Upload the relevant ad collateral (images, videos, etc);
2. Create an Ad Buy and set up its parameters (see **Section 3.2.1.** above);
3. Place a percentage of the total Ad Budget in the Ad Escrow.

4.1.1.2. Releasing / reclaiming Arbitrage Escrow

The Advertiser can use our web application or API to monitor Ad Claims and Verifiers' attestations of such Ad Claims. Based on the result of this analysis, they can then interact with the Arbitrage Escrow to release funds to the Verifier, or rescue funds in case of perceived fraud. The application helps them:

1. Analyse the Ad Claims' attestations made by the Verifier;

2. Release funds from the Arbitrage Escrow if the Verifier's attestation is deemed legitimate;
3. Rescue funds from the Arbitrage Escrow if the Verifier's attestation is deemed fraudulent.

4.1.2. Users

4.1.2.1. Making Data Claims and sharing Credentials

Users will interact with the protocol in mostly two ways: directly through our browser plugin (which functions as the Users' data wallet), or indirectly by delegating this responsibility to the website owner (which may be a Verifier or a publisher working with a Verifier). Users can use our browser plugin to:

1. Request and store Credentials issued by Attesters (in principle using the KILT protocol - see **Section 4.3.1** below)
2. Set preferences regarding which parts of the Credentials to reveal (e.g. location but not name, age range but not age)
3. Set preferences regarding which publishers/websites to allow or disallow the reading of their Credentials.

4.1.3. Verifiers

4.1.3.1. Engaging with Ad Buys

The Verifier is looking for Ad Buys for which they believe they can attract Users to fulfill the respective Required Action. A Verifier uses our web application or API to explore Ad Buys, to then work with publishers (when the Verifier is not the publisher itself) to serve them to the right Users.

4.1.3.2. Verifying claims

A Verifier is confident that a user performed the Required Action and wants to attest the User's Ad Claim. The Verifier can use our web application or API for this. This helps them:

1. Attest the legitimacy of the User's Ad Claim;
2. Secure the transaction by placing the Bid Price in the Arbitrage Escrow.

4.1.4. Insurers

4.1.4.1. Verifier liquidity provisioning

An Insurer trusts the work of a particular Verifier and wants to provide liquidity for their Arbitrage Escrow. The Insurer can use our web application or API for this. This helps them:

1. Understand the reputation and performance of Verifiers;
2. Back a Verifier by increasing the liquidity of their Arbitrage Escrow and therefore their reputation and potential scale;
3. Collect their share of the payout.

4.2. Web3 components - Security, scalability and interoperability

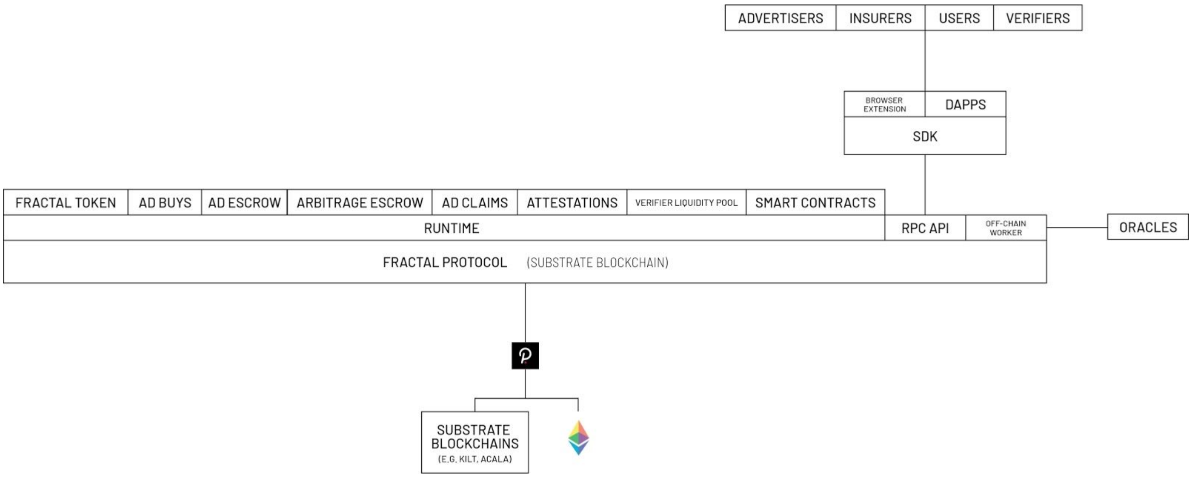
We have the technology.
— The Six Million Dollar Man, Opening Narration

We intend to build the Protocol on Polkadot. In this chapter we justify this choice by explaining the advantages that Polkadot brings to the implementation of the Protocol.

Polkadot provides us with appropriate tools and infrastructure for successful development and deployment of the Protocol, without the compromises we would have to make with other platforms.

Their vision is of a world with multiple blockchains, each tailor-built for a specific purpose[24]. In order to deliver on this vision, Polkadot created Substrate (an SDK for Polkadot-compatible blockchain building) and an infrastructure to connect and secure these unique blockchains[25].

Parachains are Substrate-based blockchains with their own runtime logic. They benefit from the pooled security and cross-chain messaging provided by the Relay Chain[26]. Building a Substrate-based chain allows for more, lower-level control and flexibility over, for instance, fee structures and monetary policy. Alternatively, a Substrate-based chain can also connect to the Relay Chain as a parathread[27], which is similar to a parachain but with less execution and pricing guarantees. These operate in a pay-as-you-go model.



Fractal protocol as a Parachain

[24] https://polkadot.network/PolkaDotPaper.pdf
[25] https://wiki.polkadot.network/docs/en/getting-started
[26] Polkadot's chain, the Relay Chain, is deliberately bare and does not support smart contracts itself. However, Substrate offers two pallets for smart contract functionality, supporting Wasm and EVM. Smart contracts functionality will be made available through purpose-built parachains making use of these pallets. Edgeware, despite naturally not yet being connected as a parachain, is live with its own validator set, and supports both ink! (Wasm) and Solidity (EVM) smart contracts. Moonbeam is close to a production deployment and will focus initially on EVM, bridging to Ethereum, and providing network migration support.
[27] https://wiki.polkadot.network/docs/en/learn-parathreads

4.2.1. Pooled security

Building a unique blockchain is often the only way to get around issues of transaction costs and scalability of the currently available public infrastructure such as Ethereum. Securing a unique blockchain is no easy feat: they require the recruitment and continuous incentivization of validators in order to keep attackers at bay.

Polkadot addresses this issue by offering a Relay Chain with its own validators, whose provisioned security is pooled and shared among the unique blockchains connected to it.[28]

4.2.2. Scalability and cheaper transaction fees

Polkadot is able to process 10,000 times more transactions per second than what Ethereum can currently offer[29]. This is a staggering improvement to scalability, a critical requirement for projects like ours which anticipate and require high frequency blockchain usage.

A consequence of this massive performance uplift is the corresponding decrease in competition for bandwidth. Together with the ability of unique chains to control their own transaction fees, this provides an environment in which scale is not only possible, but accessible.

4.2.3. Interoperability

By securing these purpose-built unique blockchains, Polkadot allows developers to focus on building the blockchain that is fittest for their use case. By connecting them, they make it possible to leverage functionality available in other blockchains[30]. Additionally, Polkadot is currently building bridging infrastructure to enable unique blockchains to communicate with other non-Substrate blockchains such as Bitcoin and Ethereum.

It is worth noting that while Polkadot's mainnet has been released and is live[31], the Polkadot ecosystem is still under active development. In particular, parachain functionality is not yet available in the live network, and consequently neither is smart contract support.

4.3. Integrations

One of our reasons for choosing Polkadot was the interoperability it facilitates, and we intend to leverage existing and promising infrastructure as much as we can.

4.3.1. Identity credential issuance and verification

Verifiable data is core to the Fractal protocol. We require a way for users to prove they have credentials on their data, and for relying parties to confirm these credentials exist and have not

[28] https://wiki.polkadot.network/docs/en/learn-security
[29] https://wiki.polkadot.network/docs/en/learn-comparisons#ethereum-1x
[30] https://wiki.polkadot.network/docs/en/learn-crosschain
[31] https://polkadot.js.org/apps/#/explorer

been revoked. KILT[32] is a protocol built on Substrate for issuing self-sovereign verifiable, revocable, anonymous credentials. The current implementation plan foresees integration with KILT to support this functionality of the Protocol. KILT's core functionality is roughly as follows:

A KILT claimer (a Protocol User):

- pays the attester for an attestation on their claim (a credential)
- sends the credential to a verifier

A KILT attester (a Protocol Attester):

- verifies the claim and attests it, creating a credential
- returns a credential to the claimer
- stores the credential hash on-chain

A KILT verifier (a Protocol Verifier):

- trusts an attester
- gets credential from claimer
- verifies that the credential hash exists on-chain
- asks the claimer for a signature to confirm credential ownership

An alternative to support this functionality of the Protocol would be integrating with Dock[33].

4.3.2. Stablecoin and price oracle

Ad Budgets and Bid Prices are denominated in a stablecoin for Advertiser cash flow predictability. We need an Oracle to produce and feed the FCL / stablecoin exchange rate for this operation. The Acala Network[34] might be able to serve both functions, since they not only provide a stable aUSD token, but also price oracle functionality. The PolkaOracle[35] project offers an alternative to this oracle.

5. FCL Token Functions

We intend that the FCL token functions as the Protocol's native cryptocurrency, fueling the incentives mechanism embedded in the Protocol. We identify the following utilities of the FCL Token:

1. Advertisers pay Bid Prices in FCL;
2. Advertisers stake FCL in the Ad Escrow;
3. Verifiers stake FCL in the Arbitrage Escrow;
4. Insurers stake FCL in the Arbitrage Escrow;
5. Users pay Attesters for their Credentials in FCL;
6. Attesters receive FCL for issuing Credentials.

[32] https://www.kilt.io/
[33] https://www.dock.io/
[34] https://acala.network/
[35] https://www.polkaoracle.com/

We are also exploring the possibility of using FCL to incentivise early adopters of the Protocol (e.g., offering Users the opportunity to stake protocol tokens on their attested data).

In a later version of the white paper we will go into further details about the FCL token, in particular regarding issuance, distribution and economic modeling.

6. Open Issues

6.1. Publisher integration

In order to encourage adoption, we must ensure onboarding for publishers and other Verifiers is as simple as possible. Enabling publishers to request and use user data should not require expert knowledge or large investment. More research is needed to understand the integration capabilities of common SSPs and DMPs, and how we can circumvent any limitations here with custom code.

6.2. Potential for abuse

Further modeling is needed to develop a threat model. Some of the immediate suspects regarding abuse on the part of users seem to be easily addressable. If we decide for a revenue share model, a user repeatedly visiting the same publisher website would only stand to increase their yield if the publisher's yield increases as well. Advertisers' frequency capping choices would be similarly unaffected since their choice not to bid on an ad request is not something the user has the ability to influence.

6.3. Privacy implications

Great care must be taken when considering enabling and incentivizing the sharing of personal data. This is not only true from a legal perspective but also, and more importantly, from an ethical one — especially given how privacy regulation tends to lag technological progress.

6.3.1. User assurance

It is important that Users feel that they are sovereign of their data, in particular that they observe that no data is ever shared without their informed consent, including by data wallet creators. While an open ecosystem allows for malicious data wallets to leak information, the user can be nudged towards choosing a data wallet from a curated list of trusted, open-source, and audited alternatives. Further modeling is needed to develop a framework that disincentivizes malicious behaviour.

6.3.2. Data hoarding and re-identification

The issue of data hoarding is harder to address. Once a User shares data with a Verifier, the Verifier must be prevented from storing, leaking or reselling these data. This could turn especially problematic if the data are used for re-identification: the process of de-anonymizing a User by correlating multiple data points related to said User.[36]

Mitigating this issue requires a more nuanced approach to data sharing. Ideally, the data flow would work in a way which enables Verifiers to use these data without being able to access them. This is a hard challenge, and solving it completely requires further research. Homomorphic encryption in particular presents a promising solution space. Data minimization techniques also approximate a solution to this problem. By way of example, suppose a scenario where a Verifier is looking to know the age range of a User who has their passport in their data wallet. A naive approach might be to share all passport data with the Verifier, who could easily derive the age range from the date of birth the passport states. A better option is to use a zero-knowledge proof such as a zk-SNARK[37]. This technique would allow this User to prove to the publisher that they are indeed within a certain age range, without needing to share their actual birthdate, much less the entirety of their passport information.

6.3.3. The unraveling effect

The unraveling effect is an emerging property afflicting certain systems which incentivize data sharing. Left unaddressed, it results in system participants being forced to share data against their will. This happens in scenarios where the choice to not disclose certain data is taken as prima facie evidence that these data are compromising for their owner.[38]

As a simplistic example, picture a health insurer who charges higher premiums to policyholders who smoke. In this scenario, a sufficient number of those choosing to offer evidence of their not smoking is bad news for those who choose not to follow suit. If a non-smoker is not willing to prove that fact about themselves, they will face a steeper bill — not because of any actual additional risk, but due to the health insurer assuming their silence is acquiescence.

Partial mitigation could be achieved through placing restrictions on the kinds of data that can be requested. We do not believe this is a good solution, as we prefer the protocol to be as flexible as possible in terms of data agnosticism. As such, we are exploring technical solutions such as homomorphic encryption[39] and differential privacy[40], both promising candidates for mitigating this issue.

Bayesian privacy[41] is particularly relevant, as it offers a mechanism for injecting noise into a dataset. The amount of noise is provable and does not significantly reduce the quality of the whole dataset. This would allow publishers to keep leveraging the data the user chooses to share, without being able to tell, for a particular user, if the data is correct or not — all the while knowing, and being able to prove, the average level of correctness.

[36] https://en.wikipedia.org/wiki/Data_re-identification
[37] https://z.cash/technology/zksnarks/
[38] https://scholar.law.colorado.edu/articles/177/
[39] https://en.wikipedia.org/wiki/Homomorphic_encryption
[40] https://en.wikipedia.org/wiki/Differential_privacy
[41] https://www.springer.com/gp/book/9789811368363 ,
https://economics.princeton.edu/working-papers/bayesian-privacy/

6.4. Remarketing

Data wallets (through which Users interact with the Protocol) could be used for remarketing without third-party cookies. Instead of asking the browser to store it and give away control over expiry, the advertiser can just talk to the extension, which then relays the same identifier to the publisher.

6.5. Protocol Governance

We intend for the Protocol to work as a decentralized network. However, as is often the case, the Protocol is starting out as a technology project where Fractal's team, the core developers and our network of advisors make the decisions. We are prototyping the governance system that is sensible to implement once the Protocol matures and the founding team steps away. Later versions of the white paper will shed light on the governance systems we are considering.

Legal Note

The purpose of this white paper is to share our current vision for the Protocol and future plans.

This white paper is not exhaustive and does not include elements of any contractual relationship. The white paper shall not be deemed to constitute a prospectus of any sort or a solicitation for investment or investment advice; nor does it in any way pertain to an offering or a solicitation of an offer to buy any securities in any jurisdiction.

For the avoidance of doubt, please note that the Protocol has not been fully developed and the FCL tokens have not yet been created. Any statements made about the Protocol and/or the FCL tokens in this white paper are forward-looking statements that merely reflect Fractal's intention for the functioning of the Protocol and/or of the FCL tokens. There are known and unknown risks that can cause the results to differ from the forward-looking statements.

Fractal does not intend to express investment, financial, legal, tax, or any other advice and any conclusions drawn from statements in this white paper or otherwise made by Fractal shall not be deemed to constitute advice in any jurisdiction.

Imprint

Trust Fractal GmbH
Wiener Straße 10, 10999 Berlin, Germany
Managing Directors: Julian Leitloff, Júlio Santos
E-Mail: support@fractal.id

Registered at the Handelsregister Charlottenburg under the number 198469 B
VAT ID pursuant to § 27a Umsatzsteuergesetz DE 315012567

Call for Feedback

The progress of the Protocol benefits from feedback from any and all interested parties. We encourage you to engage with us by joining our Telegram Community (https://t.me/fractal_protocol) or writing to us at support@fractal.id. We look forward to hearing from you.