Scoring and Rewarding

Parami Devs devs@parami.io

March 11, 2022

Abstract

We design and implement scoring and rewarding algorithms to help building auditable, reliable, reusable decentralized profiles[1] to drive the de-authoritative advertisement network.

I. Introduction

Scoring and rewarding is the cornerstone of Parami Protocol. The scoring algorithm is the key function to avoid fraud and spamming in the AD3 network. Where it provides nonintrusive universal unique decentralized identifier. People can earn rewards from advertiser directly by using their decentralized profile.

II. Goals

With the design of Parami Protocol, the goals of the scoring and rewarding algorithm are:

- Data should be shared with peers in decentralized way
- Show every score activity is based on payment
- Reward identifier based on scores when advertiser confirms
- Smurfs should have low scores
- Detect dummy identifiers

III. Implementation

i. PCAP

The Personal Crypto Advertising Preference (PCAP) 1 [2] provides an auditable and reliable way to store scores of an identifier.

An identifier can have multiple tags, each tag gets a score between -100 and 100.

To protect privacy, currently, a tag is hashed and stored opaquely. The half-opaque profile will be moved to full-encrypted PCAP in the near term by using the Paillier[3] Homomorphic Encryption and Zero-Knowledge Proof scheme.

Tag	Score
Telegram	5
Ethereum	2
Kusama	7

Table 1: *Example decrypted PCAP*

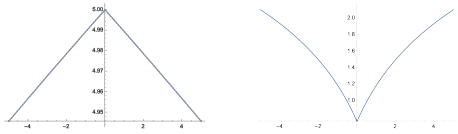

Figure 1: *s'' curve at ds=5*

ii. On-Chain Scoring

To prevent scores from fraud, the On-Chain Scoring algorithm is designed as a nonlinear

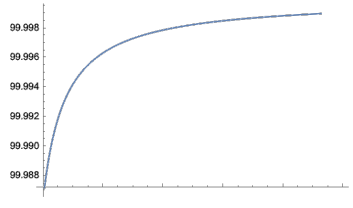

Figure 2: *scoring curve*

Tags	
Kusama	Polkadot
Discord	Telegram

Table 2: *Example Advertisement*

function 1,

$$s'' = \begin{cases} \Delta s * log_{102}(102 - |s|) & \cdots s * \Delta s \geq 0 \\ \Delta s * log_{102}(|s| + 2) & \cdots s * \Delta s < 0 \end{cases}$$

it takes as input $-100 < \Delta s < 100$ and updates the state as follows:

$$(s) \xrightarrow{\Delta s} (s')$$

It is obvious that solution of the formula is on the interval (-100, 100).

iii. Rewarding

When an advertiser confirms to send rewards to an identifier, the On-Chain Rewarding algorithm compute the rewarding weights of the identifier.

Only matched tags participate in computing the weight and reward as follows:

$$\begin{aligned} Matches &= Tags \cap PCAP, \\ Weight &= \frac{\sum_{n=1}^{m} Match_n}{c}, \\ Reward &= Weight * Base \end{aligned}$$

where c is the number of *Tags*, m is the number of *Matches*.

Thus weight for a normal identifier 1 is:

$$\frac{Kusama(7) + Telegram(5)}{4}$$

Sum of weights from Smurfs is, for example:

$$\frac{Kusama(7)}{4} + \frac{Telegram(5)}{4}$$

It is trivial to see Smurfs get less rewards normally.

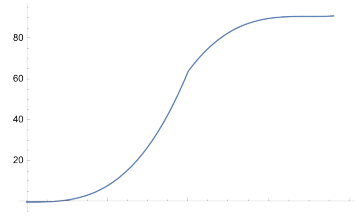

Figure 3: *example curve*

IV. Discussion

Currently, the scoring and rewarding algorithms do not provide the ability to prevent dummy identifiers or Smurfs. We're working on them to solve these issues.

i. Dummys

We suggest advertisers:

- Protect website with challenge–response test such as CAPTCHA
- Use more effective advertising type like CPA, CPS, and etc

We consider providing On-Chain APIs (extrinsics) to allow advertisers:

- Set conditions for payouts
- Score an identifier without pay rewards
- Submit proposals to mark frauds and dummys

ii. Smurfs

A new scoring algorithm may avoid Smurfs, for example 3.

Money streaming is also a option to do so.

References

[1] Manu Sporny, Dave Longley, Markus Sabadello, Drummond Reed, Orie Steele, and Christopher Allen "Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations" August 2021

[2] Parami Devs “Parami Protocol Lightpaper Building Ad 3.0 For Web 3.0” January 2021

[3] Pascal Paillier “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes” April 1999