PARAMI

Parami Protocol Lightpaper

Building Ad 3.0 For Web 3.0

Version: 1.0.0
2021-01-20

Definition & Motivation

“AD 3.0 is a human-centric and privacy-preserving network powered by blockchain, where users are smart-rewarded for attention and data while their self-sovereign identity is protected on a trust-free basis.”

AD 1.0: Era of Slavery

The AD model is inefficient and not transparent. Advertisers are faced with ambiguousness and fraud while users’ data are being monetized without consent. Users become DATA SLAVES when they have no right over their data and cannot benefit from their engagement.

AD 2.0: Era of Feudalism

Incentive AD return parts of profits back to users but users are still not in charge of their own identity and data.

Data are dispersed and isolated in various apps and websites where they can not be aggregated and utilized.

AD 3.0: Era of Democracy

The AD network is democratic and governed by all token holders. The future network traffic is directly generated from the influence of each creator and token holders, instead of being acquired from a certain website or application.

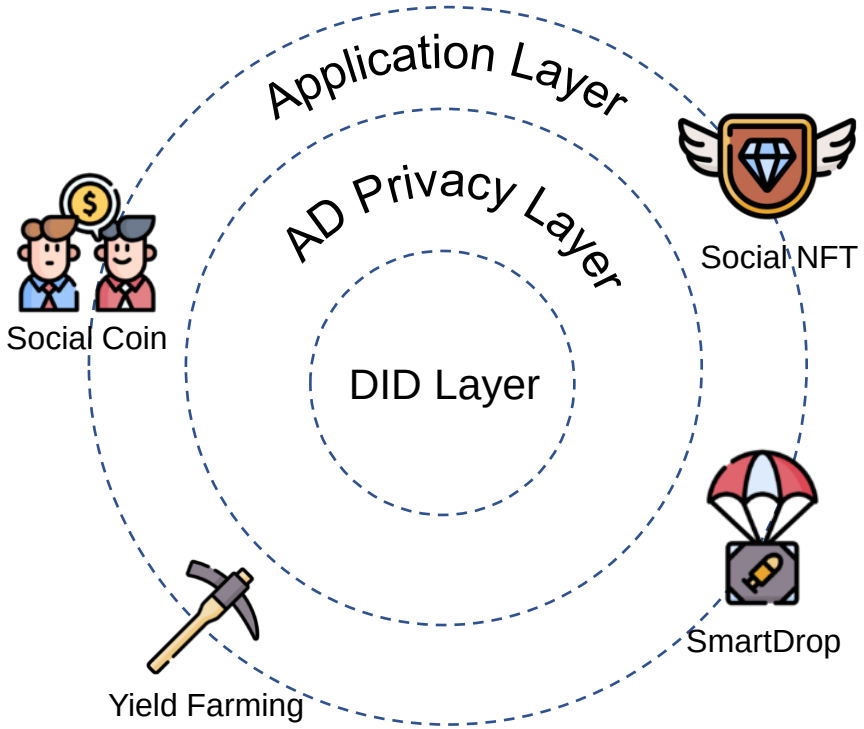
Users have absolute sovereignty over their own identity and data. They will receive smart-reward based on their attention paid and relevance score.

Definition of Important Terms:

1. AD: Advertisement; Ads: Advertisements
2. Smart-Reward: A reward given to users automatically based on their behaviour, attention paid and data contributed in the network/online.

Protocol Overview

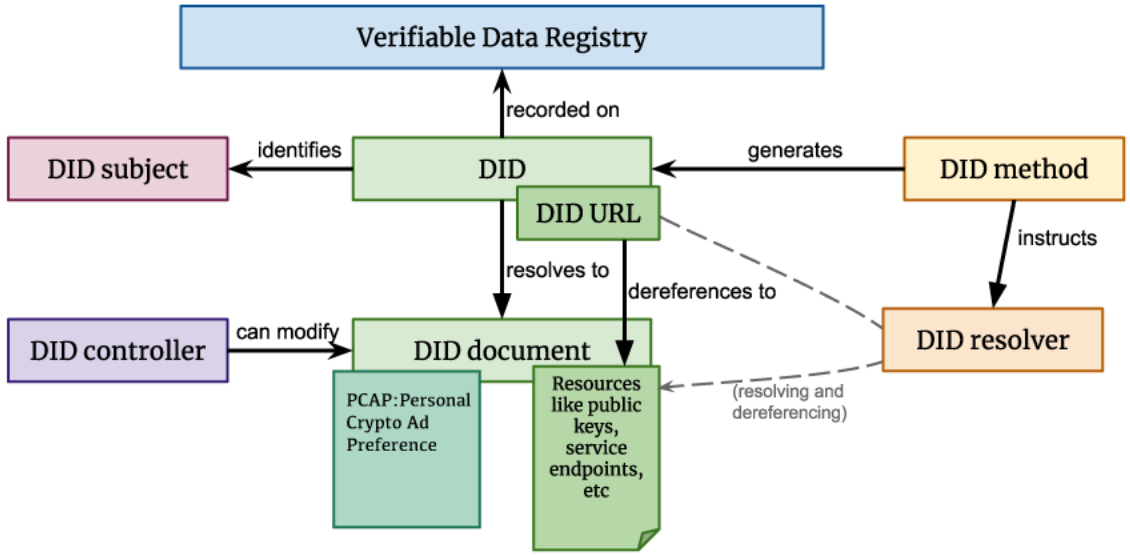
Parami Protocol proposed an AD 3.0 paradigm powered by blockchain for Web 3.0. It provides a protocol stack for building a user-centric, tokenized advertising economy. As a parachain built on Substrate, it serves all the other parachains in Polkadot/Kusama through relaychain.



- **DID Layer**: Decentralized Identity management including registry, update and revoke. DID aggregates both social media identities and blockchain identity.
- **AD Privacy Layer**: Privacy on advertising, including private file bonding, updating and monetization.
- **Application Layer**: Tokenized activities such as SmartDrop, Yield Farming, Social Coin Generation and NFT

Protocol: DID

Parami Protocol provides a complete set of PDID (Parami DID) solutions compatible with W3C DID standard on Parami Node, and expands its business on the basis of DID standard. Parami Protocol will also provide DID aggregators for other DID standards.

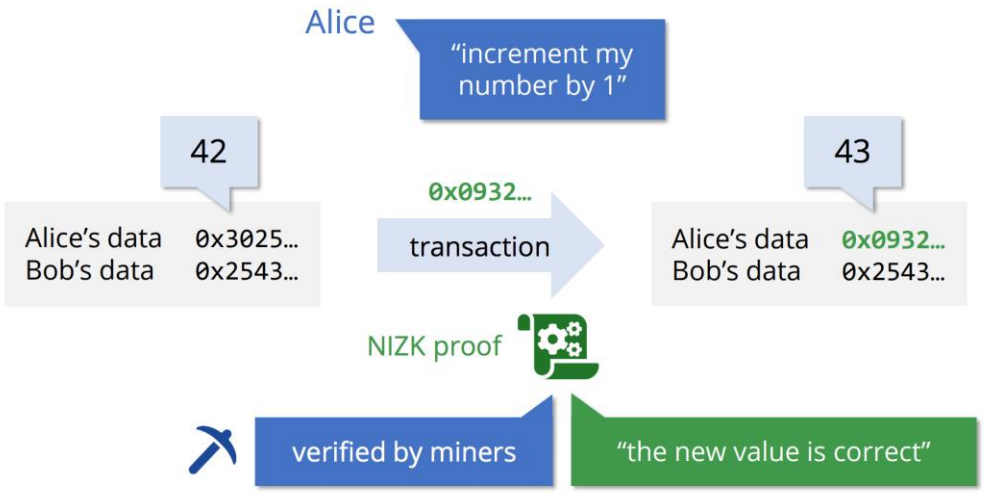


Parami DID extension

- **Web2.0 Compatible**: Parami DID provides a verification method that can connect to users'Web 2.0 social media identities.
- **NO KYC**: PDID allows users to verify DID uniqueness by building social graphs and running anti-sybil analysis without any KYC process.

Protocol: AD Privacy

The AD Privacy Layer provides a personal crypto advertising preference (PCAP) document attached to user DID, which contains user advertising privacy management service. The PCAP document works not only for payment but also for user preference data. The preserved data can be used but can not be seen.



ZKP based User Privacy Update

Blind Signature

Advertisers use blind signature to prove they have confirmed user interaction with AD, which avoid further malicious behavior.

Homomorphic Encryption

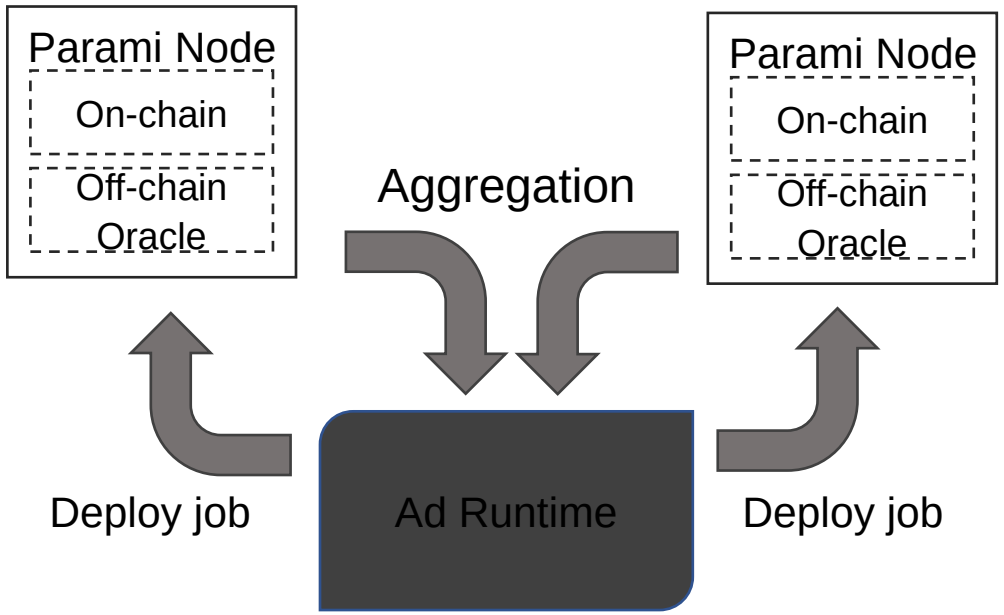
User crypto advertising preference (PCAP) data is homomorphic encrypted so that advertisers could update users'PCAP in an encrypted way.

ZKP based

The Zero-Knowledge Proof （ZKP）algorithm is used so that users can get the reward he/she deserves. The ZKP generates the corresponding proof and verifiy it on-chain to determine the reward.

Protocol: Application layer

The application layer provides decentralized oracle to collect data from conventional Internet for Ad verification. It also defines the interfaces for tokenized advertising dapp to get AD privacy support.



De-oracle for Ad verification

- **PCAP data fetch**: Dapp can fetch PCAP data (ZKP) of some DID to determine and verify the user reward he/she deserves.
- **PCAP data update**: Dapp can update (scoring some tags) PCAP data each time it sends reward to users, with updated data encrypted homomorphically.

More Highlights

IM support

Parami is designed for IM apps. The Parami SDK will support users to participate in Ad interaction in IM explorer or MiniApps.

DAO support

Parami will support other DAOs as seed groups to expand DID ecosystem. Other DAOs can register on Parami and manage their DAOs on it for extra incentive.

Governance support

Parami Protocol is fully governed by all token holders. They can vote for the council and all the proposals to optimize the network.

NFT support

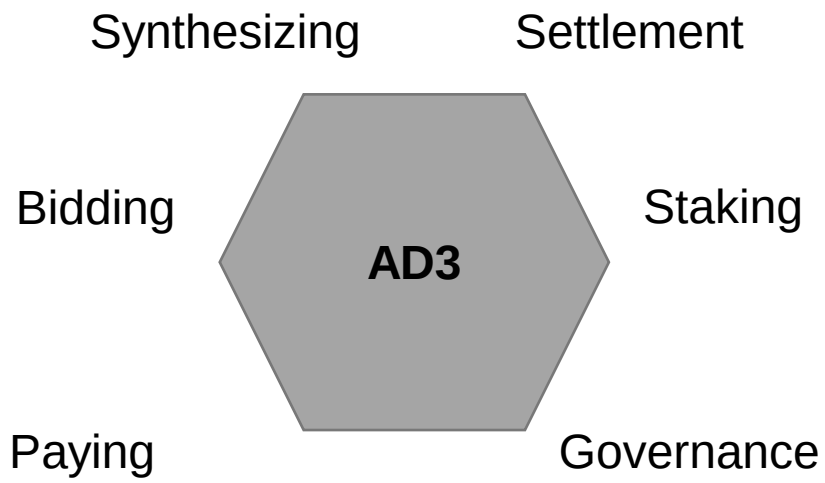
Parami Protocol supports NFT as ticket, badge or collector for advertising campaign.

Yield Farming support

Parami supports liquidity mining (Yield Farming) so that users are able to exchange rewarded token to stable coins and advertisers can easily build an advertising fund.

...

Token Economic Model

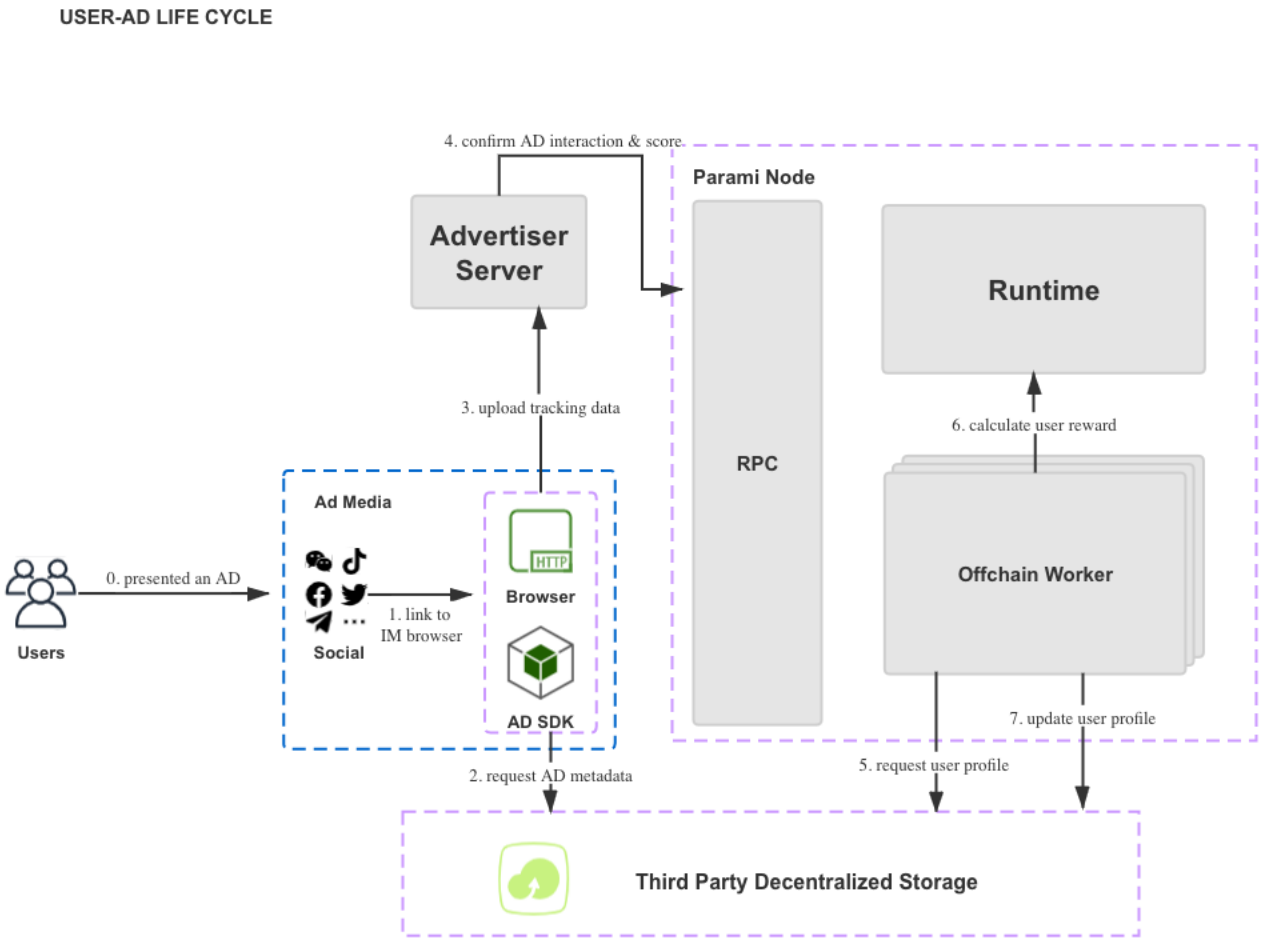


AD3 usage scenarios

The native token on Parami Protocol is **AD3**. It is an UTILITY TOKEN that can be used in 5 scenarios:

- Settlement: The price of the Ad and the price of the token will jointly determine the number of rewards the user will receive for a single advertising campaign.
- Bidding: Use tokens to bid for advertising opportunities.
- Synthesizing: Use AD3 to generate social coins and NFT.
- Paying: AD3 will be used to pay operation fee.
- Governance: Vote and adjust the chain parameter.
- Staking: Stake tokens for mining and community development.

Use Case



0. Users are shown an Ad, which is published by other user's community through IM apps.

1. The advertiser gets user's DID according to platform ID hash.

2. The SDK requests AD content from Decentralized Storage.

3. The SDK tracks user Ad action data.

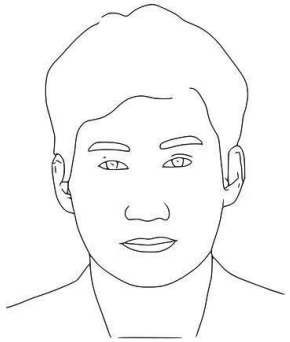
4. The advertiser tags and scores the DID with encrypted data after evaluating user's action.

5. OCW requests PCAP from Decentralized Storage.

6. Ad Runtime calculates the reward of user.

7. OCW updates PCAP

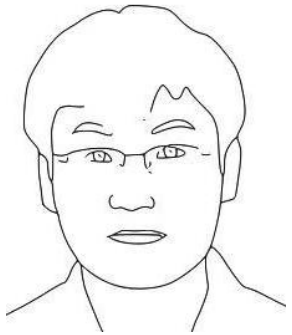
Team



Dorian

Core Architect

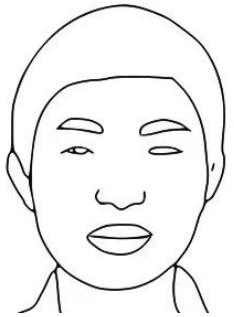
Dorian was the senior architect of DCEP (Digital Currency Electronic Payment), the core architect & technical leader of TRON and has rich practical experience in consensus mechanism, privacy calculation, cross-chain mechanism, etc. He is an early evangelist and investor of BTC.



Mono Wang

Core Dev

Full-stack engineer; senior rust engineer with 6 years‘ experience; Core Rust Chinese community evangelist; Open Tron independent developer; former Core dev of Ledger.



Edison

Core Dev

Edison was the core architect of TRON‘s TRONZ team, and is the core developer of the zero-knowledge proof virtual machine. He has deep research in the fields of zero-knowledge proof, MPC, and homomorphic encryption, and is committed to solving Web 3.0 data privacy problems.

Roadmap

2021 Q1

TestNet: Dāna

- PoC and code security audit
- WeChat wallet
- Web SDK

2021 Q2

MainNet V1: śīla

- NPOS mining
- AD platform
- Mobile wallet

2021 Q3

MainNet V2: Vīrya

- Governance
- Decentralized oracles
- NFT support

2021 Q4

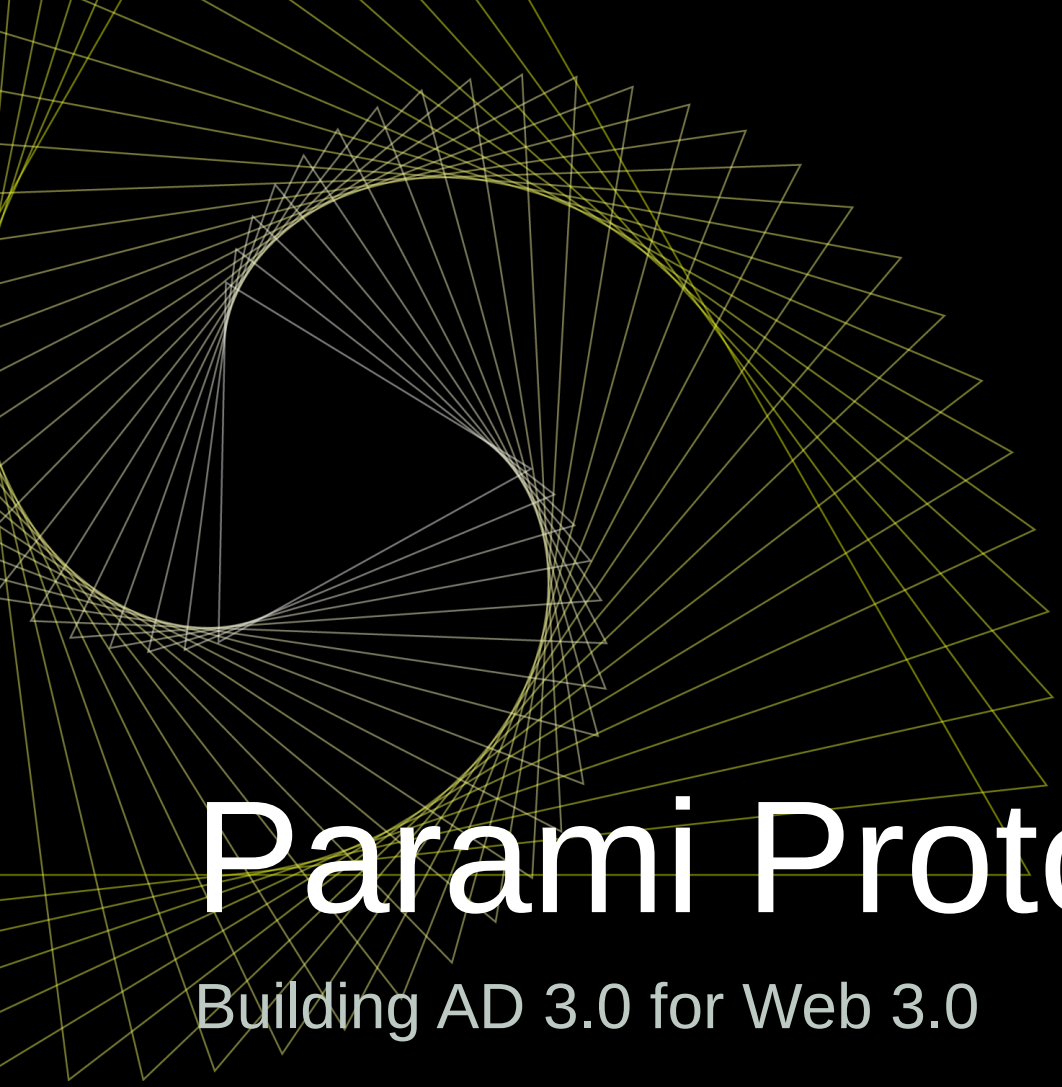
MainNet V3: dhyāna

- Privacy Computing(ZKP)
- Monetization
- On-chain analyzer

2022 Q1

MainNet V4: Prajñā

- Parachain to plug in
- Cross chain AD



Parami Protocol

Building AD 3.0 for Web 3.0

parami.io

info@parami.io

Github

Twitter

Medium