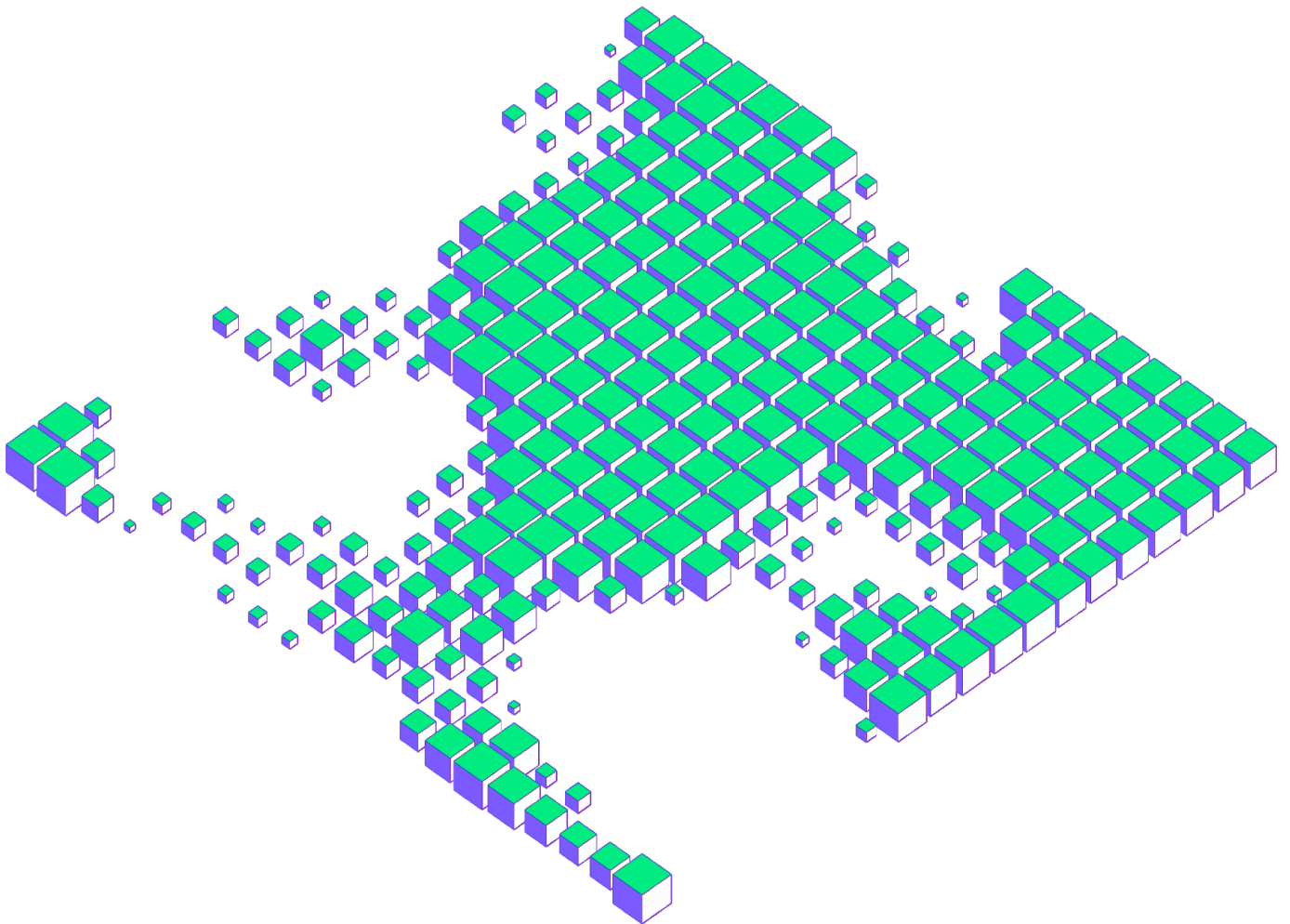# Litentry Light Paper v2

A Cross-chain Identity Aggregator

Litentry Foundation Ltd.

January 2021, Dali, China

Introduction

Concept of Identity Aggregation

Challenge

DID aggregation is the process of integrating a wide range of digital identities from multiple networks. Our definition of decentralized identity is conforming to the W3C standard, which specifies that "a decentralized identity is a globally unique persistent identifier that does not require a centralized registration authority because it is generated and/or registered cryptographically." Because different decentralized systems have different DID standards, it's critical to well integrate these standards when linking digital identities.

The demand for integrated identities data is expected to largely come from decentralized applications that are fueled by personal identity data. Besides interoperability, the identifier plays a critical role in scenarios where the server requests the client for identity data, such as KYC, credit scores, or credentials, in an attempt to provide services.

In the past and present, many applications require users to provide their information from third-party applications or directly track user activities to obtain the information they need. This inevitably compromises users due to privacy invasion and personal data breach.
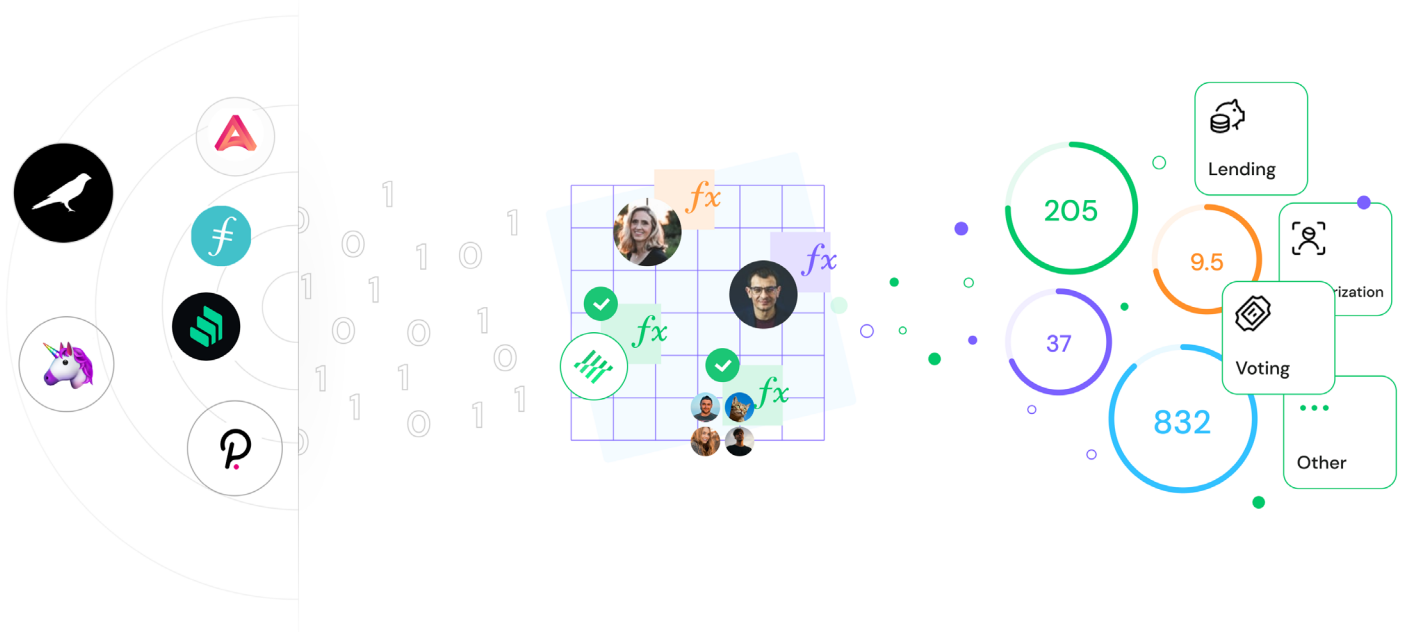
Litentry Light Paper

With decentralized identifiers (DID) and privacy-preserving storage, we have successfully protected data sovereignty in a decentralized system. However, identity data are scarce and scattered, making the corresponding application scenarios too narrow. It's a huge challenge in a decentralized system where we attempt to introduce broader scenarios, such as credit lending in DeFi, personal reputation in on-chain governance, and decentralized customized recommendation algorithms in social media.

Currently, we don't have an adequate amount of data to support such broad scenarios. As for collecting data from other networks, reading these data involves complex work of DID verification and code parsing, which is beyond inconvenience especially if there are multiple data sources.

Litentry's Role

As people have already generated massive amounts of data in various decentralized systems, a way must be found to connect these data so that they can flow across different systems and platforms, while user privacy and data sovereignty are preserved. This approach can truly reflect the core value of Web3. Meantime, the advent of blockchain provides an effective underlying data registry infrastructure that enables data to be indexed and retrieved, as well as bolstering the growth and adoption of DID.

Litentry is helping solve this problem with an identity aggregation protocol that serves for multiple networks. Litentry Network enables DID aggregation, verification, and credit calculation/grading. It mitigates the difficulty of resolving agnostic DID mechanisms by integrating all DID standards into a modularized identity model. These services can be widely implemented in DeFi, on-chain governance, and decentralized KYC. The processes of data aggregation and verification are transparent, secure, and privacy-preserving.

Highlights

1. Blockchain Powered

Litentry is built on Substrate, which inherits great features and the best technologies in the Blockchain industry. Litentry aims to be the Parachain of Polkadot Network and benefit from the thriving cross-chain ecosystem and shared security.

2. Privacy Focused

Privacy preservation is the fundamental of Litentry network and we do not want to breach the pseudo-anonymity of blockchain networks. Litentry supports an incognito on-chain data processing.

3. Decentralized

Litentry Network processes DID verification, aggregation, and computation requests from a service demander and returns a trustable result. The process will be implemented by a random set of validators in the network in a fully decentralized and transparent way.

4. Democracy

The credit computation algorithms, the data origins, and the identity registrars are all governed by the LIT stakeholders, the relationship of community and community members could be recorded on chain and generated community credit, and further all the governance credit will contribute to voting power.

Concept of Decentralization

Decentralization of identity storage

DID-account relationships under encryption by large and stored on-chain. Other DID data are directly returned to the service demander in real-time, instead of being stored on network servers.

Decentralization of identity relationships

The relationship of data, and identity could be validated with cryptographic calculation, and it is also registered in the decentralized network instead of regular centralized services like Certificate Authority used in HTTPS protocol. Different identities belonging to the owner are not discoverable and protected by cryptography.
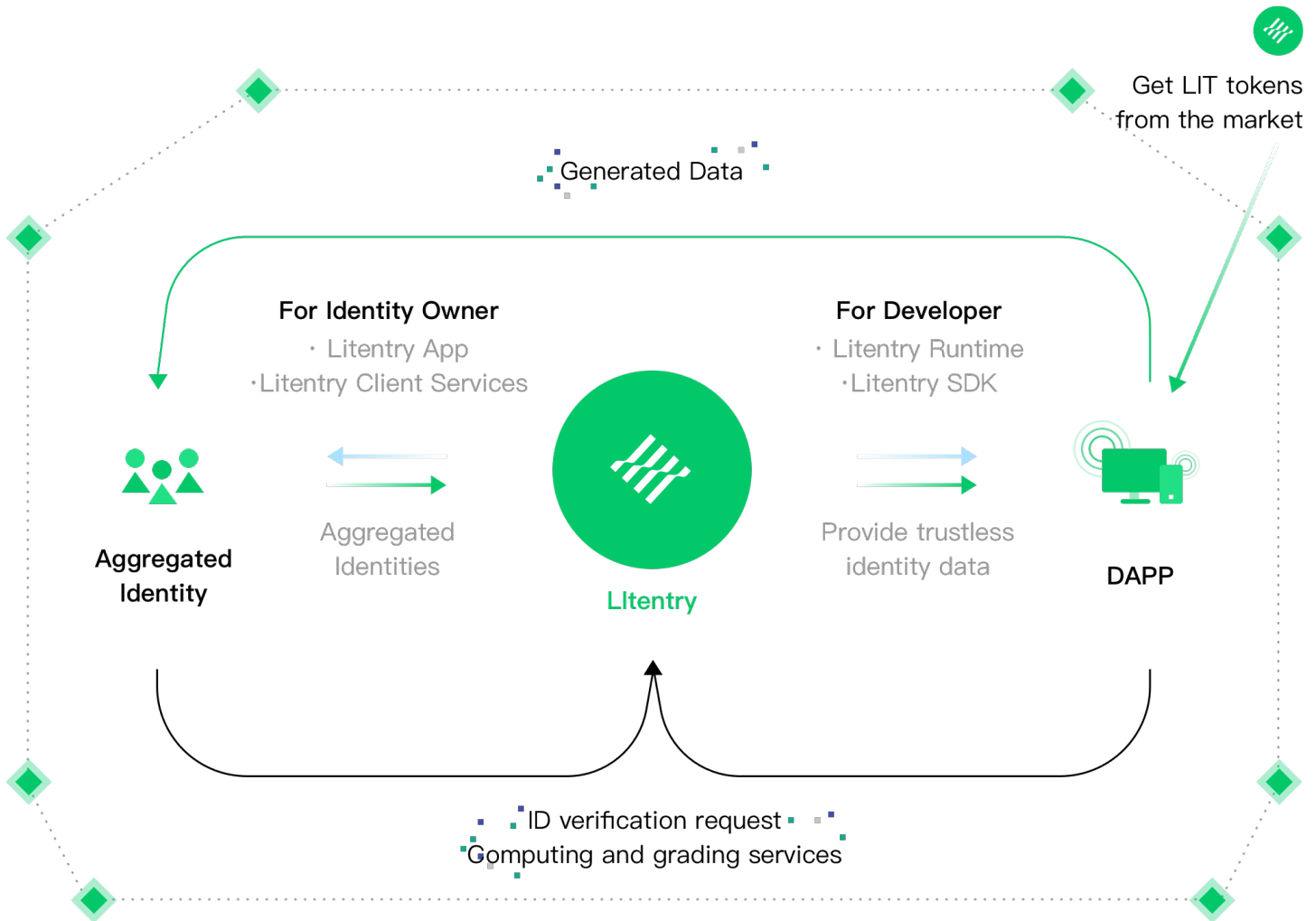
Decentralization of identity authentication

The identity validator directly connects to the decentralized network, and it could validate the authentication request independently.

Decentralization of credit computation

Once the credit computation request is sent to the Litentry network, the network will distribute the task to multiple nodes, fetching related data from multiple origins, the computation result will become valid once all the nodes have the same result.

Token Economics

Get LIT tokens from the market

Generated Data

For Identity Owner
· Litentry App
·Litentry Client Services

For Developer
· Litentry Runtime
·Litentry SDK

Aggregated Identity

Aggregated Identities

LItentry

Provide trustless identity data

DAPP

ID verification request
Computing and grading services

Litentry network native token LIT mainly has the following four usages.

Litentry Light Paper

Fee for credit/reputation computation

As Litentry network provides a trustless identity credit/reputation as a service, each time a user sends a real-time credit computation request to the network, the nodes of the network will consume its network through-put to fetch data from different sources, and use computing power to calculate the credit. For this reason the LIT token needs to be paid to the network to compensate for the efforts validator pays.

Reward for indexed identity databases

Litentry also encourages third parties to set up indexed identity data-bases from different networks, which could provide nodes with quick and reliable decentralized identity data. LIT token will also be used as a reward for them.

Staking for being an identity Registrar

For setting up an identity registrar, some LIT token is required as stake, identity registrar could provide decentralized judgements for users. Once a user gets enough judgements, he will be tagged with certain informa-tion, like "long-term liquidity provider", "frequent DOT trader", etc.

Deposits in DeFi

For analyzed DeFi lending services with identity integrated, Litentry will provide LIT token as one of the deposit currency, and also the deposit will be decreased if use has a high credit score, and Litentry Foundation will vouch for users who have credit. In the future users could also set up small DAOs to vouch for its members.

Products

For Developers

The ecosystem needs the DApp as identity contributors, we are building essential tools for developers to easily create DApp connect to Litentry.

Litentry Network / Runtime

The core of Litentry, built with Substrate, it inherits great features and the best technologies in the blockchain industry. We aim to be the Parachain of Polkadot Network and benefit from the thriving cross-chain ecosystem and shared security. Runtime's off-chain worker protects the privacy of data generation and distribution processes.

Litentry SDK

Currently support Javascript, with the integration of Polkadot api, offer scaffold and tools for developers to build client-side applications running on Web, mobile, and IoT devices. More programming languages and decentralized data storages interfaces are in the plan.

Litentry Light Client Services

Decentralized background mobile application. It enables mobile applications for Litentry to be completely independent of any third-party server. Mobile applications will connect directly to the Litentry blockchain network and decentralized storage rather than a single node. It also enables notification from blockchain rather than Apple or Google's message center.

For Users

On the user side, we have Litentry Authenticator as the user's mobile data hub. Data Explorer for users to check their own data, and DApp Playground to demo the potentials of the user-centric web.

Litentry App

Litentry app is a mobile tool integrated with identity on Litentry Network. Users could interact with multiple services like recalculate voting power in on-chain governance or get analyzed DeFi services based on credit. It could facilitate the governance process, integrate participants' more information from linked accounts on other networks, and encourage more users to join on-chain governance with LITs as incentives.
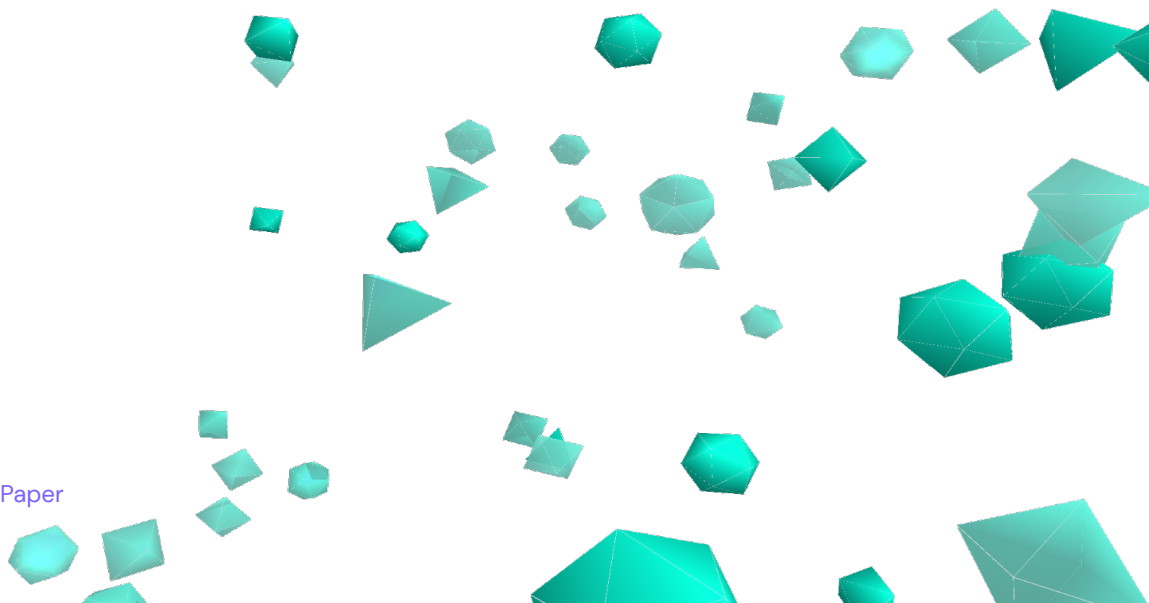
Litentry Authenticator

Litentry Authenticator is a mobile identity and data hub for a decentralized web. It features 2FA and versatile app/service interfacing, crypto wallet, aliases identity generation, private data aggregation, and NFT data authorization. In the future it will also integrate identity staking and identity matching services.
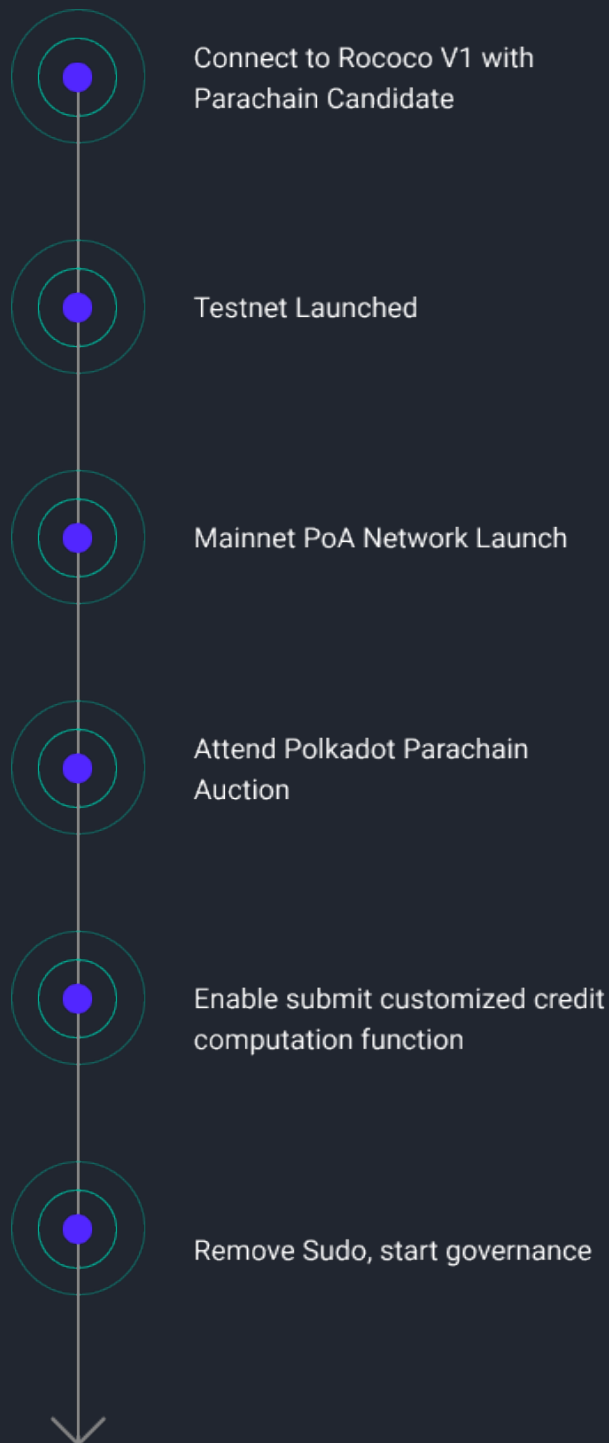
DApp Playground

Collections of DApp samples built on Litentry. It demonstrates how the decentralized 2FA works, and how the DApp works on Litentry, currently there is a decentralized music app and a decentralized tweeting app for users to play.

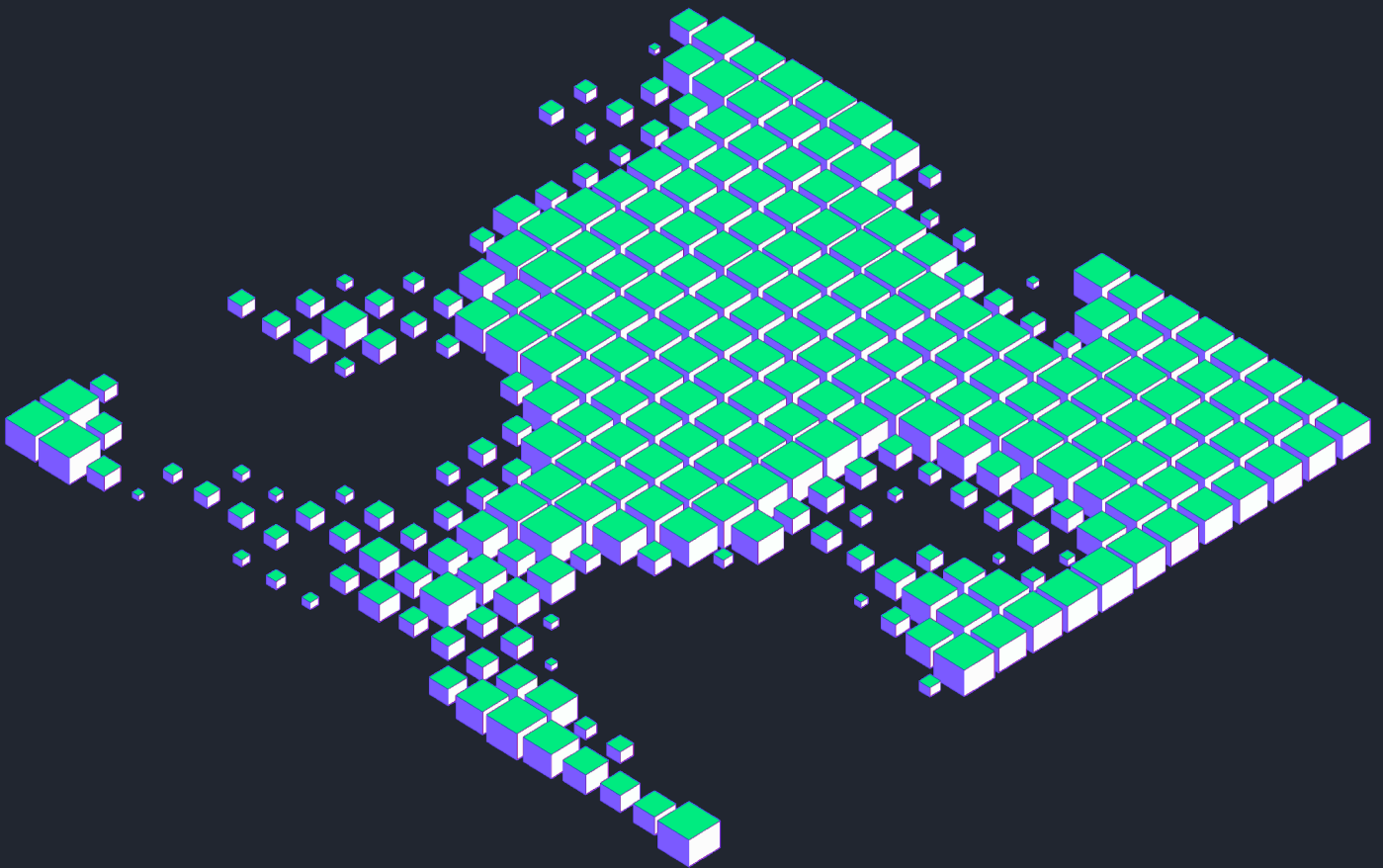Try the Playground now, no registration, no password, no App migration barriers.

Litentry Light Paper

Road Map

Runtime Upgrade

Connect to Rococo V1 with
Parachain Candidate

Testnet Launched

Mainnet PoA Network Launch

Attend Polkadot Parachain
Auction

Enable submit customized credit
computation function

Remove Sudo, start governance

Road Map

Mobile Engineering

Integrate Litentry Identity Registrar

Cross wallet communication

Native Litentry Runtime Support

Launch Light Client Services

Integrate DApp market

Identity Messaging Support

A Cross–chain Identity Aggregator