Проект представляет собой децентрализованную платформу для проведения анонимных голосований с использованием технологии блокчейна.

Проект является вариантом реализации предложенного в [1] протокола LightChain, значительно оптимизированного по временным затратам и затратам памяти по сравнению со стандартными реализациями блокчейна. Обмен данными между пирами сети на сетевом уровне реализован с помощью модернизированного протокола DHT. Адресация узлов задаётся с помощью графа с пропусками - структуры данных, состоящей из системы организованных по уровням двунаправленных списков, в которой у каждого узла на каждом уровне имеется до двух соседей, а на нулевом уровне находится полный список узлов [2]. Каждый узел графа с пропусками является либо пиром, либо транзакцией, либо блоком, и, кроме IP-адреса, имеет два (вообще говоря) различных идентификатора, называемых NumID и NameID. Оба идентификатора пира являются хешем его открытого ключа, но для транзакций и блоков они отличаются. У транзакций и блоков NameID является хешем последнего подтверждённого перед ними блока, а NumID - хешем данных, записанных в транзакцию или блок. Для графов с пропусками известны алгоритмы поиска по обоим идентификаторам ([2], [3]), а также алгоритмы вставки и удаления узлов, имеющие логарифмическую сложность, что значительно ускоряет выполнение связанных с блокчейном операций.

Кроме того, использование DHT для обмена информацией позволяет каждому узлу для проверки корректности операций хранить данные не о всех узлах сети, а только о множестве своих соседей на каждом уровне графа, что обеспечивает значительный выигрыш по памяти.

В качестве алгоритма консенсуса в данном протоколе используется предложенный в [1] алгоритм Proof-of-Validation. Этот алгоритм обладает свойством честности в том смысле что каждый участник обладает равным шансом участия в консенсусе, независимо от имеющейся у него вычислительной мощности или доли владения. При создании транзакции или блока каждый участник сети с помощью хеширования их данных вычисляет адреса так называемых валидаторов - пиров, к которым он должен обратиться для проверки. Чтобы быть подтверждённой, транзакция или блок должны быть подписана определённым числом валидаторов, которые затем, наряду с создателем, сохраняют эту транзакцию или блок у себя в памяти. Таким образом, каждый блок и транзакция хранятся в сети DHT в нескольких копиях, что позволяет обеспечить экономию памяти для каждого пира, а также распределение нагрузки по узлам сети. После валидации транзакции или блока они встраиваются их создателем в граф с пропусками, при этом в качестве IP-адреса транзакции или блока указываются IP их создателя и валидаторов. Таким образом, все запросы алгоритмов операций на графе с пропусками (например, цепочки поисковых запросов), отправляемые узлу-транзакции, будут обрабатываться её создателем, или одним из её валидаторов. Размещение транзакций и блоков в качестве узлов сети позволяет пирам искать их с помощью тех же алгоритмов, что и других пиров.

Найдя в сети новые валидированные транзакции, каждый пир имеет право собрать эти транзакции в блок, проверить его с помощью валидаторов, и вставить этот блок в граф с пропусками в качестве узла. После того как транзакция была включена в блок, её создатель выполняет алгоритм её удаления из графа.

[1] Y. Hassanzadeh-Nazarabadi, A. Kupcu, O. Ozkasap, "LightChain: A DHT-based Blockchain for Resource Constrained Environments", arXiv:1904.00375v1

[2] J. Aspnes, G. Shah, “Skip graphs,” ACM TALG, 2007

[3] Y. Hassanzadeh-Nazarabadi, O. Ozkasap, “Laras: Locality aware replication algorithm for the skip graph,” IEEE NOMS, 2016