Пояснительная записка к задаче для практикантов Arrival.

Общие сведения.

Фундаментальным понятием распределенных систем вообще и систем распределенных журналов в частности является консенсус, то есть согласие всех узлов о состоянии распределенной системы на момент времени. Консенсус является частным случаем более широкого понятия консистентности данных, которая не обязательно подразумевает распределенную систему. Достижение консенсуса является дорогостоящей и сложной операцией. Эта сложность существенно снижает эффективность распределенных систем, особенно для случая, когда невозможно гарантировать “добрую волю” всех узлов сети, например, в публичных блокчейн-сетях. В связи с этим предметом исследования являются способы упростить процедуры достижения консенсуса.

Одним из направлений повышения эффективности является идея сократить до минимума объем данных, содержащихся непосредственно в распределенной системе (в блоках блокчейна), а также обеспечивать консенсус не для каждой операции, а только в “реперных” точках.

Для практической реализации этой идеи необходимо формализовать понятие “реперных точек” в блокчейн-сети. На текущий момент наиболее известными формализациями, позволяющими заменить данные и цепочку операций над ними в распределенной системе короткой подписью (доказательством), являются ZK-SNARK и ZK-STARK. Обе эти формализации могут использоваться в рамках более широкой группы подходов для повышения эффективности блокчейн-сетей (в Ethereum эта группа часто называется Layer 2 протоколы), многие из которых предполагают хранение оригинальных данных вне блоков блокчейн-сети.

Сама идея хранения оригинальных данных вне блокчейн-сети может быть отделена от непосредственной имплементации и процедур вычисления коротких подписей/доказательств, обеспечивающих необходимые свойства консенсуса. Одним из проектов, пытающихся определить и отделить процедуру (протокол) хранения данных вне блокчейн-сети от непосредственной имплементации является Baseline. С точки зрения блокчейн-сети, ядром, обеспечивающим корректность и защищенность всей процедуры, являются исполняемые в контуре блокчейн-сети процедуры (смарт-контракты) Shield и Verifier, которые позволяют всем узлам проверить легитимность записанной в блок информации об изменении состояния системы без повторения всех вычислений над этим состоянием и даже без использования части данных, хранящейся вне блокчейн-сети.

На текущий момент в рамках проекта Baseline имеется несколько примеров имплементаций этих смарт-контрактов в упрощенном виде на основе формализации ZK-SNARK.

Цели и задачи практической работы.

В рамках практической работы от практикантов ожидается создание работающей имплементации этих смарт-контрактов на основе формализации ZK-STARK. Для генерации “доказательств” возможно использование существующей библиотеки libSTARK. Первым этапом может быть имплементация протокола для наиболее простого частного случая, например, перемещения токенов со счета A на счет B с учетом неотрицательности балансов и сохранения общего количества токенов.

Конкретный частный случай, язык имплементации и распределенная система (блокчейн-сеть) может быть выбрана по желанию практиканта. Но надо иметь в виду, что проект Baseline в своем текущем состоянии предполагает в качестве языка и базовой блокчейн-сети использовать Ethereum и Solidity, в связи с чем адаптация этого протокола для других блокчейн-сетей и языков хотя и возможна, но, вероятно, займет больше времени.

Полезные ссылки

1. Спецификация протокола, описание интерфейсов: https://www.baseline-protocol.org/
2. Описание принципов работы и свойств ZK-STARK: https://eprint.iacr.org/2018/046.pdf
3. Имплементация ZK-STARK на C++: https://github.com/elibensasson/libSTARK
4. Примеры имплементации Baseline на TS/Solidity: https://github.com/ethereum-oasis/baseline