Основы IOTA.

noise@sumus.team, engi@sumus.team

1 июля 2019 г.

1 Технология

Технология IOTA в отличие от блокчейна базируется на направленном ациклическом графе (DAG), который авторы IOTA называют “клубок”. Транзакции, выпущенные нодами образуют множество вершин графа, который является хранилищем транзакций. Набор рёбер графа получается следующим образом: когда появляется новая транзакция, она должна подтвердить две предыдущие транзакции. Эти подтверждения представляются “прямыми” рёбрами. Если между двумя транзакциями нет “прямого” ребра (то есть без промежуточных вершин), но эти две вершины соединены минимальным путём из двух рёбер, то говорят, что одна транзакция (новая) подтверждает другую транзакцию (старую). Это простейший случай. Можно предложить вариант, когда новая транзакция подтверждает $k \geq 2$ старых транзакций. Транзакция “genesis” подтверждается прямо или косвенно (непрямо) всеми другими транзакциями (здесь, видимо, не имеется в виду путь максимум из двух рёбер). Транзакция “genesis” в начале графа есть адрес (кошелёк), содержащий все токены. “Genesis” рассылает эти токены по некоторым другим адресам (кошелькам), которые являются учредителями. Все токены порождаются в нулевой момент времени и и больше в будущем не выпускаются, чтобы майнеры не получали вознаграждения “из воздуха”.

Вершины графа – это транзакции. Сеть состоит из нод (узлов) которые являются юридическими лицами, выпускающими и проверяющими транзакции. Главная идея “клубка” состоит в следующем: пользователи (ноды) должны работать, чтобы подтверждать другие транзакции. Следовательно, пользователи, выпускающие транзакции вносят вклад в безопасность сети. Предполагается, что узлы проверяют, не конфликтуют ли подтверждённые транзакции. Если узел определяет, что транзакция конфликтует с историей графа, то узел (нода) не подтвердит эту транзакцию ни прямы ни косвенным путём.

Если нода выпускает новую транзакцию, которая подтверждает конфликтные транзакции, то она рискует, что в свою очередь, другие ноды не подтвердят эту её новую транзакцию, которая будет предана забвению. Как только транзакция получает дополнительные подтверждения, она принимается системой с высочайшим уровнем доверия. Другими словами, трудно заставить систему принять транзакцию с, например, двойной тратой. Важно подчеркнуть, что мы не навязываем какие бы то ни было правила подтверждения нодой транзакций. Наоборот, мы утверждаем, что если большое число нод придерживается некоторого “эталонного” правила, то для любой ноды лучше придерживаться того же правила. Это выглядит обоснованным предположением, особенно с учётом того, что в IOT ноды – это специальные чипы с предустановленной прошивкой (видимо для $M \Leftrightarrow M$).

Чтобы выпустить транзакцию, нода делает следующее:

. . . . . .

- Нода выбирает две другие транзакции для подтверждения в соответствии с алгоритмом. Вообще говоря, эти две транзакции могут совпадать.
- Нода выявляет, конфликтуют ли эти две транзакции ине подтверждает их, если они конфликтуют.
- Нода, выпускающая валидную (выпущенную в соответствии с протоколом и не конфликтующую) транзакцию, должна решить криптографическую задачу (пазл) подобную той, которая решается в блокчейне Биткойн. Это осуществляется путём нахождения такого числа, что хеш от него, записанный в блочную ??? (конкатенацию) вместе с некоторыми данными о подтверждённой транзакции, имеет конкретную (уникальную) форму. В случае протокола Биткойн, хеш должен иметь по крайней мере заданное количество (*двоичных*) нулей в *старших битах* хеша.

Важно, что сеть IOTA асинхронна. Вообще говоря, ноды необязательно “видят” один и тот же набор транзакций. Ноды не обязаны достигать консенсуса о том, какая валидная транзакция имеет право быть включённой в каталог (в граф), подразумевая, что все они могут быть в клубке (графе). Тем не менее, в случае,

если эти валидные транзакции являются конфликтными, ноды должны решить, какие из этих транзакций станут "осиротевшими". Под "осиротевшими" понимаются транзакции, которые никогда не подтверждаются непрямым образом. Основное правило которому следуют ноды при выборе между двумя конфликтующими транзакциями таково: нода запускает алгоритм выбора транзакций, являющихся вершинами графа, много раз и смотрит, какая из двух транзакций подходит для непрямого подтверждения. Например, если транзакция (одна из двух) была выбрана 97 раз при 100 запусках алгоритма, то говорят, что она подтверждена с уверенностью 97%.

Что мотивирует ноды выпускать транзакции? Каждая нода ведёт некоторую статистику, например, количества транзакций, полученных от соседних нод. Если одна конкретная нода "слишком ленива", она будет "отброшена" (будет исключена из процесса) её соседями. Поэтому, даже если нода не выпускает транзакции и, как следствие, не имеет прямого стимула делиться (???) транзакциями, подтвердившими её собственную транзакцию, она всё ещё имеет стимул для участия в системе (в процессе).

Идея использовать DAG выдвигалась и ранее. В частности в [***] предлагается модифицировать протокол Биткойна так, чтобы сделать главный каталог (хранилище) не в виде блокчейна, а в виде дерева. Было показано, что эта модификация снижает время подтверждения и улучшает (повышает) безопасность сети. В [***] предложен DAG. Эта модель отличается от модели IOTA следующим: вершинами их DAG являются блоки, а не отдельные транзакции; майнеры в их сети соревнуются за fee и новые токены могут выпускаться блок-майнерами.

2 Веса

Вес транзакции – это величина, пропорциональная объёму работы, вложенному в неё нодой. В текущей версии IOTA вес может принимать величины 3^n, где n – натуральное число, принадлежащее непустому ограниченному интервалу (множеству) (короче – конечному непустому множеству). В конечном счёте, неважно, как вес был получен на практике. Важно только то, что каждой транзакции сопоставлено натуральное число (её вес). Вообще говоря, транзакция с бóльшим весом важнее транзакции с мéньшим весом. Во избежание атак, предполагается, что ни одно юридическое лицо (кошелёк, нода) не может за малое время выпустить много транзакций с достаточно большими весами.

Кумулятивный вес транзакции – это её собственный вес плюс суммарный собственный вес всех транзакций, прямо или косвенно подтвердивших эту.

На рис. 1 в правом нижнем углу каждого прямоугольника, соответствующего транзакции, указан собственный вес транзакции. В верхнем левом углу — кумулятивный вес транзакции. Например, транзакция F прямо или косвенно подтверждена транзакциями A, B, C, E с собственными весами 1, 3, 1, 1 соответственно. Тогда кумулятивный вес F есть $6 + 3$, где 3 собственный вес транзакции.

Пусть "tips" — неподтверждённые транзакции в графе. на рис. 1 неподтверждёнными *ни разу) являются транзакции A и C. Когда появляется новая транзакция X и подтверждает A и C, то она, в свою очередь, становится неподтверждённой транзакцией. Кумулятивный вес каждой из транзакций A и C при этом возрастает на 3 (собственный вес X).

Мы должны ввести две дополнительные переменные для обсуждения алгоритмов подтверждения транзакции.

Первое, для набора (и для каждой в отдельности) транзакций графа (клубка) мы вводим величину *height* (*высота*): максимальная длина ориентированного пути к *genesis* ("справа налево" — положительное направление ориентированного графа).

depth (*глубина*): максимальная длина пути от произвольно взятой вершины (транзакции) до правого края графа ("обратноориентированный" путь от этой транзакции до самой "свежей").

Например на рис. 2 вершина G имеет *высоту* 1 и *глубину* 4 : $G \leftarrow F \leftarrow D \leftarrow B \leftarrow A$.

Замечание

а) Если идёт подсчёт пути в положительном направлении, то ни одно из рёбер не может быть пройдено "против" стрелки, аналогично в обратном направлении все рёбра должны быть пройдены "против" стрелки.

б) "Свежая" транзакция может быть не единственной .

Для определённости, цена (оценка) транзакции — это сумма собственных весов всех транзакций, подтверждённых этой транзакцией, плюс её собственный вес.

Например, на рис. 2 транзакция A подтверждает (прямо или косвенно) транзакции B, D, F, G, поэтому её цена есть $1 + 3 + 1 + 3 + 1 = 9$. Для C цена $= 7$.

Для упрощения принимается, что собственный вес $\forall$ транзакции равен 1, тогда кумулятивный вес $\forall$ транзакции есть $1 +$ количество всех подтверждающих её транзакций, а цена этой транзакции есть $1 +$ количество подтверждающих её транзакций.

Кумулятивный вес является безусловно важнейшей метрикой, но *высота*, *глубина* и *цена* будут также обсуждаться.