**Proof of Union: алгоритм консенсуса в**

**блокчейн системах базируемый на сотрудничестве узлов**

Коваленко Геннадий Александрович

**1. Введение**

В настоящее время существует огромное количество консенсус алгоритмов для блокчейн систем, каждый из которых имеет свои преимущества и недостатки пресущие только ему, либо целому классу сходных алгоритмов. Так или иначе, в настоящее время лидирует три концепции консенсуса - основанные на майнинге (PoW) [1] и форжинге (PoS) [?], которые в свою очередь представляют конкурентную и последовательную модели генерации блоков непосредственно. Такое разделение либо предполагает крайне большое расходование материальных ресурсов, либо представляет собой необходимость комбинации с другими методами консенсуса [?], что приводит к сложности реализации и доказуемости безопасности конечного решения [?]. Альтернативной моделью конкуренции и последовательности может являться алгоритм объединения узлов (PoU), решающих общую задачу сообща, главным преимуществом которой является простота, сроднимая PoW и быстрота генерации блоков, эквивалентная PoS.

**2. Становление**

Зарождение PoU алгоритма представляет собой закономерное развитие консенсус алгоритмов, представленных в качестве синтеза уже ранее созданных и применяемых методов. Обобщая, можно представить эаолюцию блокчейн систем в следующих этапах становления.

1. Конкуренция. Представляет собой генезис блокчейн систем, тезис и начало развития непосредственно. В такой модели каждый узел выполняет однотипные и сложно-математические операции полностью децентрализованно, несвязанно между собой, что порождает выполнение одинаковых действий многократно, в большей степени без всякой полезной нагрузки. Отрицательным качеством безусловно является необходимость поддерживать конкуренцию, быть соперником относительно всей другой сети, удерживать свои мощности, что в конечном счёте приводит во-первых, к необходимости постоянного потребления майнинг-аппаратуры (процессоры, видеокарты, интегральные схемы и т.д.), во-вторых, к логичному завышению цен на подобную аппаратуру, методом искуственного дефицита средств производящими монополиями, в-третьих, к неостановимому поглощению электроэнергии и скорейшему разрушению потреблённой аппаратуры. Положительным качеством же является простота описания алгоритма и независимость от сети, что и приводит к доступности анализа конечной безопасности.

2. Последовательность. Развивается как отрицание, антитетиз конкуренции, избавляясь от самых негативных её черт. В такой модели узлы выполняют валидацию блоков поочерёдно, один за другим по общему алгоритму выбора валидатора. Сложность реализации последовательной концепции начинается на уровне сетевого консенсуса [?], когда строится сильная необходимость и даже зависимость валидации текущего и главного proposer валидатора всеми другими узлами сети, что приводит к возможности сущестовования постоянных разветвлений (форков) [?]. Для такого случая существуют дополняющие алгоритмы, способные обеспечить сетевой консенсус между узлами, подобно ядру Tendermint [?], базируемом на задаче византийских генералов [?]. Безусловным положительным качеством такой модели является отсутствие в необходимости конкурировать, что приводит к достаточно простой аппаратной составляющей, не приводящей к трате большого количества электроэнергии и быстрому устореванию используемой техники.

3. Объединение. Развивается как синтез конкуренции и последовательности, вбирая в себя простоту, монолитность и скорость, энергоэффективность. В такой модели не существует более валидаторов как отдельных и индивидуальных участников сети, теперь более блок не подписывается кем-то конкретным и определённым. Единственным и монопольным валидатором в конечном счёте становится сама сеть валидаторов, потому и не имеет значения кто станет proposer’ом блока, что приводит к финальному отрицанию последовательности как таковой. Также вторым отличием от двух предыдущих классов консенсусов является концепция слияния разных взглядов и видений на генерацию блока, вместо выбора единственно верного из предложенного множества, что приводит к единому и простому поиску решения методом объединения информации.

**3. Определение**

Главным отличием PoU консенсуса является зацикленность системы на сохранение транзакций больше, чем самой связи между блоками, что является противоречивым для самих блокчейн структур в целом. Суть заключается в том, что существует у таких алгоритмов N-ое количество блоков, подобно транзакциям, находящимся в статусе ожидания, pending’e, и в это же время существуют блоки, генерируемые после них, наперёд. Таким образом, можно сказать, что помимо транзакций, существуют также блоки, находящиеся в своеобразном mempool пространстве.

Будучи блоками неподтверждёнными, они не согласованы с сетью полностью. В таком периоде они перезаписываются и видоизменяются, находятся в этапе полиморфизма своих внутренностей. Блоки же подтверждённые находятся ранее всех неподтверждённых, они устоявшиеся и представляют уже статичность внутренностей, неизменность заложенных транзакций.

Так или иначе, доказательство объединения состоит из трёх основных функций.

1. Принятие (accept). При вызове данной функции происходит образование нового блока на базе взятых транзакций с mempool’a. При таком действии не происходит какого бы то ни было согласования с сетью, а следовательно само подтверждение является неполным, не приводящим к окончательному решению консенсуса. После данного этапа начинается временная задержка перед последующим вызовом функции accept, необходимая для согласования с сетью уже на основе второй функции merge.

2. Слияние (merge). При вызове данной функции происходит изменение ранее созданного блока с блоком принятым из вне. В такой функции особенно важен сам механизм соединения двух разных блоков в один целостный, чтобы сам отправитель мог прийти к точно такому же результатному блоку, как и получатель. Одним из решений может являться сортировка транзакций и помещение N-ого количества в блок. Все отброшенные транзакции после слияния попадают снова в mempool, ожидая следующего блока.

3. Фиксирование (commit). При вызове данной функции происходит конечное согласование блока с сетью методом подсчёта количества одинаковых блоков и выбора наиболее встречаемых из полученного множества. Предполагается, что большая часть валидаторов будет говорить истину, а потому и сохранение итогового блока исходит из количественной характеристики сети. Качественная характеристика может уже налагаться дополнительной бизнес-логикой к ядру блокчейн сети базируемом на PoU алгоритме.

Последняя фаза commit по большей части представляет необходимую меру решения функции merge, когда таковая в чистом виде может привести к fork’у сети, если сам новый merge-блок появится в момент нового вызова accept частью сети.

Ограничением данного способа консенсуса является необходимость согласовывать время между узлами в сети, чтобы генерировать блок функцией accept примерно в одно время. Стоит также сказать, что и сам описанный алгоритм может являться в теории не единственным представителем класса объединяющих методов консенсуса, а следовательно, данный анализ является лишь инициализацией и генезисом для последующих поисков.

**4. Экономическая часть**

В

**5. Заключение**

В

**Список литературы**

1. Накамото, С. Биткойн: система цифровой пиринговой наличности [Электронный ресурс]. — Режим доступа: <https://bitcoin.org/files/bitcoin-paper/bitcoin_ru.pdf> (дата обращения: 19.12.2020).
2. https://habr.com/ru/post/600113