УДК 004.031.43: 004.056 DOI: 10.26565/2519-2310-2019-1-03

ОБЗОР ПРОТОКОЛОВ КОНСЕНСУСА ПРИМЕНЯЕМЫХ В ТЕХНОЛОГИЯХ БЛОКЧЕЙН

Диана Ковальчук, Татьяна Ивко, Татьяна Кузнецова, Алексей Нарежний

Харьковский национальный университет имени В.Н. Каразина, пл. Свободы, 4, Харьков, 61022, Украина
dianakovalhyk@ukr.net, t.ivko@outlook.com, kuznetsova.tatiana17@gmail.com, o.nariezhnii@karazin.ua

Рецензент: Александр Потий, д.т.н., проф., Харьковский национальный университет имени В. Н. Каразина, пл. Свободы, 4, Харьков, 61022, Украина.
potav@ua.fm

Поступила: Март 2019

Аннотация. *Рассмотрены категории популярных проколов консенсуса: Proof of Work и его гибриды, Proof of Stake (включает LPoS, Proof of Importance) и гибриды, DAGs и его разновидности. В статье описаны их алгоритмы, характеристики, особенности, а также недостатки и преимущества. Уязвимости и атаки которым подвержены. Также приведен список использования каждого протокола в криптовалютах и других системах.*

Ключевые слова*: консенсус; блокчейн; протокол консенсуса блокчейн; децентрализованные системы; распределенный реестр.*

1 Введение

В 2009 году был сгенерирован первый блок и первые 50 биткойнов, а 1-я транзакция (перевод) произошла 12 января 2009 года. Появление биткоина положило начало технологии блокчейн [1]. В общем случае блокчейн – это цепочка блоков, каждый из которых обладает меткой времени, ссылкой на предыдущий блок и хранится на разных компьютерах.

Принцип работы блокчейна довольно прост. Его можно представить как некую «учетную книгу», которая есть у каждого участника события и которая постоянно обновляется. По сути, в эту книгу можно вписать любое событие – от финансовых операций с теми или иными криптовалютами и вплоть до результатов голосования на выборах или каких-либо идентификационных данных.

Интересная особенность блокчейна заключается в том, что страницы этой условной книги одновременно хранятся у всех пользователей сети, при этом постоянно обновляются и ссылаются на старые (предыдущие) страницы. И если кто-либо попытается скомпрометировать такую систему, несанкционированно удалив или изменив какую-либо запись, то система сразу же обратиться к десяткам тысяч других своих версий этой книги и обнаружит несоответствие в структуре блоков.

Консенсус является соглашением, которое удовлетворяет каждую из вовлеченных сторон. В контексте криптографии консенсус является процедурой принятия решения. Его цель – обеспечить всех участников сети возможностью согласования своего текущего состояния после добавления новой информации, блока данных или пакета транзакций. Иными словами, консенсус-протокол гарантирует, что сформированная цепь верна и подтверждает честность (легитимность) ее участников. Это важная структура для предотвращения ситуации, когда кто-то один контролирует всю систему, и она гарантирует то, что все участники соблюдают правила сети.

Протокол – это набор правил. Протоколы помогают:

- обеспечить стабильные условия для осуществления транзакций в сети;
- устранить возможность двойной траты;
- удостовериться, что все участники соблюдают предусмотренные правила.

Роль консенсусных алгоритмов заключается в обеспечении требуемого уровня надежности сети, построенной на серии узлов (*устройств, соединённых с другими устройствами, как часть компьютерной сети*). Консенсусные алгоритмы должны быть достаточно разви-

тыми, чтобы успешно предсказывать любые возможные сбои коммуникации внутри сети. Алгоритм автоматически спрогнозирует, что некоторые процессы и системы будут недоступны, и что в результате этого некоторые коммуникации будут потеряны. Чтобы противостоять этому, консенсусный алгоритм должен быть отказоустойчивым и работать для достижения заранее определенного консенсуса или одобрения, по крайней мере, от большинства узлов.

Блокчейн-системы, могут обладать только двумя из трёх возможных свойств: - децентрализация; - масштабируемость; - безопасность.

Каждый согласованный алгоритм имеет свой собственный сценарий применения, а выбор того, какой конкретно консенсус использовать для реализации блокчейна, зависит от типа сети и данных.

Чтобы транзакция была действительной в большинстве криптовалютных сетей, эта транзакция должна собрать определенное количество подтверждений (часто равных включению в блок цепочки блоков) из сети. Например, процесс получения 10 подтверждений означает просмотр конкретной транзакции в одном и 9 последовательных блоках.

2 Разновидности построения блокчейн реестра

2.1 Direct Acyclic Graph Tangle (DAG)

Это согласованный алгоритм DAG, используемый IOTA. Для того чтобы отправить транзакцию IOTA, необходимо проверить две предыдущие транзакции, которые вы получили. Консенсус «два к одному» с оплатой за продвижение усиливает достоверность транзакций, чем больше транзакций добавляется в направленный ациклический граф (tangle). Поскольку консенсус устанавливается транзакциями, теоретически, если кто-то может генерировать 1/3 транзакций, то он может убедить остальную часть сети, что их недействительные транзакции действительны. До тех пор, пока объем транзакции не станет достаточным, чтобы создание 1/3 тома стало невозможным, IOTA выполняет своего рода «двойную проверку» всех транзакций сети на централизованном узле - «Координаторе». Фактически, «Координатор» работает как стабилизатор (*предотвращает изменения параметров под действием дестабилизирующих факторов*) системы и будет удален, как только ациклический граф станет достаточно большим. В каждый момент времени существуют одна или несколько завершающих транзакций *(неподтвержденные транзакции - tips*), которые замыкают весь направленный граф существующих транзакций. При этом, разработчики утверждают, что при низких нагрузках на сеть количество замыкающих транзакций будет мало, а при высокой частоте появления новых транзакций число завершающих вершин будет возрастать [2].

Схематически структура реестра блокчейн на основе DAG представлена на рис. 1.

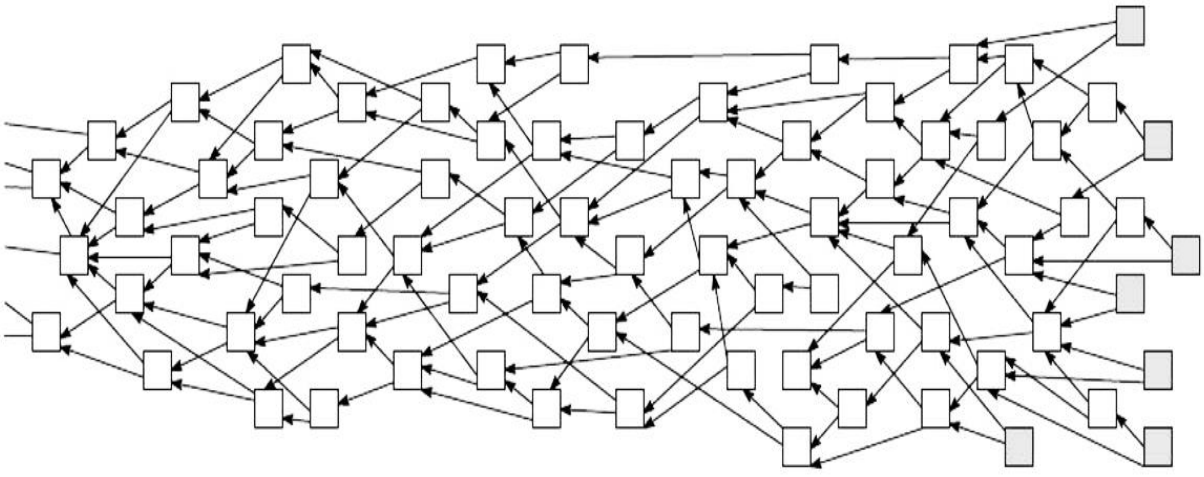


Рис. 1 – Структура реестра DAG

Используется в:
- IOTA [3].

Плюсы:
- низкие комиссии за транзакции;
- чрезвычайно малые транзакции;
- масштабируемость;
- облегченный.

Минусы:
- нет умных контрактов.
- уязвим (*требуется 34% от общей мощности хеширования*).

2.2 HashGraph

Принцип: узлы связываются случайным образом с использованием протокола «gossip about gossip» и соглашаются на консенсус после определенного раунда коммуникации.

Производительность: - очень высокая.

Среда DLT (Distributed ledger technology): - приватный блокчейн с разрешениями.

DLT - это технология хранения информации, ключевыми особенностями которой является: совместное использование и синхронизация цифровых данных согласно алгоритму консенсуса; географическое распределение равнозначных копий в разных точках по всему миру: отсутствие центрального администратора.

Завершенность: - зависит от раунда.

Ключевым отличием Hashgraph является протокол «*Gossip About Gossip*», в соответствии с которым узел получает набор транзакций с меткой времени, о которых «знает» другой узел. Для работы такого алгоритма все участники в сети должны быть известными. В результате синхронизации каждый узел хранит всю информацию и историю получения этой информации всеми узлами сети. Т.о., как только узел «видит» в своей истории, что данное сообщение уже было получено и проверено большинством, то нет сомнений, что оно действительно.

Используется в:
- Hedera Hashgraph [4].

Плюсы:
- быстрые транзакции (порядка 250 тыс. транзакций в сек).

Минусы:
- нет умных контрактов;
- не устойчив к атакам типа Sybil [5];
- не исследовано, как поведет себя в крупных масштабах использования.

2.3 Block-lattice - Directed Acyclic Graphs (DAGs)

Блочная решетка (*Block-lattice*) - это структура, в которой каждый пользователь (или адрес) получает свою собственную цепочку, в которую могут писать только они, но у каждого есть копия всех цепочек. Блочная решетка преобразует общий реестр (как в биткойн) в множество не используемых совместно асинхронных регистров, которые ускоряют время транзакций.

Блокчейн состоит из упорядоченных блоков (Рис. 2), которые содержат заголовки (*Header*) и транзакции (*Transaction*). Заголовок каждого блока, помимо других метаданных, содержит ссылку на своего предшественника в форме хеша предшественника. Начальное состояние жестко закодировано в первом блоке, называемом блоком генезиса. В отличие от других блоков, у блока генезиса нет предшественника.

В отличие от блоков, структура DAG хранит транзакции в узлах, где каждый узел содержит одну транзакцию (Рис. 3). В криптовалюте Nano каждая учетная запись связана со своей собственной цепочкой счетов в структуре, называемой блочной решеткой, эквивалентной истории транзакций.

Каждому аккаунту предоставляется цепочка аккаунтов. Цепочка учетных записей может рассматриваться как выделенная цепочка блоков, только для одной учетной записи. Узлы добавляются к цепочке счетов, а каждый узел представляет одну транзакцию в цепочке счетов. Аналогично блоку генезиса в блокчейне, DAG содержит транзакцию генезиса. Генезис транзакции определяет начальное состояние. В Nano вместо одной транзакции, которая передает значение, для полной передачи значения необходимы две транзакции.

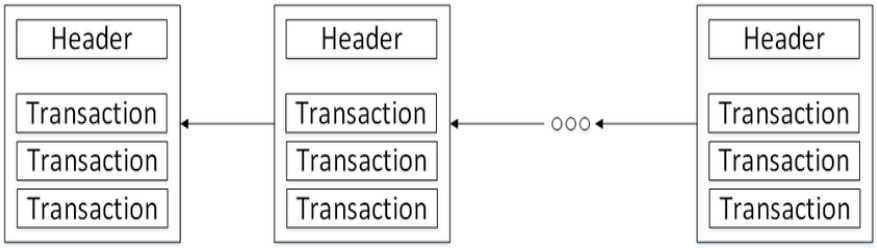


Рис. 2 - Структура блоков в Блокчейн

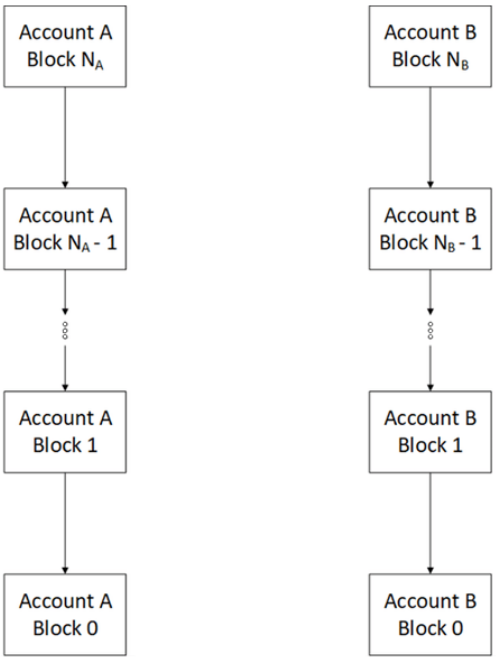
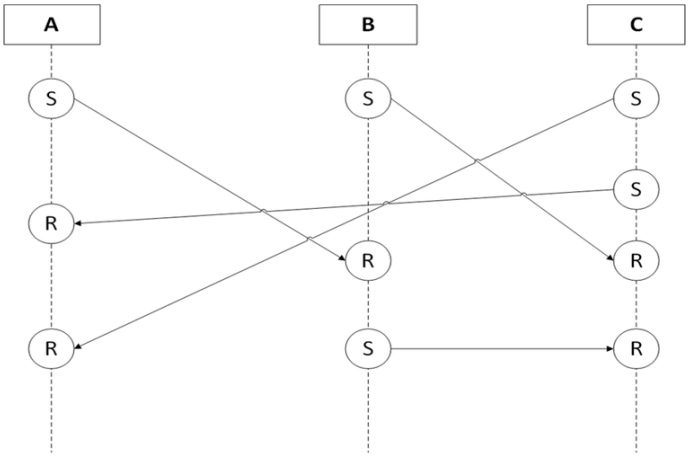


Рис. 3 - Структура блочной решетки в DAG



S - транзакция отправки;
R - транзакция приема.

Рис. 4 - Генерация транзакции отправки

Отправитель генерирует транзакцию отправки, в то время как получатель генерирует совпадающую транзакцию приема (Рис. 4). Когда выдается транзакция отправки, средства списываются с баланса счета отправителя, ожидая, пока получатель получит соответствующую транзакцию приема. В этом состоянии транзакции считаются неурегулированными. Когда транзакция получения сгенерирована, транзакция рассчитывается. Недостатком такого подхода является то, что узел должен быть подключен к сети для получения транзакции.

Обработка транзакций в блочной решетке.

Каждая транзакция разбивается на блоки отправки в цепочке отправителя и, соответственно, блок получения в цепочке получателя. Транзакция отправки вычитает средства из баланса отправителя, в то время как транзакция получения добавляет средства к балансу получающего счета. Если владелец аккаунта ведет себя подозрительно, то остальная часть

сети проголосует против недействительного блока, и он будет отклонен.

Каждая цепочка аккаунтов обновляется только владельцем аккаунта вследствие того, что каждый блок в цепочке должен быть подписан закрытым ключом учетных записей. Остальная сеть узлов по-прежнему будет подтверждать, что каждый блок является действительным (нет дубля расходов и пользователи не увеличивают свой баланс больше предусмотренного).

Nano использует Proof of Work (PoW), чтобы избежать спамеров, поскольку в сети не взимается плата за транзакции. Для работы с каждым блоком необходимо небольшое количество времени, примерно 5 секунд для генерации и 1 *мкс* для его проверки. Это заставляет злоумышленников выделять значительную вычислительную мощность для реализации атаки, в то время как всем остальным (легальным пользователям) требуется лишь небольшое количество вычислительных ресурсов. Также возможно удаление этих спам-транзакций, что ограничивает объем хранилища, которое можно использовать при атаках этого типа.

Атаки:

- *«Атака с потерей денег»*: злоумышленники увеличивают количество цепочек, которые должен отслеживать узел, отправляя незначительные суммы в широкий ряд пустых «кошельков».
- *«Двойная трата злоумышленника»*. Обе версии двойных расходов должны быть подписаны закрытым ключом пользователя. Следует определить учетные записи, которые отвечают за спам-атаки, а затем внести их в соответствующий «черный» список на определенный период времени.

Используется: - в Nano [6].

Плюсы:

- меньшие требования к хранению за счет сокращения базы данных, поскольку блокчейн каждого пользователя отслеживает баланс своего счета, а не суммы транзакций;
- блокчейн пользователя обновляется асинхронно с остальной частью блочной решетки;
- меньшее время транзакции (т.к. вся сеть не обрабатывает каждую транзакцию);
- нет комиссии за транзакции в сети.

Минусы:

- нет финансовых стимулов для запуска полного узла;
- Нано является дефляционной валютой (постоянно растет в цене);
- нет «умных» контрактов.

3 Алгоритмы консенсуса основанные на Proof of Work

3.1 Proof of Work (PoW)

Принцип: - трудно найти решение, но легко проверить результат.
Производительность: - низкая.
Среда DLT: - публичный блокчейн..
Завершенность: вероятностная.

PoW первоначально была создана как средство борьбы со спамом. Так, например, майнеры используют PoW для проверки транзакций, но его главная цель - блокировка потенциальных кибератак или подозрительных действий в сети. Суть данного алгоритма сводиться к двум основным пунктам:

- необходимости выполнения определенной достаточно сложной и длительной задачи;
- возможности быстро и легко проверить результат.

PoW задачи изначально не предназначены для их решения человеком. Решение выполняется компьютером, однако требует больших вычислительных мощностей. При этом важно то, что проверка полученного решения всегда требует гораздо меньше ресурсов и времени.

Майнеры

В криптовалютных сетях «майнеры» - это специальные узлы, которые выполняют вычисление PoW для набора транзакций, плюс хэш предыдущего блока для генерации следующего блока в цепочке блоков. Очевидно, что поскольку блок содержит хэш предыдущего блока, то

изменение «исторического» блока потребует регенерации всех последующих блоков. Таким образом, восстановление всех хэшей потребует большого объема вычислений и дополнительного расхода энергии (т.е. дополнительных финансовых расходов). Процесс использования аппаратных ресурсов компьютера для выполнения вычислений с целью подтверждения транзакций и обеспечения безопасности сети называется майнингом. Майнеры вознаграждаются за выполнение этих функций новыми монетами (*вновь создаваемыми биткойнами*).

Узлы

Узлы всегда считают, что самая длинная цепочка является правильной и продолжают работать над ее расширением. Если два узла одновременно транслируют разные версии одного блока, то некоторые узлы могут получить любой из них в первую очередь. В этом случае они работают над блоком, который был получен первым, но сохраняют и другую ветвь, на случай, если она станет длиннее. При обнаружении следующего доказательства работы, связь будет разорвана, т.к. одна ветвь станет длиннее, а узлы, которые «работали» в другой ветке, переключатся на более длинную ветвь.

Алгоритм

1. Транзакции связываются в виде блоков.
2. Майнеры проверяют транзакции внутри блоков на их подлинность.
3. Майнеры решают задачу, известную как «проблема доказательства работы».
4. Формируется награда первому, кто решит «проблему …».
5. Подлинные транзакции записываются в общедоступную цепочку блоков.

Атаки

Угроза централизации вычислительных мощностей, известная как атака 51%, считается одной из ключевых уязвимостей для алгоритма консенсуса PoW. Это происходит, когда у атакующей стороны, в роли которой может выступать сравнительно небольшое количество майнеров, находится «контрольный пакет» хэшрейта – вычислительной мощности сети.

Причиной данной уязвимости является тот факт, что майнеры могут одновременно предлагать сети верные хэши – решения, которые позволяют им подтверждать целостность данных и добавлять в сеть новые блоки. В этом случае в блокчейне происходит «разветвление». Алгоритм консенсуса PoW считает, что остальные майнеры признают верной ту ветвь, которая имеет наибольшее количество блоков, и проголосуют за ее включение в блокчейн. Таким образом, если майнер или совокупность майнеров контролируют больше половины хэшрейта, то у него/их появляется возможность добавлять свои ветви и тем самым манипулировать двусторонними операциями и не подтверждать новые транзакции.

Эта атака может привести к тому, что недобросовестные майнеры могут отзывать уже совершенные финансовые транзакции, что называется двойной тратой (*double-spending*). При этом атакующая сторона не может менять информацию в уже добавленных блоках и генерировать новые криптовалюты.

Плюсы:

- самый известный и самый безопасный;
- комиссия за транзакцию не обязательна;
- легко проверяемые решения;
- трудоемкость поиска решения;
- трудоемкость поиска решения может быть точно количественно оценена.

Минусы:

- низкая производительность;
- PoW характеризуется большим потреблением вычислительных мощностей, что само по себе снижает стимул;
- PoW уязвим для серьезных уязвимостей (например, атака 51 %);
- уменьшение награды за блок;
- доказательство работы ограничивает входные данные структурой алгоритма майнинга блокчейнов. В случае «Биткойна» это должен быть одноразовый номер, а в случае

«Эфириума» входными данными может являться случайное целое число, одноразовый номер и начальный хеш блока.

3.2 Hybrid Proof of Work (HPoW)

HPoW по-прежнему использует PoW, но модифицирует его, и как следствие, создает целую криптовалютную сеть, которая может работать на простых в настройке и недорогих компьютерах или облачных сервисах. HPoW устраняет стимул для майнеров, потому что награда за майнинг низкая. На самом деле, майнинговые фермы потеряли бы деньги, если бы попытались майнить в Lynx [7], где Lynx (LYNX) – криптовалюта или цифровой актив, а это значит, что они предоставят Lynx людям, которые хотят решить проблему устойчивости. Это забирает контроль у майнинговых ферм и отдает его в руки отдельных людей (индивидуальных майнеров), которые хотят работать на Lynx.

HPoW поддерживает обслуживание сети, стимулируя возможности тех, кто хочет использовать Lynx. С каждым подключаемым майнером сеть становится все более защищенной за счет снижения рисков, связанных с централизацией криптовалютной сети. Эта безопасность достигается, в том числе, за счет избыточности: т.е. чем больше отдельных узлов в сети, тем более устойчивой она становится. При этом если происходит сбой отдельного узла или майнера, или же если выходит из строя даже весь регион узлов (например, из-за перебоев в подаче электроэнергии или воздействия техногенных факторов), то сеть остается по-прежнему работоспособной и защищена, вследствие существования множества других ресурсов для майнинга.

Три бизнес-правила HPoW:

1. Один майнер не может выиграть блок чаще, чем раз в 30 минут.
2. Баланс адресов майнера должен быть больше или равен требуемому минимальному количеству для Lynx, чтобы выиграть блок.
3. При случайном выборе, самые «быстрые» майнеры не всегда гарантированно получают награду за блок.

Минусы:

- добыча убыточна.

3.3 Proof of Meaningful Work (PoMW).

Текущая реализация, использующая только искусственные вычислительные задачи (хеширование), слишком расточительна для рационального использования и плохо масштабируется. PoMW первоначально реализует хорошую идею, однако при ее реализации, используются значительные вычислительные ресурсы.

Основной минус**:** - атака более 50 % от общей вычислительной мощности.

3.4 Proof-of-Work-Time (PoWT).

PoWT – это относительно новый подход к формированию консенсуса, путем введения переменного времени блокировки, которое масштабируется с мощностью майнинга (*где блокчейн ускоряется с увеличением мощности*). Его использование лучше масштабирует блокчейн, увеличивает скорость транзакции и позволяет автоматически настраивать более прибыльный майнинг. Время блокировки зависит от сложности (max около 6,2 мин, min порядка 15 сек). Награды зависят от времени блокирования.

3.5 Proof of Edit Distance.

Алгоритм «Редактирование расстояний» - это класс алгоритмов, которые оценивают, насколько близко две строки находятся друг к другу. Например, расстояние редактирования для «ETH» (*Ethereum*) и «ETC» (*Ethereum Classic*) равно «0,8222», где две одинаковые строки будут иметь значение «1». Известно много алгоритмов, также в пространстве сходства строк, включая расстояние Левенштейна, расстояние Смита-Уотермана Гото и расстояние Рэтклифа-Обершелпа [8].

Использование Proof of Edit для создания новых блоков.

Майнеры конкурируют, чтобы найти строку, которая при хешировании в процессе нормализации превышает порог минимального расстояния. Эта строка может являться хэшем промежуточной цепочки блоков и заголовком хеша для следующего блока.

Пусть минимальное пороговое расстояние - «*t*», строка для поиска - «*B*», а редактированная функция расстояния – «ED», такая, что для каждого заголовка блокчейн удовлетворяет хэшу «*h*»:

$$ED\ (H\ (h),H\ (B))\ <t\ .$$

Или в случае объединения 2-х блокчейнов:

$$ED\ (H\ (h1),H\ (B))\ <t\ \&\&\ ED\ (H\ (h2),H\ (B))\ <t\ \ =\text{верно.}$$

Чтобы найти новый блок в промежуточной цепочке, майнер должен перебирать случайный набор символов (хэшируя строки), пока не найдется хэш, превышающий пороговое значение для всех блоков.

Плюсы:

- доказательством редактирования расстояния является независимый алгоритм майнинга;
- любой хеш или строковая структура могут быть предоставлены в качестве входных данных. Это означает, что пока блокчейн имеет уникальный хеш, его можно легко добавить в задачу «Доказательство редактирования».

Используется в Block Collider [9].

4 Алгоритмы консенсуса основанные на Proof of Stake

4.1 Proof of stake (PoS)

Принцип: - сеть доверяет валидатору, который предоставляет свои ресурсы в залог за возможность создавать блоки: - чем больше доля, тем выше вероятность того, что сеть разрешит создание блока.

Производительность: - высокая.

Среда DLT: - публичный/приватный блокчейн.

Завершенность: - вероятностная.

PoS работает с использованием алгоритма, который выбирает участников с самыми высокими ставками в качестве валидаторов, предполагая, что они заинтересованы в обработке транзакции. При этом у кого больше всего монет в обращении, больше всего и теряют, поэтому они готовы работать в интересах сети. Количество монет, которое сеть может потребовать изменяется, так же, как и сложность в PoW (рассматривалось выше).

В PoS блоки создаются не майнерами, выполняющими работу, а майнерами, которые ставят свои токены, чтобы «делать ставки» на то, какие блоки являются действительными. В случае разветвления, майнеры тратят свои жетоны на голосование, т.е какое ветвление поддерживать. Т.о. предполагая, что большинство пользователей голосуют за «правильную» вилку, валидаторы, проголосовавшие за неправильный вариант, «потеряют свою долю» в правильной вилке.

Общим аргументом против *proof-of-stake* является т.н. проблема «Ничто на кону» (*Nothing at Stake*). Она заключается в том, что валидаторы практически не требуют вычислительной мощности для поддержки разветвления (в отличие от PoW) и могут голосовать за обе стороны каждого ветвления. Т.о. форки в PoS могут быть гораздо более распространенными [9], чем в PoW, а это, как полагают некоторые специалисты, может снизить доверие к валюте.

Coin age (возраст монеты).

Чтобы различать пользователей, которые только что получили свои монеты, и пользователей, которые держали свои монеты в течение определенного периода времени, в алгоритмах доказательства ставки используется концепция возраста монет (*Coin age*).

Возраст монет используется, как в расчетах веса ставки, так и вознаграждения за ставку. Вознаграждение за ставку устанавливается APR монеты [10]. Данная характеристика имеет

постоянный интерес для всех кошельков со ставками, независимо от размера ввода или разумного времени простоя.

Чем дольше пользователь держит монеты, тем вероятнее возможность выиграть право создать блок сетевой цепочки блоков и получить вознаграждение.

Технология стимулирования пользователей.

Для поддержки сетевой активности и привлечения большего количества пользователей, награда за создание блока увеличивается, если в сети присутствует много пользователей.

Наказание пользователя за отсутствие активности (оффлайн).

Большинство, если не весь алгоритм PoS, наказывают держателей монет, которые остаются в автономном режиме в течение длительных периодов времени. В противном случае они могли бы получить контроль, получив более 50% прав голоса из-за размера своих владений.

Псевдо-анонимные пользователи.

Валидаторы в сети PoS - это анонимные пользователи, которые идентифицируются только по адресу своего кошелька. Это не дает никакой дополнительной ответственности по отношению к PoW плохим игрокам, которые могут накопить значительную выгоду в сети.

Безопасность.

Модель безопасности является сугубо экономической, основанной на том предположении «теории игр», что стоимость приобретения токенов, необходимых для перехода в статус производителя блоков, больше той стоимости, которую злоумышленник готов внести. Это обстоятельство связывает безопасность сети со значением ее токенов, т.е.: чем выше значение токена, тем более защищенной становится сеть.

Атака "Ничего на кону".

Без системы экономических штрафов для злоумышленников сеть может подвергнуться атакам «ничто на кону», когда заинтересованные лица мотивированы в проверке всех предлагаемых вилок для максимизации прибыли.

Алгоритм.

1. Валидаторы в качестве ставки блокируют часть своих монет.

2. Валидаторы инициируют проверку блоков. В случае обнаружения блока, который, по их мнению, может быть добавлен в цепочку, его подтверждают, делая на него ставку.

3. При добавлении блока в цепочку, валидатор получает вознаграждение, пропорциональное его ставке.

Плюсы:

- рентабельность: скорость, энергия, оборудование;
- чем большее число пользователей используют сеть и имеют монеты, тем безопаснее сеть;
- по отношению к другим более децентрализованный.

Минусы:

- характерно «экономическое неравенство», т.е. богатые становятся еще богаче;
- злоумышленники могут рассчитать вероятность получения награды, чтобы создать блок цепочки блоков, основываясь на анализе, у кого сколько монет;
- начальные цели для реализации Ethereum Casper - всего 100 TPS *(Transactions per Second)*;
- подвержен атаке «Ничего на кону».

Используется в:

- Tezos [11];
- - Decred [12];
- - Ethereum;
- - Peercoin;
- - Ada;
- - EOS.IO [13];
- Gridcoin;
- Nxt [14];

- Waves [15];
- BlackCoin;
- Qtum;
- In Future with Casper in Ethereum.

4.2 Гибридный PBFT/Aurand.

Polkadot использует гибридный механизм консенсуса PBFT/Aurand, который имеет две степени завершенности. Этот механизм допускает переходы состояний с относительно низкой задержкой при одновременном демпфировании некоторых видов атак.

PBFT обеспечивает полную завершенность, а Aurand обеспечивает быструю промежуточную завершенность. В каждой последовательности блоков есть контрольная точка PBFT, которая гарантирует завершенность, в то время как Aurand устанавливает промежуточные состояния завершенности.

С помощью Aurand один случайно выбранный валидатор может предложить блок, который «может быть отменен». Они ограничиваются, если предполагается, что блоки недействительны. Для достижения консенсуса требуется соотношение не менее PBFT > 2/3 подписанных валидаторов (для согласования блока).

Завершенность PBFT происходит ориентировочно каждые 30 сек, в то время как блоки Aurand предлагаются каждые 4-5 сек.

Используется в Polkadot.

4.3 Delegated proof-of-stake (DPoS).

Принцип: - участники делегируют производство новых блоков небольшому, фиксированному числу избранных валидаторов, чем обеспечивается высокая конкуренция и выгодность.

Производительность: высокая.

Среда DLT: - публичный/приватный блокчейн.

Завершенность: - вероятностная.

DPoS – это алгоритм достижения консенсуса в децентрализованой среде, который является альтернативой консенсусам PoW (*Bitcoin proof-of-work*) и PoS (*Peercoin или NXT proof-of-stake*).

Основной принцип работы DPoS - это разделение голосующих и валидирующих участников. В итоге, участники сети, имеющие право голоса в системе (держатели монет) не являются при этом валидаторами транзакций. Таким образом, одно подмножество участников выбирает другое подмножество, которое в свою очередь, будет формировать блоки. При этом возраст монеты не имеет значения.

Условия, в которых работает данный алгоритм, отличаются от условий, в которых работают PoW и PoS. При этом валидаторам необходимо раскрыть свою личность и заявить о готовности поддержкивать работу полноценного узла сети, своевременно выполнять верификацию транзакций и формировать новые блоки. DPoS сильно отличается от PoS: - в данном случае владельцы токенов не голосуют за достоверность самих блоков, а голосуют за то, чтобы избрать валидаторов для проверки от их имени.

При использовании консенсуса на основе модифицированного PoS каждый пользователь, по желанию, может выставить свою кандидатуру на пост верифицирующей рабочей станции (проверяющего узла - валидатора). Затем среди всех пользователей проводится голосование за кандидатов, где вес каждого голоса определяется суммой активов голосующего. По результатам этого голосования выбирается некоторое число (*обычно 20-50*) кандидатов, которые получают право формировать новые блоки транзакций. Правила протокола гарантируют корректное принятие решений, если большая часть активов, принимающих участие в голосовании, контролируется «честными» пользователями.

Выбранные в результате голосования валидаторы перемешиваются случайным образом, образуя очередь. Перемешивание выполняется в соответствии со специальным алгоритмом, так что предсказать очередь практически невозможно. Далее выделяется период времени, в течении которого каждый из валидаторов должен сформировать один блок очереди. При

этом либо валидатор успевает проверить новые транзакции и сформировать новый блок на основании предыдущего, либо эту работу сделает валидатор, но уже следующий в очереди. После завершения установленного периода времени (обычно порядка 1 сек) валидаторы снова перемешиваются и формируют новую очередь.

Важно отметить, что держатели монет могут выполнять переголосование за кандидатов в произвольное время. Т.о. текущая группа валидаторов может измениться и их новая очередь будет сформирована уже другим составом. Кроме того, один держатель монет может голосовать более чем за одного кандидата, распределяя вес своих монет пропорционально между несколькими кандидатами.

Посредством DPoS пользователи могут выбирать репрезентативный узел для голосования от их имени, выступая в качестве доверенного лица для голосования. Делегированный узел выполняет такие задачи, как проверка подписей для блоков, которые обрабатываются, а в случае конфликтующих транзакций - голосование за действительную транзакцию.

Используется в:

- Steemit;
- EOS;
- BitShares [16].

Плюсы:

- дешевые транзакции;
- масштабируемость;
- энергоэффективный;
- возраст монеты не имеет значения: - отсутствие возраста означает, что перемещение монет менее затратно;
- результатом является стабильный, постоянный интерес только для активных кошельков и только с небольшими затратами;
- время простоя значительно влияют на пользовательский интерес к DPOS.

Минусы:

- подвержен атаке «Ничего на кону»;
- частично централизованный.

4.4 Proof-of-Stake-Time (PoST).

Это новый подход к формированию консенсуса путем введения компонента времени ставки, где вероятность ставок увеличивается со временем, то есть ставка времени является произведением общего количества монет (C) и доли (f) приемлемого возраста (a). Это улучшает стимул для размещения и повышает безопасность сети. Это также усиливает децентрализацию консенсуса, что значительно превосходит существующие стандарты.

Используется в: PostCoin и Vericoin.

Плюсы: - поддерживает эффективность Proof-of-Stake.

4.5 Proof of stake Boo (PoS Boo)

PoS Boo - это PoS-схема, основанная на PoS Casper. Эта схема Casper лучше всего подходит для «POSv3» с введением фактора риска для злоумышленников. Система является прогрессивной, что значительно затрудняет выполнение таких атак, как атака 51%. Вам понадобятся большинство всех монет, и вы также столкнетесь с возможностью потерять их все при запуске такой атаки. Завершенность в основном определяется ставкой и факторами риска.

Плюсы:

- трудно выполнить атаку успешно даже с 51%;
- обеспечивает цензуру транзакций. С PoW майнер блоков может не майнить блок, содержащий определенные адреса, тем самым подвергая цензуре этот сетевой адрес. Так как создатели блоков выбираются случайным образом и валидаторы являются глобальными

с этой схемой PoS, очень сложно подвергать цензуре адреса из сети (в итоге можно потерять свою ставку).

Используется в SHIELD.

4.6 High Interest Proof of Stake (HiPoS)

Возраст монет используется в расчете для веса ставки, но не для вознаграждения за ставку. Ставка вознаграждения фиксируется по расписанию. Результатом является стабильный, постоянный интерес для размещения кошельков, поскольку время простоя минимально и затраты невелики. Большой входной размер строго наказывается HiPOS.

Используется в: - Positron (2015); - BitBean (2015); - EdgeCoin (EDGE) [17].

Плюсы:

- стимулирует и содействует удержанию пользователей, поскольку разработчики выпускают все больше информации о своих новых проектах.
- позволяет участникам с меньшими ресурсами/запасами получить большую выгоду, просто найдя несколько блоков в нужное время.

4.7 Traditional Proof of stake / Tiered Proof Of Stake (TPOS)

Это форма алгоритма, с помощью которой криптовалютная сеть Blockchain стремится реализовать распределенное соглашение. В производных от TPOS валютах источник следующего блока выбирается с помощью различных комбинаций случайного сбора и ставки.

Используется в XSN [18].

Плюсы: платежи в большей части рассчитаны на держателей монет, а не на майнеров.

4.8 Casper the Friendly Finality Gadget (FFG)

Алгоритм:

1. Валидаторы ставят часть своих ресурсов в виде ставки.
2. Валидаторы начинают проверку блоков. При обнаружении блока, который, по их мнению, может быть добавлен в цепочку, осуществляется его проверка и делается ставка.
3. В случае если блок будет добавлен, валидаторы получают вознаграждение пропорционально их ставкам.

Плюсы:

- все преимущества Proof of stake.
- возможность «наказания» валидаторов, пытающихсяпровести атаку «ничего не поставлено на карту».
- возможность «наказания» майнеров, которые уходят из сети.

Используется в Casper the Friendly GHOST: Correct-by-Construction (CBC): полный PoS.

4.9 Proof of Stake Velocity (PoSV)

PoSV предлагается в качестве альтернативы PoW и PoS для защиты одноранговой сети и подтверждения транзакций Reddcoin, криптовалюты, созданной специально для облегчения социальных взаимодействий. PoSV предназначен для поощрения как владения (Stake), так и активности (Velocity), которые напрямую соответствуют двум основным функциям Reddcoin, как реальной валюты: - хранилищу стоимости и средству обмена. Reddcoin также может функционировать в качестве расчетной единицы в разном социальном контексте.

Используется в: Reddcoin [19].

4.10 Magi's proof-of-stake (mPoS)

Цели достижения распределенного консенсуса посредством операций в дополнение к mPoW. mPoS спроектирован таким образом, что он отклоняет потенциальные атаки путем накопления большого количества монет или времени автономной игры, что приводит к проблемам с безопасностью. По аналогии с mPoW, mPoS строится в соответствии с концепцией

модели притяжения-отталкивания. Magi является гибридным решением mPoW с mPoS и объединяет оба согласованных подхода, чтобы получить преимущества от двух механизмов и создать более надежную платежную систему.

Используется в: MAGI и Bitcointalk [20,21].

4.11 Leased Proof-of-Stake (LPoS)

Вероятность нахождения нового блока зависит только от того, сколько есть токенов (т.е. от ставки).

Используется в: NXT и Waves [14,15].

Плюсы: не требует значительной вычислительной мощности, чтобы создать новый блок.

4.12 Leasing Proof of Stake (PoS/LPoS)

LPoS - это расширенная версия Proof-of-Stake. В обычной системе Proof-of-Stake каждый узел, который содержит определенную сумму криптовалюты, имеет право добавить следующий блок в цепочку блоков, но в системе LPoS на платформе Waves пользователи могут сдавать в аренду свой баланс для полных узлов. С LPoS пользователь будет иметь возможность сдавать в аренду WAVES из кошелька разным подрядчикам, которые могут выплатить процент в качестве вознаграждения. Чем больше сумма, сдаваемая в аренду для полного узла, тем выше вероятность того, что этот узел будет выбран для создания следующего блока. Если этот полный узел выбран для создания следующего блока, арендатор получит процент от суммы транзакции, которую собирает полный узел. В среде LeasedProof-of-Stake пользователи могут выбирать между выполнением полного узла или передачей своей доли в полный узел с получением вознаграждений. Эта система позволяет любому участвовать в обслуживании сети Waves. Пользователь может передавать свои волны через лизинг на любом компьютере или мобильном устройстве, имеющем интернет-браузер, поскольку Waves предоставляет облегченное клиентское решение, не требующее майнеров, которые сдают в аренду свой баланс для хранения всей цепочки блоков или для запуска кошелька.

Используется в: NXT и Waves [14,15].

5 Выводы

Протоколы консенсуса являются неотъемлемой частью распределенных систем. В первую очередь они помогают достигать справедливости, избегать сбоев системы, когда один из участников (узлов) выходит из строя. Во-вторых, децентрализованная среда требует решения, которое поможет двигаться вперёд и изменять общее состояние, даже в среде, где никто никому не доверяет. Определенные правила помогают достичь «консенсуса».

В работе рассмотрена лишь некоторая часть, наиболее распространенных, алгоритмов проколов консенсуса, которые имеют разные характеристики, особенности и уязвимости. Сделан вывод о том, что, не существует идеального алгоритма, а у каждого из них есть свои плюсы и минусы. Используя их сильные стороны, в каждом конкретном случае, следует подбирать наиболее подходящий вариант реализации алгоритма, максимально учитывающий специфику условий и основной контекст решаемой задачи.

Ссылки

[1] Roper Klacks. Blockchain. "2018. URL: https://en.wikipedia.org/wiki/Blockchain
[2] Cedric Walter. Blockchain Consensus. URL: https://tokens-economy.gitbook.io/consensus/
[3] IOTA. URL: https://www.iota.org/
[4] Hegera. URL: https://www.hedera.com/
[5] Sybil attack. URL: https://en.wikipedia.org/wiki/Sybil_attack
[6] Nano. URL: https://nano.org/en
[7] LYNX. URL: https://getlynx.io/
[8] McConlogue P. Building a Blockchain Singularity with Proof of Distance.URL: https://blog.blockcollider.org/building-a-blockchain-singularity-with-proof-of-edit-distance-1d60c328de7a
[9] Форк. URL: https://ru.bitcoinwiki.org/wiki/%D0%A4%D0%BE%D1%80%D0%BA

[10] APR Coin. URL: https://apr-coin.com/
[11] Tezos. URL: https://tezos.com/
[12] Decred. URL:https://decred.org/ru/
[13] EOIS. URL: https://eos.io/
[14] NXT. URL: https://nxtplatform.org/
[15] Waves. URL: https://wavesplatform.com/
[16] Bitshares. URL: https://bitshares.org/
[17] EdgeCoin. URL: https://www.edgecoin.io/
[18] XSN. URL: https://stakenet.io/
[19] Reddcoin. URL: https://reddcoin.com/
[20] MAGI. URL: https://www.m-core.org/
[21] Bitcointalk. URL: https://bitcointalk.com/

Reviewer: Alexandr Potii, Dr. of Sciences (Engineering), Full Prof., V. N. Karazin Kharkiv National University, Kharkiv, 61022, Ukraine. E-mail: potav@ua.fm

Received: March 2019.

Authors:
Diana Kovalchuk, student of CSD, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: dianakovalhyk@ukr.net
Tetiana Ivko, Researcher, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: t.ivko@outlook.com
Tetiana Kuznetsova, Researcher, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: kuznetsova.tatiana17@gmail.com
Oleksii Nariezhnii, Ph.D., Associate Professor, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: o.nariezhnii@karazin.ua

Review of consensus protocols used in Blockchain technologies.

Abstract. The categories of popular consensus punctures are reviewed: Proof of Work and its hybrids, Proof of Stake (includes LPoS, Proof of Importance) and hybrids, DAGs and its varieties. The article describes their algorithms, characteristics, features, as well as disadvantages and advantages. Vulnerabilities and attacks are subject to. Also provides a list of the use of each protocol in cryptocurrencies and other systems.

Keywords: Consensus; Blockchain; Blockchain Consensus Protocol; Decentralized Systems; Distributed Registry.

Рецензент: Олександр Потій, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, 61022, Україна.
E-mail: potav@ua.fm

Надійшло: Березень 2019.

Автори:
Діана Ковальчук, студентка факультету комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, Харків, 61022, Україна.
E-mail: dianakovalhyk@ukr.net
Тетяна Івко, науковий співробітник, Харківський національний університет імені В.Н. Каразіна, Харків, 61022, Україна.
E-mail: t.ivko@outlook.com
Тетяна Кузнецова, науковий співробітник, Харківський національний університет імені В.Н. Каразіна, Харків, 61022, Україна.
E-mail: kuznetsova.tatiana17@gmail.com
Олексій Нарєжній, к.т.н., доцент кафедри, Харківський національний університет імені В.Н. Каразіна, Харків, 61022, Україна..
E-mail: o.nariezhnii@karazin.ua

Огляд протоколів консенсусу, що застосовуються в технологіях блокчейн.

Анотація. Розглянуто категорії популярних проколів консенсусу: Proof of Work і його гібриди, Proof of Stake (LPoS, Proof of Importance) та гібриди, DAGs. У роботі стисло описані їх алгоритми, характеристики, особливості, а також недоліки та переваги. Зазначені відомі вразливості та атаки до яких вони схильні. Наведено приклади використання кожного з протоколів, що розглядаються, в криптовалютах та інших системах.

Ключові слова: консенсус; блокчейн; протокол консенсусу блокчейн; децентралізовані системи; розподілений реєстр.