UBF

Алгоритмы консенсуса

Введение

В рамках данной статьи мы рассмотрим, какие механизмы консенсуса существуют в криптоиндустрии, что это такое и как они устроены.

Для начала следует обратиться к такому процессу как майнинг, так как он появился вместе с биткоином и, как следствие, первым алгоритмом консенсуса.

Майнинг — это процесс добавления новых транзакций в блокчейн, представляющий собой децентрализованную цифровую бухгалтерскую книгу, которая фиксирует все транзакции конкретной криптовалюты. Майнинг является важным компонентом многих криптовалют, включая Bitcoin и Ethereum, и играет решающую роль в их безопасной и стабильной работе.

На высоком уровне майнинг предполагает решение сложных математических задач с помощью мощных компьютеров. Эти задачи создаются таким образом, чтобы их было очень сложно решить, но относительно легко проверить. Майнеры соревнуются в решении этих задач, и первый майнер, нашедший решение конкретной задачи, получает вознаграждение в виде новых единиц криптовалюты, а также комиссий, связанных с транзакциями, которые он добавил в блокчейн. Решение каждой задачи служит доказательством проделанной работы, поэтому этот процесс называется «доказательством работы», или Proof of Work.

Для осуществления майнинга необходимо запустить специализированное программное обеспечение на компьютере с высокими вычислительными мощностями, именуемым майнинговой установкой. Программное обеспечение выполняет ряд вычислений и пытается найти хэш — уникальную строку символов, которая идентифицирует решение задачи. Как только майнер находит правильный хэш, он передает свое решение в сеть, и другие майнеры проверяют правильность решения, выполнив те же вычисления. Если решение верно, майнер получает вознаграждение, а транзакция добавляется в блокчейн.

Майнинг — критически важный процесс для криптовалют, ведь благодаря ему добавляются новые транзакции в блокчейн и поддерживается целостность «бухгалтерской книги». Обеспечивая стимул для майнеров вкладывать свои вычислительные мощности в сеть, майнинг гарантирует децентрализованность и безопасность блокчейна, а также дает возможность вводить в оборот новые единицы криптовалюты. В то же время майнинг требует больших энергозатрат и может быть экологически неустойчивым, из-за чего создатели некоторых криптовалют ищут альтернативные методы подтверждения транзакций.

Существует несколько альтернативных методов подтверждения транзакций, их также называют алгоритмами консенсуса:

- Proof of Work (PoW). Это оригинальный алгоритм консенсуса, используемый в Bitcoin и предполагающий решение сложных математических задач с применением вычислительных мощностей. PoW вознаграждает майнеров новыми единицами криптовалюты за добавление новых блоков в блокчейн.

- Proof of Stake (PoS). Этот алгоритм требует, чтобы валидаторы держали определенное количество криптовалюты в качестве залога, который называется ставкой. Валидаторы выбираются случайным образом для подтверждения транзакций и добавления новых блоков в блокчейн. Валидаторы, которые правильно выполняют свои обязанности, получают вознаграждение в виде дополнительной криптовалюты.

- Delegated Proof of Stake (DPoS). Это вариант PoS, при котором валидаторы могут быть избраны держателями токенов для подтверждения транзакций и добавления новых блоков в блокчейн. DPoS обеспечивает большую масштабируемость и более быструю обработку транзакций.

- Proof of Authority (PoA). Этот алгоритм требует, чтобы валидаторы были одобрены существующими в сети валидаторами, и они, как правило, должны подтверждать свою личность. Валидаторы вознаграждаются криптовалютой за добавление новых блоков в блокчейн.

- Byzantine Fault Tolerance (BFT). Этот алгоритм разработан для работы в сети с известным числом валидаторов, и он требует, чтобы определенное число валидаторов соглашалось с подлинностью каждой транзакции. BFT используется в некоторых блокчейнах, которые зачастую применяются в корпоративных приложениях.

- Directional Acyclic Graph (DAG). Этот алгоритм используется в работе некоторых криптовалют, таких как IOTA, и позволяет осуществлять нелинейную обработку транзакций. В DAG каждая транзакция должна подтвердить две предыдущие транзакции, что позволяет увеличить масштабируемость и ускорить их обработку.

Существуют и другие алгоритмы консенсуса, только предложенные или находящиеся в разработке, включая доказательство емкости (PoC), доказательство истекшего времени (PoET) и доказательство идентичности (PoI). Каждый алгоритм консенсуса имеет свои сильные и слабые стороны и предназначен для решения различных проблем технологии блокчейн, таких как масштабируемость, энергопотребление и децентрализация.

Proof of Work

Proof of Work (PoW) — это алгоритм консенсуса, используемый во многих блокчейн-сетях, включая Bitcoin. Алгоритм PoW предназначен для обеспечения безопасности сети, подтверждения транзакций и создания новых блоков в блокчейне.

В системе PoW майнеры соревнуются в решении сложной математической головоломки с использованием вычислительной мощности, что требует значительных затрат энергии. Первый майнер, решивший головоломку, получает вознаграждение в виде новой криптовалюты и комиссии, связанной

с транзакциями, включенными в блок. Затем этот майнер передает новый блок в сеть, а другие узлы сети подтверждают блок и добавляют его в собственную копию блокчейна.

Сложность головоломки регулируется для поддержания постоянной скорости создания блоков, и сама головоломка должна быть решена для каждого нового блока, добавляемого в блокчейн. Вычислительная мощность, необходимая для решения головоломки, называется хэшрейтом. Она может быть увеличена или уменьшена путем добавления или удаления майнинговых установок из сети.

Алгоритм PoW считается безопасным, поскольку решить головоломку сложно, а приобрести оборудование с вычислительной мощностью, необходимой для решения задачи, — дорого. Таким образом, простому человеку или группе людей трудно получить контроль над сетью и осуществить атаку.

В то же время алгоритм PoW имеет некоторые ограничения, такие как высокое потребление энергии, необходимое для поддержания сети, и возможность возникновения централизации, так как небольшое количество майнеров контролирует большую часть вычислительной мощности сети. Эти ограничения привели к появлению альтернативных алгоритмов консенсуса, таких как Proof of Stake (PoS) и Delegated Proof of Stake (DPoS), которые направлены на решение этих проблем.

Proof of Stake

Proof of Stake (PoS) — это альтернатива алгоритму консенсуса Proof of Work (PoW), используемому в некоторых криптовалютах, включая Ethereum. В отличие от PoW, требующего от майнеров решения сложных математических задач с использованием вычислительной мощности, PoS полагается на валидаторов, которые ставят свою собственную криптовалюту в качестве залога для проверки транзакций и добавления блоков в блокчейн.

Определенное количество криптовалюты, вносимое валидаторами в системе PoS в качестве залога, называется ставкой. Размер ставки определяет шансы валидатора быть выбранным для подтверждения следующего блока транзакций. Чем больше ставка, тем выше шансы быть выбранным. Валидаторы выбираются случайным образом для создания нового блока, их задача — проверить транзакции в этом блоке и добавить его в блокчейн. Валидаторы, которые корректно выполняют свои обязанности, получают вознаграждение в виде дополнительной криптовалюты.

Одним из ключевых преимуществ PoS является то, что он гораздо менее энергоемкий, чем PoW. PoW требует от майнеров выполнения сложных вычислений, для которых необходимо значительное количество электроэнергии, что приводит к высокому энергопотреблению и выбросам углекислого газа. Валидаторам PoS, в свою очередь, нужно только запустить узел и проверить транзакции, что можно сделать с гораздо меньшими затратами энергии.

Еще одно преимущество алгоритма PoS заключается в том, что он снижает риск централизации в майнинге. В PoW майнеры с наибольшей вычислительной мощностью имеют наибольшие шансы добавить блок в блокчейн, и это может привести к централизации, если небольшая группа майнеров будет контролировать большую часть вычислительной мощности сети. В отличие от PoW, PoS вознаграждает тех, кто владеет наибольшим количеством криптовалюты, что может помочь предотвратить централизацию.

Однако PoS не лишена своих недостатков. Одной из главных проблем является риск атаки «ничего на кону», когда валидаторы могут попытаться подтвердить расходящиеся блоки, чтобы получить вознаграждение. Для снижения этого риска в блокчейнах PoS используется механизм, называемый финализацией, который делает практически невозможным подтверждение более одного блока в данном отрезке. Среди других проблем — обеспечение справедливого распределения криптовалюты и предотвращение сговора между валидаторами.

В целом PoS является перспективной альтернативой PoW в создании более устойчивой и децентрализованной сети блокчейн.

Proof of Authority

Proof of Authority (PoA) — это алгоритм консенсуса, используемый в некоторых сетях блокчейн. В отличие от Proof of Work (PoW) или Proof of Stake (PoS), PoA не полагается на майнеров. Вместо этого PoA требует определенного количества предварительно одобренных узлов, известных как валидаторы, для подтверждения транзакций и добавления новых блоков в блокчейн.

В системе PoA валидаторы обычно выбираются на основе их репутации, реальной личности или доли в сети. Валидаторы отвечают за проверку транзакций и добавление новых блоков в блокчейн, а за свою работу они получают криптовалюту. PoA позволяет обрабатывать транзакции быстрее и имеет более высокую степень масштабируемости по сравнению с PoW или PoS, поскольку не требует энергоемкого процесса решения сложных математических задач.

Алгоритм PoA опирается на достижение консенсуса на основе идентификации. Валидаторы выбираются на основе их репутации, и это означает, что они должны иметь положительный опыт вклада в работу сети. Они также должны подтвердить свою реальную личность, что поможет предотвратить участие в сети злоумышленников. В некоторых случаях от валидаторов также может потребоваться внесение определенной суммы криптовалюты в качестве залога, который может быть конфискован в случае совершения злонамеренных действий.

Одним из ключевых преимуществ PoA является то, что он позволяет ускорить обработку транзакций в сравнении с другими алгоритмами консенсуса. Это связано с тем, что процедура добавления новых блоков в блокчейн более оптимизирована и не требует энергоемкого процесса решения сложных математических задач. PoA также эффективенее с точки зрения потребления энергии, чем PoW, который требует значительного количества электроэнергии.

Однако PoA имеет и некоторые потенциальные недостатки. Один из них заключается в том, что сеть может стать более централизованной, поскольку валидаторы утверждаются предварительно, а их количество может быть ограничено. Кроме того, PoA, основанный на идентификации, способен вызвать проблемы с конфиденциальностью, поскольку для участия в сети пользователи должны раскрывать свою реальную личность. Наконец, PoA может быть уязвима в отношении сговора между валидаторами, если они решат действовать злонамеренно.

В целом PoA является перспективным алгоритмом консенсуса для создания более быстрых и эффективных сетей блокчейн. Однако он может подойти не для всех целей использования и потребовать тщательного рассмотрения конкретных требований сети.

Byzantine Fault Tolerance

Byzantine Fault Tolerance (BFT) — это алгоритм консенсуса, предназначенный для работы в сети, где узлы могут выйти из строя или вести себя злонамеренно. Алгоритм основан на Задаче византийских генералов, которая представляет собой теоретический сценарий, когда группа генералов должна координировать атаку на общего врага, но некоторые из них могут оказаться предателями и попытаться саботировать операцию.

В системе BFT определенное количество узлов, известных как валидаторы, отвечает за проверку транзакций и добавление новых блоков в блокчейн. Валидаторы должны общаться друг с другом, чтобы прийти к консенсусу относительно подлинности каждой транзакции, даже если некоторые из узлов неисправны или ведут себя злонамеренно.

Алгоритмы BFT работают, требуя, чтобы определенное количество валидаторов согласилось с достоверностью каждой транзакции. Это число называется кворумом и обычно составляет большинство валидаторов в сети. Если валидаторы не могут прийти к согласию, то транзакция считается недействительной и не добавляется в блокчейн.

Существует несколько вариантов алгоритма BFT, включая Practical Byzantine Fault Tolerance (PBFT) и Federated Byzantine Agreement (FBA). PBFT используется в некоторых разрешенных блокчейн-сетях, таких как Hyperledger Fabric, и требует, чтобы валидаторы общались друг с другом в одноранговом режиме для достижения консенсуса. FBA используется в некоторых публичных блокчейн-сетях, таких как Stellar, и применяет федеративный подход, при котором валидаторы группируются по различным доменам.

Алгоритмы BFT разработаны для обеспечения отказоустойчивости, а также устойчивости к атакам при условии, что кворум валидаторов честен и действует корректно. Но они могут быть менее эффективными с точки зрения производительности и масштабируемости по сравнению с другими алгоритмами консенсуса, такими как Proof of Stake или Delegated Proof of Stake.

В целом BFT — это алгоритм консенсуса, разработанный для сетей, в которых узлы могут выйти из строя или вести себя злонамеренно. BFT требует кворума валидаторов для согласования достоверности каждой транзакции, и он используется в некоторых разрешенных и публичных блокчейн-сетях для обеспечения безопасности и надежности системы.

Directional Acyclic Graph

Направленный ациклический граф (DAG) — это тип структуры данных, используемый в некоторых сетях блокчейн в качестве альтернативы традиционной линейной структуре блоков большинства блокчейн-сетей. В DAG транзакции представлены в виде узлов, и каждый узел соединен с другими узлами направленными ребрами, которые представляют порядок транзакций. В отличие от традиционного блокчейна, в DAG может создаваться несколько блоков одновременно, и каждый блок связан с одним или несколькими другими блоками.

В системе на основе DAG каждый пользователь, участвующий в сети, отвечает за проверку новых транзакций и добавление их в DAG. Этот подход известен как «безблочный», поскольку здесь нет блоков в традиционном понимании. Вместо этого транзакции организованы в графоподобную структуру с топологическим упорядочиванием, отражающим причинно-следственные связи.

Одним из ключевых преимуществ систем на основе DAG является то, что они потенциально могут предложить более быструю обработку транзакций и более высокую масштабируемость в сравнении с традиционными блокчейнами. Это связано с тем, что в системах на основе DAG нет такого «узкого места», как один майнер или валидатор, добавляющий новые блоки в блокчейн. Вместо этого транзакции могут быть подтверждены и добавлены в DAG любым пользователем, что обеспечивает параллельную обработку и большую эффективность.

Существует несколько блокчейн-сетей на основе DAG, включая IOTA и Nano. В случае с IOTA каждая транзакция должна подтвердить две предыдущие транзакции, и этот процесс подтверждения называется «выбором вершины». Это означает, что транзакции могут быть подтверждены и добавлены в сеть любым пользователем, и нет необходимости в майнинге или подтверждении.

Однако существуют некоторые потенциальные проблемы и ограничения систем на основе DAG. Одна из них заключается в том, что такие системы более уязвимы к атакам, таким как двойное расходование средств или рассылка спама, поскольку процесс проверки распределен между многими пользователями. Кроме того, структура DAG более сложная в реализации и обслуживании по сравнению с линейной блочной структурой.

В целом системы на основе DAG представляют собой многообещающую альтернативу традиционным блокчейнам и могут хорошо подойти для определенных целей, когда скорость и масштабируемость являются ключевыми требованиями. Однако они могут пригодиться не во всех случаях использования, и для полного раскрытия их потенциала необходимы дальнейшие исследования и разработки.