Проблема Византийских генералов в блокчейн-технологиях. Византийская отказоустойчивость. Основы алгоритмов консенсуса

Математика

Погорелов А.М.

10 класс, ГАУ КО ОО ШИЛИ, г. Калининград

Сегодня все легче и легче услышать слова криптовалюта, блокчейн, отказоустойчивость, однако далеко не каждый знает, что означают эти словосочетания и какие технологии за ними стоят. Предлагаю разобраться в смыслах этих слов поподробнее и понять, на чем основаны технологии сегодняшнего дня.

Для начала уточню, что далее речь пойдет о системах, посредством которых клиенты осуществляют взаимодействие друг с другом и совершают транзакции между участниками сети.

Криптовалюта - это электронное платежное средство без физического выражения формы[1]. **Блокчейн** — это распределенная база данных, которая содержит информацию обо всех транзакциях, проведенных участниками системы с помощью тех или иных криптовалют.[2] Большинство Блокчейн-сетей выступают в качестве децентрализованного цифрового регистра, который поддерживается благодаря распределенной сети компьютеров.

Такая технология позволяет создать надежную экономическую систему с неограниченными финансовыми операциями, которые могут осуществляться без необходимого участия сторонних посредников. Из-за того, что традиционные банковские и платежные системы зачастую основываются на доверии между клиентами и банками, криптовалюты сейчас выступают в качестве жизнеспособной альтернативы, в связи с тем, что они основаны на блокчейн и используются лишь в доверительных системах. Всем участникам необходимо регулярно согласовывать текущее состояние сети и это то, что мы называем достижением консенсуса (групповой процесс принятия решений)[3].

Тем не менее, достичь консенсуса в криптовалютных системах эффективным и безопасным способом далеко не простая задача. Дело в том, что сеть компьютерных узлов может согласиться даже с недостоверными данными, если некоторые из узлов сети нарушат условия и поведут себя нечестно. Этот фундаментальный вопрос тесно связан с **проблемой Византийских генералов**, решения которой вылились в концепцию **Византийской отказоустойчивости**.

Проблема Византийских генералов была разработана в 1982 году американскими учеными Лесли Лэмпортом, Робертом Шостаком и Маршаллом Пизом[4] как логическая дилемма, которая демонстрирует, как у группы византийских генералов могут возникнуть проблемы с коммуникацией при попытке принять решение и согласиться на следующий шаг. Логическая дилемма заключатся во взаимосвязи и достоверности сообщений, отправляемых между генералами.

Представим Византийскую империю, которая переживает не лучшие времена. Упадок в стране сопровождается атакующим внешним врагом, но не всё ещё потеряно. У Византии есть твердая опора – некоторое количество армий, которые находятся под руководством генералов. Если генералы примут решение атаковать неприятеля вместе – то Византия будет спасена (положительный исход); если генералы примут решение об отступлении – то армия будет спасена и начнёт готовиться к новым сражениям (промежуточный исход). Однако проигрышный вариант будет заключаться в том, что некоторые генералы пошли в атаку, а некоторые отступили. При таком раскладе вражеская армия постепенно уничтожит Византийские отряды один за другим. Условие задачи осложняется тем, что генералы могут контактировать друг с другом посредством сообщений, которые могут задерживаться или быть потерянными. Кроме того, даже если сообщение от одного военачальника будет успешно доставлено другому, имеется риск того, что один или несколько генералов по какой-либо причине могут поступить по

предательски и отправить ложное сообщение, дабы сбить с толку ничего не подразумевающих честных генералов, что приведёт к общему поражению.

Приведем пример. Есть **n** генералов. Связь между ними осуществляется посредством надежной связи (например, телефон). Из **n** генералов **m** являются предателями и пытаются воспрепятствовать соглашению между лояльными генералами. Согласие заключается в том, чтобы все лояльные генералы узнали о численности всех лояльных армий и пришли к одинаковым выводам (путь и ложным) относительно состояния предательских армий. (Последнее условие важно, если генералы на основании полученных данных планируют выработать стратегию и необходимо, чтобы все генералы выработали одинаковую стратегию)

Каждый лояльный генерал должен получить вектор длины **n**, где **i**-й элемент либо обязательно содержит численность **i**-ой армии (в том случае, если командир лоялен), либо содержит **произвольное число** в противном случае. Вектора должны быть полностью одинаковыми у всех лояльных генералов.

Шаг 1: Каждый из генералов посылает остальным сообщение, где указывает численность своей армии. Предатели могут указать различные числа в разных сообщениях, а лояльные указывают истинное количество. Генерал **g1** указал **1** (тысяча воинов), генерал **g2 - 2**, генерал **g3** соответственно указал трем остальным генералам **x, y, z**, генерал **g4 - 4**.

Шаг 2: Каждый из генералов вычисляет свой вектор из информации, полученной от остальных генералов. Получается: **vect1 (1,2,x,4)**, **vect2 (1,2,y,4)**, **vect3 (1,2,3,4)**, **vect4(1,2,z,4)**.

Шаг 3: Генералы посылают свои вектора другим. Генерал **g3** вновь посылает произвольные значения. Получаются следующие векторы:

g1	**g2**	**g3**	**b**
(1,2,y,4)	**(1,2,x,4)**	**(1,2,x,4)**	**(1,2,x,4)**
(a, b, c, d)	**(e, f, g, h)**	**(1, 2, y, 4)**	**(1, 2, y, 4)**
(1, 2, z, 4)	**(1, 2, z, 4)**	**(1, 2, z, 4)**	**(i, j, k, l)**

Шаг 4: Каждый из генералов проверяет каждый элемент в полученных векторах. В том случае, если одно значение совпадает как минимум в двух векторах, оно помещается в результирующий вектор, в противном случае, соответствующий элемент помечается как «неизвестен». В итоге все генералы получат **один вектор (1,2, неизвестен, 4)**. Следовательно, согласие достигнуто.

Для **n=3** и **m=1** согласие достигнуто не будет.[5]

Если мы применим данную технологию к блокчейн, то каждый генерал представляет собой сетевой узел и им необходимо достичь консенсуса в отношении текущего состояния системы. Это означает, что большинство участников распределенной сети должны согласовывать и выполнять одни и те же действия, чтобы избежать сбоя в работе.

Что такое Византийская отказоустойчивость? Византийская отказоустойчивость - это свойство системы, способное противостоять классу отказов, вытекающих из проблемы византийских генералов. Другими словами, византийская отказоустойчивая система способна продолжать свою работу, даже если некоторые из узлов вышли из строя или начали действовать злонамеренно. Византийская отказоустойчивость может быть достигнута, если корректно работающие узлы в сети договорятся о своих значениях. Для отсутствующих сообщений может быть задано значение голосования по умолчанию, т. е. мы можем предположить, что сообщение от определенного узла является «ошибочным», если сообщение не получено в течение определенного срока. Кроме того, мы также можем назначить ответ по умолчанию, если большинство узлов отвечают правильным значением.

Со временем были предприняты попытки найти решение проблемы, связанной с распределенной сетью (блокчейном). Были разработаны различные механизмы консенсуса (протоколы для достижения соглашения в распределенной системе), которые по своей сути решают византийскую проблему.

Алгоритм BFT(Практическая византийская отказоустойчивость), опубликованный в 1999 году математиками Мигелем Кастро и Барбарой

Лисков[6], стал первым решением проблемы византийской отказоустойчивости. Он описывает практический алгоритм согласования в блокчейн сетях, который допускает византийские ошибки. Алгоритм обеспечивает как живучесть (клиент, наконец, получает правильные ответы на свои запросы), так и безопасность при условии:

Не более ‘(n-1)/3’ узлов неисправны из ‘n’ узлов

Задержка ‘t’ растет не быстрее, чем до бесконечности.

Здесь задержка - это время между моментом, когда сообщение отправляется в первый раз, и моментом, когда оно получено адресатом (при условии, что отправитель продолжает повторную передачу сообщения до тех пор, пока оно не будет получено).

Если узлы ‘f’ являются византийскими сбоями, то системе необходимо иметь дело с двумя типами проблем. Во-первых, это вообще не отправка сообщения, а во-вторых, злонамеренная отправка другого сообщения. Таким образом, система должна хорошо функционировать после узлов ‘(n-f)’. Однако возможно, что узлы ‘f’, которые не ответили, не являются ошибочными, и, следовательно, узлы ‘f’, которые ответили, могут быть ошибочными. И так, если мы хотим, чтобы число исправных узлов превышало число неисправных, нам нужно как минимум ‘(n-f)-f > f’. Следовательно, ‘n > 3f+1’ является оптимальным.

Доказательство работы (Proof of Work или PoW) и Доказательство доли (Proof of Stake или PoS) – алгоритмы, используемые в настоящее время в современных системах блокчейна.

Биткойн имеет встроенный в свой протокол BFT и решает проблему византийских генералов, поскольку достигает соглашения большинства без какой-либо центральной власти, несмотря на присутствие неизвестных (потенциально ненадежных) сторон и, несмотря на то, что сеть не является мгновенной.

Как работает Биткойн в контексте проблемы византийских генералов?

Все генералы согласились с протоколом, в котором говорится, что для добавления сообщения об атаке необходимо решить сложную проблему. Криптографическая головоломка сложна для предлагающего генерала, но легка для рассмотрения другими генералами. Все генералы уже будут иметь необходимую структурную конфигурацию, которой должно обладать решение.

Теперь, на поле боя, предположим, что генерал разрабатывает план и хочет отправить сообщение другим, чтобы они атаковали в определенный день и время вместе с планом.

Шаги будут следующими:

Он добавит одноразовый номер к первоначальному плану.

Затем он будет хэшировать план (то есть вводить информацию любой длины и размера, например, в какое время начинать атаку, и какая численность вражеского войска), приложенный к одноразовому номеру, и увидит результат. Затем он продолжит добавлять одноразовый номер и проверять, получил ли он желаемый хэш. Другими словами, количество одноразовых номеров или решение сложной головоломки.

Затем он отправит гонцов к другим соответствующим генералам. Даже если посланников поймают, любая модификация их сообщения приведет к совершенно другому хэшу, который другие генералы могут легко идентифицировать.

Все остальные, наконец, проверяют план и действуют соответственно.

Византийская отказоустойчивость составляет 50% при условии нулевой задержки в сети. Составляет около 46% (криптовалюта Ethereum)[7] и 49,5% (криптовалюта Bitcoin)[7] отказоустойчивости при фактически наблюдаемых условиях, но снижается до 33%[7], если задержка в сети равна времени блокировки и уменьшается до нуля, когда задержка в сети приближается к бесконечности.

Решение может выйти из строя только в том случае, если злоумышленник захватит 50% мощности сети.

Мы можем определить алгоритм консенсуса, как механизм, с помощью которого блокчейн сеть достигает соглашения с другими участниками сети. Хотя Proof Of Work не безопасен на все сто процентов, доказано, что он является одним из наиболее безопасных алгоритмов для блокчейна и рассматривается многим как один из самых гениальных решений проблемы византийских генералов.

В то время как PoW, PBFT и POS, безусловно, являются наиболее популярными механизмами консенсуса, появляются и другие механизмы консенсуса, такие как Делегированное доказательство доли (DPOS), Доказательство прошедшего времени (POET) и Направленные ациклические графики (DAG), среди прочего, которые решают проблему BFT, хотя и с разной степенью успеха.

Обеспечение безопасности таких систем заключается в постоянных усилиях участников, а существующим алгоритмам консенсуса ещё предстоит преодолеть несколько барьеров, но потенциальные приложения, безусловно, вдохновляют широкое распространение данной инновации. За пределами блокчейн индустрии также существуют различные виды применения для отказоустойчивой системы, которая может использоваться в авиации, космической индустрии и в отрасли атомной энергетики.

Библиографические ссылки:

1) https://www.finam.ru/education/likbez/kriptovalyuta-kripta-chto-eto-takoe-i-kak-na-neiy-zarabotat-20190605-15210/
2) https://trends.rbc.ru/trends/industry/5f05c0a79a7947aac5c7577a
3) https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%81%D0%B5%D0%BD%D1%81%D1%83%D1%81
4) https://ruwiki.press/es/Tolerancia_a_faltas_bizantinas

5) Лекция 4. Задача о Византийских генералах и алгоритмы консенсуса.. — Текст : электронный // Инженерные классы блокчейн : [сайт]. — URL: https://vk.com/@rtublockchain-lekciya-4-zadacha-o-vizantiiskih-generalah-i-algoritmy-konse (дата обращения: 27.02.2022).
6) https://pmg.csail.mit.edu/papers/osdi99.pdf
7) https://www.hcltech.com/blogs/byzantine-fault-tolerance-bft-and-its-significance-blockchain-world