39 Протоколы консенсуса

39.1 Византийское соглашение

В наших протоколах Алиса и Боб часто прибегали к помощи доверенной стороны — Трента. Трент помогал наладить распределение секретных ключей, Трент выпускал сертификаты открытых ключей, Трент выступал в роли посредника (и гаранта) при взаимодействии по схеме «клиент — сервер — клиент». Возникает вопрос: могут ли Алиса, Боб, Карл, ... наладить безопасное взаимодействие друг с другом без Трента? Речь идет о построении так называемых *децентрализованных систем*. Частный вопрос: могут ли стороны добиться консенсуса по определенным вопросам без Трента или, другими словами, можно ли построить децентрализованный протокол консенсуса? Вопрос не является простым, поскольку предполагается наличие нечестных участников, причем их доля может быть довольно значительной.

Поставленный вопрос был формализован в 1982 году Л. Лэмпортом (Lamport), Р. Шостаком (Shostak) и М. Пизом (Pease) в форме задачи византийских генералов (Byzantine General Problem). Впоследствии проблематику децентрализованного консенсуса стали называть *византийской отказоустойчивостью* (Byzantine Fault Tolerance, BFT) или *византийским соглашением*.

В задаче византийских генералов имеется n сторон (генералов) $A, B, C, \ldots$, которые обмениваются сообщениями (приказами) друг с другом. Например, генерал A отсылает сообщение x_B генералу B, сообщение x_C генералу C и т.д. Обмен сообщениями выполняется по АКС, т. е. с гарантиями целостности и подлинности:

$$A \overset{\text{акс}}{\to} B\colon x_B, \quad A \overset{\text{акс}}{\to} C\colon x_C, \quad \ldots.$$

Для простоты, сообщение — это бит 0 или 1. Понятно, что с помощью достаточно большого числа сообщений-битов можно описать сколь угодно объемное сообщение.

Среди генералов имеется $n - t$ честных и t нечестных. Честный генерал рассылает другим генералам одни и те же сообщения:

$$x_B = x_C = \ldots.$$

Нечестный генерал действует без правил — его сообщения могут отличаться друг от друга.

Генералы обсуждают полученные сообщения, обмениваясь новыми сообщениями по некоторой схеме. Эта схема и определяет искомый протокол консенсуса. По результатам обсуждения каждый из генералов строит оценку сообщений других генералов. Например, генерал B принимает в качестве x_B сообщение y_B, генерал C принимает в качестве x_C сообщение y_C и т.д.

Протокол консенсуса обеспечивает византийское соглашение, если выполняются следующие условия:

1. Если A — честный отправитель и B — честный получатель, то $y_B = x_B$.
2. Если B и C — честные получатели сообщения A, то $y_B = y_C$.

Обратим внимание, что мы рассмотрели условия BFT в ракурсе «отправитель сообщения — получатели сообщения». В этом ракурсе отправителя будем продолжать называть генералом, а получателей назовем *лейтенантами*. Каждый из n генералов выступает в роли лейтенанта при обработке сообщений других генералов.

Первое условие BFT называется *исполнительностью*: честные лейтенанты должны исполнить приказ честного генерала.

Второе условие называется *согласованностью*: честные лейтенанты должны одинаково интерпретировать приказ генерала, даже если генерал нечестный.

Теорема 39.1. При $(n, t) = (3, 1)$ византийское соглашение невозможно.

Доказательство. Пусть A — генерал, B и C — лейтенанты. Генерал рассылает лейтенантам приказы x_B и x_C. Эти приказы лейтенанты транслируют друг другу на стадии обсуждения: B получает от C приказ x_{CB}, C получает от B приказ x_{BC}. Поскольку каждый из участников может быть нечестным, любое из равенств

$$x_B = x_C, \quad x_B = x_{BC}, \quad x_C = x_{CB}$$

может нарушаться.

Пусть B — честный и

$$x_B \neq x_{CB}.$$

Лейтенант B не знает, кто из его визави является нечестным. Если A — честный, то в силу исполнительности от должен принять решение в пользу x_B. Если C — честный, то в силу согласованности от должен принять решение в пользу x_{CB}. Одновременно удовлетворить условиям исполнительности и согласованности невозможно. □

Рассуждения, использованные в доказательстве теоремы, можно распространить на случаи $n = 3t$, $t = 2, 3, \ldots$, и доказать, что и здесь византийское соглашение невозможно.

Теорема 39.2. При $n \geqslant 3t + 1$ можно построить протокол византийского соглашения.

Доказательство. Доказательство будет конструктивным. Мы построим серию протоколов $P(\tau)$, $\tau = 0, 1, \ldots, t$, которые удовлетворяют требованиям BFT при условии, что число нечестных участников (в их качестве могут выступать и генерал, и лейтенанты) не превосходит τ.

Протокол $P(0)$ выполняется следующим образом:

1. Генерал рассылает приказ лейтенантам.
2. Каждый лейтенант безоговорочно принимает приказ генерала.

Поскольку нечестных участников нет, протокол обеспечивает и согласованность, и исполнительность.

Протокол $P(m)$, $m \geqslant 1$, выполняется следующим образом:

1. Генерал рассылает приказ лейтенантам.
2. Каждый лейтенант рассылает приказ генерала своим коллегам-лейтенантам, используя протокол $P(m-1)$ и выступая в нем в качестве генерала.
3. В результате выполнения предыдущих шагов каждый лейтенант будет располагать $n - 1$ приказом: один он получит напрямую от генерала, еще $n - 2$ будут согласованы в сеансах $P(m-1)$ с другими лейтенантами. В качестве итогового приказа (0 или 1) лейтенант принимает тот, который встречается не реже другого.

Исполнительность. Докажем, что если $n \geqslant 2k + m + 1$ и число нечестных участников $\leqslant k$, то $P(m)$ обеспечивает исполнительность.

Воспользуемся индукцией по m. При $m = 0$ исполнительность обеспечена. Пусть она обеспечена вплоть до $m - 1$. Рассмотрим протокол $P(m)$.

Честный лейтенант, получив приказ от честного генерала, рассылает его другим лейтенантам с помощью $P(m-1)$. Приказ получат $n-1 \geqslant 2k+m$ лейтенантов, среди которых не более k нечестных. По предположению индукции $P(m-1)$ обеспечивает исполнительность. Поэтому честные лейтенанты правильно передадут другим честным лейтенантам приказ генерала. В итоге каждый честный лейтенант будет располагать прямым *честным* приказом от честного генерала и не менее чем $k + m$ *честными* копиями этого приказа от других честных лейтенантов. Число *нечестных* копий не превосходит k. Поскольку

$$1 + k + m > k,$$

честные лейтенанты примут честный приказ и исполнительность обеспечена.

Согласованность. Снова воспользуемся индукцией по m. При $m = 0$ согласованность обеспечена. Пусть она обеспечена вплоть до $m - 1$. Рассмотрим протокол $P(m)$.

Если генерал честен, то согласованность следует из исполнительности (все приказы честного генерала одинаковы). Пусть генерал нечестен. Имеется не менее $3m$ лейтенантов, среди них не более $m-1$ нечестных. По предположению индукции протокол $P(m-1)$ обеспечивает согласованность, поэтому честные лейтенанты согласуют один и тот же приказ генерала. Но это означает, что $P(m)$ также обеспечивает согласованность.□

Протокол $P(m)$, описанный в доказательстве, обладает весьма высокой коммуникационной сложностью: сторонам требуется выполнить порядка n^{m+2} пересылок. Известны более совершенные протоколы византийского соглашения.