Решение «Задачи византийских генералов» с помощью принципов блокчейна Bitcoin

С.В. Вахрамов
Факультет информатики и робототехники
Уфимский государственный авиационный
технический университет
Уфа, Россия
e-mail: s@vakhramoff.ru

Аннотация[1]

В статье рассматриваются основы работы криптовалют и блокчейна, а также технологии, в которых встречается данная задача.

Рассмотрено тривиальное решение «Задачи византийских генералов» (задачи принятия решений), проведено сравнение с решением задачи с помощью методов, указанных в статье.

Приводится решение задачи с помощью методов технологии «блокчейн» криптовалюты Bitcoin.

1. Введение

В статье рассказывается о криптовалютах, технологии «блокчейн» и о задаче, которая для общего случая была впервые решена разработчиком криптовалюты Bitcoin – Satoshi Nakamoto (Сатоси Накамото). Основная суть при подтверждении операций и блоков в блокчейне – не доверять никому. Именно этот принцип помог решить задачу византийских генералов для общего случая.

Стоит отметить, что эта задача повлияла на развитие протокола TCP – Transmission Control Protocol (TCP, протокол управления передачей), а также используется, например, при синхронизации часов.

На самом деле, существует большое множество криптовалют (целые тысячи), и существует не один десяток алгоритмов для так называемого майнинга (нахождения) новых блоков.

При майнинге необходимо «вычислить текущий блок», проверить его на правильность соответствия условиям блокчейна, и, если всё верно, отправить блок соседним нодам (узлам), которые, в свою очередь, также проверят (подтвердят) блок и отправят дальше.

Труды Шестой всероссийской научной Конференции "Информационные технологии интеллектуальной поддержки принятия решений", 28-31 мая, Уфа-Ставрополь, Россия, 2018

В основе принятия решения о корректности полученного блока служит так называемая «Задача византийких генералов».

В рамках статьи введём следующие определения:

- Криптовалю́та — разновидность цифровой валюты, создание и контроль за которой базируются на криптографических методах. Как правило, учёт криптовалют децентрализирован. [1]

Для обеспечения неизменности базы цепочки блоков транзакций используются элементы криптографии (цифровая подпись на основе системы с открытым ключом, последовательное хеширование).

- Консе́нсус — процесс получения согласованного результата группой участников, основная проблема — наличие помех в среде передачи данных. В блокчейне помехой являются блоки от участников, которые пытаются нарушить целостность сети. [2]

Ключевой особенностью криптовалют является отсутствие какого-либо внутреннего или внешнего администратора, которому можно доверять. Именно поэтому необходимо выработать некий алгоритм консенсуса, с помощью которого участники сети будут подтверждать корректность найденного блока.

Стоит добавить, что даже если блок подтверждён (включая все транзакции, которые находятся в нём), это не гарантирует окончательного подтверждения его самого. Необходимо получить и также подтвердить следующие за текущим блоки в сети, чтобы считать его окончательно подтверждённым.

2. Формулировка задачи

Византия. Ночь перед великим сражением с противником. Византийская армия состоит из n легионов, каждым из которых командует свой генерал. Также у армии есть главнокомандующий, которому подчиняются генералы. В то же самое время, империя находится в упадке, и любой из генералов и даже главнокомандующий могут быть

предателями Византии, заинтересованными в её поражении.

Ночью каждый из генералов получает от предводителя приказ о варианте действий в 10 часов утра (время одинаковое для всех и известно заранее): «атаковать противника» или «отступать». [3]

Возможные исходы сражения:

•Если все верные генералы атакуют — Византия уничтожит противника (благоприятный исход).

•Если все верные генералы отступят — Византия сохранит свою армию (промежуточный исход).

•Если некоторые верные генералы атакуют, а некоторые отступят — противник уничтожит всю армию Византии (неблагоприятный исход).

Графически задача представлена на рисунке 1.

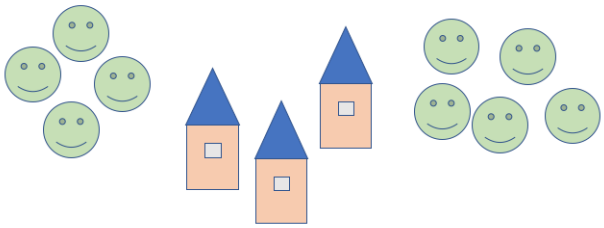

Рис 1. Иллюстрация к «задаче византийских генералов»

Также следует учитывать, что если главнокомандующий — предатель, то он может дать разным генералам противоположные приказы, чтобы обеспечить уничтожение армии. Следовательно, генералам лучше не доверять его приказам. Если же каждый генерал будет действовать полностью независимо от других (например, сделает случайный выбор), то вероятность благоприятного исхода весьма низка. Поэтому генералы нуждаются в обмене информацией между собой, чтобы прийти к единому решению.

3. Подтверждение блоков. Алгоритм Proof-of-Work (PoW).

В основе подтверждения блоков лежит так называемый алгоритм «подтверждения» работы – Proof of Work (суть алгоритма описана на рисунке 2). Разновидностей таких алгоритмов очень много, но сегодня мы поговорим именно об алгоритме «Доказательство работы».

Как уже было отмечено ранее, хоть и подтверждение блока происходит сразу, доверие к этому блоку появляется при появлении следующих подтверждённых блоков.

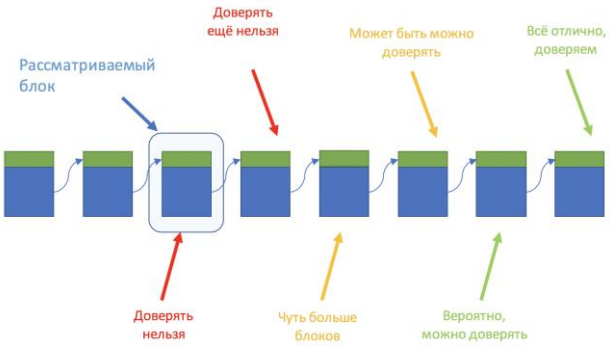

Рис 2. Подтверждение блока в сети

Из иллюстрации видно, что только что полученному подтверждённому блоку «доверять нельзя».

Появился 1 блок после текущего: всё равно «доверять текущему блоку ещё нельзя».

Появилось 2 блока после текущего: для подтверждения недостаточно, необходимо «чуть больше» блоков.

Появилось 3 блока после текущего: «может быть, можно довериться текущему блоку».

Получили 4 блока после текущего: «вероятно, всё отлично», почти можно доверять.

Получили 5 блоков после рассматриваемого: «всё отлично, можно уверенно доверять» информации, находящейся в текущем блоке.

4. Задача византийских генералов.

4.1. Тривиальное решение.

Стандартное решение задачи подразумевает отправку гонца с сообщением о необходимом действии (атака / отступление). В ответ другой генерал отправляет своего гонца, который подтверждает, что гонец с номером один доставил сообщение с таким-то содержанием (рисунок 3).

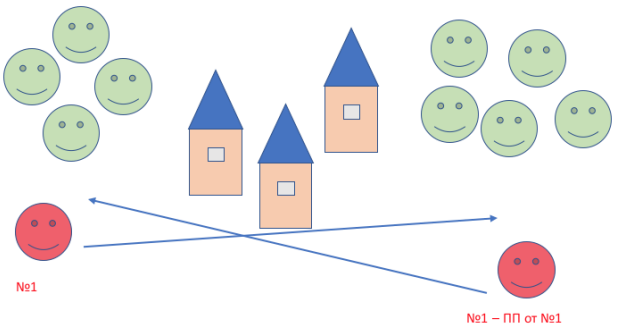

Рис 3. Иллюстрация отправки гонцов генералами

Возникают проблемы:

1. гонец может быть подменён или подговорён назвать другое сообщение, отличное от того, которое он в действительности должен передать;

2. гонца могут убить, и тогда информация до другого генерала и вовсе не дойдёт;

3. один генерал может не дождаться ответа и отправить нового гонца, с которым снова возможно несколько исходов (гонец доберётся и доставит верное сообщение, гонца или сообщение подменят, гонец не доберётся), при этом, генералу в ответ придётся снова отправить другого гонца и так далее…

В конечном итоге, для идеального решения задачи необходимо бесконечное число гонцов.

Возникает парадокс: если у нас есть бесконечное число гонцов, зачем отправлять их между генералами, если можно напасть на деревню и захватить её, ведь число воинов будет конечно, и они будут не в состоянии отбить бесконечное число гонцов.

4.2. Решение с помощью методов технологии «Блокчейн».

Решение в Bitcoin – хэширование информации в блоке вместе с дополнительным специальным словом (nonce).

Специальное слово, называемое nonce (целое число без знака), подбирается случайным образом, то есть простой догадкой, или как говорят – методом простого перебора. Обычно, начинают с «1» и ищут это число до того, пока не найдут верный вариант. Затем полученное сообщение вместе со специальным числом nonce хэшируется (вычисляется значение хэш-функции). Но при этом уславливаются, что, например, в начале полученного хэша должно стоять пять нулей.

Честно говоря, это является очень трудоёмкой задачей – нахождение хэша, который начинается на заданное количество нулей.

Допустим, в нашем случае мы посчитали это число, и оно оказалось равным 175390.

Описание результатов изображено на рисунке 4.

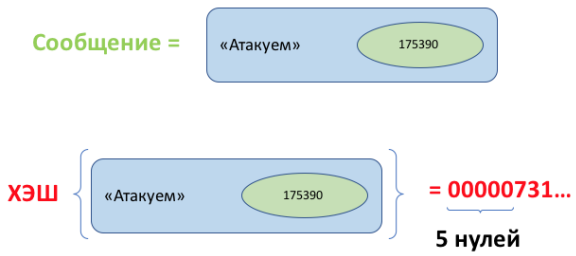

Рис 4. Хэширование сообщения со специальным словом (nonce)

Мы отправляем гонца с нашим сообщением и nonce (рисунок 5).

Даже если гонца перехватят и подменят сообщение – будет всё равно ясно, что сообщение не подлинное, так как при расчёте хэш-функции не будет получаться необходимых 5 нулей в начале её значения.

Если в деревне захотят подменить сообщение, им необходима вычислительная мощность, как у целого легиона, либо ещё большая, чтобы посчитать новое специальное слово в приемлемые сроки.

Если при получении сообщения и его хэшировании вместе со специальным словом nonce получатся необходимые 5 нулей в начале значения хэша, то, вероятно, сообщение является подлинным.

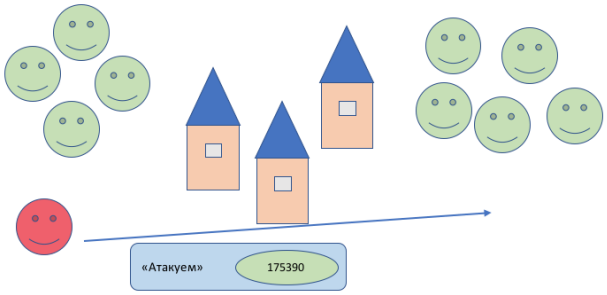

Рис 5. Отправка гонца с сообщением, содержащим в себе специальное слово (nonce)

Представим, что таких легионов с разных сторон очень много. От каждого легиона с помощью гонца посылается сообщение с необходимым действием. Причём, все гонцы несут не просто сообщение, а много сообщений, объединённых в блок (аналогия конверта с множеством писем внутри). И посылается не один гонец, а сразу три. При этом, между легионами тоже есть связь и они обмениваются между собой полученными блоками (конвертами с письмами). Ситуация описана на рисунке 6.

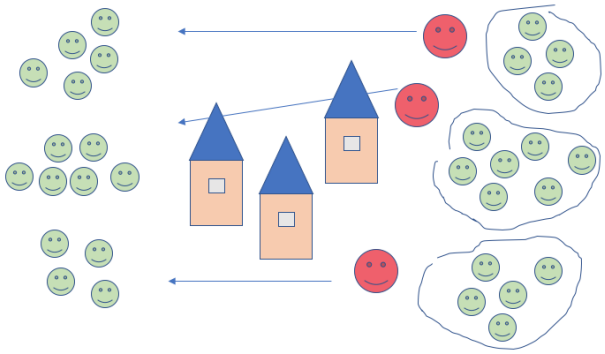

Рис 6. Обмен сообщениями между легионами с помощью принципов блокчейна Bitcoin

Специальное слово, называемое nonce, будет подобрано уже для целого блока. И, например, зададим условие, что для подтверждения операции нужно 9 нулей в начале хэша (рисунок 7).

Рис 7. Объединение сообщений в блок и его хэширование

Скорее всего, у того человека в деревне (да и у всей деревни в целом) не окажется такого количества мощностей, с помощью которых он мог бы подменить сообщения и посчитать новое специальное слово…

Теперь же, когда все получили блок, генералы видят два сообщения с текстом «Атакуем» и одно с текстом «Отступаем». По принципу «большинства» генералы решают, что армии атакуют.

5. Регулировка сложности

Количество тех самых нулей в начале хэша, говорящих о том, можно ли доверять текущему блоку, регулируется самим блокчейном в зависимости от количества вычислительной мощности сети (то есть, если блоки в сети находятся слишком быстро, – в блокчейне биткоина это 10 минут на один блок, – то сложность увеличивается, если же блоки находятся слишком медленно – сложность уменьшается, но не более, чем на 25% от начального значения – чтобы исключить вероятность того, что участники сети могли договориться и специально намеренно снизить мощность сети выключением части вычислительных мощностей).

Пересчёт сложности в блокчейне Bitcoin происходит каждые 2014 блоков.

5.1. Как взломать блокчейн?

Всё достаточно очевидно: нужно иметь строго больше 50% вычислительной мощности сети для того, чтобы иметь возможность вносить изменения в структуру блокчейна.

Стоит учесть, что если вы хотите изменить информацию в цепочке блоков, то это в крупных масштабах становится практически нереальной задачей, так как например:

если в сети находится миллион блоков, а вы хотите изменить первый блок, необходимо пересчитать сам 1-ый блок и остальные 999.999 блоков, плюс ещё те, которые остальная сеть будет присылать примерно в интервале 1 блок раз в 10 минут.

5.2. Джентльменское соглашение

В связи с ситуацией, описанной выше, в мире между всеми майнинг-пулами было достигнуто джентльменское соглашение. Пул – это специальный сервис, объединяющий нескольких майнеров (людей, решающих сложные вычислительные задачи для нахождения числа nonce) изнутри, но снаружи выглядящий как один майнер, но с колоссальным количеством вычислительных мощностей, на деле в котором решение задачи доказательства работы распределяется между очень большим количеством участников, что позволяет пулам быстрее находить решение блоков). Суть джентльменского соглашения в том, что если какой-либо пул концентрирует в себе даже чуть меньше, чем 50% мощностей, он обязан закрыть регистрацию и ввод новых мощностей. На деле, это может произойти и при концентрации уже 40-45% всех мощностей сети.

5.3. Удвоение цепочки блоков

В сети может возникнуть ситуация, когда появляются два правильных блока с одинаковым номером. Правила консенсуса сети гласят, что сеть должна выбрать блок с меньшим хэшем (так как считается, что нахождение меньшего хэша с заданными условиями требует больше работы над вычислениями).

Ситуация удвоения цепочки показана на рисунке 8.

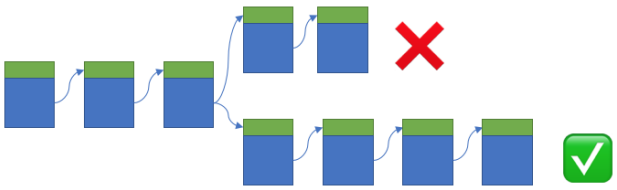

Рис 8. Удвоение цепочки. В дальнейшем сеть выбрала блок с меньшим хэшем и продолжила работу в обычном режиме.

6. Выводы

Таким образом, в статье было описано решение задачи византийских генералов для общего случая (когда число легионов и генералов может меняться). Проведено сравнение описанного метода с тривиальным решением. На данный момент другого способа решения этой задачи для общего случая не существует.

Список используемых источников

1. Википедия – свободная энциклопедия // Криптовалюта; URL: https://ru.wikipedia.org/wiki/Криптовалюта (дата обращения: 06.05.2018).
2. Википедия – свободная энциклопедия // Консенсус; URL:

https://ru.wikipedia.org/wiki/Консенсус (дата обращения: 07.05.2018).

3. Википедия – свободная энциклопедия // Задача византийских генералов; URL: https://ru.wikipedia.org/wiki/Задача_византийских_генералов (дата обращения: 10.05.2018).
4. YouTube – видео-хостинг // Bitcoin and Byzantine Generals; URL: https://www.youtube.com/watch?v=kE51N84hBxU (дата обращения: 14.03.2018).