Пояснение алгоритма работы консенсуса *sdbft*.

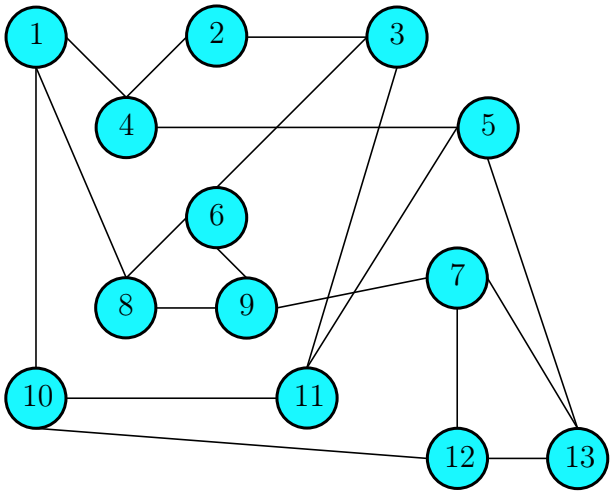
rr@sumus.team, a@sumus.team

26 августа 2019 г.

1.1.1 Пояснение алгоритма работы консенсуса *sdbft*

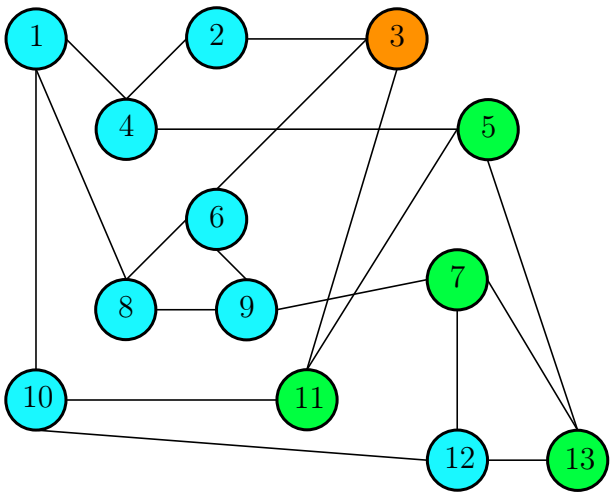
Данный раздел содержит упрощенное описание алгоритма консенсуса ***sdbft***.

1. Перед началом работы мы имеем пиринговую сеть с узлами, имеющими собственный сетевой адрес и уникальный номер, который знают все участники сети. Например, у нас будет 13 участников сети, пронумеруем все узлы номерами с 1 до 13. Так же мы договоримся, что в консенсус будет входить 5 узлов.



   Синим цветом будут обозначатся узлы, работающие в блокчейне. Зелёным цветом будут обозначаться узлы, участвующие в консенсусе. Мастер-узел будет помечаться оранжевым цветом. Узлы, находящиеся в нештатном режиме работы будут обозначаться красным цветом.

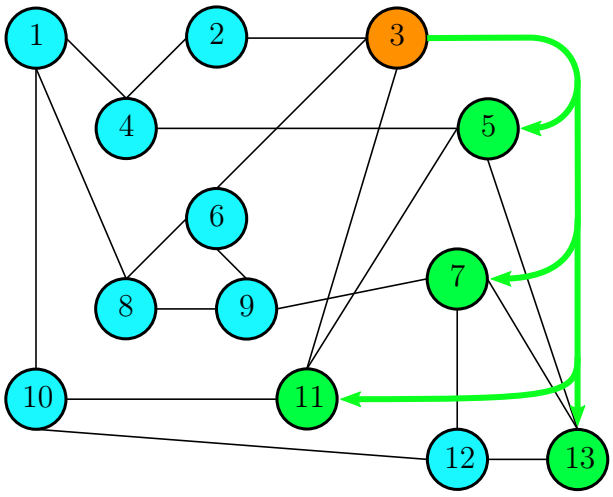
2. Начало работы консенсуса. Пусть все узлы пиринговой сети примут блок 1. В принятом блоке содержится информация, которая позволит функции f (см приложение А) создать случайную последовательность. Пусть эта последовательность будет следующей — №3,5,7,11,13. Пометим цветом узлы, имеющие №3,5,7,11,13.



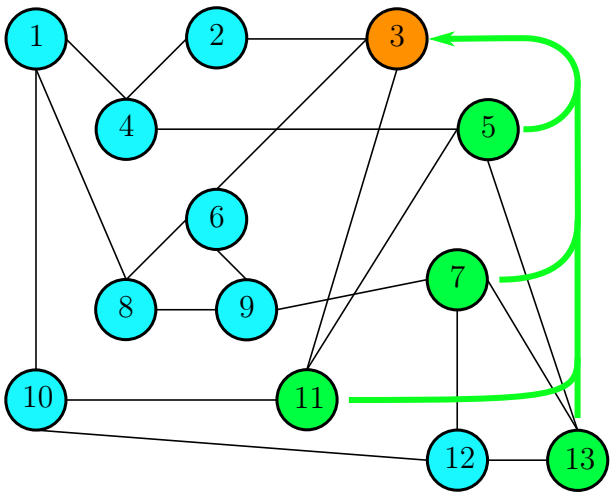
3. Как показано на рисунке выше узел №3 мы пометили оранжевым цветом, чтобы показать, что он является мастер-узлом. С этого момента узлы №3,5,7,11,13 участвуют в консенсусе.

4. Пусть узел №3 получил новую транзакцию от узла №2. Узел №3 проверяет, является ли транзакция корректной, если она признается корректной, то узел №3 пересылает ее узлам №5,7,11,13.

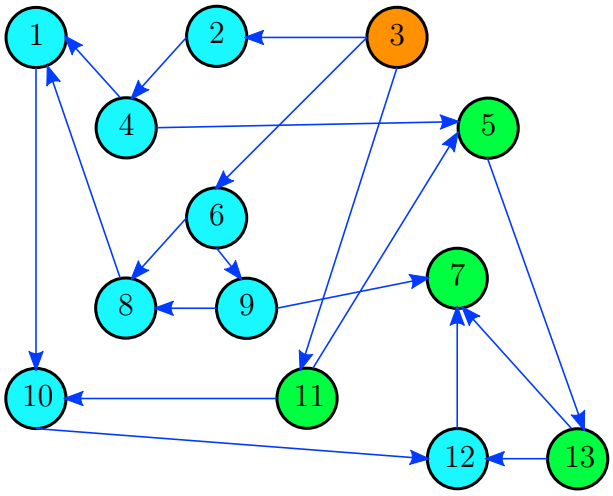
5. По завершению времени, отведённого на закрытие блока узел №3 пересылает узлам №5,7,11 и 13 сообщение о закрытии блока.



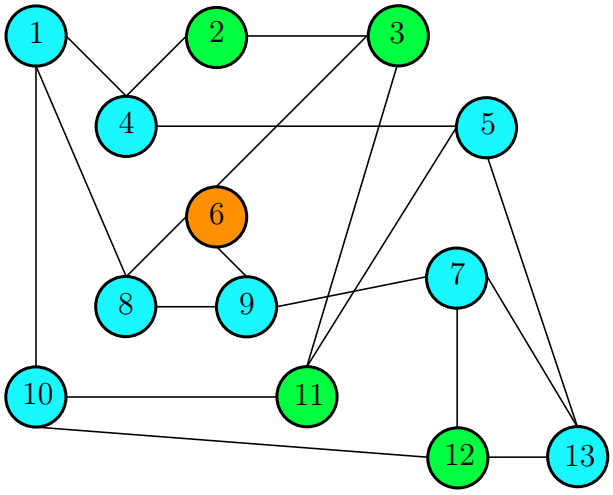
6. Узлы №5,7,11 и 13 пересылают хеш дерева Меркла, принятых ими транзакций, и свои подписи под хешем узлу №3.



7. Узел №3 считает подписи, если подписи корректны и их число удовлетворяет решению задачи византийских генералов, их не менее 3, то блок считается сформированным. Узел №3 рассылает анонс нового блока всем узлам сети.



8. Узлы принимают блок №2. Возвращаемся на второй шаг алгоритма, пусть теперь функция f (см приложение А) создаст случайную последовательность на основании принятых блоков, пусть будут номера 6,2,3,11,12.



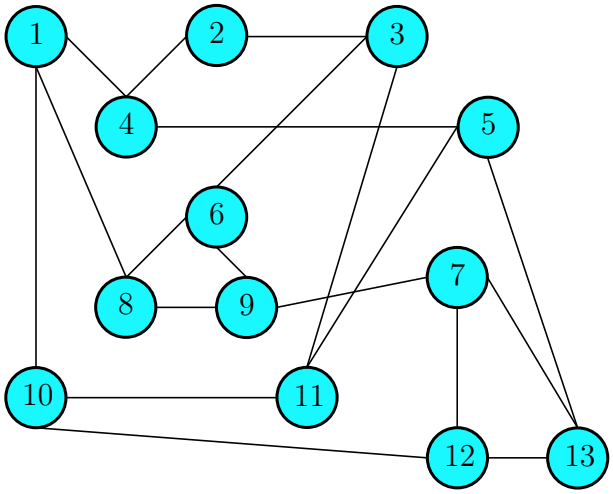
Далее процесс повторяется в соответствии с п.п. 3-8 алгоритма.

1.1.2 Обработка ошибочных ситуаций алгоритмом *sdbft*

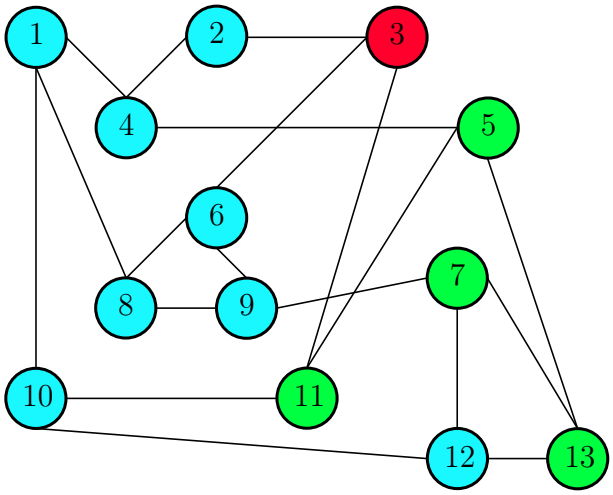
Мастер узел недоступен

1. Повторим п.п. алгоритма 1 и 2.

2. Перед началом работы мы имеем пиринговую сеть с узлами, имеющими собственный сетевой адрес и уникальный номер, который знают все участники сети. Например, у нас будет 13 участников сети, пронумеруем все узлы номерами с 1 до 13. Так же мы договоримся, что в консенсус будет входить 5 узлов.

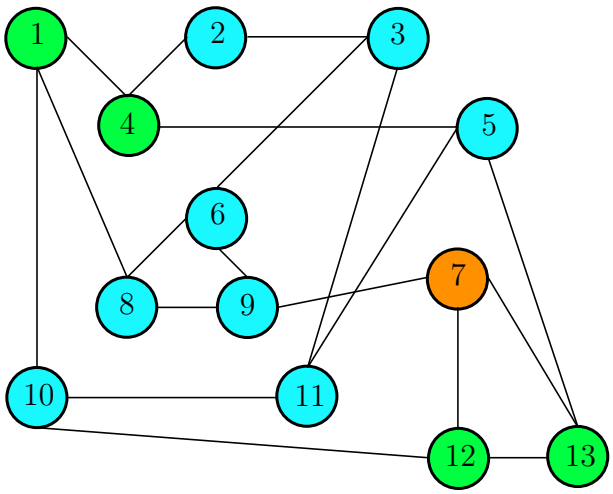


3. Начало работы консенсуса. Пусть все узлы пиринговой сети примут блок 1. В принятом блоке содержится информация, которая позволит функции f (см приложение А) создать случайную последовательность. Пусть эта последовательность будет следующей — №3,5,7,11,13. Узел №3 недоступен. Пометим цветом узлы сети.



4. Узлы эскорта не получат сообщения о закрытия блока, блокчейн сеть переходит на следующий раунд (см приложение А).

5. Возвращаемся на второй шаг алгоритма, пусть теперь функция f (см приложение А) создаст случайную последовательность на основании принятого блока и номера раунда, пусть будут номера 7,1,4,12,13. Сеть блокчейна будет выглядеть следующим образом.

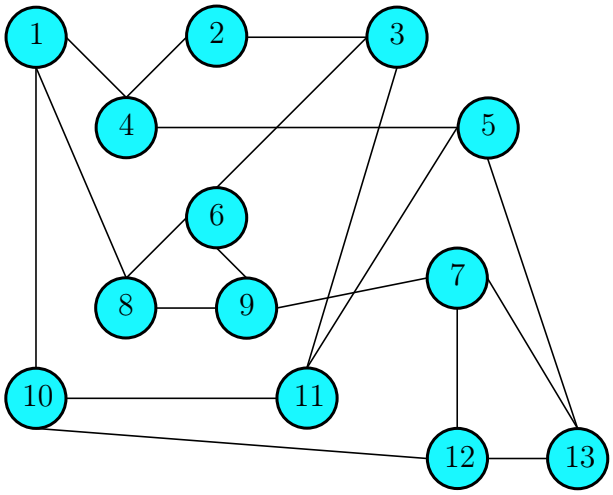


6. Далее алгоритм будет исполняться штатным образом в соответствии с п.п. 3-8.

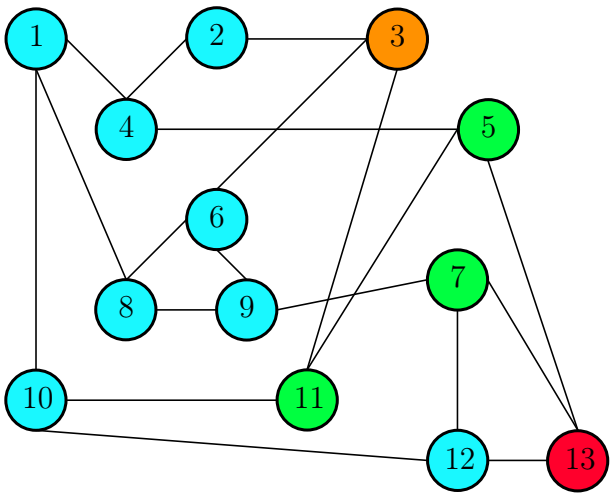
Эскорт узел недоступен

1. Повторим п.п. алгоритма 1 и 2.

2. Перед началом работы мы имеем пиринговую сеть с узлами, имеющими собственный сетевой адрес и уникальный номер, который знают все участники сети. Например, у нас будет 13 участников сети, пронумеруем все узлы номерами с 1 до 13. Так же мы договоримся, что в консенсус будет входить 5 узлов.



3. Начало работы консенсуса. Пусть все узлы пиринговой сети примут блок №1. В принятом блоке содержится информация, которая позволит функции f (см. приложение А) создать случайную последовательность. Пусть эта последовательность будет следующей — 3,5,7,11,13. Узел 13 недоступен. Пометим выбранные узлы цветом.



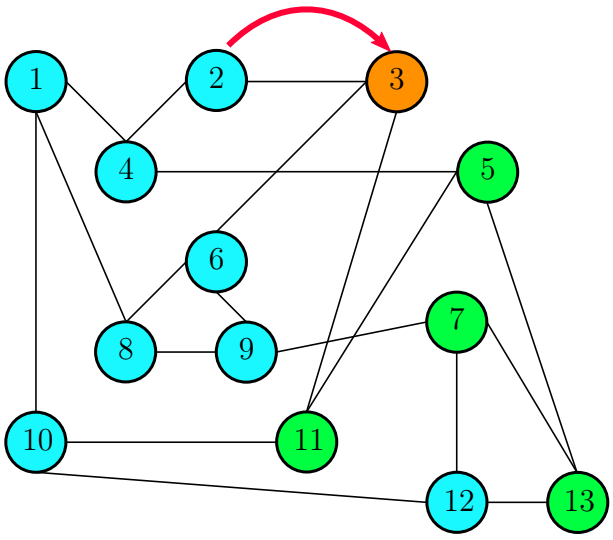
4. Узел эскорта №13 не получит сообщения о закрытия блока и не пошлёт свою подпись для закрытия блока. Если оставшиеся три узла пошлют корректные подписи транзакций формируемого блока, то блок будет сформирован. Узлы, участвующие в консенсусе будут перевыбраны.

5. Если оставшиеся три узла пошлют не корректные подписи транзакций формируемого блока, то блок не будет сформирован. Блокчейн перейдёт на следующий раунд. Узлы, участвующие в консенсусе будут перевыбраны.

Поступила некорректная транзакция

1. Пусть узел 3 получил новую транзакцию от узла №2. Узел №3 проверяет, транзакцию и признает ее некорректной.

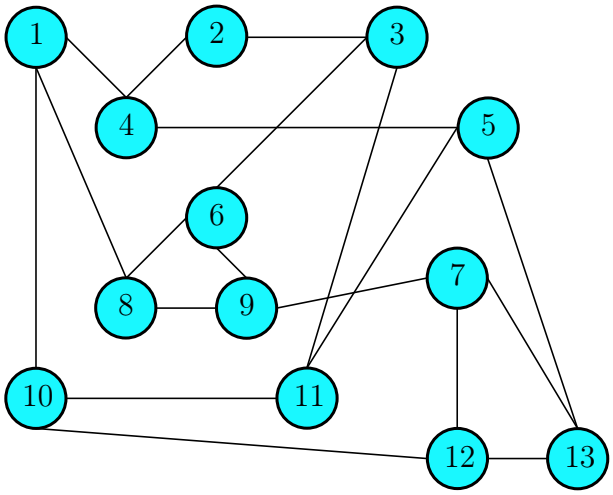
2. Если узел №3 признал транзакцию некорректной, то он ее отбрасывает, сообщение узлу №2 о некорректной транзакции не пересылается на узлы, входящие в консенсус.



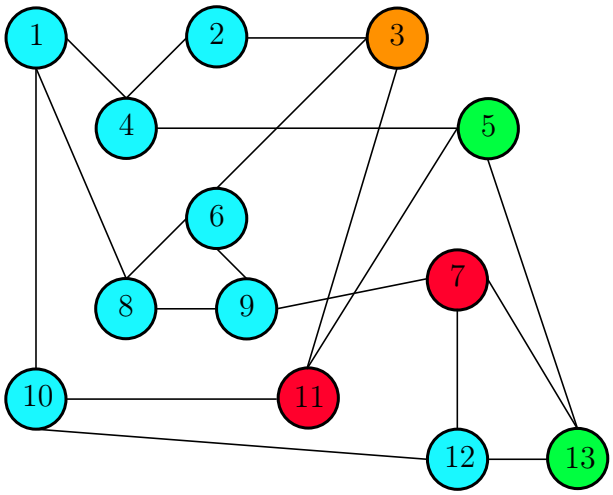
Количество блоков в блокчейне разное на разных узлах

Разное количество принятых блоков на разных узлах блокчейна может быть разным в случае, например, если сеть была сегментирована и не все узлы успели синхронизироваться. Повторим п.п. 1-5 алгоритма.

1. Перед началом работы мы имеем пиринговую сеть с узлами, имеющими собственный сетевой адрес и уникальный номер, который знают все участники сети. Например, у нас будет 13 участников сети, пронумеруем все узлы номерами с 1 до 13. Так же мы договоримся, что в консенсус будет входить 5 узлов.

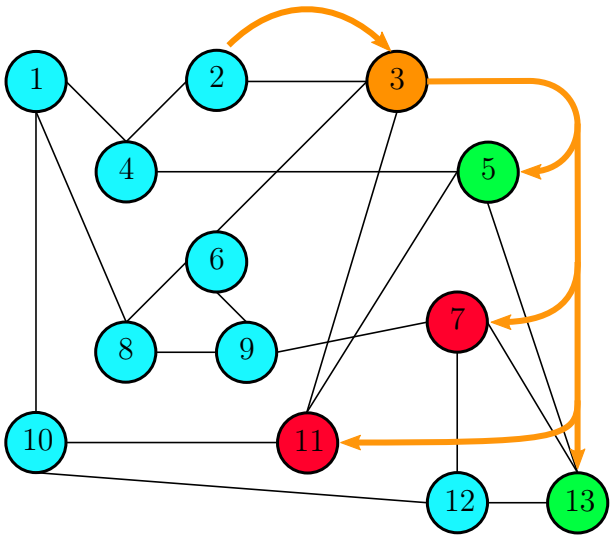


2. Начало работы консенсуса, пусть все узлы пиринговой сети примут блок 1.В принятом блоке содержится информация, которая позволит функции f (см приложение А) создать случайную последовательность. Пусть эта последовательность будет следующей — 3,5,7,11,13, узлы 7 и 11 имеют отличное число принятых блоков от узлов 3,5,13. Пометим выбранные узлы цветом.

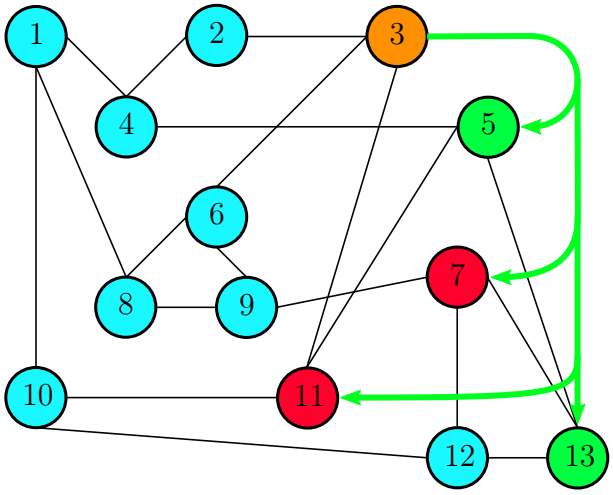


3. Как показано на рисунке узел №3 мы пометили оранжевым цветом, чтобы показать, что он является мастер-узлом. С этого момента узлы 3,5,13 участвуют в консенсусе.

4. Пусть узел 3 получил новую транзакцию от узла №2. Узел №3 проверяет, является ли транзакция корректной, если она признается корректной, то узел №3 пересылает ее узлам 5,7,11,13. Узлы 7 и 11 отвергают транзакцию.

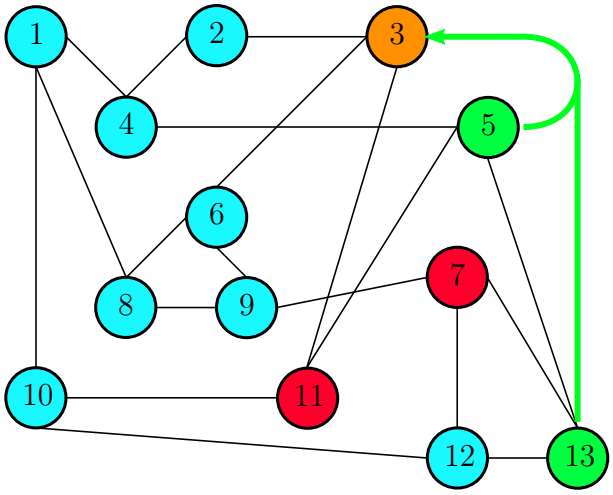


5. По завершению времени на закрытие блока узел №3 пересылает узлам №5,7,11,13 сообщение о закрытии блока, узлы 7 и 11 отвергают сообщение.



6. Узлы №5 и 13 пересылают хеш транзакций и свои подписи под хешем узлу №3.

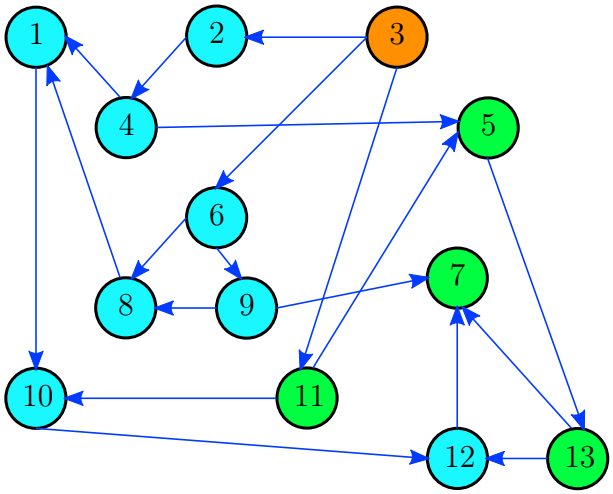
7. Узел №3 проверяет подписи узлов эскорта. Так как количество подписей узлов эскорта недостаточно для принятия блока, то блокчейн переходит на следующий раунд.



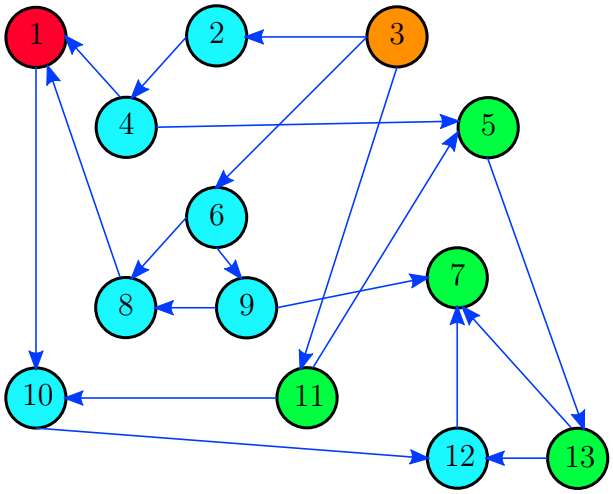
Узел отвергает новый блок блокчейна

Узел сети может отвергнуть новый блок блокчейна. Причин, по которым узел отвергает блок может быть несколько, например, на узле в следствии программного или аппаратного сбоя возникла ошибка чтения из базы данных и балансы кошельков изменились. Повторим п.7.

1. Узел №3 рассылает анонс нового блока всем узлам сети.



2. Пусть узел №1 отвергает блок.

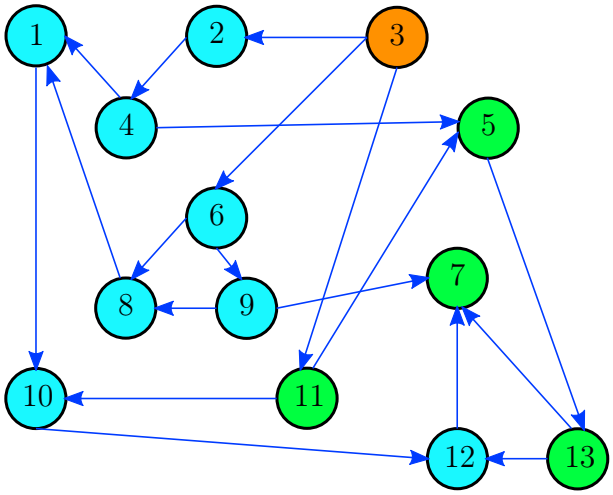


3. Узел №1 пытается найти в сети блок с отличной от признанного им ошибочным блока хеш-суммой, если узел не может найти удовлетворяющий его блок, то узел начинает процедуру пересинхронизации блокчейна см. п. 3.5.

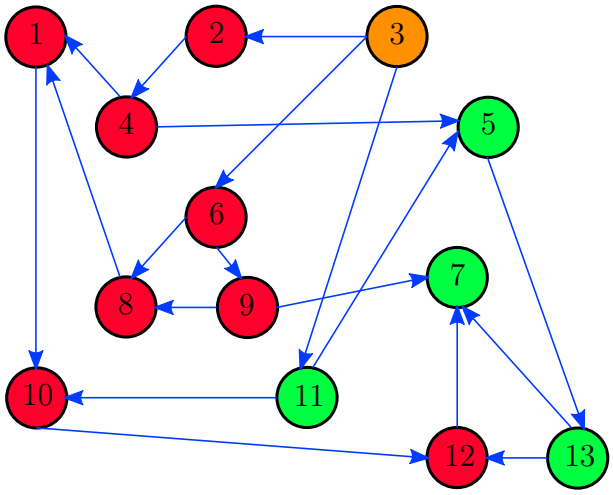
Сеть отвергает новый блок блокчейна

При создании нового блока теоретически может произойти сознательная попытка группы узлов навязать собственный, ошибочный, блок. Пусть узлы №3,5,7,11,13 пытаются навязать собственный, неправильный блок сети блокчейна Повторим п.7.

1. Узел №3 рассылает анонс нового блока всем узлам сети.



2. Все узлы сети отвергают новый блок.

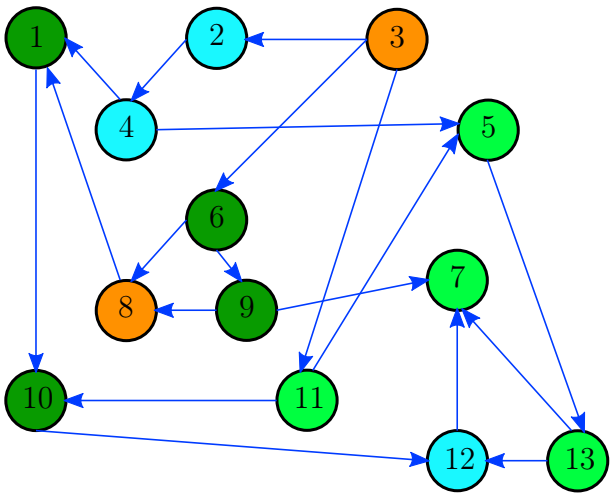


3. Блокчейн переходит на следующий раунд и далее пока не будет корректно сформирован следующий блок.

В сети появилось два блока с идентичными номерами

Два блока с идентичными номерами могут возникнуть в сети только, если будет сформировано два консенсуса из узлов с разными раундами, а это возможно если в сети возник глобальный сбой. Например, часть узлов находилась на серверах которые были одновременно перезагружены. В таком случае будет происходить следующее.

1. Предположим, что сформировалось два набора узлов для создания консенсуса - 3,5,7,11,13 и 8,9,6,1,10. Узел №3 и №8 рассылают анонс нового блока всем узлам сети.



2. Узел при принятии нового блока проверяет входит ли раунд создания блока в доверительный интервал раундов или нет. Т.е. насколько сильно раунд нового блока отличается от собственного раунда узла. Если раунд признается узлом корректным, то блок принимается. Если признается не корректным, то блок отвергается. Далее, возможно два пути развития ситуации:

   a. Раунды сформированных блоков находятся в доверительном интервале, в таком случае узлом будет принят блок, пришедший первым. Вероятность попадания в блокчейн блока будет зависеть от того какой блок был принят большинством узлов сети.

   b. Раунд одного из сформированных блоков не находится в доверительном интервале у большинства улов сети. Следовательно, большинством узлов будет принят блок с номером раунда из доверительного интервала.