AUREUS

Fast, free transaction and secure stable coin

26 августа 2019 г.

Tech Paper v.0.2

Aureus Securities AG
Short version: www.swissaureus.com

1 Введение

...почему и зачем мы создаем блокчейн Aureus Securities AG ... Существующие сегодняшние цифровые валюты также не решают эти проблемы:

- BTC децентрализованный, но слишком волатильный, медленный и стоимость транзакции постоянно растёт;
- Market Pegged Asset в BitShares привязаны к залогу в криптовалюте BTS, которая еще более нестабильна, чем BTC.

В сети со временем будут выпущены следующие базовые инструменты (USD, EUR, CNY и т.п.) ...:

Обладание токеном AUG даст ...

Поэтому мы создали пространство со следующим набором свойств

- Средства расчёта со стабильной ценой, привязанные к XDR.
- Прозрачная эмиссия на основе open source, реализованного в коде алгоритма, имеющего математически строгое доказательство.
- Бесплатные транзакции.
- Быстрые транзакции, проходящие в течение одной минуты.
- Децентрализация, основанная на 10 000 узлов по всему миру, принадлежащих различным людям и организациям.

Этот инструмент позволит людям:

- быть уверенным в сохранности своих ценностей;
- свободно, быстро, надёжно и без комиссий переносить ценность в любую точку мира.

2 Описание платформы

Финансовая платформа Aureus Securities AG создана на технологиях блокчейн-конструктора Gaus[1]. Проектно-зависимая часть блокчейна была разработана совместно со специалистами Gaus.

[1] Описание всех возможностей блокчейн-конструктора Gaus не является целью данного документа.

Основные возможности блокчейн-сети Aureus Securities AG:

- Используется алгоритм консенсуса sdBFT[2];
- Количество узлов участвующих в формировании блока - 5;
- Блок в блокчейне формируется каждые 20 секунд;
- Количество узлов в сети на начало старта 50;
- Выполнение привилегированных операций в сети осуществляется через multisign кошельки уполномоченными лицами;
- Через привилегированные операции производится добавление/исключение узлов из блокчейн-сети, регистрация новых токенов, дополнительная эмиссия токенов;
- Multisign кошельки для пользователей блокчейна;
- Автоматическое усечение блокчейна (на семилетнем интервале);
- Скоростные характеристики блокчейна: включение в блок транзакций до 10 000 в секунду (при обеспечении надлежащих каналов вязи и достаточной производительности узлов блокчейн сети).

3 Алгоритм эмиссии

В платформе Aureus Securities AG создаются токены, которые используются для расчётов. Основной токен системы AUS равен по стоимости 1 USD. Эмиссия токенов осуществляется с помощью специальной multisign транзакцией, которая должна быть последовательно подписана уполномоченными лицами (кошельками имеющими специальный тэг Owner). Для того, чтобы блокчейн осуществил эмиссию должна быть выпущена и подписана транзакция 'multi sign register token transaction' как минимум тремя уполномоченными лицами. Уполномоченными лицами являются штатные сотрудники Aureus Securities AG. Характеристики эмиссии:

- Создаваемый токен имеет трёх буквенное обозначение и десятичный код.
- Каждая дополнительная эмиссия эмитируется по прозрачному алгоритму.
- Количество разрядов целой части: 11.
- Количество разрядов после запятой: 2.

При запуске блокчейн-сети, в генезис блоке блокчейна не определены токены и их количество. Первичная эмиссия это создание токена AUS в количестве 1.

3.1 Reflection point

- Благодаря нулевой комиссии за пересылку токенов, система позволяет совершать микротранзакции, поэтому для обеспечения длительного функционирования блокчейна вводится процедура его периодического усечения.
- При достижении размера блокчейна в 4 Tb включается алгоритм усечения: система условно удаляет из рабочей части блокчейна все нулевые (пустые) кошельки и все кошельки, имеющие баланс менее 1 токена. Состояние блокчейна после очистки будет записано в новый Genesis Block. Предыдущее состояние блокчейна будет сохранено только на специализированных (архивных) узлах.

[2]Алгоритм семейства POS блокчейнов

4 Бесплатные быстрые транзакции

Транзакции в сети Aureus Securities AG бесплатны, блок закрывается за 20 секунд, проектная пропускная способность - до 10 000 транзакций в секунду. Оптимизация блокчейна происходит за счет того, что мы не храним информацию о входе-выходе (в отличие от UTXO-модели в BTC-подобных системах).

Бесплатность транзакций для пользователей возможна благодаря механизму минтинга (см. раздел "Эмиссия нодами при закрытии блока (minting)“) и функции Reflection point.

5 Блокчейн

5.1 Обоснование выбора

Цели применения блокчейна Aureus Securities AG потребовали консенсуса, отвечающего следующим характеристикам блокчейна.

1. Время создания нового блока 20 секунд.
2. Общее количество узлов, которые могут принять участие в выработке консенсуса, может меняться от 10^3 до 10^4.
3. Высокая скорость транзакций – не менее 10^3 транзакций в секунду.
4. Реализация алгоритма блокчейна не должна требовать существенных вычислительных, по сравнению с блокчейнами PoW, мощностей.

Выбор пал на алгоритм sdBFT, который обладает более высоким быстродействием по сравнению с BFT алгоритмами. Потенциально большое число участников консенсуса усложняет предварительный сговор, когда группа голосующих узлов формирует новый блок, управляя составом блока по своему усмотрению, так как при следующем установлении консенсуса будет выбрано другое множество голосующих узлов. Псевдослучайный выбор множества голосующих узлов не позволит оказать существенного влияния на выбор узлов при следующем голосовании. С описанием алгоритма можно ознакомиться в статье Article concensus sdBFT.

5.2 Алгоритм формирования нового блока

- Пусть в некий момент времени пользователь формирует транзакцию I.
- Транзакция передается ближайшей ноде, с которой связан данный клиент.
- Нода может находиться в одном из трёх состояний: пассивная, эскорт или мастер.
- Если нода пассивная, она проверяет транзакцию и передает ее далее по пиринговой сети, пока транзакция не дойдёт до эскорт-ноды.
- Эскорт-нода пересылает транзакцию мастер-ноде.
- Мастер-нода проверяет транзакцию и, если транзакция корректная, пересылает ее эскорт-нодам, а также записывает транзакцию I в формируемый блок.
- Эскорт-ноды, приняв транзакцию I, проверяют ее на корректность и записывают ее в формируемый блок.
- Данная последовательность действий повторяется до момента завершения блока, не более 20 секунд.
- После этого мастер-нода рассылает сообщение о завершении блока.
- Каждая эскорт-нода рассчитывает хеш блока транзакций, электронную подпись хеша и пересылает полученный хеш мастер-ноде.

- Мастер-нода рассчитывает количество корректных, по ее мнению, электронных подписей. Если полученное число корректных подписей превышает 2/3 от общего значения эскорт-нод, участвующих в консенсусе, блок считается сформированным. Иначе блок не формируется.
- Блокчейн находится вне времени, не проверяет и не согласовывает время транзакций, помещаемых в блок.
- Системы, работающие поверх блокчейна, будут ориентироваться на некое усредненное время закрытия блоков (около 20 секунд).

5.3 Генератор псевдослучайных чисел

Стандартные генераторы псевдослучайных чисел, встроенные в операционные системы, как правило, имеют ряд существенных уязвимостей, наиболее опасные из которых:

- В качестве seed для создания псевдослучайного числа используется timestamp. В итоге, если злоумышленник знает алгоритм генерации псевдослучайного числа и примерное время его генерации, то он может с высокой вероятностью методом перебора подобрать приватный ключ (пароль), сгенерированный таким алгоритмом.
- Даже если помимо timestamp используются иные данные, стандартные генераторы псевдослучайных чисел генерируют довольно предсказуемые последовательности, что предоставляет злоумышленниками возможность подбора паролей (хешей) методом перебора.

5.3.1 Криптография

- ECSDA Digital Signature algorithm (используется в BTC);
- Ed25519 scheme (быстрее , чем используемая BTC);
- SHA-3 алгоритм хэширования (быстрее и надежнее, чем в BTC);
- программный генератор случайных чисел, основан на двойном вычислении хеш функции с динамическим изменением начального состояния. Качество случайной последовательности, вырабатываемой генератором псевдослучайной последовательности, не хуже $0.5 + D$ на бинарный знак при $|D| < 0.01$, что удовлетворяет гипотезе о равномерном распределении анализируемой последовательности случайных чисел.

5.3.2 Общие свойства блокчейна

- Поддержка микротранзакций (“заплатить за кофе”) благодаря нулевой комиссии.
- Максимальная сумма транзакции не ограничена.
- Блокчейн периодически производит само-оптимизацию и поддерживает свой размер в заданных границах.
- Кошельки с мусорным балансом обнуляются, а их содержимое поступает нодам, участвовавшим в усечении блокчейна.

5.3.3 Типы транзакций

- Поддержка микротранзакций (“заплатить за кофе”) благодаря нулевой комиссии.
- Отправка XDR.
- Отправка Aureus Securities AG.
- Анонс на регистрацию ноды.
- Анонс об исключении ноды.

- Новый genesis block (усечение).
- Публикация курса Aureus Securities AG/XDR.
- Подача вопроса на голосование нодами.
- Голосование нодой.
- Эмиссия/обратная эмиссия XDR эмиссионным центром.

5.3.4 Управляющие параметры

- Интервал в блоках, через который запускается процедура усечения блокчейна.
- Интервал в блоках, через который повторяется процедура усечения, если предыдущая завершилась неудачно.
- Диапазон депозита, позволяющий создавать ноду.
- Предельное количество нод.
- Обновление управляющих параметров происходит посредством голосования нод.

5.3.5 Кошельки

- Адрес кошелька - последовательность символов в кодировке Base58checkerMod2, которая записывается в транзакции, размещаемой в блокчейне.
- На кошелек можно получать и принимать и XDR, и Aureus Securities AG.
- Типы кошельков:
  - Легкий:
    - Для расчетов (транзакций) и проверки баланса.
    - Использует специальный протокол, который позволяет получать необходимые блоки и проверять при этом только дерево Меркла, а не весь блокчейн.
  - Стандартный:
    - Хранит весь блокчейн.
    - Может быть зарегистрирован как нода.
  - Multisig:
    - Виртуальный кошелек, транзакцию с которого система принимает только при нескольких подписях.
  - Point wallet:
    - Кошелек разработчика, через который производится точечное управление системой за счет изменения управляющих параметров.
    - Нужен только на первый год работы блокчейна, затем будет отключён, и это будет прописано в блокчейне.
  - System wallet:
    - Кошелек для накопления комиссий с удаляемых кошельков при усечении блокчейна.
    - С него может быть сформирована исходящая транзакция только для оплаты комиссий нодам,участвовавших в усечении блокчейна.

6 Практическое применение

6.1 Свободные международные платежи

Рынок криптовалюты во многом вырос благодаря спросу на свободные быстрые и недорогие международные платежи. Особенно это касается Китая, где хождение валют сильно ограничено государством.

По итогам анализа участников конференции Money 2020 в Сингапуре, ни одна платежная система не позволяет проводить трансграничные сделки размером более 5 000 USD. Единственный инструмент для перевода более 5 000 - 10 000 USD между государствами — SWIFT. Но для осуществления перевода потребуется заполнить множество документов, дождаться проверки документов банком, обсудить перевод с менеджером валютного контроля и затем ждать несколько часов для совершения перевода. Стоимость SWIFT составляет порядка 1%.

Aureus Securities AG позволяет бесплатно переводить любые суммы в любую точку мира за несколько секунд без общения с менеджерами банков.

6.2 Независимое хранение

Хранить наличные в квартире или доме — опасно. В контрактах с банками на хранение имущества в сейфовой ячейке есть пункт о том, что банк не несет ответственности за сохранность содержимого ячейки. В результате из банковских ячеек регулярно пропадают крупные суммы денег. Статистика закрытия банков приведена во “Введении”. Aureus Securities AG позволяет надежно хранить деньги в децентрализованной сети, с нулевым риском центрального контрагента, без блокировок счетов.

6.3 Международная кооперативная экономика

Один из важнейших аспектов обеспечения ценности Aureus Securities AG — реальный оборот товаров и услуг. Авторы Aureus Securities AG видят наибольший потенциал распространения Aureus Securities AG в кооперативной экономике, особенно в развивающихся странах с нестабильной финансовой системой. Именно на этих рынках есть заметный дефицит фиатных денег, а также предрасположенность к бартерным сделкам и иным способам взаимозачетов.

Большинство развитых стран практически остановили экономический рост и наибольший вклад в развитие мировой экономики теперь вносят развивающиеся страны. То же самое относится и к бизнесу: крупные корпорации, за исключением некоторых финансовых холдингов, имеют рентабельность ниже 5 %. А в кризисные годы даже богатые финансовые компании показывают огромные убытки.

При этом **кооперативы исторически растут против рынка, особенно в кризисное время**. Например:

- Rabobank показал рост на 42 % в 2008, а его члены-учредители получили 20 %-ое увеличение депозитов. За 2008-09 годы уровень членства в кредитных союзах значительно вырос.
- Каждый 3-ий канадец является членом системы кредитных союзов, а доля кредитных союзов на розничных рынках депозитов и жилищной ипотеки выросла с 16 % до 19 % в 2010 году

[Moody's investors service global banking report, april 2010].

- С первого квартала 2012 кооператив Desjardins занимает 16-ое место из 7500 депозитарных финансовых учреждений в Северной Америке и 2-ое место по показателю капитала первого порядка, который составляет 16.8 %.

Объем кооперативной экономики огромный, кооперативы распространены и в богатых, и в развивающихся странах:

- Кооперативы насчитывают 1 миллиард пайщиков по всему миру.
- В Индии потребности 67 % сельского населения в товарах обеспечиваются кооперативами.
- 40 % африканских домовладельцев входят в кооперативы.
- Доход 1500 крупнейших кооперативных организаций в 2010 году составил почти 2 триллиона долларов.
- Development International Desjardins (DID) является лидером в микрофинансах: работает с 8.8 миллионами членов и клиентов по всему миру и обладает ссудным капиталом в 2.5 миллиарда канадских долларов.
- В некоторых африканских странах Desjardins занимает 35 % микрофинансового рынка.
- В Китае кооперативы обеспечивают 91 % рынка микрокредитов.
- Кредитные кооперативы обеспечивают миллиарды долларов доступных денежные переводов от трудовых мигрантов, работающих в развитых странах, их семьям в развивающихся странах, что особенно важно для Латинской Америки и Африки.

Кооперативная экономика работает эффективнее, потому что:

- Работа кооператива нацелена на заработок для всех пайщиков, а не на раздувание биржевой капитализации.
- Все пайщики вовлечены, не надо тратить деньги и время на мотивацию.
- В корпорациях топ-менеджмент зарабатывает в 100 раз больше рядовых сотрудников, а в кооперативах — всего в 10 раз, т.е. издержки на поддержание структуры на порядок ниже.
- За счет внутреннего контура экономики и взаимозачетов между участниками кооператива можно сократить издержки на налоги, транзакции и посредников, а также уменьшить потребность в фиатных кредитах.
- В итоге цена товаров и услуг внутри кооперативов получается на 40 % ниже, чем на внешнем рынке. Это создает стимул для привлечения капитала и людей извне, а также мотивацию для долгосрочного участия в кооперативе.

Инструменты, которые создаются для кооперативов на базе Aureus Securities AG:

- бухгалтерия взаимозачетов,
- депозитарий для хранения расписок и балансов,
- привлечение финансирования извне,
- подготовка отчетности в налоговые органы,
- юридические шаблоны для оформления работы с токенами,
- маркетплэйс товаров и услуг с большими скидками.

7 Мотивация участников экосистемы

Пользователи:

- Получают возможность совершать быстрые бесплатные транзакции или длительно хранить ценность, оставаясь в крипто-пространстве.

Инвесторы:

- Заинтересованы в возврате инвестиций.
- Возврат может происходить через поддержку системы - любой участник может стать нодой блокчейна и/или эмиссионным центром.

Эмиссионные центры:

- Заинтересованы в росте курса Aureus Securities AG, так как это будет увеличивать их капитал и регулярный доход.

Владельцы нод:

- Заинтересованы в получении комиссии за подписание блоков в блокчейне.
- Диапазон дохода владельца ноды - 8-13 % годовых в XDR.

8 Юридическая оболочка

Первичная продажа

Первый раунд первичной продажи будет непубличным, закрытым, с KYC и подписанием контрактов между командой разработки и первыми владельцами токенов. Все публичные сделки будут заключаться строго на вторичном рынке и поэтому не потребуют регуляции.

Повседневное использование

В случае, если этого не требуют местные законы, либо объемы сделок малы, либо регулярность сделок отсутствует, использование Aureus Securities AG можно никак не оформлять юридически.

В остальных случаях, особенно при активном проведении сделок в больших объемах, рекомендуется создавать локальные кооперативы или потребительские общества, либо вступать в существующие.

Главный инструмент в кооперативе — это пай. Паевой взнос — имущественный взнос пайщика в паевой фонд потребительского общества деньгами, ценными бумагами, земельным участком или земельной долей, другим имуществом либо имущественными или иными правами, имеющими денежную оценку. Возврат паевого взноса налогом не облагается независимо от суммы или цены товара, полученного пайщиком.

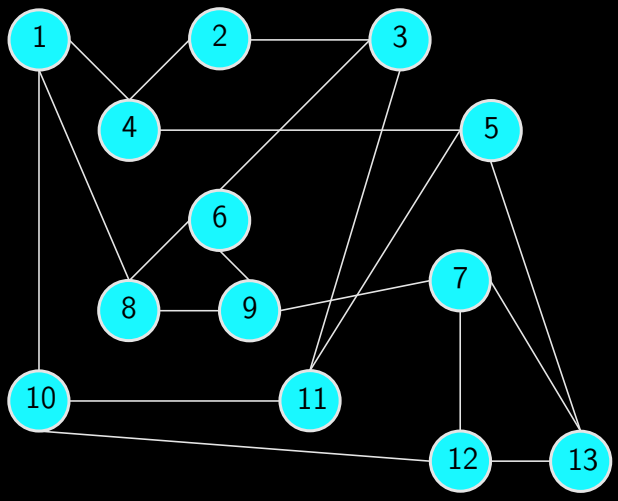
Любой обмен паев внутри кооператива возможен и не облагается налогами, т.е. юридически Aureus Securities AG может быть использован как инструмент для оценки стоимости паев.

Для внешних людей, которые не являются участниками кооператива, можно оформить работу с Aureus Securities AG в виде программы лояльности:

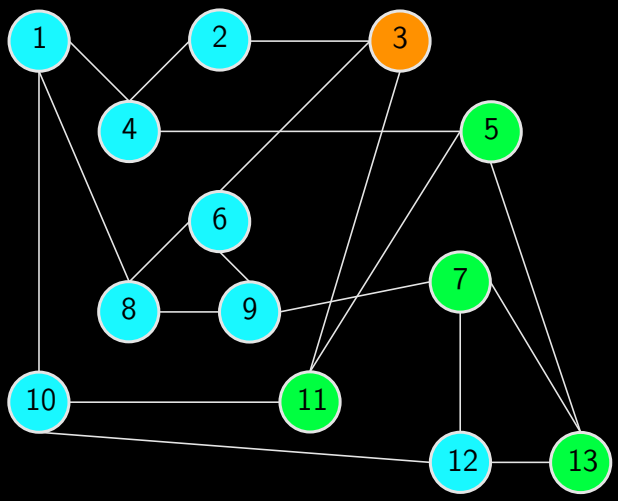
- Токен — право требования бонусного балла. Это право можно продать юридическому лицу и физическому лицу, также учесть в бухгалтерии.
- В момент обмена токена на товар/услугу владелец токена реализует право требования бонусных баллов, получает баллы, а за них получает товар.
- По такой схеме работают бонусные баллы супермаркетов или бонусные мили авиакомпаний.

9 Пояснение алгоритма работы консенсуса *sdbft*

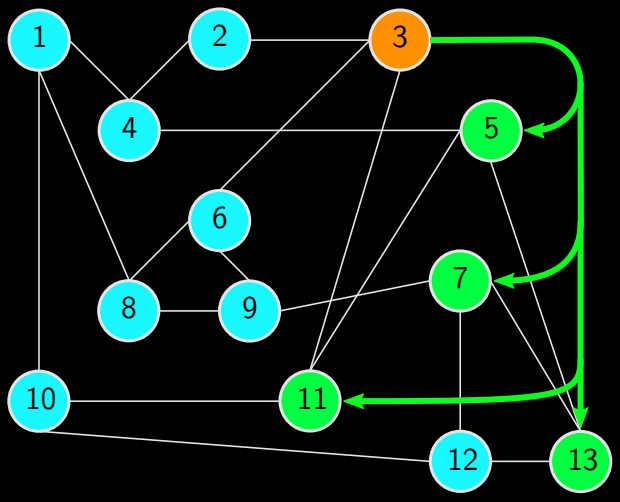
1. Перед началом работы мы имеем пиринговую сеть с узлами, имеющими собственный сетевой адрес и уникальный номер, который знают все участники сети. Например, у нас будет 13 участников сети, пронумеруем все узлы номерами с 1 до 13. Так же мы договоримся, что в консенсус будет входить 5 узлов.



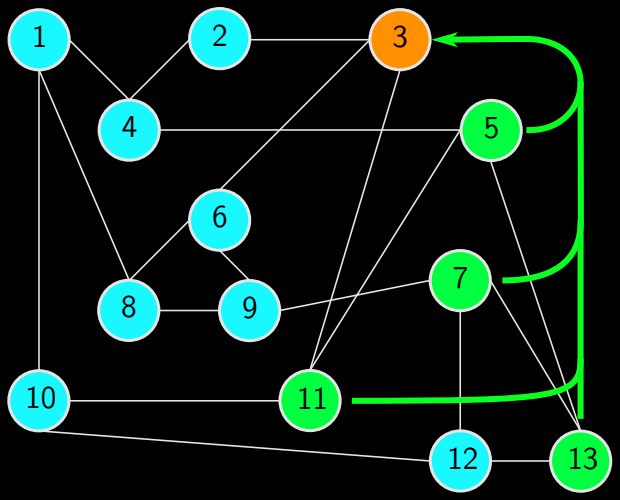
   Синим цветом будут обозначатся узлы, работающие в блокчейне. Зелёным цветом будут обозначаться узлы, участвующие в консенсусе. Мастер-узел будет помечаться оранжевым цветом. Узлы, находящиеся в нештатном режиме работы будут обозначаться красным цветом.
2. Начало работы консенсуса. Пусть все узлы пиринговой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



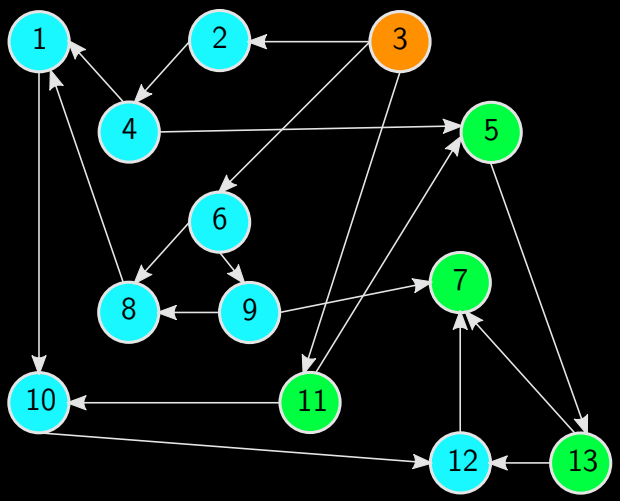
3. Как показано на рисунке выше узел №3 мы пометили оранжевым цветом, чтобы показать, что он является мастер-узлом. С этого момента узлы №3,5,7,11,13 участвуют в консенсусе.
4. Пусть узел №3 получил новую транзакцию от узла №2. Узел №3 проверяет, является ли транзакция корректной, если она признается 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.



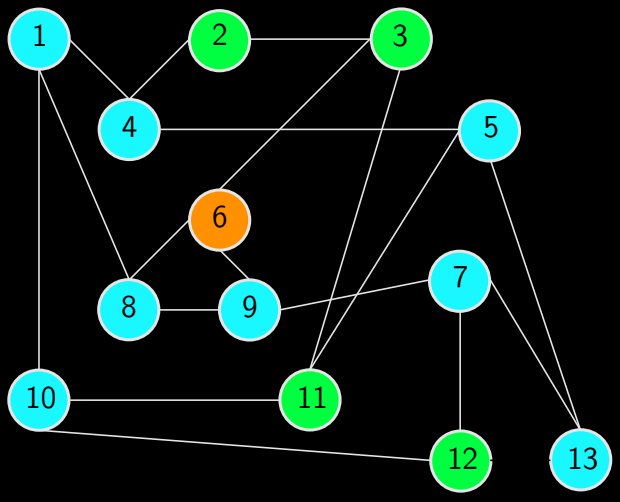
6. Узлы №5,7,11 и 13 пересылают хеш дерева Меркла, принятых ими транзакций, и свои подписи под хешем узлу №3.



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.

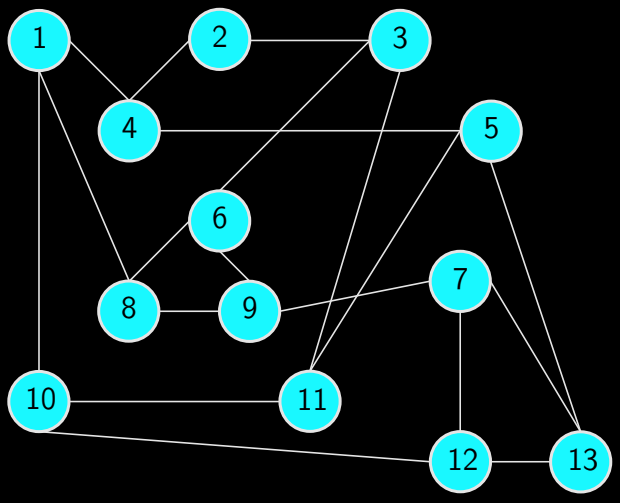


Далее процесс повторяется в соответствии с п.п. 3-8 алгоритма.

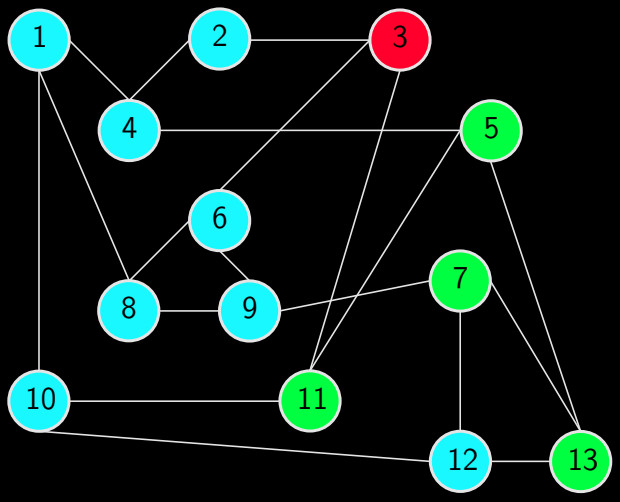
9.0.1 Обработка ошибочных ситуаций алгоритмом *sdbft*

Мастер узел недоступен

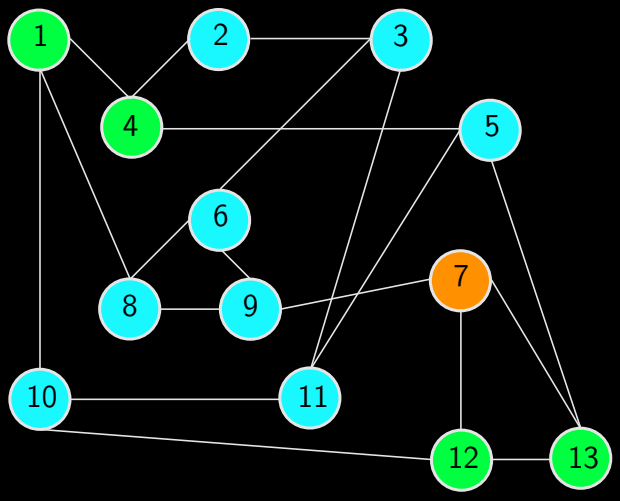
1. Повторим п.п. алгоритма 1 и 2.
2. Перед началом работы мы имеем пиринговую сеть с узлами, имеющими собственный сетевой адрес и уникальный номер, который знают все участники сети. Например, у нас будет 13 участников сети, пронумеруем все узлы номерами с 1 до 13. Так же мы договоримся, что в консенсус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



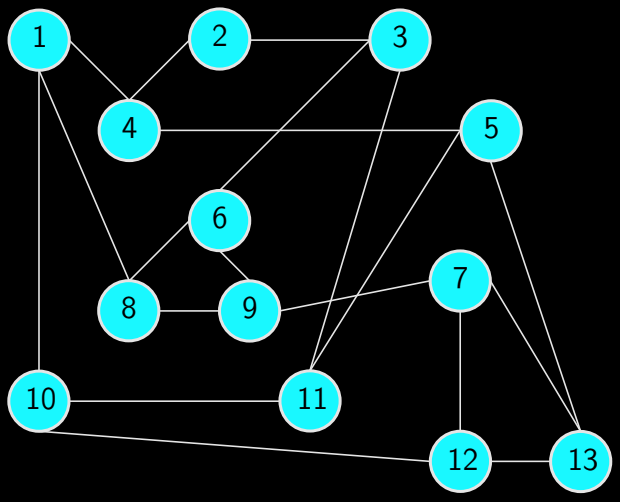
4. Узлы эскорта не получат сообщения о закрытия блока, блокчейн сеть переходит на следующий раунд (см приложение А).
5. Возвращаемся на второй шаг алгоритма, пусть теперь функция f (см приложение А) создаст случайную последовательность на основании принятого блока и номера раунда, пусть будут номера 7,1,4,12,13. Сеть блокчейна будет выглядеть следующим образом.



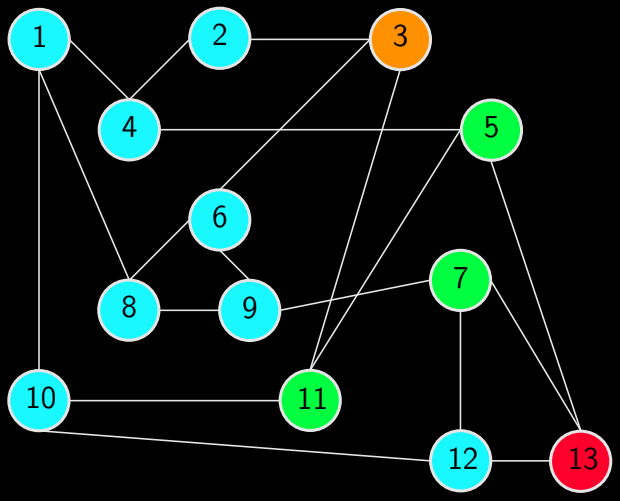
6. Далее алгоритм будет исполняться штатным образом в соответствии с п.п. 3-8.

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.



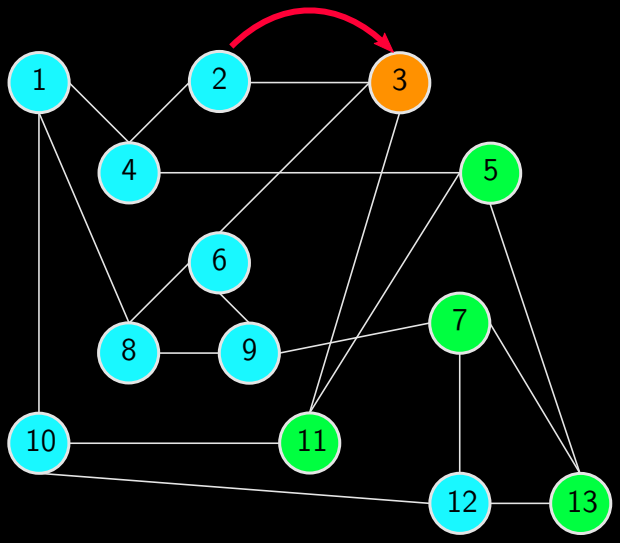
3. Начало работы консенсуса. Пусть все узлы пиринговой сети примут блок №1. В принятом блоке содержится информация, которая позволит функции f (см. приложение А) создать случайную последовательность. Пусть эта последовательность будет следующей — 3,5,7,11,13. Узел 13 недоступен. Пометим выбранные узлы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

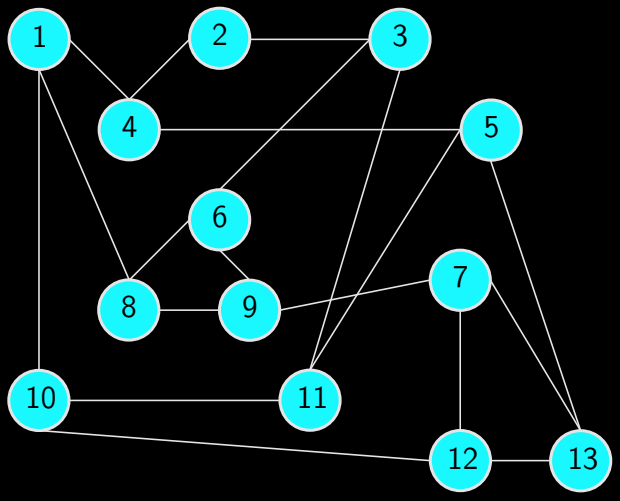
1. Пусть узел 3 получил новую транзакцию от узла №2. Узел №3 проверяет, транзакцию и признает ее некорректной.
2. Если узел №3 признал транзакцию некорректной, то он ее отбрасывает, сообщение узлу №2 о некорректной транзакции не пересылается на узлы, входящие в консенсус.



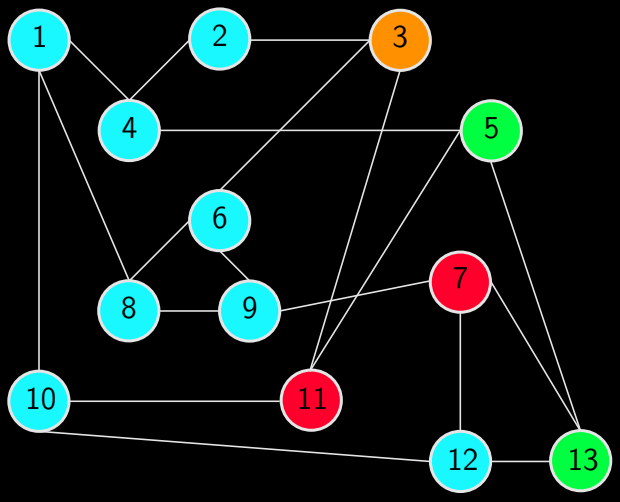
Количество блоков в блокчейне разное на разных узлах

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.

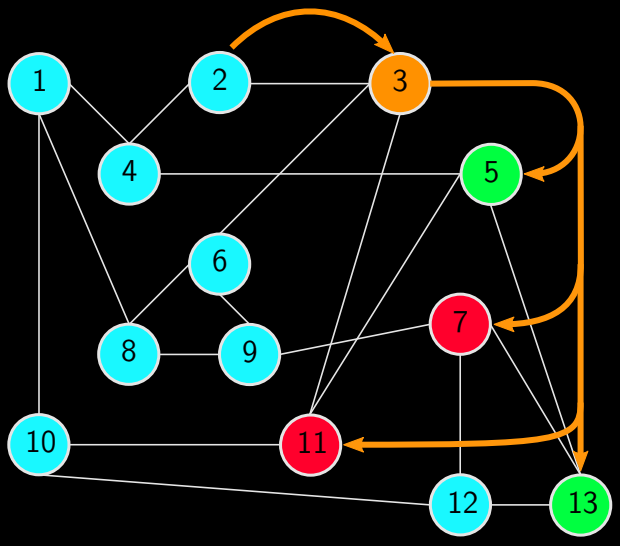
1. Перед началом работы мы имеем пиринговую сеть с узлами, имеющими собственный сетевой адрес и уникальный номер, который знают все участники сети. Например, у нас будет 13 участников сети, пронумеруем все узлы номерами с 1 до 13. Так же мы договоримся, что в консенсус будет входить 5 узлов.



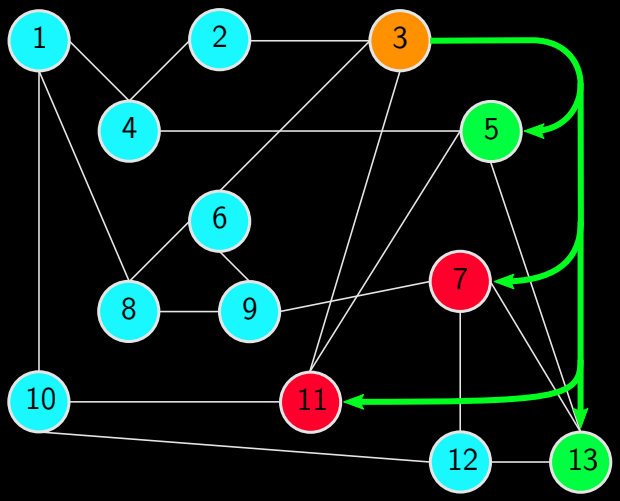
2. Начало работы консенсуса, пусть все узлы пиринговой сети примут блок 1.В принятом блоке содержится информация, которая позволит функции f (см приложение А) создать случайную последовательность. Пусть эта последовательность будет следующей — 3,5,7,11,13, узлы 7 и 11 имеют отличное число принятых блоков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

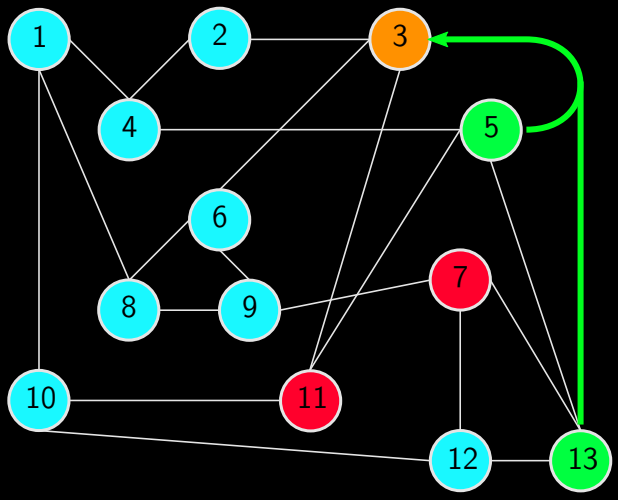


5. По завершению времени на закрытие блока узел №3 пересылает узлам №5,7,11,13 сообщение о закрытии блока, узлы 7 и 11 отвергают сообщение.



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

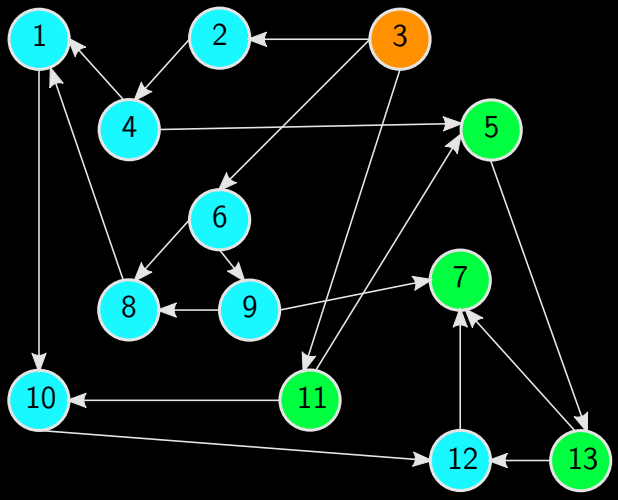
7. Узел №3 проверяет подписи узлов эскорта. Так как количество подписей узлов эскорта недостаточно для принятия блока, то блокчейн переходит на следующий раунд.



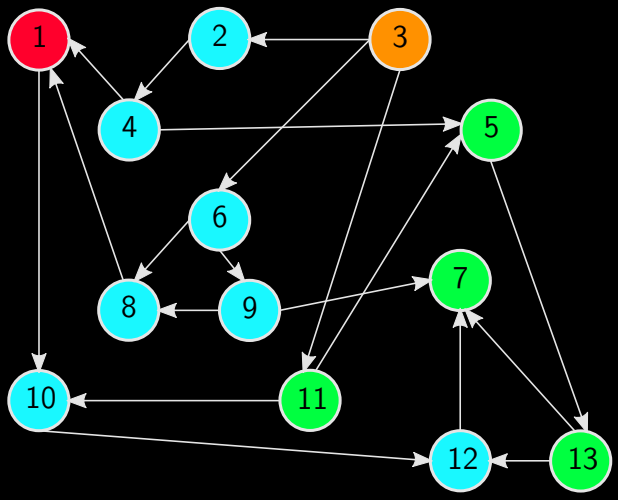
Узел отвергает новый блок блокчейна

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.

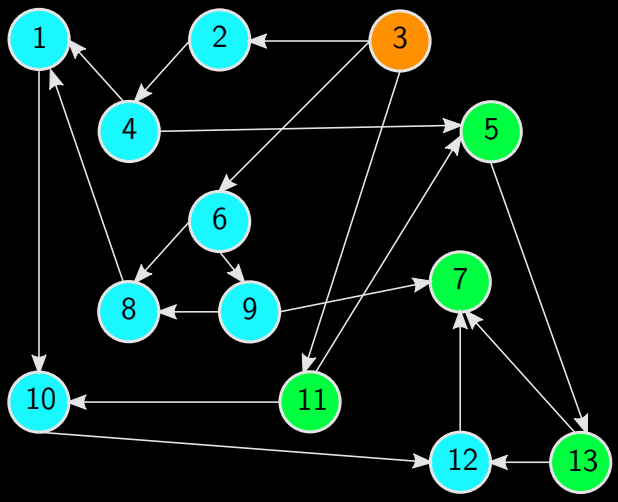


3. Узел №1 пытается найти в сети блок с отличной от признанного им ошибочным блока хеш-суммой, если узел не может найти удовлетворяющий его блок, то узел начинает процедуру пересинхронизации блокчейна см. п. 3.5.

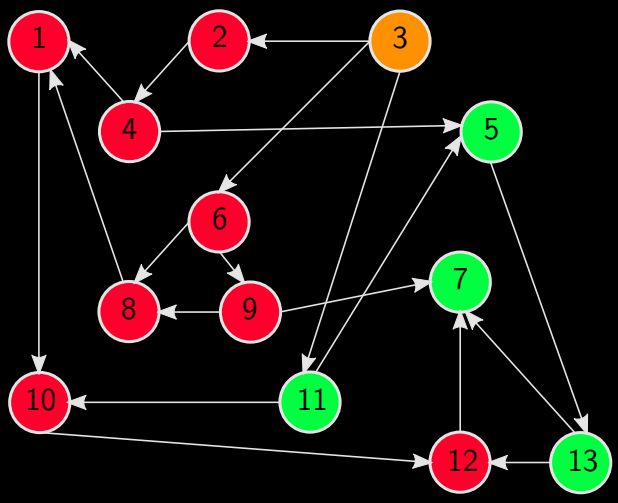
Сеть отвергает новый блок блокчейна

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.

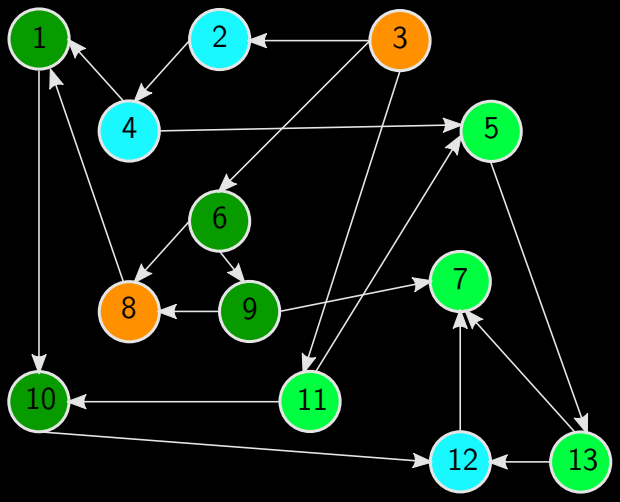


3. Блокчейн переходит на следующий раунд и далее пока не будет корректно сформирован следующий блок.

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.