ИНТЕРНЕТ-ТЕХНОЛОГИИ

МОЛОДЕЦКАЯ СВЕТЛАНА ФЕДОРОВНА, E-MAIL (MOLODEZKAYASF@MAIL.RU)

ИНТЕРНЕТ-ТЕХНОЛОГИИ

технологии создания и поддержки различных информационных ресурсов в компьютерной сети Интернет:

сайтов, блогов, форумов, чатов, электронных библиотек и энциклопедий, мобильных приложений.

ЧТО ИЗУЧАЕМ В КУРСЕ:

- **ТЕХНОЛОГИЯ БЛОКЧЕЙН.**
- **ОБЛАЧНЫЕ ТЕХНОЛОГИИ.**

ЧТО ИЗУЧАЕМ В КУРСЕ:

Web-разработка:

- Сетевые протоколы
- Веб-серверы
- Серверная разработка
- Обработка пользовательских данных
- HTML, CSS, JAVASCRIPT,PHP
- Платформы для разработки: JOOMLA, DRUPAL

ЧТО ИЗУЧАЕМ В КУРСЕ:

МОБИЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ:

- iOS;
- Android;
- Windows Phone.

ТЕХНОЛОГИЯ БЛОКЧЕЙН

это распределенная база данных, у которой устройства хранения данных **не подключены** к общему серверу.

Эта база данных хранит постоянно растущий список упорядоченных записей, называемых блоками. ...

В **технологию блокчейн** изначально заложена безопасность на уровне базы данных.

БЛОКЧЕЙН ИЗНУТРИ

Блокчейн был описан в статье **Сатоши Накамото**

«Bitcoin: A Peer-to-Peer Electronic Cash System».

Там всего на восьми страницах автор описал основы криптовалюты Биткоин, в основе которой лежал как раз алгоритм Блокчейна.

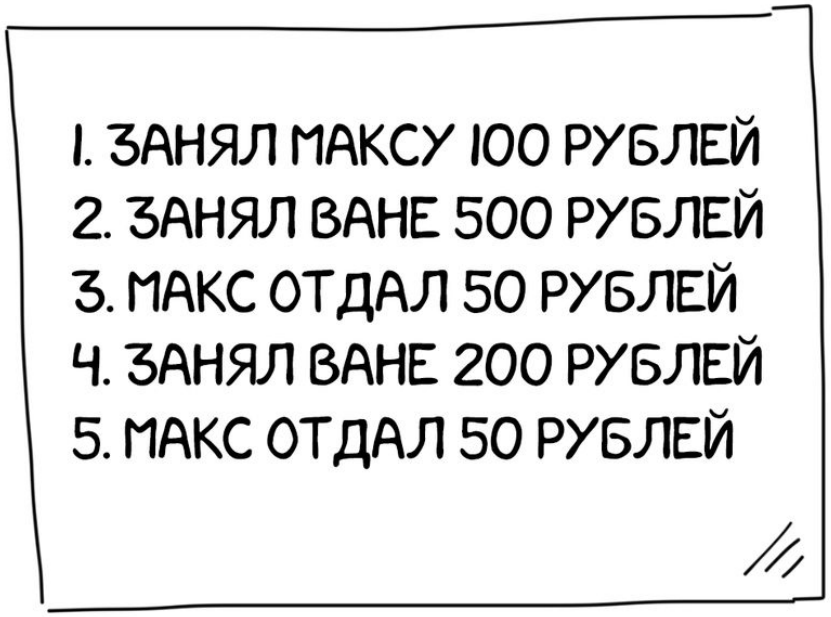
Блокчейн появился вместе с биткоином, но может использоваться независимо от него и даже модифицироваться. Любой может сделать свой блокчейн хоть у себя на ноутбуке.

ПРОСТЫМИ СЛОВАМИ…

Блокчейн — цепочка блоков или другими словами связный список. В таком списке каждая следующая запись ссылается на одну предыдущую и так по цепочке до самой первой.

Как вагоны поезда, каждый тащит за собой следующий.

РАЗБЕРЕМСЯ…


1. ЗАНЯЛ МАКСУ 100 РУБЛЕЙ
2. ЗАНЯЛ ВАНЕ 500 РУБЛЕЙ
3. МАКС ОТДАЛ 50 РУБЛЕЙ
4. ЗАНЯЛ ВАНЕ 200 РУБЛЕЙ
5. МАКС ОТДАЛ 50 РУБЛЕЙ


ОЛЕГ
МОЛОДЕЦ

РАЗБЕРЕМСЯ…

СТРОКА: ВАСТРИК

ХЕШ: 110A84203960300D21F1C422FAA76089C9
D912345DA701AB09E5A02920F95059E

СТРОКА: ВАСТРИК.

ХЕШ: 7D762A3227E6B1A66F49A54B7C749FA8
B5E5C733B15C05F7B4DF9BA2D9AEEC00

РАЗБЕРЕМСЯ...

SHA-256

1. ЗАНЯЛ МАКСУ 100 РУБЛЕЙ -> 4D1DDF888722...

2. ЗАНЯЛ ВАНЕ 500 РУБЛЕЙ -> 74CA68E54029...

3. МАКС ОТДАЛ 50 РУБЛЕЙ -> 0F32DE069639...

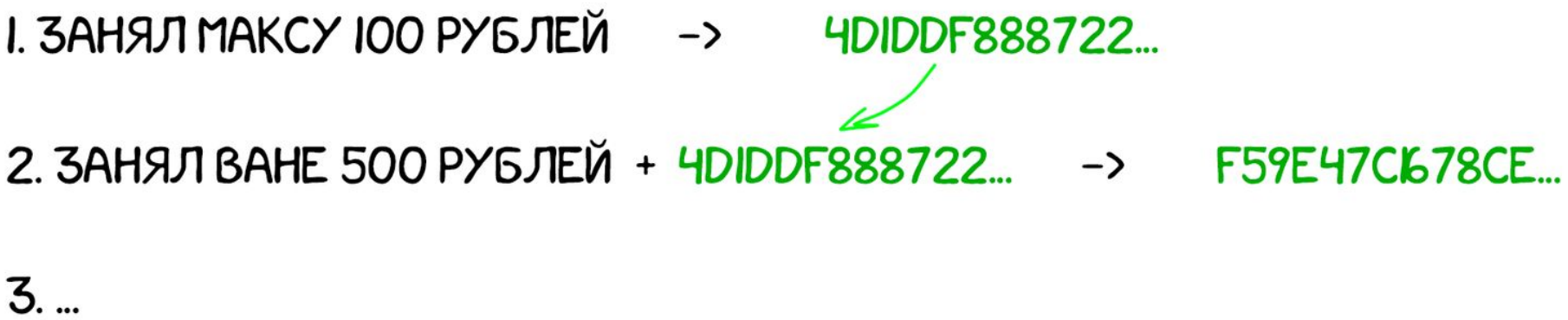
4. ЗАНЯЛ ВАНЕ 200 РУБЛЕЙ -> 4FC7534C7E2B...

5. МАКС ОТДАЛ 50 РУБЛЕЙ -> F41223E2DEAF...

РАЗБЕРЕМСЯ…

Ваня тоже знает хэширование SHA-256 и легко может изменить запись вместе с её хешем. Особенно, если хеш написан прямо рядом на доске.

Потому для большей безопасности Олег решает хешировать не саму только запись, а складывать её вместе с хешем от прошлой записи. Теперь все следующие записи зависят от предыдущих. Если изменить хотя бы одну строчку, то придется пересчитать хеши всех остальных ниже по списку.



РАЗБЕРЕМСЯ…

Так у Олега появляется личный связный список.

РАЗБЕРЕМСЯ…

Но однажды Иван прокрадывается ночью, изменяет нужную ему запись и обновляет хеши для всего списка до конца. У него это занимает несколько часов, но Олег всё равно крепко спит и не слышит. Наутро Олег обнаруживает абсолютно верный список — все хеши совпадают. Но Иван всё равно его обманул, хоть и потратил на это бессонную ночь.

Как еще можно защититься от Ночного Ивана?

Олег решает как-то усложнить ему жизнь. Теперь для добавления новой записи в список, Олег будет решать связанную с ней сложную задачку, например **математическое уравнение**. Ответ он будет **добавлять в итоговый хеш**.

РАЗБЕРЕМСЯ…

Олег силен в математике, но даже у него на добавление записи уходит по десять минут. Несмотря на это, потраченное время того стоит, ведь если Иван опять захочет что-то изменить, ему придется заново решать уравнения для каждой строки, а их могут быть десятки. На это уйдет куча времени, ведь уравнения каждый раз уникальны и связаны с конкретной записью.

Зато проверить список всё так же просто: сначала нужно как раньше сравнить хеши, а потом проверить решения уравнений простой подстановкой.

Если всё сходится — список не изменен.

РАЗБЕРЕМСЯ…

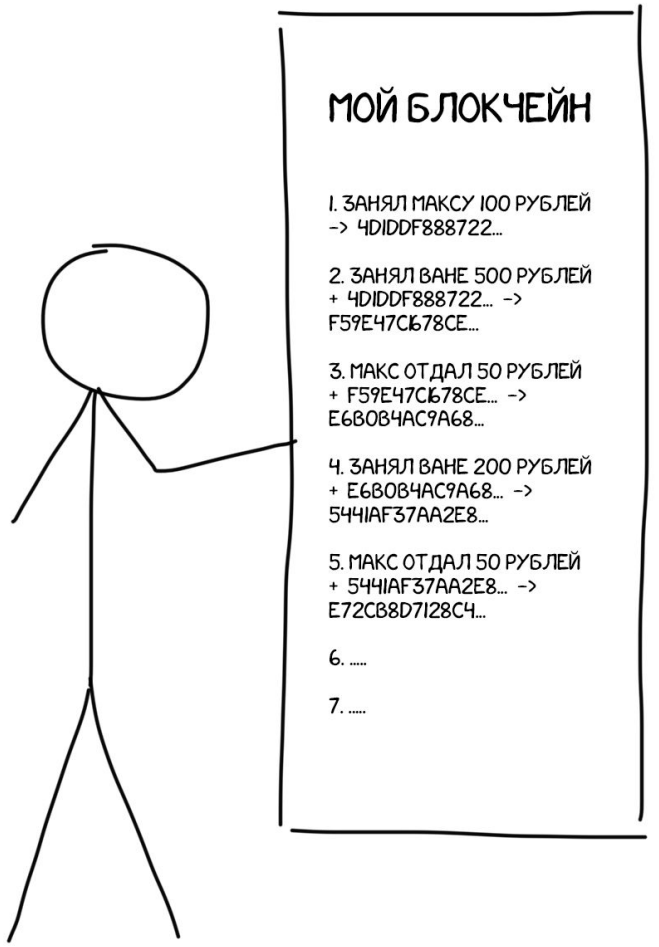
В реальности же с уравнениями не всё так хорошо: компьютеры слишком хорошо их решают, да и где хранить столько уникальных уравнений. Потому авторы блокчейна придумали более красивую задачу: нужно найти такое число (nonce), чтобы итоговый хеш всей записи начинался на 10 нулей.

Такой nonce сложно найти, зато результат всегда можно проверить просто глазами.

РАЗБЕРЕМСЯ…

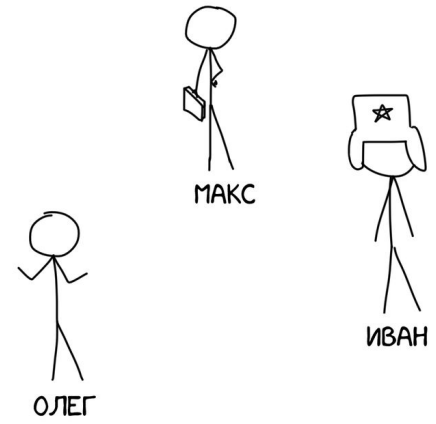
Теперь Олег сверяет все хеши и дополнительно убеждаются, чтобы каждый начинался на оговоренное количество нулей. Хитрый Иван, даже вооружившись мощным ноутбуком, не успеет за ночь пересчитать все хеши так, чтобы они удовлетворяли условию — не хватит времени.

Такой список по сути и есть домашний блокчейн на коленке. Его безопасность гарантирована математиками, которые доказали, что эти хеши нельзя вычислить как-то быстрее, кроме как перебором. Такой перебор хешей к каждой записи и есть майнинг, о котором сегодня будет много и подробно.

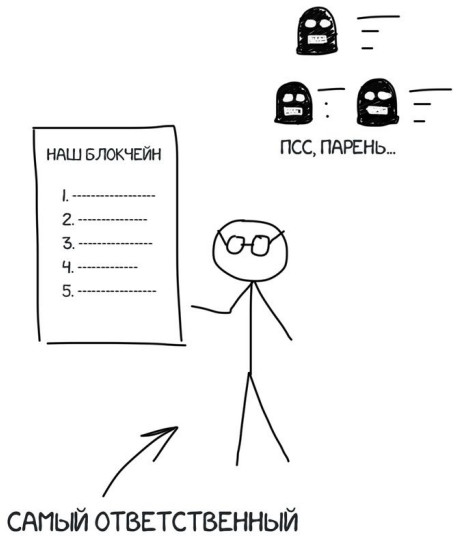


ЦЕНТРАЛИЗАЦИЯ ДОВЕРИЯ

Идея вести неподделываемый список «кто кому занимал» понравилась нашим друзьям. Они тоже не хотят запоминать кто за кого заплатил в баре и сколько еще остался должен — всё записано на стене. Вы обсудили идею и решили, что теперь вам нужен единый список на всех.



Но кому доверить вести столь важную бухгалтерию? Ведь когда дело касается денег — доверие выходит на первый план. Мы не доверим хранить свои деньги неизвестному. Наши предки для этого придумали банки которым со временем стали доверять, потому что они подкреплены лицензией, законами и страховкой Центрального Банка.



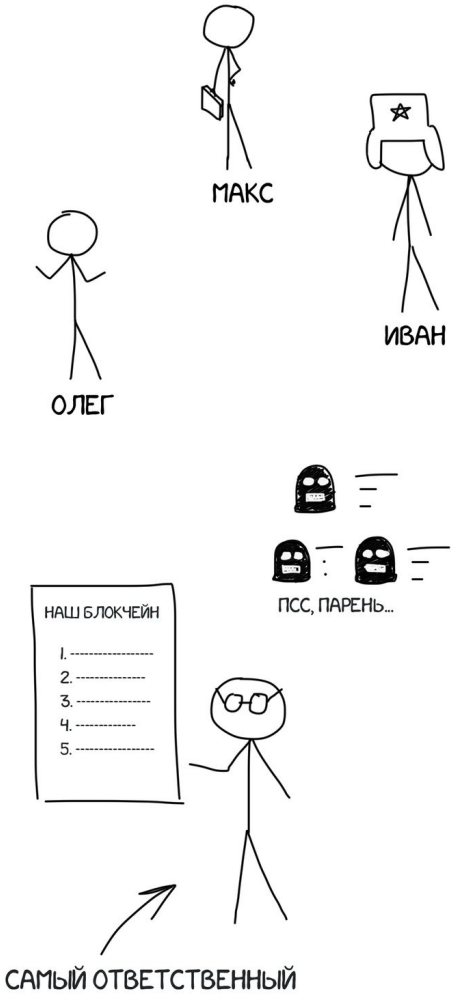
ЦЕНТРАЛИЗАЦИЯ ДОВЕРИЯ

В кругу друзей все доверяют друг другу и можно просто выбрать на эту **роль самого ответственного**.

Но что если вопрос касается незнакомых людей.

Целого города, страны, или всего мира, как в случае с биткоином?

Там вообще никто никому не может доверять.



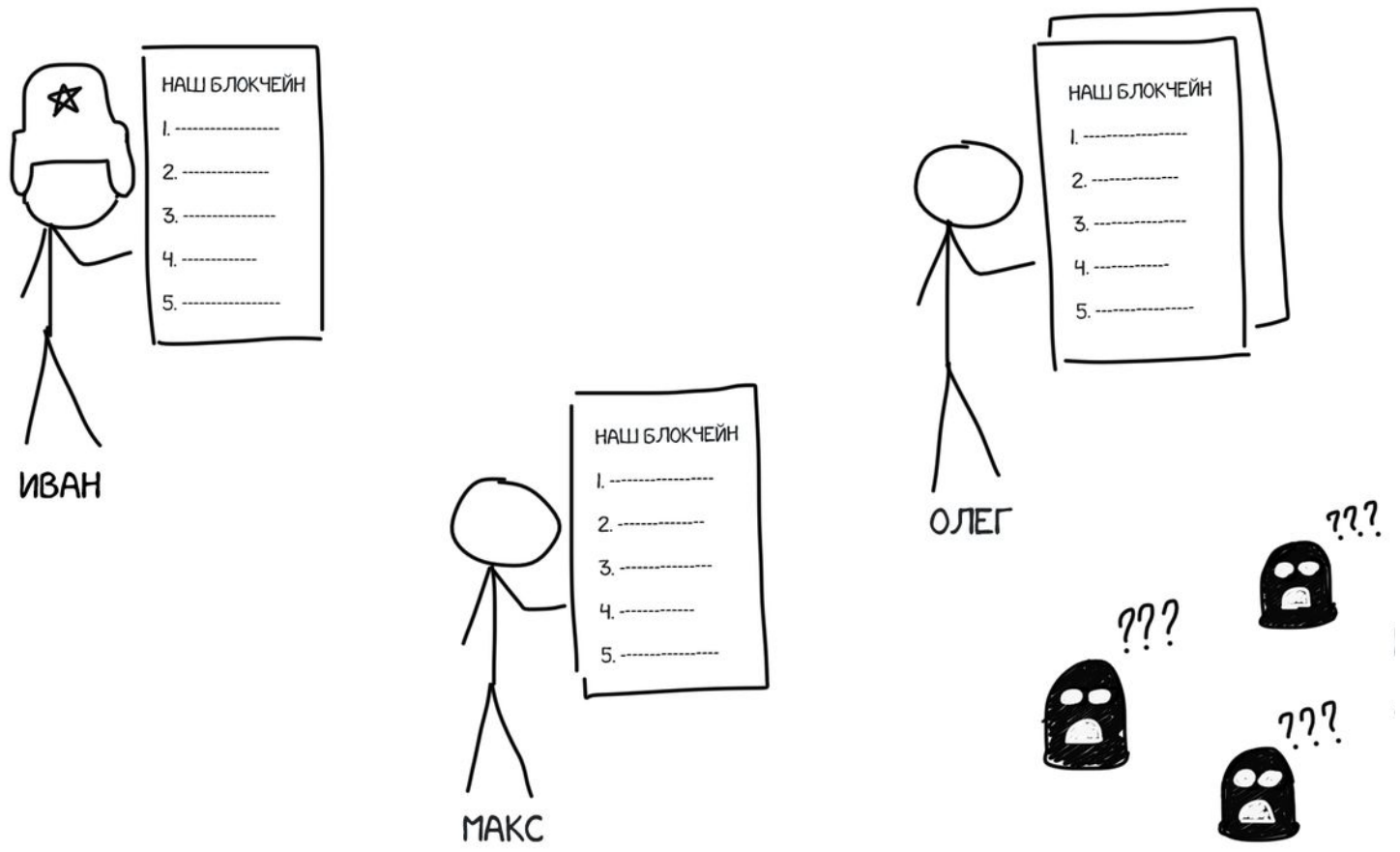
ДЕЦЕНТРАЛИЗАЦИЯ: НИКТО НЕ ДОВЕРЯЕТ НИКОМУ

Так придумали альтернативный подход: хранить копию списка у каждого. Таким образом злоумышленнику придется не просто переписать один список, но и прокрасться в каждый дом и переписать списки там. А потом выяснится, что кто-то хранил у себя дома аж несколько списков, о чем никто не догадывался. Это и есть децентрализация.

Минусом такого подхода является то, что для внесения новых записей придется обзванивать всех остальных участников и сообщать каждому из них свежие изменения. Но если эти участники — бездушные машины, это перестаёт быть хоть какой-то проблемой.

В такой системе не существует единой точки доверия, а значит и возможности подкупа и жульничества. Все участники системы действуют согласно единому правилу: никто не доверяет никому. Каждый верит только той информации, которой располагает сам. Это главный закон любой децентрализованной сети.

РАЗБЕРЕМСЯ...


НАШ БЛОКЧЕЙН
1.
2.
3.
4.
5.
ИВАН
НАШ БЛОКЧЕЙН
1.
2.
3.
4.
5.
МАКС
НАШ БЛОКЧЕЙН
1.
2.
3.
4.
5.
ОЛЕГ
???
???
???

ТРАНЗАКЦИИ

Покупая доширак в магазине, вы вводите пин-код от своей карты, разрешая магазину спросить у банка есть ли у вас

на счету 35 рублей. Другими словами, вы подписываете своим пин-кодом транзакцию на 35 рублей, которую банк подтверждает или отклоняет.

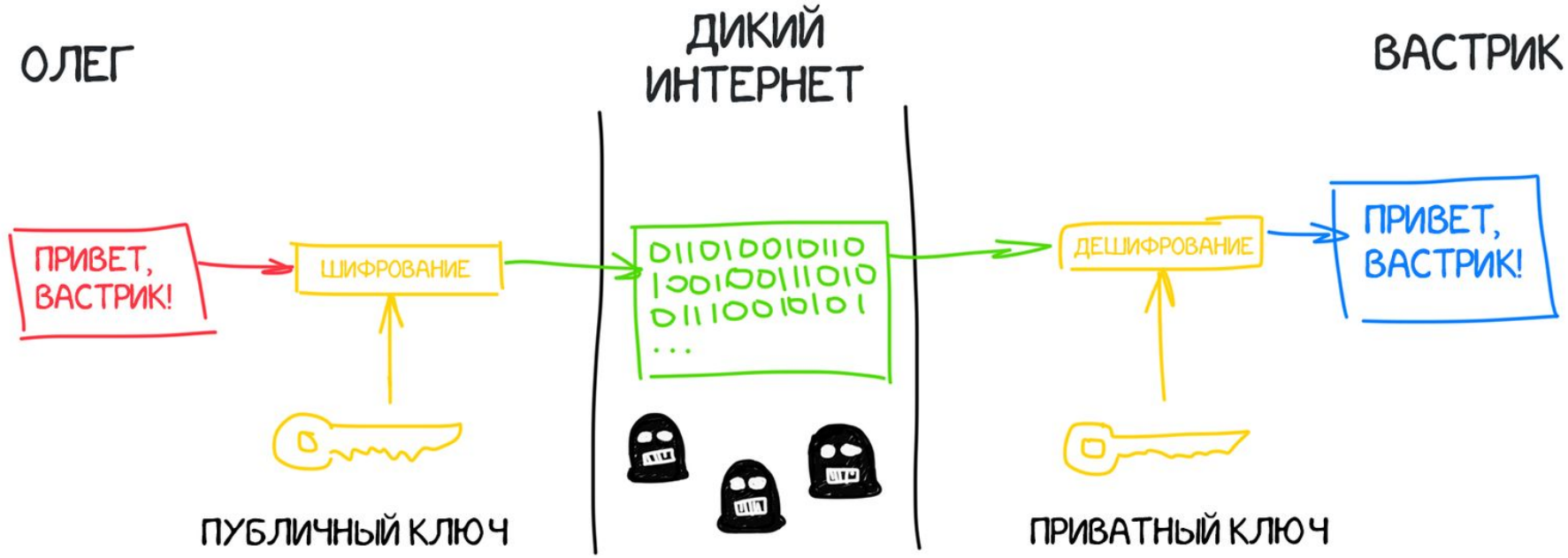
Наши записи типа «Занял Ване 500 рублей» — тоже транзакции.

Но у нас нет банка, авторизующего автора транзакций. Как нам проверить, что Иван втихую не добавил запись «Макс должен Олегу 100 500 рублей»?

ТРАНЗАКЦИИ

В блокчейне для этого используется механизм публичных и приватных ключей, айтишники давно используют их для авторизации в том же SSH. Коротко о том, как работает эта сложная, но красивая математика: вы у себя на компьютере генерируете пару длинных простых чисел — публичный и приватный ключ. Приватный ключ считается супер-секретным, потому что может расшифровать то, что зашифровано публичным. Но наоборот тоже работает. Если вы расскажете публичный ключ всем друзьям, они смогут зашифровать им любое сообщение так, что прочитать его сможете только вы, так как владеете приватным. Но кроме этого у публичного ключа есть полезный эффект — с помощью него можно проверить, что данные были зашифрованы именно вашим приватным ключом, не расшифровывая при этом сами данные. Обо всех этих свойствах хорошо рассказано в «Книге Шифров» по ссылке выше.

ТРАНЗАКЦИИ



Мы находимся в децентрализованном интернете, где никому нельзя доверять. Транзакция подписывается приватным ключом и вместе с публичным ключом отсылается в специальное хранилище — пул неподтвержденных транзакций. Так любой участник сети может проверить, что именно вы были её инициатором, а не кто-то еще хочет расплатиться вашими деньгами.

Этим достигается открытость и безопасность сети. Если раньше за это отвечали банки, то в блокчейне за это отвечает математика.

ТРАНЗАКЦИИ

Мы находимся в децентрализованном интернете, где никому нельзя доверять. Транзакция подписывается приватным ключом и вместе с публичным ключом отсылается в специальное хранилище — пул неподтвержденных транзакций. Так любой участник сети может проверить, что именно вы были её инициатором, а не кто-то еще хочет расплатиться вашими деньгами.

Этим достигается открытость и безопасность сети. Если раньше за это отвечали банки, то в блокчейне за это отвечает математика.

ТРАНЗАКЦИИ

Простым пользователям, не желающим разбираться как выпускать и хранить приватные ключи, помогут сервисы онлайн-кошельков. Чтобы копировать длинные публичные ключи, там делают удобные QR-коды. Лично я пользуюсь Blockchain Wallet, потому что у него есть удобное мобильное приложение и он поддерживает две главные криптовалюты — BTC и ETH

ОТСУТСТВИЕ ПОНЯТИЯ «БАЛАНСА»

Как и наша доска, блокчейн по сути состоит только из истории транзакций.

Он не хранит баланс каждого кошелька, иначе бы нам пришлось изобретать дополнительные способы защиты.

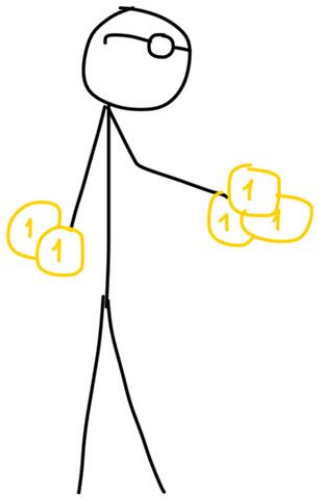
Владение кошельком подтверждает только приватный ключ. Но как другие участники сети убедятся, что у меня есть достаточно денег для покупки?

ОТСУТСТВИЕ ПОНЯТИЯ «БАЛАНСА»

Раз у нас нет баланса — это должны доказывать вы. Потому в транзакцию блокчейна входит не только ваша подпись и сколько вы хотите потратить, но и ссылки на предыдущие транзакции, в которых вы получили нужное количество денег. То есть если вы хотите потратить 400 рублей вы пробегаете по всей своей истории доходов и расходов, и прикрепляете к своей транзакции те доходы, где вам дали 100 + 250 + 50 рублей, тем самым доказывая, что у вас есть эти 400 рублей.

ОТСУТСТВИЕ ПОНЯТИЯ «БАЛАНСА»

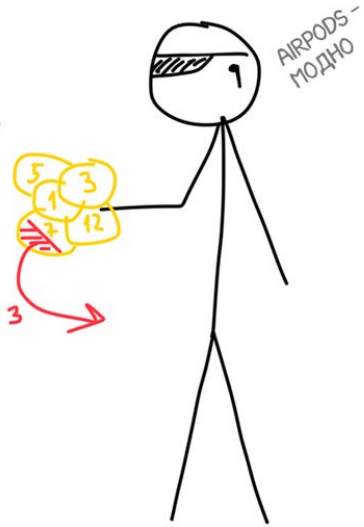
КЛАССИЧЕСКИЕ ТРАНЗАКЦИИ



«У МЕНЯ ЕСТЬ 5 РУБЛЕЙ, ДЕРЖИ 3»

ТРАНЗАКЦИИ В БЛОКЧЕЙНЕ

«ДЕРЖИ 25 BTC, ИЗ КОТОРЫХ 5 МНЕ ДАЛ ВАНЯ, 12 МАКС, ..., И ВЕРНИ 3 BTC СДАЧИ»



ОТСУТСТВИЕ ПОНЯТИЯ «БАЛАНСА»

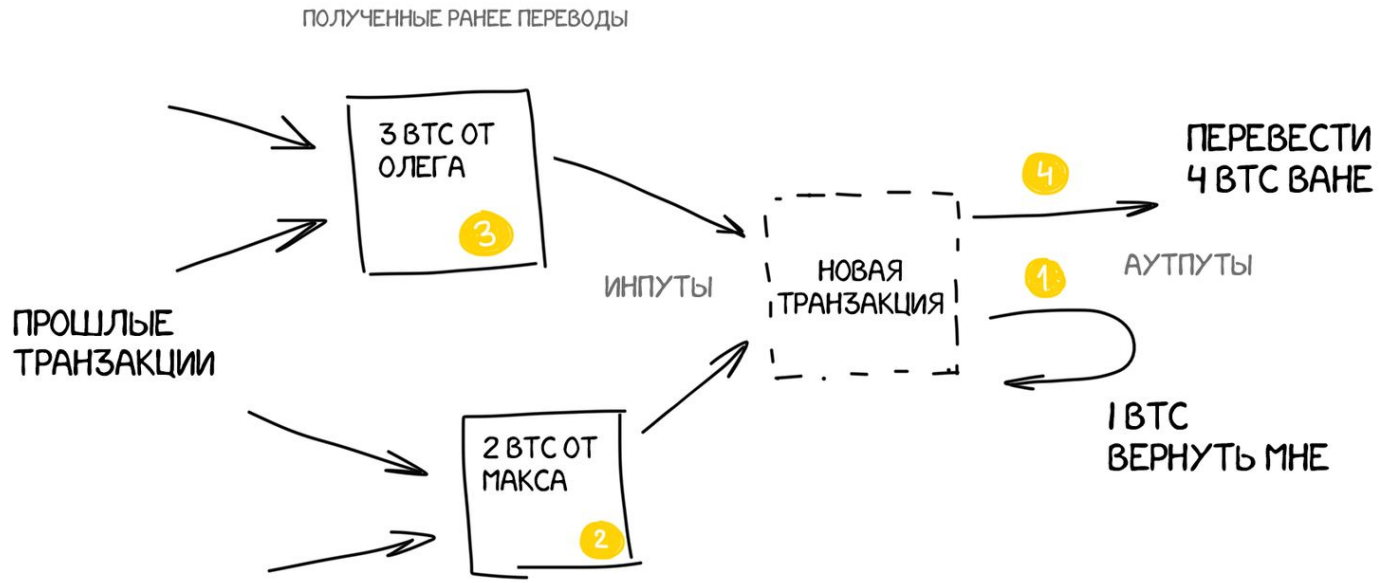
Каждый участник сети еще раз обязательно проверит, что вы не прикрепляли доходы дважды. Что те 300 рублей, что дал Макс на прошлой неделе, вы действительно еще не потратили.

Такие прикрепленные к транзакции доходы в блокчейне называются инпутами (input), а все получатели денег — аутпутами (output). Сумма всех инпутов редко бывает ровно такой, сколько вы хотите перевести за раз — потому один из аутпутов чаще всего будете вы сами. Другими словами транзакция в блокчейне выглядит как «мне дали 3 и 2 BTC, я хочу из них перевести 4 BTC и оставшийся 1 BTC вернуть себе обратно».

ОТСУТСТВИЕ ПОНЯТИЯ «БАЛАНСА»

Забегая немного вперед: дополнительно из этой «сдачи» еще можно указать комиссию за транзакцию, чтобы майнеры активнее её добавляли в блоки. Тогда майнер получит копеечку, а вы немного меньше сдачи назад.

Поговорим о майнинге.



ОТСУТСТВИЕ ПОНЯТИЯ «БАЛАНСА»

Красота блокчейна еще и в том, что инпуты не обязательно должны быть с одного кошелька. Проверяется ведь только ключ. Если вы знаете приватный ключ всех инпутов, то вы без проблем сможете прикрепить их к своей транзакции и расплатиться этими деньгами. Как если бы вы в супермаркете платили сразу с нескольких карт, от которых знаете пин-код.

Однако если вы потеряете свой приватный ключ, ваш диск умрет или украдут ноутбук, ваши биткоины будут потеряны навсегда. Никто не сможет использовать их в качестве инпутов для новых транзакций. Эта сумма будет недоступна для всего мира навсегда — как если бы вы сожги пачку банкнот. Здесь нет единого банка, куда можно написать заявление с копией паспорта, и он еще напечатает. Для этого нужен еще дополнительный выпуск новых биткоинов «из воздуха».

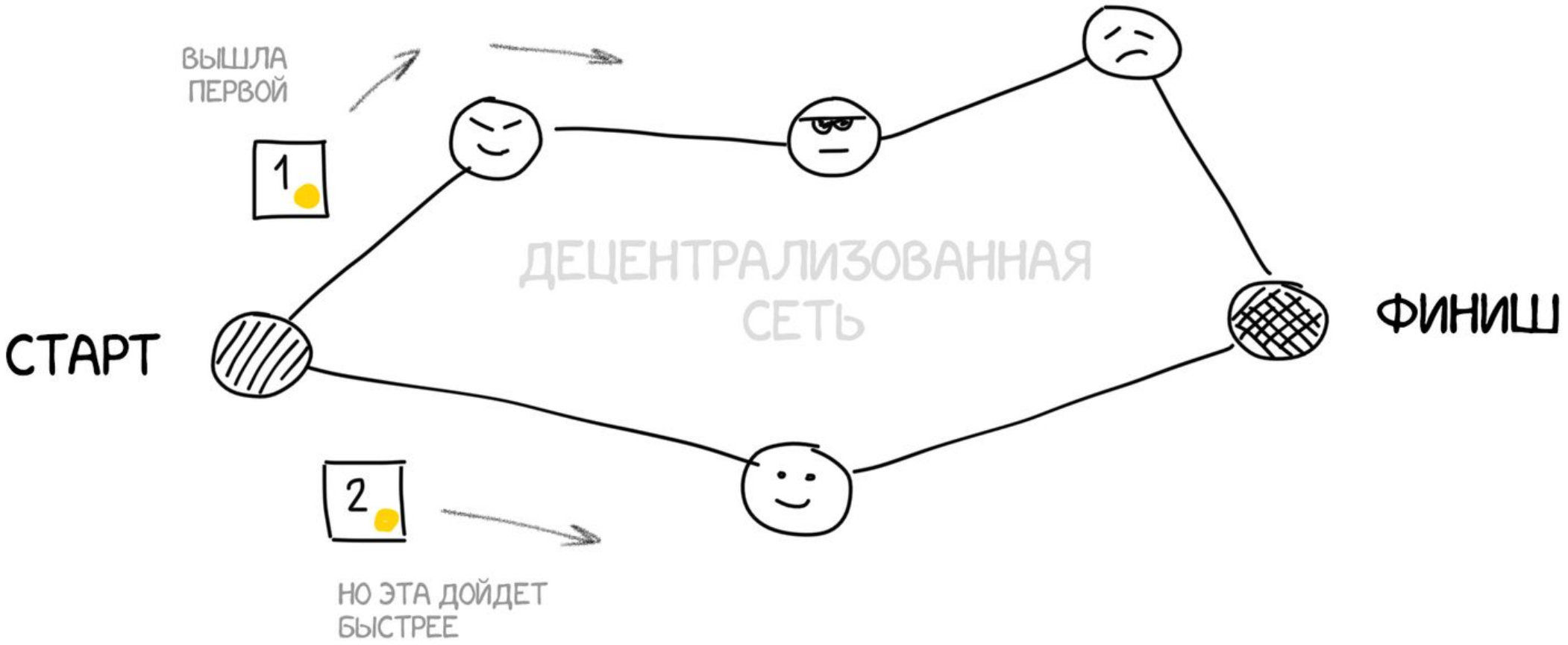
ПРОБЛЕМА ДВОЙНОЙ ТРАТЫ

- Забегая немного вперед: дополнительно из этой «сдачи» еще можно указать комиссию за транзакцию, чтобы майнеры активнее её добавляли в блоки. Тогда майнер получит копеечку, а вы немного меньше сдачи назад.

- Транзакции добавляются в специальный «пул неподтвержденных транзакций». Зачем нам какая-то промежуточная сущность, если у нас уже есть по сути готовые подписанные транзакции? Почему не писать их сразу в блокчейн?

Потому что сигналы из пункта А в пункт Б всегда идут с задержкой. Две транзакции могут пойти абсолютно разными путями. И транзакция, которая была инициирована первой, может дойти до получателя позже, потому что шла более длинным путём. Так получается **двойное расходование**, когда одни и те же деньги были отправлены сразу двум адресатам, о чем они даже не догадаются. передавать.

ПРОБЛЕМА ДВОЙНОЙ ТРАТЫ



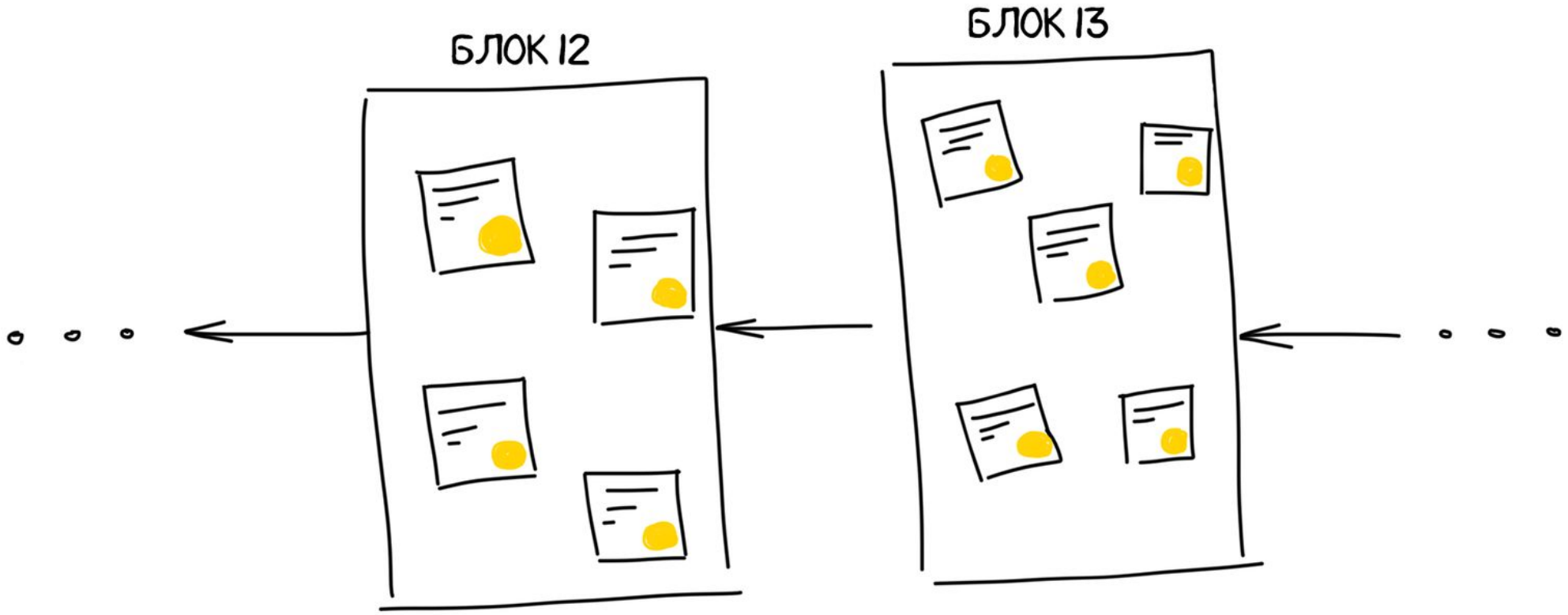
ПРОБЛЕМА ДВОЙНОЙ ТРАТЫ

Для децентрализованной сети, в которой никому нельзя доверять, эта проблема стоит особенно остро. Вот как вы убедитесь, что одна транзакция точно была раньше другой? Попросите отправителя вшивать в неё время отправки, не так ли? Но вспомните — никому нельзя доверять, даже отправителю. Время на всех компьютерах обязательно будет отличаться и нет способа их гарантировано синхронизировать. Копия блокчейна хранится на каждом компьютере сети и каждый участник доверяет только ей.

Как же убедиться, что одна транзакция была раньше другой?

Ответ прост: ЭТО НЕВОЗМОЖНО! Нет способа подтвердить время транзакции в децентрализованной сети. И вот в решении этой проблемы и заключается третья важная идея блокчейна, которую придумал Сатоши и которая, как ни странно, прописана прямо в его названии — блоки.

ПРОБЛЕМА ДВОЙНОЙ ТРАТЫ



ЕСЛИ ДОБАВЛЯТЬ ТРАНЗАКЦИИ БЛОКАМИ РАЗ В 10 МИНУТ,
ТО НЕ БУДЕТ ВОПРОСОВ КТО БЫЛ ПЕРВЫМ

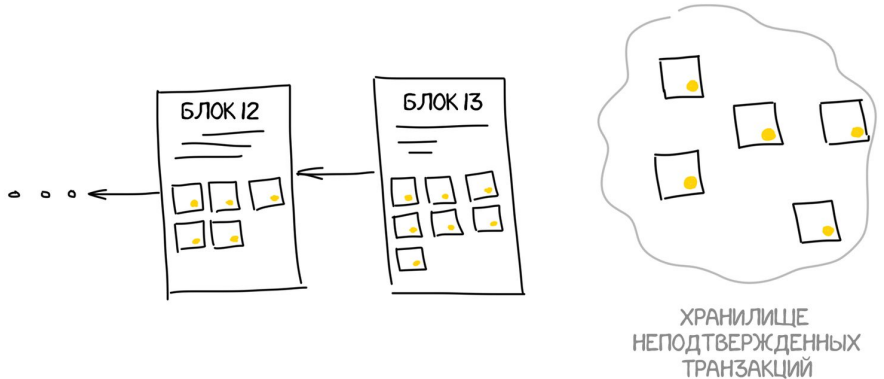
БЛОКИ — ОСНОВА БЛОКЧЕЙНА

Каждый работающий компьютер в сети выбирает из общего пула любые транзакции, которые ему нравятся. Обычно просто по самой высокой комиссии, которую он может на ней заработать. Так он набирает себе транзакции, пока их суммарный размер не достигнет обговорённого лимита. В Биткоине этот лимит на размер блока равен 1 Мб (после SegWit2x будет 2 Мб), а в Биткоин Кэше — 8 Мб.

А вот в сетях типа Ethereum всё немного сложнее, там количество транзакций на блок зависит от вычислительной сложности включенных в них смарт-контрактов. Но суть не меняется — есть определенный лимит.

БЛОКИ — ОСНОВА БЛОКЧЕЙНА

Весь блокчейн по сути и есть список таких блоков, где каждый ссылается на предыдущий. По нему можно отследить любую транзакцию за всю историю, разматывая блокчейн хоть до самой первой записи. Именно этот список и весит сейчас сотни гигабайт и должен быть полностью скачан на все компьютеры, которые хотят принимать участие в работе сети (но чтобы просто создавать транзакции и переводить деньги, это не обязательно). Скачивается он так же со всех ближайших компьютеров сети, как будто вы качаете сериал с торрентов, только новые новые серии в нём выходят каждые 10 минут.



БЛОКИ — ОСНОВА БЛОКЧЕЙНА

Набрав себе транзакций из пула компьютер начинает составлять из них такой же неподделываемый список, как мы в начале поста на доске у себя дома. Только делает он его в виде дерева — хеширует записи попарно, потом результат еще раз попарно и так пока не останется лишь один хеш — корень дерева, который и добавляется в блок. Почему именно деревом — ответа я не нашел, но предполагаю, что так просто быстрее.

В комментариях пояснили почему именно дерево. Потому что появляется возможность удалять ненужные (потраченные) транзакции из блока. Т.е. например есть две транзакции, объединённые хэшом, одна или обе уже не нужны т.к. это уже всё давно отдано другими транзакциями - так вот эти старые можно удалить, а хэш оставить, в итоге ничего не нарушается. См.пункт "7. Reclaiming Disk Space" в оригинальной статье Стоши.

БЛОКИ — ОСНОВА БЛОКЧЕЙНА

БЛОКИ — ОСНОВА БЛОКЧЕЙНА

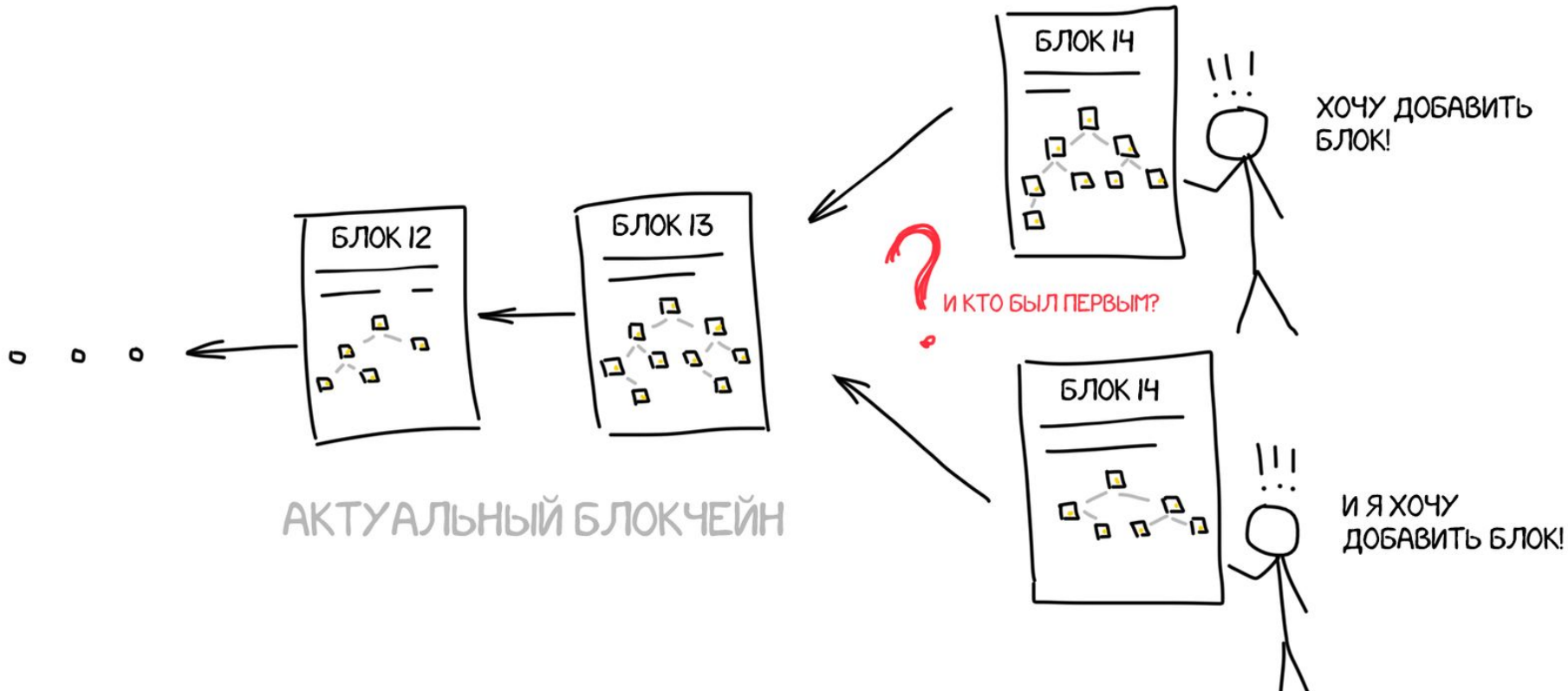
Так как актуальный блокчейн уже скачан, наш компьютер точно знает какой в нём сейчас последний блок. Ему остается только добавить ссылку на него в заголовок блока, захешировать всё это и сообщить всем остальным компьютерам сети «смотрите, я сделал новый блок, давайте добавим его в наш блокчейн».

Остальные должны проверить, что блок построен по всем правилам и что мы не добавили туда лишних транзакций, а затем добавить к себе в цепочки. Теперь все транзакции в нём подтверждены, блокчейн увеличен на один блок и всё идет хорошо?

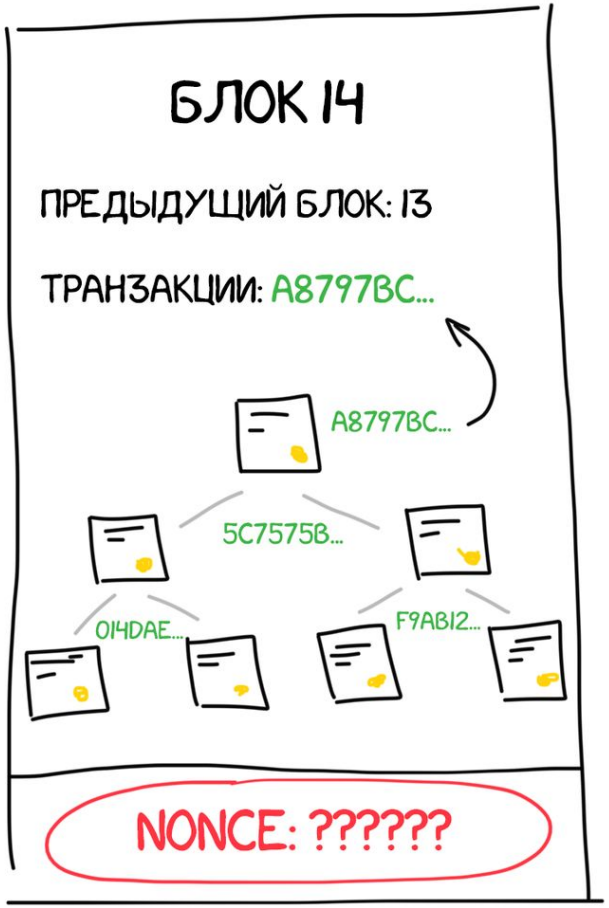
А вот и нет. В сети одновременно работают тысячи компьютеров, и как только они соберут новый блок, они почти одновременно ринутся сообщать всем, что их блок был создан первым. А из предыдущего раздела мы уже знаем, что в децентрализованной сети невозможно доказать кто действительно был первым.

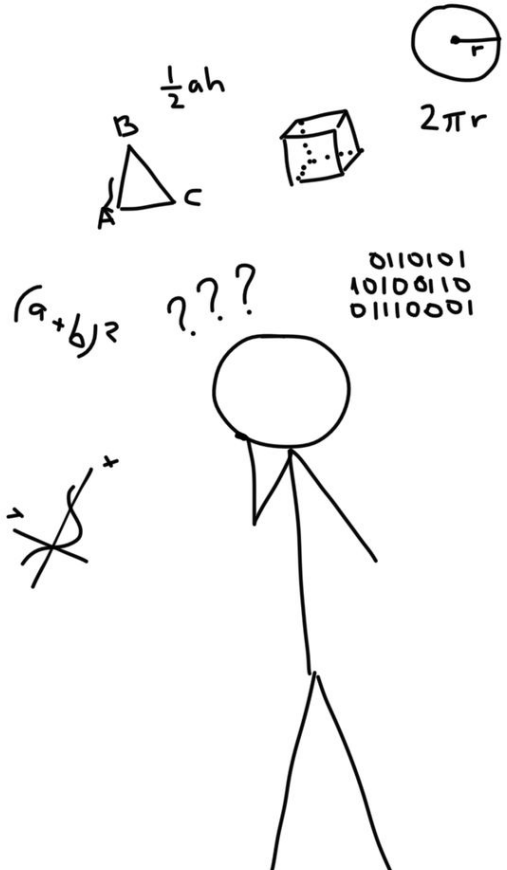
БЛОКИ — ОСНОВА БЛОКЧЕЙНА

- *Поэтому для включения блока в цепочку компьютеры должны решить какую-то сложную задачку, которая займет у них определенное время.*
- Как в школе, когда все решали сложную контрольную, очень редко бывало так, что даже отличники сдавали ответы абсолютно одновременно.



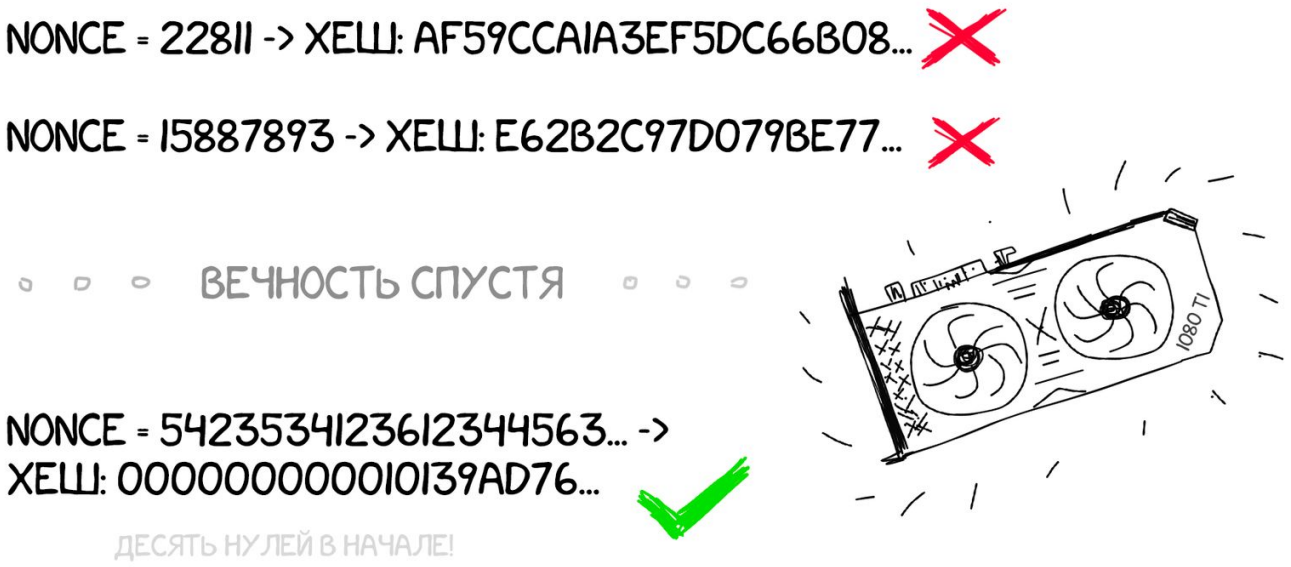
БЛОКИ — ОСНОВА БЛОКЧЕЙНА



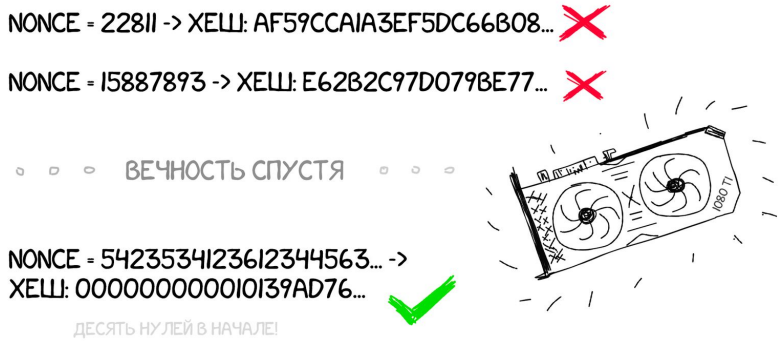


МАЙНИНГ

Майнинг биткоина — не какое-то там священное таинство. Майнинг не связан с поиском новых биткоинов где-то в глубинах интернета. **Майнинг** — это когда тысячи компьютеров по всему миру гудят по подвалам, перебирая миллионы чисел в секунду, пытаясь подобрать хеш, начинающийся на 10 нулей. Им даже не обязательно для этого находиться в сети.



МАЙНИНГ

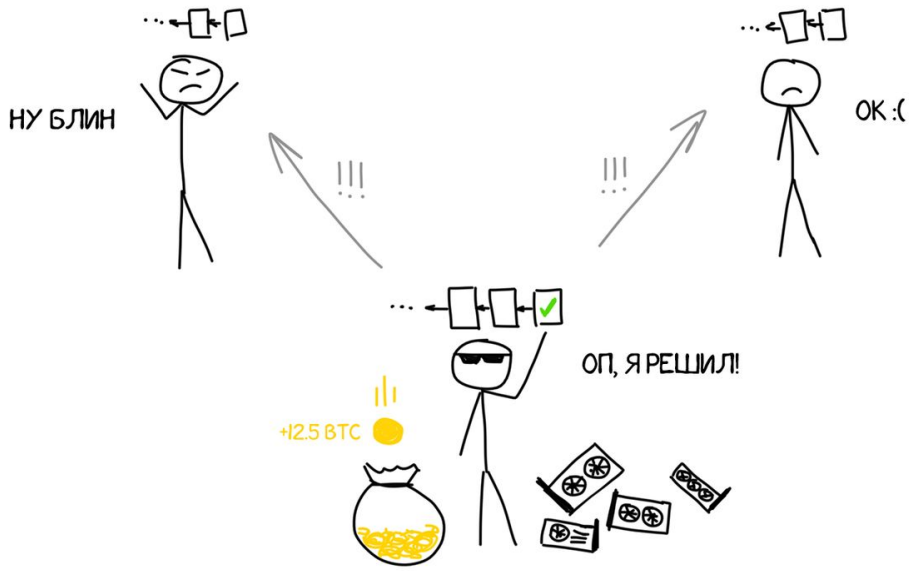


Почему именно на 10 нулей? А просто так, в этом нет никакого смысла. Так придумал Сатоши. Потому что это одна из тех задач, на которую точно всегда есть решение, но оно точно не может быть найдено быстрее, чем долгим монотонным перебором вариантов.

Сложность майнинга напрямую зависит от размера сети, то есть её суммарной мощности. Если вы создадите свой блокчейн и запустите его себя дома на двух ноутбуках, то задача должна быть попроще. Например чтобы хеш начинался только с одного нуля, или чтобы сумма четных разрядов была равна сумме нечетных.

МАЙНИНГ

Чтобы найти начинающийся на 10 нулей хеш, у одного компьютера уйдет несколько десятков лет. Но если объединить тысячи компьютеров в единую сеть и искать параллельно, то по теории вероятностей эта задача решается в среднем за 10 минут. Это и есть время появления нового блока в блокчейне биткоина. Каждые 8-12 минут кто-то на земле находит такой хеш и получает привилегию анонсировать свою находку на всех, избежав тем самым проблемы кто был первым.



МАЙНИНГ

- За нахождение ответа компьютер (по данным на 2017 год) получает 12.5 BTC — это сумма вознаграждения, которая генерируется системой биткоин «из воздуха» и уменьшается каждые четыре года. Технически это означает, что каждый майнер всегда добавляет в свой блок еще одну транзакцию — «создать 12.5 BTC и отправить их на мой кошелек». Когда вы слышите «количество биткоинов в мире ограничено 21 млн, сейчас наймайнили уже 16 млн» — это и есть такие генерируемые сетью вознаграждения.

- *Любой блокчейн существует только пока существуют его майнеры.*

МАЙНИНГ

- Именно майнеры добавляют появляющиеся транзакции в блокчейн. Так что если кто-то рассказывает вам, что он «сделает блокчейн для ***», первый вопрос, на который он должен ответить — кто и зачем будет майнить на нём. Чаще всего правильный ответ — «будут все, потому что за майнинг мы даём наши коины, которые будут расти и майнерам это выгодно». Но это применимо не для всех проектов. Например какой-нибудь Минздрав завтра создает свой закрытый блокчейн для докторов , кто его будет майнить? Терапевты по выходным?

- Но какая выгода майнерам будет потом, когда вознаграждения исчезнут или станут мизерными?

- По задумке Создателя, к тому времени люди должны будут поверить в реальность биткоина и майнинг начнет окупаться суммой комиссий, включенных в каждую транзакцию. К этому всё и идет.
- Еще в 2012 году все комиссии были нулевые, майнеры майнили только за вознаграждения от блоков. Сегодня же транзакция с нулевой комиссией может провисеть в пуле несколько часов, потому что появилась и конкуренция, и люди готовы платить за скорость.

МАЙНИНГ

- Суть майнинга — решить любую вычислительную задачу. Эта задача должна быть достаточно простой, чтобы у участников сети была стабильная вероятность найти ответ — иначе транзакции будут подтверждаться вечность. Представьте, что на кассе в магазине вам надо каждый раз ждать по пол часа, пока банк подтвердит вашу транзакцию. Никто не будет пользоваться таким банком.

- Но задача должна быть одновременно и сложной, чтобы ответ не нашли сразу все пользователи сети. Потому что в таком случае они анонсируют в сеть много блоков с одинаковыми транзакциями и будет вероятность «двойной растраты. Или еще хуже — разделения единого блокчейна на несколько веток, в которых уже никто не сможет разобраться какая транзакция подтверждена, а какая нет.

МАЙНИНГ

- Если награда в 12.5 BTC вручается лишь раз в 10 минут и только одному нашедшему блок, получается надо впустую жечь видеокарты несколько лет в надежде, что однажды упадет $40000 (по текущему курсу)?
- Для биткоина именно так. Но так было не всегда. Раньше сеть была меньше, сложность ниже, а значит и выше вероятность единолично найти хеш для нового блока. Но и биткоин тогда стоил не так дорого.

- Сейчас биткоины в одиночку уже никто не майнит. Теперь участники объединяются в специальные группы — майнинг пулы, где все вместе пытаются найти правильный хеш. Если хоть один из группы находит, то всё вознаграждение делится между участниками в зависимости от их вклада в общую работу. Получается, что ты майнишь и тебе еженедельно падает копеечка от общей доли.

МАЙНИНГ

- Но одиночный майнинг вполне возможен в других сетях. Вот еще недавно было легко майнить Ethereum, где блоки находятся каждые 10 секунд. Вознаграждение за блок там намного ниже, но вероятность заработать копеечку получается выше.

- Значит мы так и будем сжигать тысячи видеокарт впустую и никакого выхода нет?
- Этот майнинг является классическим и называется Proof-of-Work (доказательство работы). То есть каждая машина доказывает, что она работала на благо сети тем, что решает бессмысленные задачки с заданной вероятностью.

БЛОКЧЕЙН

Сейчас вторая по популярности концепция — это Proof-of-Stake (доказательство доли владения). В таком виде майнинга, чем больше «коинов» на счету у участника сети, тем больше его вероятность вставить в блокчейн свой блок. *Как самый громкий парень на деревне.*

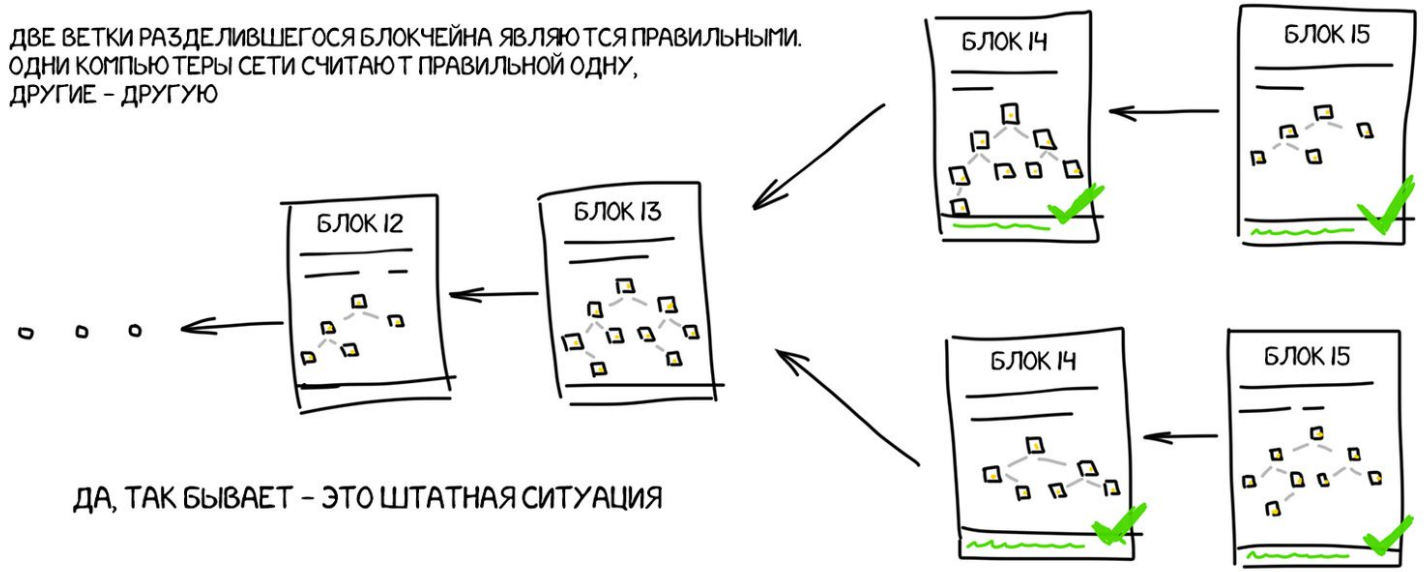
БЛОКЧЕЙН

Представим ситуацию, в которой несмотря на всю нашу теорию вероятностей, два майнера всё равно умудрились одновременно найти правильный ответ. Они начинают рассылать два абсолютно верных блока по сети. Эти блоки гарантировано отличаются, ведь даже если они чудом выбрали одинаковые транзакции из пула, составили абсолютно идентичные деревья и угадали одинаковое Randomчисло (nonce), их хеши всё равно будут разными, так как каждый пропишет в блок свой номер кошелька для вознаграждения.

Теперь у нас есть два валидных блока и снова возникает проблема кого считать первым. Как поведет себя сеть в таком случае?

АЛГОРИТМ БЛОКЧЕЙНА

В алгоритме блокчейна прописано, что участники сети просто принимают первый правильный ответ, который до них дошел. Дальше они живут исходя из собственной картины мира. Оба майнера получат своё вознаграждение, а все остальные начинают майнить, опираясь на последний ими лично полученный блок, отбрасывая все остальные повторно-верные. В сети появляется две версии правильного блокчейна. Та



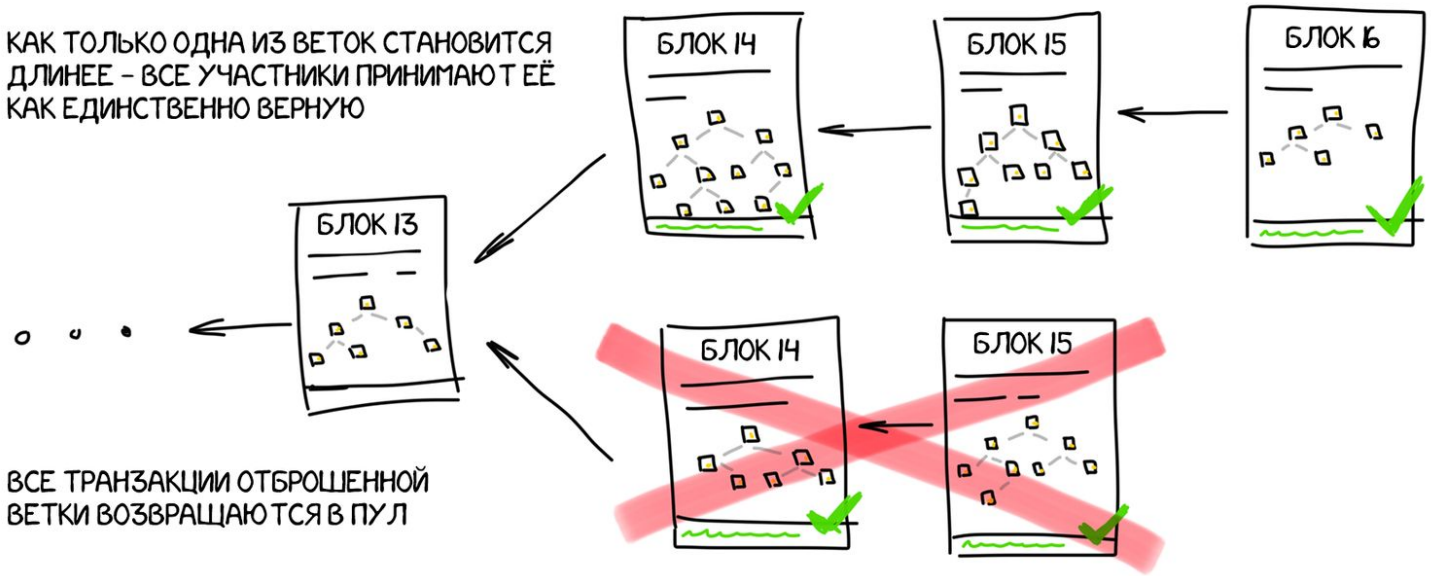
АЛГОРИТМ БЛОКЧЕЙНА

Это штатная ситуация, в которой снова помогает теория вероятностей. Сеть функционирует в таком вот раздвоенном состоянии, пока кто-то из майнеров не находит следующий блок к одной из этих цепочек. Как только такой блок находится и вставляется в цепочку, она становится длиннее и включается одно из соглашений сети блокчейн: **при любых условиях, самая длинная цепочка блоков принимается как единственно верная для всей сети.**

Короткая цепочка, несмотря на всю свою правильность, отвергается всеми участникам сети. Транзакции из неё возвращаются в пул (если они не были подтверждены в другой), а их обработка начинается заново. У майнера пропадает его вознаграждение, потому что его блока больше не существует.

«СБРОС» ЦЕПОЧКИ

С ростом сети такие совпадения из «очень маловероятных» переходят в разряд «ну иногда бывает».



ИЗ-ЗА ЭТОГО БЫЛИ ПРИДУМАНЫ ТРИ ПРАВИЛА БЕЗОПАСНОСТИ ХВОСТА БЛОКЧЕЙНА (END OF CHAIN INSECURITY):

1. Вознаграждениями за майнинг, можно пользоваться только спустя еще 20 подтвержденных блоков после получения. Для биткоина это около трёх часов.

2. Если вам переслали биткоины, использовать их в качестве инпутов в новых транзакциях можно только спустя 1-5 блоков.

3. Правила 1 и 2 всего лишь прописаны в настройках каждого клиента. Никто не следит за их соблюдением. Но закон о самой длинной цепочке всё равно уничтожит все ваши транзакции, если вы попытаетесь обмануть систему, не соблюдая их.

ПЫТАЕМСЯ ОБМАНУТЬ БЛОКЧЕЙН

Можно ли как-то специально обмануть блокчейн, составив самую длинную цепочку самому, тем самым подтвердив свои фейковые транзакции.

ПЫТАЕМСЯ ОБМАНУТЬ БЛОКЧЕЙН

Предположим у вас есть самый мощный компьютер на Земле. Датацентры Google и Amazon вместе взятые в вашем распоряжении и вы пытаетесь просчитать такую цепочку, которая станет самой длинной в сети блокчейн.

ПЫТАЕМСЯ ОБМАНУТЬ БЛОКЧЕЙН

Вы не можете взять и сразу просчитать несколько блоков цепочки, ведь каждый следующий блок зависит от предыдущего. Тогда вы решаете как можно быстрее считать каждый блок на своих огромных датацентрах параллельно с тем, как все остальные участники продолжают увеличивать основной блокчейн. Возможно ли их обогнать? Вероятно, да.

Если ваша вычислительная мощность будет составлять больше 50% от мощности всех участников сети, то с вероятностью 50% вы сможете построить более длинную цепочку быстрее всех остальных вместе взятых. Это теоретически возможный способ обмануть блокчейн, просчитав более длинную цепочку транзакций. Тогда все транзакции настоящей сети будут считаться неверными, а вы соберете все вознаграждения и начнете новую веху в истории криптовалюты, которая называется «разделение блокчейна». Однажды из-за бага в коде так было с Ethereum.

РЕЗЮМЕ

Но в реальности ни один датацентр не сравнится по мощности со всеми компьютерами в мире. Никто в мире пока не может составить конкуренцию в одиночку, даже Google.

Это примерно как выйти на улицу и пытаться убедить каждого человека в мире, что доллар теперь стоит 1 рубль и успеть до того, как в СМИ вас разоблачат. И вот если вы умудритесь убедить всех, то сможете обвалить мировую экономику. В теории ведь это возможно? Но на практике почему-то ни у кого не получалось.

ETHEREUM

«Эфиры» — второе по популярности слово, которое вы слышите в новостях о криптохайпе, после биткоина. Для обывателей это еще одна криптовалюта и способ делать ICO.

Разработчики описывают Ethereum как «конструктор блокчейнов для ваших нужд».

Это не просто сеть с монетками. Это огромная общемировая вычислительная машина, где пользователи исполняют код чужих программ (смарт-контрактов), получая за каждую выполненную строчку вознаграждение. И всё это децентрализованно.

ВОПРОСЫ

1. Курс Эфириума онлайн
2. Обменные пункты Ethereum
3. Что я могу сделать с Ethereum сегодня?
4. Как мне получить эфир?
5. Какой кошелек?
6. Как работает Ethereum