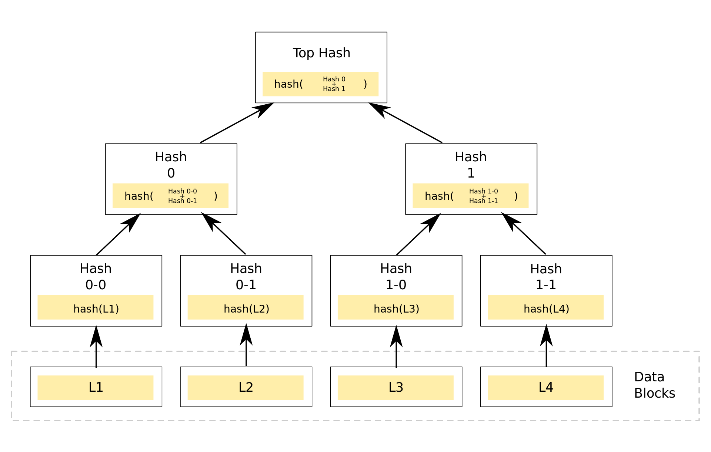
31 октября 2008 года несколько сотен энтузиастов и специалистов по криптографии, включенных в закрытый список e-mail рассылки (The Cryptography Mailing list) на сайте [metzdowd.com](http://metzdowd.com/), получили письмо, подписанное неким Сатоши Накамото (*Satoshi Nakamoto*). В нём он сообщил, что работает над созданием новой электронной системы денежных расчетов, в которой операции производятся непосредственно между участниками без привлечения третьей доверенной стороны.

В письме содержалась ссылка на короткий текст (9 страниц) доклада под названием [Bitcoin: A Peer-to-Peer Electronic Cash System](https://bitcoin.org/bitcoin.pdf) («Биткоин: Одноранговая электронная денежная система»), в котором в строгом академическом стиле, кратко, но ясно, со схемами и формулами описывалась технология новой денежной системы, названная автором Биткоином.

На сегодняшний день, сложно найти того, кто еще не слышал ничего про эту нашумевшую криптовалюту. Однако явление Биткоина - только верхушка айсберга. Ее концепт основывается на такой структуре данных как Blockchane. Впервые, упоминание криптоустойчивых цепочек блоков было описанно еще в 1991 году в статье How To Time-Stamp a Digital Document by Stuart Haber and W. Scott Stornetta, а затем в 1992 Bayer, Haber and Stornetta в своей статье Improving the Efficiency and Reliability of Digital Time-Stamping внедрили в блокчейн дерево Меркла, так же известное как древовидное хеширование – структура данных, в которой хеши всех включенных элеметнов помещаются в листья бинарного дерева, а затем считаются хеши каждой пары хешей предыдущего уровня, пока не образуется один корневой хеш, зависимый от всех включенных эллементов (см. Рисунок 1).

Рисунок 1. Дерево Меркла и демонстрация алгоритма его постраения на примере 4 элементов



Преимущество такого подхода дает возможность проверить включен ли определенный элемент в дерево с логарифмической сложностью:

например, имея 16 элементов (см. рисунок 2), нам необходимо знать всего 4 промежуточных хеша и сделать всего 4 итерации

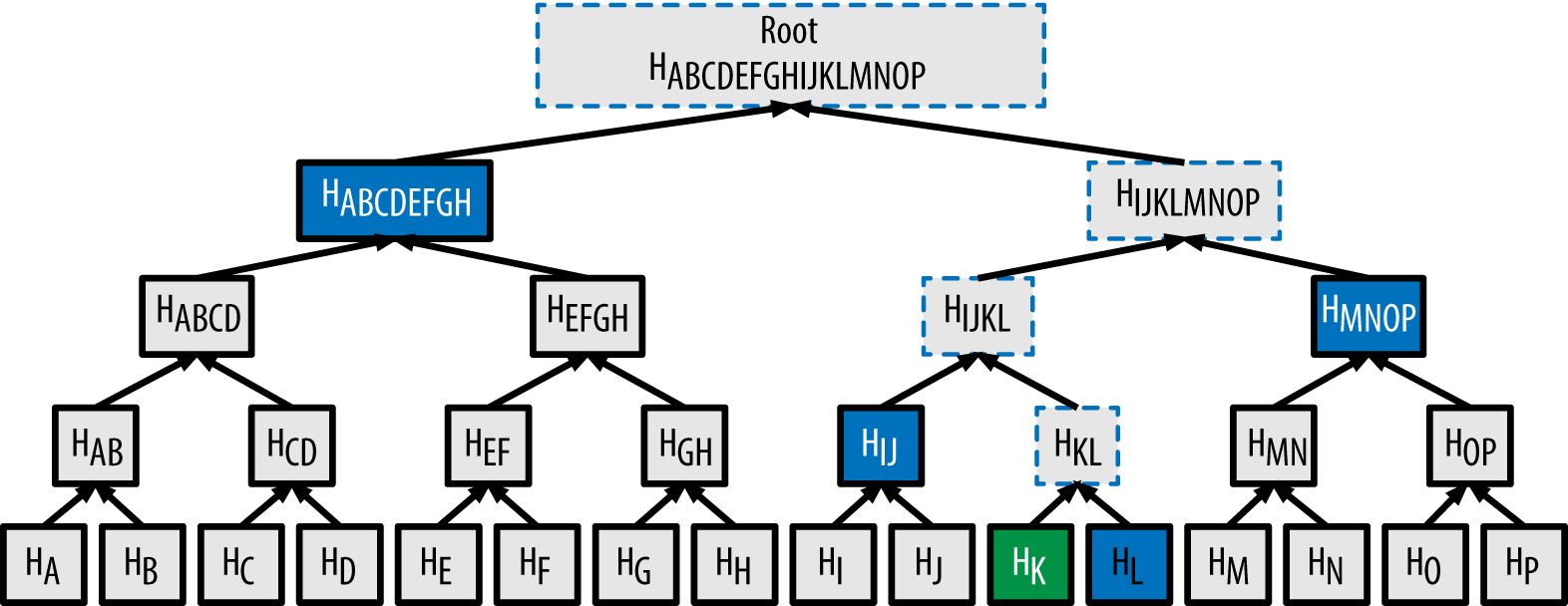


Рисунок 2. Дерево Меркла для 16 элементов и демонстрирация количества необходимой информации и количество итераций для проверки включения одного из элементов.

Это позволило эффективно собирать несколько документов в один блок. Это и стало началом того блокчейна, который сейчас набирает попюлярность с невероятной скоростью.

«Блокчейн – это неподкупная цифровая учетная книга экономических транзакций, которая может быть запрограммирована на запись не только финансовых транзакций, но и практически любых ценностей» [Don & Alex Tapscott, authors Blockchain Revolution (2016)]

Другими словами - это последовательная цепочка блоков, содержащих информацию, с жестким правилом: что каждый блок хранит хеш предыдущего, таким образом изменение блока внутри цепи затрагивает каскадное изменение всех последующих блоков. Таким образом, с помощью Blockchain формируются журналы, которые невозможно модифицировать (запись, попавшую в такой журнал уже нельзя ни изменить, ни удалить).

Отсюда всплывает возможность создания децентрализованных структур хранения немодифицируемых журналов транзакций. При этом под транзакцией может пониматься что угодно: финансовая транзакция (перевод между счетами), аудит событий аутентификации и авторизации, записи о выполненных ТО и ТУ автомобилей. В такой структуре событие считается случившимся, если запись о нём включена в журнал.

В такой системе существует 3 роли:

* Источник транзакций – участник сети который добавляет новую информацию в сеть (привилегированный пользователь)
* Источник блоков - участник сети, поддерживающей ее работоспособность за некое вознаграждение (их так же называют майнерами)
* Наблюдатель – участник сети который только получает существующие блоки и транзакции (обычный пользователь)

В зависимости от реализации Blockchain, эти роли могут пересекаться.

Но чтобы действительно понять - что такое Blockchain, нужно сперва разобраться как реализуется запрет модификации. Его основа – это криптографически стойкая хеш-функция и алгоритмы шифрования с открытым ключем (так же известные как алгоритмы асимметричного шифрования).

Криптографически стойкая хеш-функция – это такая функция, которая обладает 3 основным критериям:

* Необратимость или стойкость к [восстановлению прообраза](https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%D0%BD%D0%B0%D1%85%D0%BE%D0%B6%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BF%D1%80%D0%BE%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%B0): для заданного значения хеш-функции m не должен быть вычислен блок данных X, для которого: H(X) = m
* Стойкость к [коллизиям](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BB%D0%BB%D0%B8%D0%B7%D0%B8%D1%8F_%D1%85%D0%B5%D1%88-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D0%B8) первого рода или восстановлению вторых прообразов: для заданного сообщения M должно быть вычислительно невозможно подобрать другое сообщение N, для которого H(M) = H(N)
* Стойкость к коллизиям второго рода: должно быть вычислительно невозможно подобрать пару сообщений (M, M') имеющих одинаковый хеш H(M) = H(M')

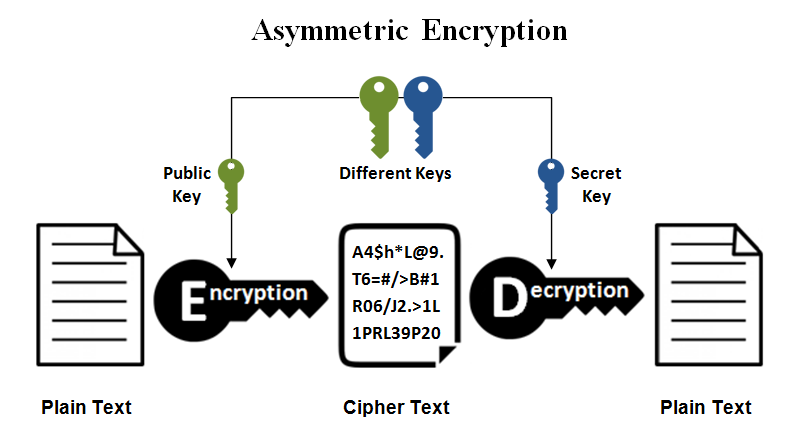
Эти функция используется, во-первых, для того, чтобы включить в блок набор транзакций, из существующих транзакций составляется дерево Меркла, корень которого и хранится в блоке.

Во-вторых, для того, чтобы сформировать хеш предыдущего блока и поместить в новый.

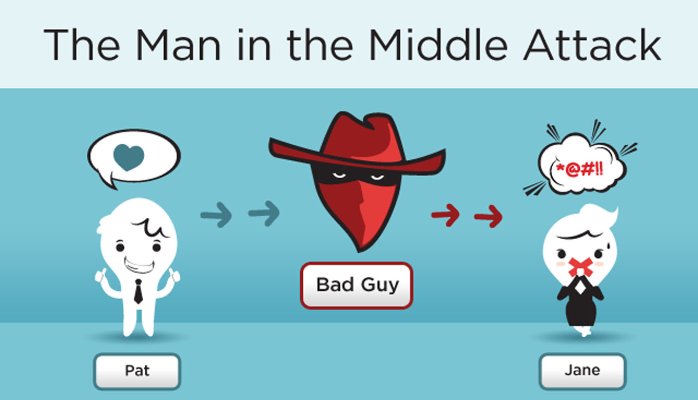
В-третьих – для формирования электронной подписи для транзакций, для подтверждения права ее регистрации.

И в-четвертых, в случае доказательства выполнением работы (принцип Proof-of-work о котором мы поговорим позже).

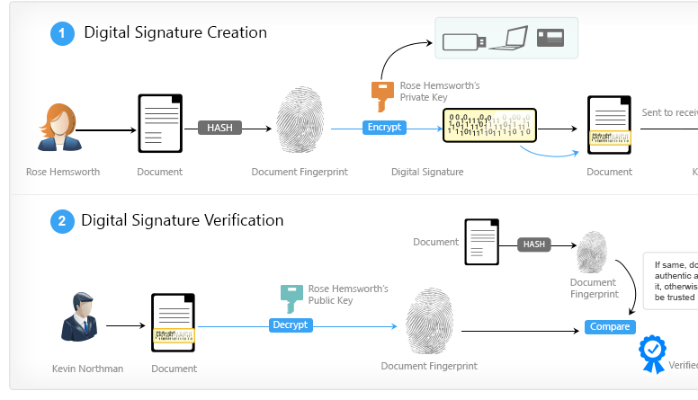
Системы шифрования с открытым ключем – это такие системы, которые используют пару ключей: публичный (он же - открытый ключ, тот который предоставляется пользователем системы всем желающим) и приватный (он же – закрытый ключ, тот который пользователь системы хранит только у себя), и основываются на односторонних функциях. Один из ключей может только зашифровывать текст, а другой расшифровывать. В зависимости от того где и как используется система шифрования, публичным ключем может быть и зашифровующий (для передачи зашифрованных документов), так и разшифровующий (для проверки заверения электронной подписью).



При обмене зашифрованными сообщениями – публичный ключ помещается в открытый источник, и любой желающий написать с помощью него шифрует свое сообщение. Получатель дешифрует это сообщения своим приватным ключем, тем самым получает исходное сообщение. Такой вид шифрования защищает от атаки Man-in-the-middle (так же известная как Атака посредника – вид атаки, когда в общение 2 пользователей через открытый канал связи может вмешаться третий участник и читать и/или изменять проходящие через него сообщения)

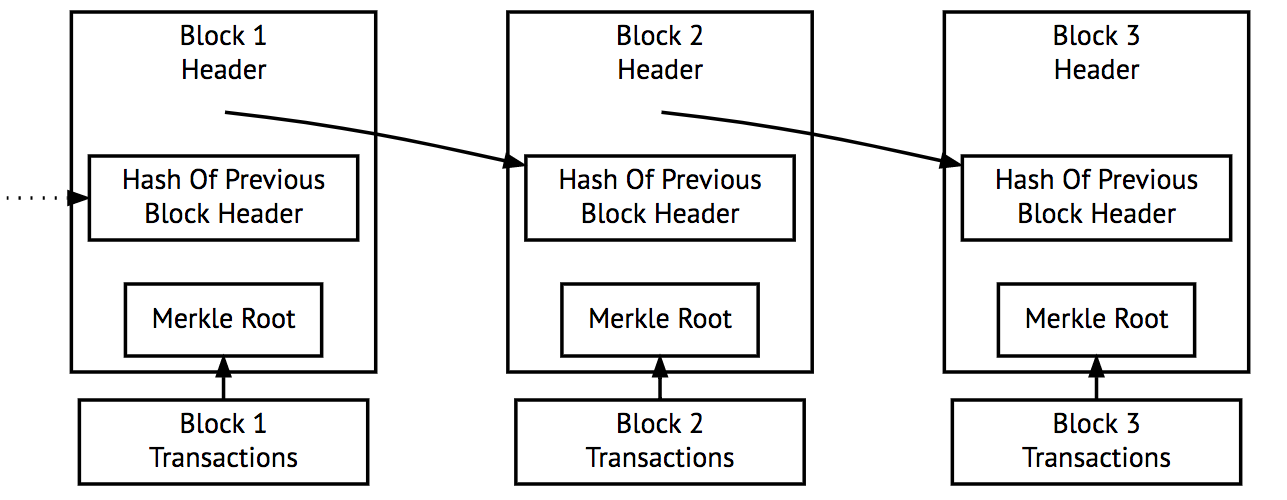


Электронная подпись – это схема демонстрации подлинности цифрового сообщения. Для ее формирования формируется хеш документа, этот хеш шифруется приватным ключом пользователя, полученная подпись прикладывается к документу вместе с открытым дешифрующим ключом. Таким образом любой желающий может взять публичный ключ, расшифровать подпись, сформировать хеш исходного документа, и сравнить их. Если они идентичны – то значит и документ не мог подвергнуться модификации.



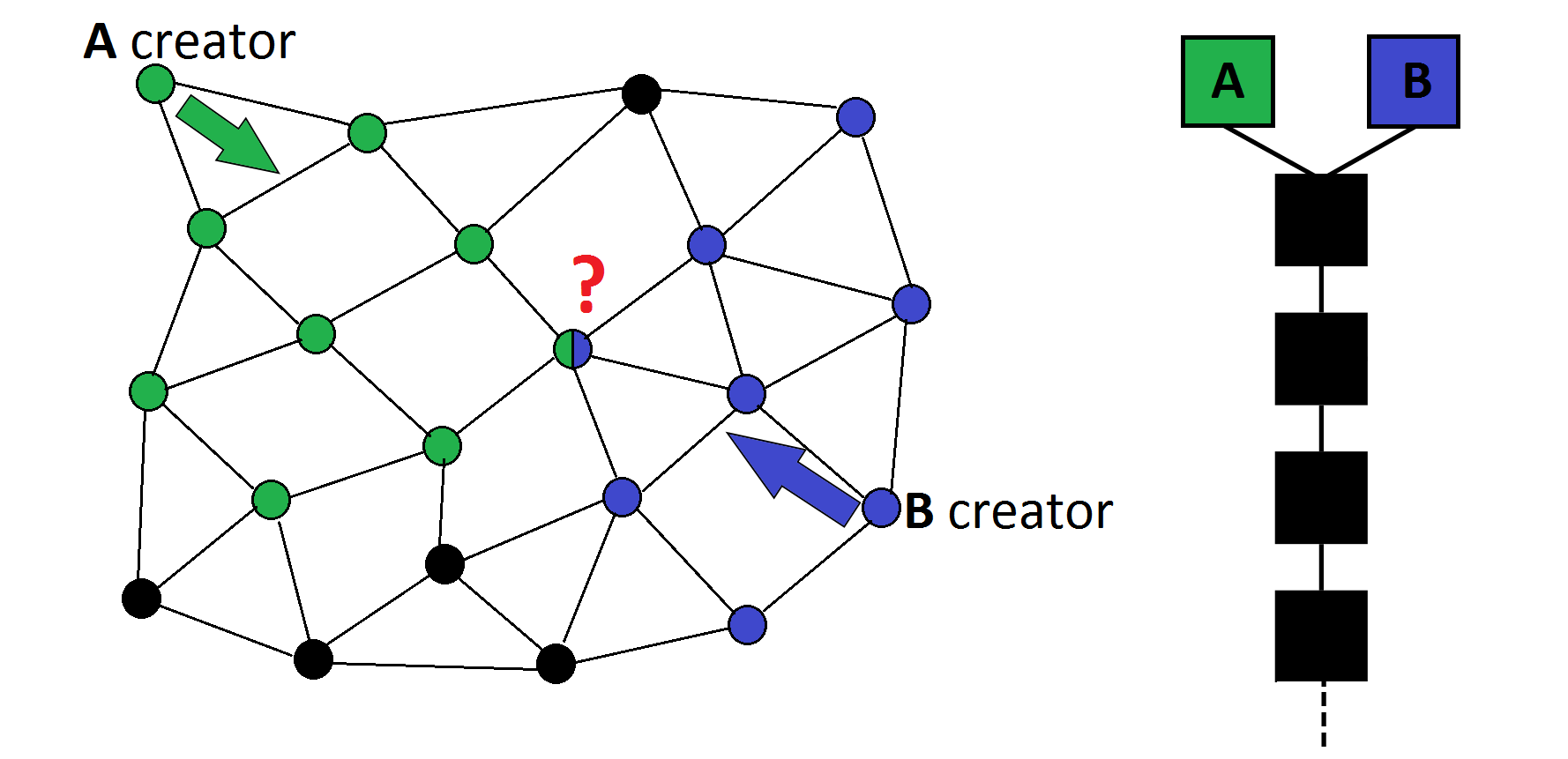
Ассиметричные алгоритмы используются, как уже упоминалось выше (вместе с хешированием) – для формирования электронной подписи транзакций для подтверждения права их регистрации.

Так же, важным фактором системы, работающей на цепочке блоков - является ее децентрализованность, что значит что версия блокчейна хранится у каждого пользователя сети. Пользователи – источники транзакций формируют новые транзакции и отправляют их в некий пул транзкций ожидающих подтверждения. Майнеры собирают эти транзакции и формируют новый блок, который состоит из хеша предыдущего блока, списка включенных транзакций, и корневого хеша дерева Меркла для всех включенных транзакций.



После того как блок сформирован, сформировавший его майнер разсылает его всем участникам сети к которым у него есть непосредственный доступ. Каждый участник сети, который получил этот новый блок сперва проверяет его валидность (вычисляет хеш предыдущего блока, и сравнивает его с указанным в новом, рассчитывает дерево меркла и сравнивает его корень с полеченным в новом блоке), и если оно валидно – то разсылает его всем участникам сети.

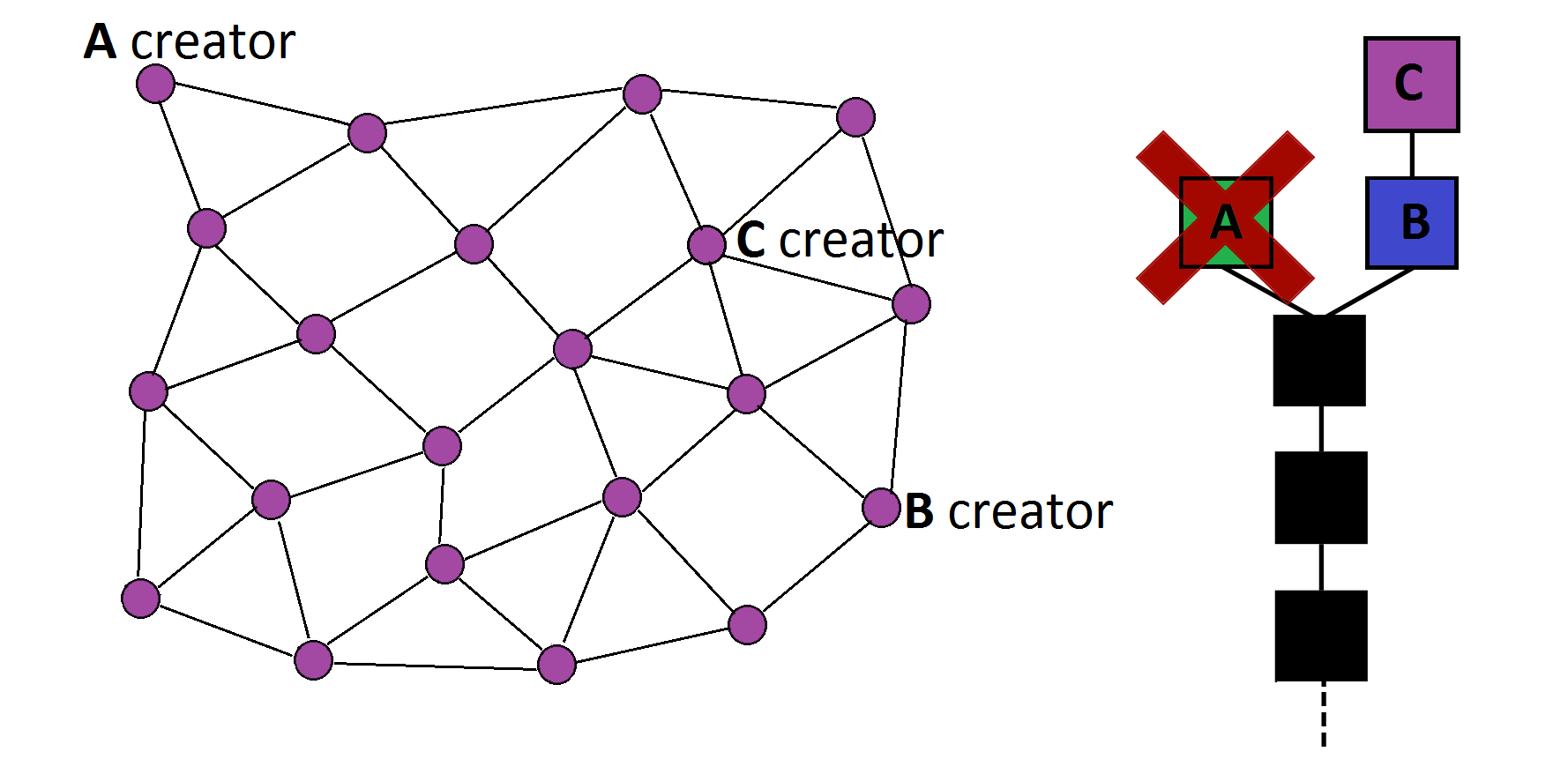
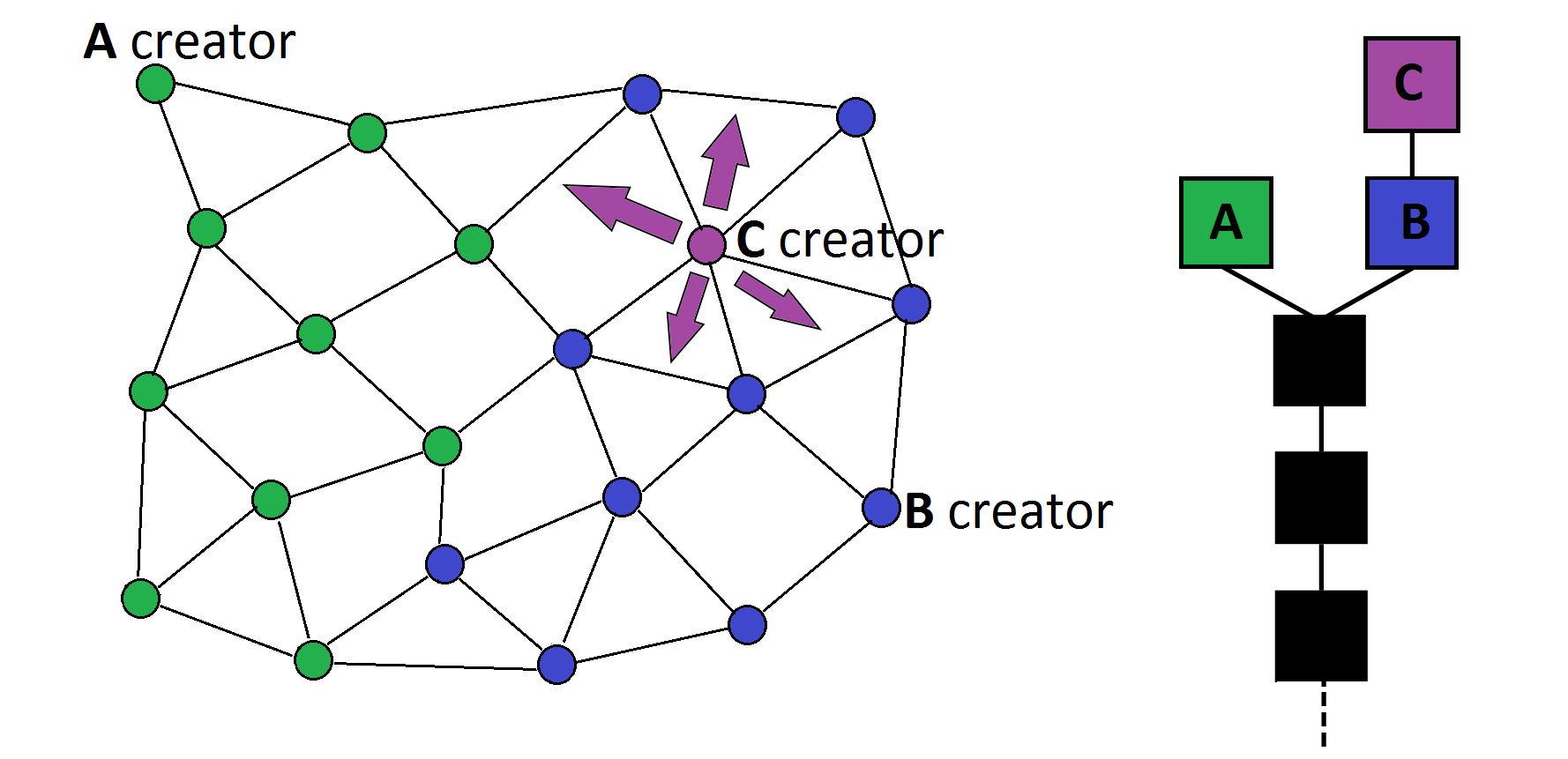
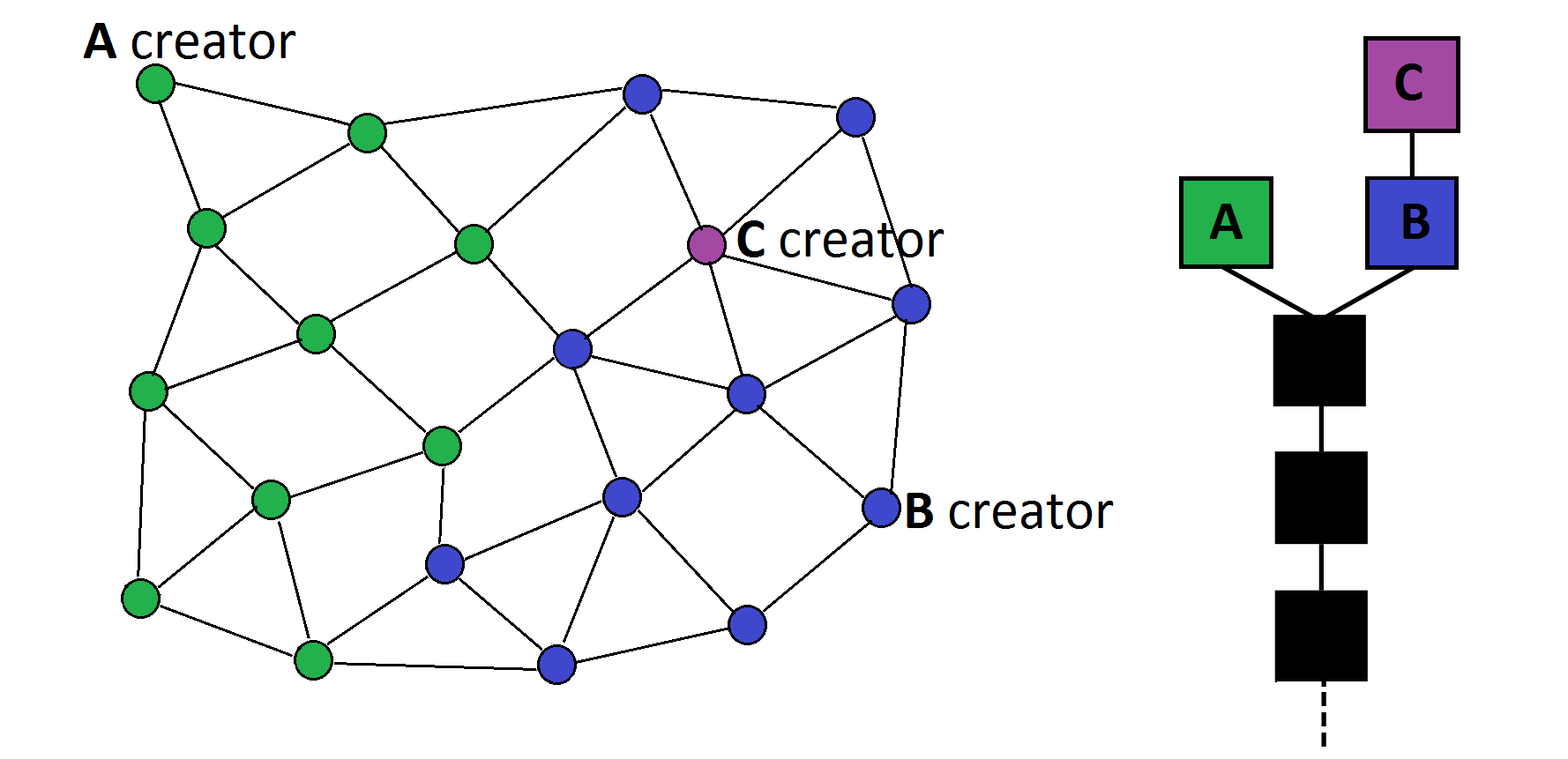
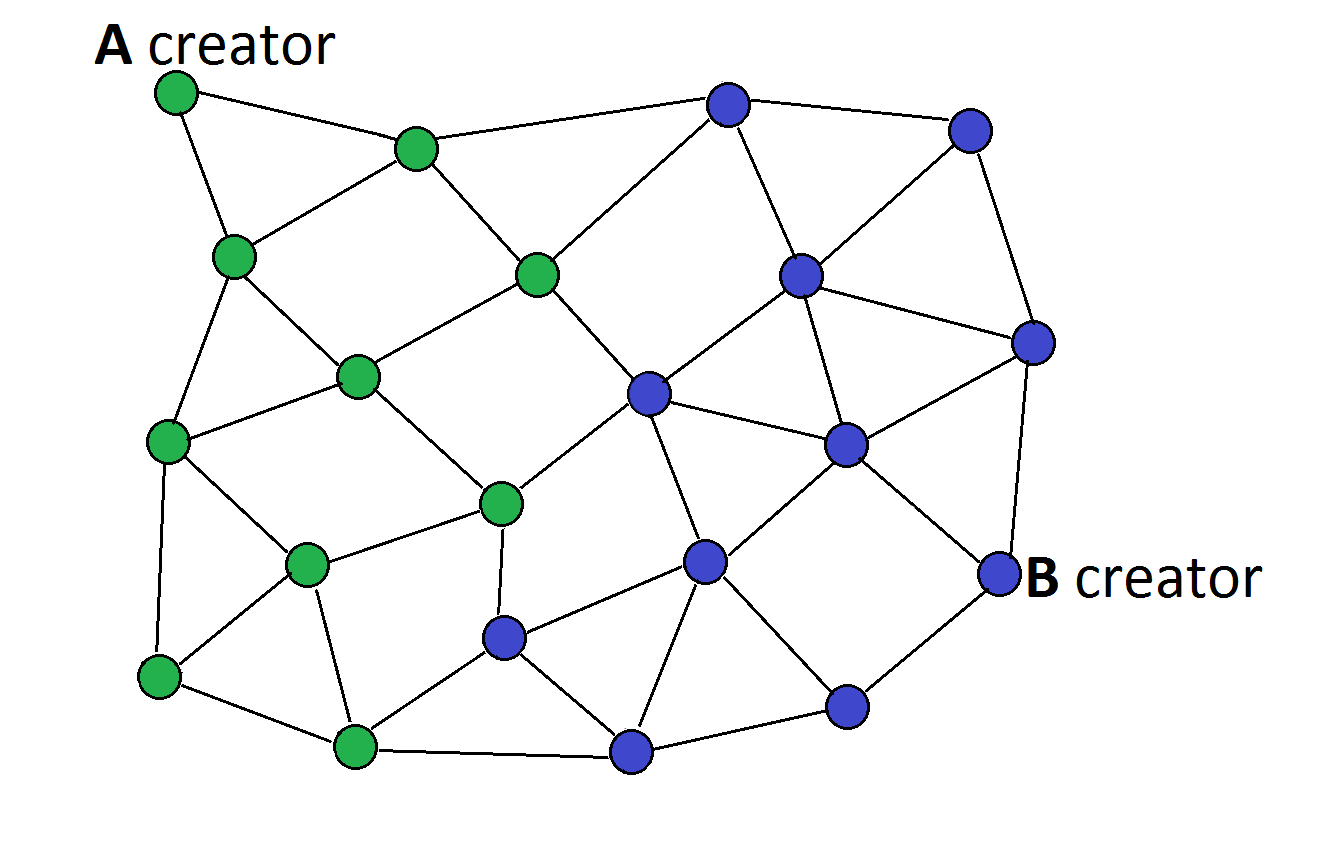
Однако может случиться так, что одновременно (или условно одновременно, по сравнению со временем передачи блока) два, или более майнеров соберут новый блок и начнут из разных сторон сети разсылать эти блоки



Возникнет «неразбериха» какой блок использовать за истинный, ведь в разные блоки могут быть включенны разные транзакции.

Разрешается эта проблема таким правилом: Актуальной версией цепи считается та, которая длинее, при одинаковой длине – та которая пришла раньше. Таким образом в этом случае сеть делится на части с разным верхним блоком.

И затем, первый кто смайнит следующий блок и определит какую ветку считать за истинную, так как его версия цепи остальными пользователями примется за истинную по правилу наибольшей длины.



Однако, что мешает злоумышленнику сфальсифицировать несколько новых блоков и разослать их как валидные блоки наибольшей длины? А мешает ему механизмы заверения блоков. Существует 2 основных алгоритма консенсуса:

Proof-of-Work и Proof-of-Stake.

Суть их в том, чтобы создать блок мог не кто-попало, а какой-либо «уважаемый» или «доверенный» участник сети. Однако, как можно доверять кому-либо в анонимной сети?

Для этого анонимному пользователю нужно как-то доказать свою уважаемость, делается это экономическим фактором. Тут и вступают в силу алгоритмы консенсуса: Первый - Proof-of-Work, заключается в том, что майнер создающий блок, должен выполнить какую-либо сложную задачу, дабы доказать, что он обладает дорогостоящим оборудованием. Второй - Proof-of-Stake, заключается в том, что приоритет заверения блока отдается тому, кто обладает большим виртуальным капиталом.

Добавить:

\*Криптовалюта – основы криптоэкономики, зачем нужна в среде – манипуляции с транзакциями

\*Умные контракты – концепт, примеры применения

# \*Etherium и solidity, другая парадигма разработки - Move Fast and Break Things (где подразумевается быстрая разработка как попало, и фикс после релиза) высказанная Jonathan Taplin не подходит

# \*Прозоро – перенести платформу на смарт контракты и децентрализовать