Розсоховатский Владимир Владимирович, Корниловска Наталья Владимировна, Лурье Ирина Анатольевна Херсонский национальный технический институт, г. Херсон, Украина, 2018 год

**Основы технологии Blockchain и концепты ее практического применения.**

***В работе рассматриваются основные принципы работы технологии Blockchain и возможности применения данной технологии в различных сферах структуры.***

**Введение**

31 Октября 2008 года, несколько сотен энтузиастов и специалистов по криптографии, включенных в закрытый список e-mail рассылки (The Cryptography Mailing list (Криптографическая рассылка) на сайте metzdowd.com, получили письмо, подписанное неким Satoshi Nakamoto(Сатоши Накамото). 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 доклада под названием Bitcoin: A Peer-to-Peer Electronic Cash System («Биткоин: одноранговая электронная денежная система»), в которой кратко описывалась технология новой денежной системы, названная автором Bitcoin (Биткоин).

Блокчейн берет свое начало из пиринговых сетей, для которых впоследствии Брэн Коэн добавил распределенные хэш-таблицы и таким образом реализовал BitTorrent. Биткойн используя достижения BitTorrent и решив проблему децентрализованного консенсуса, создал первый блокчейн.

Основой для транзакций с новыми электронными деньгами стала система блокчейн. Впервые термин «Блокчейн» появился как название распределённой базы данных, реализованной в криптовалюте «биткойн».

Блокчейн – это база данных, хранящая все когда-либо совершенные транзакции в виде публично доступных блоков информации. Копии этой базы хранятся в каждом биткоин-кошельке каждого владельца биткоинов. Всякий раз, когда происходит транзакция с биткоинами, информация о ней проверяется и записывается в эту базу. Необходимо это для того, чтобы невозможно было отправить один и тот же платеж двум разным людям одновременно.

В дальнейшем развитие данной технологии начало движение семимильными шагами.

В докладе Всемирного экономического форума (ВЭФ) дано следующее определение технологии блокчейн (blockchain) или технологии распределенного реестра (distributed ledger technology – DLT): это технологический протокол, который позволяет обмен данными напрямую между различными договаривающимися сторонами внутри сети без необходимости в посредниках [5]. Участники сети взаимодействуют с зашифрованными идентификаторами (анонимно); каждая транзакция затем добавляется к неизменяемой цепочке транзакций и распределяется по всем сетевым узлам. По мнению аналитиков ВЭФ, технологии блокчейн могут стать драйвером радикальных изменений в широком спектре отраслей, бизнес-моделей и операционных процессов, таких как расчет платежей, учет или использование карт клиентов и лояльности.

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 («Как подписывать документы временной меткой» Стюарта Хабера и У. Скотт Сторнетта), а затем в 1992 Bayer, Haber and Stornetta (Байер, Хабер и Сторнетта) в своей статье «Improving the Efficiency and Reliability of Digital Time-Stamping» (Совершенствование эффективности и надежности цифровой временной метки) внедрили в блокчейн дерево Меркла, так же известное как древовидное хеширование, которое основывается на криптографических хеш функциях.

Как известно - хеш функция (До начала 1990-х годов в русскоязычной литературе в качестве эквивалента термину «хеширование», благодаря работам Андрея Петровича Ершова, использовалось слово «расстановка»), это любая функция, которая отображает данные произвольного размера в данные фиксированной длины.

Криптографически стойкой хеш функцией называют такую хеш функцию, которая обладает 3 основными критериями:

* Необратимость или стойкость к восстановлению прообраза: для заданного значения хеш-функции m не должен быть вычислен блок данных X, для которого: H(X) = m

Другими словами, невозможно (кроме полного перебора) подобрать исходное сообщение, зная его хеш.

* Стойкость к коллизиям первого рода, или восстановлению вторых прообразов: для заданного сообщения M, должно быть вычислительно невозможно подобрать другое сообщение N, для которого H(M) = H(N)

Другими словами, невозможно (кроме полного перебора) подобрать сообщение, отличное от исходного, хеш которого будет равен хешу исходного.

* Стойкость к коллизиям второго рода: должно быть вычислительно невозможно подобрать пару сообщений (M, M') имеющих одинаковый хеш: H(M) = H(M').

Другими словами, невозможно (кроме полного перебора) подобрать 2 сообщения, у которых будет одинаковый хеш.

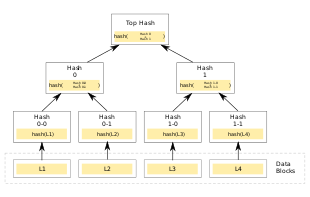
Полный перебор, в случае для наиболее используемой хеш функции SHA-256 потребует 2^256 итераций.

Самые сильные майнеры, обладают вычислительными мощностями порядка Терахешей (1 000 000 000 000) в секунду. И даже при такой вычислительной мощности, понадобится порядка 10^59 лет, что несоизмеримо больше нынешнего возраста вселенной (10^10).

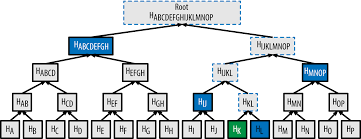
Такой алгоритм шифрования ещё называют Хэш-деревом или Деревом Мэркла.

Дерево Меркла – структура данных, в которой хеши всех включенных элементов помещаются в листья бинарного дерева, а затем считаются хеши каждой пары хешей предыдущего уровня, пока не образуется один корневой хеш, зависимый от всех включенных элементов (см. Рисунок 1).

**Рисунок 1.** Дерево Меркла и демонстрация алгоритма его построения 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 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. И следовательно , с помощью Blockchain формируются журналы, которые невозможно модифицировать (запись, попавшую в такой журнал уже нельзя ни изменить, ни удалить).

Благодаря этому появляется возможность создания децентрализованных структур хранения немодифицируемых журналов транзакций. Под транзакцией может пониматься что угодно: финансовая транзакция (перевод между счетами), аудит событий аутентификации и авторизации, записи о выполненных ТО и ТУ автомобилей.

Они распространяются на сферы государственного управления, здравоохранения, науки, образования, культуры и искусства [7]. Основной и главной особенностью блокчейна является использование алгоритмов математического вычисления, а также исключение «человека» и человеческого фактора при принятии решения системой [5]. Хотя в настоящее время большинство блокчейнов обрабатывают финансовые транзакции, в общем случае последние можно рассматривать просто как атомарные изменения состояния некоторой системы. Например, блокчейн может использоваться для регистрации документов и защиты их от изменений.

Все транзакции в блокчейне хранятся в едином реестре. Так как транзакции полностью упорядочены по времени, текущее состояние системы (набор балансов пользователей в случае финансового блокчейна) определяется исключительно этим реестром транзакций. Хранение полной истории изменений состояния системы имеет свои преимущества, например возможность определить состояние системы в произвольный момент времени, просто «проиграв» заново соответствующие транзакции. В идеальном случае обработка транзакций в рамках блокчейн-технологии должна удовлетворять следующим свойствам:

— транзакции должны быть согласованы с текущим состоянием системы, т. е. в случае финансовых транзакций если баланс некоторого индивидуума А составляет 1000 ед., он не может перевезти индивидууму В 10 000 ед.;

— транзакции должны быть авторизованы, т. е. только у А должен быть ключ к осуществлению транзакций от имени А;

— транзакции должны быть неизменяемыми, т. е. после того как транзакция записана в реестр, ее невозможно изменить (например, если в реестре записана транзакция, в которой А перевёл В 100 ед., у злоумышленника не должно быть возможности изменить количество единиц, его отправителя или получателя);

— транзакции должны быть конечными, т. е. после того как транзакция записана в реестр, ее невозможно оттуда удалить, что, по сути, привело бы к возврату отправленных единиц отправителю;

— устойчивость к цензуре, т. е. если транзакция удовлетворяет всем правилам блокчейна, она должна быть в конце концов в него добавлена.

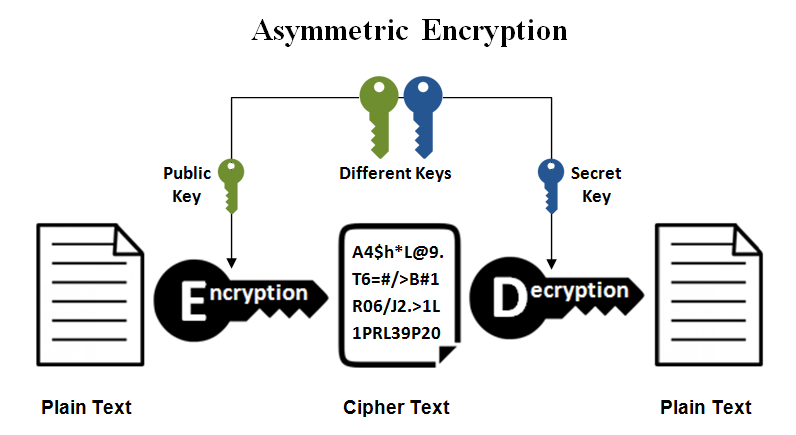
Соответствие текущему состоянию системы удовлетворяется за счет проверки транзакции совместно с этим состоянием, хранящимся в защищенной от злоумышленников памяти. Поскольку текущее состояние системы можно восстановить при помощи блокчейна, предположение защищенности не сужает безопасность системы в целом. Это предположение вводит ограничение на блокчейн, которое заключается в организации хранения транзакций таким образом, чтобы надежная верификация транзакций занимала не слишком много времени. Для финансовых блокчейнов один из возможных способов такой организации:

— использование непотраченных выходов транзакций (англ. unspent transaction outputs, UTXO) вместо явно заданных балансов пользователей. Состояние системы в таком случае фактически представляет собой реестр владения, который содержит информацию об условиях, определяющих владельца каждой единицы активов, циркулирующих в системе. Проблема авторизации решается за счет использования криптографии с открытым ключом [9]. Каждому пользователю системы выдается пара из секретного и открытого ключа; открытый ключ может быть без проблем опубликован для определения цифровой личности пользователя, так как секретный ключ невозможно вывести из открытого. Например, если А желает перевести 100 ед. В, он (или его доверенный агент) подписывает соответствующую транзакцию цифровой подписью, использующей его секретный ключ. Поскольку:

— корректная подпись может быть сделана исключительно лицом, знающим секретный ключ А;

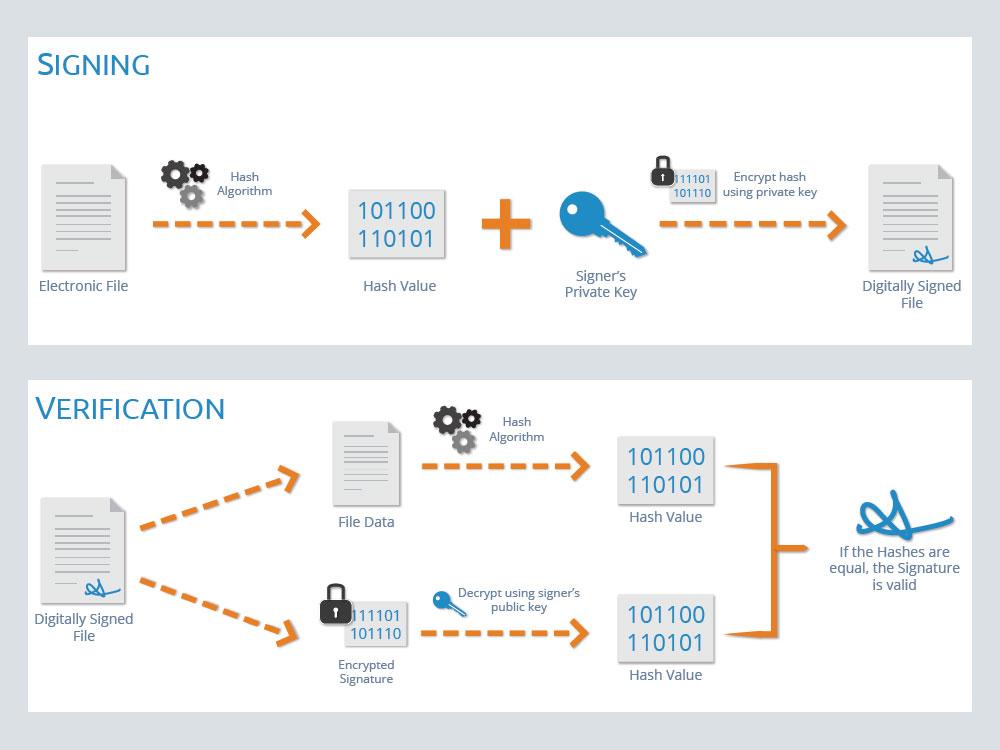
— для проверки подписи достаточно знания открытого ключа А;

— подпись становится некорректной при изменении какого-либо из параметров подписываемой транзакцию



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)

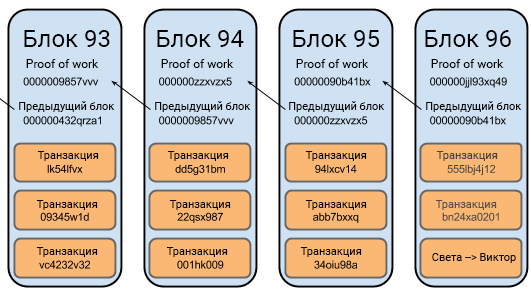
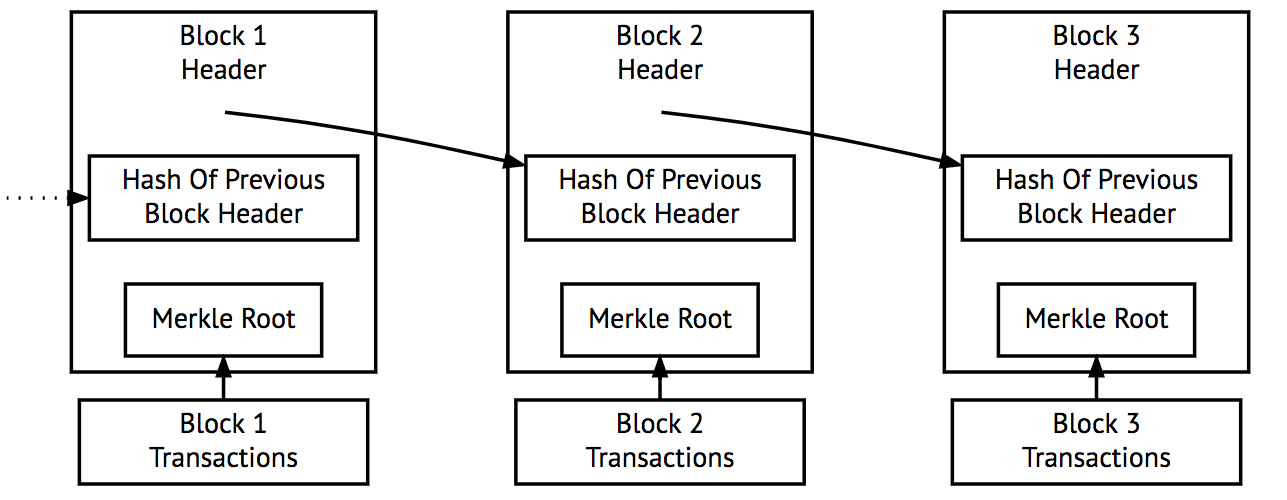
Электронная подпись – это схема демонстрации подлинности цифрового сообщения. Для ее формирования формируется хеш документа, этот хеш шифруется приватным ключом пользователя, полученная подпись прикладывается к документу вместе с открытым дешифрующим ключом. Таким образом любой желающий может взять публичный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



Если они идентичны – то значит и документ не мог подвергнуться модификации.

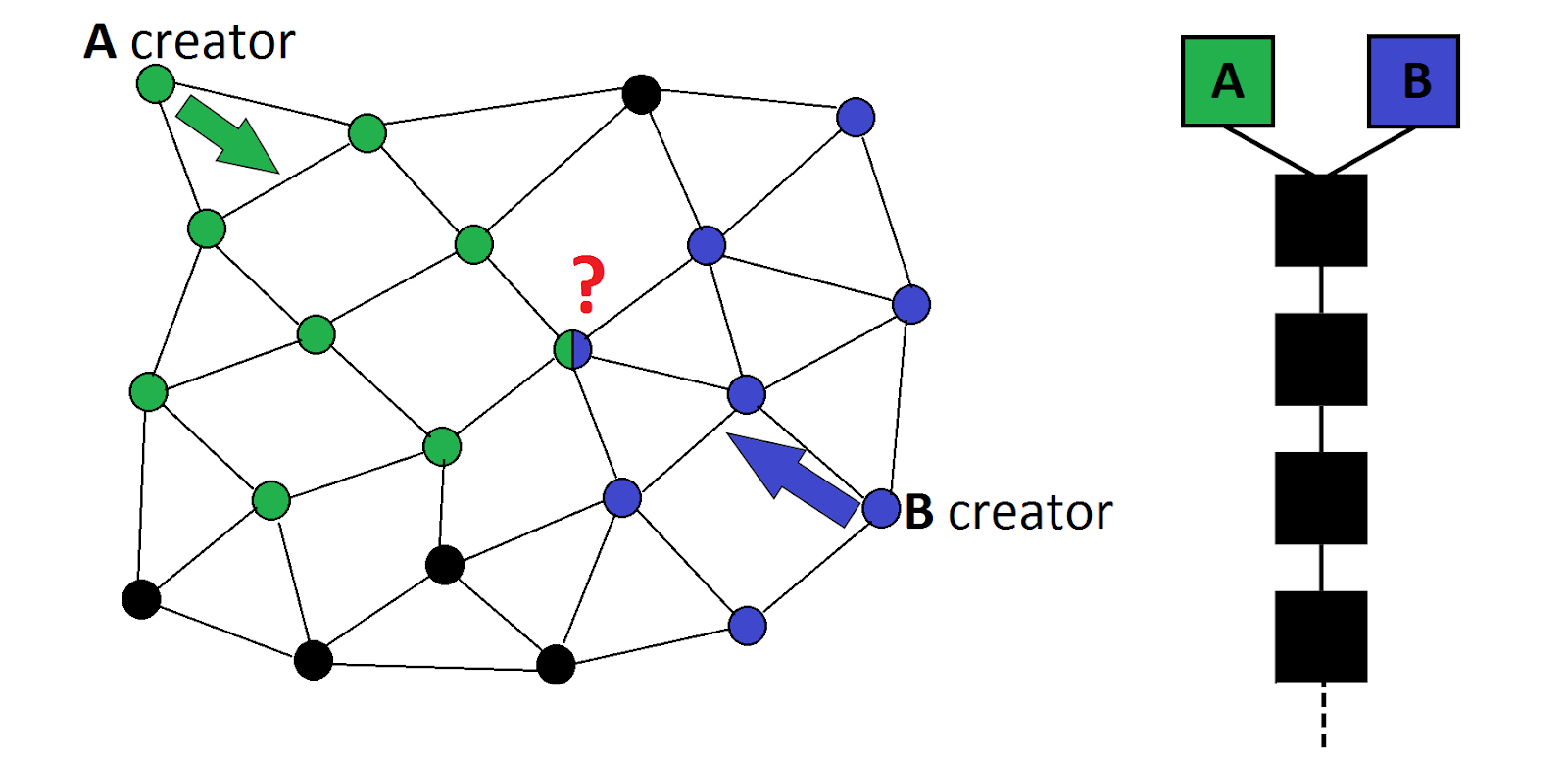
Использование цифровых подписей решает не только проблему авторизации, но также и проблему изменяемости транзакций. Если цифровые подписи используются для всех транзакций в блокчейне, злоумышленник, получивший внутренний доступ к системе (например, хакер или бывший служащий), не может изменить эти транзакции. Неизменяемость и конечность транзакций в системе на основе блокчейна достигается при помощи разделения транзакций в блоки, упорядоченные во времени, и расчете криптографической хэш-функции для каждого из блоков.

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.



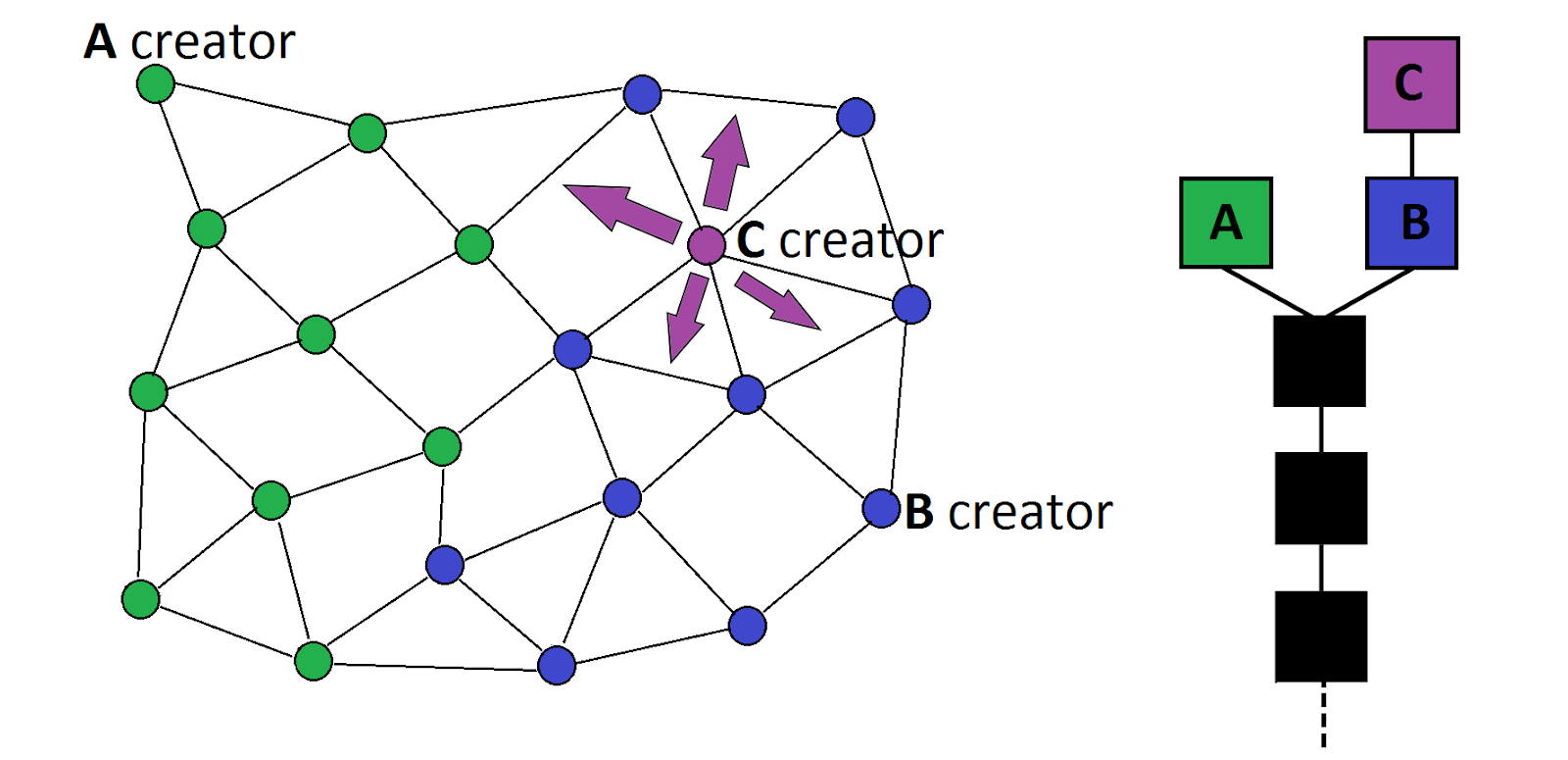
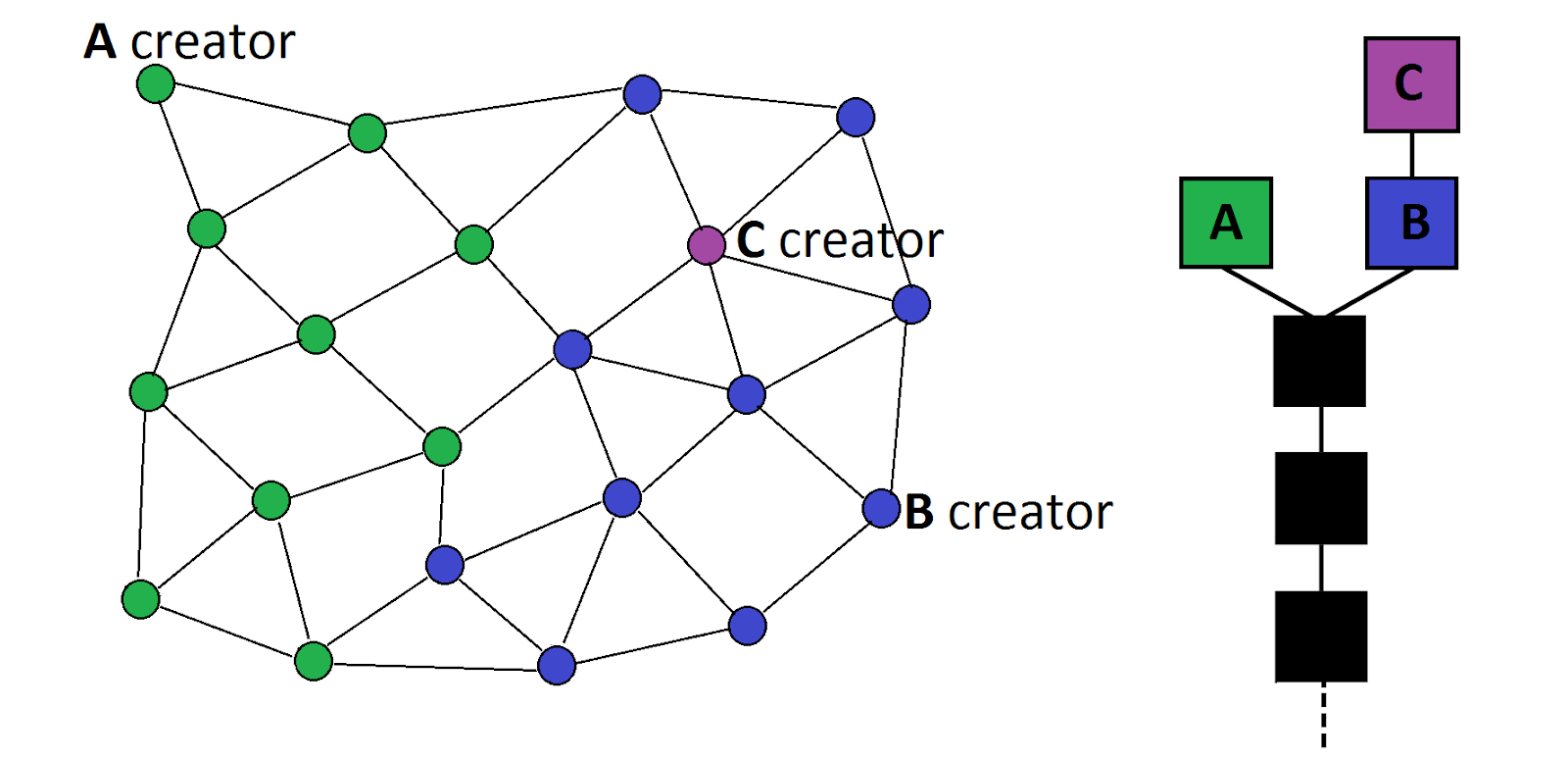
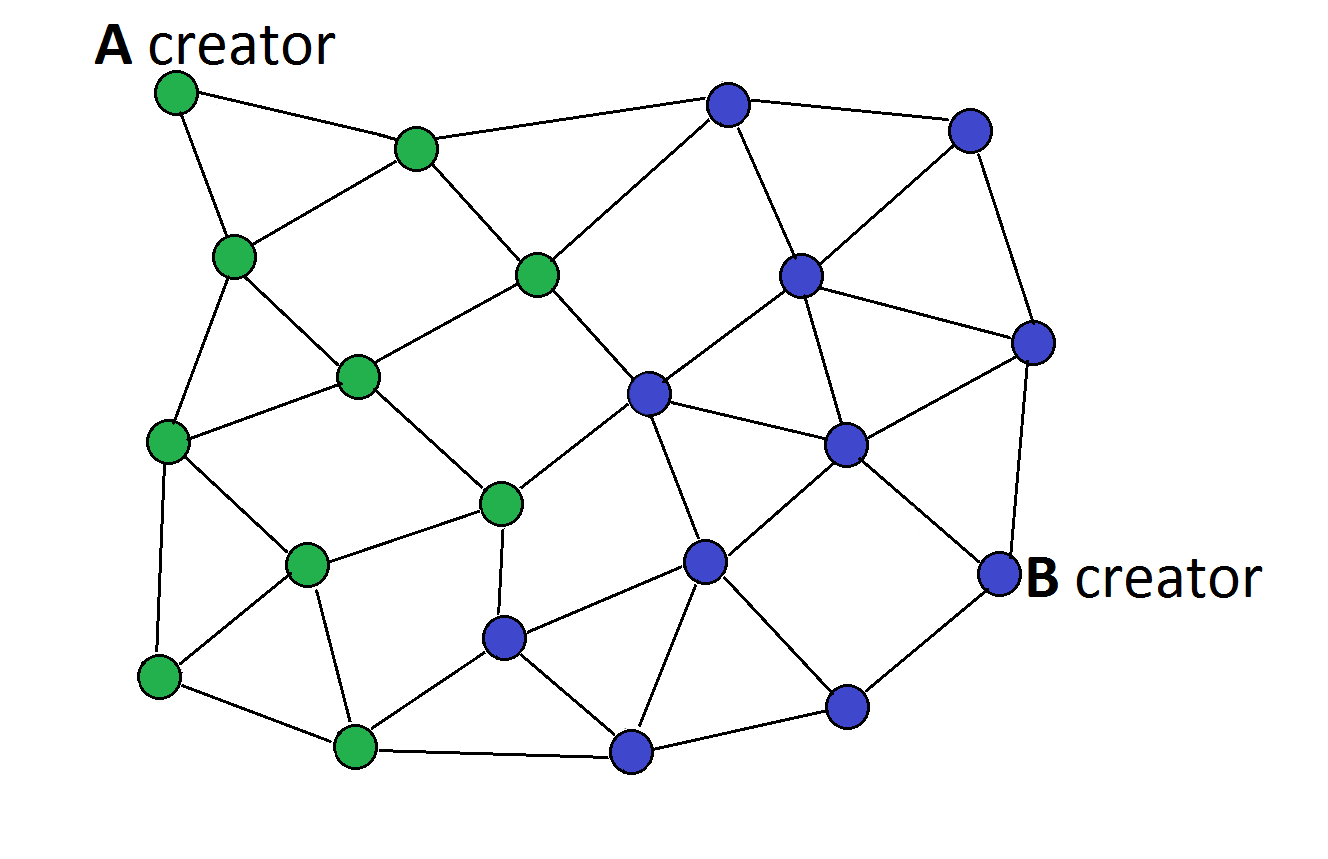
После того как блок сформирован, сформировавший его майнер разсылает его всем участникам сети к которым у него есть непосредственный доступ. Каждый участник сети, который получил этот новый блок сперва проверяет его валидность (вычисляет хеш предыдущего блока, и сравнивает его с указанным в новом, рассчитывает 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

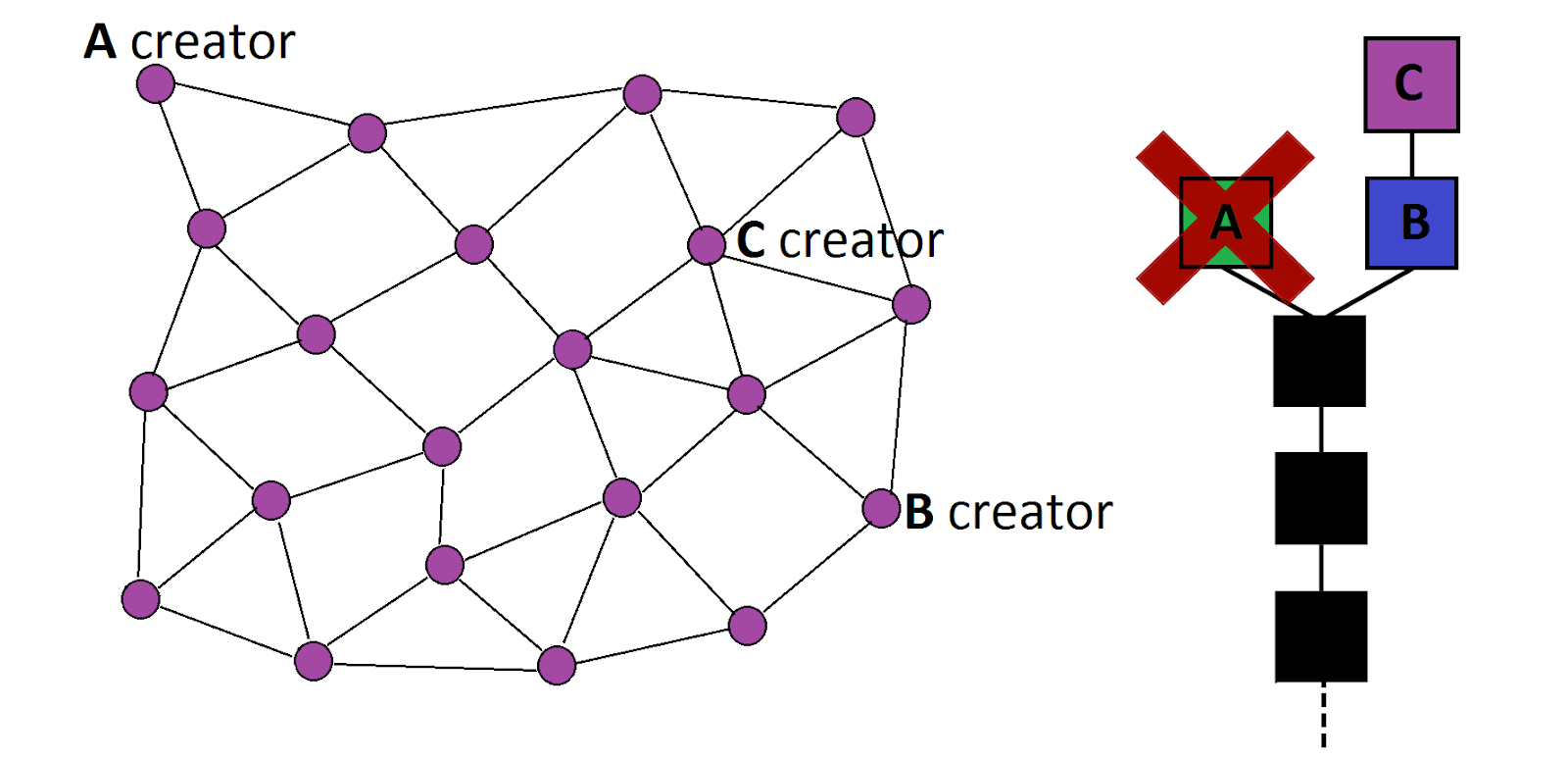


Возникнет «неразбериха» какой блок использовать за истинный, ведь в разные блоки могут быть включены разные транзакции.

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.



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.

**Классификация типов блокчейн.**

Блокчейн можно разделить на следующие типы: открытый, закрытый, комбинированный. Сравнительная характеристика их представлена в табл. 5. Открытый блокчейн — это такой тип блокчейна, в котором отсутствует ограничение на чтение блоков, при котором полностью отсутствует надзорный орган («либеральный» тип управления системой). Закрытый блокчейн — это такой тип блокчейна, в котором существует прямой доступ к данным формирующими экосистему организациями, где имеется наличие контролирующего органа. Суть блокчейна как распределительного реестра отсутствует, что порождает уязвимость сети со стороны атак хакеров и «искажением» блоков транзакций (информации), что нивелирует основной принцип блокчейн — доверие к системе. Такой тип управления системой присущ дирижизму. Однако, можно выделить третий тип технологии блокчейна, в которой можно взять все преимущества и недостатки остальных типов — комбинированный. Таким образом, комбинированный блокчейн — это такой тип блокчейн, в котором происходит идентификация в сети, а также допуск клиентов сети к определенным группам раскрытия информации, например, клиент может просматривать свои и/или чужие транзакции и/или только заголовки, при этом, имеется контролирующий орган, который будет видеть полную информацию о транзакции. Преимущества этого типа в том, что в нем присутствует элемент распределенного реестра, он надежнее защищен от хакерских атак, и в нем есть контролирующий орган, что очень важно для государства, так как это способствует противодействию получения доходов, полученных преступным путем. [11].

**Сравнительная характеристика типов блокчейн**

|  |  |  |  |
| --- | --- | --- | --- |
| Описание | Тип блокчейна | | |
| **открытый** | закрытый | комбинированный/эксклюзивный |
| Отсутствует идентификация | Идентификация участников сети | Идентификация в сети |
| Отсутствует ограничение участия пользователей | Допуск к участию в сети узкого круга участников (т. е. доступ к данным полностью ограничен и не прозрачен для клиентов) | Допуск к участию в сети, оговорен- ный определенными правилами (например, клиент сети может просматривать только свои транзакции) |
| Статус процесса не закреплен за участниками | Статус валидаторов закреплен за определенными контрагентами | Статус валидаторов закреплен за определенными контрагентами |
| Отсутствует надзор | Есть контролирующий орган | Есть контролирующий орган |

Для упорядочения и удобства разделим различныетехнологические аспекты блокчейн-технологии на три категории: блокчейн 1., 2., и 3.

Блокчейн 1.0 — это валюта. Криптовалюты применяются в различных приложениях, имеющих отношение к деньгам, например системы переводов и цифровых платежей.

Блокчейн 2.0 — это контракты. Целые классы экономических, рыночных и финансовых приложений, в основе которых лежит блокчейн, и которые работают с различными типами финансовых инструментов — с акциями, с облигациями, закладными, правовыми и умными контрактами.

Блокчейн 3.0 — это приложения, область применения которых выходит за рамки денежных расчетов, финансов и рынков. Они распространяются на сферы государственного управления, здравоохранения, науки, образования, культуры и искусства.

Использование технологии блокчейн стало прорывом в области криптографии, которая уже оказала влияние на финансовую сферу, но еще не до конца реализовала свой потенциал. Данная технология применяется как для создания криптовалют, так и для предоставления распределенных сервисов.

Блокчейн не просто обеспечивает защищенное хранение данных пользователя и финансовой информации, его преимуществом является предоставление гарантий достоверности этих сведений.

Существенная территориальная распределенность децентрализованной сети делает ее невосприимчивой к потере отдельных серверов, например в связи с неблагоприятными последствиями катастроф, кратковременными неполадками в работе самих серверов и каналов связи, действиями злоумышленников и др.

Технологии блокчейн являются перспективными для реализации корпоративных информационных систем, так как на сегодняшний день преобладают изолированные внутренние бизнес процессы, которые чрезвычайно сложны, запутанны и не прозрачны. Можно констатировать, что технологии блокчейн востребованы в современном мире из-за множественных взаимодействий по обмену и хранению данных