ЛЕКЦИЯ №1 ВВЕДЕНИЕ В БЛОКЧЕЙН

Москва, 2020

Time Stamp Protocol

Time stamp protocol (протокол штампа времени) или TSP — это криптографический протокол, позволяющий создавать доказательство факта существования электронного документа на определённый момент времени.

«Штамп времени» (англ. time-stamp) — это документ, подписанный электронной подписью (ЭП). Этим документом «центр штампов времени» удостоверяет, что в определённый момент времени ему был предоставлен результат вычисления хеш-функции от содержимого документа, факт существования которого необходимо подтвердить. Результат вычисления хеш-функции и момент времени указываются в «штампе».

Типы блокчейнов

- **Публичная блокчейн-цепь.** Публичные блокчейны (*public blockchains*), такие как Биткойн, представляют собой большую распределенную сеть, в которой запущен собственный токен. Присоединиться к ней может любой желающий и на любом уровне. Публичный блокчейн имеет открытый код, который поддерживается его сообществом.
- **Эксклюзивная блокчейн-цепь.** Эксклюзивные блокчейны (*permissioned blockchains*), такие как Ripple (*Рипл*), предполагают наличие центрального органа, определяющего все те действия, которые сторонним лицам разрешено осуществлять в этой сети. Это также большие распределенные системы, в которых используется собственный токен. Ядро их программного кода может быть как открытым, так и закрытым.
- **Частная блокчейн-цепь.** Частные блокчейны (*private blockchains*), как правило, имеют относительно небольшой размер и обычно не предполагают использование токена. Их членский состав строго фиксирован, все транзакции отслеживаются и контролируются центральным органом. Это тот тип блокчейна, который предпочитают консорциумы, имеющие доверенных членов, манипулирующих конфиденциальной информацией.

Блокчейн

Блокчейн - это распределенная база данных, которую контролирует группа индивидуумов с целью обеспечения совместного хранения и доступа к ней.
Существуют различные типы блокчейнов и блокчейн приложение
Блокчейн - представляет собой структуру данных для создания цифрового распределенного реестра и организацию совместного доступа к нему

Задача о византийских генералах

В составе войска древней Византии есть несколько легионов, каждый из которых подчиняется своему генералу. Всеми военными действиями руководит верховный главнокомандующий, который отдает приказы генералам. Любой из военачальников может перейти на сторону врага и желать поражения своему войску, в том числе сам главнокомандующий. В столь непростых условиях требуется выработка общей стратегии, которая позволит выиграть битву.
Все генералы получают приказы командующего, согласно которым они должны действовать одним из двух способов: идти в атаку или отступить. Далее события могут развиваться по нескольким сценариям:

1. если все честные генералы поведут свои легионы в атаку – Византия одержит победу (благоприятный исход);
2. если все честные генералы прикажут отступать – будут сохранены жизни легионеров (промежуточный исход);

Задача о византийских генералах

Нужно учитывать и вариант, при котором верховный главнокомандующий продался врагу и отдал генералам (всем или некоторым) преступные приказы. Зная об этом, генералы могут отказаться выполнять приказ и начнут действовать по своему усмотрению. В этом случае вероятность благоприятного и даже промежуточного исхода весьма невелика. У всех участников сражения должна быть налажена связь для обмена информацией и принятия коллективных решений. Они должны избегать рисков, связанных с недоверием к центру и друг к другу.

Есть определенное число генералов – N. Их войска дислоцированы в горах и собираются атаковать противника в долине. M генералов из общего числа N перешли на сторону врага и хотят сорвать соглашение между верными генералами. Цель соглашения – узнать численность верных Византии легионов и легионов, возглавляемых генералами-перебежчиками. Соглашение очень важно, ведь для победы или как минимум согласованного отступления необходимо выработать общую стратегию.

Задача о византийских генералах

Предположим, что один из четырех генералов оказался предателем (N = 4 , M = 1). Следовательно, трое верных военачальников пошлют верные сведения о количестве своих легионеров, а в сообщениях предателя цифры могут быть какими угодно. Допустим, первый генерал сообщил, что в составе его легиона есть 1 тысяча воинов, у второго – 2 тысячи, у четвертого – 4 тысячи. Третий генерал (перебежчик) указал остальным случайно выбранные цифры x, y, z.

Из полученных данных каждый военачальник формирует свой вектор:

1-й вектор — 1,2,x,4;

2-й вектор — 1,2,y,4;

3-й вектор — 1,2,3,4;

4-й вектор — 1,2,z,4

Далее генералы передают векторы друг другу, при этом предатель повторно искажает информацию. В результате каждый получает четыре вектора, из которых формируется ядро:

Задача о византийских генералах

Далее генералы передают векторы друг другу, при этом предатель повторно искажает информацию. В результате каждый получает четыре вектора, из которых формируется ядро:

1	2	3	4
(1,2,x,4)	(1,2,x,4)	(1,2,x,4)	(1,2,x,4)
(1,2,y,4)	(1,2,y,4)	(1,2,y,4)	(1,2,y,4)
(a,b,c,d)	(e,f,g,h)	(1,2,3,4)	(i,j,k,l)
(1,2,z,4)	(1,2,z,4)	(1,2,z,4)	(1,2,z,4)

Составление векторов при обмене информацией между участниками блокчейна

Затем генералы определяют количество воинов в каждом легионе. Для расчета первого легиона берется три числа: численность этого легиона, известная из сообщений всех генералов за исключением командующего самим первым легионом. Если одно из 3-х чисел повторяется дважды или трижды, оно помещается в итоговый вектор. Если совпадений нет, значение итогового вектора определяется как «неизвестное».

Доказательство устойчивости криптовалютных систем

Еще одно свойство биткоина было обнаружено известным американским ученым Лесли Лэмпортом. Он доказал, что согласия в штабе N генералов можно достичь лишь в случае, если количество перебежчиков не превышает N/2 минус один генерал. Это правило, работающее при генерации биткоинов, получило название «правило 51 процента». Говоря проще, если мощности предателей превышают мощности честных генералов, то последние не смогут построить корректную систему векторов по причине недостатка правильной информации. В случае с биткоинами это позволит «перебежчикам» выборочно подтверждать чужие блоки, а значит, контролировать процесс добычи криптовалюты.

Почему блокчейн-технология так важна

Сейчас блокчейн-технология признана как “пятая волна” в компьютерной революции, принесшая в мир тот самый недостающий уровень доверия к Интернету. Это одна из причин, по которым такое множество людей сейчас заинтересовались данной темой.

Блокчейн-технология позволяет создать необходимый уровень доверия на основе цифровых данных. Как только информация будет записана в базу данных блокчейна, станет практически невозможно удалить ее оттуда или изменить. Такой возможности никогда ранее не существовало.

Блокчейн добавляет дополнительное измерение время.
Возможность поиска в реестре что когда либо происходило.
- нельзя задним числом сто-то исправить, требуется рассудительные решения
- третье отличие - это ценность, в инете информация обильна ненадежна подвержена разрушения
  а в блокчейне - информация редка защищена от изменений и перманента

БЛОКЧЕЙН

» **Блок**. Блок содержит перечень транзакций, занесенных в реестр за некоторый период. Размер блока, период накопления транзакций и инициирующее запись блока событие различаются в каждой конкретной реализации блокчейна.

Не во всех блокчейн-проектах основной целью являются запись и хранение информации о перемещениях их собственной криптовалюты. Однако во всех без исключения блокчейн-проектах записываются перемещения их криптовалюты или токена. *Транзакцию* можно понимать просто как запись некоторых данных. Назначение им ценности (как это имеет место в финансовых транзакциях) используется лишь для интерпретации того, что эти данные означают.

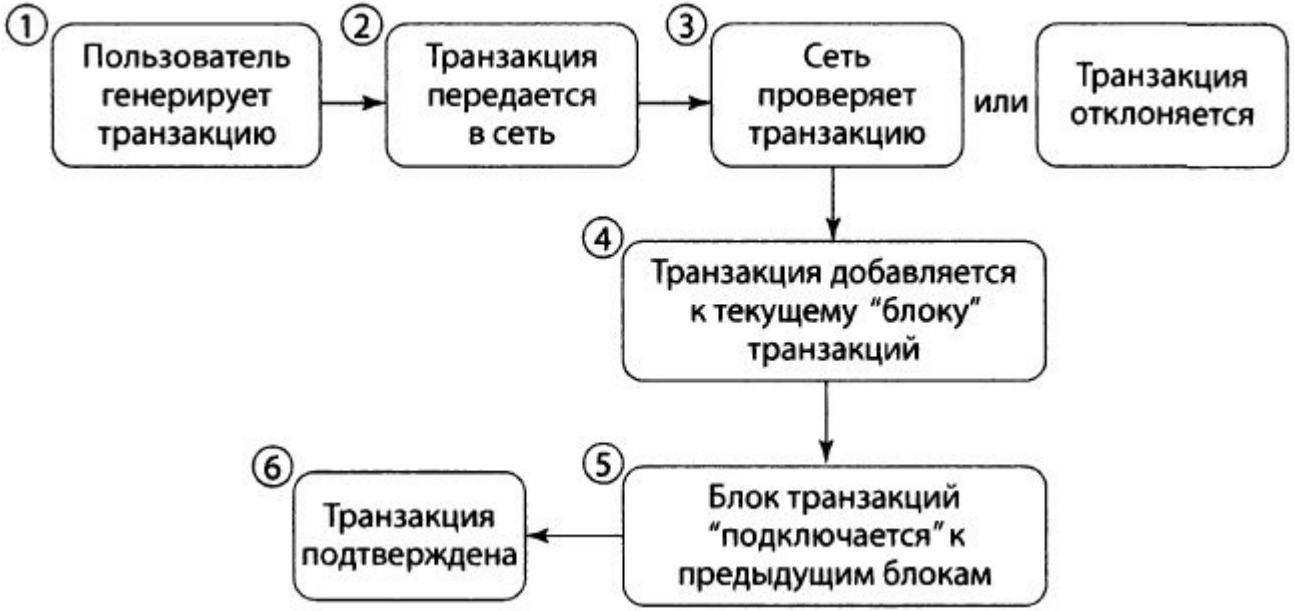
» **Цепочка.** *Хеш* — число, полученное как результат математической операции хеширования — связывает один блок данных с другим, математически объединяя их в единую цепь. Это одна из самых сложных для понимания концепций блокчейн-технологии. В действительности это та самая "магия", которая склеивает элементы блокчейна в единое целое, обеспечивая тем самым математический гарантированный уровень доверия.

Консенсус: правящая сила блокчейна

Технология блокчейна — это мощный инструмент, поскольку она позволяет создавать честные системы, обеспечивающие самокоррекцию без необходимости подключения третьих сил с целью контроля за соблюдением правил. Соблюдение установленных правил в блокчейн-технологии реализуется за счет использования алгоритма консенсуса.

В мире блокчейна термин *консенсус* определяет процесс достижения соглашения среди группы исходно не доверяющих друг другу участников системы. В данном случае ими являются полные узлы, функционирующие в сети. Полные узлы проверяют транзакции, которые были созданы в сети и должны быть записаны в реестр.

РАБОТА БЛОКЧЕЙНА



РАБОТА БЛОКЧЕЙНА

быть очень высокими. Работа системы биткойна построена в предположении, что злоумышленник может предпринять попытку нарушить историю записей о транзакциях с целью похищения токенов. В биткойне эта опасность предотвращается за счет использования модели консенсуса, называемой "доказательство выполнения работы" (*proof-of-work*). Такой подход позволяет успешно решить задачу византийских генералов: "Как можно узнать, что поступившая информация не была искажена изнутри или извне?" Поскольку изменение данных или манипуляция ими возможна практически всегда, обеспечение надежности данных — это большая проблема в компьютерных науках.

Большинство блокчейн-систем функционируют в предположении, что они будут атакованы — со стороны или изнутри, самими пользователями системы. Ожидаемые угрозы и степень доверия, которую сеть предъявляет к узлам, контролирующим запись в блокчейн, определяют тип консенсусного алгоритма, который используется в этой сети для обоснования достоверности записей ее реестра. Например, в сетях Биткойн и Эфириум предполагается очень высокая степень угрозы, и по этой причине используется очень жесткий алгоритм консенсуса, называемый *proof-of-work*. В такой сети доверие априори к кому-либо полностью отсутствует.

КРИПТОВАЛЮТА

Криптовалюта – разновидность цифровой валюты, создание и контроль за которой базируются на криптографических методах.

Как правило, учёт криптовалют децентрализирован.

Функционирование данных систем основано на технологии блокчейна.

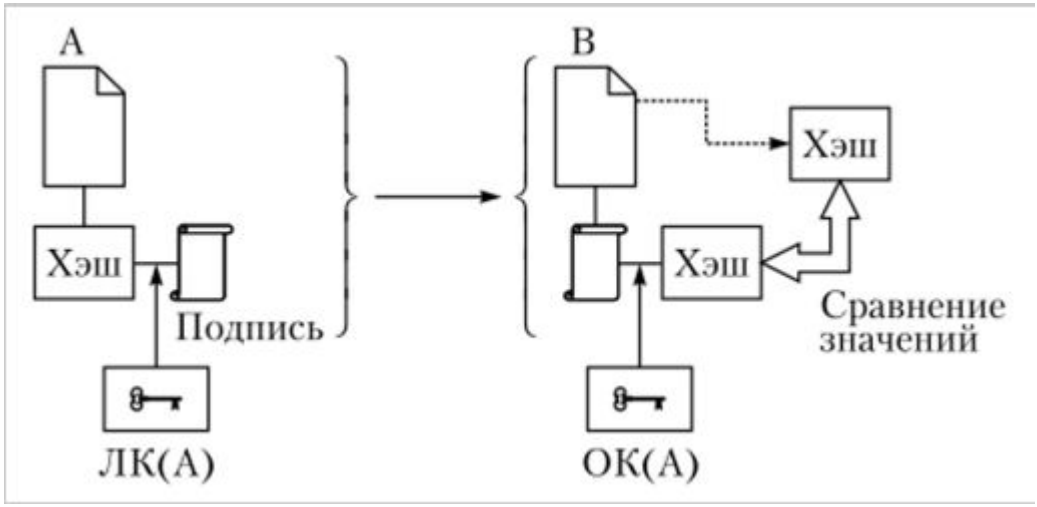
Информация о транзакциях обычно не шифруется и доступна в открытом виде. Для обеспечения неизменности базы цепочки блоков транзакций используются элементы криптографии (цифровая подпись на основе системы с открытым ключом, последовательное хеширование).

КРИПТОВАЛЮТА

Электронная цифровая подпись на основе RSA ЭЦП на основе алгоритма RSA заключается в следующем:

• отправитель А подвергает документ хэшированию с помощью однонаправленной хэш-функции;

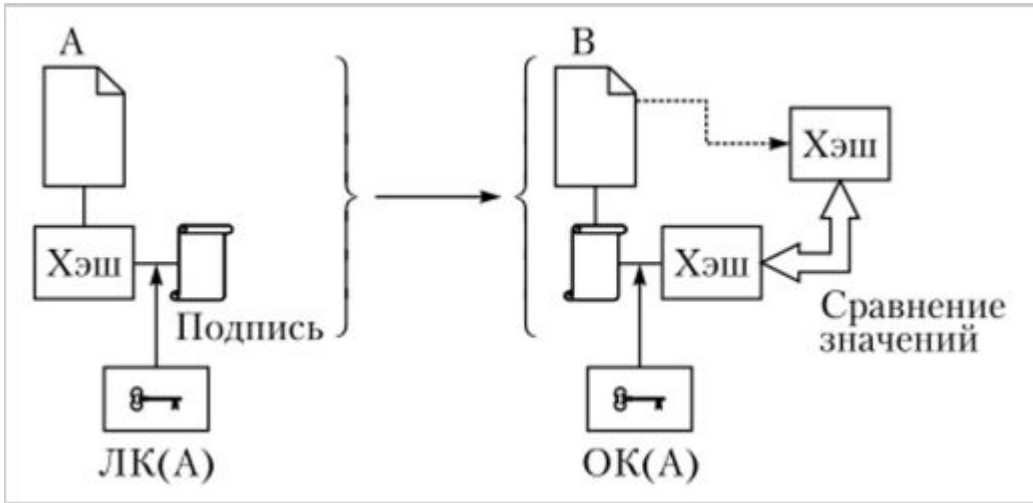
• отправитель А шифрует вычисленное хэш-значение своим личным ключом, тем самым ставя под документом свою подпись;



КРИПТОВАЛЮТА

хэш-значение в зашифрованном виде вместе с документом отправляется получателю;

• получатель В самостоятельно вычисляет хэш-значение документа, а также расшифровывает хэш-значение, присланное ему отправителем, с использованием открытого ключа отправителя. Если два полученных хэш-значе- ния совпадают, то подпись отправителя под документом вер



ETHEREUMWORKS.COM

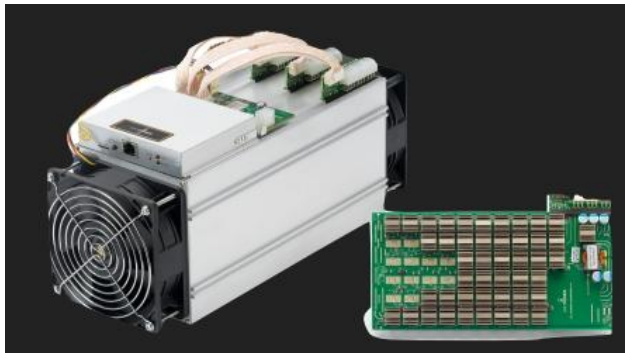
ГЛОССАРИЙ

Адрес - то место, куда вам отправляют то или иное количество криптовалюты.

По адресу можно однозначно идентифицировать пользователя.

Доступ к одному адресу есть только у одного пользователя (в основном)

АДРЕС



Специальное устройство, конструкция и архитектура которого предназначена для определенной цели.

В случае блокчейна - устройство сделанное специально для майнинга.

ASIC - одна из причин первого роста стоимости альткоинов

ASIC

Составная часть блокчейна, в которой хранится некоторое количество транзакций и метаинформация, такая как: адрес того, кто смайнил этот блок, хэш этого блока и так далее.

Блокчейн состоит из блоков.

BLOCK

Приложение, обычно браузерное, использующееся для просмотра содержимого блоков и информации о транзакциях.

Для Ethereum - Etherscan

BLOCK EXPLORER

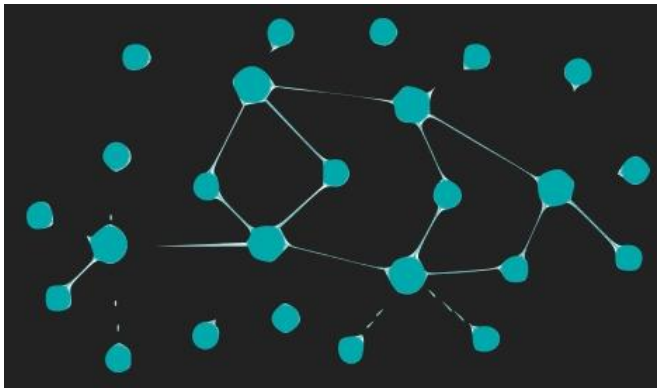
Вознаграждение, которое майнер получает за подбор подпись блока.

На ранних этапах развития любой криптовалюты - главная мотивация для майнеров.

BLOCK REWARD

Процесс включения транзакции в состав найденного блока называется подтверждением транзакции. Включение в 1 блок = 1 подтверждение, когда таких подтверждений набирается N и выше транзакция считается подтвержденной.

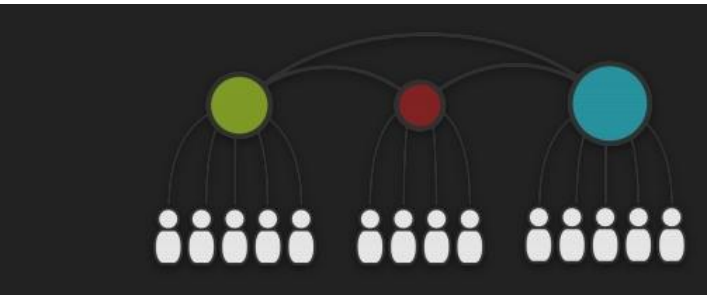
CONFIRMATION



Приложение, исходный код который исполняется на нодах в блокчейне.

Любой смарт-контракт написанный для Ethereum - DApp

DAPP



Децентрализованное приложение, которое регулирует правоотношения между его участниками.

DAO - всегда DApp

DApp - далеко не всегда DAO

DAO

То, с какой вероятностью и с какой приблизительной сложностью будет выполнена операция подтверждения следующего блока.

С ростом числа блоков сложность нахождения новых, как правило, увеличивается

СЛОЖНОСТЬ

Механизм верификации личности и аутентификации, позволяющий гарантировать, что транзакции с вашего адреса будет проводиться только вами.

ЦИФРОВАЯ ПОДПИСЬ

Процесс подбора красивого хэша (в случае, например BitCoin и Ethereum)

Проведение вычислительных операций для того, чтобы подтвердить свое право на подпись блока.

MINING

Способ аутентификации, который требует более одной подписи для отправки транзакций с адреса

MULTI-SIGNATURE

Сервис для получения off-chain данных из сети Ethereum.

ORACLES

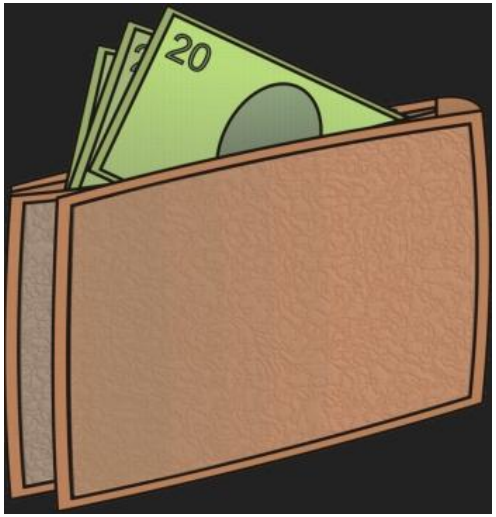
Ключ, использующийся для подписи транзакций с определенного адреса

PRIVATE KEY

Комиссия за транзакцию.

В Ethereum комиссия за транзакцию называется газом.

TRANSACTION FEE



Место хранения приватных ключей.

В самом простом случае - текстовый файл с приватным ключом.

Обычно - десктопное или мобильное приложение, с помощью которого можно отправлять транзакции

WALLET