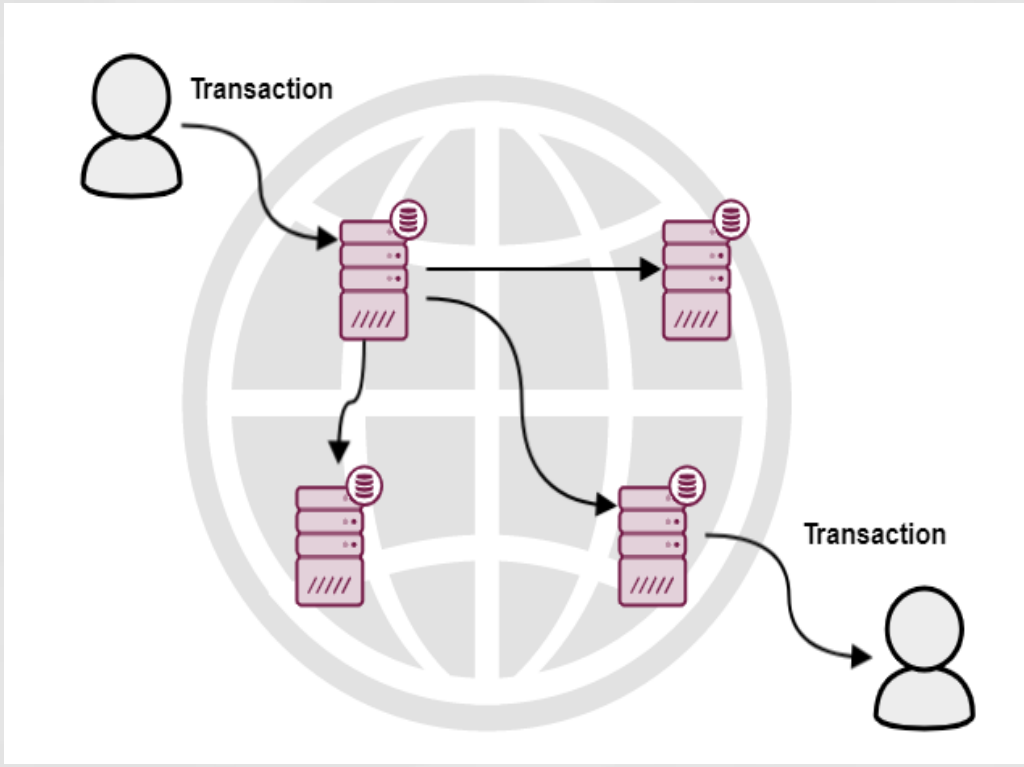
Введение в технологию Блокчейн (Blockchain)

Задача блокчейна

- Совершение доверительной передачи собственности на цифровые активы (assets) в недоверительной среде без посредников.
- Примеры:
  - В сети Bitcoin цифровой актив — это цифровые монеты Bitcoin
  - В сети Ethereum цифровой актив – это программные коды Smart-Contracts

Централизованная сеть

- Доверительный Центр имеет сервера с базами данных, расположенных в разных дата-центрах
- При переводе актива отправителя Центром проверяется и регистрируется транзакция
- Транзакция реплицируется на все сервера
- Активы доходят до получателя



Проблемы централизованной сети

- Необходимость идентификации (персонализации) участников со стороны Центра и желание анонимности транзакций участниками
- Корректность выполнения транзакций базируется на доверии к Центру.
- Возможность мошенничества, называемое двойной тратой (double-spending) – потенциальная возможность потратить свой баланс несколько раз, пока транзакция не реплицировалась на все сервера.

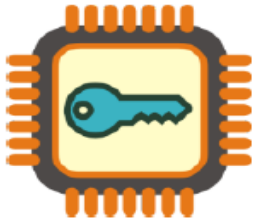
Проблемы централизованной сети (продолжение)

- Возможность атаки на конечное число серверов Центра, которые станут недоступными непредумышленно или по злому умыслу
- Центр обязательно возьмет свою ощутимую комиссию
- Ограниченность управления транзакциями: желание участников не только переводить активы друг другу, но и проверять различные условия прохождения транзакции, программировать сценарии работы, автоматически выполнять действия в зависимости от условий и т.д.

Принципы технологии блокчейн

Децентрализованная - отсутствует единый центр контроля и эмиссии.

Распределенная – данные и их обработка распределены по разным вычислительным узлам системы



Доверие – участники доверяют алгоритмам и проверяют ими информацию других участников, неизменность информации

Публичность – доступность всей информации всем участникам сети

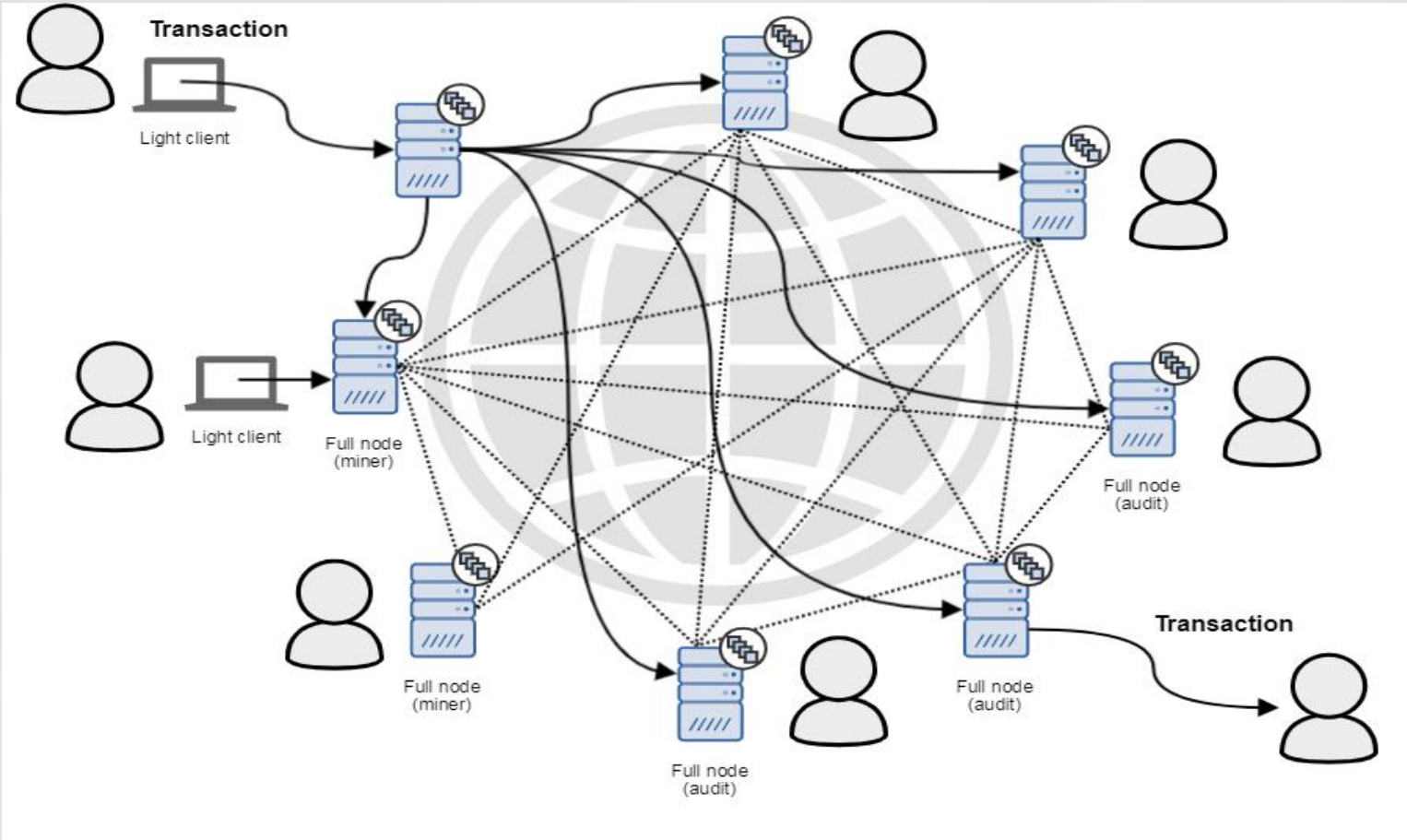
Технологическое решение проблем

- Идентификация участников осуществляется с помощью пары ключей: закрытого и открытого, а алгоритм цифровой подписи однозначно идентифицирует отправителя и получателя, оставляя их личности анонимными
- Транзакции собираются в блоки, вычисляется хеш блока, который записывается в следующий блок. Это делает невозможным незаметное изменение / удаление блоков или отдельных транзакций из блоков
- Мошенничество double-spending предотвращается путем достижения консенсуса в сети, какие данные считать верными, а какие отбрасывать

Технологическое решение проблем

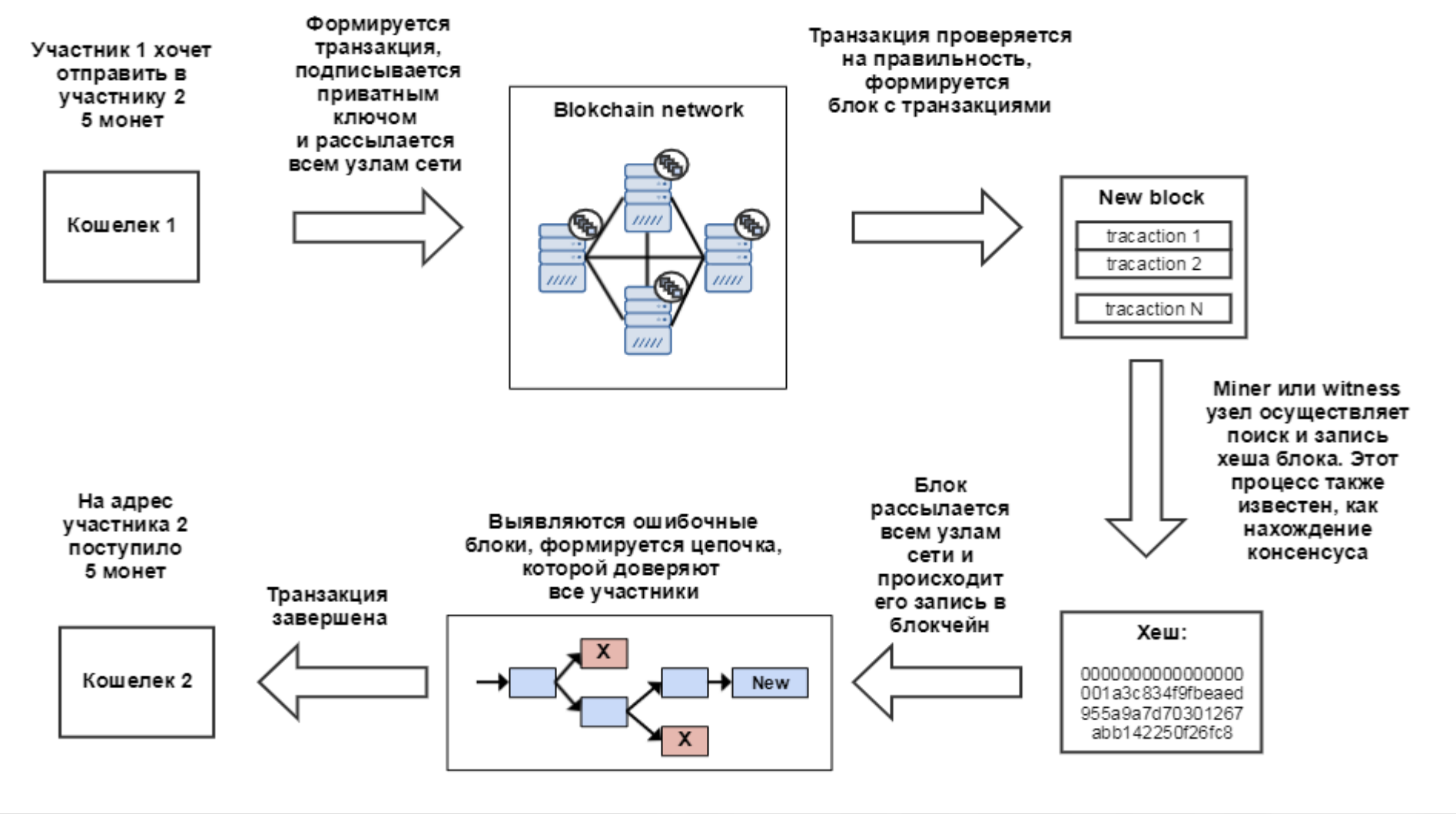
- Надежность функционирования сети достигается тем, что блокчейн является публичным, где каждый участник может получить полную копию блокчейна и, более того, самостоятельно начать проверять транзакции на правильность
- Полностью от комиссии в блокчейне не избавится, т.к. надо платить людям поддерживающим сеть, но в блокчейне необходимость комиссии убедительно доказывается
- Современные блокчейны имеют возможность реализовывать бизнес логику, которая в блокчейне называется Smart Contracts. Логика смарт контрактов реализуются на различных языках высокого уровня.

Архитектура сети блокчейн



- Нода (node) — это ПО, позволяющее взаимодействовать с сетью, подтверждать транзакций и блоки, проверять блоки, таким образом, обеспечивать безопасность и безотказную работу сети.

Жизненный цикл транзакции



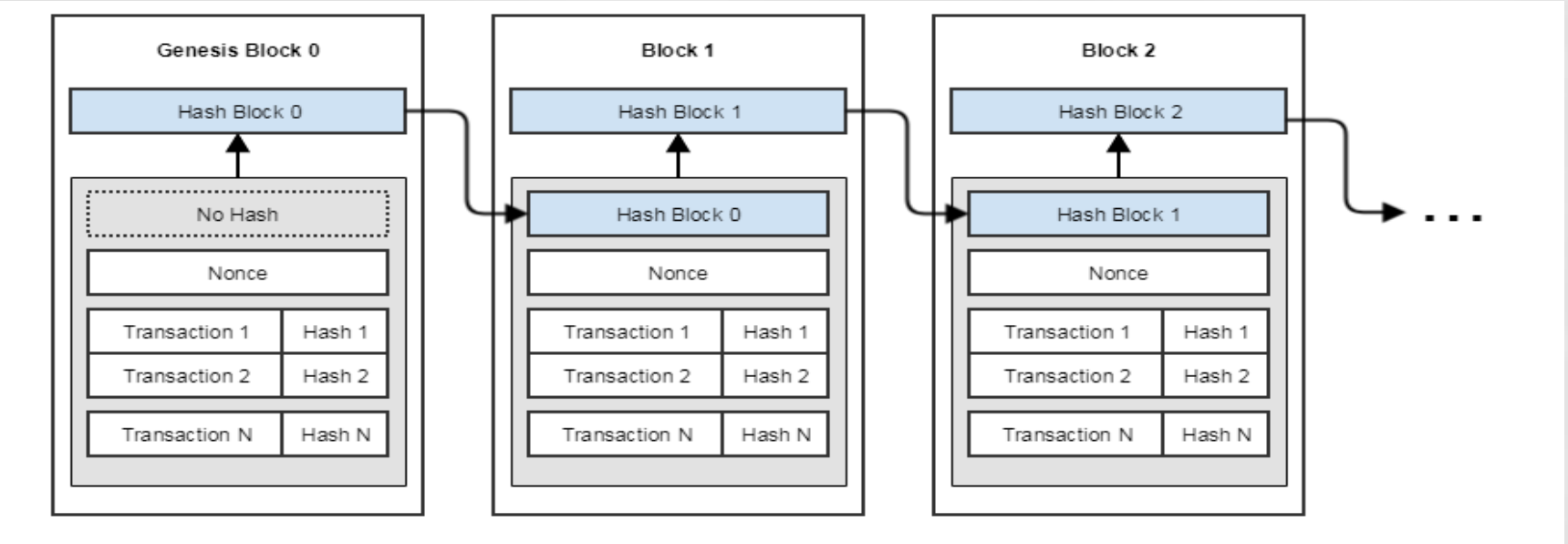
Идентификация

- Каждая блокчейн транзакция должна быть подписана цифровой подписью, например, алгоритмом на эллиптических кривых
- Для совершения транзакции каждый участник должен иметь пару ключей: private / public.
- Эту пару ключей называют кошелек (wallet), т.к. ключи однозначно связаны с уникальным цифровым адресом и балансом участника
- Закрытый ключ должен быть строго секретен и храниться в безопасности. При его утери доступ к цифровому активу восстановить невозможно

Транзакции

- Каждая транзакция имеет по крайней мере следующие данные:
  - *From: 0x48C89c341C5960Ca2Bf3732D6D8a0F4f89Cc4368 - цифровой адрес отправителя*
  - *To: 0x367adb7894334678b90afe7882a5b06f7fbc783a - цифровой адрес получателя*
  - *Value: 0.0001 - сумма транзакции T*
  - *Transaction Hash: 0x617ede331e8a99f46a363b32b239542bb4006e4fa9a2727a6636ffe3eb095cef - хэш транзакции*
- Транзакция подписывается секретным ключом и рассылается всем узлам (нодам) в блокчейне для проверки на валидность.
- Алгоритм проверки транзакции включает два десятка шагов, например, передаваемый актив не превышает запаса этого актива

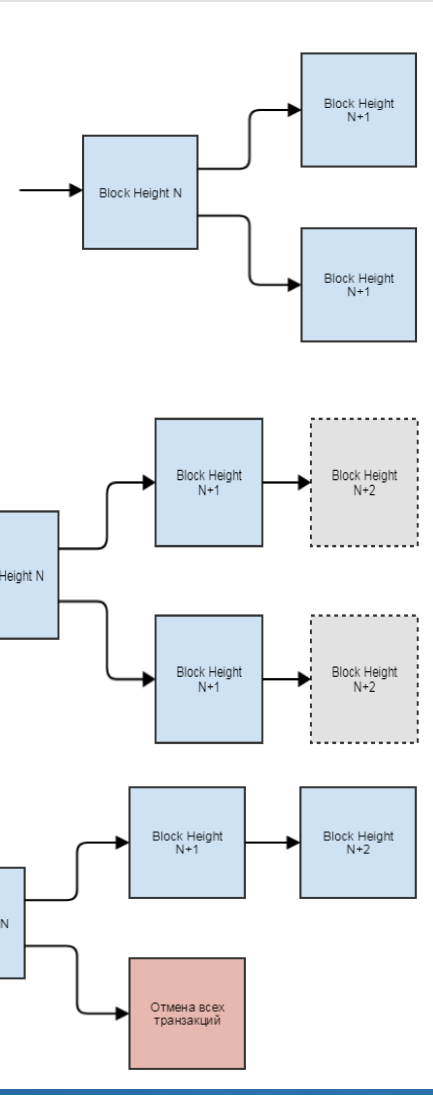
Блоки транзакций



- Хеш блока должен обладать установленным условиям сложности – не превосходить заданное число (т.е. иметь определенное число нулей в начале)
- Для подбора хеша используется поле Nonce - это единственные данные в блоке, которые можно изменить
- Успешное нахождение хеша и является доказательством проделанной работы (Proof-of-Work, PoW) для сетей Bitcoin или Ethereum.
- Процесс нахождения хешей называется майнингом (mining)

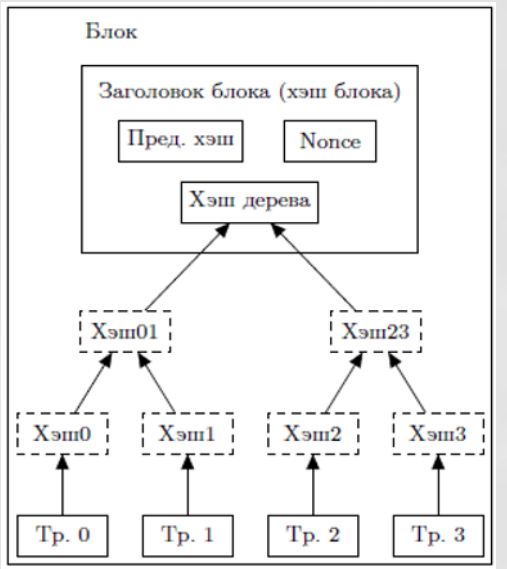
Развилка (fork)

- Развилка – это случай, когда несколько узлов пришли к разным консенсусам (т.е нашли разные по значению хеши удовлетворяющие условиям сложности) и записали блоки в блокчейн
- В этом случае часть сети начинает работать над блоком N+2 от одной цепочки, а часть от другой
- Какой-то из этих блоков будет найден раньше и отправлен в блокчейн и тогда по правилам блокчейн должен будет переключиться на более длинную цепочку и отменить все транзакции из альтернативного блока

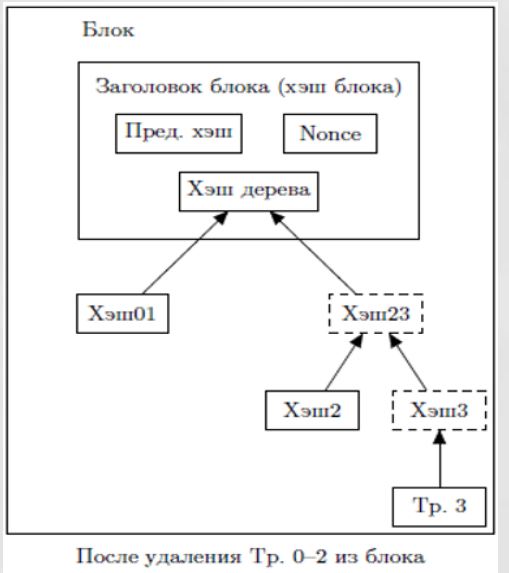


Экономия дискового пространства

- Как только последняя транзакция в цепочке, связанной с активом, окажется внутри достаточно старого блока, все предшествующие ей транзакции в цепочке могут быть удалены в целях очистки дискового пространства.
- Чтобы хэш блока остался неизменным, все транзакции в блоке хранятся в виде хэш-дерева Меркла и лишь его корень включается в хэш блока
- Размер старых блоков может быть уменьшен за счет удаления ненужных ветвей этого дерева, а хранить промежуточные хэши необязательно



Хэш-дерево транзакций



После удаления Тр. 0–2 из блока

Примеры применения технологии

Сферы применения blockchain вне финансовых сервисов

- Авторство и право владения
- Операции с товарами и сырьем
- Управление данными
- Бриллианты
- Цифровая идентичность, проверка подлинности и подтверждение прав доступа
- Энергетика
- Средства электронного голосования
- Азартные и видеоигры
- Организация частного и государственного управления
- Интернет вещей
- Биржи труда
- Прогнозирование рынка
- Распространение мультимедиа и другого контента
- Сетевая инфраструктура
- «Прозрачная» благотворительность и общественно полезная деятельность
- Недвижимость
- Репутационные рейтинги
- Сервисы райдшеринга
- Социальные сети
- Сертификация цепочек поставки в пищевой промышленности

Авторство и право владения

Операции с товарами и сырьем

Управление данными

factom

Бриллианты

everledger

Цифровая идентичность, проверка подлинности и подтверждение прав доступа

Энергетика

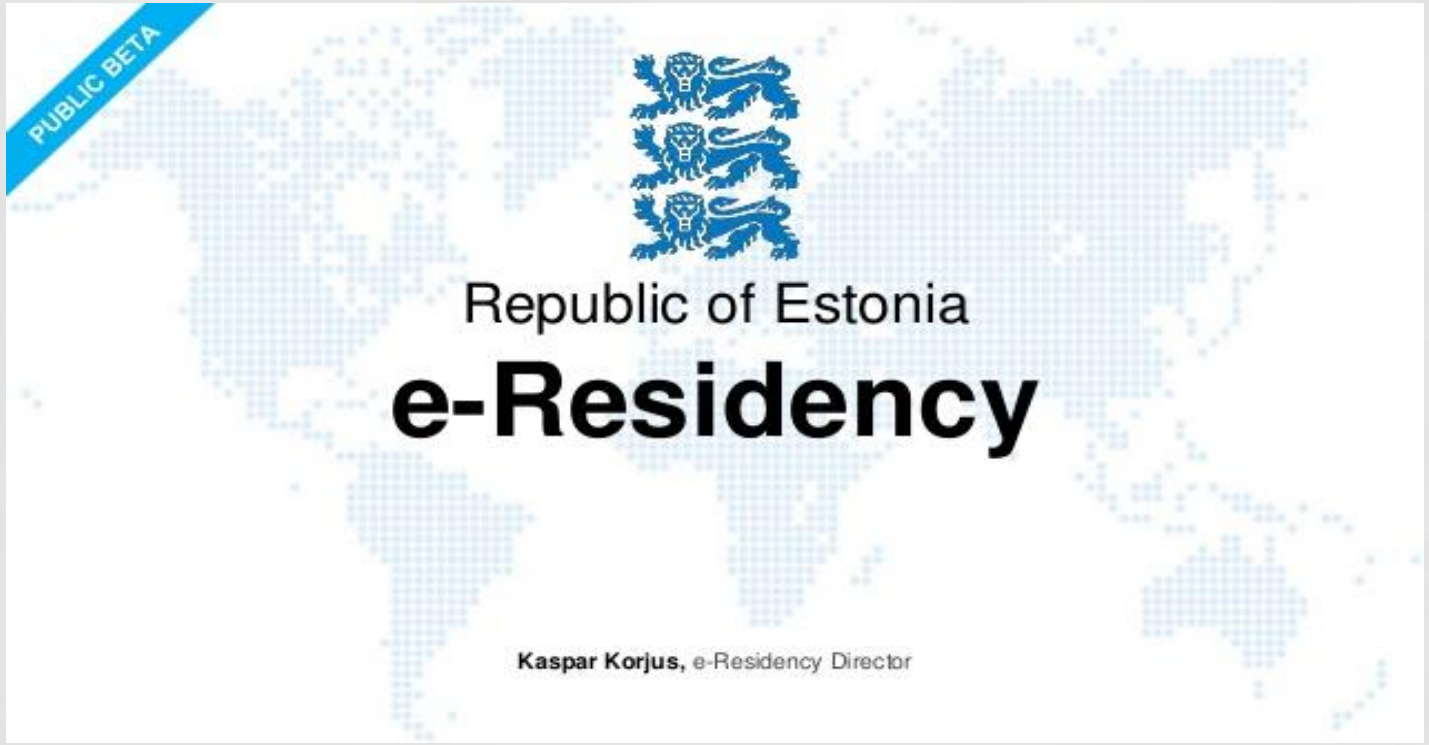
ENERGY BLOCKCHAIN LABS

Gridgularity

TRANSACTIVEGRID

Средства электронного голосования

followmyvote.com



Азартные и видеоигры

FIRST BLOOD™

ETHEROII

Организация частного и государственного управления

Интернет вещей

FILAMENT

Биржи труда

Прогнозирование рынка

Распространение мультимедиа и другого контента

Сетевая инфраструктура

«Прозрачная» благотворительность и общественно полезная деятельность

GiveTrack

HELPERBIT

alice

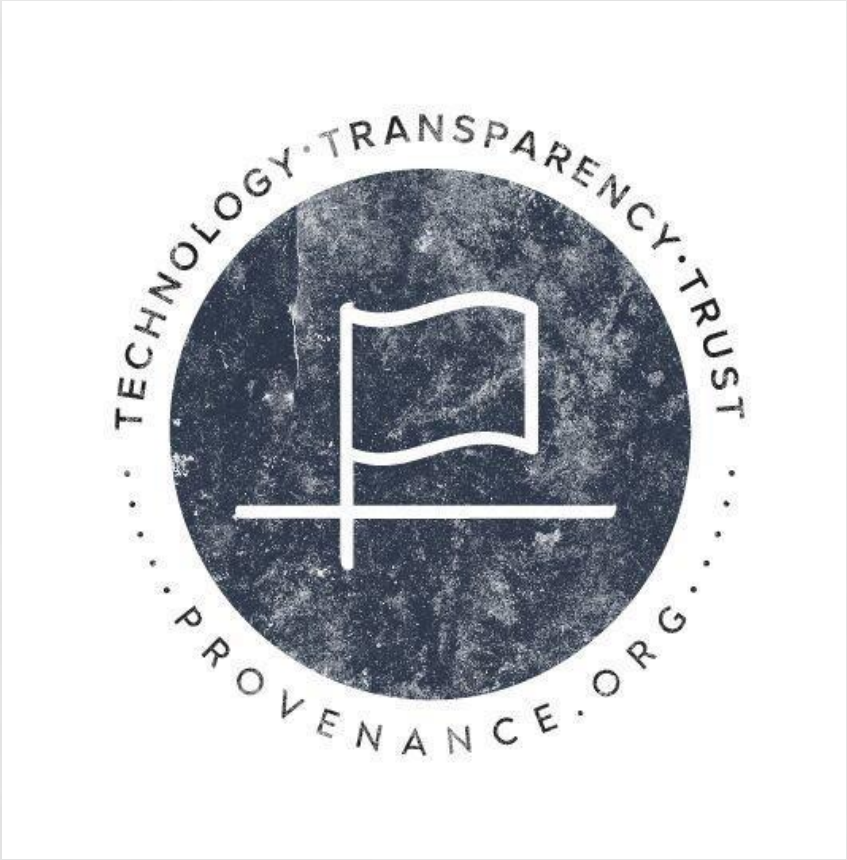
Недвижимость

Репутационные рейтинги

Сервисы райдшеринга

Социальные сети

Сертификация цепочек поставки в пищевой промышленности



Библиографический первоисточник:

- Перевод статьи Сатоши Накамото. «Биткоин: цифровая пиринговая наличность» https://coinspot.io/technology/bitcoin/perevod-stati-satoshi-nakamoto/