Технология

BLOCKCHAIN

не только **Bitcoin**

BLOCKCHAIN – это:

- Технология

  Учета и обмена правами собственности на цифровые активы в одноранговой сети

- Структура данных

  Синонимы

  - Распределенный реестр
  - **Distributed Ledger**

Традиционные (централизованные) системы электронных расчетов и учета

Посредник:

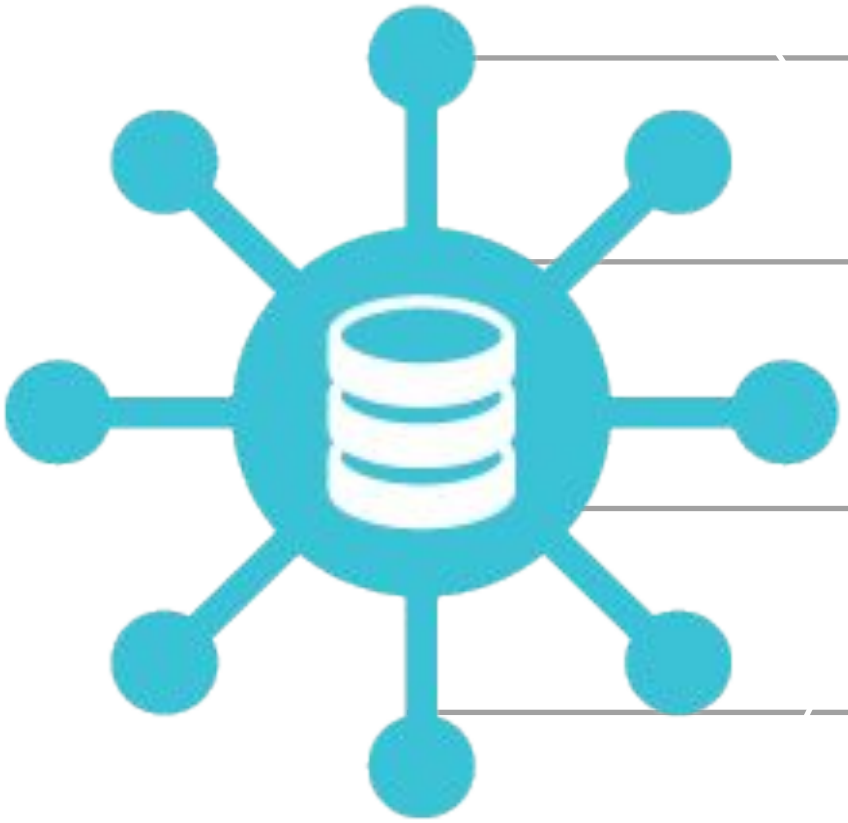
Аутентифицирует участников

Ведет **Реестр** транзакций

Ведет **Счета** участников

- Предотвращает **Двойное списание**

Традиционные (централизованные) системы электронных расчетов и учета



Уязвимость к атакам и отказам

Возможность удаления/изменения транзакций после выполнения

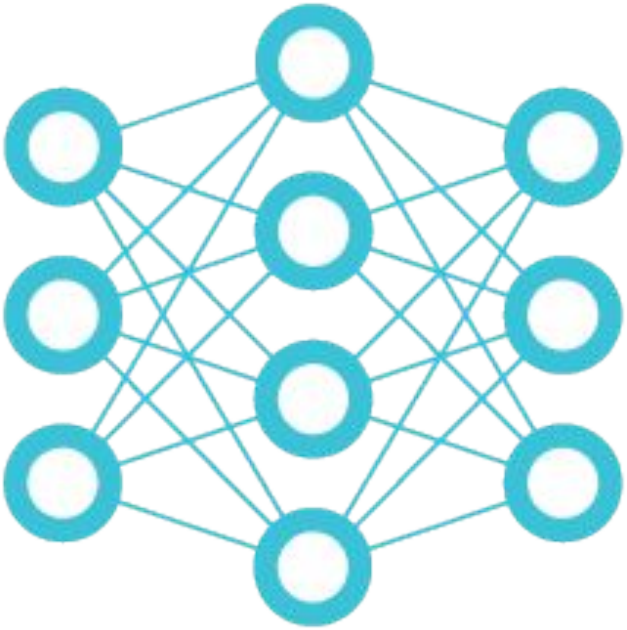
Удорожание транзакций из-за комиссии

- Непрактичность маленьких и/или разовых (casual) транзакций

Закрытость данных

- Затрудненность контроля и аудита

Одноранговые (p2p) системы электронных расчетов и учета



BLOCKCHAIN:

Аутентификация участников с помощью **ЭЦП**

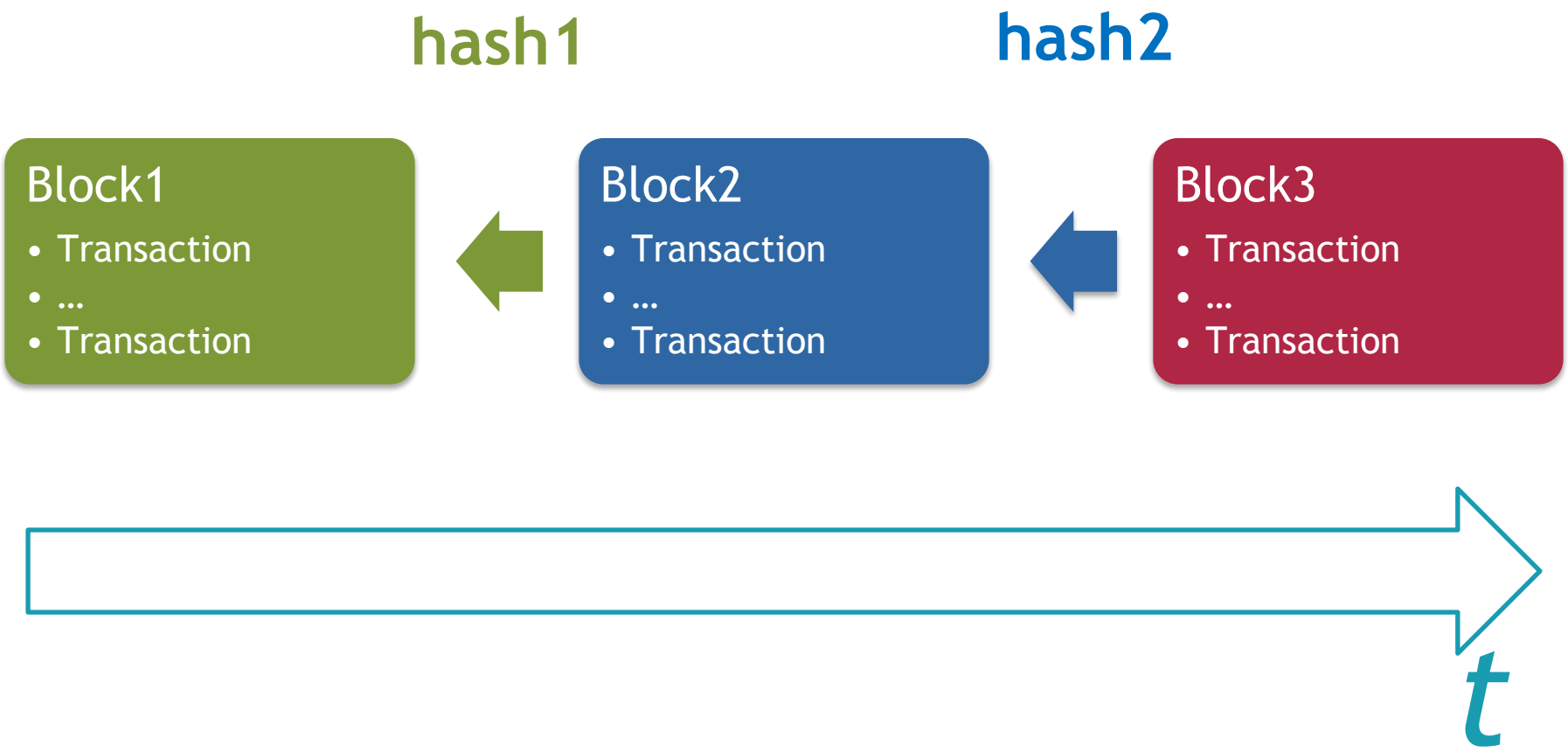
Реестр транзакций
- ведется коллективно
- хранится у каждого

Счета участников **не** ведутся
- **Двойное списание - избегается коллективным консенсусом**

BLOCKCHAIN: структура данных

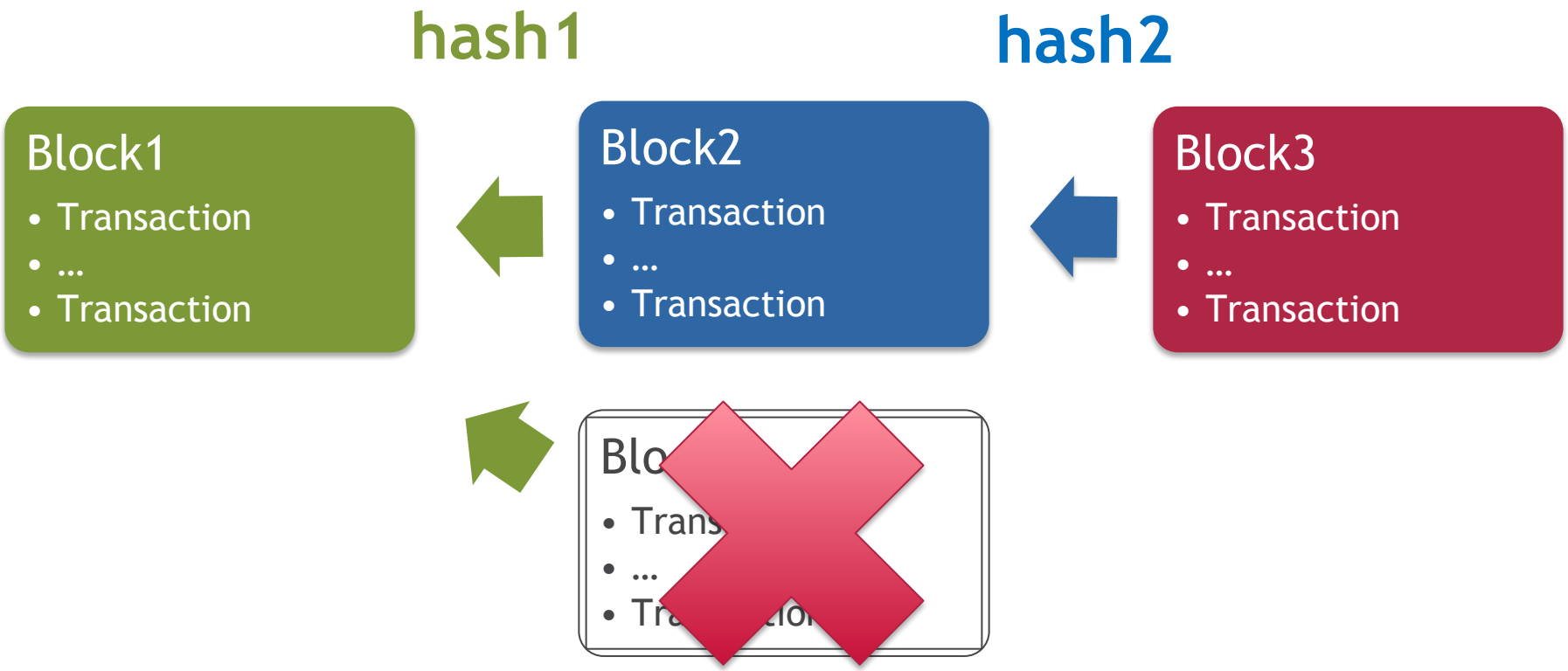
Транзакции объединены в **Блоки**

Каждый блок включает хэш предыдущего



BLOCKCHAIN: структура данных

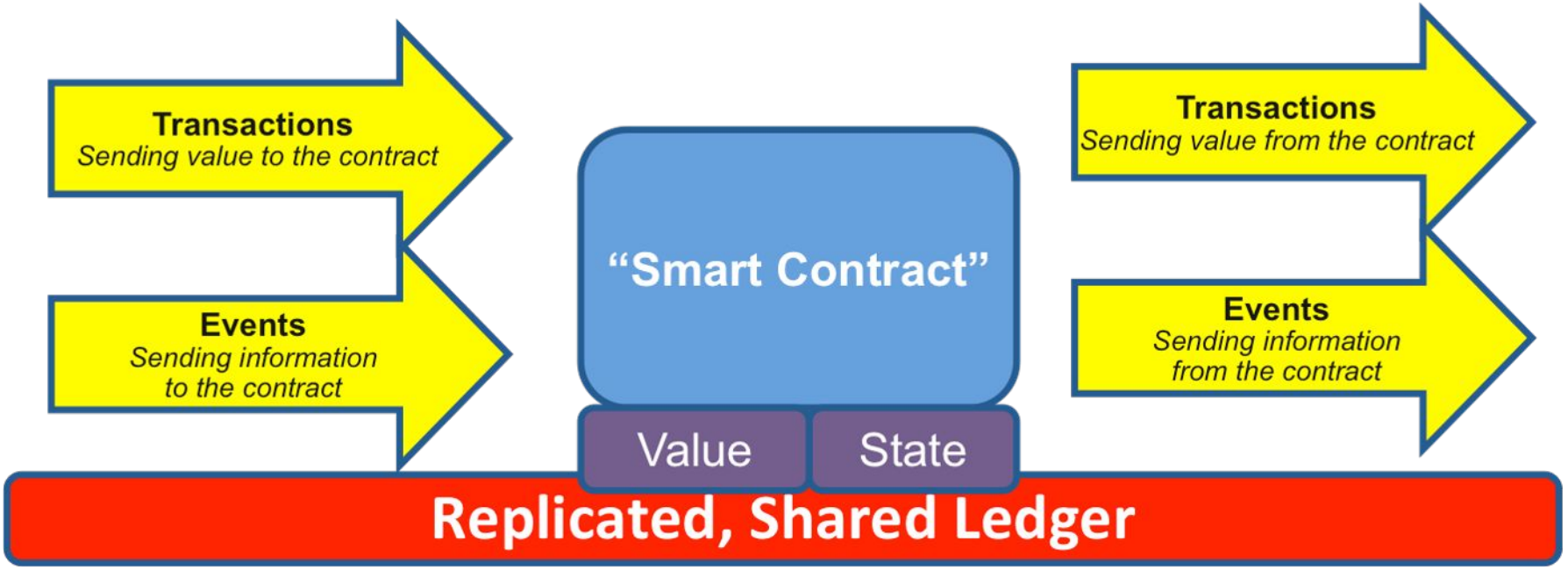
Правильный **порядок** блоков определяется «**консенсусом**» **большинства** узлов сети

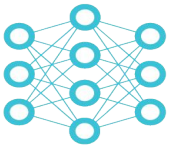


BLOCKCHAIN: Смарт-контракты

Исполняемый код в Блокчейне.

Обеспечивает выполнение контракта без участия человека (например - пари)





BLOCKCHAIN: основные идеи и характеристики

❑ **Децентрализация**	Исключение посредника обмене. Обмен выполняется по схеме p2p.	Удешевление операций (нет комиссии посредника); Упрощение процесса.
❑ **Распределенность**	Вся информация о всех транзакциях хранится на всех компьютерах участников обмена. Нет единого центра уязвимости.	Устойчивость к атакам и отказам оборудования
❑ **Открытость**	Все участники знают обо всех транзакциях (но не о конкретных участниках транзакций).	Прозрачность, публичность, легкость аудита
❑ **Криптозащита**	Все транзакции подписываются ЭЦП	Верифицируемость
❑ **Анонимность**	В качестве адреса участника транзакции используется абстрактное 32-битное число	
❑ **Историчность**	Все транзакции связаны друг с другом в цепочку.	Исключение двойного списания. Прослеживаемость источников ресурсов (денег)

BLOCKCHAIN: основные недостатки

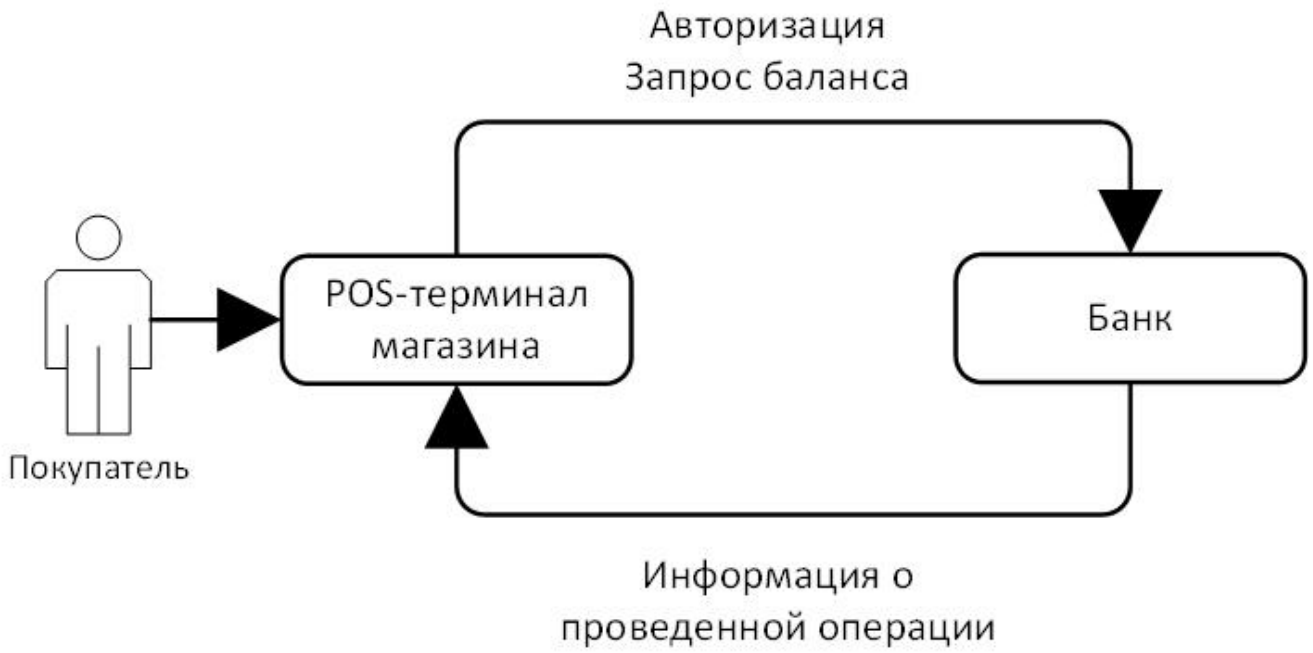
Производительность	каждый узел в сети верифицирует каждую транзакцию.	Низкая производительность сети (~7 tps Bitcoin, ~25 tps Ethereum)
Защита информации	Затруднено обеспечение недоступности для просмотра определенной информации транзакции/контракта или ее части	
Уязвимость ключей ЭЦП	При потере/компрометации ключа участнику становится недоступна вся информация и функциональность сети	Возможность безвозвратно потерять деньги, недвижимость, интеллектуальную собственность.

Вопросы

Самый первый и известный **Blockchain**

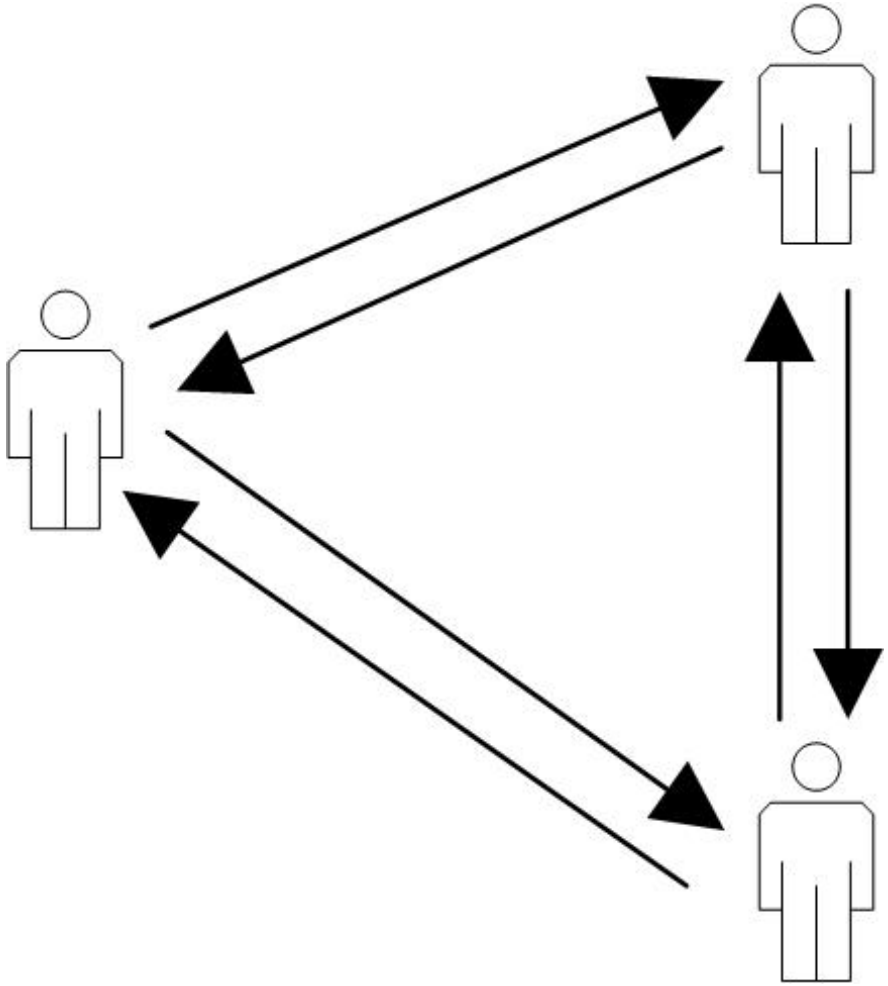
BITCOIN

Электронные платежи: проблемы



- Уязвимость к атакам и физическим воздействиям
- Возможность заморозки счетов
- Комиссии

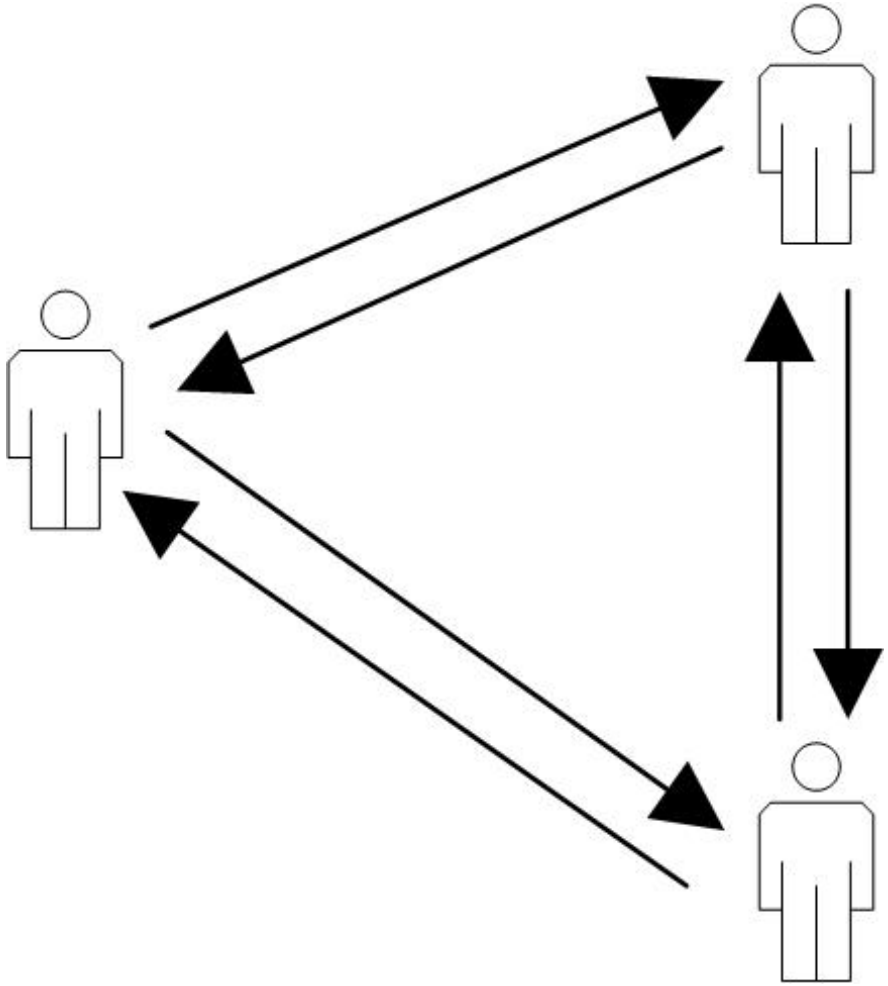
Одноранговая сеть (без посредника)



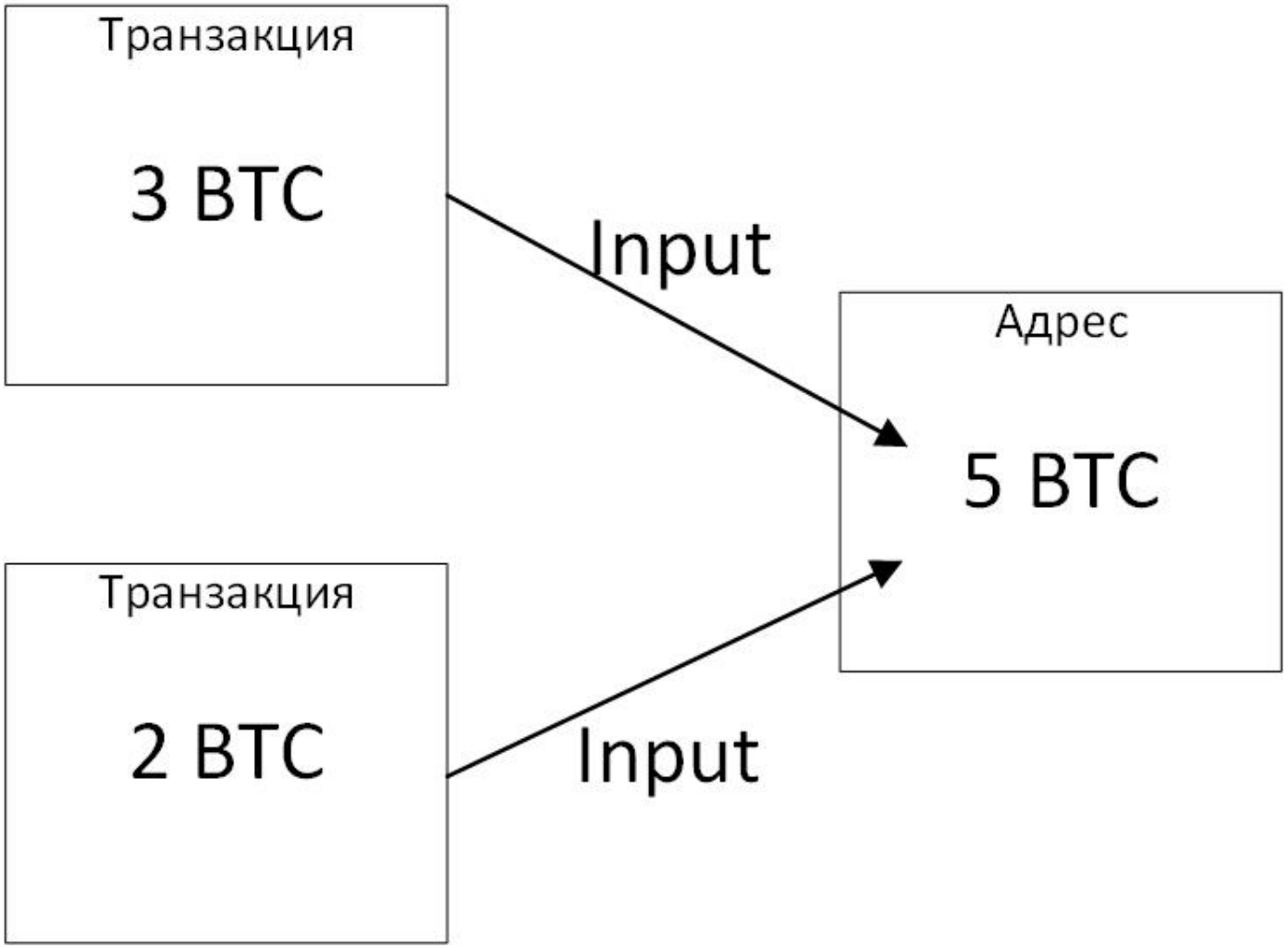
Одноранговая сеть (без посредника)

Проблемы

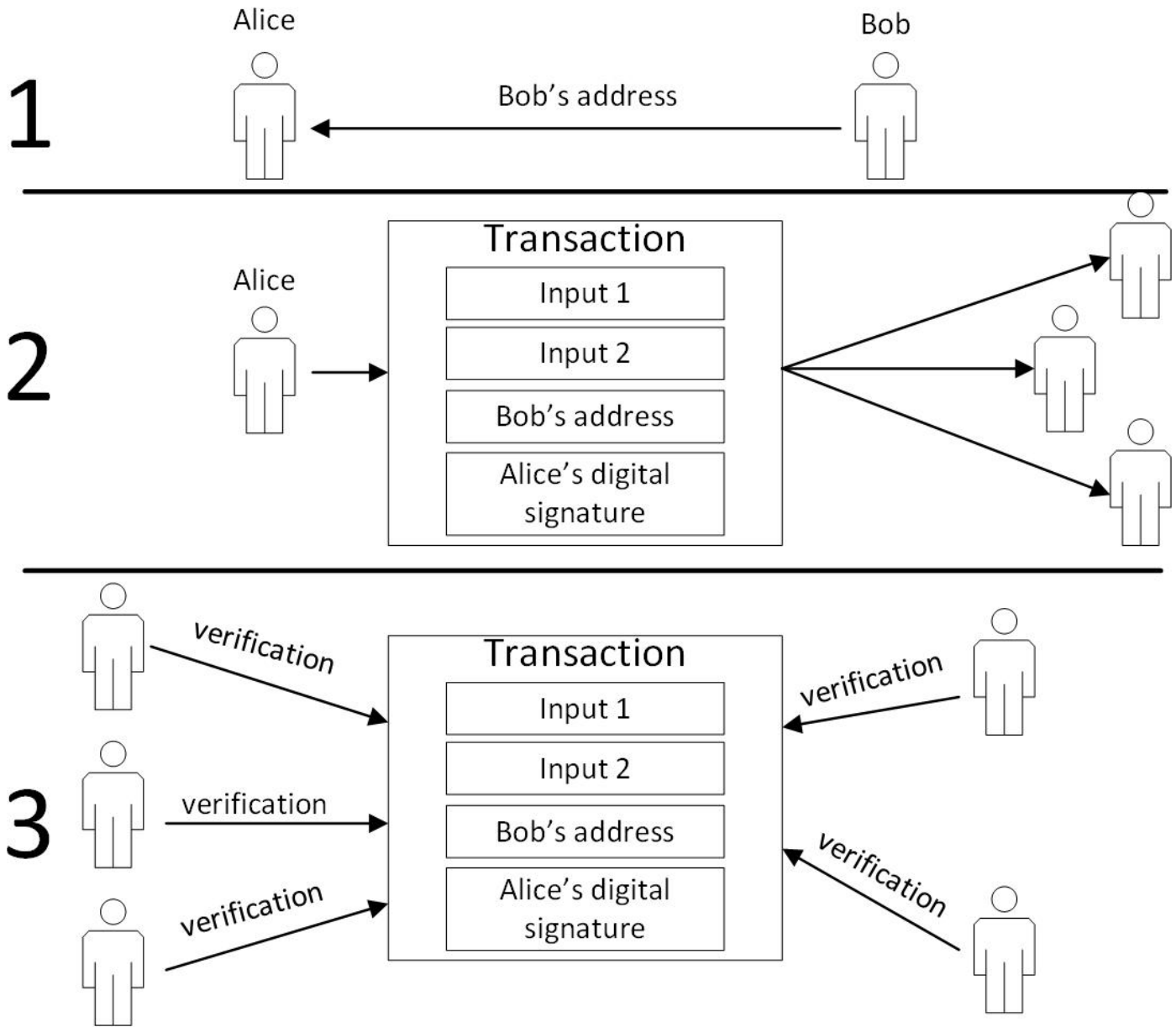
- Вести баланс
- Исключить двойную трату
- Обеспечить защиту транзакций от искажения



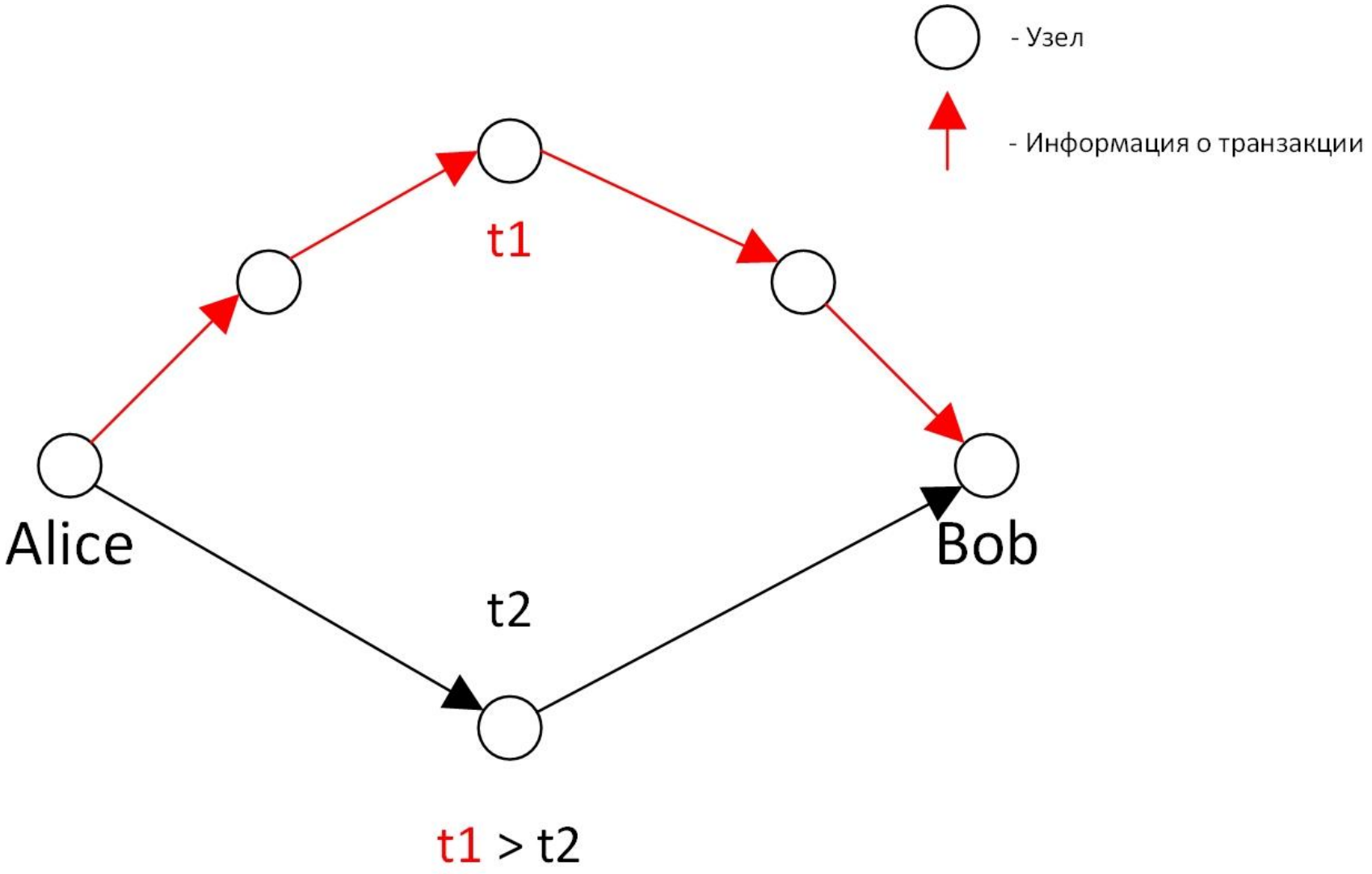
BITCOIN: Баланс



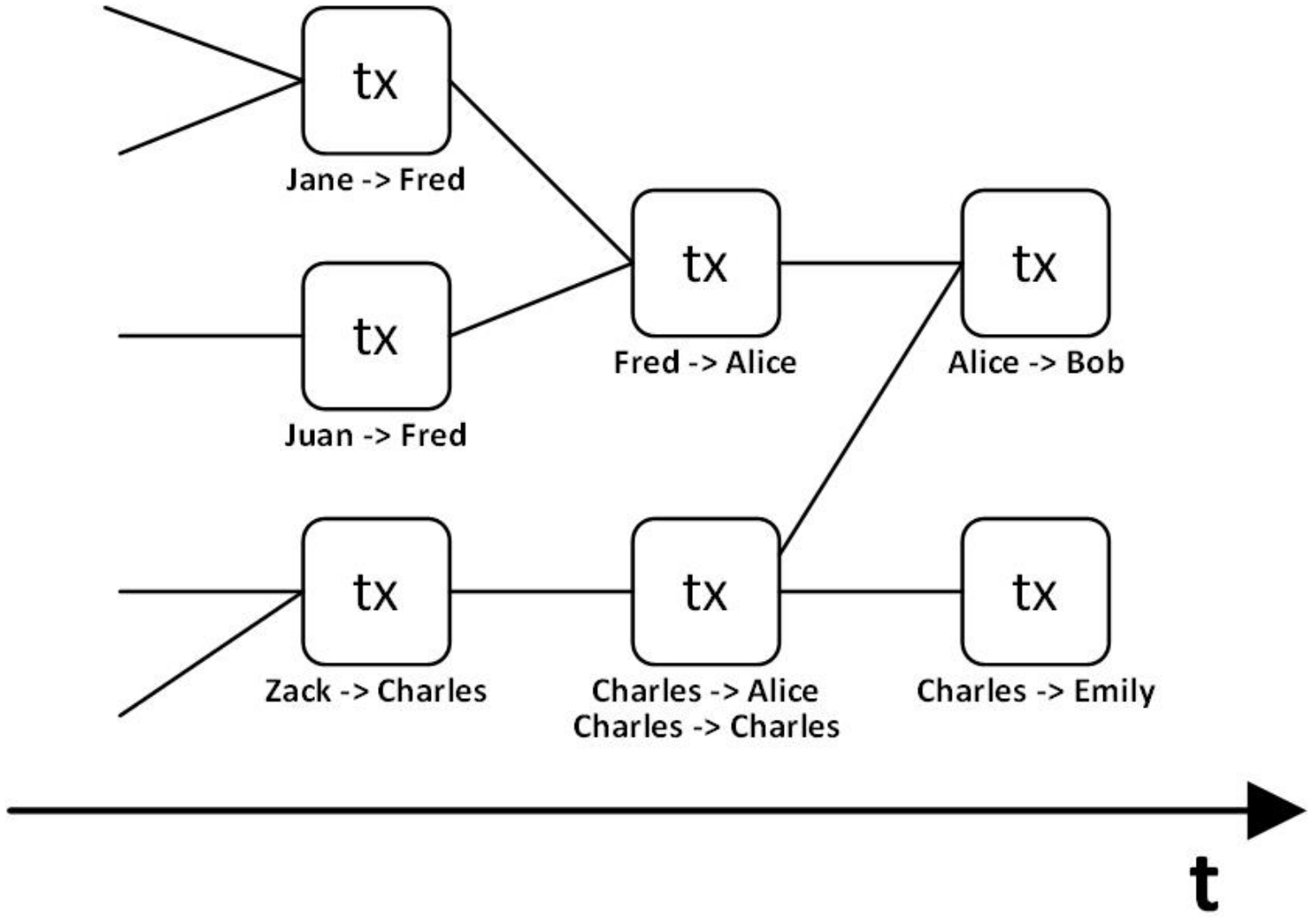
BITCOIN: Транзакции



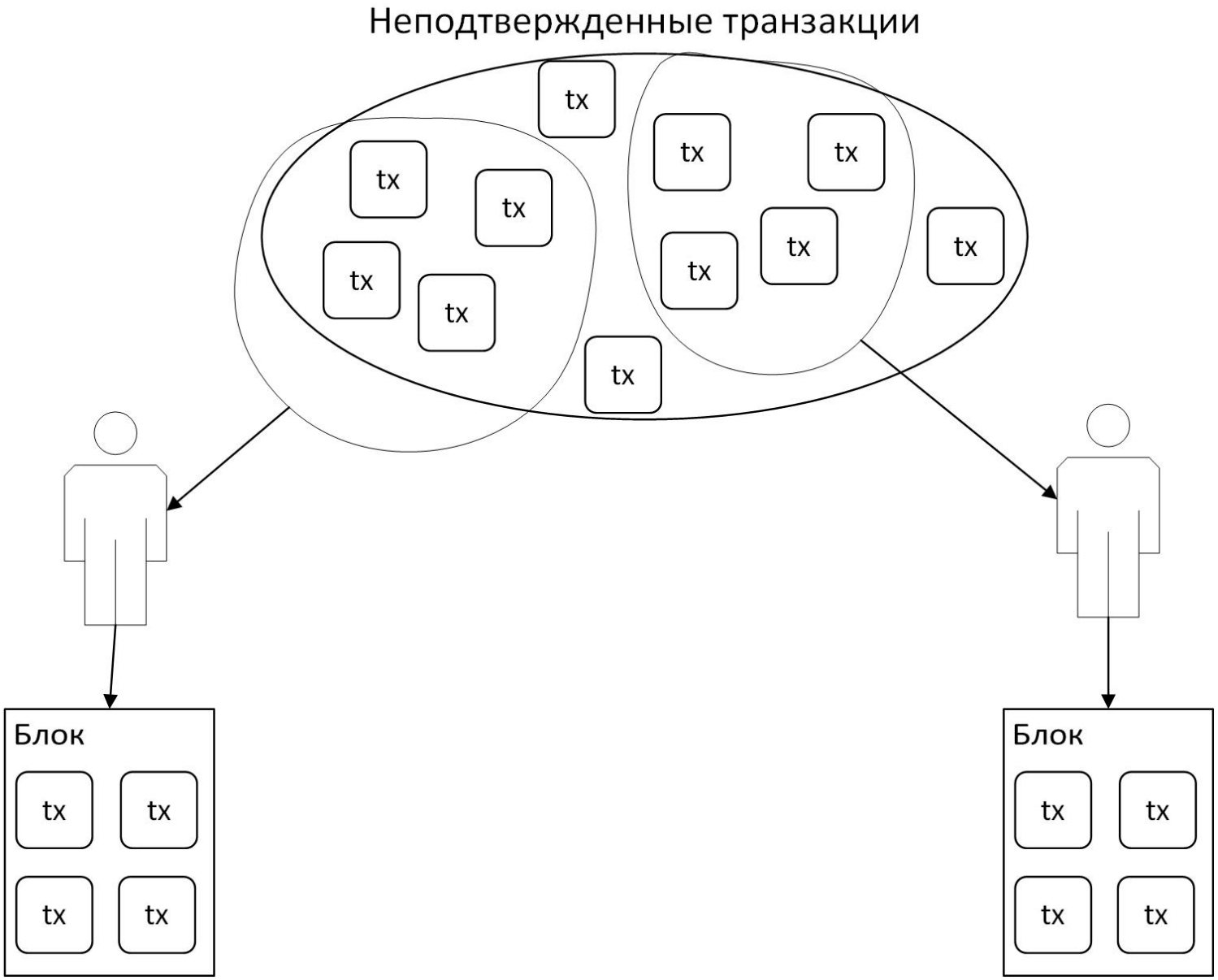
BITCOIN: Двойная трата за счет разного времени получения транзакции разными узлами



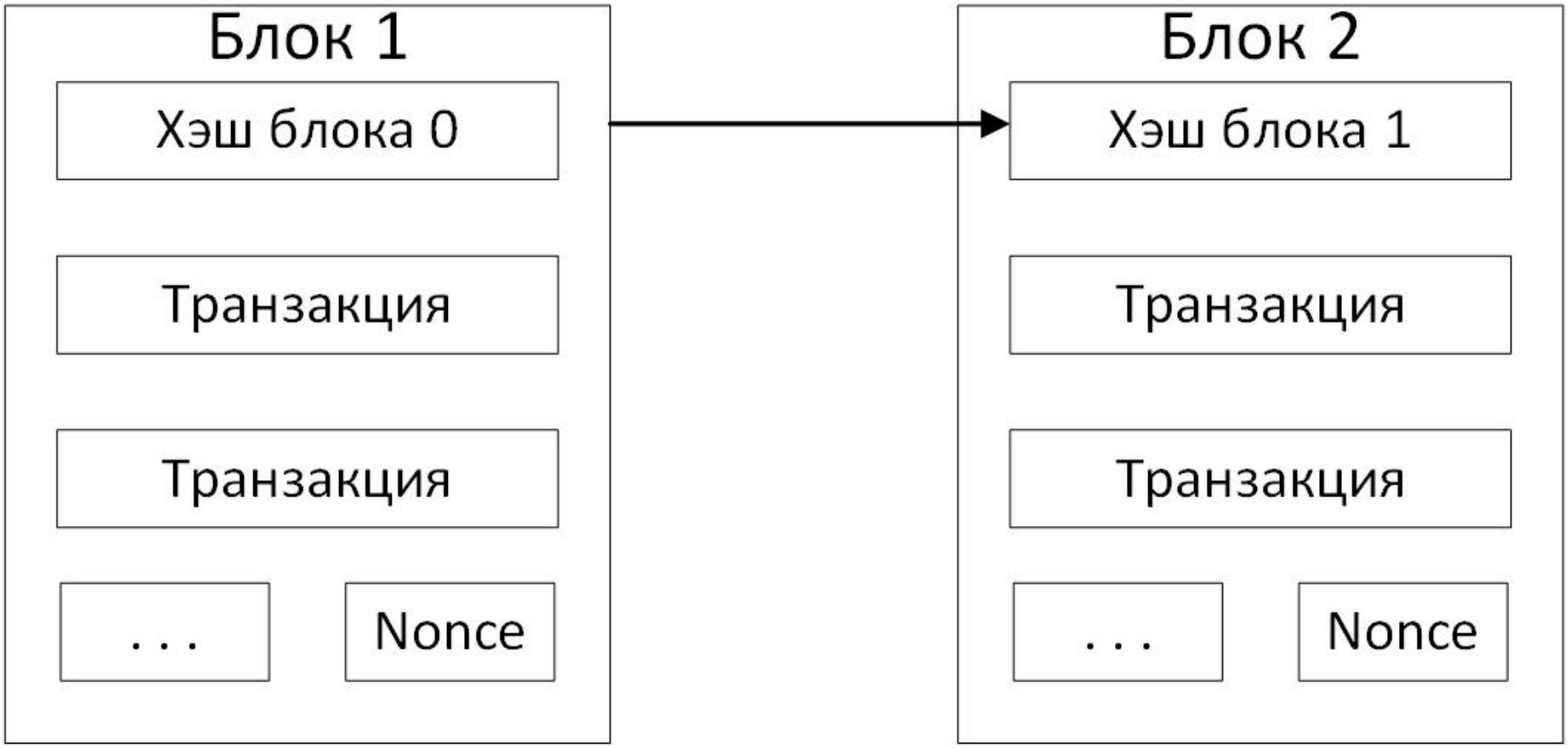
BITCOIN: цепочка транзакций



BITCOIN: Формирование блоков

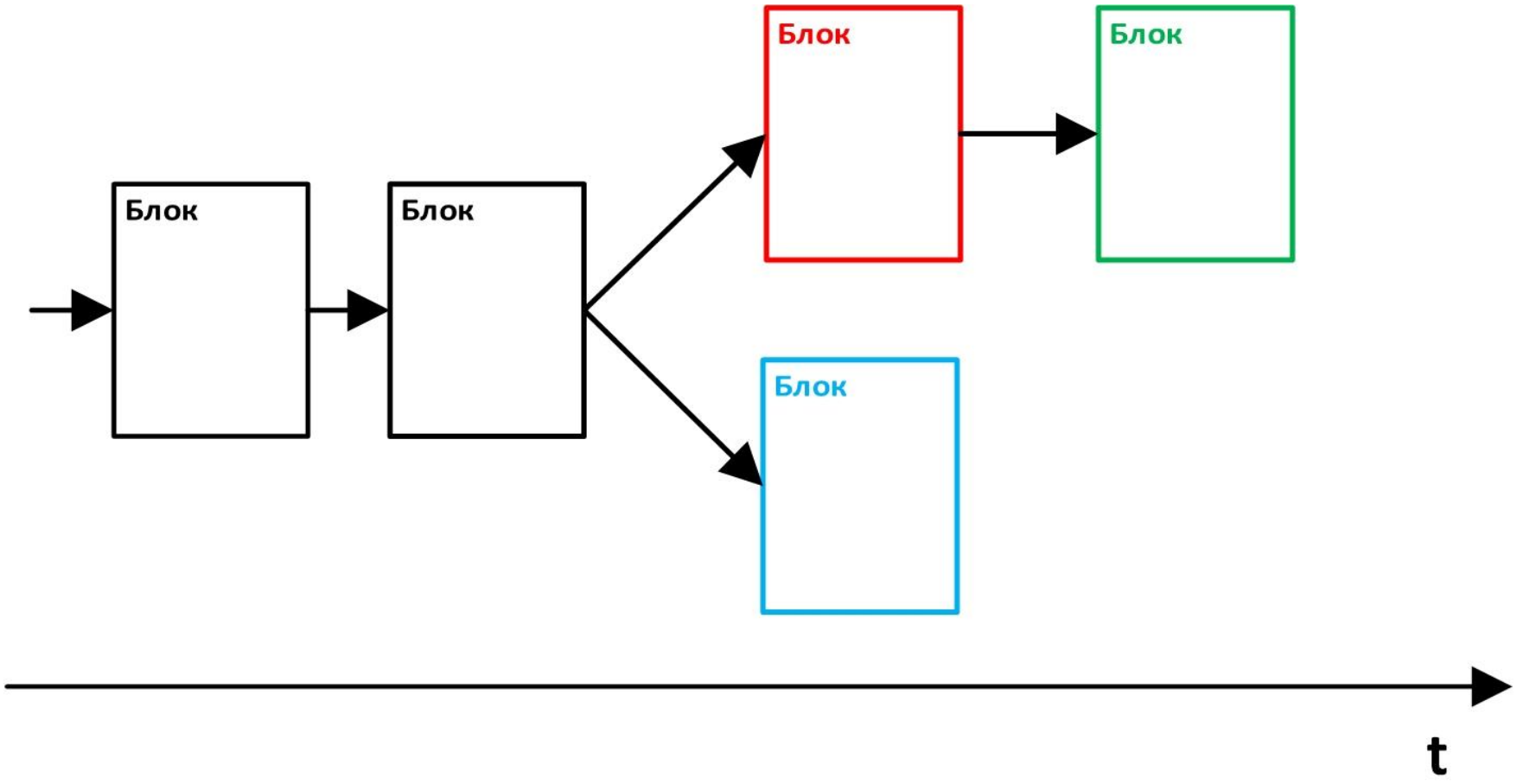


BITCOIN: цепочка блоков



BITCOIN: определение истинной цепочки блоков

Истинная – самая длинная цепочка:



BITCOIN: решения проблем электронных платежей

Проблема	Решение BITCOIN
Уязвимость к атакам и отказам	Децентрализация реестра. Распределенная валидация транзакций.
Заморозка счетов	
Комиссия посредников и другие накладные расходы	
Ведение баланса	Цепочка транзакций: защита выходов ЭЦП, прослеживаемость входов и выходов
Исключение двойной траты	Цепочка блоков: самая длинная – истинная
Защита от фальсификации данных	Цепочка блоков: связь по хэшам

Вопросы

А что кроме **Bitcoin?**

ОБЛАСТИ ПРИМЕНЕНИЯ BLOCKCHAIN

BLOCKCHAIN: Криптовалюты

Существующие криптовалюты:

- Bitcoin
- Litecoin
- Peercoin
- Nubits
- И др.

BLOCKCHAIN: Другие применения

Авторство и право владения

- Ascribe
- Bitproof
- Blockai
- Stampery
- Verisart
- Monegraph
- Crypto-Copyright.com
- Proof of Existence

Операции с товарами и сырьем

- The Real Asset Company
- Uphold

Управление данными

- Factom

Идентификация и управление доступом

- 2WAY.IO
- ShoCard
- Guardtime
- BlockVerify
- HYPR
- Onename
- Civic
- UniquID Wallet
- Identifi

Энергетика

- Energy Blockchain Labs
- Grid Singularity
- TransActive Grid от LO3 Energy

Электронное голосование

- Follow My Vote
- **Nasdaq** и правительство **Эстонии**

Азартные и видеоигры

- Etheria
- First Blood
- Etheramid
- FreeMyVunk
- CoinPalace
- Etheroll
- Rollin
- Ethereum Jackpot

Частное и государственное управление

- BITNATION
- Advocate
- Borderless
- Otonomos
- BoardRoom
- Colony

Интернет вещей

- Chronicled
- Filament
- Chimera

BLOCKCHAIN: Другие применения

Биржи труда
- Verbatm
- Appii
- Satoshi Talent
- Coinality

Прогнозирование рынка
- Augur.net

Мультимедиа
- Bittunes
- PeerTracks
- JAAK
- Paperchain

Сетевая инфраструктура
- Ethereum
- ChromaWay

Благотворительность, волонтерство
- GiveTrack
- Helperbit
- Alice
- Start Network.

Недвижимость
- UBITQUITY
- Silvertown

Репутационные рейтинги
- Open Reputation
- ThanksCoin

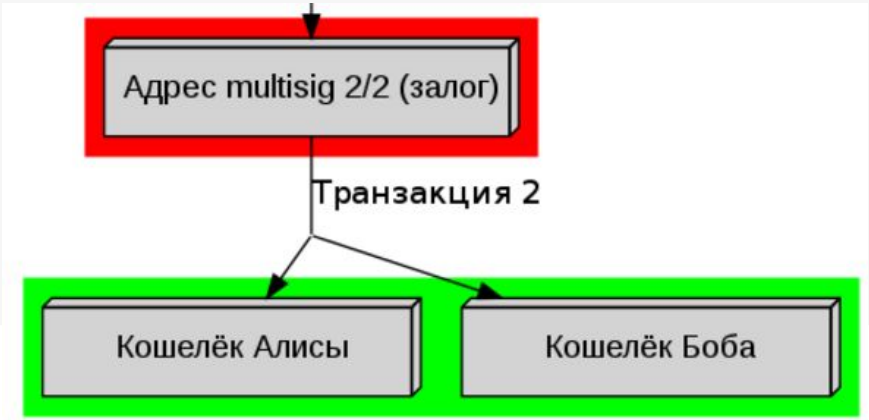
Сервисы райдшеринга
- Arcade City
- La ‘Zooz,

Социальные сети
- Datt,
- DECENT,
- Diaspora*,
- AKASHA
- Synereo.

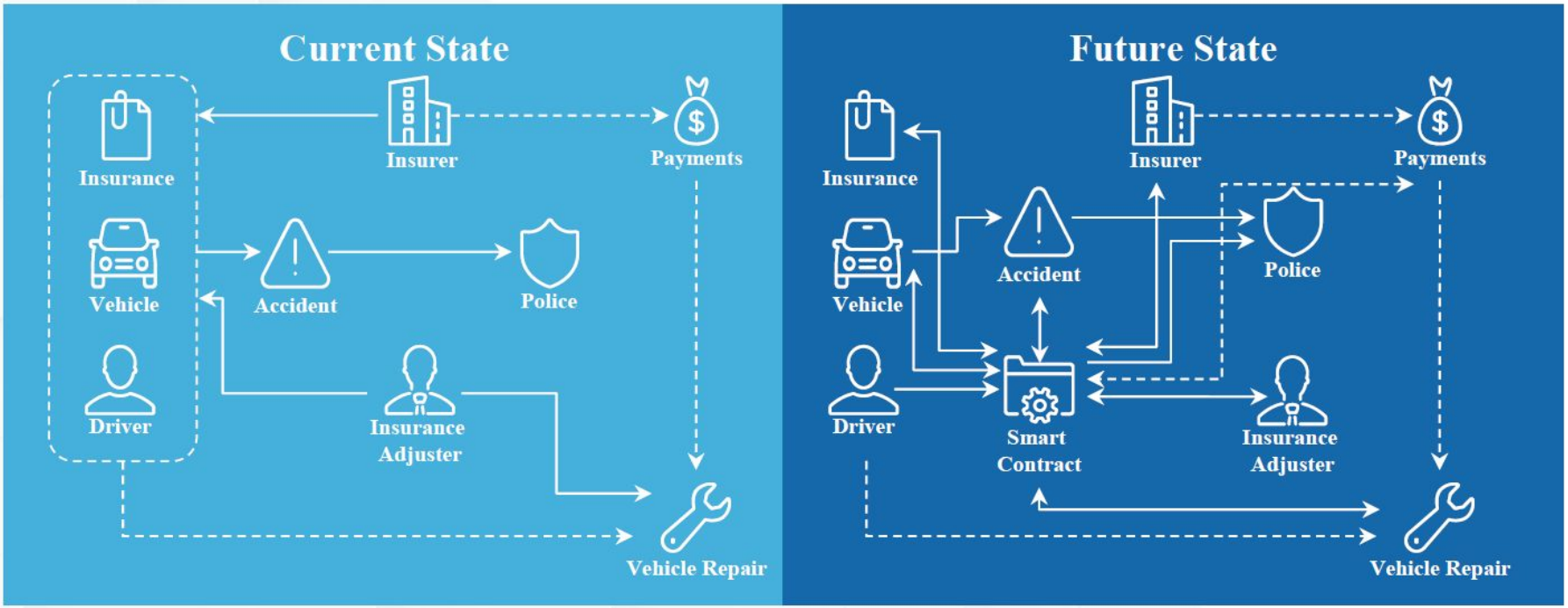
Цепочки поставок
- Provenance

Пример: Безопасные сделки без посредников

1	**Покупатель и продавец создают multisig-адрес 2/2 и переводят туда залог.**
2	**Собственно сделка** (в блокчейне, или вне)
3	**Если сделка успешна, то участники сделки забирают залог.**



Пример: Автострахование



Множество форм, отчетов и источников данных

Двойная работа страховщика по проверке документов

Субъективная диагностика

Блокчейн-репозиторий с записями о застрахованном

«Умное» авто; Оценка повреждений с помощью датчиков (вызов Смарт-контракта)

Сокращение времени на проверки документов

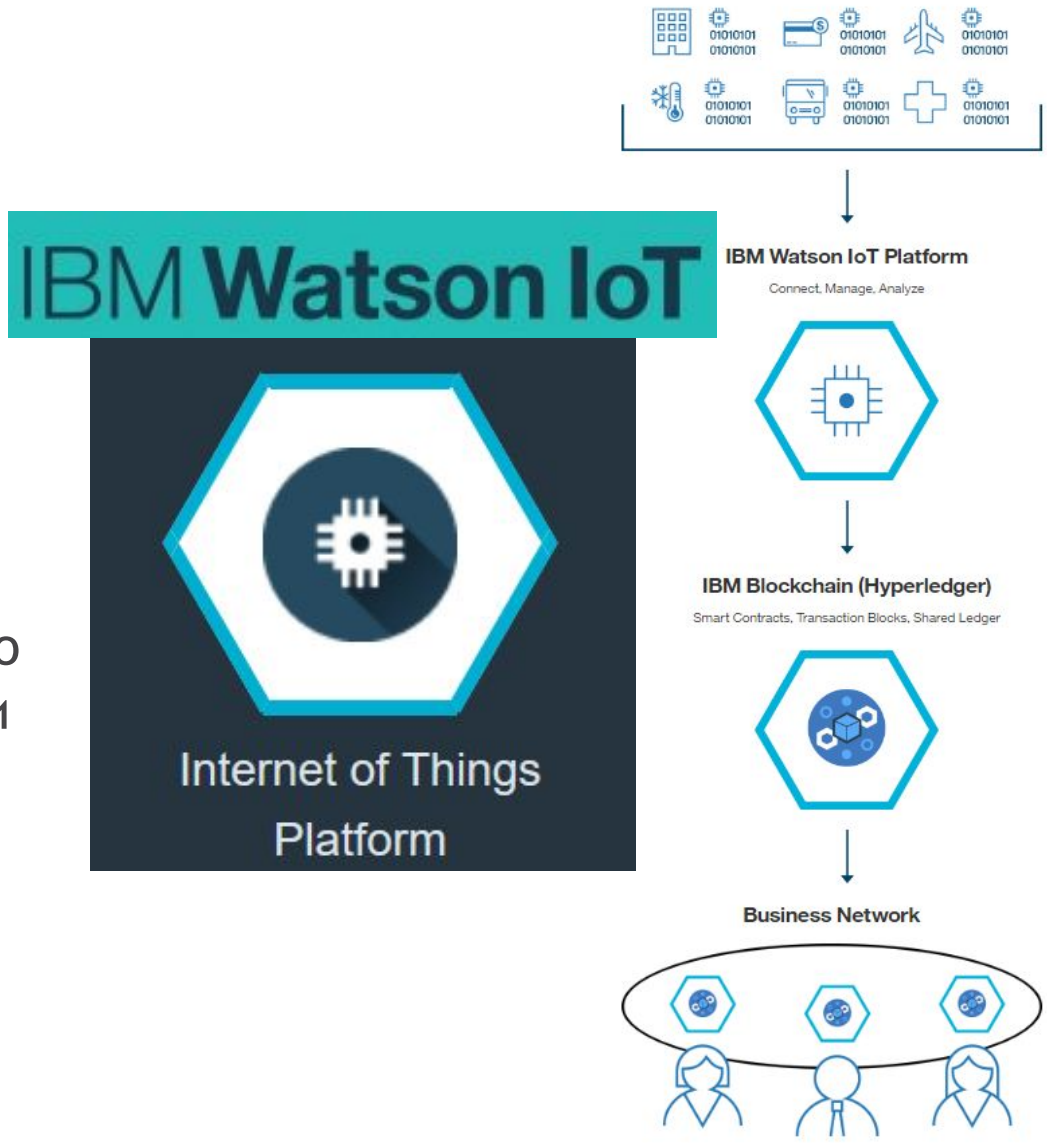
Пример: Нотариат. Завещание

- 1.Орган ЗАГС фиксирует факт смерти гражданина в блокчейне
- 2.Данный факт выступает начальным условием реализации смарт-контракта наследства
- 3.Собственность гражданина автоматически перечисляется лицам, указанным в завещании, в долях, указанных в завещании

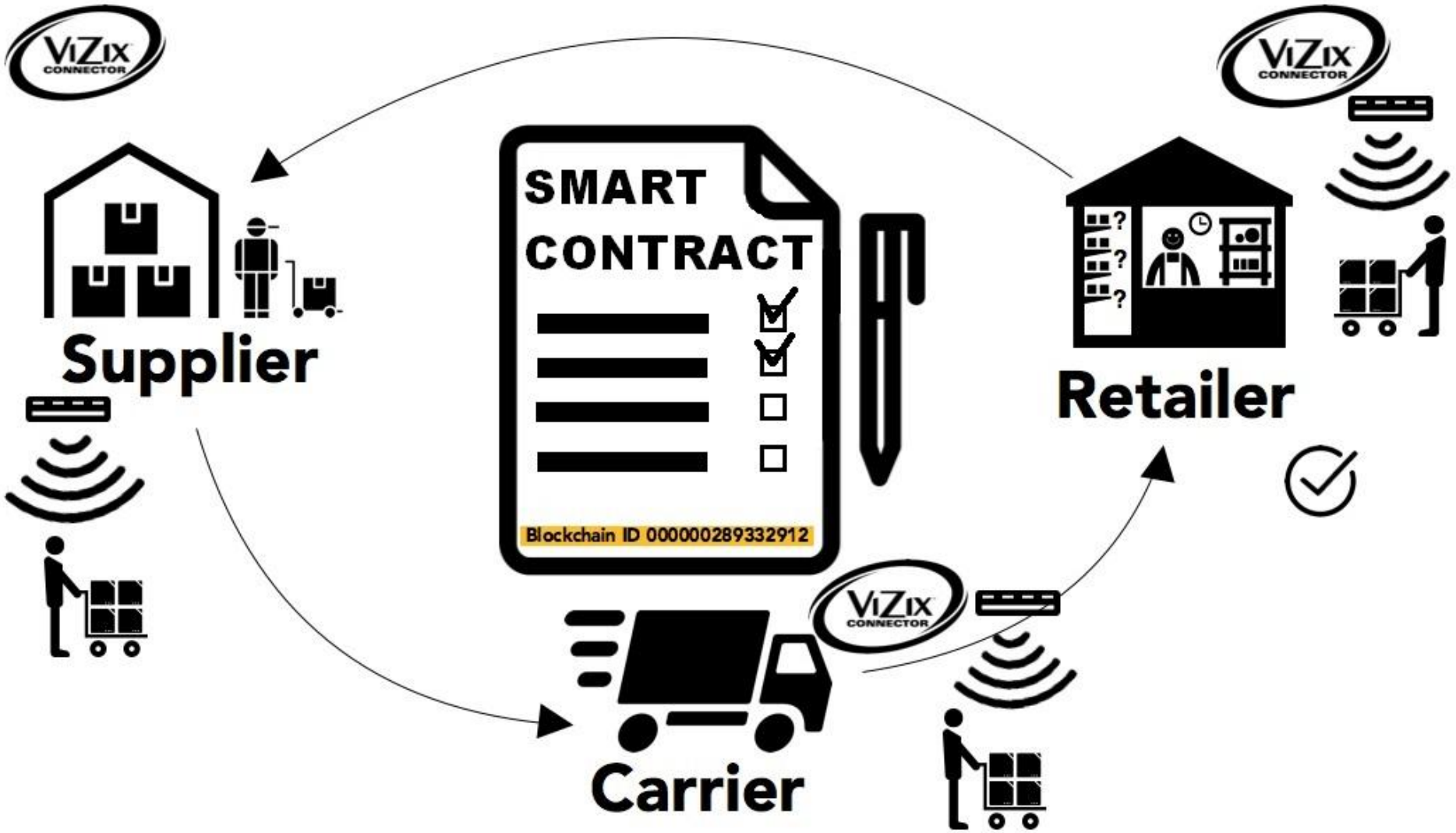
BLOCKCHAIN и Интернет вещей (IoT)

Блокчейн как **хранилище** информации, генерируемой интернет-вещами:

- Распределенность
- Неизменность
- Нет централизованного контроля и уязвимости
- Возможность генерировать транзакции, инициировать смарт-контракты



Пример: Мониторинг логистических цепочек (проект **Manifest**)



BLOCKCHAIN: В России

ЦБ РФ

- ЦБ решит проблему забалансовых вкладчиков при помощи blockchain

Сбербанк

- Управлении счетом через доверенность
- в 2017 запустит Blockchain-систему электронного документооборота

Деловая среда (Сбербанк)

- Сделки на смарт-контрактах

QIWI

- **QIWI** переведет весь процессинг на технологию блокчейн к 2021 году

BLOCKCHAIN: цитаты

Герман Греф, председатель правления Сбербанка

- Блокчейн — это та технология, которая имеет шанс вообще перевернуть сферу государственного регулирования, сферу государства в целом, финансы — все до одной сферы

Алексей Моисеев, зам. министра финансов

- Технология блокчейн является крайне важной для развития различных интернет-услуг

Николай Никифоров, министр связи

- Надо смотреть на горизонт 5-10 лет, как эта технология может помочь народному хозяйству, взаимоотношениям государства и человека, там много разных задумок

Андрей Шамраев, зам. дир.деп.ЦБ РФ

- технология блокчейн, которая может использоваться для самых различных полезных целей, трансформироваться в банковскую систему и финансовый рынок,— это то направление, в котором следует двигаться

Ольга Скоробогатова, зампред Банка России

- Эта технология точно будет развиваться. Можно закрывать на это глаза, но в 2017-2018 годах мы увидим реальные примеры использования этой технологии в финансовой сфере

BLOCKCHAIN: В мире

Microsoft & Bank of America

- Trade finance transacting

Intel

- Seafood Tracking

Intel

- Bond-trading

IBM & Maersk

- Tracks Cargo

IBM & Walmart

- Pork supply chain

BLOCKCHAIN: as a Service (BaaS)

ETH BaaS
Ethereum Blockchain as a Service

Microsoft

- Создание среды разработки и выполнения Blockchain-приложений в один клик
- Частные, публичные, консоциумные сети

IBM Blockchain

- HyperLedger **based**
- Создание тестовой Blockchain-сети в один клик
- Высокая защищенность
- Выделенная инфраструктура

amazon web services

Amazon AWS

Deloitte Rubix

- Создание универсальных Blockchain-приложений и смарт-контрактов
- Частные сети

Вопросы

Что можно «пощупать»?

ПЛАТФОРМЫ И РЕШЕНИЯ

BLOCKCHAIN: Платформы

Ethereum

- Opensource blockchain platform for distributed applications

Hyperledger Fabric

- Opensource distributed ledger platform for corporate applications

R3 Corda

- Opensource distributed ledger platform for finance

ETHEREUM: Платформа универсальных распределенных приложений **(Đapps)**

- Использует внутреннюю **криптовалюту** (Ether)
- **Баланс** хранится в аккаунте (не вычисляется)
- Алгоритм **консенсуса PoW** (планируется переход на **PoS**). Генерация блока каждые **15 сек.**
- **Кастомизация**
  - Смарт-контракты (языки: Solidity, Serpent, LLL)
  - Собственные криптовалюты
  - Семантика **транзакций** произвольная
- **Безопасность**
  - **НЕ** поддерживает Blockchain с контролем доступа (**Permissionless**)

HYPERLEDGER: Платформа корпоративных распределенных приложений

- **Не используется цепочка блоков (!)**
- **Модульная** структура: подключаемые модули, определяющие
  - Семантику **транзакций**
  - Алгоритм **консенсуса** (по умолчанию - PBFT без майнинга блоков, без внутренней криптовалюты)
  - Алгоритмы **криптографии**
  - **Хранилища** данных
- **Смарт-контракты** (языки Java, Go)

HYPERLEDGER: Платформа корпоративных распределенных приложений

- **Безопасность**
  - Поддерживает Blockchain с **контролем доступа (Permissioned)**
  - **Конфиденциальные** транзакции и смарт-контракты
- **Идентифицируемость**
  - **Участников**
  - **Модулей системы**
  - **Ресурсов**
  - **Смарт-контрактов**
- **Межсетевые** транзакции и коммуникации
- **Переносимость** модулей между разными платформами, сетевыми средами

R3 CORDA: Платформа распределенных финансовых приложений

- **Не используется цепочка блоков (!)**
- **Нет майнинга блоков** – использует децентрализованный сервис валидации транзакций (**notary nodes**)
- Узлы обрабатывают **только «свои» транзакции**
- **Разные/подключаемые** алгоритмы **консенсуса** (по умолчанию – BFT или Raft, без внутренней криптовалюты)
- Смарт-контракты (языки Java, Kotlin)

R3 CORDA: Платформа распределенных финансовых приложений

- **Безопасность**
  - Поддерживает Blockchain с **контролем доступа** (**Permissioned**)
  - **Конфиденциальные** транзакции и смарт-контракты

- **Идентифицируемость** участников
- Хорошая **масштабируемость** (за счет отсутствия майнинга, и наличия контроля доступа)

BLOCKCHAIN: Сравнение платформ

	Ethereum	Hyperledger	R3 Corda
Membership type	Permissionless	Permissioned	Permissioned
Smart Contracts	Yes. Solidity, Serpent, LLL languages	Yes, so called “chaincode”. Go or Java, other languages	Yes, but limited. Tweaked JVM. Java or Kotling languages
Consensus protocol	Proof of Work	Different/pluggable. (P)BFT by default	Different/pluggable . BFT or Raft by default
Blocks	Yes	No	No
Mining	Yes	No. “Validating Peer”	No. “Notary node”
Permissionless	Yes	No	No
Oracles	Yes	No	Yes. Built-in support
Access Control Lists (ACL)	No	Yes	Yes

SMART CONTRACT: Пример требований

- **Участники**: ***СтрахЗемТряс*** корп. («страхователь») и ***Нетряска*** корп. («застрахованный»)
- **Зона покрытия**: Пять районов г. Нью-Йорка (Оракул 1)
- **Условия страхования**: Застрахованный получает 5 миллионов американских долларов в биткоинах (BTC) в случае, если геологическая служба Соединенных Штатов (ГССШ) сделает публичное заявление о том, что эпицентр землетрясения был зафиксирован в пределах зоны покрытия
  - 3.1 Реагировать на землетрясения с магнитудой 5.0 и выше, согласно данным службы уведомлений о землетрясениях ГССШ (или данные формата синдикации Atom) (Оракул 2)
  - 3.2 Определять курс биткоина следует на сайте CoinDesk в разделе Bitcoin Price Index на момент времени выплаты премии

SMART CONTRACT: Пример требований (продолжение)

- 3.4 Выплачивать страховые выплаты на кошелек застрахованного на *[адрес кошелька]*

5. **Премия**: 50 тысяч американских долларов в биткоинах (BTC) за 12 месяцев страхования

   4.1. Определять курс биткоина следует на сайте CoinDesk в разделе Bitcoin Price Index на момент времени выплаты премии (Оракул 3)

   4.2. Оплачивать на кошелек страхователя на *[адрес кошелька]*

6. **Изменение условий страхования**: застрахованный имеет право изменить условия страхования на второй 12месячный период после выплаты второй премии не позднее, чем через 72 часа после завершения первого 12месячного периода.

7. **Минимальный уровень платежеспособности**: Страхователь обязан обеспечить ликвидный актив в размере как минимум 30% от

SMART CONTRACT: Пример требований (окончание)

6.1. Баланс ликвидного актива страхователя доступен на *[адрес кошелька]*

6.2. Ежедневные показатели уровня возможных убытков застрахованного в зоне покрытия доступны на [*адрес кошелька*]

6.3. Страхователь обязуется выплатить премию застрахованному, если баланс его ликвидного актива упадет ниже 30% от максимального дневного уровня возможных убытков застрахованного в пределах зоны покрытия за последние 30 дней.

7. **Дополнительно**: общие нормы и условия

7.1 Землетрясения и подземные толчки которые были зафиксированы в течении 168 часов

Вопросы

Спасибо!