

Технология

# BLOCKCHAIN

## BLOCKCHAIN - ЭТО:

- **Технология**

Учета и обмена **правами** собственности на цифровые активы  
в **одноранговой** сети

- **Структура данных**

Синонимы

- Распределенный реестр
- **Distributed Ledger**

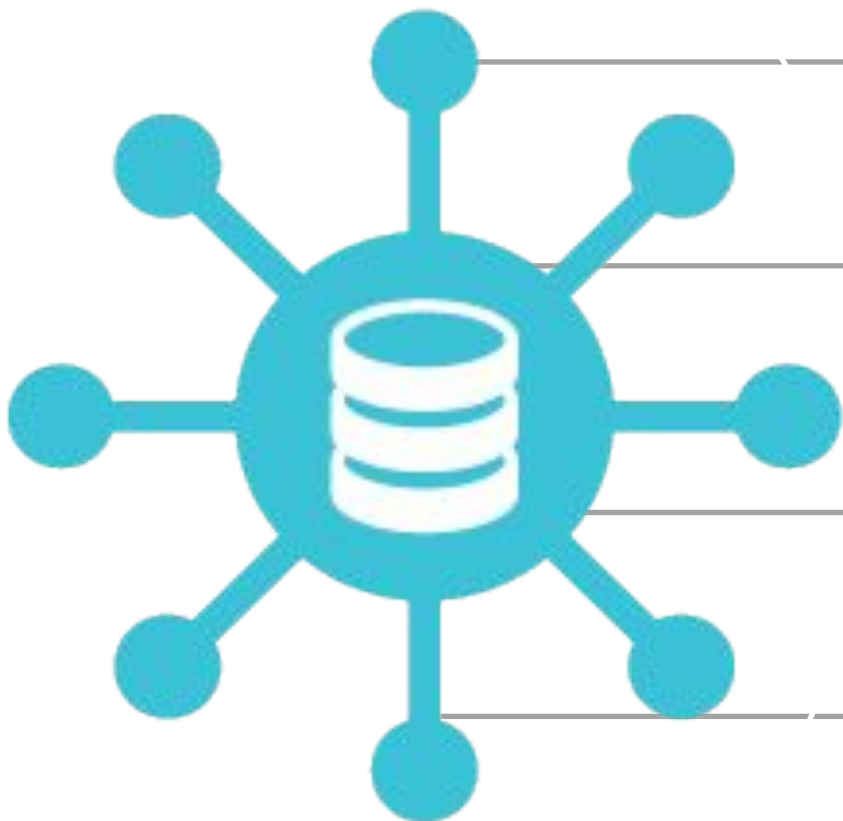
# Традиционные (централизованные) системы электронных расчетов и учета



## Посредник:

- Аутентифицирует участников
- Ведет Реестр транзакций
- Ведет Счета участников
- Предотвращает Двойное списание (double spending)

# Традиционные (централизованные) системы электронных расчетов и учета



## Уязвимость

к атакам и  
отказам



Возможность  
удаления/измене  
ния транзакций



после  
выполнения  
Удорожание  
транзакций из-за  
КОМИССИИ



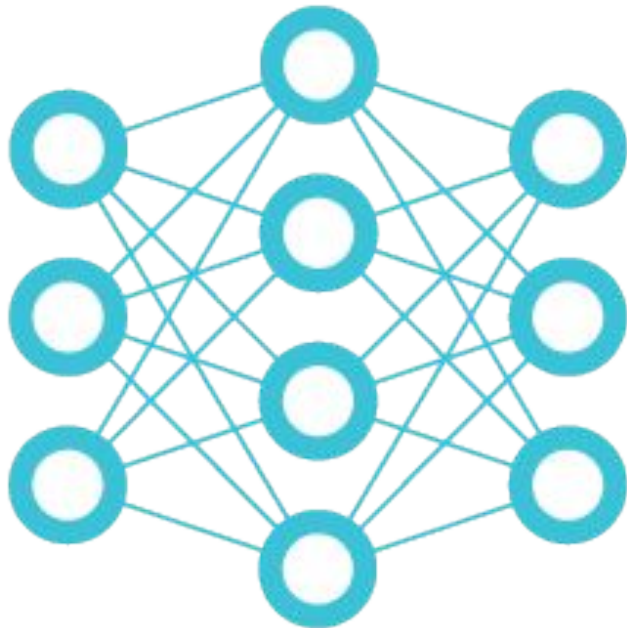
• Непрактичность  
маленьких и/или  
разовых (casual)  
транзакций

## Закрытость данных



• Затрудненность  
контроля и  
аудита

# Одноранговые (p2p) системы электронных расчетов и учета



## BLOCKCHAIN:



Аутентификация участников с помощью ЭЦП

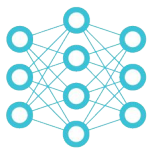
Реестр транзакций

- ведется коллективно
- хранится у каждого



Счета участников не ведутся

- Двойное списание - избегается коллективным консенсусом



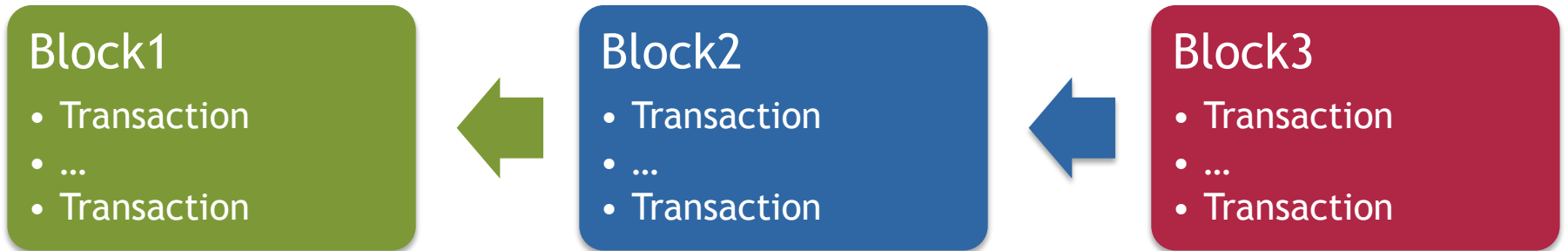
# BLOCKCHAIN: структура данных

Транзакции объединены в Блоки

Каждый блок включает хэш предыдущего

hash1

hash2



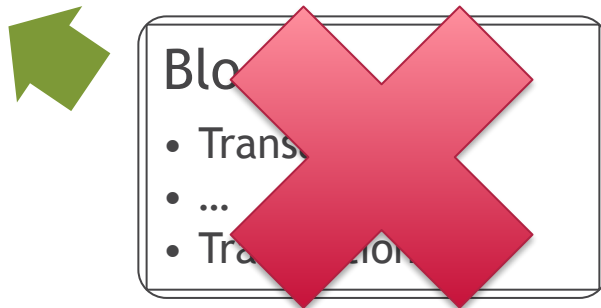
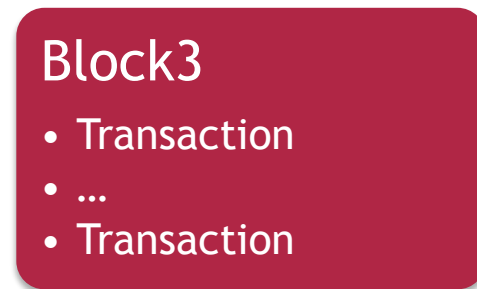
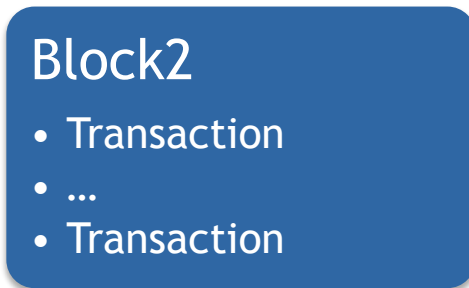
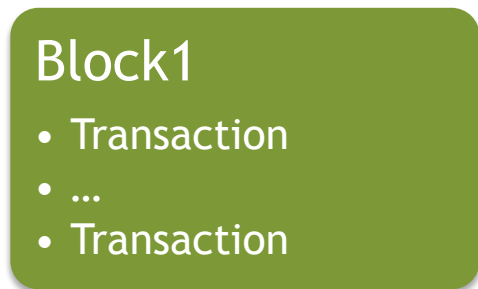


# BLOCKCHAIN: структура данных

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

hash1

hash2

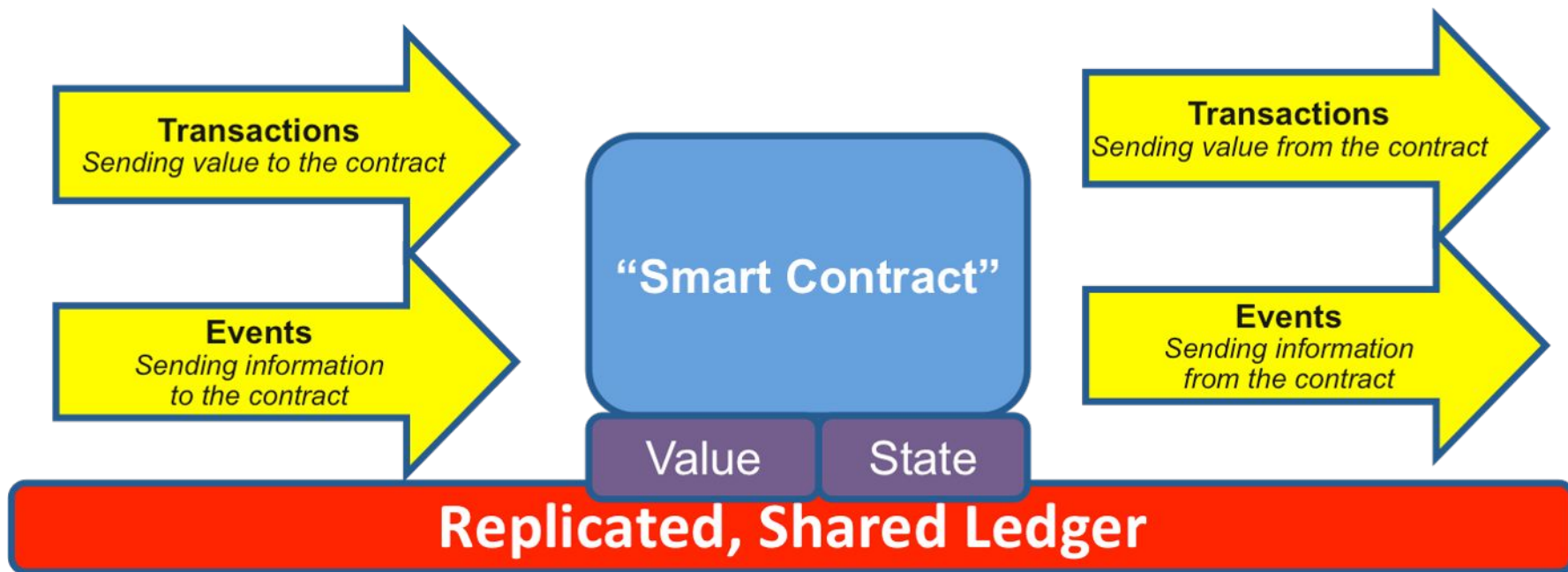




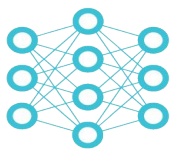
# BLOCKCHAIN: Смарт-контракты

Исполняемый код в Блокчейне.

Обеспечивает выполнение контракта без участия человека (например - **пари**)

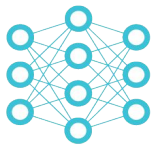






# ВЛОКЧЕЙН: ОСНОВНЫЕ ИДЕИ И характеристики

<input type="checkbox"/> Децентрализация	Исключение посредника обмене. Обмен выполняется по схеме p2p.	Удешевление операций (нет комиссии посредника); Упрощение процесса.
<input type="checkbox"/> Распределенность	Вся информация о всех транзакциях хранится на всех компьютерах участников обмена. Нет единого центра уязвимости.	Устойчивость к атакам и отказам оборудования
<input type="checkbox"/> Открытость	Все участники знают обо всех транзакциях (но не о конкретных участниках транзакций).	Прозрачность, публичность, легкость аудита
<input type="checkbox"/> Криптозащита	Все транзакции подписываются ЭЦП	Верифицируемость
<input type="checkbox"/> Анонимность	В качестве адреса участника транзакции используется абстрактное 32-битное число	
<input type="checkbox"/> 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.

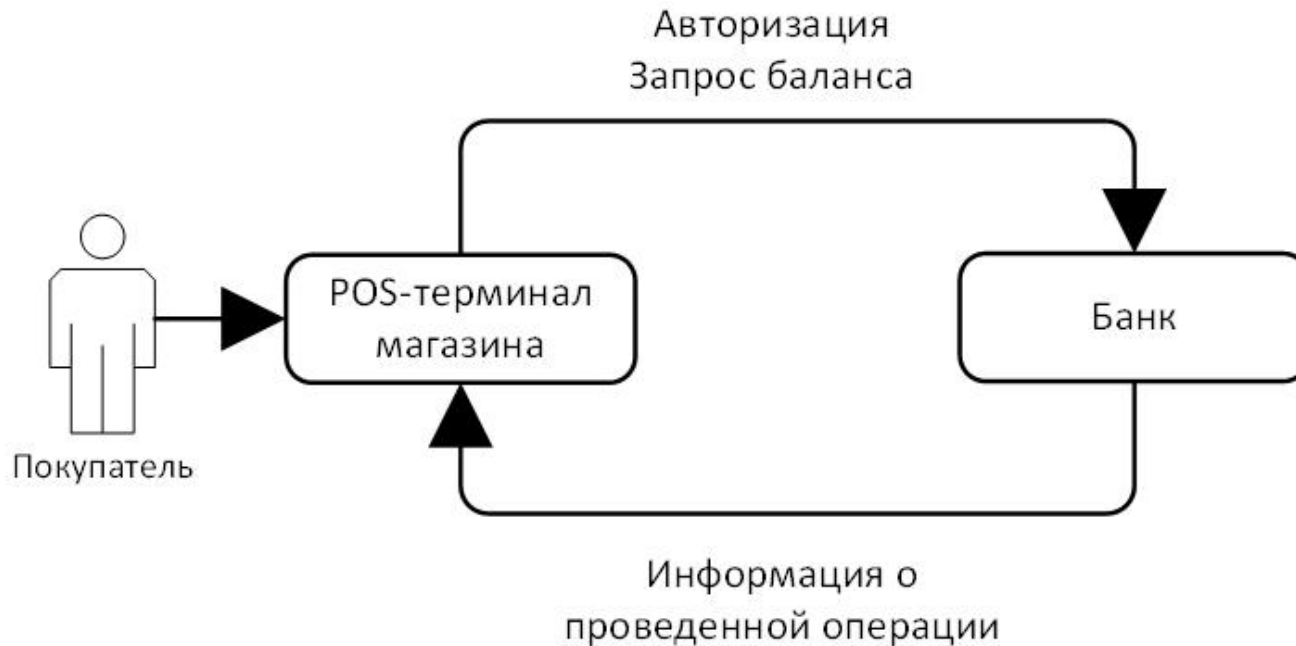
# Вопросы



Самый первый и известный **Blockchain**

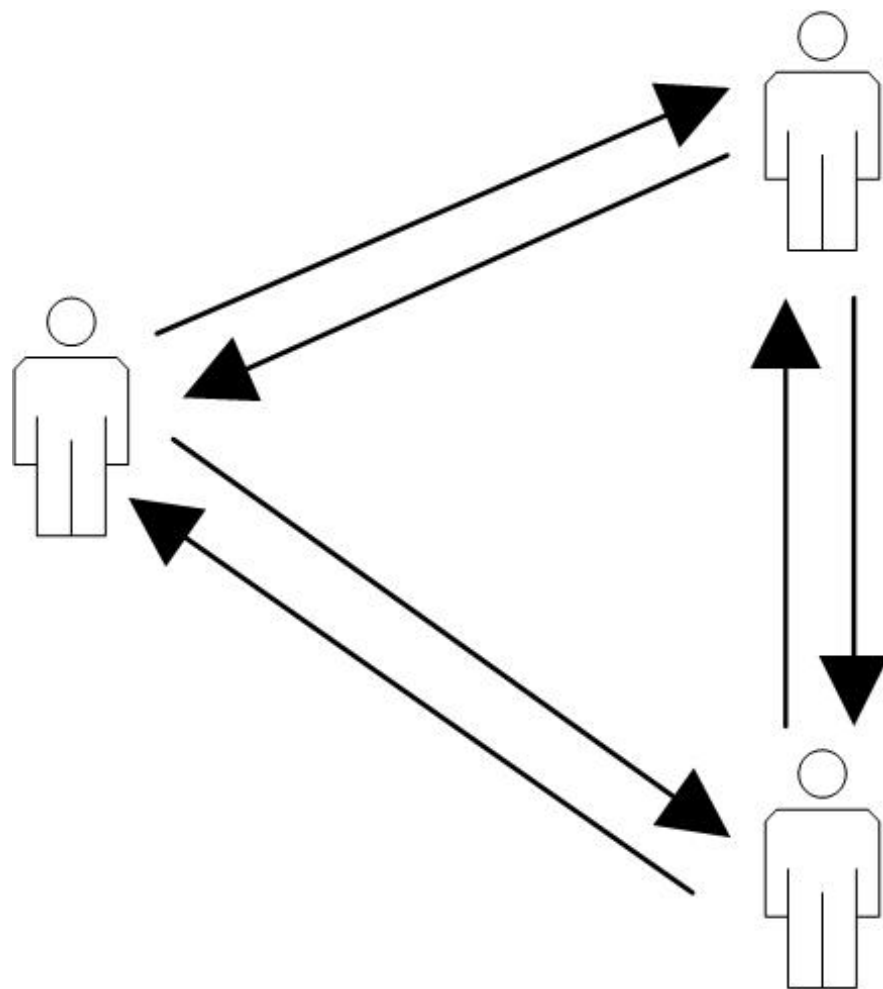
# BITCOIN

# Электронные платежи: проблемы



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

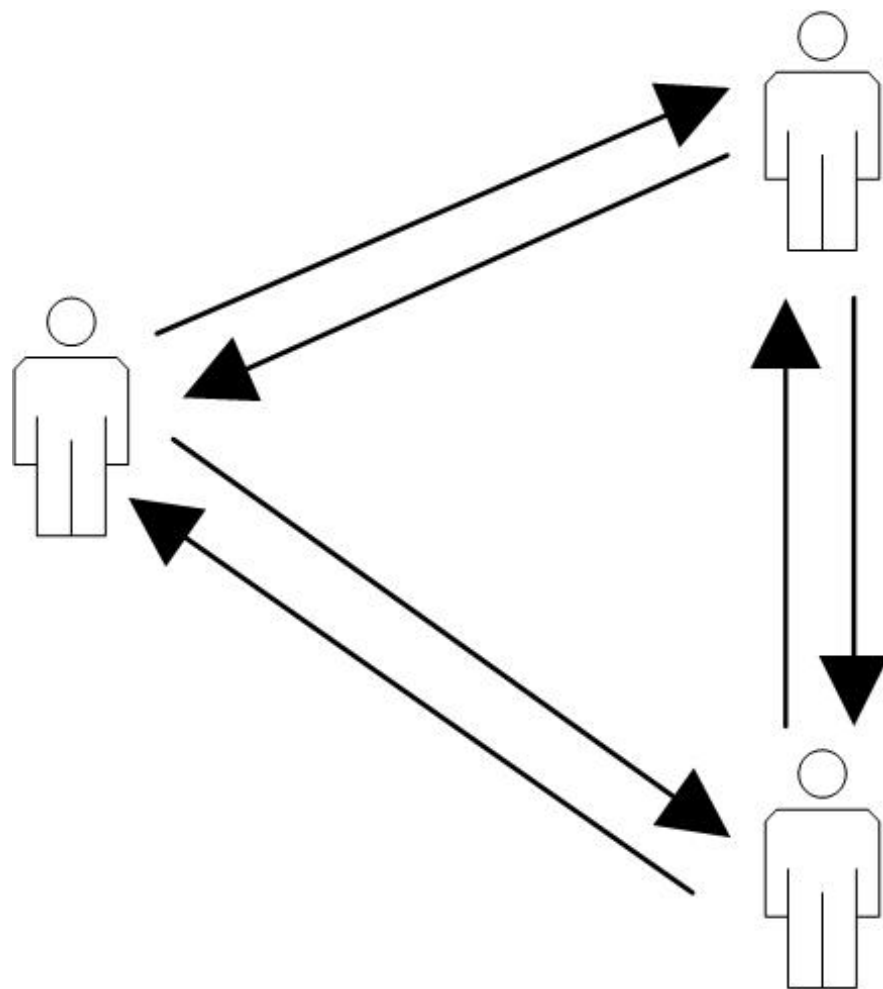
# Одноранговая сеть (без посредника)



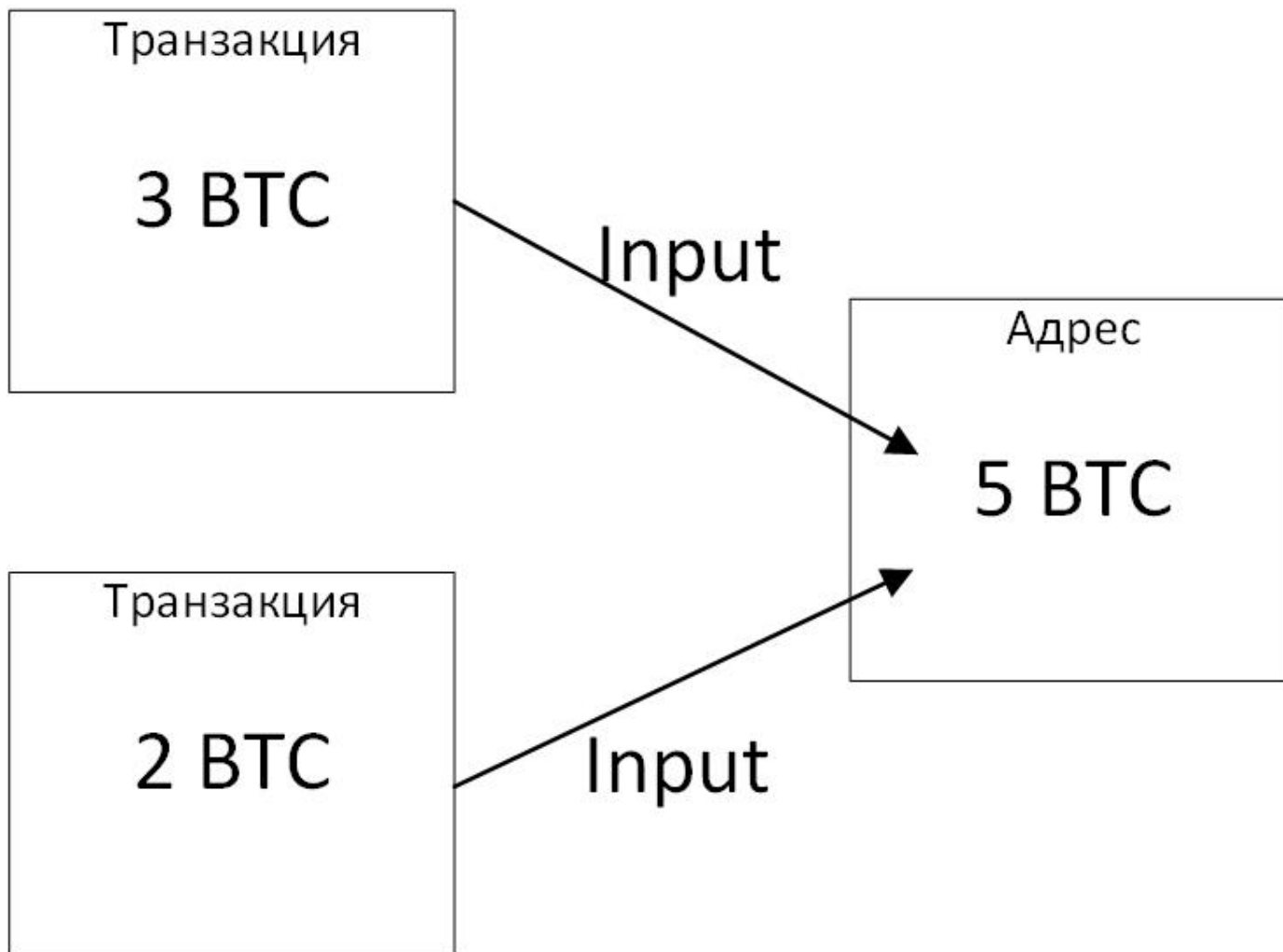
# Одноранговая сеть (без посредника)

## Проблемы

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

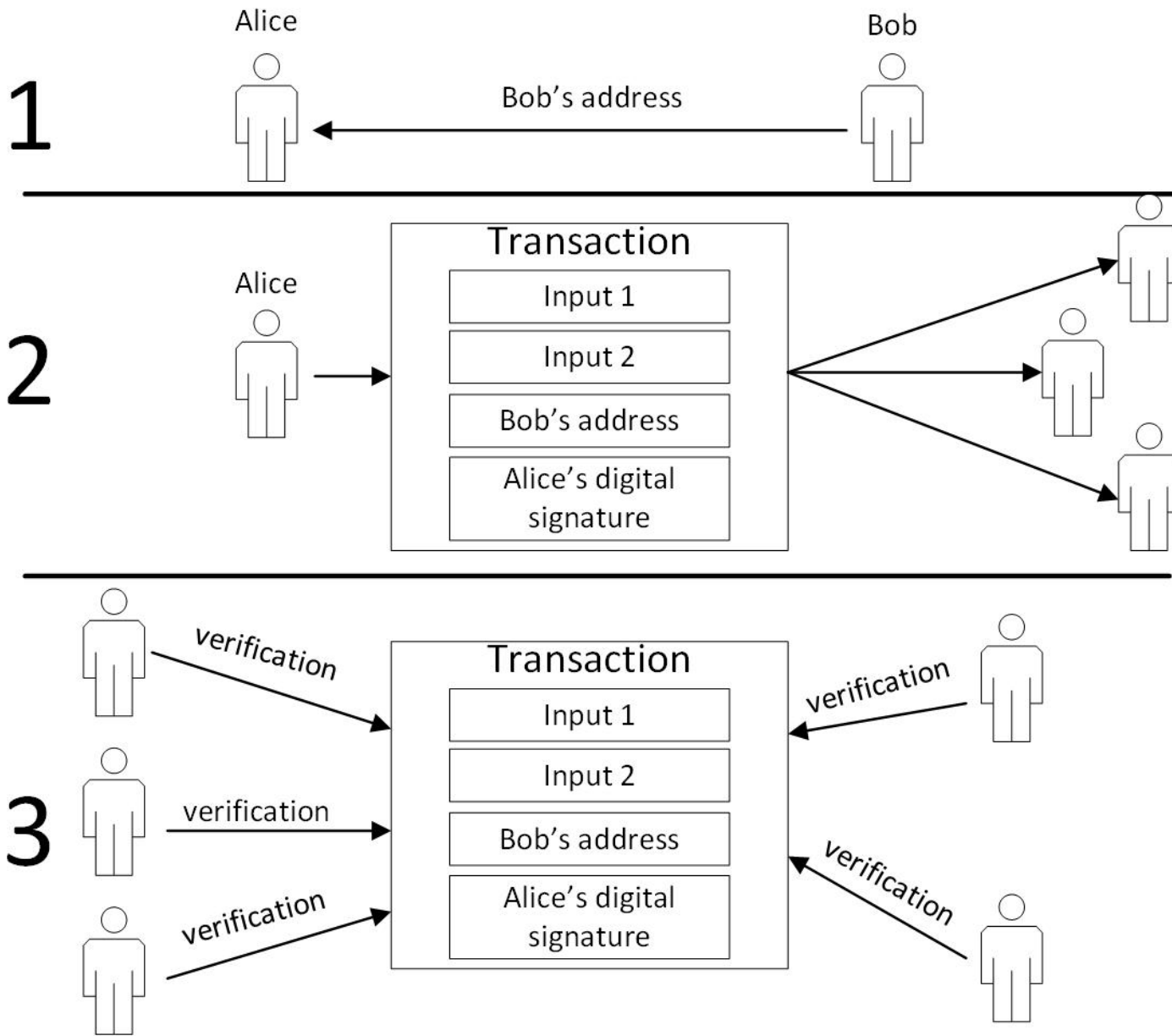


# BITCOIN: Баланс

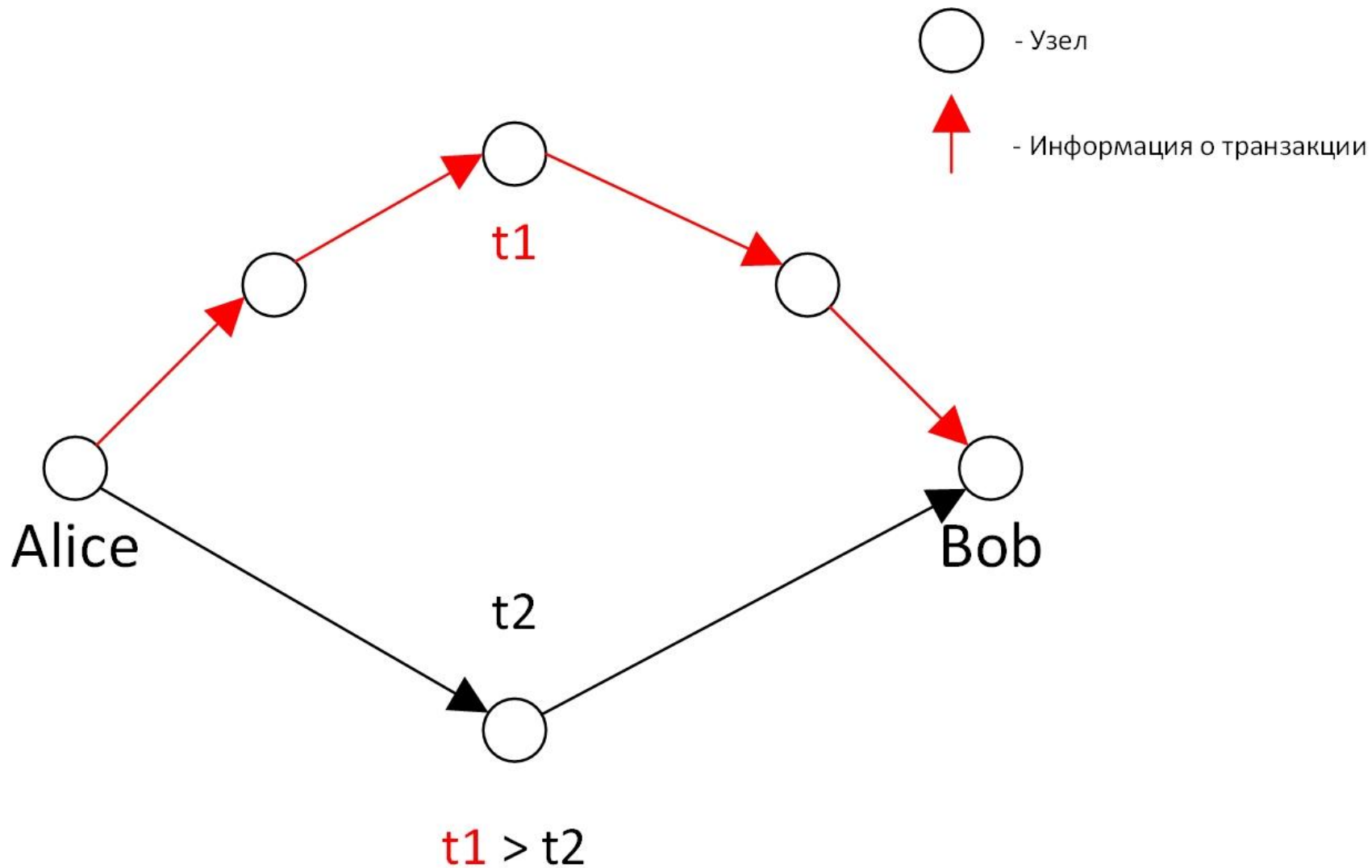




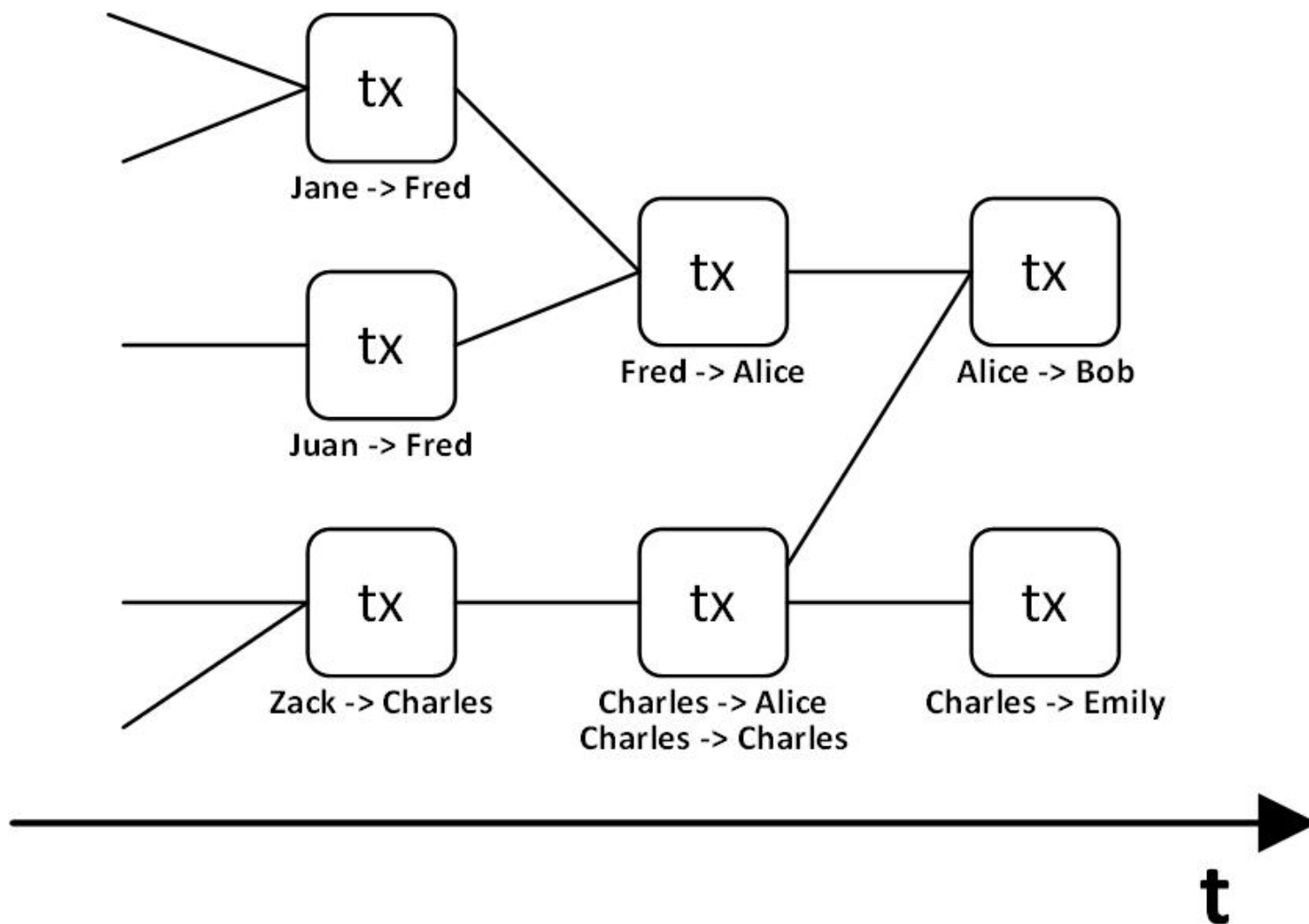
# BITCOIN: Транзакции



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

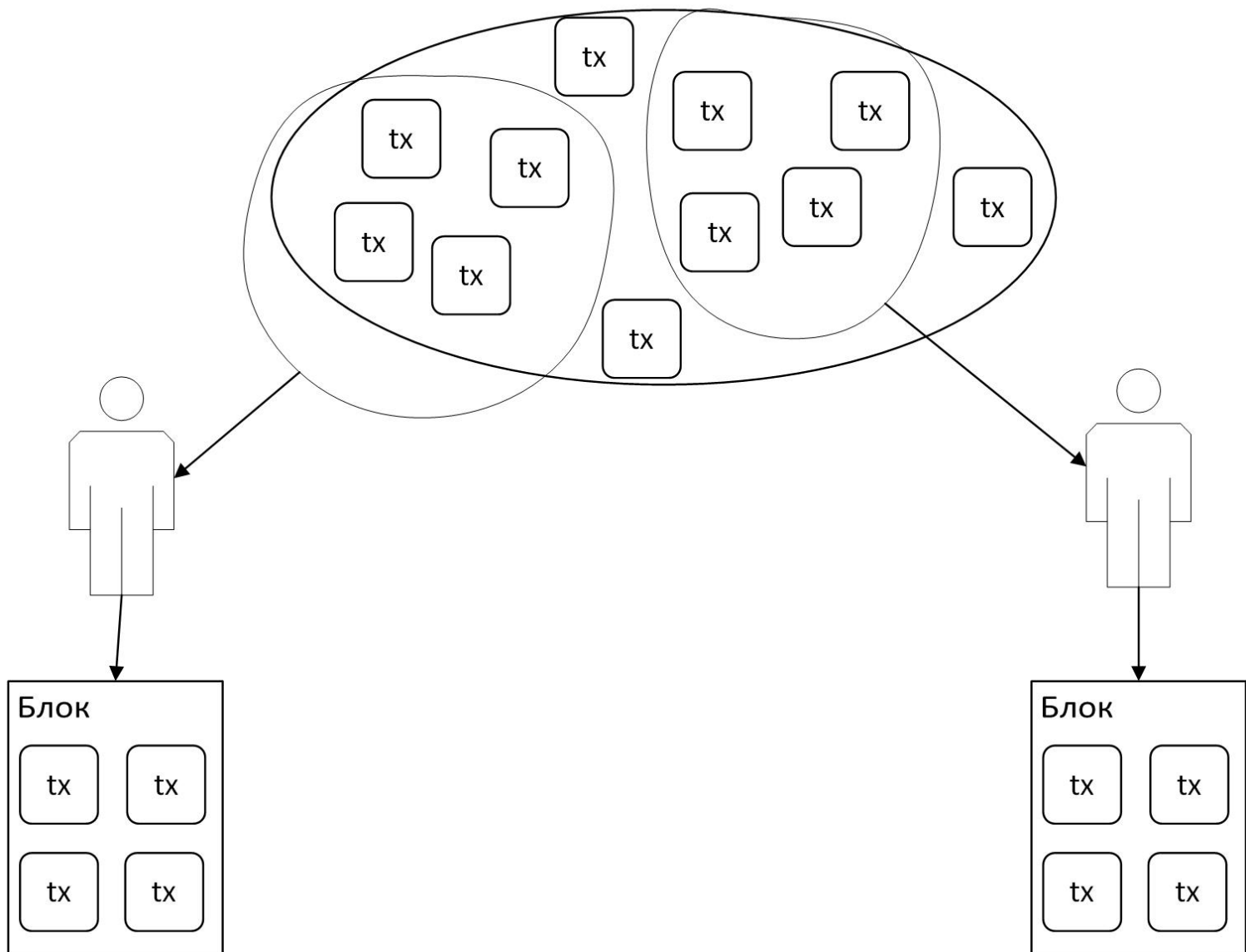


# BITCOIN: цепочка транзакций

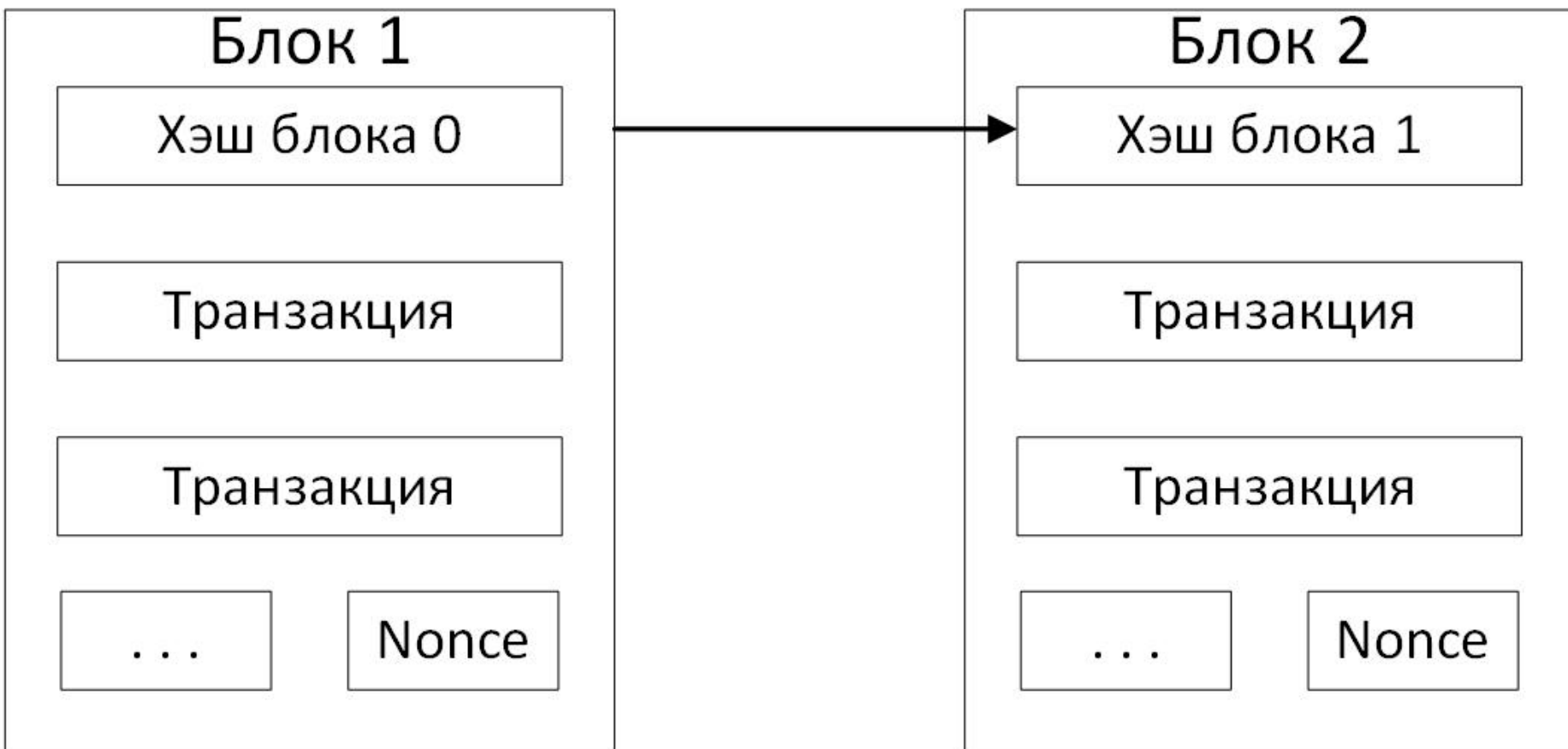


# BITCOIN: Формирование блоков

Неподтвержденные транзакции

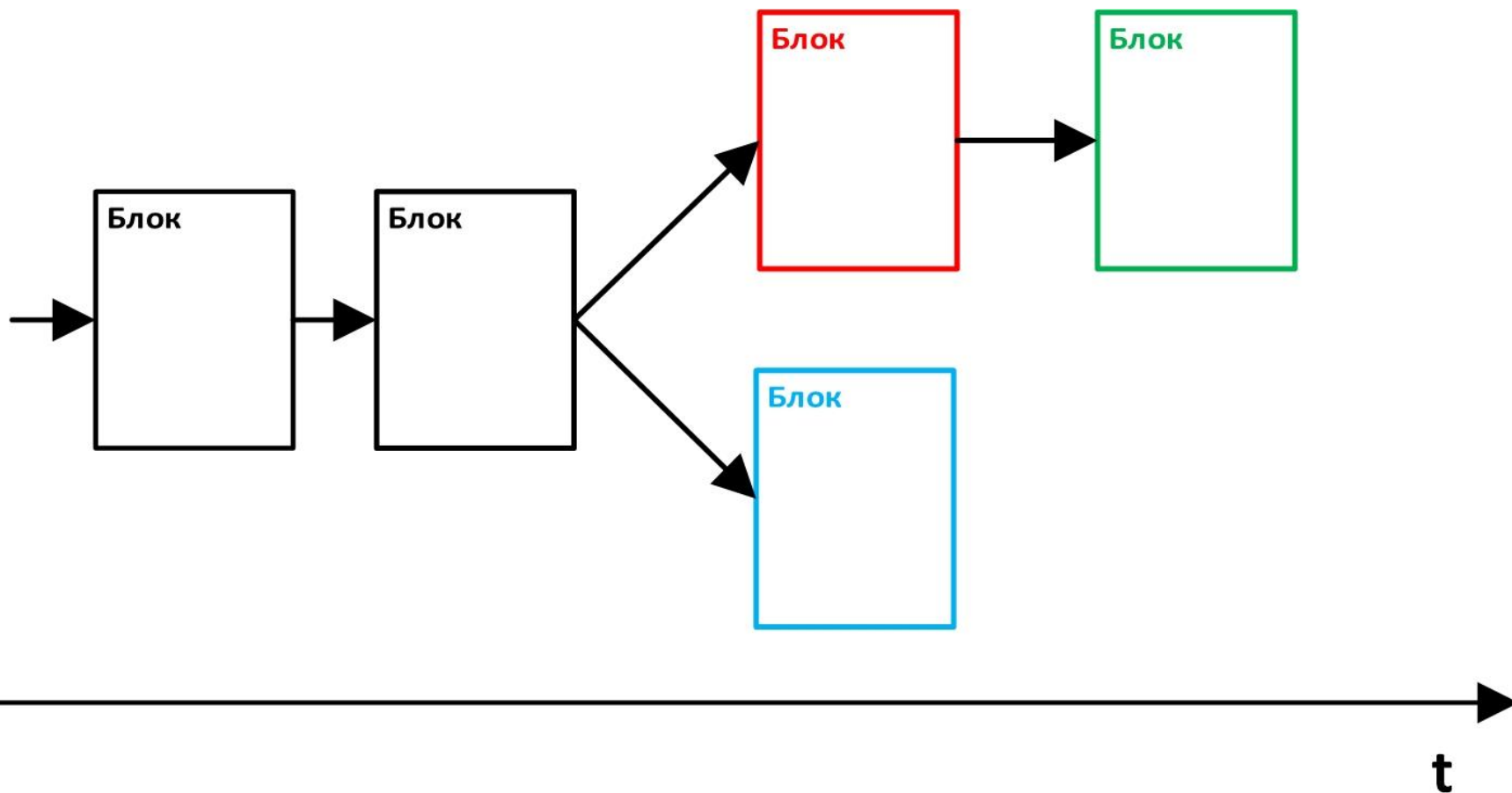


# BITCOIN: цепочка блоков



# 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

# БЛОКЧЕЙН: 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**.



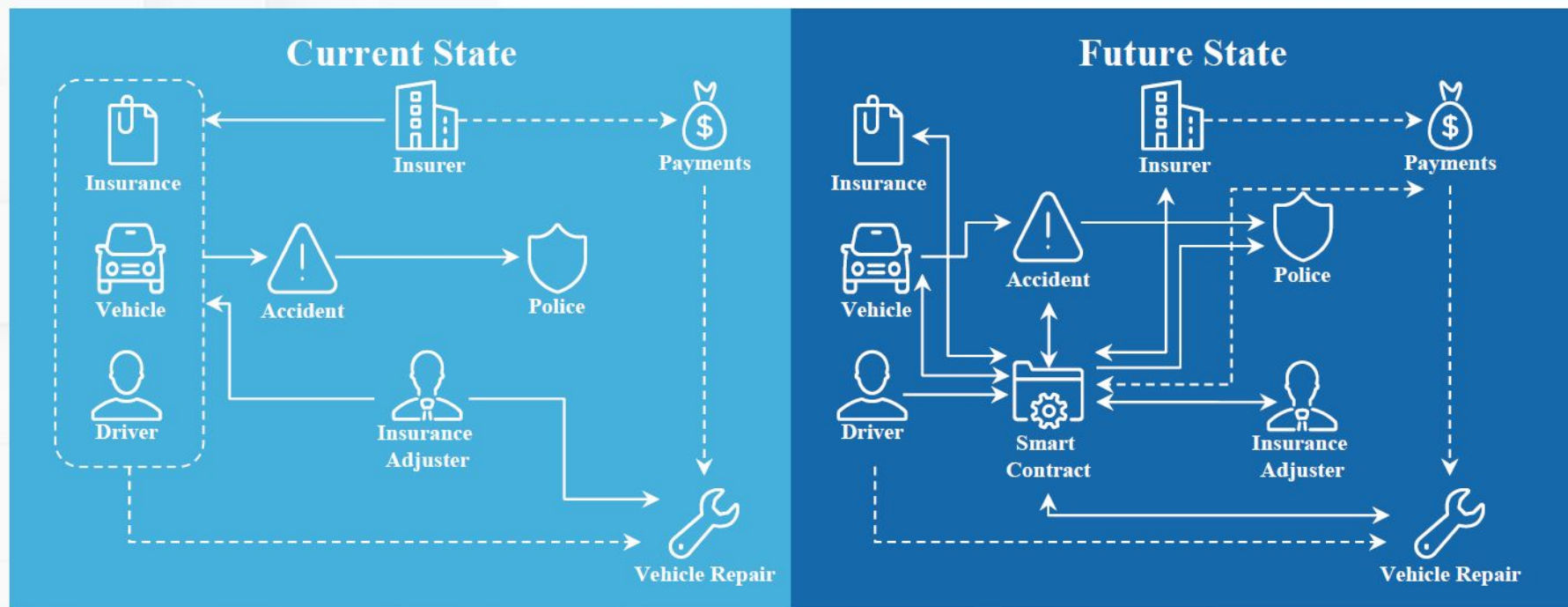
**2** Собственно **сделка** (в блокчейне, или вне)



**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

IBM Watson IoT



IBM Watson IoT Platform

Connect. Manage. Analyze

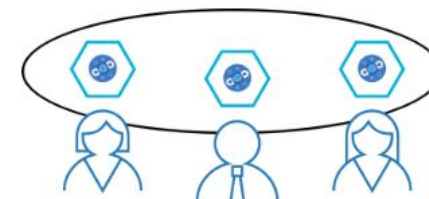


IBM Blockchain (Hyperledger)

Smart Contracts, Transaction Blocks, Shared Ledger

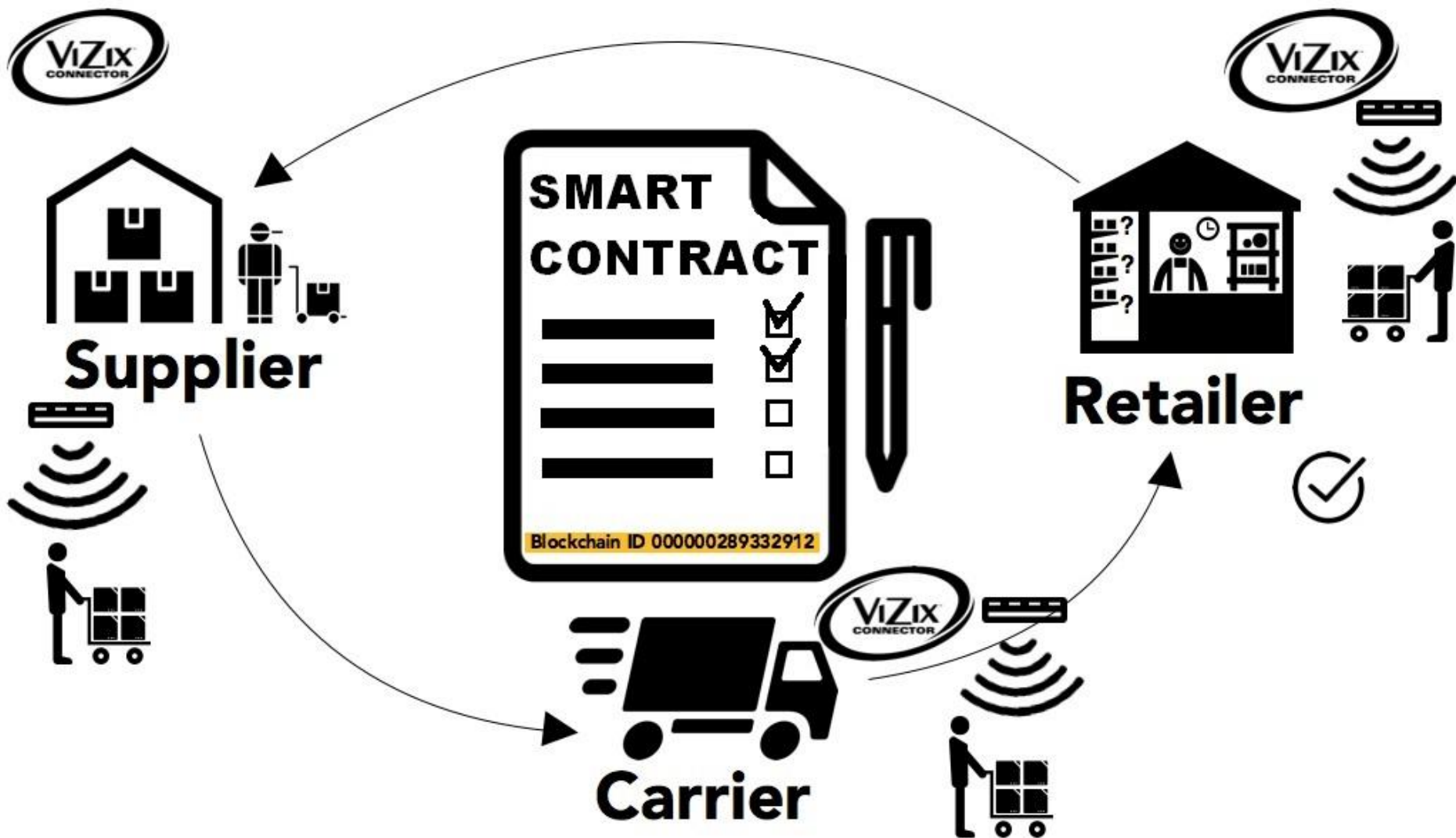


Business Network





# 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