Федеральное государственное автономное образовательное учреждение высшего образования
Национальный исследовательский ядерный университет «МИФИ»

Кафедра «Криптология и кибербезопасность»

Основы блокчейн-технологий

Запечников Сергей Владимирович,
д.т.н., профессор

7 октября 2025 г.

Примерное содержание курса (1/3)

Лекции:

Тема 1. Введение в блокчейн-технологии. Краткая история развития блокчейн-технологий. Бизнес-идея блокчейн-технологий. Основная терминология. Свойства распределенного реестра. Архитектура блокчейн-платформ. Понятие консенсуса. Сложность достижения консенсуса. Уровни консенсуса и упорядочения сообщений. Виды блокчейн-платформ. Уровень распределенного реестра. Формат хранения данных. Уровни децентрализованных приложений и пользовательского интерфейса. Сферы применения блокчейн-технологий. Проблемы блокчейн-технологий.

Тема 2. Криптография в блокчейн-технологиях. Обзор криптографических методов защиты информации, применяемых в блокчейн-технологиях: симметричные шифры, криптографические хэш-функции, электронная цифровая подпись, криптография на эллиптических кривых.

Тема 3. Блокчейн-платформы открытого типа. Платформа Bitcoin. Консенсус типа proof-of-work (PoW). Майнинг. Вычислительно трудоёмкая задача, решаемая при майнинге. Регулирование трудоёмкости майнинга. Вилки и их разрешение. Алгоритм формирования блоков. Модель непотраченных транзакций (UTXO). Формат хранения данных и формат транзакций в распределенном реестре Bitcoin. Демонстрация работы блокчейн-платформы с механизмом консенсуса PoW. Применение браузерных инструментов просмотра блоков Bitcoin. Демонстрация роста цепочки блоков Bitcoin. Платформа Ethereum. Консенсус типа proof-of-stake (PoS). Два типа аккаунтов на платформе Ethereum. Децентрализованная виртуальная машина Ethereum, выполнение смарт-контрактов.

Примерное содержание курса (2/3)

Лекции (продолжение):

Тема 4. Блокчейн-платформы закрытого типа. Платформа Hyperledger Fabric. Архитектура платформы, модель выполнения транзакций. Задача о византийских генералах. Консенсус на основе византийского соглашения.

Тема 5. Приложения блокчейн-технологий. Случаи, в которых необходимо применение блокчейна. Масштабирование блокчейна. Криптовалюты. Цифровые финансовые активы (ЦФА). Цифровые права. Нормативное регулирование обращения криптовалют. Справочные ресурсы по криптовалютам и ЦФА. Расчётные центры (rollups). Платёжные каналы. Сети платёжных каналов (lightning networks). Децентрализованные финансовые сервисы (DeFi). Стейблкоины. Децентрализованные организации (DAO).

Тема 6. Обеспечение безопасности распределенных реестров. Проблемы конфиденциальности и целостности информации в распределенных реестрах и операций с ними. Доказательства с нулевым разглашением и их применение. Анонимные криптовалюты. Миксеры и децентрализованные криптобиржи.

Примерное содержание курса (3/3)

Практические занятия:

Тема 1. Инструментарий и приложения экосистемы Ethereum. Знакомство с основными инструментами экосистемы Ethereum. Работа с приложением Metamask и браузерной IDE Remix.

Тема 2. Виртуальная машина Ethereum и смарт-контракты. Работа с виртуальной машиной Ethereum. Разработка кода смарт-контрактов, компиляция и размещение их на блокчейн-платформе. Язык Solidity. Виртуальная машина Ethereum (EVM).

Тема 3. Межконтрактное взаимодействие. Разработка и использование смарт-контракта, взаимодействующего с другим смарт-контрактом. Основы безопасности смарт-контрактов. Формальная верификация смарт-контрактов.

Тема 4. Взаимодействие со смарт-контрактами из внешних информационных систем. Получение практических навыков взаимодействия со смарт-контрактами из внешних информационных систем. Способы получения данных из распределенного реестра. Разработка клиентского JS-приложения для взаимодействия со смарт-контрактом.

Тема 5. Создание программной модели блокчейн-платформы. Анализ требований учебного ТЗ на создание модели блокчейн-платформы. Анализ программной реализации модели блокчейн-платформы на языке программирования Python.

Литература

Основная:

1. CS 251: Cryptocurrencies and Blockchain technologies. Stanford university. 2025. URL: https://cs251.stanford.edu/

2. Сонг Дж. Python для программирования криптовалют. Как научиться программировать биткойн «с чистого листа». М.: Диалектика. 2020. 370 стр.

3. Narayanan A., Bonneau J., Felten E. et al. Bitcoin and cryptocurrency technologies. A comprehensive introduction. Princeton university press. 2016. 406 pp.

4. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. URL: https://bitcoin.org/bitcoin.pdf

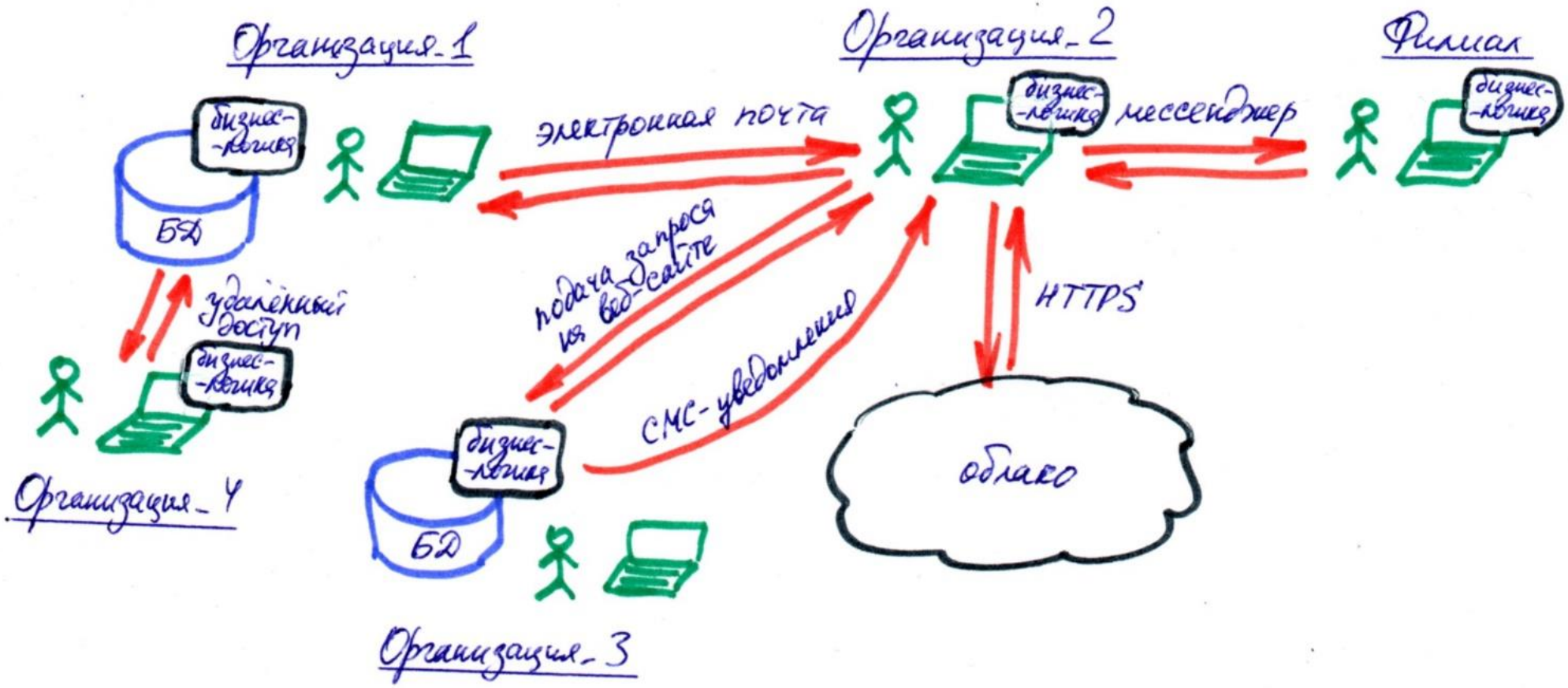
5. Wood G. Ethereum: A secure decentralised generalised transaction ledger. (“Yellowpaper”). URL: https://ethereum.github.io/yellowpaper/paper.pdf

6. Androulaki E., Barger A., Bortnikov V. et al. Hyperledger Fabric: A distributed operating system for permissioned blockchains. URL: https://arxiv.org/pdf/1801.10228v1.pdf

Литература по отдельным темам будет сообщаться дополнительно.

Тема 1.
Введение в блокчейн-технологии

Традиционные технологии управления и обмена данными



Технологии разнородны: собственные базы данных у каждой организации, разные способы взаимодействия (эл. почта, телефонные звонки, СМС, мессенджеры, заполнение форм на веб-сайтах и пр.).

Следствия: многократное дублирование и перепроверка данных, разные форматы документов, длительное время рассмотрения заявок, человеческий фактор (ошибки) и пр.

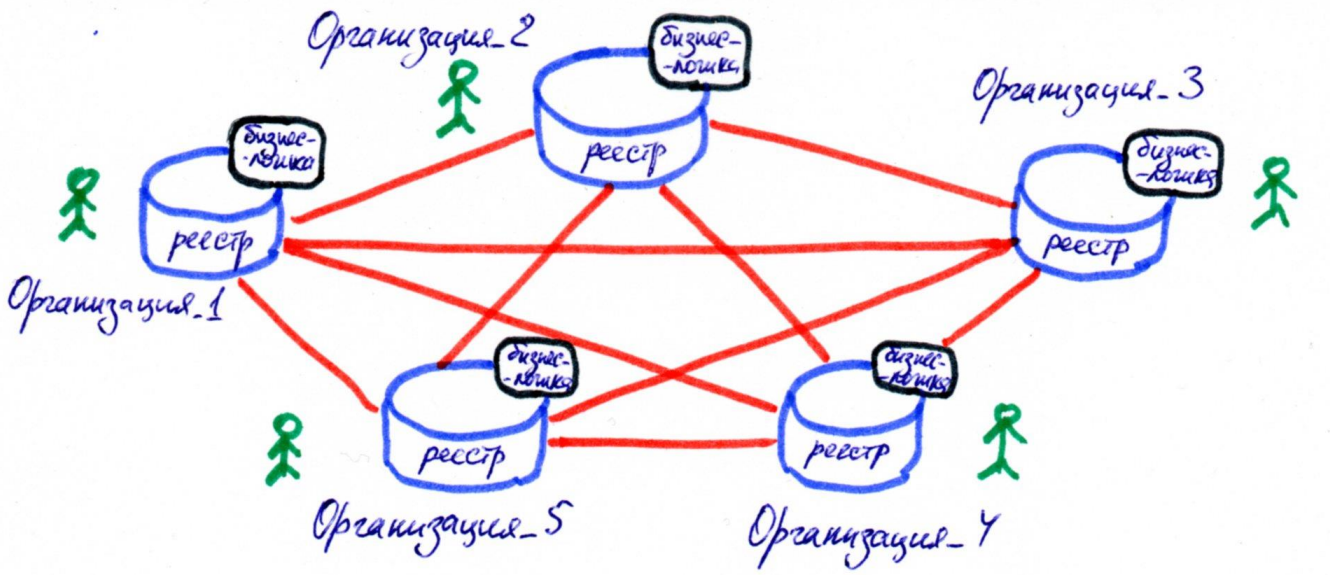
Что такое блокчейн-технологии?

Abstract answer: a blockchain provides
coordination between many parties,
when there is no single trusted party

if trusted party exists ⇒ no need for a blockchain

[financial systems: often no trusted party]

Разнородные технологии управления и обмена данными заменяются новой единой технологией, которая предоставляет платформу взаимодействия между потенциально не доверяющими друг другу участниками деловой деятельности.



Бизнес-идея блокчейн-технологий

- Сеть строится вокруг некоторого ***бизнес-процесса***. Участниками являются разные физические и (или) юридические лица. Все они в этой сети равноправны.

Бизнес-процесс – это совокупность взаимосвязанных мероприятий или работ, направленных на создание определённого продукта или услуги для потребителей. Бизнес-процесс может охватывать одну или несколько организаций. Вокруг бизнес-процессов в современных условиях строятся информационные системы. Бизнес-процесс подразумевает операции с активами.

Активом называется все, что обладает ценностью для бизнес-процесса.

- Все участники сети ведут общую базу данных активов, которые они обрабатывают в бизнес-процессе. Эта база активов называется ***распределенным реестром (РР)***.
- Приложения, надстроенные над реестром, обеспечивают возможность учета жизненного цикла любых видов активов и выполнение сколь угодно сложных операций над этими активами. Для этого реализуется ***бизнес-логика***. Операции с активами подчиняются установленным в сообществе правилам.

***Примеры активов, учитываемых в распределенных реестрах*:** денежные средства, ценные бумаги, права и обязательства, товары, транспортные средства, медицинские карты пациентов и пр.

Свойства распределенного реестра с точки зрения пользователя

- Внести в РР новую информацию можно только по поручению одного из участников сети.
- Любую информацию в РР можно добавлять только с согласия квалифицированного большинства участников (должен быть достигнут консенсус).
- Информацию в РР можно только добавлять, нельзя ни модифицировать, ни удалять ранее введенные данные – таким образом сохраняется вся история операций с активами.
- Каждый участник имеет свою копию истории операций с активами, а также свою копию текущего состояния РР либо только части РР, описывающей его собственные активы. Все копии (почти) синхронны.
- Над РР можно надстраивать логику. Все операции с активами должны соответствовать определенному набору правил. Эти правила запрограммированы в виде смарт-контрактов. Нельзя записывать в РР никакую иную информацию, не соответствующую правилам. Операции с активами могут быть обусловлены атрибутами участников, их состояниями в текущий момент времени, событиями вне системы.

Краткая история развития блокчейн-технологий (1/2)

2009

Bitcoin

Several innovations:

- A practical **public append-only data structure**, secured by replication and incentives
- A fixed supply asset (BTC). Digital payments, and more.

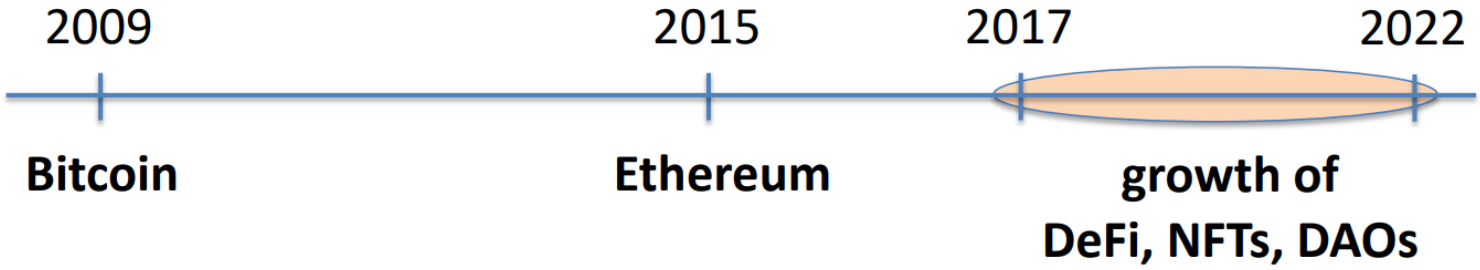
2009 2015

Bitcoin **Ethereum**

Several innovations:

- **Blockchain computer**: a fully programmable environment
  $\Longrightarrow$ public programs that manage digital and financial assets
- **Composability**: applications running on chain can call each other

Краткая история развития блокчейн-технологий (2/2)



(1) Basic application: a digital currency (stored value)

- Current largest: Bitcoin (2009), Ethereum (2015)
- Global: accessible to anyone with an Internet connection

(2) Decentralized applications (DAPPs)

- **DeFi**: financial instruments managed by public programs
  - examples: stablecoins, lending, exchanges, ….
- **Asset management** (NFTs): art, game assets, domain names.
- **Decentralized organizations** (DAOs): (decentralized governance)
  - DAOs for investment, for donations, for collecting art, etc.

---

(3) New programming model: writing decentralized programs

Замечание о терминологии

Термин «блокчейн-технологии» – в значительной мере условный, используется по традиции, но не совсем верно отражает суть технологии.

Decentralized computations – Децентрализованные вычисления – это наиболее общая функция, правильнее всего было бы говорить «технологии децентрализованных вычислений».

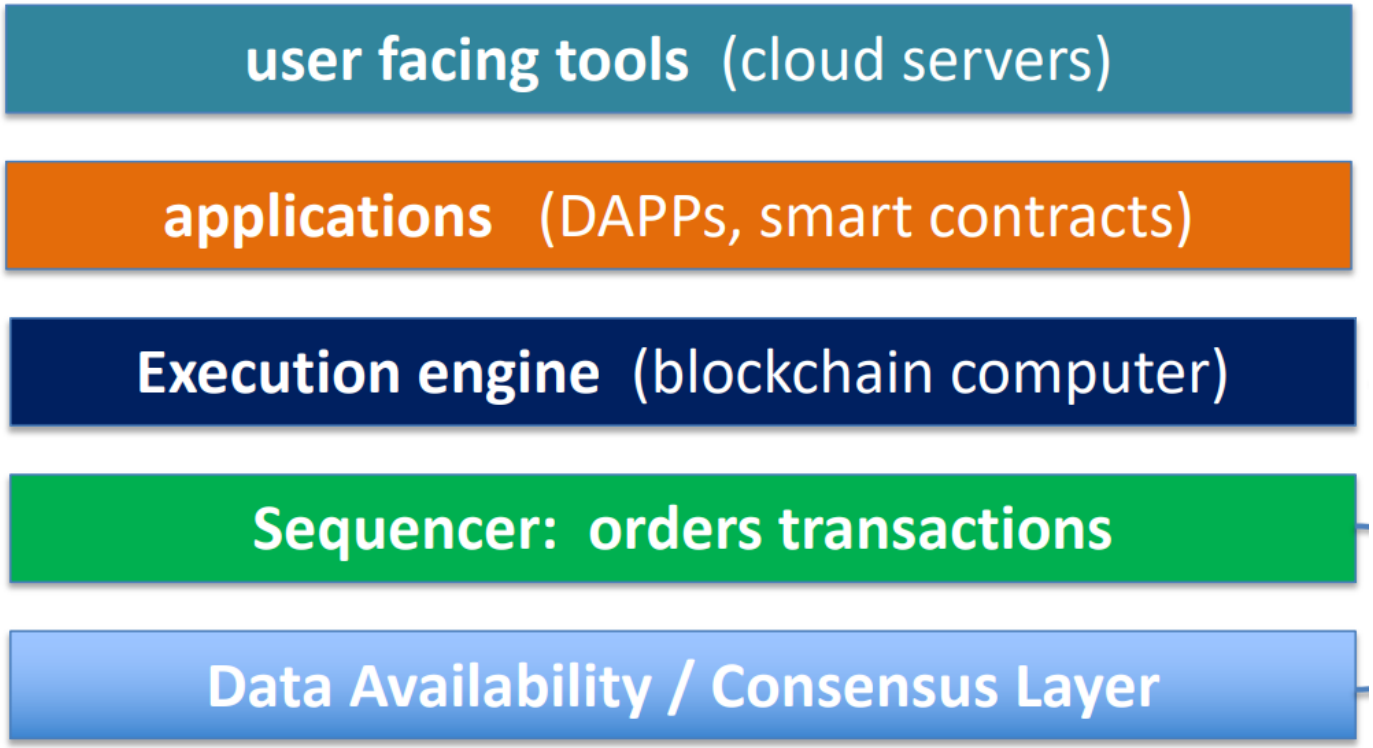
Distributed ledger – Распределенный реестр – обязательная составляющая децентрализованных вычислений, но может использоваться и как самостоятельная функция, поэтому говорят о «технологиях распределенного реестра».

Blockchain – Блокчейн – цепочка блоков – наиболее распространённый способ реализации распределенного реестра, но не единственно возможный.

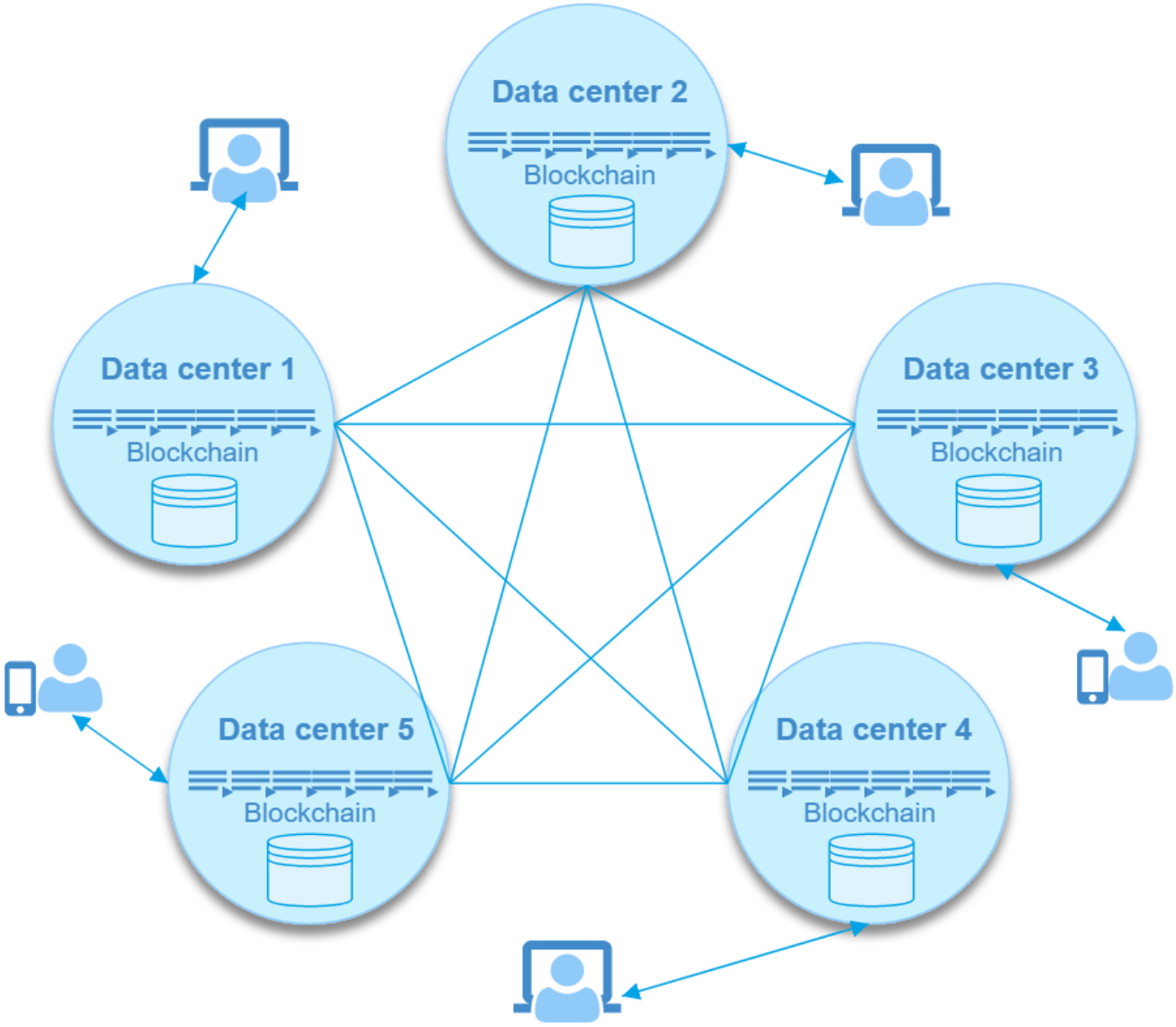
BlockDAG – Ациклический направленный граф блоков – обобщение блокчейна, ещё один способ реализации распределённого реестра.

Архитектура блокчейн-платформ

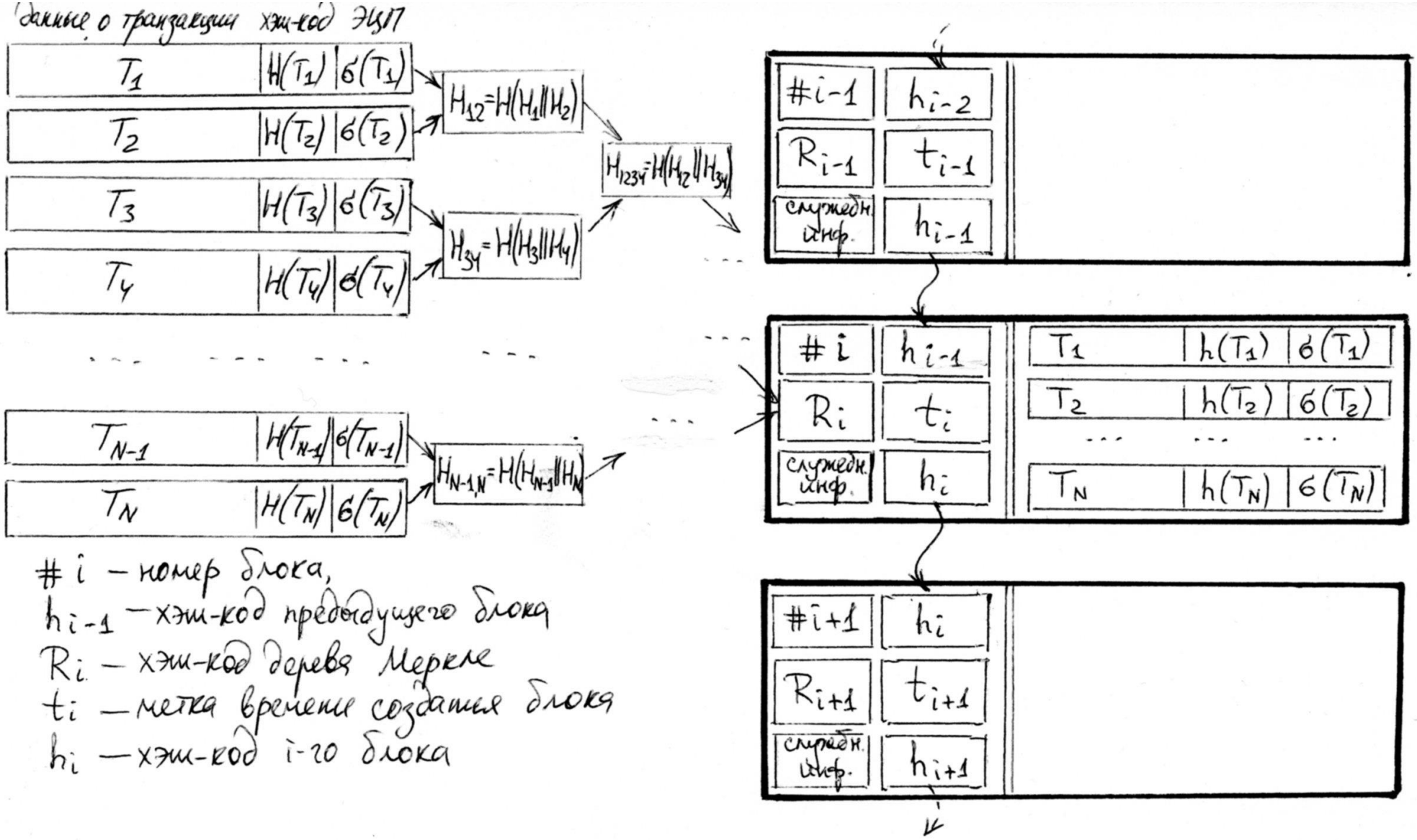
Платформа распределенного реестра (блокчейн-платформа) – конкретное воплощение технологии децентрализованных вычислений, в том числе, PP.



Уровни консенсуса и упорядочивания сообщений: техника – одноранговая сеть

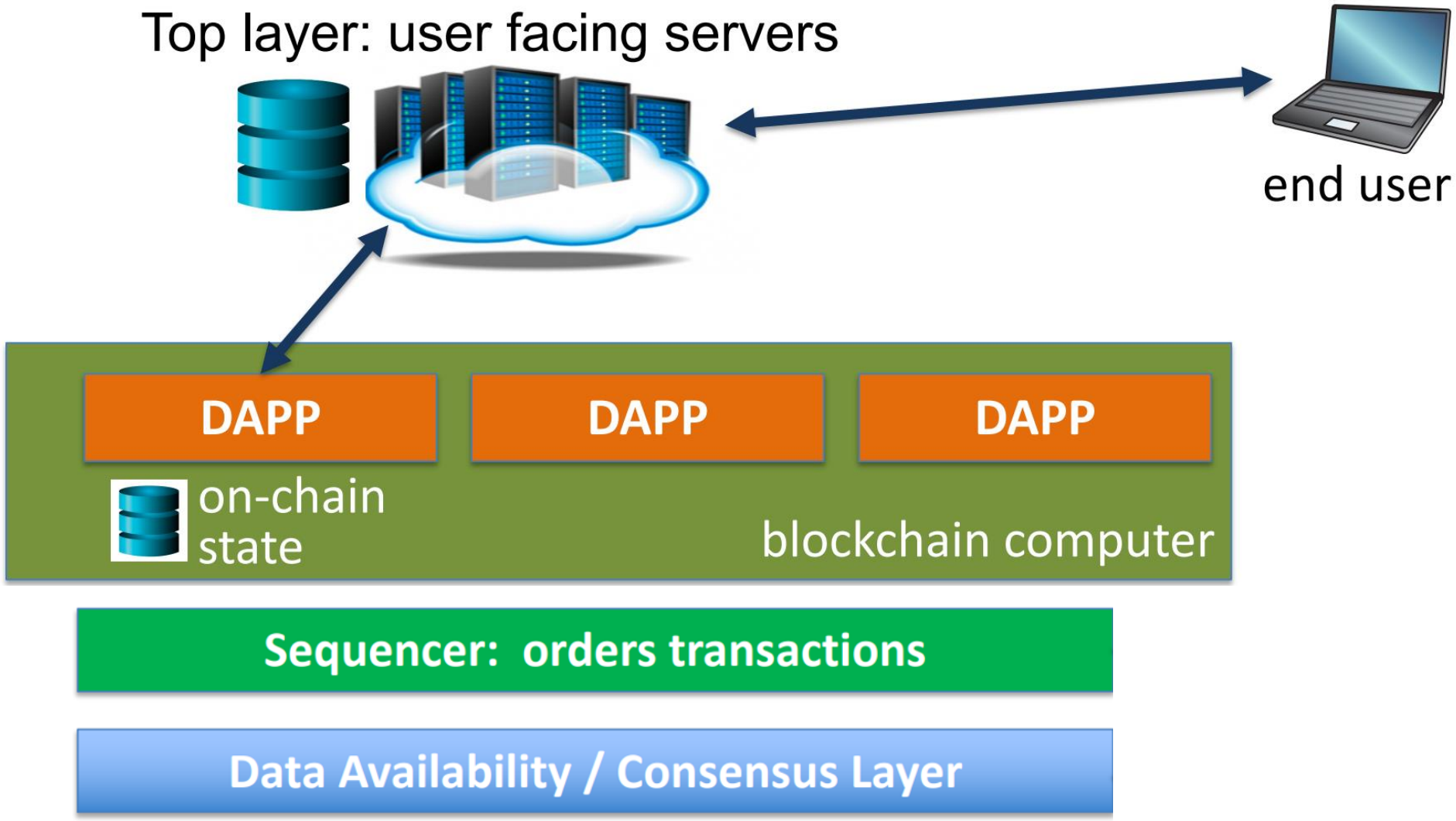


Уровень распределенного реестра



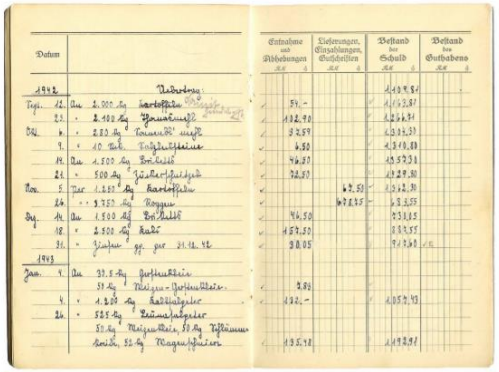
#i – номер блока,
h_{i-1} – хэш-код предыдущего блока
R_i – хэш-код дерева Меркле
t_i – метка времени создания блока
h_i – хэш-код i-го блока

Уровень приложений и пользовательских интерфейсов



Сферы применения блокчейн-технологий

- **преимущественно реестровые приложения** – замена реестров, ведущихся в традиционной форме, на децентрализованные: криптовалюты, государственные цифровые валюты (Central Bank Digital Currency), реестры государственных органов и частных организаций (недвижимого имущества, нотариальных действий, ЗАГС, реестры акционеров и пр.).



- **приложения со сложной надстроенной логикой:**
  DeFi – финансовые инструменты, управляемые публичными программами: стейблкоины, биржи, кредитные площадки и пр.;
  ЦП и ЦФА – цифровые права и цифровые финансовые активы: токены, в том числе, невзаимозаменяемые (NFT – Non-Fundable Tokens);
  DAOs – децентрализованные организации: для инвестиций, для сбора пожертвований, для коллекционирования предметов искусства;
  системы валовых расчетов реального времени (RTGS – Real-Time Gross Settlement);
  системы международных банковских переводов, не подверженных цензурированию**;**
  страхование: обработка страховых случаев;
  международная торговля: экспортно-импортные операции;
  логистика: управление цепочками поставок (supply chain management), в том числе транспортная логистика;
  кредитование юридических лиц: синдицированный кредит;
  медицинские информационные системы.

Виды платформ распределенного реестра

Платформа распределенного реестра (блокчейн-платформа) – конкретное воплощение технологии распределенного реестра.

Платформы открытого типа (permissionless), или ***публичные*** – платформы, которые позволяют стать их участниками неограниченному кругу лиц, никакой регистрации или отзыва полномочий не требуется.

Примеры: Bitcoin, Ethereum, многочисленные “Altcoins” и пр.

Платформы закрытого типа (permissioned), или ***частные, корпоративные, разрешительные*** – ограничивают круг участников пределами сообщества, для участия требуется регистрация, при выходе из сообщества право доступа отзывается.

Примеры: проект Hyperledger (самые известные – Hyperledger Fabric, Hyperledger Iroha, Hyperledger Sawtooth, Hyperledger Indy, Hyperledger Burrow), Corda, Tendermint, Quorum, Exonum, NEM Catapult и др.

Смешанного, или комбинированного типа – платформы открытого типа, которые используют для достижения консенсуса технологии построения платформ закрытого типа.

Примеры: Toda-Algorand, Omniledger, BitcoinNG и др.

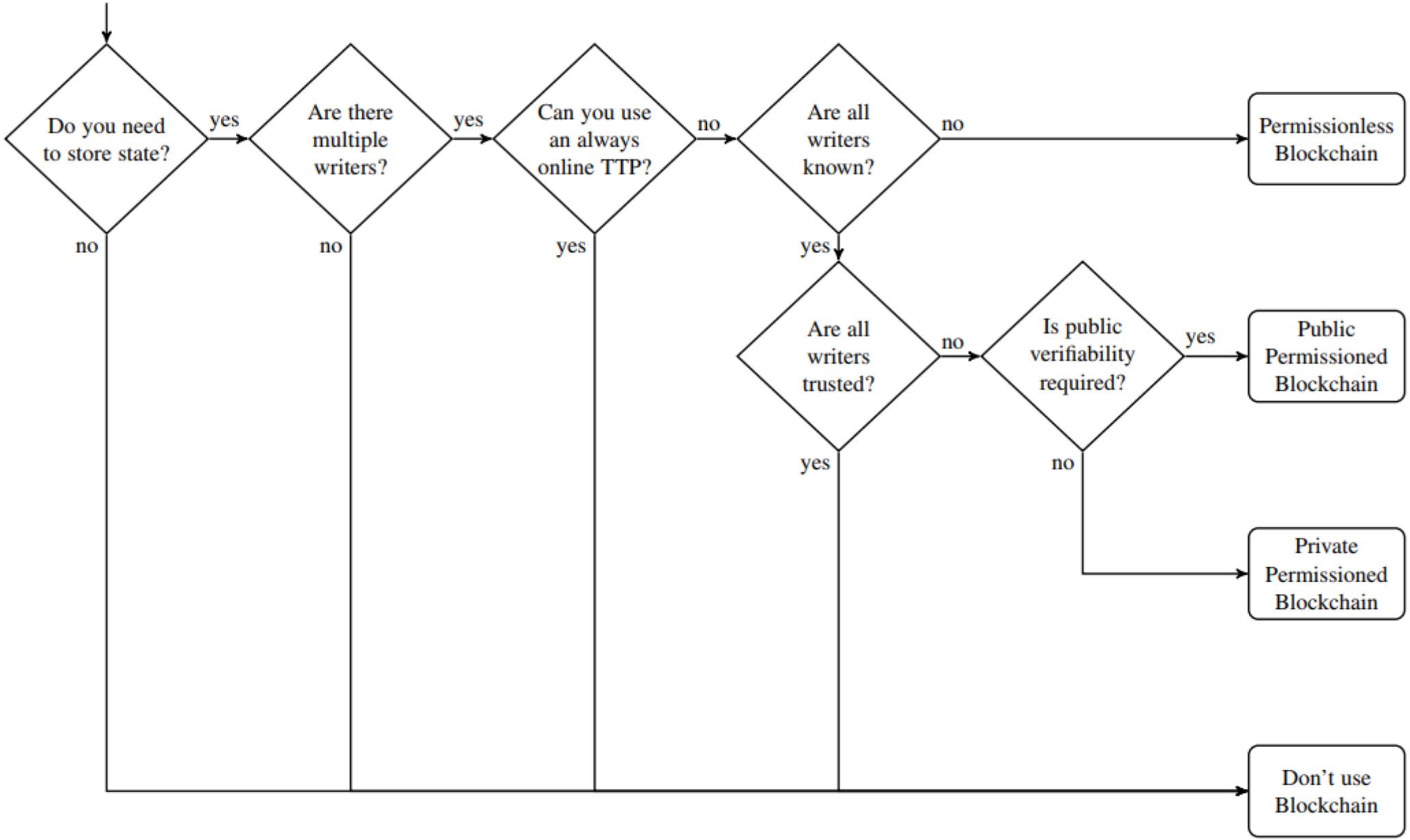
Особенности блокчейн-платформ открытого типа

- Участники могут легко добавляться и выходить из блокчейн-сети, от присутствия или отсутствия конкретного участника в целом ничего не зависит, возможно анонимное (точнее, псевдонимное) участие.
- Формирование новых блоков транзакций происходит посредством «доказательства выполнения работы» (proof-of-work), «доказательства обладания долей» (proof-of-stake) или другим аналогичным способом *(принцип лотереи)*. Квалифицированное большинство участников – это подмножество участников, обладающих более чем 50% некоторого вида ресурсов, а не более чем 50% численности.
- Две базовые модели транзакций: UTXO-модель, модель аккаунтов.
- Для работы блокчейн-платформы открытого типа *требуется криптовалюта*, чтобы стимулировать майнеров или валидаторов. Есть разные модели её применения при PoW, PoS, но она в любом случае нужна.
- Блокчейн-платформы открытого типа с PoW очень ресурсоёмки (электроэнергия, машинное время): предполагается, что к 2035 году на майнинг биткоинов будет тратиться столько же электроэнергии, сколько потребляет среднее европейское государство.

Особенности блокчейн-платформ закрытого типа

- Участники не могут самостоятельно добавляться и выходить из блокчейн-сети – для этого центр регистрации (удостоверяющий центр, MSP – membership service provider и т.п.) должен выдать участнику его цифровой идентификатор и ключи.
- Формирование новых блоков транзакций происходит посредством выполнения специального протокола достижения консенсуса *(принцип голосования)*. Квалифицированное большинство участников – это подмножество участников, составляющих не менее чем 50% их численности.
- Блокчейн-платформы закрытого типа обладают высоким быстродействием и хорошей масштабируемостью.
- Для работы блокчейн-платформы закрытого типа *не требуется криптовалюта*.

Когда нужен и когда не нужен блокчейн?



Проблемы технологий распределенного реестра (1/2)

Производительность. **Скорость записи новых транзакций в базу данных значительно ниже, чем в традиционных системах, а по сравнению с высоконагруженными системами – на порядок ниже.**

Решения:

- новые, более быстрые и масштабируемые протоколы консенсуса;
- экстенсивный путь (увеличение количества транзакций в блоке, размера блоков и т.п.) – хардфорки, отсутствие обратной совместимости;
- разбиение реестра на шарды;
- платёжные каналы (lightning networks и др.) – депонирование средств и транзакции напрямую между участниками, ведение реестров транзакций у участников, периодическое сохранение изменений балансов в основном реестре;
- расчётные центры (rollups) – смарт-контракт, который реализует транзакции между участниками, периодическое сохранение балансов в основном реестре.

Проблемы технологий распределенного реестра (2/2)

Информационная безопасность. **Системы распределенного реестра в классическом виде обеспечивает высокую доступность (невозможность уничтожения) и целостность (гарантии неизменности) информации, но не обеспечивает конфиденциальности информации (все записи в базе данных видны для всех участников системы).**

Решения:

- обеспечение конфиденциальности балансов счетов (кошельков) при совершении транзакций;
- обеспечение конфиденциальности входных и выходных данных, передаваемых смарт-контрактам;
- обеспечение конфиденциальности кодов смарт-контрактов;
- архитектурные решения на уровне блокчейн-платформы по разграничению доступа – пример: каналы в блокчейн-платформе закрытого типа Hyperledger Fabric.

Спасибо за внимание!

Вопросы?