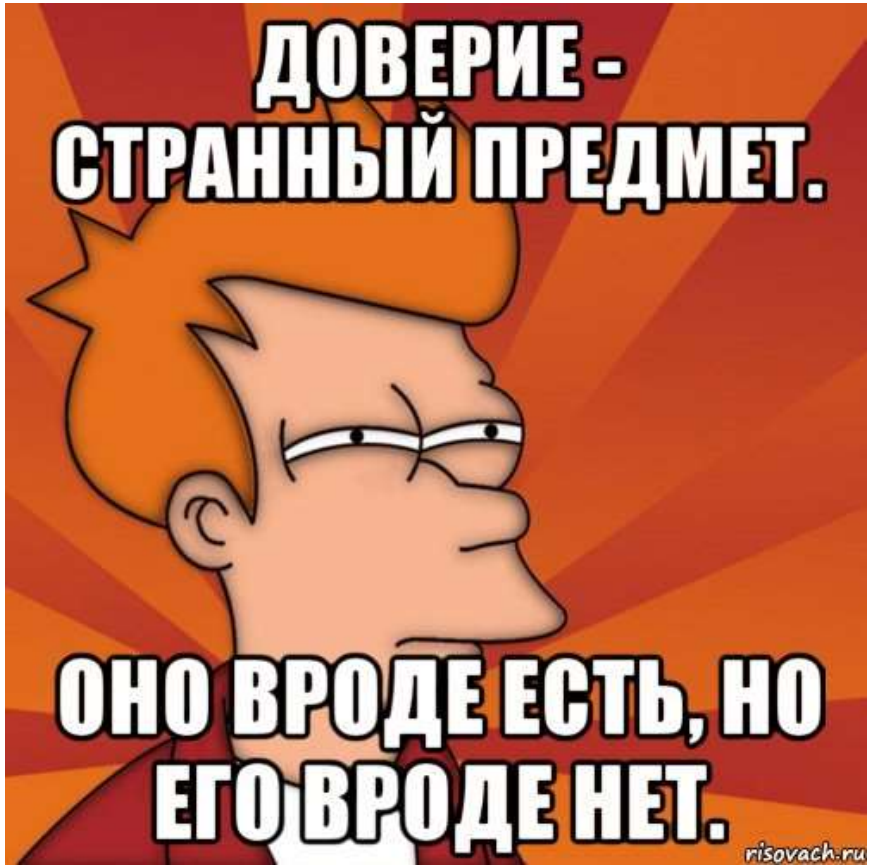
Блокчейн — трезвый взгляд, реальные применения и текущие проблемы

Маршалко Г.Б.

Доверие

Фундаментальной проблемой некоторых блокчейн-решений является то, что за основу берется идея о том, что транзакции без доверия – это хорошо.

Джон Вундерлих,
Совет по стандартам Канады



Доверие

ГОСТ 54581-2011 «Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к ИТ»

доверие - выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемый объект соответствует своим целям

В России и мире – различные формы *аттестации*, *сертификации* и т.п.

Куда идти

- ФСТЭК России - в случаях отсутствия необходимости применения криптографических средств для защиты информации, подлежащей обязательной защите.
- ФСБ России - в случаях применения криптографических средств относящихся к сфере компетенции ФСБ России.
- Банк России - в случаях использования блокчейн-система в финансовом секторе.

Но сначала надо понять, что за система, где и как она работает, какая информация обрабатывается и подлежит ли все это защите.

Что это такое?

МР 26.4.001-2018 Термины и определения в области технологий цепной записи данных (блокчейн) и распределенных реестров

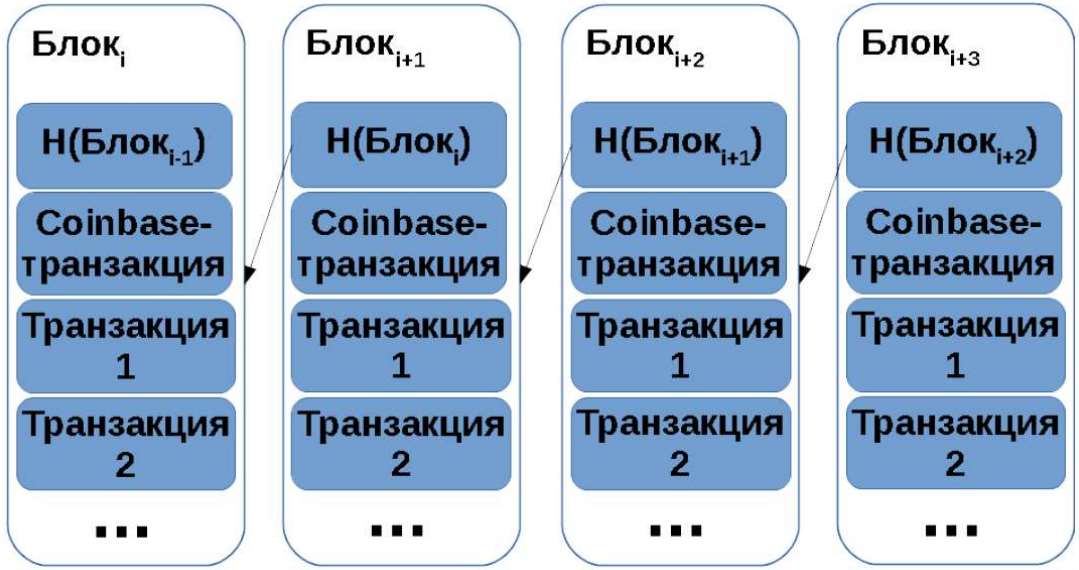
- Объекты
- Субъекты
- Действия
- Свойства

Что это такое?

- **Информационная система** (information system); ИС: Организованное множество аппаратных средств, программных средств, предметов снабжения, политик, процедур и пользователей, которое используется для хранения информации, ее обработки и предоставления доступа к ней
- **Реестр** (ledger): Совокупность данных, в том числе в электронном виде, структурированных и хранимых в целях их учета, поиска, обработки и контроля
- **Цепная запись данных; Блокчейн** (blockchain): Реестр, данные в который записываются блоками таким образом, что каждый новый блок включает информацию о предыдущем блоке
- **Информационные системы с реестром** … (реестры, пользователи, действия)

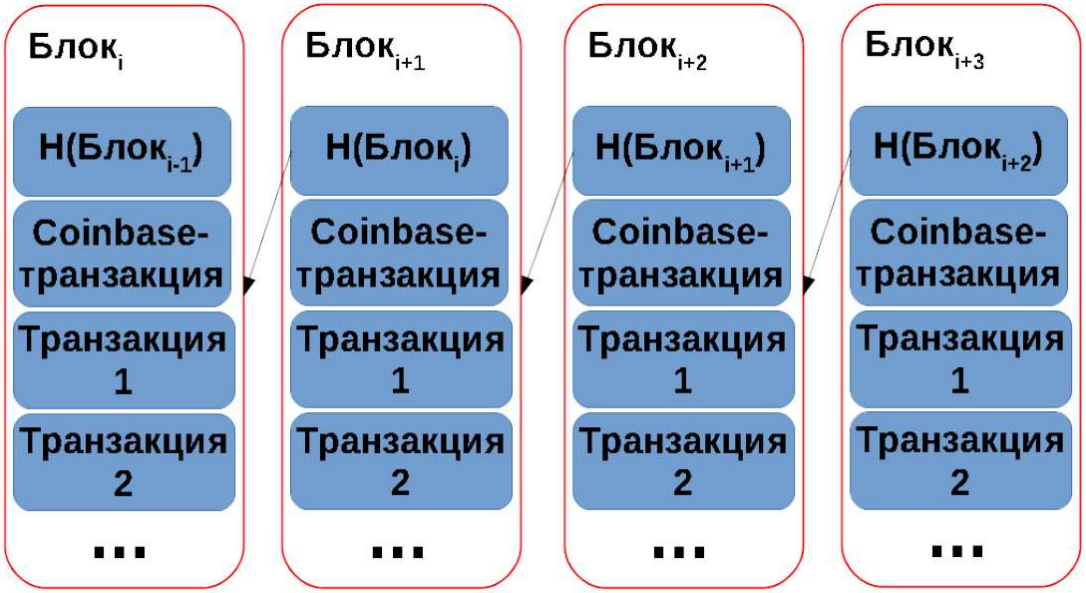
Информационная система

- **Логический уровень –** представление информации, обработка, передача



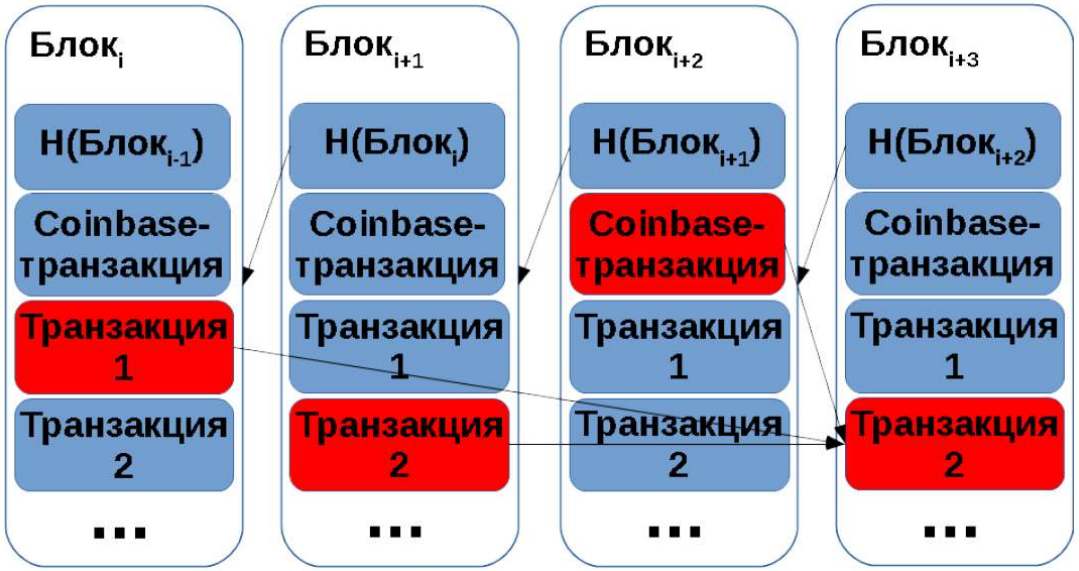
Информационная система

- **Логический уровень –** представление информации, обработка, передача



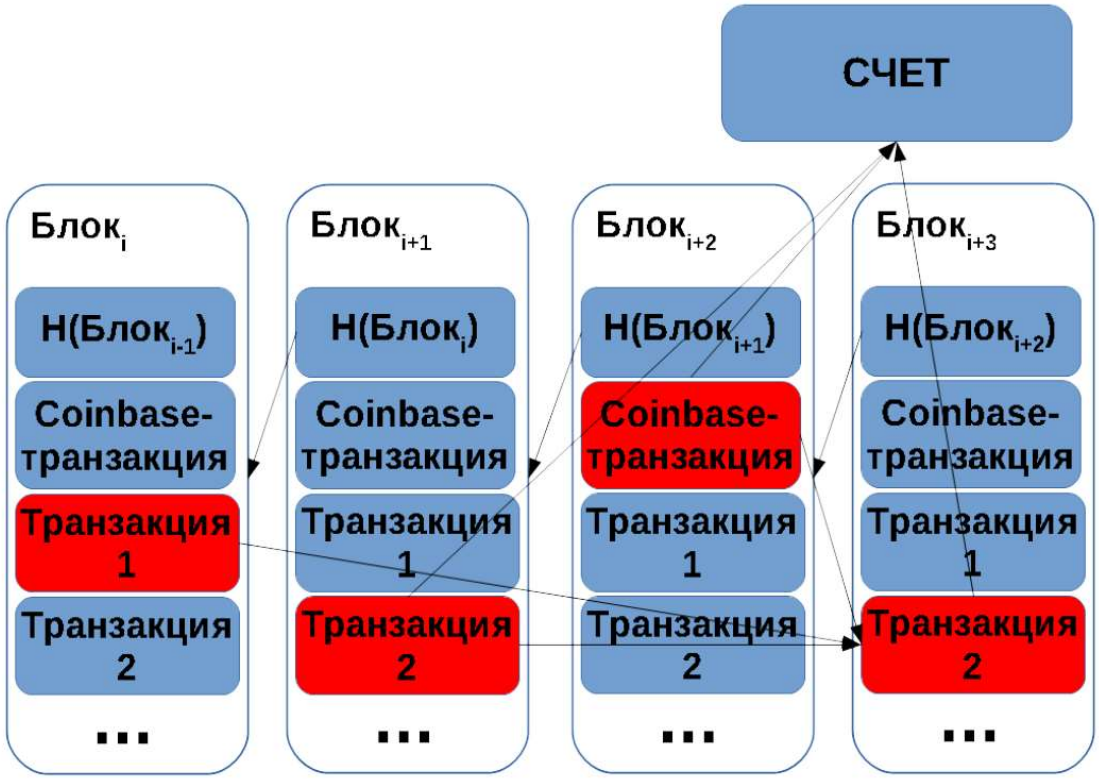
Информационная система

- **Логический уровень –** представление информации, обработка, передача



Информационная система

- **Логический уровень –** представление информации, обработка, передача



Информационная система

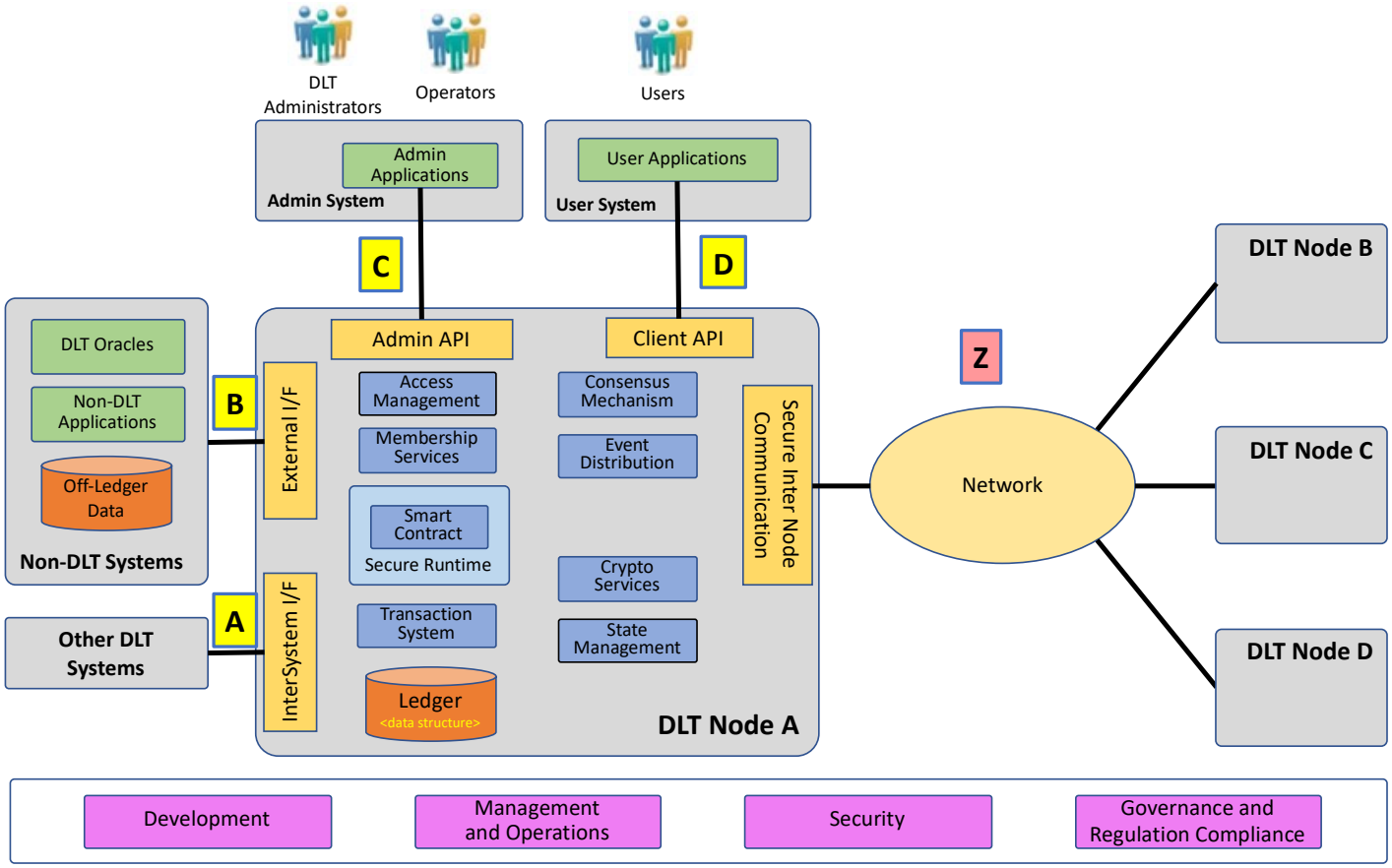
- **Логический уровень –** представление информации, обработка, передача
- **Уровень реализации** - набор исходных текстов и скомпилированных модулей со всеми вытекающими проблемами в области безопасности

Необходимо четко разделять эти уровни.

- Модульность: критические и некритические функции (модули)
- Роли пользователей, привилегии
- Тип обрабатываемой информации

Важно понимать, что и как делает система.

Информационная система



Модель нарушителя

- нарушитель администратор/привилегированный пользователь/пользователь?
- нарушитель имеет возможность (в том числе и потенциальную) влиять на работу (как удаленно так и локально) на систему в целом?
- обрабатывается конфиденциальная информация, персональные данные?
- нужна ли юридическая значимость совершенных действий?

Р 1323565.1.012-2017 Принципы синтеза и модернизации шифровальных (криптографических) средств

Почему именно Р 1323565.1.012-2017?

- В блокчейн-системах происходит достижение консенсуса при реализации *протокола взаимодействия* между участниками информационного обмена. Доверие к консенсусу формируется за счет использования *криптографических атомарных запросов*.
- С этой точки зрения алгоритм достижения консенсуса или построенный поверх него смарт-контракт - криптографические протоколы
- Новый криптографический протокол - новой тип СКЗИ

Консенсус

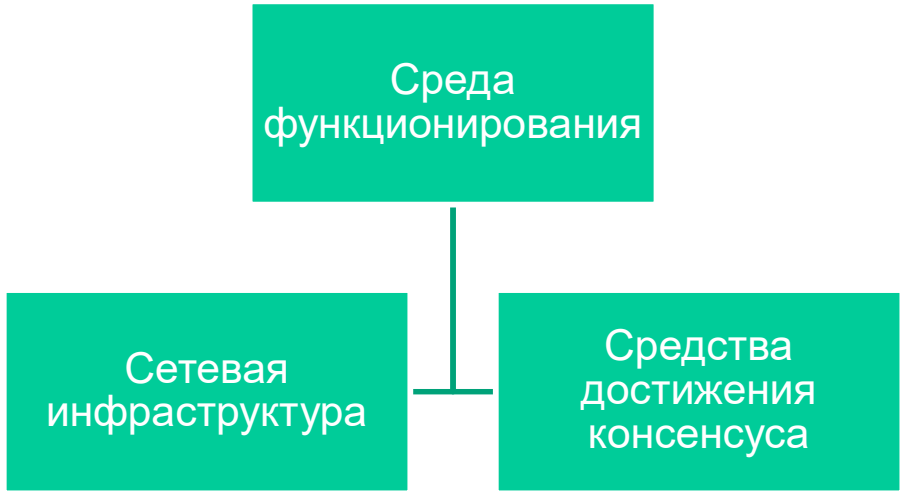
- Процедура выбора пользователя, который может изменить состояние реестра.
- Большое количество различных вариантов:
  - Византийское соглашение
  - С доказательством работы, владения…
  - С доказательством владения … и наличием выделенных пользователей

Консенсус

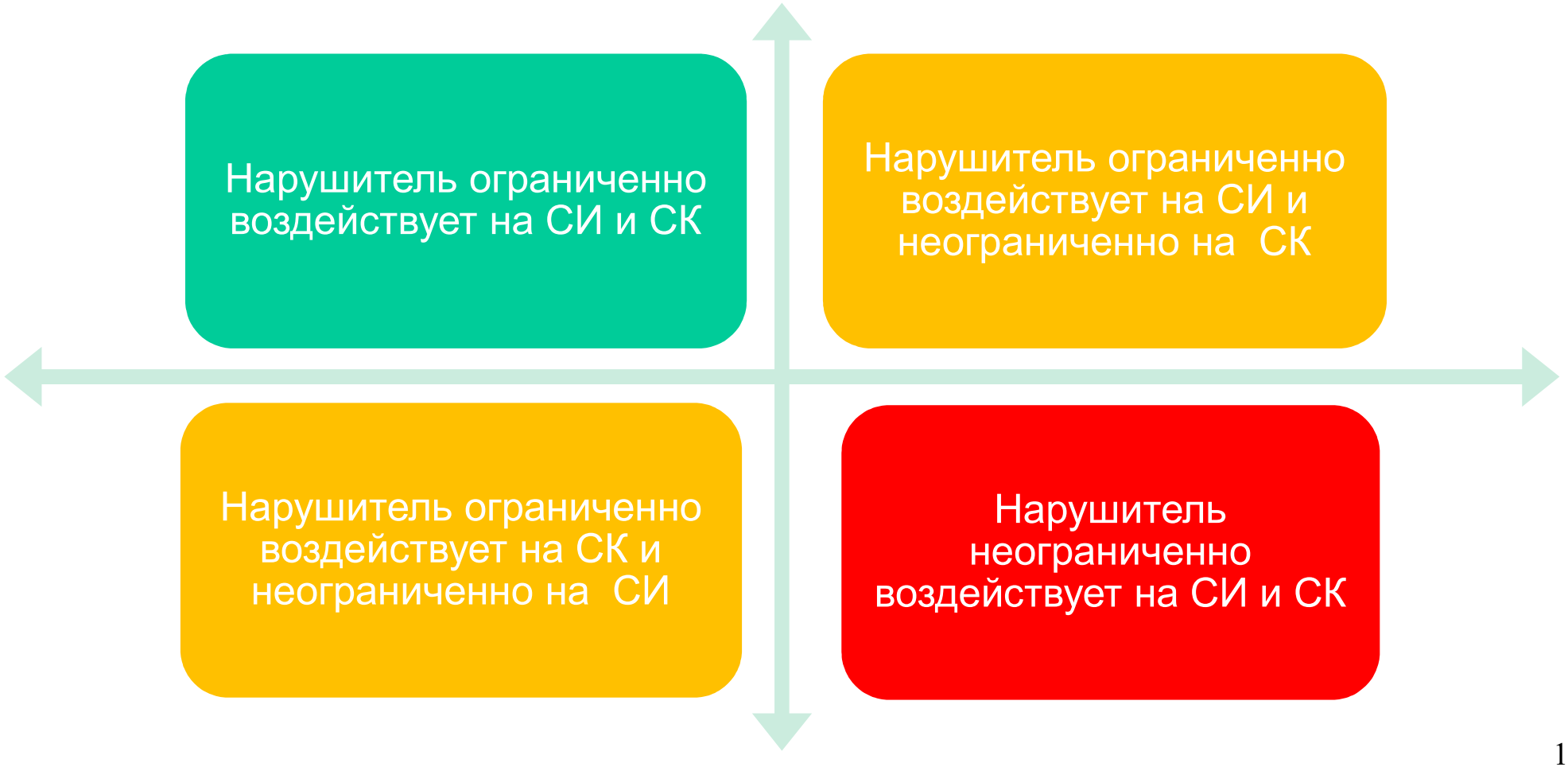
- Большое количество атак на протоколы консенсуса:
  - Атаки на узлы сети (подкуп, DDoS, Sybill…)
  - Атаки на сетевые соединения (Eclipse, Задержка пакетов…)
- Функция достижения консенсуса является критической

Среда функционирования протокола достижения консенсуса

- **среда функционирования ДК;** (СФДК): Совокупность *сетевой инфраструктуры (СИ)* и одного или нескольких *средств достижения консенсуса (СК),* с использованием которых функционирует ДК и которые способны повлиять на выполнение предъявляемых к ДК требований.



Варианты моделей нарушителя для протоколов достижения консенсуса



Умные контракты

Умный контракт (smart-contract), **чейнкод** (chaincode):

совокупность условий и последовательность действий, описанные в соответствии с политиками и процедурами ИС. Выполнение всех оговоренных условий, зависящее от конкретного состояния (состояний) ИС (в том числе, в результате проверки внешних по отношению к ИС условий), влечет автоматическое выполнение заранее определенной последовательности действий. Выполнение указанной последовательности действий, в свою очередь, также ведет к изменению состояния ИС.

Умные контракты оперируют с информацией на логическом уровне.

Умные контракты

- Разработка:
  - Логические ошибки
    - Ошибки на логическом уровне обработки информации (не учтены все возможные варианты входных условий и реакций на них)
    - *Формальная верификация*
  - Ошибки реализации (программирования)
    - Переполнения
    - Деления на 0
    - Некорректная работы с динамическими структурами
    - …
    - *Безопасное программирование*
- Исполнение
  - Отсутствие доверенных интерпретаторов (не следует использовать для критических функций)

Заключительные ремарки

- Блокчейн-системы – это в первую очередь информационные системы, для которых существует большой опыт разработки и исследования по безопасности, который необходимо использовать
- Использование блокчейн-систем в областях, регулируемых государством, требует консервативного подхода, заключающегося в использовании классических подходов к оценке и нейтрализации угроз.