Технологии цепной записи данных и распределенных реестров: криптографический скачок вперед, шаг назад или путь в никуда?

В. Шишкин,
Г. Маршалко,
А. Гуселев,
Иван Лавриков

— ТК 26 —
РусКрипто 2017

Дисклэймер:

- Представленные в настоящем докладе материалы являются частным мнением докладчика (и частично – соавторов доклада), их не стоит трактовать как мнение какой-либо организации или организованной группы лиц.
- Все факты являются вымышленными, совпадения с реально существующими мнениями являются случайными.

- *Если кто ожидает формальной формализации – не дождётся.*
- *Над иллюстрациями не смеяться. Если только чуть-чуть...*

Содержание доклада

Перейдём к пункту

История?

2009 – 2014 – 2017 – 19xx

«blockchain» – «блокчейн» – «цепная запись данных»

в. 1.0	–	в. 2.0	–	в. 3.0
единицы	–	инструменты	–	приложения

Интерес общественности

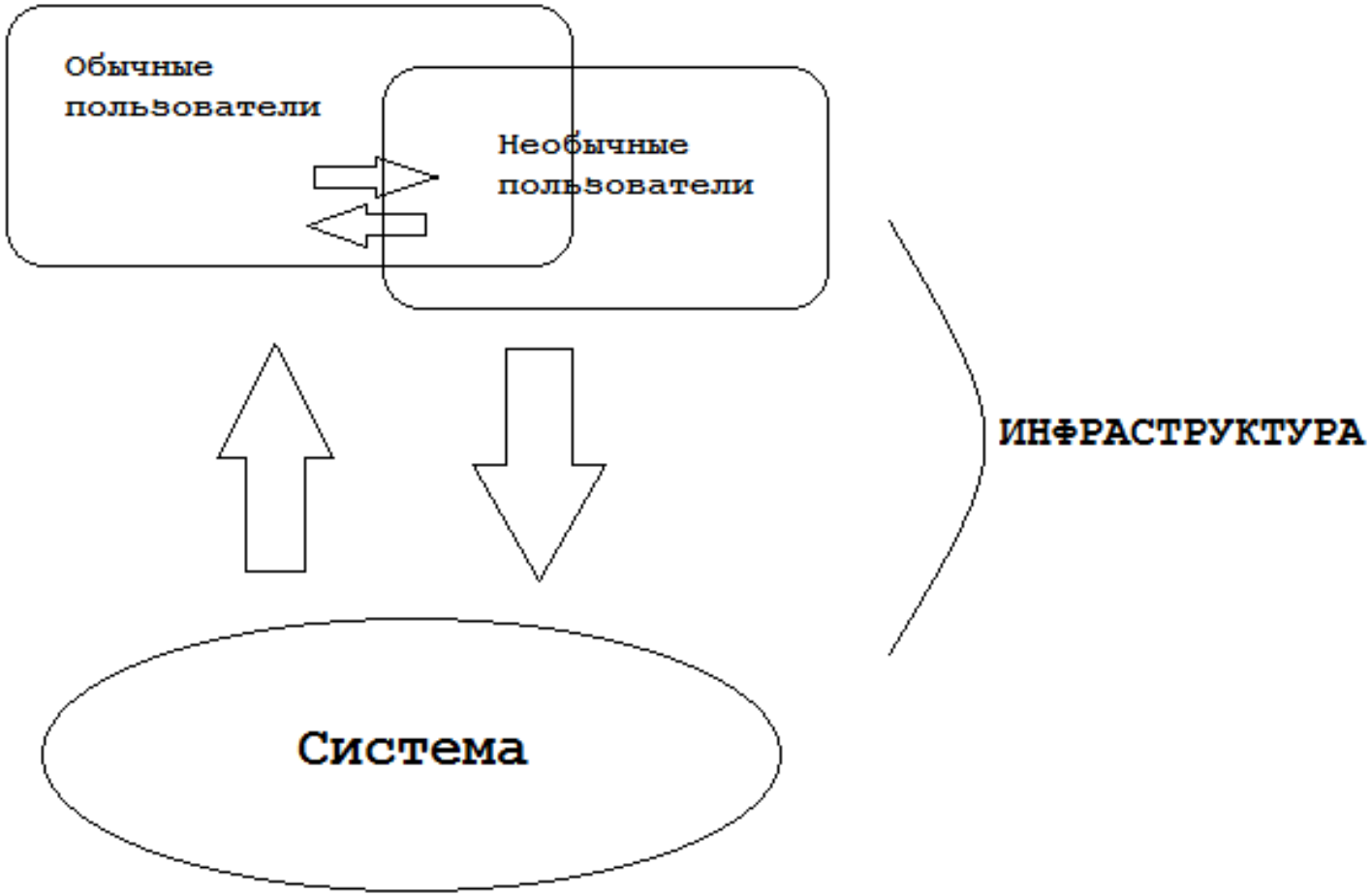
- разогревался постепенно;
- перешёл от «компьютерных гиков» к «обычным людям»;
- существенно возрос
  - [мировые финансовые кризисы, разоблачения о слежке] $\mapsto$ [кризис доверия];
  - [информатизация всех сфер общественной жизни] $\mapsto$ [с технологиями проще и быстрее];
  - [переход финансов в виртуальное пространство] $\mapsto$ [чемоданы денег выходят из моды].

Также не забываем о возможности победить коррупцию, да и вообще любые проблемы...

Базовые понятия

- **Единица** : то, что нельзя измерить – нельзя оценить.
- **Пользователь** : простой, привилегированный, системообразующий, др.
- **Система** : совокупность структур данных и механизмов взаимодействия с ними.
- **Инфраструктура** : совокупность программно-аппаратных и инженерно-технических решений на основе которых обеспечивается функционирование системы и взаимодействие с ней пользователей.

Базовая абстракция



Сферы приложения

Цепная запись данных = подорожник.
Приложить можно к чему угодно, не всегда понятно (всегда понятно (?)) – поможет ли.

- запись истории изменений состояний произвольной системы;
- реализация «финансовых» инструментов;
- организация производственных цепочек;
- автоматизация процессов снабжения и управления активами;
- оцифровка документов, контрактов, личностей;
- система управления деловой и личной репутацией;
- и др. */Ledra Capital 84 приложения в 2015 году/*

Перейдём к пункту

Основное положение

Считается, что...

Технология цепной записи данных (блокчейн) – новый этап развития _____ (общества / государства / человечества / вселенной (?)), в котором основополагающую роль играют формальные правила, определяемые криптографическими методами.

Основной постулат

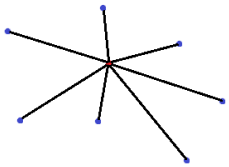
При этом постулируется, что...

Использование криптографических методов $\mapsto$ отказ от классической вертикально ориентированной иерархически организационной структуры общества/системы $\mapsto$ замена организационно-технических методов обеспечения безопасности криптографическими.

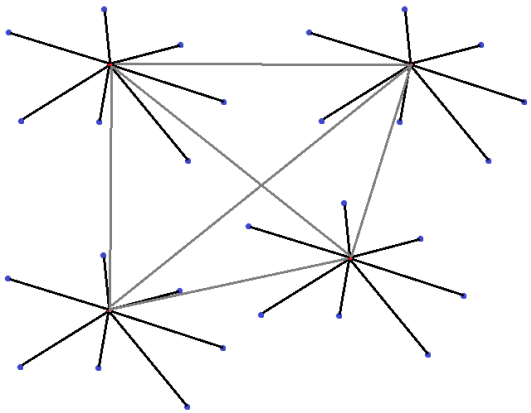
Основные цели/задачи/плюсы/...:

- решение проблемы доверия;
- оптимизация процессов работы с массивами информации.

Ожидание: «решение» проблемы доверия



Проблема существует.
Понятия подменяются.



Кому мы доверяем?

- себе?
- программе?
- устройству/аппарату/механизму?
- человеку/группе лиц/организации?

Реальность: отрицание проблемы

Избегание ответственности.

Передача прав.

Увеличение числа «надзорных лиц/организаций».

Сохранение коррупционных и бюрократических составляющих. **Реализуется не доверие третьему лицу, а доверие (децентрализованной) системе третьих лиц, контролирующих друг друга.**

ОколоКриптографические подходы к решению проблемы доверия

Обмен единицами $\mapsto$
Проблема **тиражирования** неразличимых единиц $\mapsto$
Необходимость **консенсуса** относительно решений $\mapsto$
Византийские генералы $\mapsto$
p2p + **криптография** с открытым ключом

Одна из основных проблем: реалистичная модель взаимодействия участников системы является асинхронной.

Ключи, ограничения, условия на количество генералов, и пр.

Блоки против таблиц

Перейдём к «оптимизации» процессов обработки информации.

? Базы данных существуют много лет, чем они плохи?
! Ничем не плохи.

Вопрос исключительно в идеологическом отношении к информации и её преобразованию при передаче и хранении.

Таблицы

База данных – некоторое хранилище структурированной информации, организованной в таблицы.

Ключевой момент – правила заполнения ячеек таблиц и возможности по представлению информации.

Вопросы

- организации хранения и сохранности,
- организации и разграничения доступа,
- организации достоверности хранимой информации,
- фиксации вносимых изменений

как правило, остаются за рамками понятия базы данных.

Блоки

Блоки при реализации технологии цепной записи данных – некоторые информационные массивы, сформированные по некоторым правилам.

Вопросы

- организации хранения и сохранности,
- организации достоверности хранимой информации,
- фиксации вносимых изменений

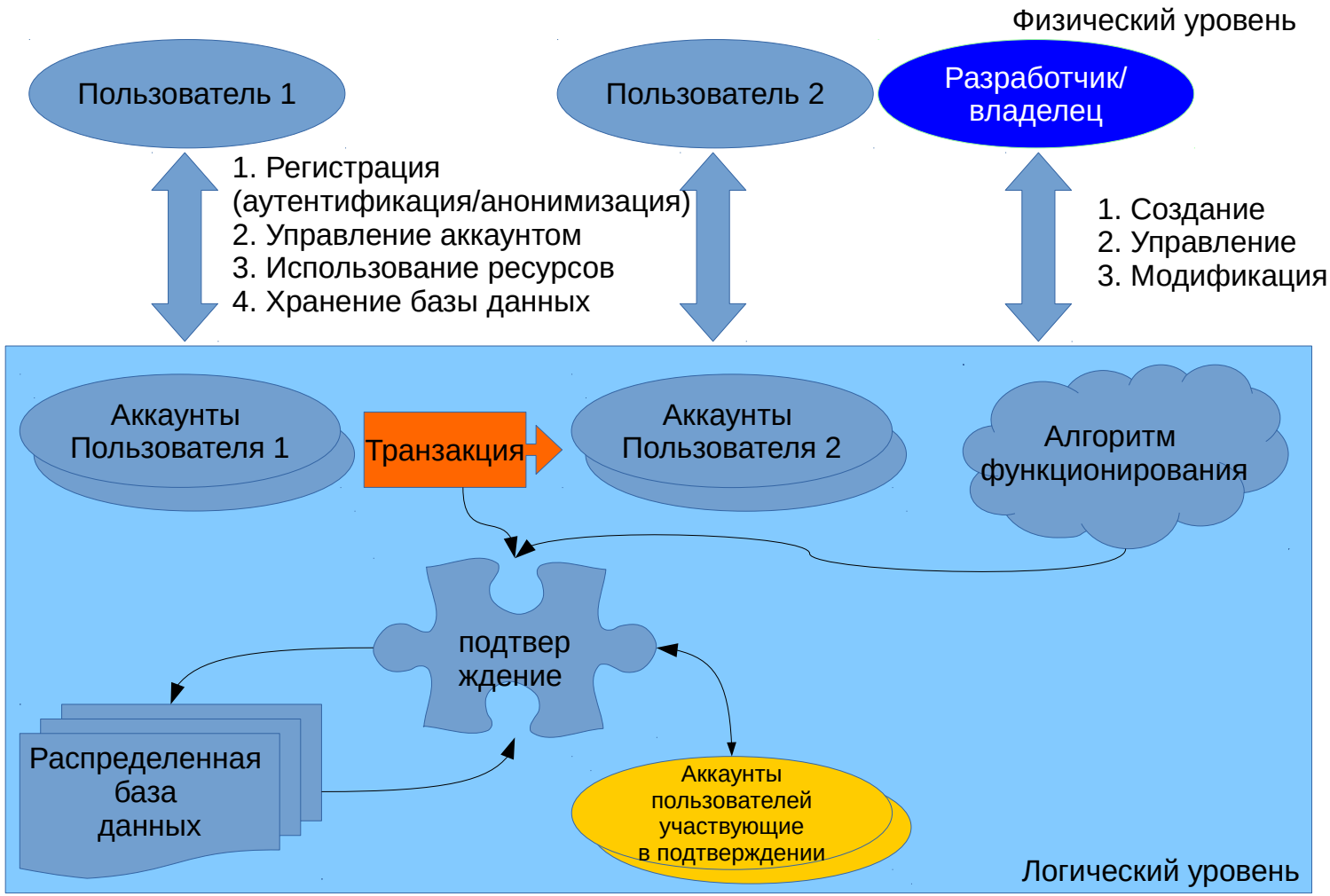
как правило, (в том или ином виде) решаются с использованием криптографических механизмов.

Вопросы организации и разграничения доступа, как правило, остаются за рамками описания системы.

Назад: блоки против таблиц?!

Фактически, технология цепной записи данных – это «надстройка» над классической базой данных, **описывающая и регламентирующая** порядок представления информации в базе и механизмы обеспечения целостности и достоверности хранимой информации, а также порядок внесения, фиксации и отслеживания изменений.

Базовая картинка («привет» из 2016)



Уровни работы системы и/или представления

1. уровень реализации «контрактов»
   - виртуальные машины vs. скриптовые языки.
2. уровень обеспечения
   - эмиссия единиц, распределение единиц, уничтожение единиц.
3. уровень консенсуса
   - Proof-of-Smthng...
4. сетевой уровень
   - топология, механизмы обмена, механизмы подтверждения.
5. уровень данных
   - представления, структуры, криптографические примитивы.

Возникающие вопросы и задачи

- как и зачем?
- до каких пор?
- почему?
- выбор типа уровнения;
- пользовательские задачи и ожидания от системы;
- обеспечение доверия к системе и консенсусу;
- переход от доверия одному центру к доверию распределённым центрам (некоторые из которых злоумышленники по определению);
- делегирование прав;
- бегство от ответственности;
- вопросы законодательного регулирования...

Текущие механизмы и текущие проблемы

- реализация инфраструктуры и топологии (см. цели и задачи);
- SHA-256 и аналоги (см. SHA-1);
- DSA и аналоги (см. квантовые вычисления и квантовый компьютер);
- AES и аналоги (см. вопросы выработки и распределения ключей, обеспечения доступности информации);
- механизмы консенсуса (см. исследования в данной области, например, ePrint 2015/430, 946)

Не реклама!

Перспективные механизмы

- датчики ПСП;
- постквантовые подписи (с неограниченным числом вычислений) + подписи без использования датчиков ПСП;
- протоколы с нулевым разглашением;
- групповые и/или слепые подписи;
- гомоморфная криптография;
- отказуемые подписи;
- криптографические методы на основе использования личностной информации и атрибутов.

Перейдём к пункту

В докладе не сделано

- не предъявлено самое большое простое число;
- не доказано всему миру, что ему как воздух нужна технология цепной записи данных;
- не решены какие-либо криптографические задачи.

В докладе

- снова затронут проблемный вопрос – а зачем?
- предпринята попытка разделить абстракцию на составные части;
- всё «упёрлось» в вопросы конкретных приложений абстрактных решений (сколько задач – столько решений);
- в очередной раз с высокой трибуны продекламирована «правильная» терминология;
- сформулировано много вопросов и мало ответов.

Ответ на главный вопрос

Пока понятие «технология цепной записи данных» будет у каждого своим – у каждого будет свой ответ на главный вопрос.

Важно: бурное внедрение технологии в различные сферы жизни даёт широкий простор для синтеза и анализа разнообразных механизмов обеспечения информационной безопасности, а что ещё надо для людей, занимающихся (около-)научными изысканиями?

Спасибо за внимание

Вопросы?