Блокчейн в России: взгляд с точки зрения криптографии

Смышляев Станислав Витальевич, к.ф.-м.н.,
начальник отдела защиты информации
ООО «КРИПТО-ПРО»
Технический комитет по стандартизации Росстандарта
«Криптографическая защита информации» (ТК 26)

Алексеев Евгений Константинович, к.ф.-м.н.,
ведущий инженер-аналитик
ООО «КРИПТО-ПРО», ТК 26

Текущее состояние

- Повсеместные активные обсуждения, большое число новых рабочих групп и проектов по использованию технологии блокчейн, стремление не упустить тенденцию.
- Зачастую: предложения о внедрении блокчейна в предметные области, в которых в нем нет необходимости (см. K. Wüst, A. Gervais, «Do you need a blockchain?»).
- Раннее состояние теоретической проработанности вопросов, ошибки в безопасности, повсеместное устранение проблем «ad hoc» решениями, зачастую противоречащими исходной идеологии.
- Требуется существенная дополнительная проработка фундаментальных вопросов, связанных с безопасностью (в том числе, с учетом российской специфики).

Текущее состояние

- Повсеместные активные обсуждения, большое число новых рабочих групп и проектов по использованию технологии блокчейн, стремление не упустить тенденцию.
- Зачастую: предложения о внедрении блокчейна в предметные области, в которых в нем нет необходимости (см. K. Wüst, A. Gervais, «Do you need a blockchain?»).
- Раннее состояние теоретической проработанности вопросов, ошибки в безопасности, повсеместное устранение проблем «ad hoc» решениями, зачастую противоречащими исходной идеологии.
- Требуется существенная дополнительная проработка фундаментальных вопросов, связанных с безопасностью (в том числе, с учетом российской специфики).

Международная и национальная стандартизация

- Международная организация по стандартизации (ISO): TC 307 «Blockchain and distributed ledger technologies»
- В Российской Федерации деятельность сопровождается Техническим комитетом по стандартизации Росстандарта «Криптографическая защита информации» (ТК 26)
  - Рабочая группа «Безопасность технологий цепной записи данных и распределенных реестров»
  - Рабочая группа «Сопутствующие криптографические алгоритмы и протоколы»

Блокчейн в России: частные задачи в области криптографии

- Управление открытыми ключами: PKI/децентрализация.
- Функционирование блокчейнов при ограниченном сроке криптографической защиты.
- Обеспечение конфиденциальности хранимых данных.
- Трансграничное взаимодействие с учетом использования российских алгоритмов (в т.ч. в рамках сайдчейна).
- Полное обоснование криптографической стойкости предполагаемых к внедрению протоколов.

Блокчейн в России: общие задачи

- Определение типов блокчейнов и протоколов консенсуса, приоритетных для внедрения, и моделей нарушителя.
- Анализ защищенности выделенных типов блокчейнов в зафиксированных моделях нарушителя.
- Проведение исследований до принятия стратегических решений о внедрении технологии.

Блокчейн в России: частные задачи в области криптографии

- Управление открытыми ключами: PKI/децентрализация.
- Функционирование блокчейнов при ограниченном сроке криптографической защиты.
- Обеспечение конфиденциальности хранимых данных.
- Трансграничное взаимодействие с учетом использования российских алгоритмов (в т.ч. в рамках сайдчейна).
- Полное обоснование криптографической стойкости предполагаемых к внедрению протоколов.

Блокчейн в России: общие задачи

- Определение типов блокчейнов и протоколов консенсуса, приоритетных для внедрения, и моделей нарушителя.
- Анализ защищенности выделенных типов блокчейнов в зафиксированных моделях нарушителя.
- Проведение исследований до принятия стратегических решений о внедрении технологии.

Управление открытыми ключами

Транзакции снабжаются ЭП, задача управления открытыми ключами (ключами проверки ЭП).

- Принятый подход: обеспечение доверия к открытым ключам, инфраструктура открытых ключей, удостоверяющие центры, аккредитация, МР ТК 26, 63-ФЗ, приказы ФСБ России 795 и 796.
- Исходная идеология блокчейн: отсутствие единых центров управления и доверия, децентрализация.
- Фактическая проблема развитых систем блокчейнов: тенденции к централизации для решения проблем масштабируемости.
- Контроль за кодом, разрешение конфликтных ситуаций («хардфорки», The DAO), делегирование проверок сервисам, «свой» майнинг для гарантии транзакций.

Управление открытыми ключами

Транзакции снабжаются ЭП, задача управления открытыми ключами (ключами проверки ЭП).

- Принятый подход: обеспечение доверия к открытым ключам, инфраструктура открытых ключей, удостоверяющие центры, аккредитация, МР ТК 26, 63-ФЗ, приказы ФСБ России 795 и 796.
- Исходная идеология блокчейн: отсутствие единых центров управления и доверия, децентрализация.

- Фактическая проблема развитых систем блокчейнов: тенденции к централизации для решения проблем масштабируемости.
- Контроль за кодом, разрешение конфликтных ситуаций («хардфорки», The DAO), делегирование проверок сервисам, «свой» майнинг для гарантии транзакций.

Срок криптографической защиты

- Принятый подход: оценка сроков действия ключей и криптозащиты при тематических исследованиях, срок действия секретного ключа от одного до трех лет.
- Исходная идеология блокчейн: доверие обеспечивается при «вечном» хранении полной базы подписанных транзакций.
- Потенциальная возможность появления полномасштабных квантовых компьютеров, развитие классического криптоанализа, в том числе с использованием побочных каналов, риски компрометации ключей.
- Аналогичная проблема в электронном документообороте: архивное хранение электронных документов.

Срок криптографической защиты

- Принятый подход: оценка сроков действия ключей и криптозащиты при тематических исследованиях, срок действия секретного ключа от одного до трех лет.
- Исходная идеология блокчейн: доверие обеспечивается при «вечном» хранении полной базы подписанных транзакций.

- Потенциальная возможность появления полномасштабных квантовых компьютеров, развитие классического криптоанализа, в том числе с использованием побочных каналов, риски компрометации ключей.
- Аналогичная проблема в электронном документообороте: архивное хранение электронных документов.

Срок криптографической защиты

- Принятый подход: оценка сроков действия ключей и криптозащиты при тематических исследованиях, срок действия секретного ключа от одного до трех лет.
- Исходная идеология блокчейн: доверие обеспечивается при «вечном» хранении полной базы подписанных транзакций.

- Потенциальная возможность появления полномасштабных квантовых компьютеров, развитие классического криптоанализа, в том числе с использованием побочных каналов, риски компрометации ключей.
- Аналогичная проблема в электронном документообороте: архивное хранение электронных документов.

Конфиденциальность данных в блокчейне

- Юридический аспект: из открытых информационных систем данные лица могут быть удалены по решению суда. Как быть с блокчейном?
- Криптографический аспект: обеспечение конфиденциальности данных поднимает дополнительные вопросы об управлении ключами, тенденция к централизации.

Адаптация применения в РФ и трансграничный обмен

- Принятый подход: обеспечение защиты информации с использованием российских криптографических алгоритмов и протоколов.
- Исходная идеология блокчейн: трансграничная работа.

- Требуются обоснования стойкости, разработка сопутствующих алгоритмов (в т.ч. «memory-hard» функций на основе российских стандартов).
- Возможный компромисс — сайдчейн. Требуется интерфейс взаимодействия.
- В случае трансграничной работы либо сайдчейнов — непрерывное плотное взаимодействие с зарубежными коллегами в рамках ISO, IETF и т.п.

Адаптация применения в РФ и трансграничный обмен

- Принятый подход: обеспечение защиты информации с использованием российских криптографических алгоритмов и протоколов.
- Исходная идеология блокчейн: трансграничная работа.

- Требуются обоснования стойкости, разработка сопутствующих алгоритмов (в т.ч. «memory-hard» функций на основе российских стандартов).
- Возможный компромисс — сайдчейн. Требуется интерфейс взаимодействия.
- В случае трансграничной работы либо сайдчейнов — непрерывное плотное взаимодействие с зарубежными коллегами в рамках ISO, IETF и т.п.

Адаптация применения в РФ и трансграничный обмен

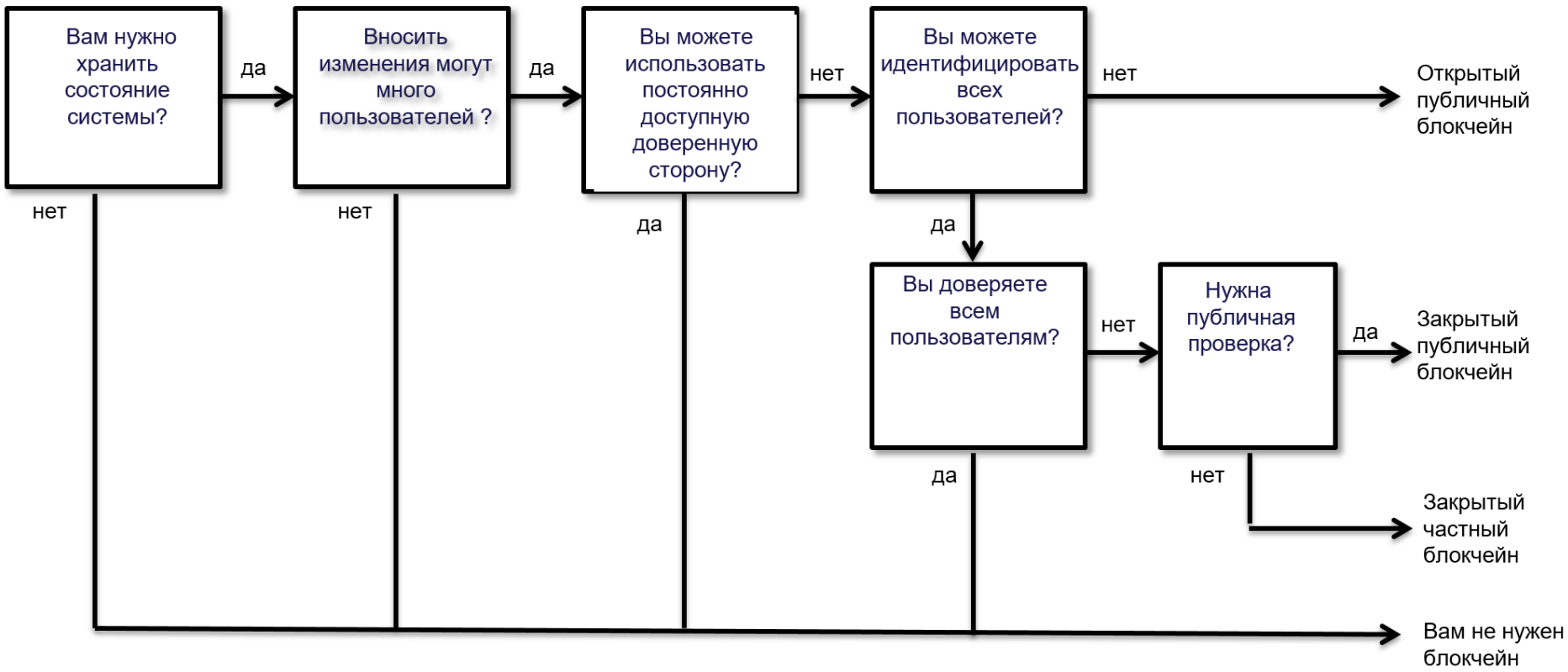
- Принятый подход: обеспечение защиты информации с использованием российских криптографических алгоритмов и протоколов.
- Исходная идеология блокчейн: трансграничная работа.

- Требуются обоснования стойкости, разработка сопутствующих алгоритмов (в т.ч. «memory-hard» функций на основе российских стандартов).
- Возможный компромисс — сайдчейн. Требуется интерфейс взаимодействия.
- В случае трансграничной работы либо сайдчейнов — непрерывное плотное взаимодействие с зарубежными коллегами в рамках ISO, IETF и т.п.

Определение применимости и оценка защищенности протоколов консенсуса

- Proof-of-Work: проблема — отсутствие полных обоснований (только в частных моделях), исследования ведутся (см. «Analysis of the Blockchain Protocol in Asynchronous Networks», «Practical Synchronous Byzantine Consensus»).
- Proof-of-Authority — потеря децентрализации, Proof-of-Stake — дополнительные задачи для отслеживания «nothing-at-stake»-махинаций.
- Предпосылки для юридической значимости, кроме случая закрытого частного блокчейна, представляются крайне трудным вопросом.
- Существующие прототипы (QIWI, Открытие, Сбербанк, Альфа-Банк) пока имеют локальный характер.

- Karl Wüst, Arthur Gervais, «Do you need a blockchain?».



- Привлечение криптографического сообщества и анализ безопасности конечных протоколов необходимы.
- Пример: CryptoNote–ByteCoin, критическая уязвимость из-за неграмотного совмещения энтузиастами двух (стойких) криптографических объектов.

Направления работы в области криптографической защиты

- Терминология, методология оценки защищенности, обоснования стойкости должны быть сформированы до внедрения систем.
- Привлечение криптографического сообщества и анализ безопасности конечных протоколов необходимы.
- Задачи рабочих групп ТК 26, обсуждений на конференциях (круглый стол на CTCrypt 2017 5-7 июня).
- Развитие пилотных проектов — стандартизация должна идти с учетом опыта тестовой эксплуатации, а тестовая эксплуатация помогать выявлять модели угроз и нарушителя.

Выводы

Требуется:

- координация действий рабочих групп в области блокчейн;
- обсуждения конкретных проектов на основе блокчейн должны проводиться с участием экспертов в области криптографической защиты информации;
- привлечение к рабочим группам в области блокчейн экспертов в области криптографической защиты информации (в том числе, представителей РГ ТК 26).

CRYPTOPRO

Спасибо за внимание!

Вопросы?

- Материалы, вопросы, комментарии:
  - svs@cryptopro.ru