Перспективы национальной и международной стандартизации в области технологии блокчейн

И. В. Лавриков, Г. Б. Маршалко, В. А. Шишкин

Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26)
ISO TC 307 «Blockchain and distributed ledger technologies»

Система международной и национальной стандартизации

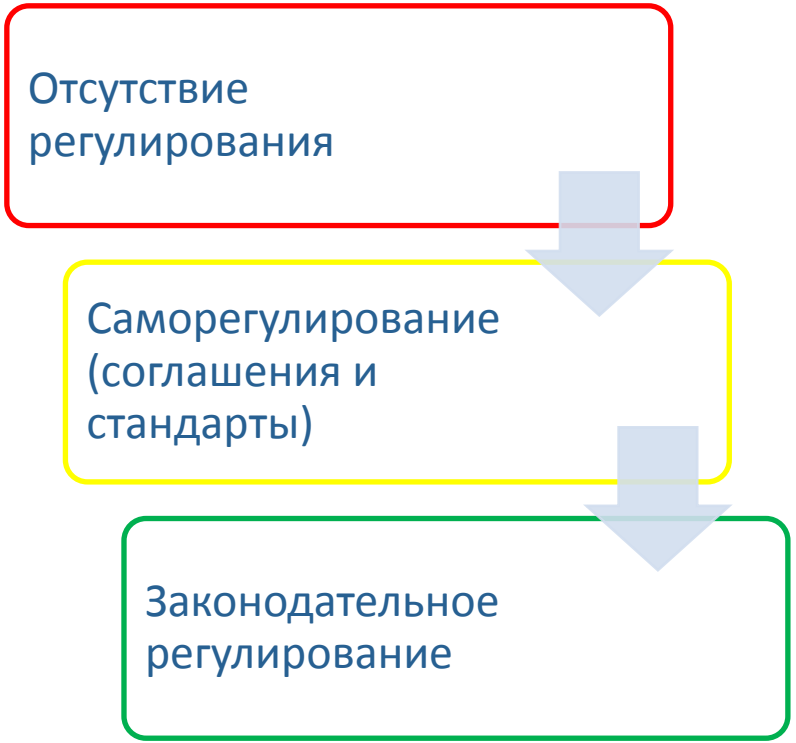
ТК 26:
- с 2007 г.
- 74 организации
- 4 национальных стандарта
- 1 международный
- 6 рекомендаций по стандартизации
- методические документы

ISO:
- с 1947 г.
- 163 страны
- 21579 международных стандартов

Росстандарт:
- с 1925 г.
- 310 комитетов

©2017, Технический Комитет по Стандартизации ТК26

Законодательное регулирование и стандартизация



©2017, Технический Комитет по Стандартизации ТК26

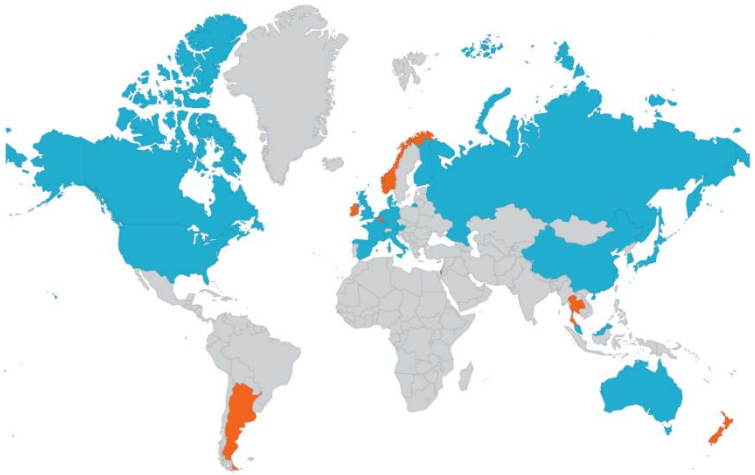
Блокчейн – текущее состояние

- **новая** технология
- **попытки** применить в различных сферах
- **различные** подходы к созданию
- **несформировавшаяся** область исследований
- **высокий** интерес и повышенные ожидания

©2017, Технический Комитет по Стандартизации ТК26

ISO/TC307 Blockchain and distributed ledger technologies

- создан в **сентябре** 2016 по инициативе Standards Australia
- **тематика**: стандартизация в области технологий цепной записи данных (блокчейн) и распределенных реестров
- 16 постоянных членов
- 9 стран-наблюдателей
- 2 внешние организации: SWIFT, Европейская комиссия
- *в Российской Федерации деятельность сопровождается Техническим комитетом по стандартизации «Криптографическая защита информации» ТК 26*



©2017, Технический Комитет по Стандартизации ТК26

ISO/TC307. **Деятельность**

Рабочие и исследовательские группы:

- **Терминология** (*Великобритания*)
- **Эталонные реализации и таксономия** (*США*)
- **Сценарии использования** (*Япония*)
- **Безопасность** (*Россия*)
- **Идентификация** (*Корея*)
- **Умные контракты** (*Германия*)

Терминология

- (!) общемировая проблема – **отсутствие** устоявшейся терминологической базы
- необходимо **сформировать** единый язык – основу понимания

©2017, Технический Комитет по Стандартизации ТК26

ISO/TC307. **Деятельность**

Рабочие и исследовательские группы:

- **Терминология** (*Великобритания*)
- **Эталонные реализации и таксономия** (*США*)
- **Сценарии использования** (*Япония*)
- **Безопасность** (*Россия*)
- **Идентификация** (*Корея*)
- **Умные контракты** (*Германия*)

Эталонные реализации и таксономия

- (!)большое количество реализованных вариантов на текущий момент
- формулировка **общих** подходов к построению
- определение «строительных» **блоков**
- **классификация**

©2017, Технический Комитет по Стандартизации ТК26

ISO/TC307. **Деятельность**

Рабочие и исследовательские группы:

- **Терминология** (*Великобритания*)
- **Эталонные реализации и таксономия** (*США*)
- **Сценарии использования** (*Япония*)
- **Безопасность** (*Россия*)
- **Идентификация** (*Корея*)
- **Умные контракты** (*Германия*)

Сценарии использования

- попытки применения в **различных сферах** деятельности: *финансы, страхование, производство, Интернет вещей, торговля, государственное управление, здравоохранение*
- (?) вопрос о плюсах/минусах использования
- необходимо выделить **особенности**, требуемые **свойства** и **характеристики** в *каждой* сфере

©2017, Технический Комитет по Стандартизации ТК26

ISO/TC307. **Деятельность**

Рабочие и исследовательские группы:

- **Терминология** (*Великобритания*)
- **Эталонные реализации и таксономия** (*США*)
- **Сценарии использования** (*Япония*)
- **Безопасность** (*Россия*)
- **Идентификация** (*Корея*)
- **Умные контракты** (*Германия*)

Безопасность

- 2015-2016: начало **фундаментальных** исследований
- подходы к **оценке** безопасности: *безопасность данных, консенсус, стабильность, майнинг, активные атаки, использование криптографических алгоритмов (квантовые компьютеры), …*
- (!) в настоящий момент **нет** полного понимания, что такое ***безопасный*** *блокчейн*
- направление **критически важно** для доверия к технологии

©2017, Технический Комитет по Стандартизации ТК26

ISO/TC307. **Деятельность**

Рабочие и исследовательские группы:

- **Терминология** (*Великобритания*)
- **Эталонные реализации и таксономия** (*США*)
- **Сценарии использования** (*Япония*)
- **Безопасность** (*Россия*)
- **Идентификация** (*Корея*)
- **Умные контракты** (*Германия*)

Идентификация/аутентификация/авторизация

- **пользователей** при использования системы
- **объектов/субъектов** при ее функционировании
- (!) один из самых проблемных вопросов с точки зрения **регулирования** криптовалют

©2017, Технический Комитет по Стандартизации ТК26

ISO/TC307. Деятельность

Рабочие и исследовательские группы:

- **Терминология** (*Великобритания*)
- **Эталонные реализации и таксономия** (*США*)
- **Сценарии использования** (*Япония*)
- **Безопасность** (*Россия*)
- **Идентификация** (*Корея*)
- **Умные контракты** (*Германия*)

Умные контракты

- **потенциально** могут облегчить/ заменить существующие правовые отношения
- действительно ли / в какой мере (?):

Scott Farrell. The (green and) gold standard. Designing blockchains to work in the real world

©2017, Технический Комитет по Стандартизации ТК26

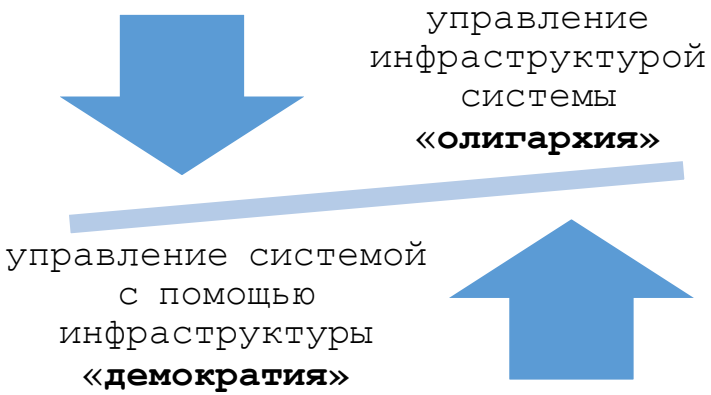
ISO/TC307. Перспективные направления

Предполагаются исследования

- управление системами
- взаимодействие
- (?)

Управление системами

- как **управлять** распределенной и/или децентрализованной системой
- **кризис биткойна**:



Primavera De Filippi, Bejamin Loveluck. **The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure**

©2017, Технический Комитет по Стандартизации ТК26

ISO/TC307. Перспективные направления

Предполагаются исследования

- управление системами
- взаимодействие
- (?)

Взаимодействие

- взаимодействие **между** системами, использующими блокчейн (сайдчейн)
- взаимодействие **с существующими** системами

©2017, Технический Комитет по Стандартизации ТК26

Деятельность ТК 26

- ноябрь 2016 – рабочая группы по **безопасности** технологий *цепной записи данных* и распределенных реестров (**ЦЗД и РР**)
- **тематика** – исследование возможности стандартизации технологий ЦЗД и РР
- специалисты 9 организаций-членов ТК 26 и 3 внешних организаций (QIWI, **МГИМО**, **Минкомсвязь** России)

Определены **вопросы** к изучению:

- терминология/классификация (проект – **ноябрь** 2017)
- методология оценки безопасности (проект – **март** 2018)
- **сценарии** внедрения в России

©2017, Технический Комитет по Стандартизации ТК26

Деятельность ТК 26

- 5-7 июня, поселок Репино, Санкт-Петербург
- VI симпозиум CTCrypt «Современные тенденции в криптографии»
- Секция **«Блокчейн: ожидание рынка и мнения экспертов»**

Вопросы к обсуждению:

- опыт **внедрения** решения на основе блокчейн: плюсы и минусы
- **безопасность** решений на основе блокчейн с позиции современных подходов к защите информации
- пользовательские **сценарии**

©2017, Технический Комитет по Стандартизации ТК26

Проблемы развития блокчейн

- **законодательное** регулирование (*в т.ч. частные вопросы, электронная подпись обеспечение юридической значимости*)
- разнообразие решений
- слабо проработанная область с **научной** точки зрения
- обеспечение **конфиденциальности**
- идентификация/аутентификация/авторизация
- **стабильность** систем/способы управления/противодействие атакам
- **эффективность**

©2017, Технический Комитет по Стандартизации ТК26

Мысли о перспективах.
Что было бы неплохо сделать

- законодательное **регулирование**
- научное обоснование **эффективности** и **безопасности** систем, использующих блокчейн
- **доверенные** криптографические методы обеспечения безопасности в системах подобного рода

Не потерять технологическую иголку в стоге (не)возможных приложений…

©2017, Технический Комитет по Стандартизации ТК26

Перспективы.
Что реально можно сделать

- подготовка рамочных (определяющих правила игры: терминология, принципы синтеза, безопасность) **стандартов** – 1,5–2,5 года
- подготовка полноценных **научных** обоснований для всех аспектов используемых технологий – 1–5 лет
- получение содержательных теоретических и практических результатов в данной области – бесконечно…

©2017, Технический Комитет по Стандартизации ТК26

Спасибо за внимание

Вопросы?

www.tc26.ru

www.ctcrypt.ru

tc26@tc26.ru

@CryptographyRU

©2017, Технический Комитет по Стандартизации ТК26