

Проблемы технологии блокчейн с точки зрения стандартизации

Григорий Маршалко

Терминология и базовые определения

- ▶ Техническая сторона вопроса и существующие стандарты:

распределенная база данных \approx

\approx распределенный реестр \geq

\geq блокчейн

- ▶ Разные подходы к определению
 - частный случай распределенного реестра
 - цепочка связанных между собой транзакций
- ▶ ТК 26 – пробуем альтернативные варианты



Хаотичная разработка и большое число существующих вариантов

- ▶ Криптовалюты – единственный в каком-то смысле состоявшийся пример применения
- ▶ Попытки применения в других областях наталкиваются на несоответствие исходной модели функционирования системы решаемым задачам
- ▶ Как результат: рост числа различных вариантов:
 - централизованные/децентрализованные
 - общедоступные/закрытые
 - с аутентификацией/ без аутентификации
 -
- ▶ Разные варианты -- разные характеристики



Пример: консенсус

- ▶ Классика: доверенная третья сторона
- ▶ Отсутствие доверия: протоколы консенсуса
 - вероятностная природа
 - соревновательный принцип выбора лидера (доверенной третьей стороны)
- ▶ PoW –
 - энергонезэффективен
 - большое число вариантов атак
- ▶ Поиск вариантов PoS, DPoS, PoSp,....
- ▶ Различные варианты -- различные характеристики



Связь с физическим миром

- ▶ Попытки применения вне цифровой среды – проблема достоверного внесения информации
- ▶ Пока решения, кроме организационных мер нет – какова модель?
- ▶ Каждый вариант применения – свои решения



Возможное развитие

- ▶ В условии разнообразия вариантов – движение от конкретных примеров с описанием их характеристик к формулировке общих требований к системам

