Введение в технологии Blockchain

Курс Информационные системы

Севрюков С.Ю.

Поиск проблем

Нет доверительной среды передачи данных

- Нет прямой связи между большим количеством участников информационного обмена (Прямой и монопольный канал между каждой парой участников)
- Есть общая сеть, действия в которой не могут контролироваться участниками информационного обмена

Если данные хранятся и обрабатываются в «центре», то они им могут быть искажены или утеряны (без ведома участников информационного обмена)

Средства аутентификации и контроля целостности могут быть уязвимы методом перебора (брутфорс)

- Подбор пароля
- Подделка подписи

Для повышения надёжности мы можем прибегнуть к услугам надёжных посредников, за которые надо платить

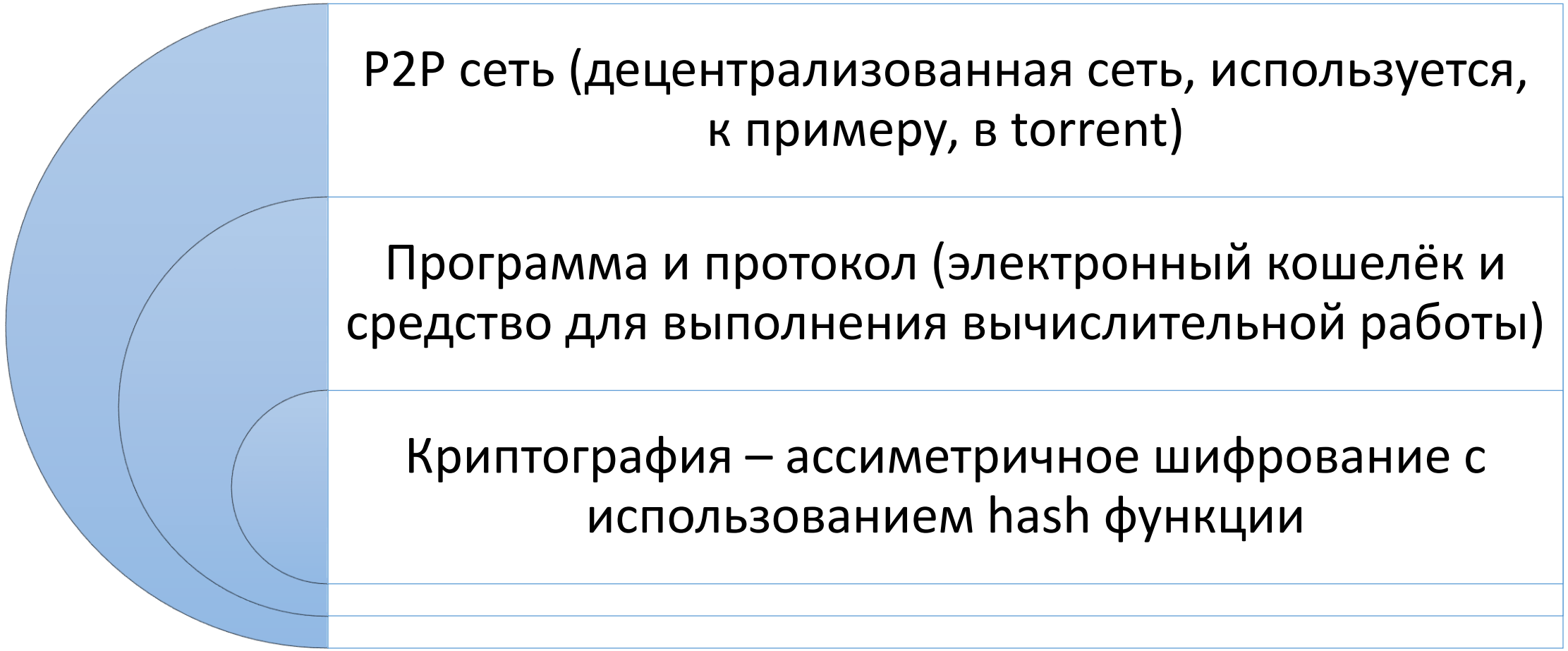
Постановка задачи: Реализовать БД и средства работы с ней с акцентом на

- Достижение соглашения с другими участниками в отсутствие надежной системы коммуникаций
- Независимость от центра (единой точки принятия решения)
- Надёжность хранения
- Целостность (корректность и достоверность) данных

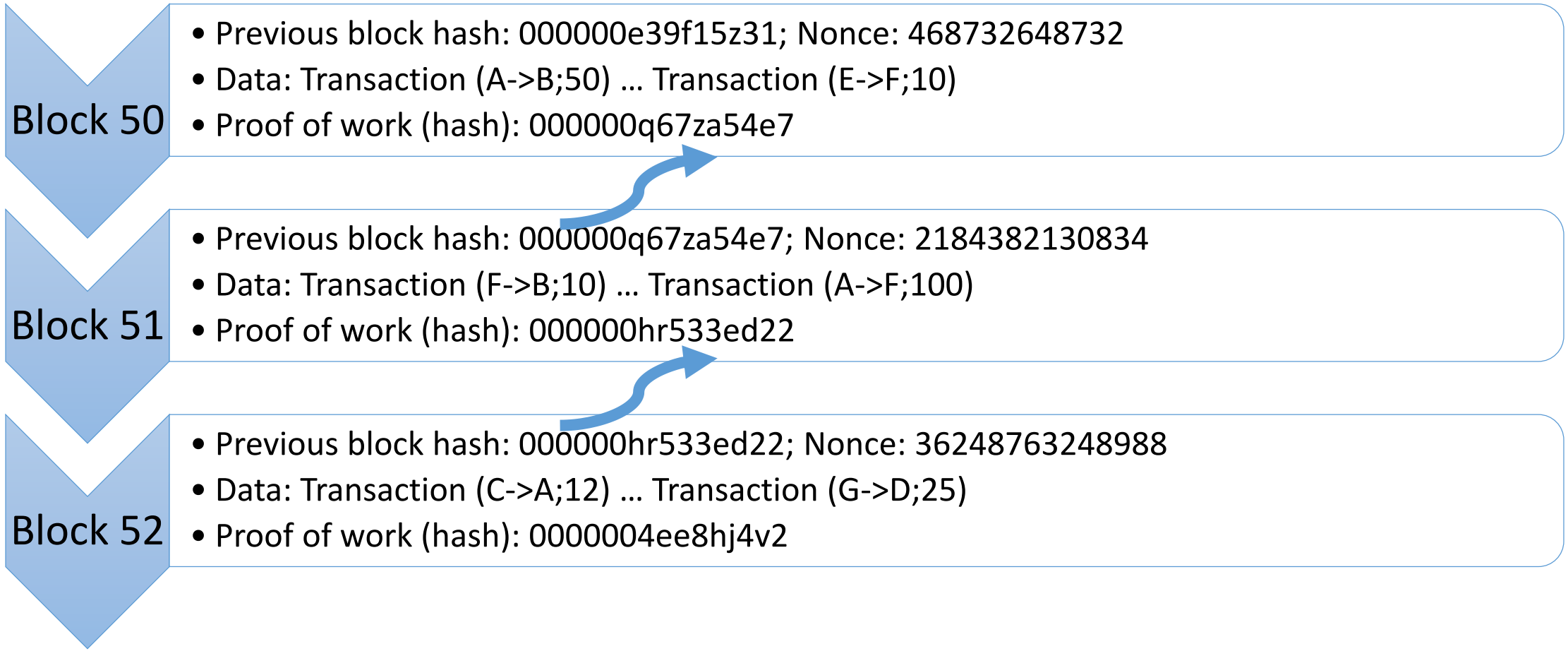
Формальное определение: Blockchain

- Связанный список данных (данные блока, метаданные, ссылки и электронные подписи)
- Избыточность по хранению блоков (множество копий)
- Вычисление с помощью множества независимых друг от друга узлов
- Наличие только одной непротиворечивой цепочки блоков (отказ от возможных ветвей, возникающих из-за распределённого и параллельного порядка вычисления)
- Каждый блок подтверждается всеми последующими (снижение рисков подделки)

Используемые технические средства



Структура Blockchain



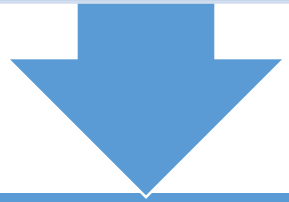
Структура блока

Previous block hash: 000000e39f15z31	Ссылка на предыдущий блок в виде hash (предыдущего блока)
Nonce: 468732648732	Случайное значение (результат майнинга)
Data: Transaction (A->B;50) … Transaction (E->F;10)	Данные. Например, данные о денежных переводах
Proof of work (hash): 000000q67za54e7	Контрольная сумма, отпечаток, подпись на основе hash функции

Влияние изменений на результат применения sha256

Previous block hash: 000000e39f15z31; Nonce: 468732648732;
Data: Transaction (A->B;50) … Transaction (E->F;10)

7ab00b56c41414a0c4f455a1479c595f9b85e347a14b9f61a839eed5509113f0



Previous block hash: 000000e39f15z31; Nonce: 468732648732;
Data: Transaction (A->B;500) … Transaction (E->F;10)

c39edca7d35f27d19f2c0425be3155d21b2e97def8b0b45f72a959547e8f82f4

Вычислительная сложность (mining)

- Требование: получить не просто hash исходных данных, а hash удовлетворяющий условию
  - Содержит определённые символы в определённой позиции
  - Начинается с определённого количества нулей
  - Является простым числом
- Единственный способ получить такой hash – перебрать все возможные значения, меняя небольшое количество исходных данных
- Такими изменяемыми данными являются не целевые, а специальная добавка (nonce)

Криптовалюты: пока больше вопросов

Сколько их существует?

Какова их общая рыночная стоимость?

Каковы затраты энергии для реализации вычислений, гарантирующих целостность и достоверность данных?

Сколько времени уходит на полное подтверждение транзакции?

Противоречия криптовалют

Не нужны посредники	Нужны майнеры, чтобы подтвердить сделку, биржи для обмена криптовалют на обычные деньги
Bitcoin вытеснит кредитные карты	Объём банковских транзакций пока на много порядков превосходит крипто-платежи, а времени уходит на порядки меньше
Независимость валюты от государства	Да это так. Но независимость не означает легитимность (в разных аспектах). Управление экономикой требует зависимости
Анонимность	Если криптовалюта гарантирует прозрачность, то это снижает анонимность (с технической т.з.). Действия в сети пока далеки от анонимности, Blockchain открыт
Защищённость	Права покупателей и потребителей не распространяются на операции с криптовалютами (нужен дополнительный договор). Потеря кошелька необратима

Смарт-контракты

В качестве данных электронного документа могут выступать не только данные о транзакциях, но и код

Код может обрабатывать другие данные (проверять условия, вычислять значения)

Для подписания используется электронная подпись

Может выступать дополнением к платёжной транзакции

Требует правовой основы, но не потребует участия договорных посредников (например, нотариусов)

Знания и области деятельности для понимания и развития технологии

Экономика и финансы	• Стоимость и обеспечение денег, волатильность, инфляция
Право	• Защита прав, правовая основа
Информационные технологии	• Распределённые вычисления, информационная безопасность
Математика	• Криптография, теория игр
Психология	• Азартные игры, психология потребителя

Резюме

- У любой технологии есть не столь проблема надёжности, сколь проблема интеграции
  - Для встраивания Blockchain в широкую практику нужны правовые, экономические, гражданские и административные основы
- Любая технология, созданная и используемая людьми была и будет обременена человеческим фактором
- Игра на курсе криптовалют более доступна, чем другие финансовые игры, но остаётся игрой
- Отсутствие централизованного контроля и эффект толпы – их превосходство является пока непроверенной гипотезой

Рекомендуемые ресурсы

- Подборки материалов
  - «Ультимативный» блокчейн-дайджест: полезные материалы на Хабре и другие источники по теме
  - Блокчейн 101: книги, исследования и статьи по теме
- Криптовалюты
  - Место и роль виртуальных валют в современной платежной системе
  - Курс криптовалют
  - Сайт с большим количеством статистики 1
  - Сайт с большим количеством статистики 2
  - Сайт для просмотра (деталей) блокчейна Bitcoin
  - Сколько стоит биткоин в баррелях нефти?
  - Bitcoin Energy Consumption Index
  - Криптовалюты и виртуальная экономика
  - Не поддавайтесь хайпу, или почему цена биткоина не отражает его реальной ценности
- Видео
  - https://www.youtube.com/watch?v=bBC-nXj3Ng4
  - https://www.youtube.com/watch?v=SSo_EIwHSd4

Рекомендуемые ресурсы

- Безопасность
  - Распределённые реестры и информационная безопасность: от чего защищает блокчейн
  - Что угрожает блокчейн-сетям: рассматриваем атаки и способы защиты
  - Программные кошельки для Bitcoin и безопасность
- Правовые и юридические аспекты
  - Юридические аспекты операций с криптовалютами для резидентов РФ
  - Правовые аспекты майнинга криптовалют
  - Криптовалюта с точки зрения гражданского права
  - Консервативное национальное крипторегулирование. Что несут нам новые законопроекты?
- Практика использования
  - Прошло 10 лет, а никто не придумал, как использовать блокчейн