Электронные деньги (Цифровые деньги)

Системы электронной наличности

Лекция Ливак Е.Н.

Электронные деньги

- Электронные монеты (купоны)
- Электронные чеки

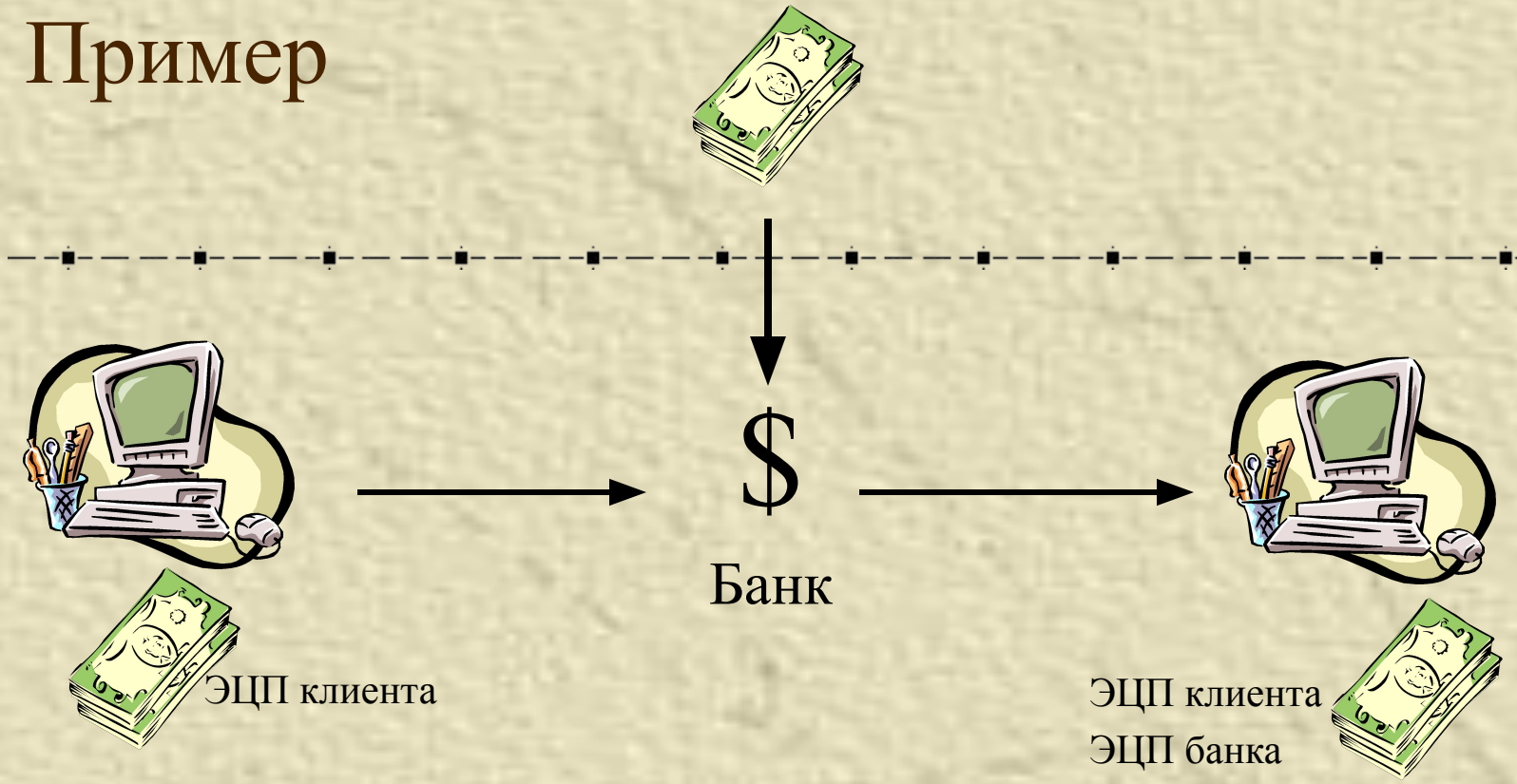
Идея. Аналоги наличных купюр

- Предварительно у банка-эмитента покупаются электронные АНАЛОГИ наличных купюр (монет)

  ≡ Электронные монеты, купоны (tokens)

✔ Каждый купон банк заверяет своей цифровой подписью

Пример



- Клиент создает на своем компьютере электронные купюры (определяет их номинал, серийный номер) и заверяет их своей ЭЦП
- Посылает электронные купюры в банк

- Банк при поступлении реальных денег на счет подписывает эти купюры (знает только номинал) и отправляет их клиенту.

Что такое электронная (цифровая) монета?

- **Электронная монета (купон) – файл**

  Последовательность бит специального вида

  - Идентификатор монеты (купона)
  - Денежный номинал
  - Электронная Цифровая Подпись (ЭЦП) банка

Электронная монета (купон) – файл-обязательство банка-эмитента платежной системы, подписанное цифровой подписью эмитента

Электронная монета подтверждает факт, что эмитент должен клиенту соответствующую сумму денег

✔ Файл-монету можно передать продавцу или другому лицу

Идея. Оплата товара/услуги

- При оплате покупатель отправляет электронные купоны продавцу
- Продавец передаёт купоны в банк на проверку и погашение

✔ Продавец не получает сведений о клиенте

Идея. Расчеты

- Банк
  - проверяет подлинность купонов
  - снимает со счёта плательщика сумму, эквивалентную сумме купонов
  - производит зачисления на счет продавца

Для предотвращения повторных выплат

банк записывает серийные номера

всех погашенных купонов

1. Эмиссия электронной монеты
(технология реализации цифровой наличности)

- Клиент генерирует

случайную цифровую последовательность – идентификатор монеты

- Добавляет номинал монеты

$$a = \text{идентификатор монеты} + \text{номинал купюры}$$

- Вычисляет значение

$$R = H(a) * b^e \pmod N,$$

где b – blinding factor (слепой множитель) – случайное число

e – экспонента открытого ключа банка

H – хэш-функция

ЭЦП банка
e – экспонента открытого ключа
d – экспонента закрытого ключа

R ——> банк

2. Эмиссия электронной монеты
(технология реализации цифровой наличности)

1. Банк списывает со счета клиента значение номинала монеты
2. Зашифровывает R закрытым ключом, т.е. вычисляет и отправляет клиенту

$$\mathbf{R}^{d} \pmod N \longrightarrow \textbf{клиент}$$

ЭЦП банка
e – экспонента открытого ключа
d – экспонента закрытого ключа

3. Эмиссия электронной монеты
(технология реализации цифровой наличности)

$$\mathbf{R}^{d} \pmod N = H(a)^{\mathbf{d}} * b \pmod N$$

- Зная $\mathbf{R}^{d} \pmod N$ и **b**

клиент находит $H(a)^{\mathbf{d}} \pmod N$

(с помощью алгоритма Эвклида нахождения наибольшего общего делителя b и N)

✔ Цифровое выражение электронной монеты

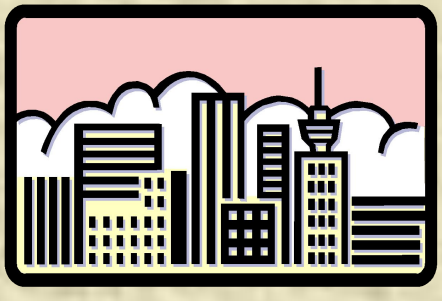
последовательность $(a, H(a)^{\mathbf{d}} \pmod N)$

Эмиссия электронной монеты
(технология реализации цифровой наличности)

a =
идентификатор
монеты
+ номинал купюры

$\mathbf{R} = H(a) * b^{e} \pmod N$

$\mathbf{R}^{d} \pmod N$



?

$(a, H(a)^{\mathbf{d}} \pmod N)$

Свойства электронных денег

- Анонимность
- Возможность обмена на товары и услуги
- Делимость суммы

электронные деньги = обычным деньгам

Большое количество проблем

Что такое электронные чеки?

- АНАЛОГ бумажного чека из чековой книжки

Это указание покупателя банку перечислить деньги на указанный счет

- Выдается получателю платежа
- Получатель предъявляет чек в банк для получения наличных либо зачисления на счет

✔ Электронный чек можно передать для оплаты товара или услуги по сети

Системы электронной наличности

История вопроса

- Идея электронных наличных возникла в 1980-х годах

David Chaum (Давид Шаум, Дэвид Чом)

голландец (проживал в США)

- Получил патенты на криптографические алгоритмы «слепой подписи»

✔ Протоколы Чома позволяли создавать виртуальные электронные анонимные деньги

- Основал компанию DigiCash для распространения электронной наличности
- В **1995 г.** систему DigiCash лицензировали некоторые банки США, Европы, Австралии и Японии, т.е. она начала работать
- В 1998 г. компания DigiCash обанкротилась (отсутствие спроса, недостаток финансирования)
- В **2000 г**. все выкупила компания eCash Technologies и продолжила внедрение электронных денег

Системы электронных чеков

- Зарубежные системы
  - CyberCash
  - FSTC (Financial Services Technology Corporation)
- Российская система PayCash

Российская система PayCash

- Клиент имеет электронную платежную книжку (эквивалент чековой книжки)
- Электронная книжка пополняется в банке

✔ **Программы** на клиентских компьютерах, обслуживающие операции в системе, часто называются **кошельками**:
Кошелек пользователя, Кошелек продавца

Российская система PayCash
Схема покупки товара / услуги

1. Кошелек продавца посылает кошельку покупателя **текст договора** о покупке, подписанный ЭЦП
2. Кошелек покупателя отправляет продавцу
    1) Подписанный текст договора ЭЦП покупателя
    2) Электронный чек
3. Продавец отправляет электронный чек в банк для авторизации
4. Банк
    1) проверяет подлинность чека и остаток средств
    2) переводит деньги на счет продавца
    3) высылает продавцу электронную квитанцию для покупателя
5. Продавец высылает квитанцию клиенту и доставляет товар

✔ **Программы** на клиентских компьютерах, обслуживающие операции в системе, называются **кошельками**:

Кошелек пользователя, Кошелек продавца

Российская система PayCash
Схема покупки товара / услуги

Договор

Чек

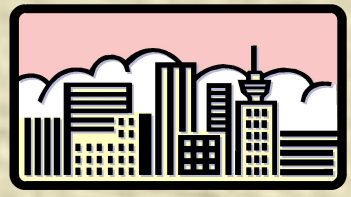
Квитанция об оплате

Товар

Покупатель

Чек

Торговое предприятие



Банк

Системы электронных наличных

- **Российская система WebMoney**

Первая официальная в Беларуси

- Платежная система EasyPay

  Система микроплатежей через Internet

Преимущества схем электронной наличности (по сравнению с системами пластиковых карт)

- Надежные (более дешевые) средства аутентификации участников транзакции
- Себестоимость транзакции в схеме электронной наличности в несколько раз ниже

  При использовании пластиковых карт помимо Internet применяются выделенные телекоммуникационные системы

- Комиссионные банкам меньше

Формула комиссионных
X%, но не менее Y

- Небольшие платежи (сравнимые с Y) невыгодны
- Для больших платежей X% может оказаться слишком большим

При более низкой себестоимости транзакции
(в системах цифровой наличности) X и Y много меньше