Цифровые деньги

Электронные платежи

- Преимущества электронных денег
    - Дешевизна банковских операций
    - Анонимность
    - Защищенность от подделки
    - Возможность использования в электронном бизнесе

Требования и характеристики платежных систем

- Безопасность
  - Невозможность подделки
  - Невозможность превысить кредит
  - Невозможность двойной траты
  - Анонимность
  - Аппаратная/криптографическая основа стойкости

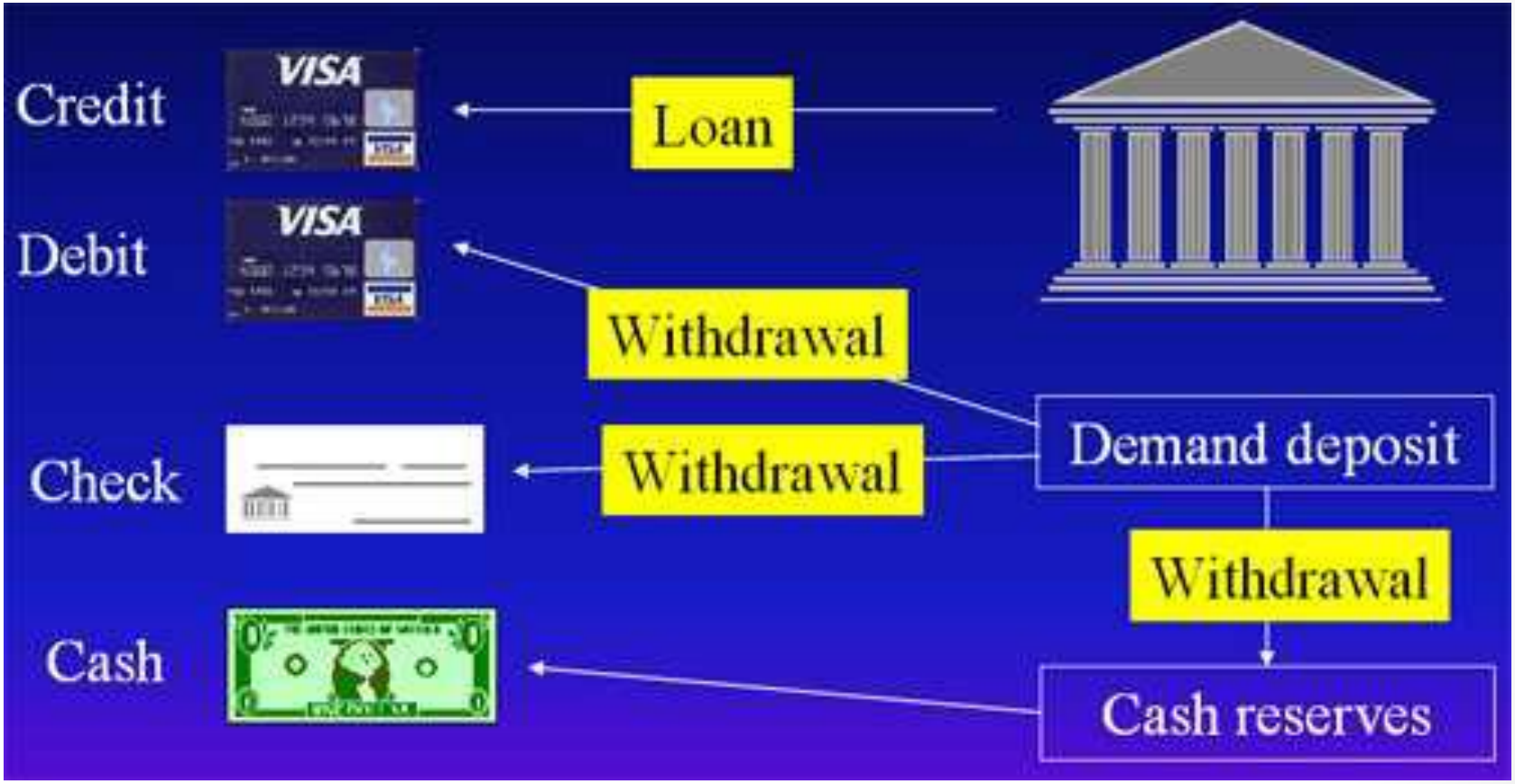
Требования и характеристики платежных систем

- Эффективность
  - Масштабируемость
  - Вычислительная трудоемкость
  - Коммуникационная сложность
  - Стоимость банковского обслуживания

Возможности платежных систем

- Возможности
  - Переносимость
  - Делимость
  - Универсальность
  - Возможность удаленной оплаты

Типы платежей

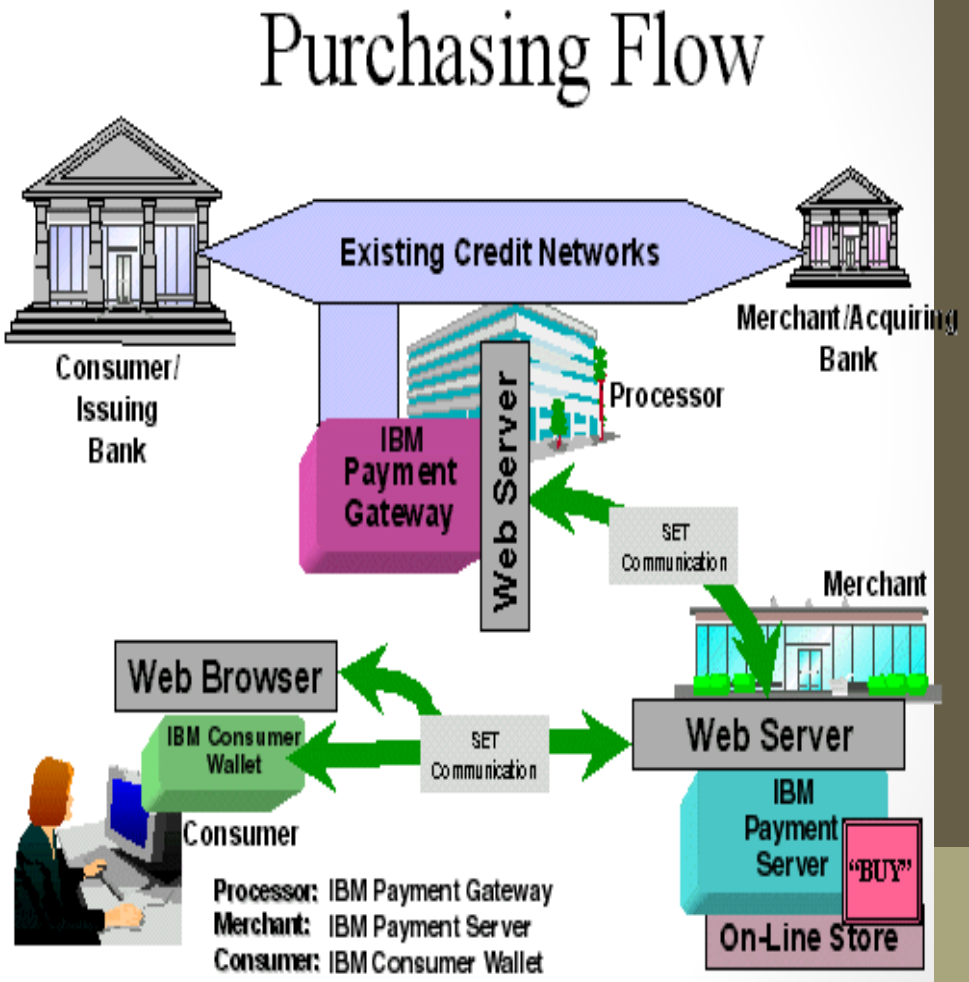


Кредитные карты

- Дебетные карточки
  - Кладем деньги
  - Сумма хранится на карточке
  - Потраченные деньги вычитаются из баланса карточки
- Кредитные карточки
  - Заводим счет в банке
  - Деньги снимаются со счета
- Криптографическая основа
  - Протокол SET

Secure Electronic Transaction (SET)

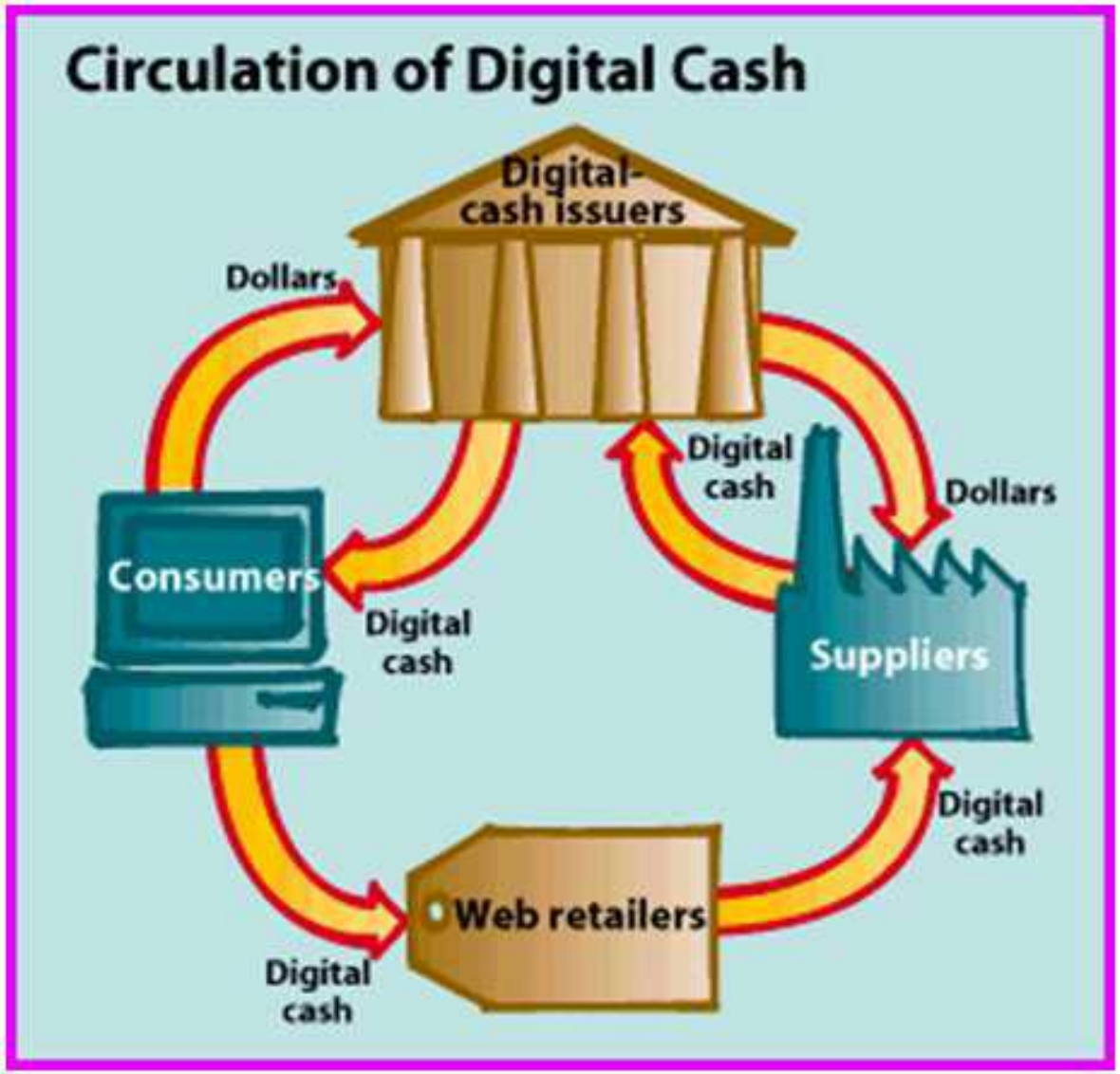
- Протокол разработан Visa International и MasterCard International
- SET использует цифровые сертификаты для удостоверения всех участников протокола
  - Покупателя, продавца, банки продавца и покупателя



Микроплатежи

- Специфика
  - Не требуется анонимность
  - Минимизация криптографических вычислений
- Современные решения
  - Millicent
  - Payword

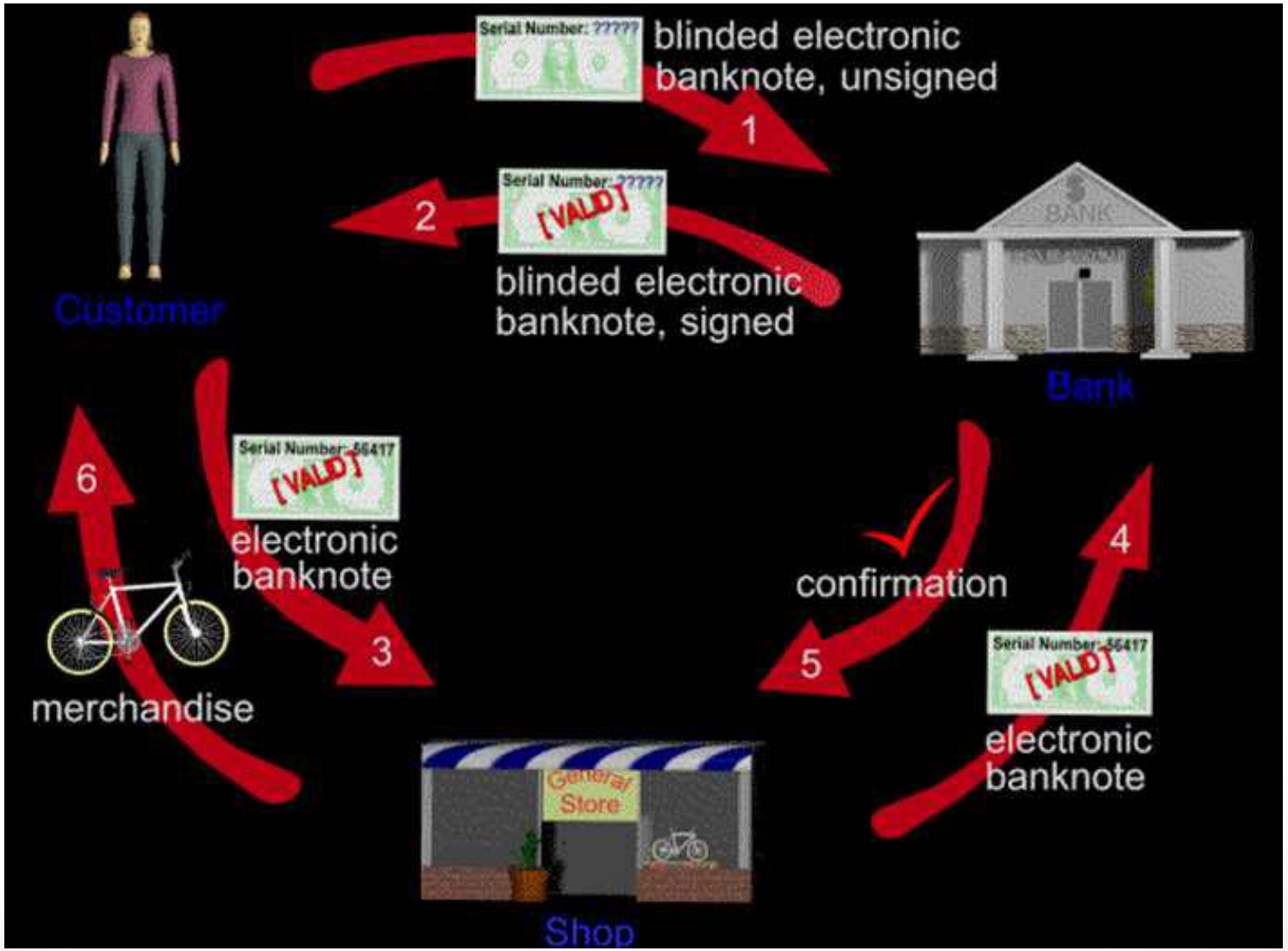
Электронные наличные



Используемая криптография

- Аутентификация сообщений
  - Гарантирует целостность
- Шифрование
  - Гарантирует секретность операций от посторонних
- Цифровые сертификаты
  - Защищают от мошенников
- Слепая подпись
  - Используется для электронных наличных (Аннонимность)

Общий вид схемы



Наивный протокол

- Обналичивание
  - 1) Участник просит Банк выдать 100$
  - 2) Банк присылает счет на 100$: { Я счет на 100$ #4257 }SK_B
  - 3) Участник проверяет подпись и признает счет
- Оплата
  - 1) Участник посылает продавцу счет
  - 2) Продавец проверяет подпись и признает счет
- Получение денег
  - 1) Продавец посылает счет в Банк
  - 2) Банк проверяет свою подпись и переводит деньги продавцу

Недостатки

- Можно тратить дважды
- Нет анонимности

Построение анонимности

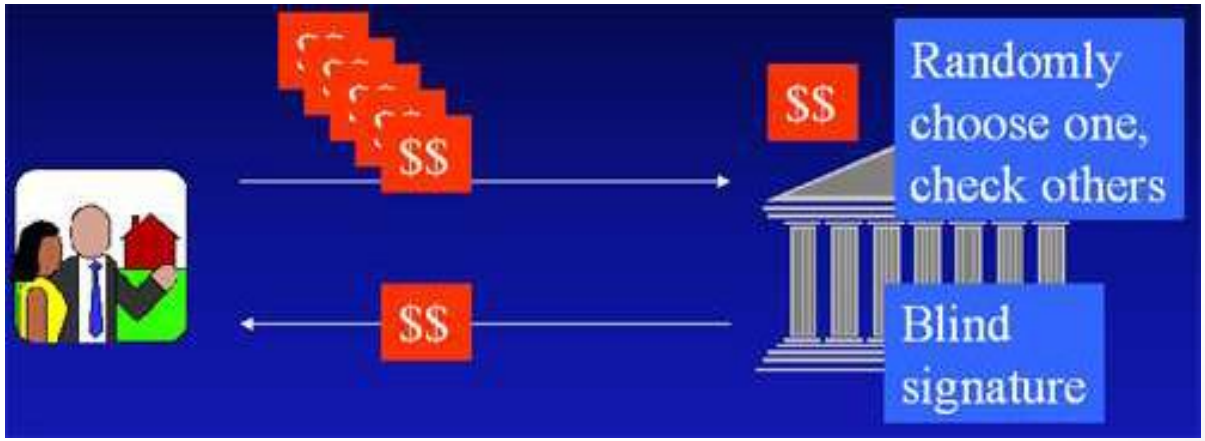
- Обналичивание - новый вариант
  - 1) Участник просит Банк выдать 100$
  - 2) Участник готовит счет: { Я счет на 100$ #4257 }
  - 3) Банк вслепую подписывает счет
  - 4) Участник проверяет подпись и признает счет

- Остались проблемы:
  - 1) Двойной траты
  - 2) Банк подпишет 1000$ вместо 100$

Проверка выдаваемой суммы

- Выборочная проверка
  - 1) Участник посылает Банку 1000 счетов
  - 2) Банк проверяет (открывая) 999 и подписывает 1000-ый счет

- Система ключей:
  - 1) У банка есть набор секретных ключей SK_1, SK_{10}, SK_{100}, . . .
  - 2) Каждая подпись годится только для фиксированной суммы



Контроль двойной траты

- On-line контроль
  - Продавец высылает запрос Банку

    “Была ли уже потрачена купюра 4257?”
- Off-line контроль:
  - 1) Участник генерирует $x_1, \ldots x_k, y_1, \ldots, y_k$ так, что $ID = x_i \oplus y_i$
  - 2) Участник посылает Банку хэш-функции от этих значений
  - 3) К каждой электронной купюре добавляется набор из k значений, по одному из пары по выбору Продавца
  - 4) Два раза потратили $\Rightarrow$ с вероятностью $1 - 2^{-k}$ можно установить нарушителя

Пошаговая схема протокола