

# Криптография - 3

Виталий Павленко, «Интеллектуал»

# Повторяем симметричное шифрование

- Правило рубрики: на каждый вопрос отвечает человек, который пока что отвечал меньше остальных
- Что такое шифр Виженера?
- Что такое SP-сеть?
- Используются ли шифры вроде AES на практике?

# Что это?

к	н	с	а	а	я	с	о
м	ж	ы	к	п	д	е	т
р	о	е	ы	щ	м	д	й
о	е	с	а	ж	в	а	е
с	л	т	т	м	и	т	р
с	з	е	е	п	а	т	с
и	п	а	е	м	е	с	р
ь	б	с	а	я	я	н	й

т о у ч у с е ш  
 е х б в н и н о  
 в и м е н ч и о  
 т е с л о в о в  
 е о о ц б и р и  
 у е у о б н у н  
 р в я о н а к т  
 в в о е о ! л !





# Повторяем хеши


- Какими свойствами должна обладать функция  $h(x)$ , чтобы человечество её использовало в качестве хеш-функции?
- Как устроена хеш-функция SHA-1?
- Какие атаки на хеш-функции известны?
- Как и зачем люди солят хеши?
- Догадайтесь, какая атака на SHA-3 до сих пор не была проведена ни одним человеком?


# Повторяем публичный ключ

- Как работает разделение секрета по методу Диффи-Хеллмана?
- А можно ничего не брать по модулю?
- Как быстро посчитать  $g^b \pmod{p}$ , если  $b$  большое?



# Что это значит?

 Недоверенное соединение



## Это соединение является недоверенным

Вы попросили Firefox установить защищённое соединение с **intra.grsu.by**, но мы не можем гарантировать, что это соединение является защищённым.

Обычно, когда вы пытаетесь установить защищённое соединение, сайты предъявляют проверенный идентификатор, служащий доказательством того, что вы направляетесь в нужное место. Однако идентификатор этого сайта не может быть проверен.

### Что мне делать?

Если вы обычно без проблем соединяетесь с данным сайтом, эта ошибка может означать, что кто-то пытается подменить этот сайт другим. В этом случае вам не следует продолжать соединение.

Уходим отсюда!

- ▶ **Технические детали**
- ▼ **Я понимаю риск**

Если вы понимаете что происходит, вы можете попросить Firefox начать доверять идентификатору данного сайта. **Даже если вы доверяете этому сайту, эта ошибка может означать, что кто-то вклинивается в ваше соединение с сайтом.**

Не добавляйте исключение, если вы не знаете о веской причине, по которой этот сайт не использует доверенный идентификатор.

Добавить исключение...



# Trusted timestamping

# Как подписать документ текущей датой?

Например, мы хотим уметь доказывать,  
что 2 апреля эта презентация уже существовала

# Протокол

- Алиса хочет переслать Бобу документ с отметкой времени
- Алиса пересылает документ  $T$  в центр подписи
- Центр подписи получает документ  $T$ , смотрит на текущее время  $t$  и зашифровывает пару  $(T, t)$  своим закрытым ключом

# Проблемы протокола

- Алиса вынуждена разглашать документ T центру подписи, а он может быть секретным
- Где гарантия, что Алиса не вступила в сговор с центром подписи? Как центр подписи может доказывать свою безупречную репутацию?
- Предлагайте улучшения к протоколу

Электронный чек

# Зачем нужен электронный чек?

- Обычные платежи: есть банк, который хранит наши деньги. Для каждой транзакции банк знает отправителя и получателя
- Хотим, чтобы Алиса могла передать деньги Бобу, и Боб как получатель не стал известен банку
- Выпишем Бобу анонимный чек, подписанный банком. По этому чеку Боб обналичит деньги
- Чек не должен содержать имени Алисы, но должен содержать подпись банка

# Протокол 1

Alice creates a message  $M = \text{"This is worth \$20, date, time, } S\text{"}$ . Here  $S$  is a long random serial number used to distinguish this bill from others. She creates a random  $r$  with  $\gcd(r, n_B) = 1$ . Alice sends  $M' := Mr^{e_B} \bmod n_B$  to the bank and tells them to deduct \$20 from her account. The bank signs blindly as above and sends Alice  $M'' := (M')^{d_B} \bmod n_B$ . Alice computes  $M''' := M''r^{-1} \equiv M^{d_B} \bmod n_B$ . Alice computes  $(M''')^{e_B} \equiv (M^{d_B})^{e_B} \bmod n_B$  and confirms it equals  $M$ . Alice sends  $M, M'''$  to Carol. Carol computes  $(M''')^{e_B} \bmod n_B$  and confirms it equals  $M$ . Carol reads "This is worth \$20 ...". Carol sends  $M'''$  to the Bank. The bank computes  $(M''')^{e_B} \bmod n_B = M$  and puts \$20 in Carol's account. Only then does Carol give the book to Alice.



# Проблема протокола 1

Problem 1. Alice could create the message  $M$ ="This is worth \$20 ... " and tell the bank to deduct \$5 from her account. Since the bank can not figure out  $M$  during the interaction with Alice, the bank can not detect the cheating.

# Протокол 2

Solution 2 (preferred as it will work well with eventual full solution). Alice blinds 100 different messages  $M_i$  = “This is worth \$20, date, time,  $S_i$ ” for  $i = 1, \dots, 100$ , each with a different  $r_i$  ( $S_i$  is the serial number). The bank randomly picks one of them and signs it and asks Alice to unblind the rest. (In homework, you will determine how to unblind.) The other 99 had better say “This is worth \$20  $\dots$ ,  $S_i$ ”. You can increase the number 100 to make it harder for Alice to cheat.

# Проблема протокола 2

Problem 2. Alice can buy another book from David for \$20 using the same  $M''' = M^{d_B}$  again. The bank will notice that the serial number has been used twice, but not know that it was Alice who cheated. Putting a serial number in  $M$  that is tied to Alice will not help because then Alice loses her anonymity.

# Решение существует

Подробности:

[Edward Schaefer. An introduction to cryptography and cryptanalysis](#)

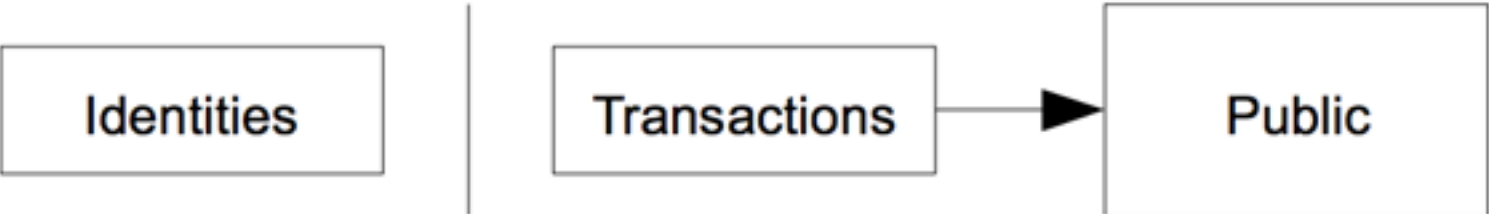
# БИТКОИНЫ

- Хотим децентрализованную платежную систему
- Хотим анонимность всех пользователей
- Хотим хранить историю операций
- Хотим, чтобы поддерживать работоспособность сети было выгодно владельцам серверов

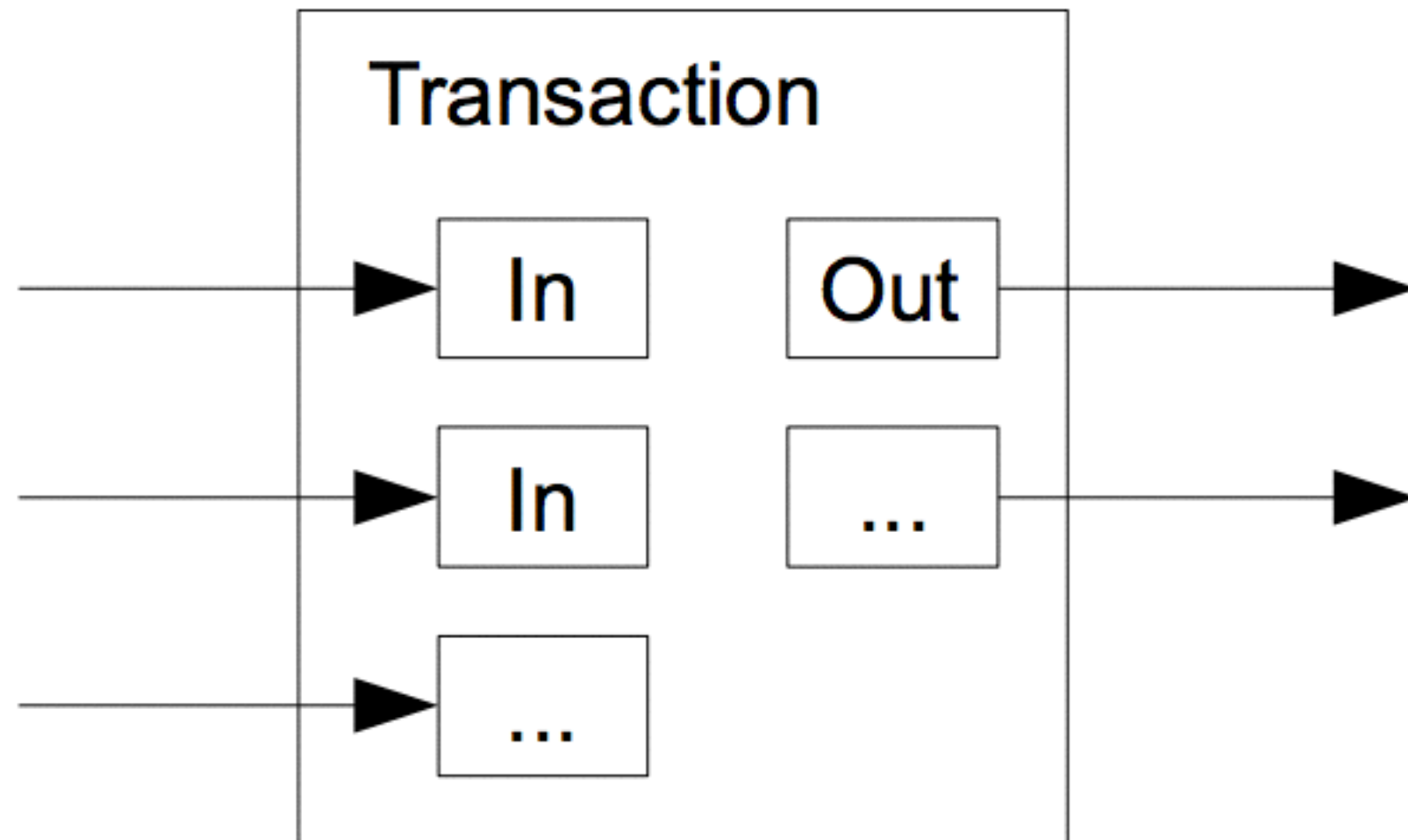
Traditional Privacy Model



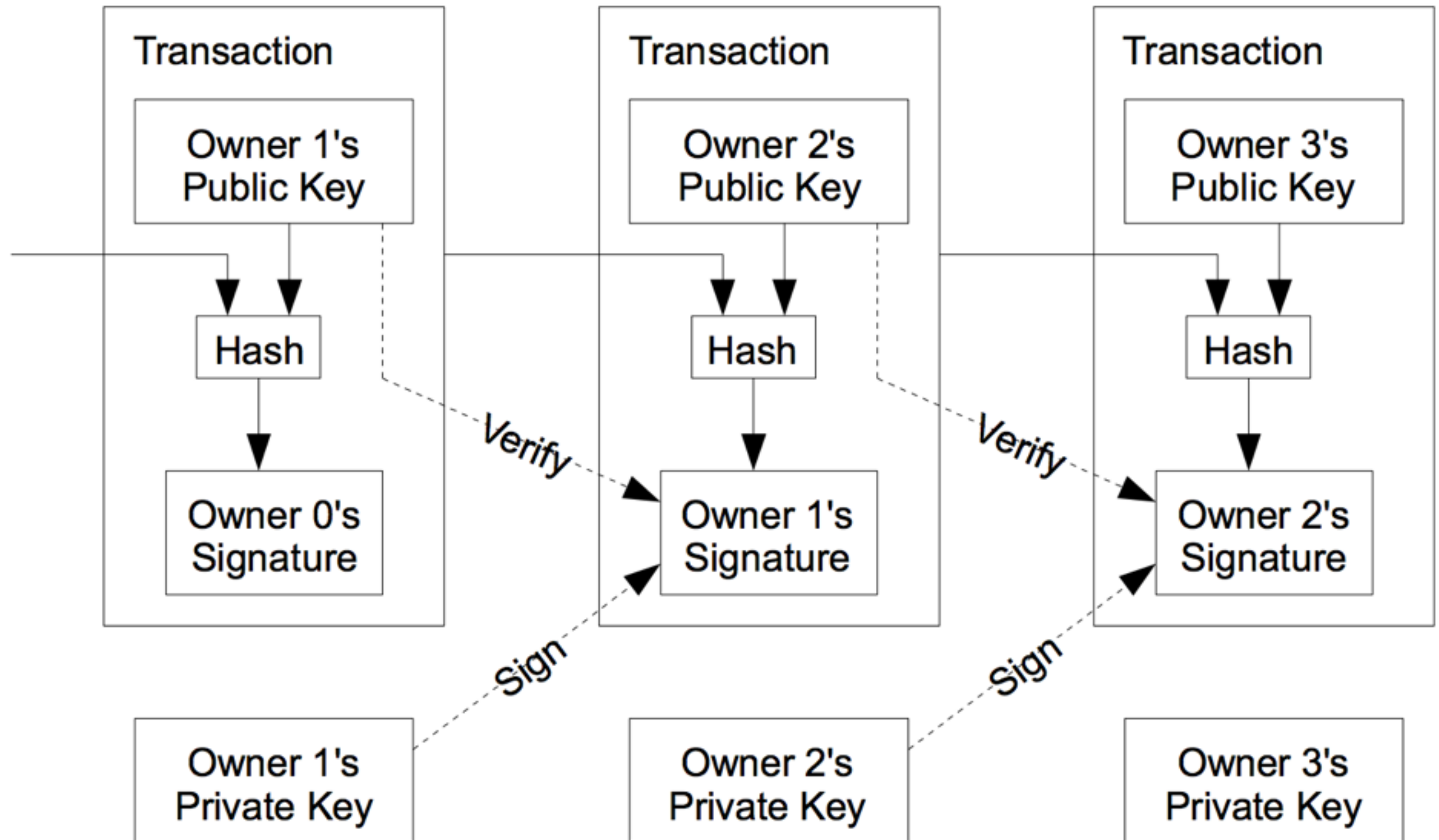
New Privacy Model

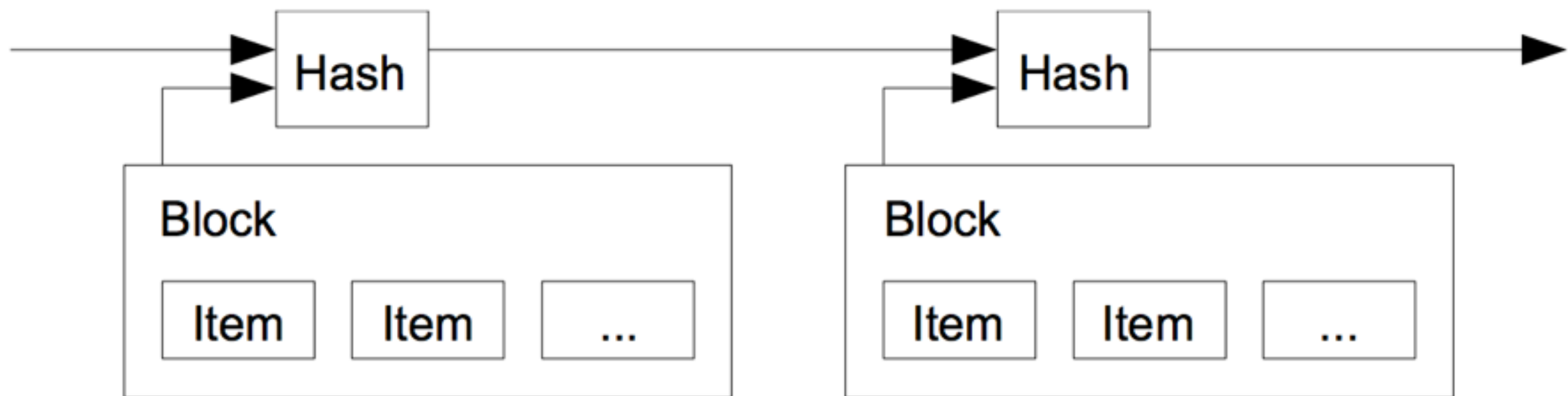


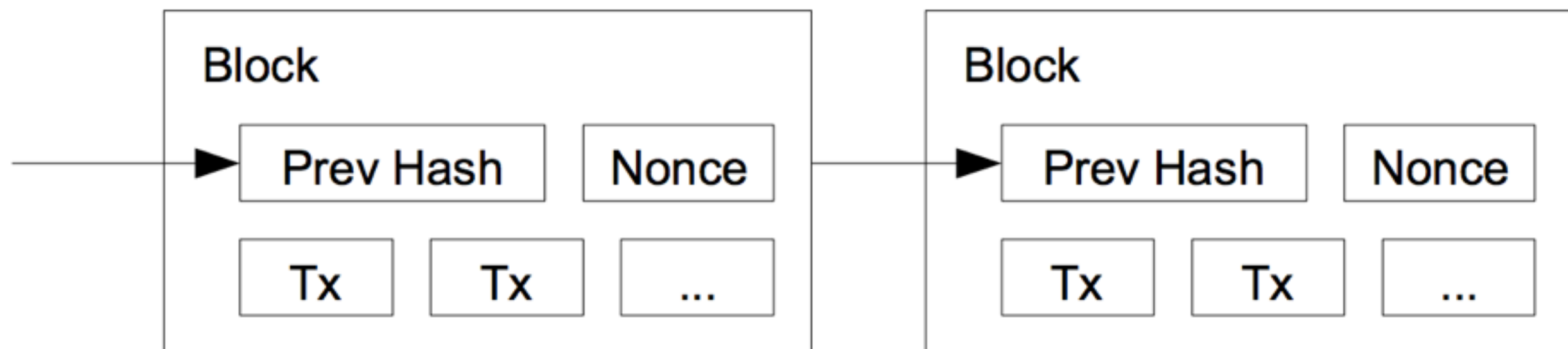




- Что будет кошельком?
- Что будет монетой?







## Latest blocks?

Number?	Hash?	Time?	Transactions?	Total BTC?	Size (kB)?
<a href="#">292464</a>	<a href="#">59705f3d41...</a>	2014-03-25 22:05:47	64	146.24506407	22.226
<a href="#">292463</a>	<a href="#">79c8d11531...</a>	2014-03-25 22:04:37	502	2137.39838491	255.894
<a href="#">292462</a>	<a href="#">85303040fd...</a>	2014-03-25 21:54:36	70	76.23582743	34.721
<a href="#">292461</a>	<a href="#">778983280c...</a>	2014-03-25 21:51:48	116	458.80589651	48.363
<a href="#">292460</a>	<a href="#">1f2a0c4dc9...</a>	2014-03-25 21:51:23	32	144.99830633	14.45
<a href="#">292459</a>	<a href="#">8883f66886...</a>	2014-03-25 21:50:11	113	237.89875672	50.782
<a href="#">292458</a>	<a href="#">5e9c264a1e...</a>	2014-03-25 21:48:15	153	363.23782918	99.156
<a href="#">292457</a>	<a href="#">cf4a37a16e...</a>	2014-03-25 21:46:30	64	641.63862277	19.75
<a href="#">292456</a>	<a href="#">b124aac633...</a>	2014-03-25 21:46:20	739	4912.44256269	349.188
<a href="#">292455</a>	<a href="#">651ba18b29...</a>	2014-03-25 21:32:08	623	2744.03085719	349.23
<a href="#">292454</a>	<a href="#">4fbf3bc2aa...</a>	2014-03-25 21:17:30	472	1044.82570058	258.216
<a href="#">292453</a>	<a href="#">b17c3e348f...</a>	2014-03-25 21:11:58	108	1245.36900078	160.751
<a href="#">292452</a>	<a href="#">b124176e62...</a>	2014-03-25 21:08:15	605	2267.37893542	346.006

# Block 292464?

Short link: <http://blockexplorer.com/b/292464>

Hash?: 00000000000000000059705f3d414037bed010007cbc37469277b51323b3680d4a

Previous block?: [00000000000000000079c8d11531b7f8bbb8edd4f655c46520dedd6b82de884bc9](#)

Time?: 2014-03-25 22:05:47

Difficulty?: 5 006 860 589.2054 ("Bits"?: 1900db99)

Transactions?: 64

Total BTC?: 146.24506407

Size?: 22.226 kilobytes

Merkle root?: c030f134e6564d1d2219366c36bfb6c7ffb4920becc901a264320ef6be6bd48

Nonce?: 3055388252

[Raw block?](#)

## Transactions

Transaction?	Fee?	Size (kB)?	From (amount)?
<a href="#">c47d782749...</a>	0	0.138	Generation: 25 + 0.01940685 total fees
<a href="#">50809938ba...</a>	0.001	0.258	<a href="#">12ksSe8ZgHLhkDguPrR3TQakf4ZsAg2pUu</a> : 25.104:



```
{
  "hash": "0000000000000000059705f3d414037bed010007cbc37469277b51323b3680d4a",
  "ver": 2,
  "prev_block": "0000000000000000079c8d11531b7f8bbb8edd4f655c46520dedd6b82de884bc9",
  "mrkl_root": "c030f134e6564d1d2219366c36bfbb6c7ffb4920becc901a264320ef6be6bd48",
  "time": 1395785147,
  "bits": 419486617,
  "nonce": 3055388252,
  "n_tx": 64,
  "size": 22226,
  "tx": [
    {
      "hash": "c47d78274932e38695bc98498ef230ad158e31a92f96d6c218f053cbf987c0a3",
      "ver": 1,
      "vin_sz": 1,
      "vout_sz": 2,
      "lock_time": 0,
      "size": 138,
      "in": [
        {
          "prev_out": {
            "hash": "0000000000000000000000000000000000000000000000000000000000000000",
            "n": 4294967295
          },
          "coinbase": "03707604065331fdbb03559f140000892b0000"
        }
      ],
      "out": [
        {
          "value": "0.00000001",
          "scriptPubKey": "OP_DUP OP_HASH160 70a419336ae604ddf73e4f8199f1d03b3c2f2601"
        },
        {
          "value": "25.01940684",
          "scriptPubKey": "OP_DUP OP_HASH160 63dd7f90e949f8e354415233e51d3392d4d8f55:"
        }
      ]
    }
  ]
}
```

Домашнее задание

# Электронный журнал на асимметричном шифровании

- Процессор Уязвимов хочет сообщить ученикам оценки за контрольную с помощью протокола Диффи-Хеллмана. Он просит каждого ученика создать 2048-битную пару ключей для Диффи-Хеллмана и послать публичный ключ  $(p, g, g^{**}a)$  в чат класса, а приватный ключ  $a$  сохранить от всех в тайне. Профессор зашифрует оценку  $s$  каждого ученика шифром DES, сгенерировав число  $0 \leq b < p$  и используя в качестве симметричного ключа  $g^{**}(a * b)$ , после чего опубликует таблицу с указанием шифрограммы и  $g^{**}b$  для каждого ученика. Оценки за контрольную - это целые числа от 0 до 100 баллов.
- а) Может ли умный ученик узнать оценки всех одноклассников?
- б) Можно ли немного поменять эту схему, чтобы устранить уязвимость?

Можно ли в качестве коммутативного шифра при игре в покер использовать XOR (одноразовый блокнот)?