Электронные деньги и криптовалюта

https://www.cypherpunks.ru/

Критерии криптографов для идеальной криптовалюты

- **Независимость** от каких-либо физических условий — деньги просто передаются по сетям
- **Безопасность** — нельзя дважды использовать и нельзя подделать
- **Приватность** (анонимность) — связь между пользователем и его покупками не отслеживаема

Критерии криптографов для идеальной криптовалюты

- **Независимость** от каких-либо физических условий — деньги просто передаются по сетям
- **Безопасность** — нельзя дважды использовать и нельзя подделать
- **Приватность** (анонимность) — связь между пользователем и его покупками не отслеживаема
- Возможность отправки (**transferability**) денег другим пользователям
- Возможность дробления (**dividability**)
- Возможность работы в режиме **offline**

Проблемы внедрения

- Специализированные инструменты (отсутствующие в человеках)
- Невозможность цензуры
- Невозможность отслеживания перемещений
- Отмывание денег
- Потеря золотой жилы на комиссиях

Проблемы внедрения

- Специализированные инструменты (отсутствующие в человеках)
- Невозможность цензуры
- Невозможность отслеживания перемещений
- Отмывание денег
- Потеря золотой жилы на комиссиях
- **Иногда** колоссальная сложность систем (вместе с системами голосования это одна из самых сложных в криптографии тем), бывает и ресурсоёмкость (200MiB на транзакцию)

Централизованная криптовалюта

Первый подход к снаряду

- Отправляем файл с суммой денег банку ("$100")
- Банк снимает со счёта сумму и подписывает файл, возвращая нам
- Подписанный файл отсылается продавцу
- Продавец проверяет подпись, пересылает банку файл с просьбой пополнить его счёт
- Банк проверяет подпись, увеличивает сумму на счёте

Централизованная криптовалюта

Первый подход к снаряду

- Отправляем файл с суммой денег банку ("$100")
- Банк снимает со счёта сумму и подписывает файл, возвращая нам
- Подписанный файл отсылается продавцу
- Продавец проверяет подпись, пересылает банку файл с просьбой пополнить его счёт
- Банк проверяет подпись, увеличивает сумму на счёте

Можно накопировать подписанных файлов — double spending

Централизованная криптовалюта

Решаем проблему double spending

- Пользователь добавляет в каждый файл уникальный идентификатор (случайное число)
- Банк при принятии денег сохраняет в базе данных уникальный номер, не давая заново использовать подписанный файл с ним

Централизованная криптовалюта

Решаем проблему double spending

- Пользователь добавляет в каждый файл уникальный идентификатор (случайное число)
- Банк при принятии денег сохраняет в базе данных уникальный номер, не давая заново использовать подписанный файл с ним

Нету анонимности — владелец RN известен

Централизованная криптовалюта

Решаем проблему анонимности (**слепые подписи**)

- Перед отправкой банку чека на сумму, помещаем его в конверт копировальной бумаги. Создаём тысячи их
- Банк просит вскрыть 999 из 1000 конвертов и сравнивает все ли они одинаковы
- Оставшийся один закрытый конверт подписывает (подпись будет и на чеке внутри)
- Вскрываем конверт и подписанный чек отправляем продавцу

Централизованная криптовалюта

Решаем проблему анонимности (**слепые подписи**)

- Перед отправкой банку чека на сумму, помещаем его в конверт копировальной бумаги. Создаём тысячи их
- Банк просит вскрыть 999 из 1000 конвертов и сравнивает все ли они одинаковы
- Оставшийся один закрытый конверт подписывает (подпись будет и на чеке внутри)
- Вскрываем конверт и подписанный чек отправляем продавцу

А кого наказывать за обнаружение double spending?

Централизованная криптовалюта

Пытаемся решить проблему кого наказывать

- При приёме денег от пользователя, продавец просит предоставить идентификатор (случайное число)
- Пользователь подчиняется и идентификатор передаётся вместе с чеком банку
- Банк вместе с RN сохраняет и его
- Если при обнаружении использованного RN будет такой же ID, то обманщик — продавец, пользователь в противном случае

Централизованная криптовалюта

Пытаемся решить проблему кого наказывать

- При приёме денег от пользователя, продавец просит предоставить идентификатор (случайное число)
- Пользователь подчиняется и идентификатор передаётся вместе с чеком банку
- Банк вместе с RN сохраняет и его
- Если при обнаружении использованного RN будет такой же ID, то обманщик — продавец, пользователь в противном случае

Но пользователь анонимен, а так хочется его наказать

Централизованная криптовалюта

Решаем проблему наказания пользователя ⇒ offline

- В чек перед подписыванием добавляются его идентификаторы (N–штук):

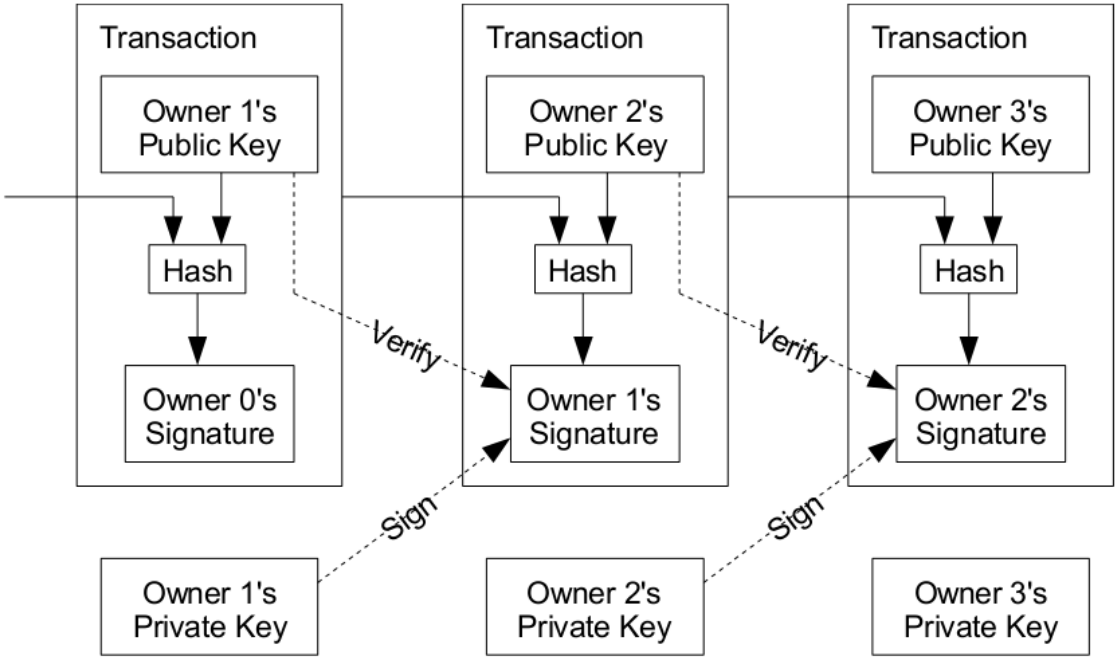
Сумма	
Уникальный ID	
ID_{1L}	ID_{1R}
ID_{2L}	ID_{2R}
...	
ID_{NL}	ID_{NR}

- Разбитые на две части (разделённый секрет (secret splitting))
- Левая и правая часть каждого N зашифрованы (bitcommit–ed)
  - Банк при открытии конвертов просить раскрыть и идентификаторы, убеждаясь что все они равны
  - Продавец при приёме чека просить в каждом идентификаторе раскрыть либо правую, либо левую часть (случайно выбирает N–бит)
  - Отправляет commit ключи банку вместе с чеком

Децентрализованная криптовалюта

Первый подход к снаряду

- Каждый пользователь имеет кошелёк — пара асимметричных публичного и приватного ключа
- Для передачи монеты я (владелец приватного ключа своего кошелька) подписываю ID (хэш) входящей мне монеты (транзакции) и публичный ключ получателя



Bitcoin

Решаем проблему double spending

- Централизованная БД — не вариант

Bitcoin

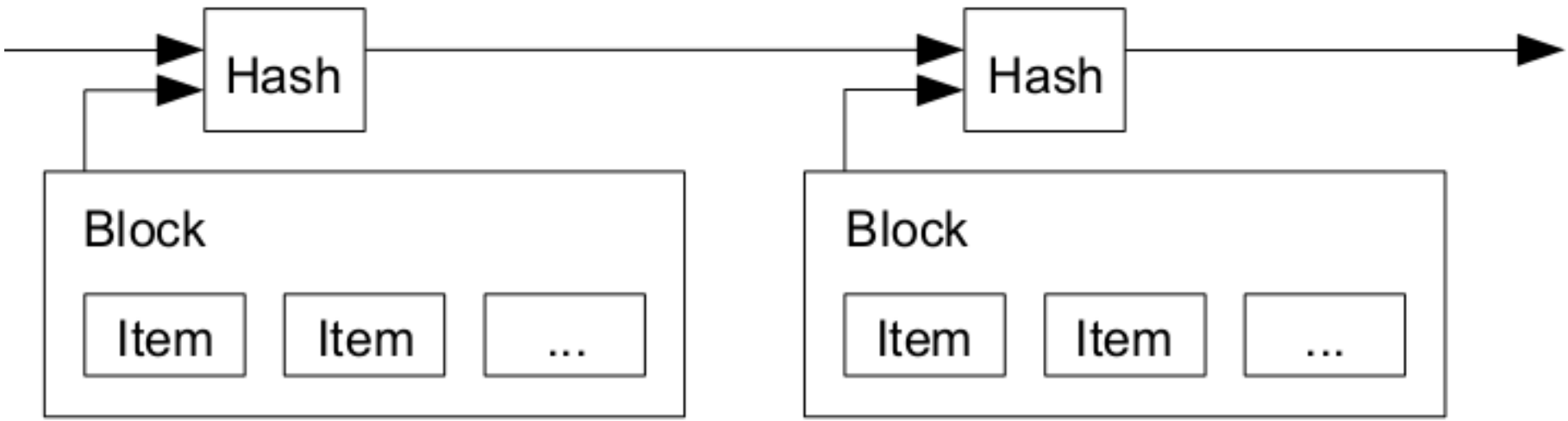
Решаем проблему double spending

- Централизованная БД — не вариант
- Распределённый сервер временных штампов

Bitcoin

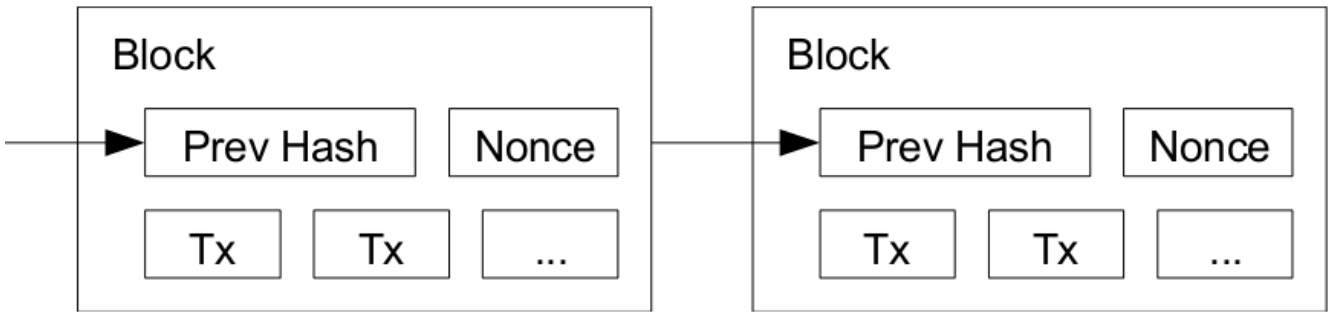
Решаем проблему double spending

- Централизованная БД — не вариант
- Распределённый сервер временных штампов
- Основа которого — proof–of–work



Bitcoin

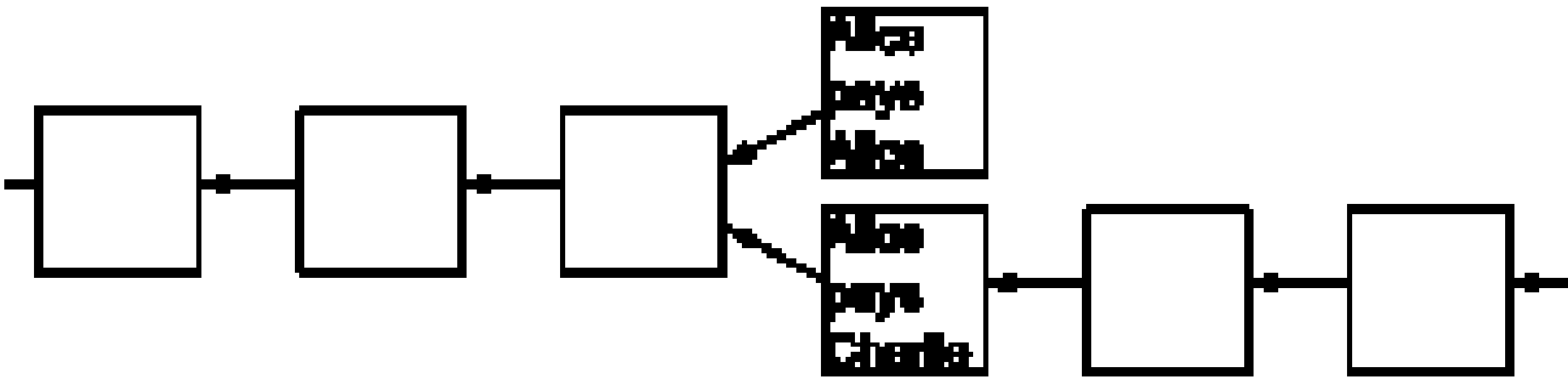
Цепочка блоков



- Первая транзакция блока — поощрение за его расчёт (miner–у), плюс комиссии с транзакций
- Перебираем nonce чтобы получить нужное кол–во нулей в хэше

Bitcoin

Цепочки блоков



- Выбирается самая длинная цепочка

Проблема proof–of–work

- PoW придуман для борьбы со спамом
- Все уяснили что у злоумышленника (спаммера) всегда больше ресурсов
- Спаммер не сможет отправить сообщение — мы не сможем аналогично
- PoW — tradeoff между задержками нашей отправки писем и количеством спама

Проблема proof–of–work

- PoW придуман для борьбы со спамом
- Все уяснили что у злоумышленника (спаммера) всегда больше ресурсов
- Спаммер не сможет отправить сообщение — мы не сможем аналогично
- PoW — tradeoff между задержками нашей отправки писем и количеством спама

Вас устроит **гарантированная** возможность появления нечестной транзакции в $xxxM?

Проблема proof–of–work

Стоимость создания своей цепочки блоков (с блэкджеком . . .)

- Текущая производительность сети — 6000 Thash/sec
- ASIC–система за \$6000 производительностью 2 Thash/sec
- Таких надо $6000/2 = 3000$ штук: \$18M, 2.25 МВт

Bitcoin

Проблемы

- **Внезапно** появилась простая идея
- Гос–ва рекламируют и банки разрешают

Bitcoin

Проблемы

- **Внезапно** появилась простая идея
- Гос–ва рекламируют и банки разрешают
- Анонимность?
- Отсутствие комиссий?
- Нецензурируемая?
- Быстро уходят деньги (подтверждение транзакций)?
- Равноправие и одноранговость?

Bitcoin

Проблемы

- **Внезапно** появилась простая идея
- Гос–ва рекламируют и банки разрешают
- Анонимность?
- Отсутствие комиссий?
- Нецензурируемая?
- Быстро уходят деньги (подтверждение транзакций)?
- Равноправие и одноранговость?

Все остальные похожие криптовалюты (dodgecoin, litecoin, primecoin, yacoin) имеют заменённую SHA256 на scrypt или факторизацию.

Bitcoin

Проблемы

- **Внезапно** появилась простая идея
- Гос–ва рекламируют и банки разрешают
- Анонимность?
- Отсутствие комиссий?
- Нецензурируемая?
- Быстро уходят деньги (подтверждение транзакций)?
- Равноправие и одноранговость?

Все остальные похожие криптовалюты (dodgecoin, litecoin, primecoin, yacoin) имеют заменённую SHA256 на scrypt или факторизацию.

Bitcoin далеко как никто от идеала.

Bitcoin

Проблемы

- **Внезапно** появилась простая идея
- Гос–ва рекламируют и банки разрешают
- Анонимность?
- Отсутствие комиссий?
- Нецензурируемая?
- Быстро уходят деньги (подтверждение транзакций)?
- Равноправие и одноранговость?

Все остальные похожие криптовалюты (dodgecoin, litecoin, primecoin, yacoin) имеют заменённую SHA256 на scrypt или факторизацию.

Bitcoin далеко как никто от идеала. Но она полностью устраивает гос–ва.

Резюме

- Рабочего децентрализованного решения не придумано (возможно задача не разрешима)
- Рабочее анонимное, offline, безопасное решение придумано (почти 30 лет назад уже)
- Гос–ва, банковские системы не дадут прохода и развития подобной криптовалюте
- Всё зависит от людей, которые используя средства коммуникации и криптографии гипотетически могут сделать независимую от давления силовиков экономическую ноосферу

Спасибо за внимание!