

# Виртуальные валюты и электронные деньги

Семинар ГПСЭП

Санкт-Петербург, Российская Федерация

Июнь 2018



GPEN

Global Prosecutors E-Crime Network

# Вступительное слово

- Хайн Дрис
- VIGILO consult
  - Совет Европы
  - Европейская комиссия
  - Академия европейского права
  - Многие регулирующие государственные органы и правительственные учреждения
- Программа
  - Виртуальные валюты (с видео)
  - Задачи следствия и технологии
  - Демонстрация
  - Нормативно-правовые подходы
  - Легализация доходов, полученных преступным путем
  - Денежные потоки и типологии
- Интерактивный блок (пожалуйста, задавайте вопросы. Мы обязательно закончим вовремя).



GPEN

Global Prosecutors E-Crime Network

# Виртуальные валюты и электронные деньги

Вступительное слово



GPEN

Global Prosecutors E-Crime Network

# Что такое валюта?

- Платежное средство
- Два типа:
  - Фиатная валюта
  - Товарная валюта
- Различие: базисный сырьевой товар (обычно: ценный металл)
- Большинство валют на сегодняшний день полностью обмениваемы.
  - Могут обмениваться на другую валюту
  - Обменный курс валюты зависит от торговли на свободном рынке и/или регулятивных норм
  - Централизовано (монополия)



GPEN

Global Prosecutors E-Crime Network

Различные  
типы  
цифровой  
валюты

электронные  
деньги  
vs.  
виртуальная  
валюта

Виртуальная валюта:

- Основные характеристики:
  - Виртуальная (существует в виде компьютерного кода)
  - Представление стоимости (может быть связано с фиатной валютой)
  - Все более взаимобменна (Биткойн – следующий слайд)
  - Но также может представлять ценность в цифровой среде (игры)
- Децентрализованная
  - Центральный орган отсутствует

	Централизованная	Децентрализованная
Виртуальная валюта	eGold Liberty reserve	Биткойн Эфириум
Электронные деньги	Paypal	X



GREN

Global Prosecutors E-Crime Network



# Виртуальные валюты

Order food the easy way

Find restaurants in your area

Address, i.e. Amstelplein 10

SHOW



PayPal



VISA

AMEX



GPEN

Global Prosecutors E-Crime Network

# Биткойн

- Наиболее известная виртуальная валюта
- Впервые разработана Сатоши Накамото (псевдоним)
- Версия 0.1 клиента была выпущена 9 января 2009 года
- Является программным обеспечением (Биткойн клиент) и “системой” (протокол), которая описывает то, как операции в “виртуальной валюте” становятся валидными и регистрируются в децентрализованном журнале.
- Также описывает создание валюты в ходе процесса под названием “майнинг”.



GPEN

Global Prosecutors E-Crime Network

## Биткойн: преимущества

- Большая пользовательская база
- Высокая рыночная стоимость
  - 17 мая: 17М BTC, ≈ \$ 138.000.000.000
- Быстро (по сравнению со SWIFT)
  - Операции подтверждаются в течение 10-20 минут
- Необратим
- Низкие сборы
- Международная
  - <http://coinmap.org>



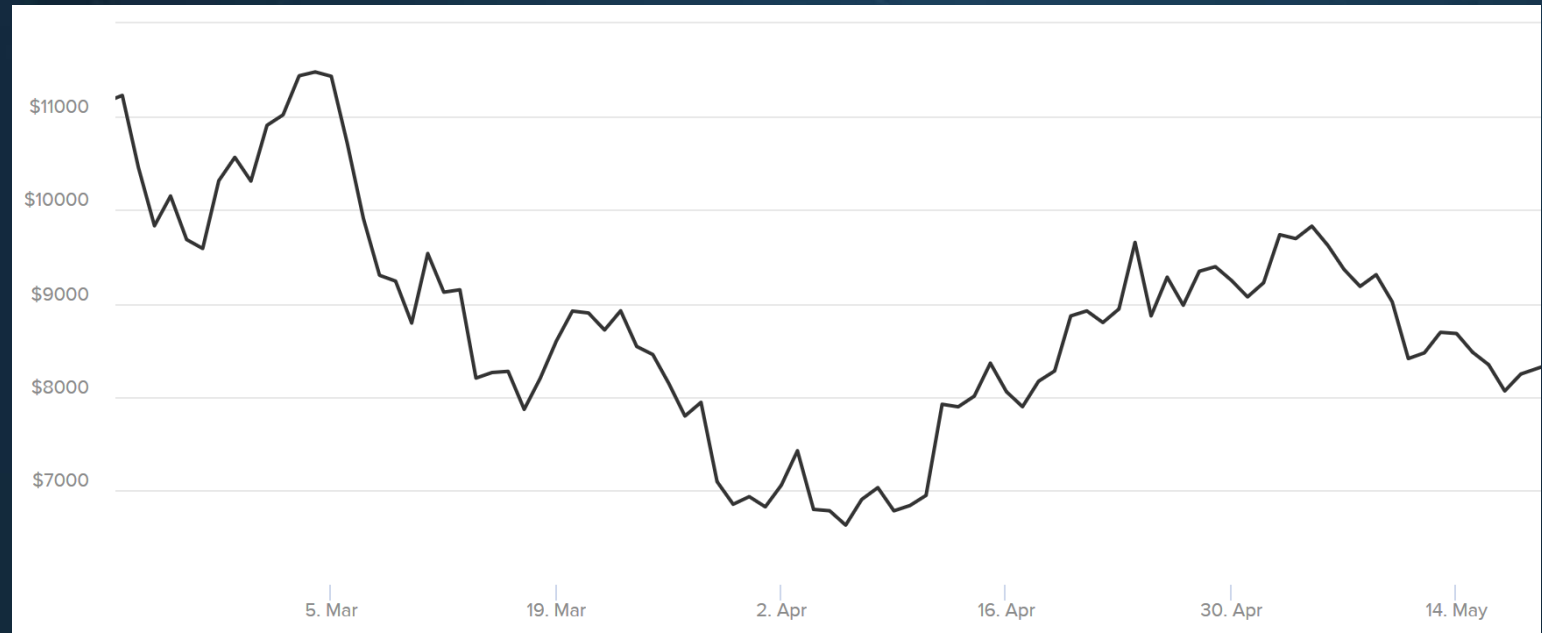
GREN

Global Prosecutors E-Crime Network



# Биткойн: недостатки

- Волатильность
- Без обеспечения государства и правительства
- Быстрая, необратимая (преступное использование!)
- Отсутствие идентификации клиента или центрального органа (преступное использование!)
- Невозможность отчетности о подозрительных операциях и других мер, связанных с БОД (..)
- Невозможность контролировать создание денег



GPEN

Global Prosecutors E-Crime Network

# Технология

- Я хочу показать вам видео, чтобы продемонстрировать, как это работает
- Тем не менее, давайте сперва обсудим два криптографических метода, использующихся в технологии распределенного реестра



GPEN

Global Prosecutors E-Crime Network

# Криптографическая защита с открытым ключом

- Биткойн не анонимен, а скорее имеет псевдоним
- Состоит из децентрализованного реестра учета, реестра операций (технология распределенных реестров биткойна)
- Реестр использует адреса (псевдонимы), которые указывают на контроль за рядом биткойнов
- С этой целью биткойн использует технологию под названием «криптография с открытым ключом»
  - Этот метод позволяет показать, что лицо контролирует ряд виртуальных валют



Биткойн также использует метод под названием хеширование

- Используется, среди прочего, для проверки валидности блоков и цепочек блоков операций, которые составляют распределенный реестр



G PEN

Global Prosecutors E-Crime Network



Bitcoin Address:

1EhX1rhE6AKDTjroWJmGoTS3qb52JVEEEL

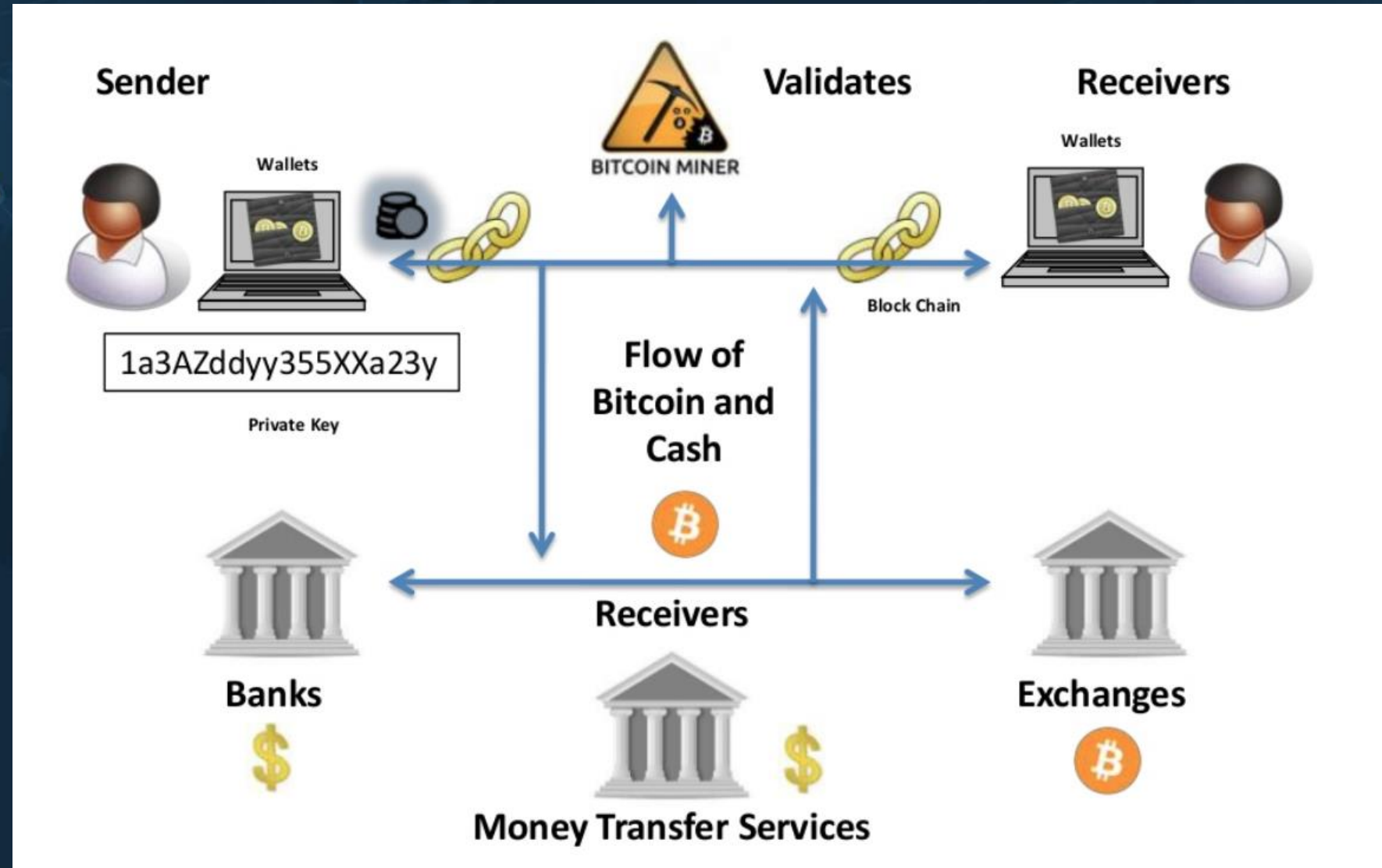
Private Key (Wallet Import Format):

5JEG43vx2dE4EescBfNwPcuFCUFCuk9Th1qZMgZoGLWGknowAAo

2012-09-21 01:22:33.203



# Как это работает?



G PEN

Global Prosecutors E-Crime Network

# Видео

- Как работают криптовалюты?
- <https://www.youtube.com/watch?v=bBC-nXj3Ng4>



GPEN

Global Prosecutors E-Crime Network



# Биткойны:

## Где хранятся?

- Все биткойны хранятся в кошельке
- Кошелек содержит ряд адресов, которые могут получать и тратить отправленные им биткойны



GPEN

Global Prosecutors E-Crime Network

# Кошельки

- Два различных типа кошельков
- Онлайн
  - Хранятся поставщиком услуг
  - Открытые и закрытые ключи хранятся от вашего имени
  - Поставщику услуги необходимо доверить ваши биткойны!
  - Операции авторизуются через поставщика
  - Подумайте: совсем как банк (только это не банк!)
- Пользовательский кошелек
  - Управление ключами и кошельком осуществляется на локальном компьютере
  - Кошелек можно вести онлайн
  - Или даже в автономном режиме (в печатном виде)
  - Операции



GREN

Global Prosecutors E-Crime Network

Онлайн  
кошелек

Обычно:  
Часть обмена

- Обмены предусматривают кошелек
- Предоставляется обмен на фиатные валюты (обычно банковским переводом)
- Возможно предоставление иных сервисов
- Примеры:
  - Coinbase
  - Bitstamp



GPEN

Global Prosecutors E-Crime Network

# Где узлы?

- <http://bitnodes21.co>
- В настоящий момент относительно небольшое количество узлов
  - Потребляет ресурсы
  - Отсутствует вознаграждение
  - Ограниченное количество кошельков



GPEN

Global Prosecutors E-Crime Network

# Масштабирование

- Ограниченное число операций на блок
- Ограниченное число узлов
- Биткойн не может обработать более 10 операций в секунду
- Проблема: не изменить масштаб
  - Микроплатежи
  - Долгое ожидание операции
- Решение:
  - Lightning network
  - Создание каналов между сторонами
  - Средства выделяются заранее в основном распределенном реестре
  - После проведения “всех операций” передается окончательный расчет
  - Это дает возможность проводить больше операций
  - Создается в настоящий момент



GREN

Global Prosecutors E-Crime Network



# Майнинг



G PEN

Global Prosecutors E-Crime Network

## На практике?

- Майнеры получают кратковременный операционный сбор
- Это мотивирует их включать операции в распределенный реестр
- Пул памяти (неподтвержденных) операций обычно хранится 72 часа или (если случится ранее) до достижения объема 300MB
  - Затем операции «умирают»
  - Операции с более низкими сборами «умирают» в первую очередь
  - Следовательно биткойн остается с изначальным адресом (кошельком) и может быть снова потрачен



GPEN

Global Prosecutors E-Crime Network

# Биткойн: демонстрация



GPEN

Global Prosecutors E-Crime Network

# Демонстрация 1

- Заказ продукта



GPEN

Global Prosecutors E-Crime Network



# Демонстрация 2

- Создание нового адреса в клиенте



GPEN

Global Prosecutors E-Crime Network



# Демонстрация 3

- Покупка биткойна
- Легализация при помощи “Tumblr”
- Отправка в другой кошелек



GPEN

Global Prosecutors E-Crime Network

# Миксеры Тумблеры



- Маскировка
- Обнаруживаемость из-за схемы
- Необходимо много данных!



GREN

Global Prosecutors E-Crime Network

# Преступное использование и расследование



GPEN

Global Prosecutors E-Crime Network

# Мошенничество • Мошенничество, основанное на доверии:



G PEN

Global Prosecutors E-Crime Network



## Bitcoin Exchange Hit By Armed Robbers in Thwarted Theft

## MARKETS

PRE-MKT | US | EU | ASIA

# Japanese cryptocurrency exchange loses more than \$500 million to hackers

- Japanese cryptocurrency exchange Coincheck says Friday that around 523 million of the exchange's NEM coins were sent to another account around 3 a.m. local time.
- The stolen coins were worth about 58 billion yen at the time of detection, or roughly \$534.8 million, according to the exchange.
- Coincheck management says it held the NEM coins in a "hot" wallet, referring to a method of storage that is linked to the internet.

Evelyn Cheng | @chengevelyn

Published 12:55 PM ET Fri, 26 Jan 2018 | Updated 12:15 PM ET Mon, 29 Jan 2018



Annaliese Milano

Jan 24, 2018 at 23:00 UTC | Updated Jan 25, 2018 at 17:48 UTC

NEWS

Ottawa police are seeking two suspects after an attempted armed robbery at a cryptocurrency exchange.

Three people entered the offices of Canadian Bitcoins in Ottawa carrying handguns and restrained four employees on Tuesday morning, according to CBC News. At that point, they attempted to compel one of the employees to make an outbound transaction from the exchange. A fifth employee called police before any assets could be taken, police told the news service.

One suspect has been arrested and charged, according to police. The charges include robbery with a firearm and forcible confinement.

The names of the suspects were not released.



## BROWSE CATEGORIES

- Fraud 40
- Drugs & Chemicals 21
- Guides & Tutorials 14
- Counterfeit Items 8
- Digital Products 16
- Jewels & Gold 1
- Weapons 4
- Carded Items 3
- Services 7
- Other Listings 3
- Software & Malware 3
- Security & Hosting

INDY/TECH

# ALPHABAY: DARK WEB DRUGS

# MARKETPLACE MYSTERIOUSLY GOES

# OFFLINE SPAR

# HEIST



ABOUT EUROPOL

ACTIVITIES & SERVICES

CRIME AREAS & TRENDS

PARTNERS & AGREEMENTS

HOME > NEWSROOM > MASSIVE BLOW TO CRIMINAL DARK WEB ACTIVITIES AFTER GLOBALLY COORDINATED OPERATION

# MASSIVE BLOW TO CRIMINAL DARK WEB ACTIVITIES AFTER GLOBALLY COORDINATED OPERATION

20 July 2017

*Press Release*



Takedown of AlphaBay and Hansa will lead to hundreds of new investigations in Europe

Dark Web marketplace exit schemes aren't entirely

HOME SALES MESSAGES ORDERS LISTINGS BALANCE FEEDBACK

Weapons Pistols **Pistols** Glock 17 - General Listing

LISTING OPTIONS

Contact Seller

Favorite Listing

Favorite Seller

Alert when reslock

Report Listing

- BROWSE CATEGORIES
- Fraud 39843
  - Drugs & Chemicals 215372
  - Guides & Tutorials 14077
  - Counterfeit Items 8034
  - Digital Products 10950
  - Jewels & Gold 1630
  - Weapons 3991
  - Carded Items 3544
  - Services 7177
  - Other Listings 3555
  - Software & Malware 3068
  - Security & Hosting 748



**Glock 17** Transferring data from accounts us1.giiva.com

One near new G17 Tested and fully functional. Ask me for a custom listing if you wish to purchase ammunition with this. I'm able to source other pistols, machine pistols, sub-machine guns. just PM me

Sold by Goblinking - 14 sold since Apr 24, 2016 Vendor Level 1 Trust Level 6

Product class	Features	Origin country	Features
Quantity left	Physical package	Ships to	Worldwide
Ends in	Unlimited	Payment	Worldwide
	Never		Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 1,500.00

Qty: 1

1.900 BTC / 70.190 USD

Description Bids Feedback Refund Policy

**Product Description**

One near new G17 Tested and fully functional.


Ask me for a custom listing if you wish to purchase ammunition with this.

I'm able to source other pistols, machine pistols, sub-machine guns. just PM me



# Программа, требующая выкупа

[#] CryptoLocker [#]

Choose a convenient payment method:  
**Bitcoin (most cheap option)**



Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution.



action ID, which

FireEye and Fox-IT have partnered to provide free keys designed to unlock systems infected by [CryptoLocker](#).

Please provide your email address [1] and an encrypted file [2] that has been encrypted by CryptoLocker. This portal will then email you a master decryption key along with a download link to our [recovery program](#) that can be used together with the master decryption key to repair all encrypted files on your system.

**Time left**  
**95 : 23 : 05**

Enter the transaction ID and press «Pay»:

2 BTC

<< Back      PAY



G PEN

Global Prosecutors E-Crime Network

# Получение прибыли?

- Лето 2014: база данных криптографических ключей программы, требующей выкупа (decryptcryptolocker.com)
- 1.3% выплаченного “выкупа”
- Стоимость: минимум \$400 (320 евро)
- $500.000 * 0,013 * 320 \approx 2.1$  миллионов евро (2015 год)
- NotPetya:
  - Операции были видны
  - <https://blockchain.info/address/1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX>
  - 35 тысяч \$



GPEN

Global Prosecutors E-Crime Network

# Виртуальная валюта: аспекты БОД



GPEN

Global Prosecutors E-Crime Network

# Что делать?





# БОД

- Отмывание денег:
- Традиционно относится к сокрытию доходов от преступной деятельности.
- Все в большей степени: также финансирование терроризма.
- Основной компонент: сокрытие источника средств.
- Этапы:
  - Размещение
  - Наслоение
  - Интеграция
- Размещение: размещение “грязной” криптовалюты вместе с “чистой”
- Наслоение: сокрытие источника (tumbler!)
- Интеграция: также предполагает контакт с финансовой системой
- Проблема: биткойн все еще имеет псевдоним...



GPFEN

Global Prosecutors Forum

# Международное законодательство в сфере БОД

- Палермская и Венская конвенции
- Преступление по легализации незаконных денежных средств (отмывание собственных доходов)
- Отмывание денег как часть санкций (и продолжение) основного преступления



GPEN

Global Prosecutors E-Crime Network

# Международные стандарты

- Рекомендация 20 Группы по разработке финансовых мер борьбы с отмыванием денег
- Статья 33 Директивы ЕС **2015/849**

К подозрительным операциям также относятся такие операции, которые на разумных основаниях вызывают подозрения в том, что денежные средства содержат полученные незаконным путем.

Отчет о подозрительной операции:

- Идеально: до выполнения
- Указание в списке или подозрение
- Вопрос: какой уровень анализа?



**GREN**

Global Prosecutors E-Crime Network

Законода  
тельство:  
СДСЕ 185  
СДСЕ 198

- Россия является стороной СДСЕ 198 (Варшавская конвенция)
  - Не входит в СДСЕ 185 (Будапештская конвенция)
  - СДСЕ 198: 34 страны вступили, 8 подписавших стран откладывают ратификацию
- Процессуальное право и положения о следствии
- Криминализация преступлений по отмыванию денег, меры пресечения
- Отсрочка подозрительных операций на территории страны
- Международные запросы об информации по банковским счетам, банковским операциям
- Отслеживание банковских операций
- Организация органов финансовой разведки (ОФР)
- Сотрудничество ОФР
- Комитет Совета Европы по оценке мер противодействия отмыванию денег и финансированию терроризма



GPEN

Global Prosecutors E-Crime Network

# Требования БОД

- Связанные обязательством организации →
- БОД – Требуемые меры (по крайней мере):
  - Идентификация клиента
  - Подход на основе оценки риска: надлежащая проверка клиента/ усиленная проверка клиента
  - Отчет о подозрительных операциях
  - Часто: обязательная или минимальная группа показателей
  - Порог отчетности (наличные средства > 10.000 евро)
  - Отчет о подозрительных операциях
    - Отмывание денег
    - Доходы от преступной деятельности(!)



GPEN

Global Prosecutors E-Crime Network



# Расширенная конфискация

- Обычно для блокировки, изъятия или конфискации денежных средств необходимо доказательство основного преступления, в результате которого были получены денежные средства
- Во многих случаях в кошельке находится больше средств, чем та часть, чье прямое отношение к преступлению доказано.
- В этом случае иногда происходит перенос бремени доказывания
- Это значит, что законность другой части, сопряженного дохода должна быть доказана, иначе она может быть также заблокирована, изъята или конфискована



GREN

Global Prosecutors E-Crime Network

# Признаки

- Как банки могут обнаружить операции с виртуальной валютой
- В общем:
  - Легко обнаружить при надлежащей проверке клиентов
  - Надлежащая проверка клиентов: обычно легче обнаружить обмены и поставщиков кошельков
  - Сложнее обнаружить частные лица, которые заняты бизнесом, связанным с виртуальной валютой
- Традиционные признаки – все еще хорошее начало расследования
  - Общий оборот счета
  - Подозрения банковских служащих
  - Схемы операций
- Более передовые способы обнаружения:
  - Упоминание адреса биткойна в операции
  - Использование методов анонимизации в сети (Идентификация клиента/Надлежащая проверка клиентов)
  - Текущие выплаты отслеживают стоимость биткойна/другой виртуальной валюты



GPEU

Global Prosecutors' E-Unit

## Типичные признаки в существующих случаях

- Операции относятся к покупке или продаже виртуальной валюты (например, Биткойны, Litecoin, Эфириум, Zcash).
- Биткойн упоминается в переводах Western Union
- Наличие адресов биткойна в сведениях об операции
- Упоминание обменов, известных счетов для обмена и поставщика кошелька
- В реальности также:
  - Посредники (схемы операции, страны, САТО)
  - Большая сумма наличных средств
  - Операция касается перевода выигрыша с онлайн платформы для азартных игр
  - Клиент запрашивает срочное выполнение операции или конфиденциальный статус операции.



GREN

Global Prosecutors E-Crime Network

# Виртуальная валюта: регулирование



GPEN

Global Prosecutors E-Crime Network

# Виртуальные валюты?

- Рассматриваются как имеющие высокий риск
- Волатильность
- Не является системной угрозой (пока)
- Вопрос: что можно урегулировать?
  
- Важное различие:
  - Локальный кошелек
  - vs:
  - Обмены и
  - Онлайн поставщики кошельков

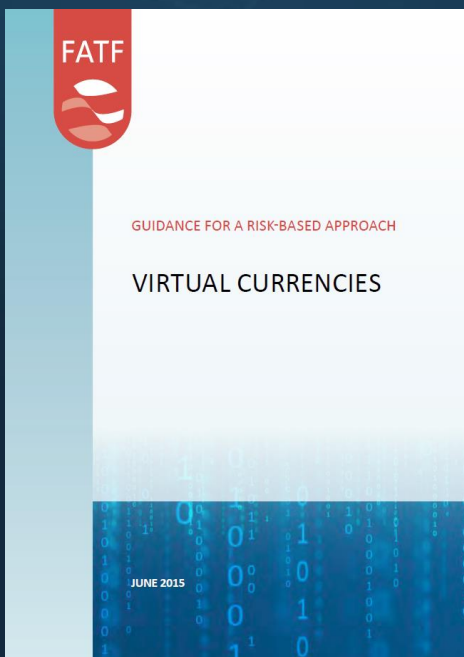


GPEN

Global Prosecutors E-Crime Network



# Руководство FATF Основанный на риске подход



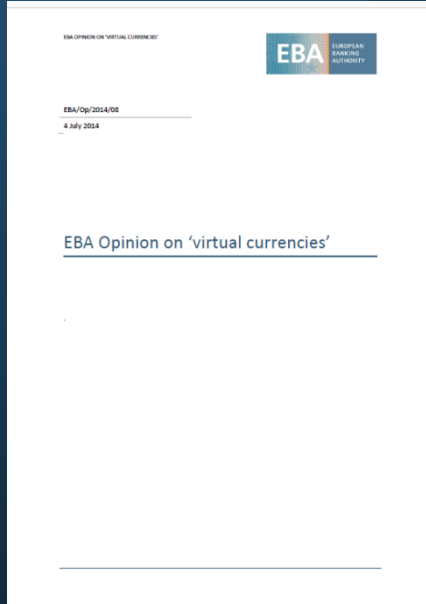
- Общий язык/определения
  - Криптовалюта
  - Типы, отличия
- Очевидные риски:
  - Относительно анонимный
  - Отсутствует надзор, нет центрального органа
  - Быстрые изменения
  - Международный, межюрисдикционный характер
- Анализ примеров:
  - Liberty reserve
  - Silk Road (торговая площадка Даркнет в tumbler)
  - Western Express



GPEEN

Global Prosecutors E-Crime Network

# ЕС мнение ЕБА



- Расширенный анализ рисков (аббревиатура)
  - Риски для пользователей
    - Например, проникновение в кошелек или к поставщику кошелька
    - Потеря ключей или документов
    - Инвестиционные риски
  - Участники рынка, не являющиеся пользователями
    - Продавцы
    - Поставщики кошельков
  - Риски для финансовой безупречности
    - ПОД/ФТ
    - Финансовая преступность
  - Риски для платежной системы ФВ
  - Риски для регулирующих органов



GPEN

Global Prosecutors E-Crime Network

ЕС:  
4<sup>ая</sup> Директива  
БОД

(Поправка по  
ВВ)

- Закон ЕС 2015 года
  - Реестр бенефициарной собственности
- Поправка внесена в 2017 году:
  - Обмены: введена по требованиям БОД (включая идентификацию клиента и отчет о подозрительной операции)
  - Необходимо пороговое значения для отчета
  - Отчет о подозрительной операции
  - Идентификация клиента



GPEN

Global Prosecutors E-Crime Network

# Состояние Первичный выпуск монет

дел:

- Инвесторы получают криптовалюту взамен инвестиций в ФВ или свободно обмениваемой ВВ (эфириум, биткойн)

Проверка ценных бумаг в ВВ

- Инвестиции используются для финансирования разработки проекта и для вознаграждения инвесторов, так как выдаваемые цифровые денежные знаки (криптовалюта) приносит прибыль в случае успешности проекта.
- На практике это создает систему, подобную ценным бумагам.

Первичный выпуск монет

ЕС:

- Мнение Европейского управления по надзору за рынком ценных бумаг: ПВМ могут являться ценными бумагами, что ведет к применению строгих требований по ценным бумагам (часто: лицензирование, идентификация клиента)
- Комиссия по ценным бумагам и биржам: обращение с ПВМ как с ценными бумагами

ПВМ

GPEN

Global Prosecutors E-Crime Network

- Великобритания – Инспекция по контролю за деятельностью финансовых организаций: Очень свободная позиция по ПВМ, только вынесли предупреждение; рассматривается вариант «регулятивной песочницы»

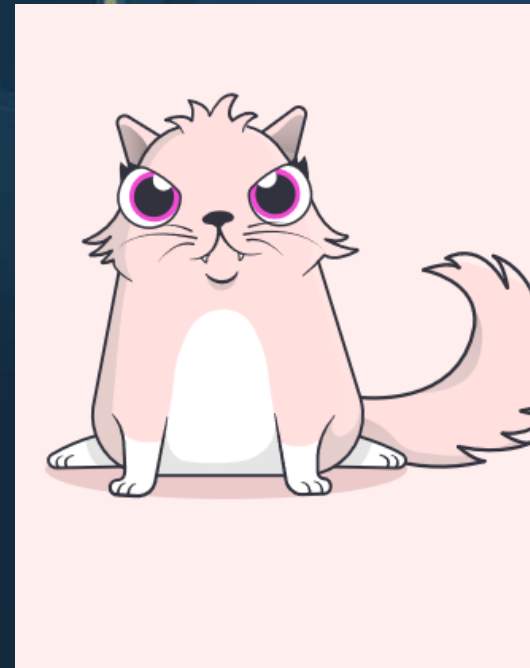
- Германия: вновь подтверждает, что ПВМ закономерно, но согласно Закону о ценных бумагах может являться ценной бумагой



# Потребительский риск при ПВМ

## Преимущества:

- Нет проспекта
- Нет условий лицензирования, ограничивающих инвестиционные риски
- Высокий риск мошенничества
- Стоимостные риски и риски колебаний
- Но некоторые проекты могут быть очень прибыльными:



G PEN

Global Prosecutors E-Crime Network



# Сложные следственные задачи



GPEN

Global Prosecutors E-Crime Network

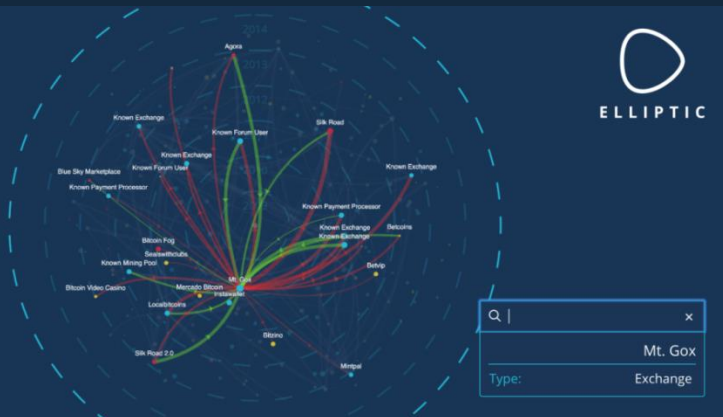
# Расследование биткойнов

- Blockchain.info

- Распределенный реестр может просматриваться несколькими обозревателями
  - Blockchain.info
- Это помогает при наличии данных об интересующих адресах криптовалют или данных о соответствующих операциях
- Существует несколько инструментов для проведения расследования
  - Chainalysis
  - Elliptic

• Эти сервисы собирают данные и хранят соответствующие адреса криптовалют в базе данных. Данные могут использоваться для создания графиков и отслеживания использования биткойнов в кошельке/с адреса.

THE BITCOIN  
BIG BANG



ELLIPTIC



## Несколько аспектов

- Узнать об основных обменах и поставщиках платежных услуг легко
- Узнать об индивидуальных пользователях сложно
- Исключение: когда есть привязка к сайту с идентификацией клиента
- Или при доставке/ином связанном фактическом адресе или личности
- Обмены: операция также может быть привязана к банковскому счету или кредитной карте с требованиями об идентификации личности



GPEN

Global Prosecutors E-Crime Network

# Полезная информация

- Google (или Yandex) вам в помощь
- Используйте обозреватель blockchain
  - Изучите данные (коммерческая услуга или самостоятельно)
- Используйте [wallethexplorer.com](http://wallethexplorer.com)
  - Используйте различные методы идентификации других адресов в кошельке
  - В основном идентифицирует более крупные услуги
- Учтите, что на всех адресах, с которых проводится операция полностью расходуются все средства, хотя входной адрес также может быть и выходящим (так происходит возврат части средств обратно владельцу).
- Обычно для операций со “сдачей” (с возвратом средств) используются новые адреса.



GREN

Global Prosecutors E-Crime Network

# Изменение адресов

- Может быть обнаружено
- И связано с кошельком (одним человеком)
- Используя:
  - Анализ операций

- Схемы
- Люди как округленные числа (0.01 и 0.47998899 биткойнов)?
- <https://blockchain.info/tree/148088608>



GREN

Global Prosecutors E-Crime Network



# Личная информация?

- IP адреса?

- IP адрес узла/клиента, который изначально осуществляет передачу операции известен по ряду узлов.
- Биткойн обезличивает эти данные, так как является одноранговой сетью.



G PEN

Global Prosecutors E-Crime Network



# Личная информация 2

- Существуют несколько ВВ, верификацию которых можно провести без адреса в распределенном реестре.
  - Zk-SNARK
  - Сложно объяснить, но используется математический алгоритм для предоставления доказательства с нулевым разглашением (для верификации в распределенном реестре не должно быть сведений об операции)
- Обеспечивает анонимную верификацию операции
  - Zcash (использует zk-Snarks)
  - Другой вариант: Monero (использует передовое наложение и маскировку)



GPEN

Global Prosecutors E-Crime Network

# Изъятие биткойнов

- Что искать:
  - Кошелек на подозреваемом компьютере
    - Wallet.dat
    - Программное обеспечение
  - Веб-браузер: доступ к платформам по обмену и торговле биткойнами
  - Доступ к Dark web?
  - Бумажные копии!
  - Электронные копии!
  - Ключи восстановления!
- Что делать?
  - Как можно скорее удостоверьтесь, что вы управляете биткойном
  - Это можно осуществлять при переводе только на собственный (государственный) кошелек

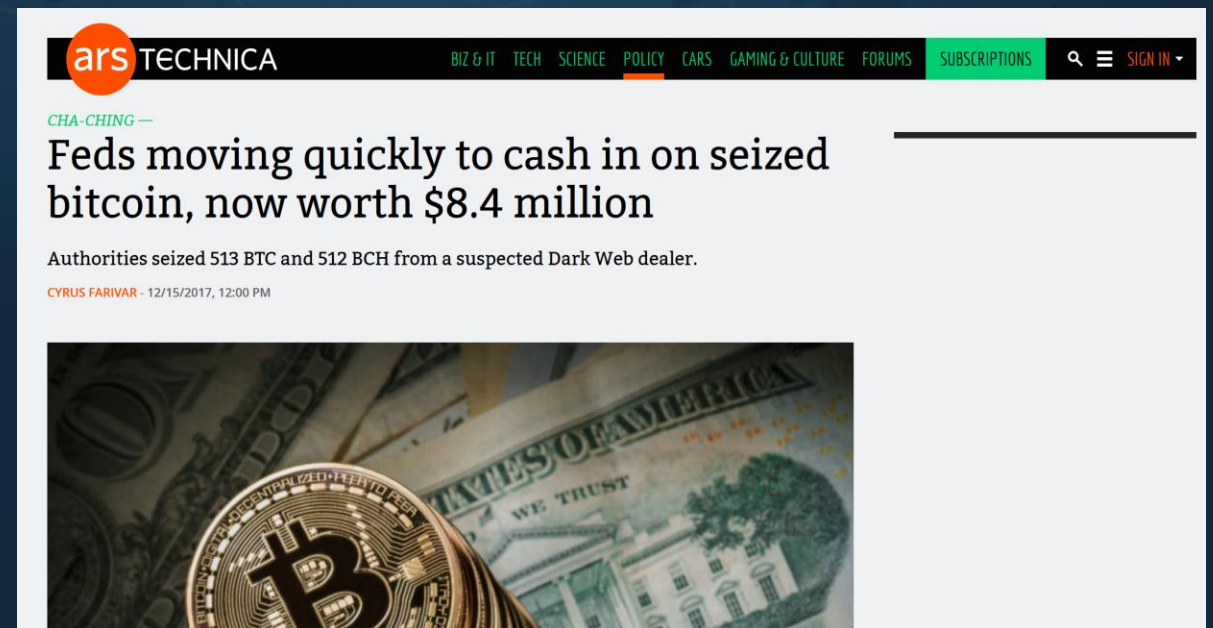


GREN

Global Prosecutors E-Crime Network

# Управление активами

- Две возможности:
  - Хранить в биткойне, возвращать в биткойне
    - Риск: стоимость фиатной валюты
    - Биткойн может упасть?
    - Риск судебного разбирательства!
  - Продавать биткойн, сохранять стоимость в фиатной валюте
    - Риск устранения подозреваемого финансового интереса
- Большое количество биткойнов (или особенно другой ВВ): продавайте с осторожностью.



The screenshot shows a news article from the website 'ars TECHNICA'. The navigation bar includes categories like 'BIZ & IT', 'TECH', 'SCIENCE', 'POLICY', 'CARS', 'GAMING & CULTURE', 'FORUMS', and 'SUBSCRIPTIONS'. The article title is 'Feds moving quickly to cash in on seized bitcoin, now worth \$8.4 million'. The sub-headline reads 'Authorities seized 513 BTC and 512 BCH from a suspected Dark Web dealer.' The author is 'CYRUS FARIVAR' and the date is '12/15/2017, 12:00 PM'. The image at the bottom of the article depicts a stack of gold Bitcoin coins in the foreground, with US dollar bills and the White House in the background.



G PEN

Global Prosecutors E-Crime Network

# Многочисленные входные операции

- Много входных:

A (0.45)

B (0.2)

C (0.1)

D (0.75)

# Мало выходных:

Y (1.2)

Z (0.3)

- Что вероятно в данном случае?
  - Маскировка?
  - Или обычная операция?
    - На какой адрес отправляется «сдача»?
- Что мы еще узнали?



GPEN

Global Prosecutors E-Crime Network



# БОД и киберпреступность

Некоторые случаи



GPEN

Global Prosecutors E-Crime Network

# БОД и киберпреступ ность

- Международная группа по борьбе с финансовыми злоупотреблениями
- MONEYVAL Комитет Совета Европы по оценке мер по БОД/ФТ
- Директивы ЕС
- ООН (Санкционный перечень, Резолюция СБ ООН 2253/2015)
- США (Управление по контролю за иностранными активами)
- Международная организация органов финансовой разведки «Эгмонт»
- Кэмденская межведомственная сеть по возвращению активов КАРИН
- Многие другие



GPEN

Global Prosecutors E-Crime Network

# Примеры

- Пример 1: Использование услуги по переводу биткойнов
- Гражданин страны получил денежные средства по переводу.
- Сумма, хотя и значительная, не превышает порога отчетности (12 тысяч € vs 15 тысяч €)
- Средства получены из разных стран (например, Италия, Великобритания, Мальта...).
- При изъятии клиент указал, что он использует средства для покупки биткойнов для друга.
- Такой случай встречается не часто – пока.



GPEN

Global Prosecutors E-Crime Network

# Примеры

- Мошенничество с использованием банковских карт
- Карты (или данные карты, так называемые данные БИН) приобретаются в других странах.
- Часто денежные средства легализованы и тщательно рассмотрены в стране.
- Также может использоваться копирование данных карты с помощью банкоматов.
- Копирование данных карты часто связывают с румынскими и болгарскими преступными группами.
- Однажды лицо использовало украденную карту для азартных игр и успешно потратить более 1 миллиона евро до того, как это было обнаружено.



GPEN

Global Prosecutors E-Crime Network

## Примеры

(Пример страны, не входящей в ЕС)

- Отчет о подозрительных операциях (ОПО), связанных с киберпреступностью в стране, был подан местным банком в 2012 году:
- Этот случай относится к иностранному (региональному) преступнику, который предположительно присвоил денежные средства физического лица в Великобритании и который при помощи местных преступников перевел €170,000 из Великобритании в банк своей страны.
- Местные граждане, действующие в качестве посредников (безработные), сняли в банках наличные денежные средства.
- В результате ОПО Управление финансовой разведки отложило вторую операцию и сообщило о произошедшем в полицию и прокуратуру.
- Вследствие такого вмешательства вторая часть средств была возвращена в Великобританию.



GPEN

Global Prosecutors E-Crime Network



# Отмывание средств с помощью биткойнов (Нидерланды)

- Операция NOCIS
- С 2013 года 3 мужчин покупали биткойны и меняли их на наличные.
- Также оказалось, что главный подозреваемый выращивал коноплю
- 3 граждан Голландии были осуждены за легализацию средств, полученных незаконным путем
  - Денежные средства размером 10 миллионов евро
- Предлагается в качестве услуги
  - Как таковая не является незаконной
  - Но отмывание средств подразумевало значительный риск
    - Отсутствие идентификации клиента
    - Гарантированная анонимность
    - Необычайно высокая плата
- В общем радуется, что они по крайней мере сознательно взяли на себя высокий риск по отмыванию незаконных средств.



GPEN

Global Prosecutors E-Crime Network

# Денежный поезд (Нидерланды)

- Случай одного человека с отмыванием NOCIS/Bitcoin
- Менял биткойны на евро (наличные)
- Биткойн обменивался на фиатную валюту в Кипрской компании в Латвии и возвращался обратно на банковские счета в Нидерланды
- Высокие комиссии по операциям за обмен биткойнов
- Первое подозрение было связано с ограблением на отдаленной железнодорожной станции
- В ходе дальнейшего расследования выяснился полный масштаб операции



GPEN

Global Prosecutors E-Crime Network

# Обзор



GPEN

Global Prosecutors E-Crime Network

# Использование ВВ?

- Вероятно возрастет
  - Законное использование
  - При возрастании законного использования: незаконное использование
- Альтернативные криптовалюты
  - Все больше используются
  - Усиление защиты личных данных/вероятно усиление маскировки
  - Напряжение в сфере защиты личной информации (Общие положения о защите данных)



GPEN

Global Prosecutors E-Crime Network

# Стратегии уголовного преследования

- Увеличенное использование расширенной конфискации
- Более совершенное использование данных и технологий
- Более высокая специализация в возврате активов и финансовых расследованиях (в сфере киберпреступности)
- Усовершенствованные призаки



GPEN

Global Prosecutors E-Crime Network



# Возможности

- Необходимость в больших возможностях в целом
- Понимание ВВ и отслеживание (в органах финансовой разведки и судебной системе по части киберпреступности)
- Более совершенные методы работы в криминалистике
  - Кошельки часто пропадают
  - Не часть поисков или методов работы
- Сотрудничество с поставщиками онлайн-кошельков.



GPEN

Global Prosecutors E-Crime Network

- # Урегулирование
- Усиленное урегулирование, предполагающее регламентирующий договор между поставщиком ВВ <-> Международной банковской системой
  - Применение традиционных требований по финансовой отчетности к поставщикам ВВ
  - ПВМ: все больше урегулирования
    - Рынок с высоким уровнем риска
    - Риск мошенничества
    - Мошенничество, основанное на доверии vs. “драгоценности”
    - Защита потребителя?



GPEN

Global Prosecutors E-Crime Network

# Признаки

## Общие:

- Азартные онлайн игры
- Клиент просит о конфиденциальности

## Признаки, связанные с банковскими счетами:

- Клиент получает платеж через PayPal без данных об отправителе или цели операции.
- Клиент отправляет запрос на платеж поздно в пятницу во второй половине дня на перевод заказчику в страны, в часовом поясе которых остается еще несколько часов предоставления банковских услуг.



GPEN

Global Prosecutors E-Crime Network

# Признаки

- Клиент осуществляет изъятие средств, полученных из иностранной юрисдикции, перевод которых был сделан незадолго до завершения рабочего дня в иностранной юрисдикции, и изъятие осуществляется после завершения работы, в особенности после завершения рабочего дня в пятницу в иностранной юрисдикции.
- Обнаруживаются значительные языковые ошибки или необычное содержание в ходе связи по факсу и электронной почте между банком и клиентом или в документах, представляемых клиентом в банк.
- При формировании платежного поручения в адрес получателя клиент связывается с ним только по электронной почте.
- Возврат денежных средств за товары/услуги осуществляется на кредитную карт, отличную от той, что использовалась изначально при покупке.



GREN

Global Prosecutors E-Crime Network

# Признаки

Признаки, относящиеся к корпоративным и коммерческим операциям:

- Корпоративный клиент с установившимися отношениями меняет получателя/реквизиты счета (например IBAN) на известного получателя.
- Корпоративный клиент с установившимися отношениями запрашивает платеж в адрес подозрительного нового получателя.
- Инструкции по оплате получает новый сотрудник корпоративного клиента.



GPEN

Global Prosecutors E-Crime Network



# Признаки

## Географический риск

- Операция связана со страной, известной ассоциацией с онлайн мошенничеством или подобной преступной деятельностью в киберпространстве (со стороны жертвы, подозреваемого или посредника).



GPEN

Global Prosecutors E-Crime Network

Вопросы?



GPEN

Global Prosecutors E-Crime Network

# Вопросы

- Хайн Дрис
- VIGILO consult
- [hein@vigilo.nl](mailto:hein@vigilo.nl)
- +31717113243



GPEN

Global Prosecutors E-Crime Network