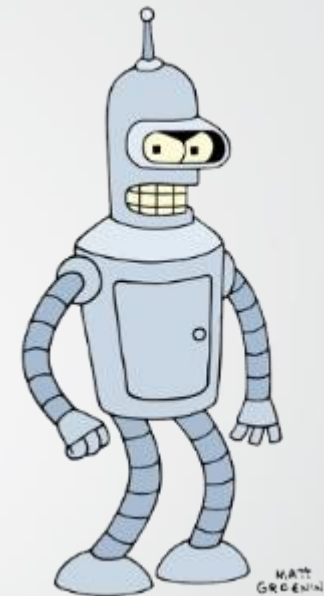


«Крипторазметка. Отслеживание виртуальных активов»

ПАВЕЛ НИКОЛАЕВИЧ БИРЮКОВ

Доктор юридических наук, профессор,
заведующий кафедрой международного и евразийского
права Воронежского государственного университета

E-mail: birukovpn@yandex.ru



Майнить надо, пока
молодой. Потом поздно
будет

Что значит не
хочешь
биткоины?
Биткоины все
хотят, не
выдумывай

А ты почему не майнишь?
Часики-то тикают

Майнить - это счастье. Дал бог интернет,
даст и видеокарту

«Главное – определиться с понятийно-
категориальным аппаратом». © П.Н. Бирюков

Три положения.

1. ***В число виртуальных активов (далее ВА) не входят цифровые валюты - фиатные деньги в электронной форме (цифровые рубли, юани, рупии).***

2. ***Криптовалюты и другие ВА не являются фиатными деньгами, а считаются в РФ ИМУЩЕСТВОМ. Сами ВА и операции с ними можно отследить и проверить.***

3. ***«Криптовалютная разметка» - это процесс отслеживания и анализа перемещения ВА в блокчейне. Участники сети могут просматривать и проверять транзакции, узнавать, куда откуда им были перечислены ВА, как они были использованы.***

Для начала. Различают *три вида ВА*:

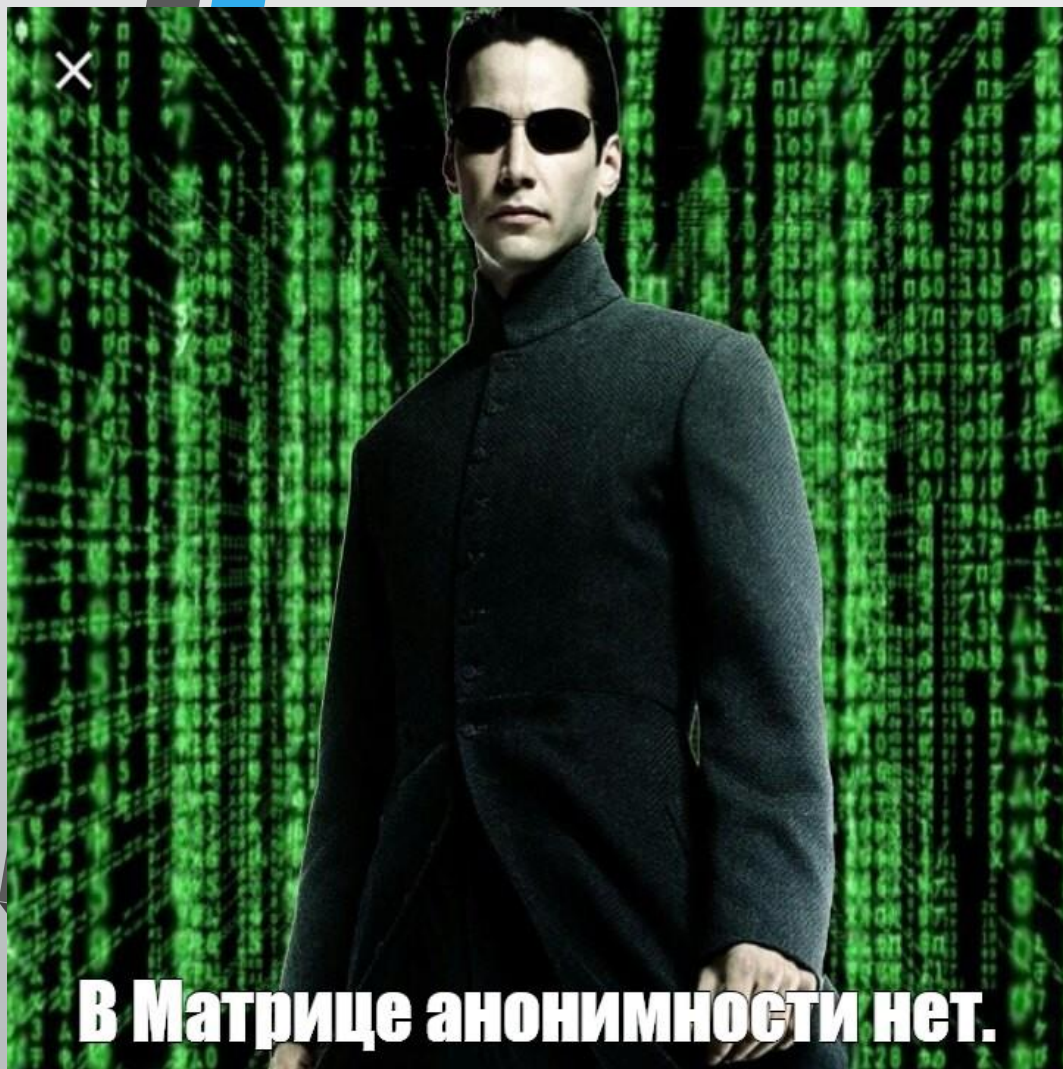
1) необеспеченные – классические «криптовалюты» (биткойн, альткойны). За ними ничего нет, кроме веры пользователей в их ценность. Их цена волатильна (прыгает как кенгуру) и зависит лишь от спроса на них. Таких ВА несколько тысяч;

2) обеспеченные – «стейблкойны» (Digix Gold, TrueUSD, USDT и др.). В их основании лежит имущество (золото, нефть, фиатные деньги и т.п.). Точное количество неизвестно, почти все они выпущены за рубежом (в РФ их выпускают пока всего 12 компаний);





3) **токенизированные активы** (далее ТА). Эмитент создает на площадке блокчейна, который это позволяет, новый смарт-контракт. Он рассчитан на электронный реестр пользователей данного проекта. Инициатор проекта эмитирует определённое число токенов, создает записи о праве владения в реестрах и выставляет объекты на торги. При совершении сделки в реестре меняются сведения о собственнике ТА.



Сейчас злодеи часто используют ВА (особенно криптовалюты) в целях коррупции, торговли наркотиками, отмывания денег, финансирования терроризма и т.д. **Перемещения ВА оставляет свои цифровые следы, которые можно обнаружить и идентифицировать.**

В отношении каждого вида ВА применяются свои правила «крипторазметки». Поговорим о необеспеченных ВА – т.е. криптовалютах (далее КВ, крипта).

– Сообщите свои данные...



Сама структура блокчейна позволяет отслеживать перемещения монет (токенов); это заложено в принципах ее функционирования. Отслеживание ВА, необходима прежде всего, государству для контроля за всеми участниками процесса и за ситуацией в целом.

Специальные компании во многих странах занимаются изучением путей движения криптовалют, выявление адресов (криптокошельков) и их анализом. Они позиционируются как коммерческие структуры, однако в реальности они действуют в интересах госорганов.



Указанные структуры собирают инфу о принадлежности адресов конкретным сайтам или лицам. Накопив достаточный объем данных, программы начинают «размечать» адреса криптовалют. Они относят их к конкретным биржам, обменным сервисам, криптофондам, либо связанные с криминалом.

Выявив несколько адресов, принадлежащих какой-либо структуре, программы узнают о целой группе адресов (криптокошельков), используемых данным сервисом, «размечают» их.



- Это же элементарно, Ватсон!

«Крипторазметка» видит сервисы по обмену крипты, майнер-пулы, «мостами», «криптомиксерами» и др. Отдельную роль играет «криминальная разметка» - отнесение тех или иных адресов к т.н. «даркмаркетам». Сюда же могут относиться адреса, связанные с вымогателями, хакерами, финансовыми пирамидами и т.п.

«Криминальная окраска» адреса означает для пользователя фактическую невозможность вывести его активы или превратить их в фиатные деньги через площадку, соблюдающую требования антиотмывочного законодательства (AML).



хорошо, что вы мне всё объяснили

плохо, что я ничего не понял

Сейчас AML-проверки проводятся большинством криптобирж и обменников. В странах, где эта деятельность детально регулируется правом, – подобные проверки являются обязательными.

AML-деятельность базируется на анализе оценки рисков, источников происхождения средств и характере самой операции. Знание разметки конкретного ВА снижает для лица риск стать владельцем «грязных» денег. Снижает риск быть вовлеченным в их отмывание.



- Вы еще скажите, что у вас и аккаунты на криптобирже одинаковые!

Для российских граждан и юрлиц вопрос вывода средств, заблокированных на основании данных о принадлежности к криминальной деятельности, встает еще острее, поскольку в РФ вопрос оборота ВА решен не полностью, а влияние санкций растет. Наши враги часто «окрашивают» российские адреса как «рискованные» или «криминальные».

На криптобиржах и обменниках, соблюдающих AML-стандарты, нужно проходить идентификацию. Там риск получить «грязные» монеты ниже, чем на нерегулируемых обменниках, которые проводят AML проверки только на словах.



Различают следующие источники происхождения «окрашенной» крипты:

1) Darkmarket — площадка, обычно расположенная в анонимной сети (например, Tor), где осуществляется отмывание денег и продаются нелегальные товары. Наличие в криптокошельке монет, поступивших от кошелька, помеченного как «darkmarket», в глазах других пользователей, P2P-площадок и криптобирж, превращает клиента в продавца или получателя незаконных товаров или услуг.



2) Blackmail — рассылка писем с угрозами распространения приватной информации пользователя. Угрозы могут быть вполне реальными, если у вымогателя имеется компромат.

Активы, полученные из таких адресов, может соответственно «окрасить» КК владельца.



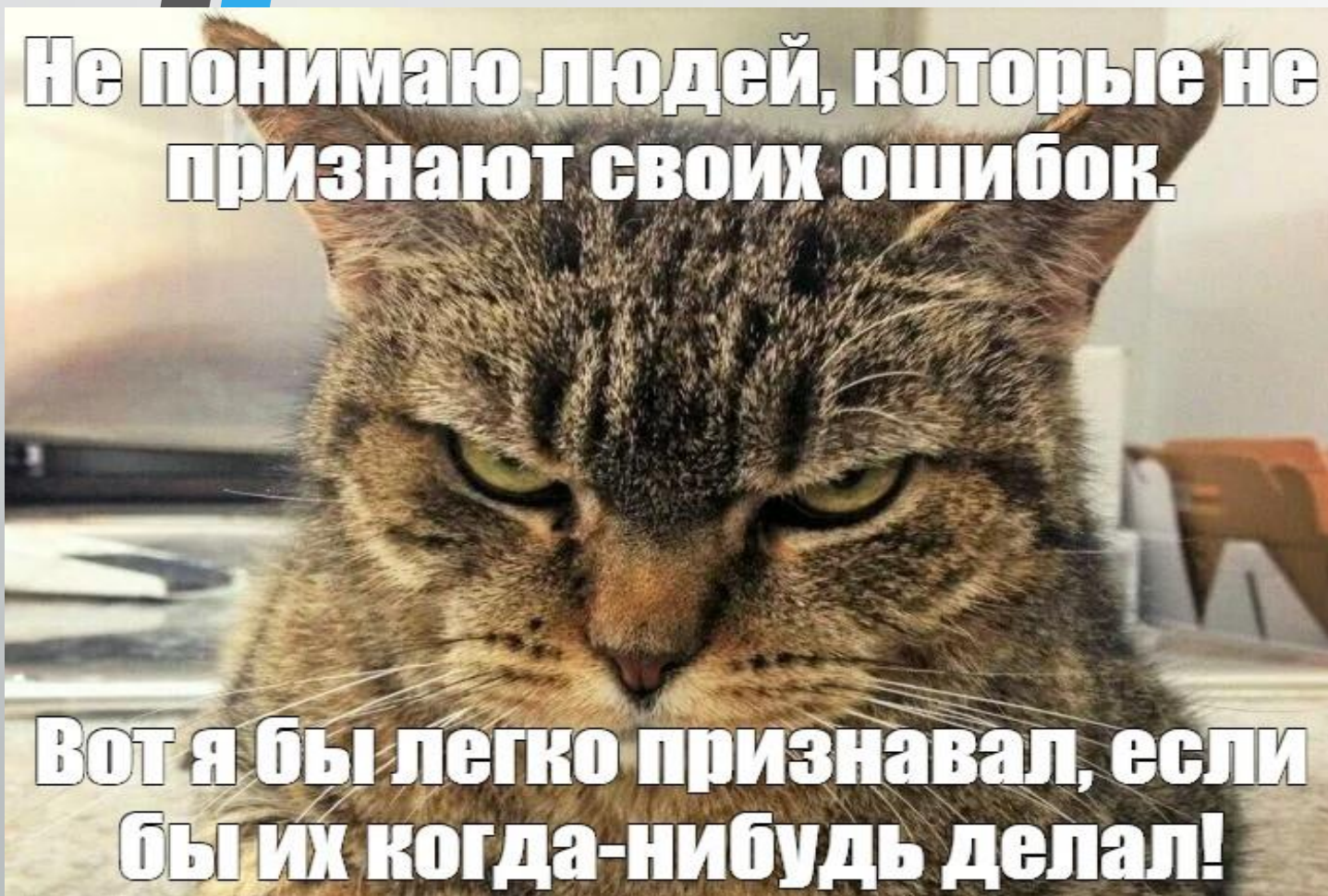
3) Hacking — хакерские атаки, в ходе которых могла быть получена крипта. Само по себе обладание такими монетами на КК может говорить о связи с хакерами. Такой же ущерб «репутации» КК могут нанести и средства, связанные с программами-вымогателями (ransomware), фишингом (phishing) и скамом (scam).



Древние славяне во избежание санкций свою крипту хранили в лукошках, а транзакции совершали на ярмарках.

4) Sanctions — источник находится под международными (ЕС) или национальными санкциями (США, Канада, Япония и др.). Велик риск, что контрагенты или биржа, которые находятся в юрисдикциях, соблюдающих санкции, откажутся от совершения операций.

5) Mixer — если крипто имеет преступное происхождение, злодеи стараются скрыть данный факт и используют специальные сервисы — миксеры. Они позволяют перемешивать транзакции и таким образом скрывать истинное происхождение средств. Обладание криптой из миксера также повышает риски в глазах криптобирж и контрагентов.¹⁴



6) Ponzi schemes — финансовые пирамиды. В отношении организаторов пирамид во многих юрисдикциях возбуждаются уголовные дела, а также ведутся процессы по возврату средств вкладчиков. Обладание криптой из подобных адресов также повышает уровень рисков.



Он не прошел KYC-проверку

Криптовбиржи собирают личную информацию о пользователях в целях их идентификации. Верификация через процедуру KYC позволяет им соответствовать требованиям правовых норм и правил регуляторов, бороться с отмыванием денег и финансированием терроризма.

Обладание «грязной» криптой существенно повышает и уровень риска для КК, который оценивается биржами и получателями средств.¹⁶



В числе последствий нахождения «окрашенных» криптовалют в кошельке можно назвать:

- 1) риск блокировки «горячего» кошелька на криптобирже;
- 2) отказ в получении средств контрагентами и расторжение договора о купле-продаже крипты;
- 3) невозможность проведения обмена или покупки крипты на «окрашенный» кошелек;
- 4) проблемы с правоохранителями.

ВСЕ, ЧТО НАЖИТО НЕПОСИЛЬНЫМ

ТРУДОМ, ВСЁ ПОГИБЛО!

Кроме того, банковские счета и карты могут быть заморожены банком или ФНС, также Росфинмониторингом.

Велик риск получить «грязную крипту». Если уж совсем «повезет», можно отправить активы мошенникам, ничего не получив взамен 😊.

Конечно, можно проверить чистоту адреса контрагента до совершения операции через т.н. «сервисы безопасности». Однако и они не дают 100% гарантии законности сделки и ее завершения. Да и сами такие сервисы часто бывают фейковыми.

Выберите все картинки, где изображен

**Инвестор в
криптовалюты**



VERIFY

joyreactor.cc

Важно помнить, что криптовалютный рынок — это высокорисковая среда. Ожидания лёгких денег не оправдываются. Над помнить бессмертную фразу: «лох - не мамонт; он не вымрет» 😊

Спасибо за внимание!

© Бирюков П.Н., 2025

