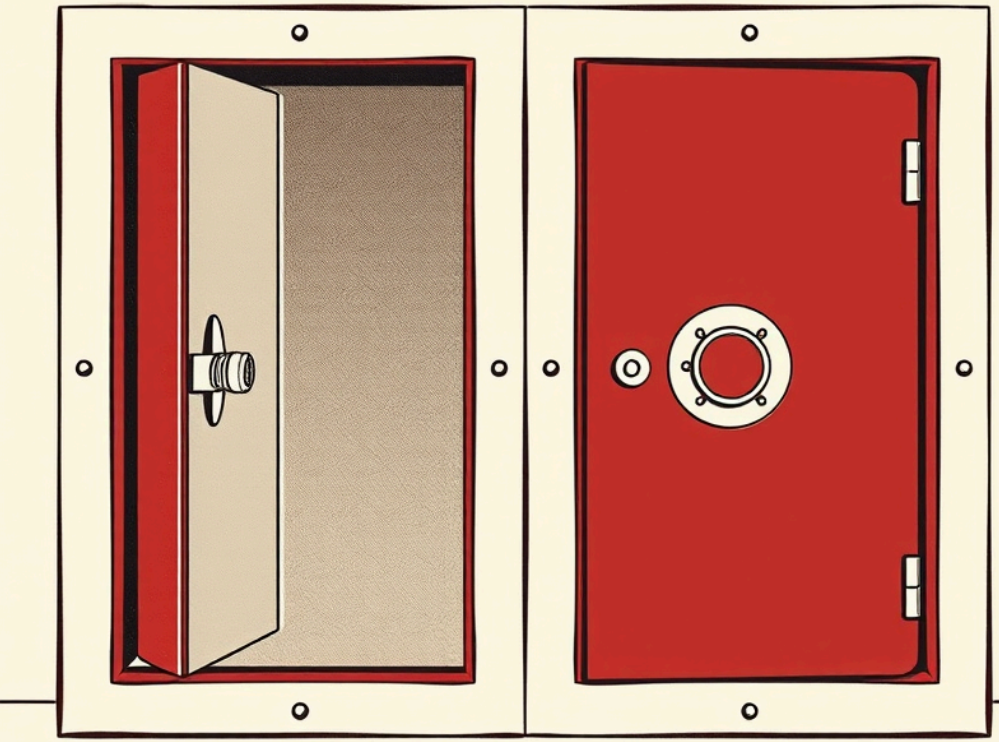
Путеводитель по деньгам, которых вас научили бояться

ПО СРАВНЕНИЮ С ЧЕМ?



Настоящие опасности крипты —
и те, что постарше, уже в вашем банке.

ДМИТРИЙ ЧИСТЯКОВ

ПО СРАВНЕНИЮ С ЧЕМ?

Настоящие опасности крипты —
и те, что постарше, уже в вашем банке.

ДМИТРИЙ ЧИСТЯКОВ

Введение: Уговор

Есть два типа людей, которые расскажут вам про крипту, и ни один из них не говорит с вами.

Первый тип продаёт. Вы их уже знаете — те, что с арендованным Lamborghini, закатом и словом *свобода*, обнаружившие, что легче всего продаётся ощущение, будто ты успел раньше всех. Они расскажут вам про рост. Они не расскажут, что будет дальше, потому что «дальше» нет в презентации.

Второй тип знает, о чём говорит, и пишет друг для друга. Их работа настоящая, она отличная и она нечитаема, потому что никогда не предназначалась вам: она обращена к следователям, к комплаенс-командам, к людям, которые уже знают, что такое nonce. Можно прочитать её всю до слова и по-прежнему не понимать, стоит ли бояться.

Так что есть зазор, и именно в этом зазоре все на самом деле и стоят. Миллионы людей, подходящих к двери, с продавцами по одну сторону и специалистами по другую, и никого посередине, кто не продаёт и не красуется.

Это книга, которой мне не хватало, когда я сам там стоял.

Что это

Я потратил годы, собирая каталог каждого задокументированного способа, которым люди теряли деньги в этой штуке, — сотни инцидентов, начиная с 2010-го, каждый с источником, перепроверенный и разложенный по механизму, а не по драме. Он бесплатный, он публичный, и это не эта книга. Это справочник для профессионалов, и он уморит вас скукой.

Это то, что справочник *знает*, — только рассказанное как то, что оно есть на самом деле: набор историй про людей, большинство из которых не сделали ничего плохого.

Не предупреждение. Не реклама. Не курс. **То, что я хотел бы получить целиком, у двери, прежде чем принялся сочинять всё это на ходу.**

Уговор

Вот что я обещаю, и спрашивайте с меня за каждый пункт, потому что такая книга стоит ровно столько, сколько стоит её худшее предложение.

Каждое число здесь проверяемо, а те, что нет, выбрасываются у вас на глазах. Вы не раз увидите, как я выкидываю собственное лучшее доказательство, потому что у меня есть несколько эффектных цифр, которые выиграли бы спор и за которые я не могу поручиться. Если я возьму число, выдуманное вендором, потому что оно мне льстит, у вас не будет повода верить ни одному другому числу в книге, и вы будете правы.

У каждой главы есть вердикт, и вердикты не все в одну сторону. Это приём, на котором держится вся книга, так что вот он заранее: я беру одну опасность в крипте, став-

лю рядом с версией той же опасности, уже работающей в вашей обычной финансовой жизни, и прямо говорю, что хуже. Иногда ответ — крипта. Крипта во второй главе, и в седьмой, и разгромно в восьмой. Если бы все вердикты вышли в одну сторону, вам стоило бы закрыть книгу, и мне тоже.

Ничего не реконструировано. Где я чего-то не знаю, я так и говорю. Здесь есть кража на $282 млн — крупнее, чем что-либо ещё на этих страницах, — вокруг которой я отказываюсь строить главу, потому что никто не может установить, как это произошло, а история с выдуманными интересными частями — это не история, это ложь со сносками.

И я не собираюсь говорить вам, что делать с вашими деньгами. Ни разу. Я не знаю вашего положения, я вам не советчик, и вся индустрия людей, которые *скажут*, — это и есть причина, по которой вам понадобилась эта книга.

Что вы получите

К концу вы будете знать, что такое кошелёк на самом деле и почему это слово — ложь. Что такое приватный ключ и почему двенадцать слов могут быть четвертью миллиарда долларов. Что такое стейблкоин и что происходит, когда умная его разновидность перестаёт быть умной. Зачем им ваш паспорт и что система, его требующая, на самом деле ловит. Как мемкоин строится, секунда за секундой, чтобы легально забрать у вас деньги. Что значит «чистый» и почему ни у одной монеты этого нет.

И вы будете знать форму всего этого — часть, которую больше нигде не взять: **что почти ничего из этого не ново.** Звонок, забравший $243 млн, — это звонок, с которым ваш банк воюет тридцать лет. Поддельный аппаратный

кошелёк — это скиммер на заправке. Мемкоин — это бойлерная, а бойлерные старше телефона. Мошенничества не пришли с криптой. Они пришли с деньгами и всё это время работали, с размахом, там, где вы уже держите свои.

Что сделала крипта — так это записала их.

Вот и весь довод. Всё остальное — доказательства, их двести страниц, и каждую строку можно проверить.

Ещё одно, перед первой главой

Страх, который привёл вас сюда, оправдан.

Я не буду вас от него отговаривать и не буду говорить, что это безопасно. Первые три главы — худшее в книге, и они намеренно поставлены в начало: человек, теряющий $243 млн из-за звонка; система без отмены; и десятилетие бирж, оказавшихся числом в чьей-то базе данных.

Прочитайте их первыми. Если после этого вы закроете книгу — это честный исход, и книга свои деньги уже отработала.

Но если останетесь, вопрос перестанет быть *опасно ли это* — опасно — и станет тем, который никто не задаёт и который всегда был единственным полезным вопросом обо всём этом:

По сравнению с чем?

1
Звонок

Первый звонок был от Google.

Не от кого-то, кто выдаёт себя за Google в привычном смысле — плохая связь, странный номер, ссылка, ведущая не туда. На экране был номер Google. Голос знал, о чём говорит. С аккаунтом возникла проблема, и человек звонил, чтобы помочь её уладить.

К концу этого звонка у них были его почта и его облако. То есть — всё, что он когда-либо записывал о своих деньгах.

Через час пришёл второй звонок, и этот был от Gemini — криптобиржи, которой он действительно пользовался. Человек на этом звонке знал многое. Знал, какие у него счета. Знал примерно, сколько на них. Знал детали, ко-

торые не может знать ни один случайный звонящий и не имеет права знать ни один мошенник, — и каждая из них была правдой, потому что часом раньше те же люди достали их из почты жертвы.

Вот и весь механизм, и его стоит назвать, потому что именно он отделяет развод, который распознал бы кто угодно, от того, который не распознаёт никто: **каждый этап крадёт данные, которыми удостоверяется следующий.** Первый звонок тонкий и добывает немного. Немногого хватает, чтобы второй звонок стал плотным. Второй звонок забирает всё.

Где-то на втором часу, девятнадцатого августа 2024 года, его провели через сброс двухфакторной аутентификации и перевод средств на кошелёк, который контролировали они. Четыре тысячи шестьдесят четыре биткоина ушли одной транзакцией. Двести тридцать восемь миллионов долларов, один клик. Всего вышло около $243 млн.

Это самая большая сумма, когда-либо отнятая у одного человека разговором.

Кошелёк — это не кошелёк

Два слова в том абзаце — *кошелёк* и *ушли* — делают много тихой работы, и если вы здесь впервые, оба вам слегка врут. Разберёмся с ними сейчас, потому что на них держится вся книга.

Кошелёк ничего не хранит. В него ничего не кладётся и из него ничего не достаётся. Это не вместилище. Он хранит *ключ* — секретное число, — и всё, что делает этот ключ, — разрешает перемещать монеты, которые записаны в другом месте. Думайте о нём не как о бумажнике, а как о фамильной печатке: перстень — это не поместье, это то, что

доказывает, что распоряжение исходит от вас. Потеряете бумажник — потеряете то, что внутри. Потеряете перстень — и кто-то другой сможет распорядиться продать всё поместье целиком.

А монеты никуда не «уходили». Они лежат в реестре, и реестр — то место, где расплетается вторая ложь.

Представьте самую скучную книгу на свете. Каждая страница — список переводов: столько-то, отсюда, туда, в такую-то секунду. Когда кто-то отправляет деньги, добавляется строка. Вот и всё. Вот всё изобретение. Тут нет счетов в привычном смысле, нет имён, нет отделений, нет времени закрытия. Есть список того, кто что куда переместил, и ваш баланс нигде не хранится числом; это то, что получится, если сложить все строки, где вы когда-либо упоминались.

Три вещи об этой книге, и третья — то, из-за чего эта история кончается так, как кончается.

Ею никто не владеет. Нет компании, которая её ведёт. Тысячи компьютеров держат одинаковые копии и постоянно сходятся на том, что говорит следующая страница. Это согласие — достигнутое машинами, которые не знают друг друга и не обязаны, — и есть то, что имеют в виду под словом «блокчейн», и это по-настоящему умная часть.

Ничего никогда не стирается. Нельзя вырвать страницу. Нельзя исправить строку. Ошибку не исправляют; добавляют *новую строку*, которая возвращает деньги, — если тот, у кого они, согласен их вернуть. Никто не может дотянуться до прошлого.

Читать может кто угодно. Не «кто угодно с допуском». Не «кто угодно с ордером». Кто угодно. Прямо сейчас, с телефона, вы можете смотреть, как происходит любой перевод на земле, включая те, что только что что-то украли. Книга пишется публично, навсегда, и так было всегда.

Последнее — самое странное свойство во всех финансах, и эта глава сейчас покажет вам оба его лезвия сразу.

Потому что именно из-за него деньги ушли и не смогли вернуться — и именно из-за него мы знаем имена людей, которые их забрали.

Человек, который их потерял

Он был кредитором в банкротстве Genesis Global Capital и жил в Вашингтоне.

Первый факт не случаен — именно поэтому его и выбрали, и он переворачивает то, что большинство думает о том, как это происходит. Он не был беспечным. Он не был лохом. Он не забрёл сюда, потому что так сказал ролик. Он был искушённым институциональным контрагентом, который по-крупному одалживал кредитной компании, и когда та рухнула, его требование стало частью открытых материалов дела.

Они его не нашли. Они навели о нём справки.

Вот часть, которую труднее всего удержать, и книга к ней вернётся: **найти жертву — это исследовательская задача, и исследование публично.** Материалы банкротства говорили, кому должны. Цепочка говорила, сколько лежит и двигалось ли это. В другом деле, задокументированном тем же способом, атакующие составили список целей, просканировав реестр на крупные балансы, которые годами лежали без движения, — спящий капитал читаем снаружи, и его владелец где-то привязан к нему именем.

Прозрачность, позволяющая следователю проследить кражу, — это та же прозрачность, что позволяет атакующему составить список целей. Одного без другого не бывает. Это не

изъян конструкции; это и есть конструкция, и в этой главе за неё приходит счёт.

Всё сработало

Вот что не случилось девятнадцатого августа.

Не был взломан ни один смарт-контракт. Не была сломана криптография. Не была скомпрометирована прошивка кошелька, не была взломана биржа, не отказал протокол, не нашлась ошибка, не была сожжена ни одна уязвимость нулевого дня. Ничто в технологии не пошло не так ни в один момент из тех двух часов, за которые сдвинулась четверть миллиарда долларов.

Каждый компонент сделал ровно то, что было предписано. Кошелёк подписал корректно составленную транзакцию, потому что корректно составленная транзакция — это то, что ему подали, а подписывать такие — вся его задача. Сеть её подтвердила, потому что она была валидной. Цепочка записала её навсегда и показала любому на земле за секунды, а для этого цепочка и существует.

В этом стеке нет ни одного компонента, который дал сбой. Есть человек у телефона, и всё, что ниже него, работает безупречно.

Вот уступка, которую книга должна сделать, прежде чем что-либо доказывать: **здесь есть слой, до которого не дотягивается никакая инженерия, и это тот слой, к которому прикручено всё остальное.** Можно держать свои ключи, отказаться от всех кастодианов, купить железо, никогда не заходить на сайт, который не набрал сам, — и всё сооружение всё равно упирается в человека, которому можно сказать неправду голосом, который звучит убедительно и знает его баланс.

Люди, которые их забрали

Это были дети.

Малоуну Ламу было двадцать. Он родился в Сингапуре в июле 2004-го и вырос в Чоа-Чу-Канг, районе социального жилья на западе острова. Ходил в среднюю школу Unity и подростком бросил её, чтобы проводить время за торговлей криптой и в онлайн-сообществах, которые его вырастили, — серверах Minecraft и Discord.

С соседями по квартире в Техасе он, согласно федеральному обвинению, основал штуку, которую они назвали, без видимой иронии, **«Предприятием социальной инженерии»**. Оно разрослось до четырнадцати человек в нескольких штатах. Они работали с ворованными базами, данными из даркнета и фишинговой почтой, и то, чем они занимались, было не хакерством. Это были телефонные звонки.

Джандиэлю Серрано был двадцать один год; он был из Лос-Анджелеса и звался «VersaceGod». **Вир Четал** по прозвищу «Wiz» был ещё младше — подросток.

Двадцатилетний, ушедший из школы в Discord, забрал двести сорок три миллиона долларов у институционального кредитора в Вашингтоне по телефону, примерно за два часа, ничего не сломав.

Это предложение, ради которого глава и существует, и ни одна его часть не преувеличена.

А потом они это сняли

Они транслировали ограбление своим друзьям в прямом эфире.

Не как улику. Для зрителей. Есть запись, где люди, только что забравшие $243 млн у незнакомца, смотрят, как прилетают уведомления, — сигналы, подтверждения, приходящие деньги, — и радуются, и обсуждают, что дальше. Сделана она была друг для друга, по той причине, по которой люди, только что сделавшие что-то огромное, хотят сохранить этот момент.

Потом она утекла и стала тем, по чему их опознали.

Дальше были тридцать три люксовые машины. Часы. Ночные клубы. Путешествия. Это не была попытка уйти безнаказанными; это был кутёж на публике в исполнении людей, которые, похоже, не думали дальше ближайшей недели.

FBI арестовало Малоуна Лама в Майами восемнадцатого сентября 2024 года, через месяц после кражи. Полицейский не при исполнении успел предупредить его, что за ним придут, и по дороге к собственному аресту он выбросил телефон в залив Бискейн.

Вир Четал признал вину. Он лишился почти тридцати дизайнерских часов, гардероба и более чем $36 млн в эфире. Потом, выйдя под залог в ожидании приговора за то, что было тогда крупнейшей криптокражей у одной жертвы, он лишился залога — после того, как обвинение заявило о его участии в краже ещё двух миллионов долларов.

Держите всё это в уме на фоне остальной главы, потому что это единственный свет в ней. Это книга, которая потратит большую часть страниц на людей, потерявших деньги и так и не узнавших, что с ними случилось. У этой истории есть имена, возраст, видео, три уголовных дела и телефон на дне залива.

А есть они у неё из-за той книги, что была несколько страниц назад.

Вот что на самом деле значит «идти по следу денег», потому что это совсем не то, что подсказывает фраза, и это самое полезное, что может понять новичок.

Когда $238 млн сдвинулись, появилась строка: *столько-то, с этого адреса, на тот адрес, в такую-то секунду*. Публичная. Навсегда. Дальше воры сделали то, что делают воры, — разделили деньги натрое и побежали. Пятнадцать бирж или больше. Биткоин поменян на лайткоин, лайткоин на эфир, эфир на монеро, всё быстрее и быстрее, и каждый хоп должен был оборвать след.

Каждый хоп записывал ещё одну строку.

В этом и ловушка, и у неё нет дна. В мире, который вы знаете, идти по следу украденных денег — значит спрашивать. Спрашивать банк, для чего нужна причина; спрашивать банк в другой стране, для чего нужен договор; ждать; получать отказ; спрашивать снова. Каждый хоп — это дверь, за каждой дверью — человек, который может сказать «нет», и достаточное число дверей измотает кого угодно.

Здесь дверей нет. У реестра нет разрешений. Вор, гонящий деньги через пятнадцать бирж, не заметает пятнадцать следов — он пишет ещё пятнадцать строк в книге, которую и так может читать любой, и перестать писать он не может, потому что двигать деньги здесь и *значит* писать. Он может сделать путь запутанным. Он не может сделать его приватным и не может сделать так, чтобы завтра его там не стало.

И вот кто-то это прочитал.

Он не живёт под своим именем, и так задумано, поэтому будем пользоваться тем, которым пользуется он сам: **ZachXBT**. Его аватар — мультяшный утконос в детективном плаще. Он не полицейский. Он не регулятор, не агент, не ана-

литик в фирме и ничей не сотрудник. У него нет никакой следовательской подготовки — никакой: ни курса, ни значка, ни единого дня. Он сам это говорил.

Что у него есть — так это счёты.

Он пришёл в 2017-м, во время бума, когда любой мог продать токен, написав о нём документ, и делал то, что делали все: покупал разрекламированные. Смотрел, как они исчезают. Потом, в 2018-м, кто-то взломал его кошелёк и забрал около пятнадцати тысяч долларов — по тем временам изрядную часть его денег.

И где-то в последствиях этого — тех самых последствиях, описанию которых эта книга посвятила главу, тех, где нет отдела по борьбе с мошенничеством и некому позвонить, — он сделал то, чего не делает почти никто.

Он пошёл и посмотрел.

Не на собственную кражу. На *реестр*. И нашёл он там то, о чём всем говорили и чего никто не понял: всё было по-прежнему там. Каждый хоп, сделанный вором, всё ещё лежал на виду — нестёртый, ждущий. Никто это не убрал, потому что никто не мог. Никто это не спрятал, потому что никто не мог. Оно просто *было там* — было всё это время, и почти никто это не читал.

Это, если хотите, момент в духе Майкла Льюиса — один человек замечает правду о системе раньше людей, которым платят за то, чтобы замечать. Только это было не озарение про ипотечные облигации. Это было больше похоже на то, как войти в библиотеку, про которую всем говорили, что это сейф.

Публиковаться он начал в 2021-м. К тому времени, как люди с того звонка забрали $243 млн у незнакомца в Вашингтоне, он был причиной, по которой на их имена ушёл месяц, а не вечность.

К 2025 году сооснователь Paradigm оценивал сумму, которую он помог вернуть жертвам, **более чем в триста пятьдесят миллионов долларов**.

Человек, потерявший пятнадцать тысяч и понятия не имевший, что делает, отвоевал обратно триста пятьдесят миллионов для людей, которых никогда не встречал.

Без значка. Без повестки. Без ордера. Без чьего-либо разрешения. Он прочитал то, что и так было публично — и что останется публичным через сто лет.

Он ещё вернётся. Всё остальное в этой книге тихо вертится вокруг того, что он понял.

(Одна оговорка — раз уж эта книга собирается двести страниц называть людей по именам. Его настоящее имя — часть публичной записи: оно всплыло в судебном документе, потому что кто-то, кому не понравилось, что его расследуют, подал на него в суд. Здесь оно не появится. Он просит его не называть, книге это не нужно, и в этом есть своя симметрия: человек, сделавший видимыми чужие деньги, — единственный на этих страницах, чьё имя я не напечатаю.)

Чем эта глава не является

Отсюда было бы легко написать предложение, которое всё это делает выносимым. Что ему надо было положить трубку. Что было правило, и он его пропустил.

Он ничего не пропустил. Не было момента, в котором осторожный человек это поймал бы, потому что второй звонок пришёл уже *с доказательствами* — доказательствами, украденными у него часом раньше, отчего они и были точны. Его обманул не незнакомец, который удачно угадал. Его обманул незнакомец, который прочитал его почту.

А когда всё кончилось, сделать было нечего. Некуда обратиться, нечего отменить, никакой инстанции над транзакцией, потому что транзакция была валидной, корректно составленной и сделала ровно то, что в ней написано. Он смотрел, как $243 млн уходят в форме, у которой нет отмены, и правильность системы была причиной, по которой её нельзя было отменить.

Что-то вернулось позже — изъятия, конфискации, гардероб, гора часов и тридцать три машины. Большая часть — нет.

Вот он, страх, и страх оправдан. Это не суеверие, это не выдумка СМИ, и эта книга не собирается никого от него отговаривать. **Когда деньги уходят здесь, они уходят навсегда, и необратимость — это реальное свойство с реальной ценой, и цена ровно такая, какой выглядит.**

Побудьте с этим ещё одну главу, прежде чем что-либо доказывать. Это заслужило себе место.

Но две вещи возьмите с собой, потому что на них построено всё остальное.

Первая — что **ничего не сломалось.** Ни строчки кода, ни ключа, ни цепочки. Сбой дал человек, поверивший голосу, который знал его баланс.

Вторая — что мы знаем имена людей, которые ему звонили, сколько им было лет, что они купили и где утонул телефон.