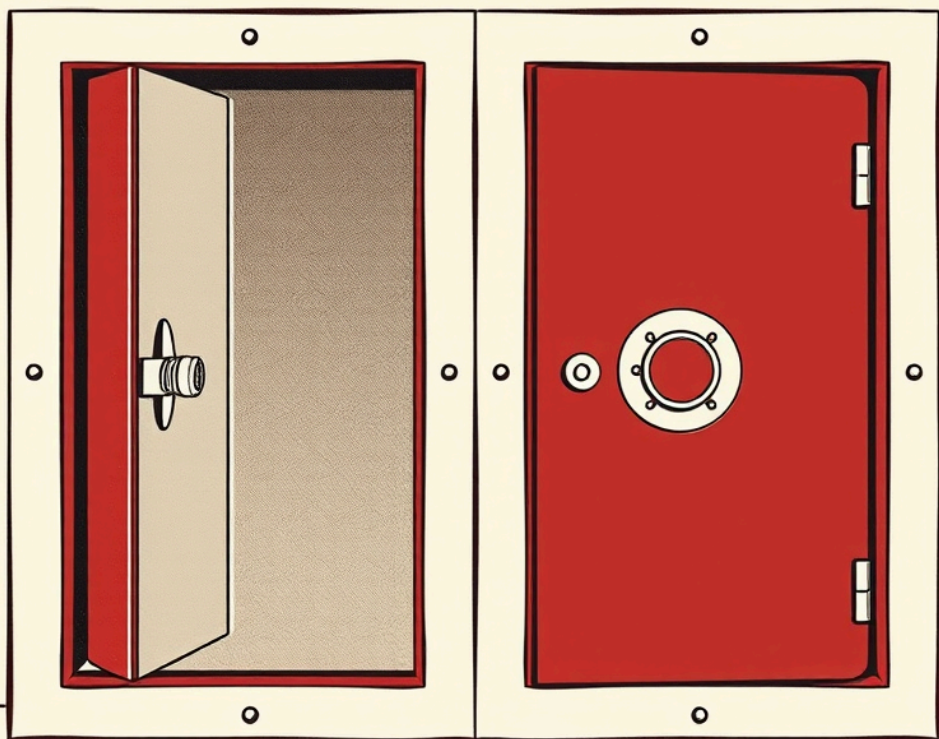


Путівник по грошах, яких вас навчили боятися

ПОРІВНЯНО З ЧИМ?



Справжні небезпеки крипто —
і ті, що старші, вже у вашому банку.

ДМИТРО ЧИСТЯКОВ

ПОРІВНЯНО З ЧИМ?

Справжні небезпеки крiпти —
і ті, що старші, вже у вашому банку.

ДМИТРО ЧИСТЯКОВ

Вступ: Угода

Є два типи людей, які розкажуть вам про крипту, і жоден із них не говорить із вами.

Перший тип продає. Ви вже їх знаєте — ті, з орендованим Lamborghini, заходом сонця і словом *свобода*, які виявили, що найлегший актив для продажу — це відчуття, ніби встиг раніше за інших. Вони розкажуть вам про зиск. Вони не розкажуть, що буде далі, бо того, що буде далі, немає у презентації.

Другий тип знає, про що говорить, і пише для своїх. Їхня праця справжня, вона чудова — і її неможливо читати, бо вона ніколи не призначалася вам: вона адресована слідчим, комплаєнс-командам, людям, які вже знають, що таке попсе. Ви могли б прочитати кожне її слово — і все одно не знати, боятися вам чи ні.

Тож є проміжок, і саме в цьому проміжку насправді стоять усі. Мільйони людей підходять до дверей: продавці з одного боку, фахівці з іншого, і нікого посередині, хто не продає й не хизується.

Це книжка, якої я хотів, коли сам там стояв.

Що це таке

Я роками збирав каталог кожного задокументованого способу, у який люди втрачали гроші в цій справі, — сотні інцидентів, аж від 2010 року, кожен із джерелом, перехресно перевірений і впорядкований за механізмом, а не за драмою. Він безкоштовний, він публічний — і він не ця книжка. Це довідник для фахівців, і він занудить вас до смерті.

Ця книжка — те, що довідник *знає*, розказане як те, чим воно є насправді: набір історій про людей, більшість із яких не зробили нічого поганого.

Не попередження. Не реклама. Не курс. **Те, що я хотів би отримати цілісним, у дверях, перш ніж почав вигадувати все на ходу.**

Угода

Ось що я обіцяю, і ви маєте вимагати від мене кожного пункту, бо така книжка варта рівно стільки, скільки варте її найгірше речення.

Кожне число тут можна перевірити, а ті, які не можна, я викидаю на ваших очах. Ви не раз побачите, як я відкидаю власні найкращі докази, бо в мене є кілька ефективних цифр, які виграли б суперечку, але за які я не можу поручитися. Якщо я вживу цифру, яку вигдав якийсь поставальник, лише тому що вона мені лестить, у вас не буде підстав вірити жодному іншому числу в книжці — і ви матимете рацію.

Кожен розділ має вирок, і вирoki не всі в один бік. Це прийом, на якому тримається вся книжка, тож ось він наперед: я беру одну небезпеку в крипті, ставлю її поряд із версією тієї самої небезпеки, яка вже діє у вашому звичайному

фінансовому житті, і прямо кажу, яка гірша. Іноді відповідь — крипта. Це крипта в другому розділі, і в сьомому, а у восьмому — розгромно. Якби всі вироки виходили в один бік, вам варто було б закрити книжку — і мені теж.

Нічого не реконструйовано. Там, де я чогось не знаю, я так і кажу. Тут є крадіжка на \$282 млн — більша за все інше на цих сторінках, — навколо якої я відмовляюся будувати розділ, бо ніхто не може встановити, як це сталося, а історія, у якій цікаві частини вигадані, — це не історія, це брехня з виносками.

І я не збираюся вказувати вам, що робити з вашими грошима. Жодного разу. Я не знаю вашої ситуації, я не ваш радник, і ціла індустрія людей, які *таки* вам скажуть, — це причина, чому вам знадобилася ця книжка.

Що ви отримаєте

Наприкінці ви знатимете, чим насправді є гаманець і чому це слово — брехня. Що таке приватний ключ і чому дванадцять слів можуть бути чвертю мільярда доларів. Що таке стейблкоїн і що стається, коли розумний його різновид перестає бути розумним. Чому вони хочуть ваш паспорт і що система, яка його вимагає, насправді ловить. Як мемкоїн будують, секунда за секундою, щоб законно забрати у вас гроші. Що означає «чистий» і чому жодна монета такою не є.

І ви знатимете форму цього явища — частину, якої не дістати більше ніде: **майже ніщо з цього не нове.** Телефонний дзвінок, який забрав \$243 млн, — це той самий дзвінок, з яким ваш банк воює вже тридцять років. Підроблений апаратний гаманець — це скимер на заправці. Мемкоїн — це бойлерна, а бойлерні старші за телефон. Шахрайства при-

йшли не з криптою. Вони прийшли з грошима—і весь цей час працюють, у великих масштабах, у тому самому місці, де ви вже тримаєте свої.

Крипта їх просто записала.

Ось і весь аргумент. Усе інше—докази, і їх тут двісті сторінок, і ви можете перевірити кожен рядок.

Одне, перед першим розділом

Страх, який привів вас сюди, — правильний.

Я не відмовлятиму вас від нього і не казатиму, що це безпечно. Перші три розділи—найгірше, що є в книжці, і вони навмисно поставлені спереду: чоловік, який втрачає \$243 млн через телефонний дзвінок; система без кнопки «скасувати»; і десятиліття бірж, які виявилися просто числом у чийсь базі даних.

Прочитайте спершу їх. Якщо після цього ви закриєте книжку—це цілком слушний результат, і свої гроші ви витратите даремно.

Але якщо ви залишитеся, питання перестає бути *чи це небезпечно*—так, небезпечно—і стає тим, якого ніхто не ставить, єдиним корисним питанням, яке взагалі коли-небудь існувало про все це:

Порівняно з чим?



1

Телефонний дзвінок

Перший дзвінок був від Google.

Не від когось, хто видавав себе за Google — так, як це зазвичай буває: погана лінія, дивний номер, посилання, що веде кудись не туди. Номер на екрані був номером Google. Голос знав, про що говорить. З акаунтом виникла проблема, і чоловік телефонував, щоб допомогти її владнати.

До кінця того дзвінка вони вже мали його пошту й хмарне сховище. Тобто мали все, що він будь-коли записував про свої гроші.

За годину надійшов другий дзвінок — цього разу від Gemini, криптовалютної біржі, якою він справді користувався. Чоловік на цьому дзвінку дещо знав. Він знав, які акаун-

ти існують. Знав приблизно, що в них лежить. Він знав деталі, яких не міг знати ніхто з тих, хто дзвонить навімання, і які не мали б бути відомі жодному шахраєві, — і кожна з них була правдою, бо годину тому ті самі люди дістали їх зі скриньки, яку відкрив перший дзвінок.

Це і є весь механізм, і його варто назвати, бо саме він відрізняє шахрайство, яке помітив би будь-хто, від того, яке не помічає ніхто: **кожен етап краде облікові дані, що автентифікують наступний**. Перший дзвінок благодійний і дістає трохи. Ця децима робить другий дзвінок переконливим. Другий дзвінок дістає все.

Десь на другій годині, дев'ятнадцятого серпня 2024 року, вони провели його через скидання двофакторної автентифікації й переказ коштів на гаманець, який контролювали. Чотири тисячі шістдесят чотири біткоіни пішли одним переказом. Двісті тридцять вісім мільйонів доларів, один клік. Загалом вийшло приблизно \$243 млн.

Це найбільша сума грошей, яку будь-коли забрали в однієї людини, просто розмовляючи з нею.

Гаманець — це не гаманець

Два слова в тому абзаці — *гаманець* і *пішли* — роблять багато тихої роботи, і якщо ви тут новачок, обидва трохи вам брешуть. Виправмо це зараз, бо на них тримається вся ця книжка.

Гаманець не містить нічого. У нього нічого не потрапляє й нічого з нього не виходить. Це не контейнер. Він містить *ключ* — таємне число, — а цей ключ дозволяє переміщати монети, записані десь в іншому місці. Уявляйте його не як гаман, а радше як перстень-печатку: перстень — це не

маєток, це те, що доводить, що розпорядження надійшло від вас. Загубіть гаман — втратите те, що в ньому. Загубіть перстені — і хтось інший може наказати продати весь маєток.

А монети нікуди не «пішли». Вони — у реєстрі, і реєстр — те місце, де розплітається друга брехня.

Уявіть найнуднішу книжку у світі. Кожна сторінка — це список переказів: стільки-то, звідси, туди, о цій секунді. Коли хтось надсилає гроші, додається рядок. Ось і все. Ось і весь винахід. Тут немає рахунків у звичному вам розумінні, немає імен, немає відділень, немає години закриття. Є список того, хто, що й куди переказав, і ваш баланс — це не число, що десь зберігається; це те, що ви отримуєте, коли складаєте всі рядки, які будь-коли вас згадували.

Три речі про цю книжку, і третя — це причина, чому ця історія закінчується саме так.

Вона нікому не належить. Немає компанії, яка її веде. Тисячі комп'ютерів зберігають ідентичні копії й постійно узгоджують, що каже наступна сторінка. Ця згода — досягнута машинами, які не знають одна одну й не мусять, — і є тим, що люди мають на увазі, коли кажуть «блокчейн», і це справді розумна частина.

Ніщо ніколи не стирається. Ви не можете вирвати сторінку. Не можете виправити рядок. Помилку не виправляють; додається *новий рядок*, який повертає гроші назад — якщо той, хто їх тримає, погоджується їх повернути. Ніхто не може дотягнутися до минулого.

Будь-хто може її читати. Не «будь-хто з дозволом». Не «будь-хто з ордером». Будь-хто. Просто зараз, зі свого телефона, ви можете спостерігати за кожним переказом на землі в мить, коли він відбувається, зокрема за тими, що щойно щось украли. Книжка пишеться публічно, назавжди, і так було завжди.

Остання властивість — найдивніша в усіх фінансах, і цей розділ зараз покаже вам обидва її леза водночас.

Бо саме через неї гроші пішли й уже не могли повернутися — і саме через неї ми знаємо імена людей, які їх забрали.

Чоловік, який їх втратив

Він був кредитором у справі про банкрутство Genesis Global Capital і жив у Вашингтоні.

Перший факт не випадковий — саме через нього його й обрали, і він перевертає те, у що більшість вірить щодо того, як таке стається. Він не був необачним. Він не був легкою здобиччю. Він не забрів сюди тому, що якесь відео йому так порадило. Він був досвідченим інституційним контрагентом, який позичав великі суми кредитній компанії, і коли та компанія завалилася, його вимога потрапила до публічних документів.

Вони на нього не натрапили. Вони його розшукали за документами.

Це найважче втримати в голові, і книжка ще до цього повернеться: **знайти жертву — це дослідницька задача, а дослідження публічне.** Документи про банкрутство казали, кому винні. Ланцюг казав, хто що тримає й чи воно рухалося. В іншому випадку, задокументованому так само, зловмисники склали свій короткий список, скануючи реєстр у пошуках великих балансів, які роками лежали нерухомо, — бездіяльне багатство помітне ззовні, а його власник — це десь прикріплене до нього ім'я.

Та сама прозорість, що дозволяє слідчому простежити крадіжку, дозволяє зловмиснику скласти список цілей. Одне без одного не дається нікому. Це не вада в конструкції; це і є

конструкція, і саме в цьому розділі надходить рахунок до сплати.

Кожна система спрацювала

Ось що не сталося дев'ятнадцятого серпня.

Не використали вразливості жодного смартконтракту. Не зламали жодної криптографії. Не скомпрометували прошивку жодного гаманця, не зламали жодної біржі, не відмовив жоден протокол, не знайшли жодного багу, не спалили жодного зеродея. У жодну мить тих двох годин, за які перемістили чверть мільярда доларів, з технологією нічого не пішло не так.

Кожен компонент зробив рівно те, для чого був призначений. Гаманець підписав коректно сформований переказ, бо коректно сформований переказ йому й передали, а підписувати такі — весь його сенс. Мережа його підтвердила, бо він був чинний. Ланцюг записав його назавжди й за секунди показав будь-кому на землі — а саме *для цього* ланцюг і існує.

У цьому стеку немає жодного компонента, який відмовив. Є чоловік із телефоном — і все, що нижче за нього, працює бездоганно.

Це поступка, яку книжка винна, перш ніж бодай щось доводити: **тут є шар, до якого не дотягується жодна інженерія, і саме до цього шару прикручене все інше.** Ви можете тримати власні ключі, відмовитися від усіх кастодіанів, купити залізо, ніколи не заходити на сайт, адресу якого не набрали самі, — і вся ця споруда все одно завершується людиною, якій хтось, хто звучить переконливо й знає її баланс, може сказати неправду.

Ті, хто їх забрав

Це були діти.

Мелоуну Ламу було двадцять. Він народився в Сінгапурі в липні 2004 року й виріс у Чоа-Чу-Канг, районі соціального житла на заході острова. Він ходив до Unity Secondary School і підлітком кинув школу, щоб торгувати криптою й жити в онлайн-спільнотах, які його виростили, — на серверах Minecraft і в Discord.

Разом зі своїми співмешканцями в Техасі він, згідно з федеральним обвинуваченням, заснував щось, що вони без видимої іронії назвали **Social Engineering Enterprise** — «Підприємством соціальної інженерії». Воно розрослося до чотирнадцяти людей у кількох штатах. Їхньою сировиною були зламані бази даних, дані з дарквебу й фішингові листи, а те, що вони робили, не було зломом. Це були телефонні дзвінки людям.

Джеандіелю Серрано був двадцять один рік, він був із Лос-Анджелеса й мав прізвисько «VersaceGod». **Вір Четал**, відомий як «Wiz», був іще молодшим — підліток.

Двадцятирічний хлопець, який проміняв школу на Discord, забрав двісті сорок три мільйони доларів в інституційного кредитора у Вашингтоні телефоном, приблизно за дві години, не зламавши жодної речі.

Це те речення, заради якого й існує цей розділ, і жодна його частина не перебільшена.

А потім вони це зняли

Вони вели пряму трансляцію пограбування для своїх друзів.

Не як доказ. Для глядачів. Існує запис, на якому люди, що щойно забрали \$243 млн у незнайомця, спостерігають, як надходять сповіщення — повідомлення, підтвердження, гроші, що прибувають, — і святкують, і говорять про те, що буде далі. Його зробили для своїх, з тієї причини, з якої люди, що щойно зробили щось грандіозне, хочуть зберегти цю мить.

Потім він витік і став тим, що їх ідентифікувало.

Далі були тридцять три розкішні автомобілі. Годинники. Нічні клуби. Подорожі. Це не була спроба вийти сухими з води; це був марнотратний загул на очах у всіх, влаштований людьми, що, схоже, не думали далі, ніж на тиждень уперед.

FBI заарештувало Мелоуна Лама в Маямі вісімнадцятого вересня 2024 року, за місяць після крадіжки. Поліцейський не при виконанні попередив його, що арешт наближається, і дорогою до затримання він викинув свій телефон у затоку Біскейн.

Вір Четал визнав провину. Він віддав майже тридцять дизайнерських годинників, гардероб і понад \$36 млн в ефірі. Потім, перебуваючи під заставою в очікуванні вироку за те, що на той момент було найбільшою крадіжкою крипти в однієї жертви, він втратив заставу — після того, як обвинувачення заявило про його участь у крадіжці ще двох мільйонів доларів.

Тримайте все це супроти решти розділу, бо це єдине світло тут. Це книжка, яка більшість своїх сторінок присвятить людям, які втратили гроші й так і не дізналися, що з ними сталося. А в цій історії є імена, вік, відео, три судові переслідування й телефон на дні затоки.

Причина, з якої все це є, — та сама книжка, про яку йшлося кілька сторінок тому.

Ось що насправді означає «йти за грошима», бо це зовсім не те, що підказує ця фраза, і це найкорисніша річ, яку може зрозуміти новачок.

Коли \$238 млн рушили, з'явився рядок: *стільки-то, з цієї адреси, на ту адресу, о цій секунді*. Публічно. Назавжди. Далі злодії зробили те, що роблять злодії,—розділили суму на трьох і кинулися тікати. П'ятнадцять чи більше бірж. Біткоїн міняли на лайткоїн, лайткоїн на ефір, ефір на монеро, дедалі швидше, і кожен хоп мав обірвати слід.

Кожен хоп писав іще один рядок.

Ось у чому пастка, і в неї немає дна. У знайомому вам світі йти за краденими грошима означає просити. Просити банк, для чого потрібна підстава; просити банк в іншій країні, для чого потрібен договір; чекати; отримувати відмову; просити знову. Кожен хоп—це двері, і за кожними дверима стоїть людина, яка може сказати «ні», а достатня кількість дверей виснажить будь-кого.

Дверей немає. У реєстрі немає дозволів. Злодій, що переганяє гроші через п'ятнадцять бірж, не замітає п'ятнадцять слідів—він пише ще п'ятнадцять рядків у книжці, яку всі й так можуть читати, і він не може перестати писати, бо рухати гроші—це тут і є писати. Він може зробити шлях заплутаним. Він не може зробити його приватним і не може змусити його зникнути завтра.

Тож хтось це прочитав.

Він не живе під своїм іменем, і так задумано, тож користуватимемося тим, яким він користується: **ZachXBT**. Його аватар—мультяшний качкодзьоб у плащі детектива. Він не поліцейський. Він не регулятор, не агент, не аналітик у якійсь фірмі й не чийсь працівник. Він не має жодної слідчої підготовки—жодної, ні курсу, ні значка, ні дня. Він сам це казав.

Зате в нього є образа.

Він з'явився у 2017-му, під час буму, коли будь-хто міг продати токен, просто написавши про нього документ, і він робив те, що робили всі: купував розхайпані. Він дивився, як вони зникають. Потім у 2018-му хтось зламав його гаманець і забрав близько п'ятнадцяти тисяч доларів, що на той час було чималою частиною його грошей.

І десь посеред тих наслідків — тих самих, які книжка вже цілий розділ описує, тих, де немає відділу боротьби з шахрайством і немає кому подзвонити, — він зробив те, чого майже ніхто не робить.

Він пішов і подивився.

Не на власну крадіжку. На *реєстр*. І те, що він там знайшов, було тим, що всім казали й чого ніхто не зрозумів: воно все ще було там. Кожен хоп, який зробив злодій, досі лежав у публічному доступі, нестертий, чекав. Ніхто його не прибрав, бо ніхто не міг. Ніхто його не сховав, бо ніхто не міг. Воно просто *було там*, і було там увесь час, і майже ніхто його не читав.

Це, якщо хочете, момент Майкла Льюїса — одна людина помічає щось правдиве про систему раніше, ніж ті, кому за це платять. Тільки це не було прозоріння щодо іпотечних облігацій. Це було ближче до того, щоб зайти в бібліотеку, про яку всім казали, що це сейф.

Він почав публікуватися у 2021-му. На той час, коли люди з того дзвінка забрали \$243 млн у незнайомця у Вашингтоні, саме він був причиною, чому їх назвали за місяць, а не ніколи.

До 2025-го співзасновник Paradigm оцінив суму, яку той допоміг повернути жертвам, у **понад триста п'ятдесят мільйонів доларів**.

Чоловік, який втратив п'ятнадцять тисяч і гадки не мав, що робить, відвоював триста п'ятдесят мільйонів для людей, яких ніколи не зустрів.

Ні значка. Ні повістки. Ні ордера. Нічийого дозволу. Він прочитав те, що вже було публічним і що залишатиметься публічним і за сто років.

Він іще повернеться. Уся решта цієї книжки тихо обертається навколо того, що він збагнув.

(Одне зауваження, бо ця книжка збирається двісті сторінок називати людей поіменно. Його справжнє ім'я — у публічних документах: воно сплигло в судовому позові, бо хтось, кому не сподобалося, що його розслідують, подав на нього до суду. Тут воно не з'явиться. Він просить не ідентифікувати його, книжці це не потрібно, і в цьому є певна симетрія: чоловік, який зробив видимими чужі гроші, — єдина людина на цих сторінках, чиє ім'я я не друкуватиму.)

Чим цей розділ не є

Звідси було б легко написати речення, яке робить це стерпним. Що йому слід було покласти слухавку. Що було правило, а він його прогавив.

Він його не прогавив. Не було миті, коли обережна людина це вловлює, бо на момент другого дзвінка той мав докази — докази, забрані в нього годиною раніше, і саме тому він був точним. Його обдурих не незнайомець, який вдало вгадав. Його обдурих незнайомець, який прочитав його пошту.

А коли все скінчилося, робити було нічого. Ні до кого звернутися, ні скасування, ні інстанції над переказом, бо переказ був чинний, коректно сформований і зробив рівно те,

що в ньому написано. Він дивився, як \$243 млн ідуть у формі, яка не має кнопки «скасувати», і саме коректність системи була причиною, чому це не можна було скасувати.

Дещо згодом повернули — арешти майна, конфіскації, гардероб, купа годинників і тридцять три автомобілі. Більшість — ні.

Це і є той страх, і цей страх правильний. Це не забобон і не вигадка медіа, і ця книжка нікого від нього не відмовлятиме. **Коли гроші зникають тут, вони зникають назавжди, і незворотність — це реальна властивість із реальною ціною, і ця ціна саме така, якою й здається.**

Побудьте з цим іще один розділ, перш ніж бодай щось доводитиметься. Воно заслужило місце.

Але пронесіть крізь усе дві речі, бо на них будується решта.

Перша — що **нічого не зламалося**. Ні рядок коду, ні ключ, ні ланцюг. Збій дав чоловік, який повірив голосу, що знав його баланс.

Друга — що ми знаємо імена людей, які йому телефонували, скільки їм було років, що вони купили й куди полетів телефон.