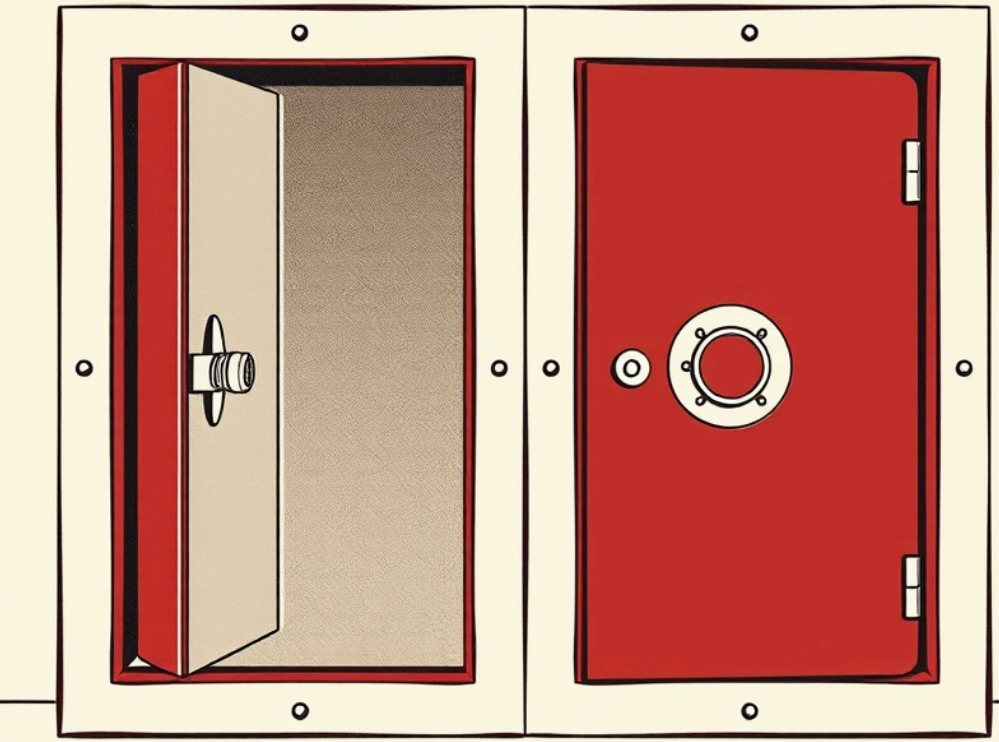
Um guia de campo sobre o dinheiro que te ensinaram a temer

COMPARADO COM O QUÊ?



Os perigos reais das criptomoedas —
e os seus gêmeos, que já estão no seu banco.

DMYTRO CHYSTIAKOV

COMPARADO COM O QUÊ?

Os perigos reais das criptomoedas —
e os seus gêmeos, que já estão no seu banco.

DMYTRO CHYSTIAKOV

Primeira edição, 2026

Tradução do original em inglês: Compared to What?

Cada incidente deste livro está documentado em registro público; há uma nota sobre as fontes no final.

Este livro é informativo. Não constitui aconselhamento financeiro, de investimento ou jurídico.

Algumas pessoas citadas neste livro foram acusadas de crimes, mas não condenadas; presumem-se inocentes até que se prove o contrário. Situações processuais e números referem-se a julho de 2026.

Nomes de produtos e marcas pertencem a seus respectivos donos e são usados apenas para identificação; a menção não implica afiliação nem recomendação, inclusive das ferramentas do guia de campo. Ferramentas e endereços mudam — verifique por conta própria.

Composto em Iowan Old Style.

Introdução: O Trato

Há dois tipos de pessoas dispostas a falar de cripto com você, e nenhum dos dois está falando com você.

O primeiro tipo está vendendo. Você já conhece — a Lamborghini alugada, o pôr do sol, a palavra *liberdade*; gente que descobriu que o ativo mais fácil de vender é a sensação de ter chegado cedo. Eles vão falar dos ganhos. Não vão falar do que vem depois, porque o que vem depois não está nos slides.

O segundo tipo sabe do que está falando — e escreve para os seus pares. O trabalho deles é sério, é excelente e é ilegível, porque nunca foi feito para você: é dirigido a investigadores, a equipes de compliance, a gente que já sabe o que é um nonce. Você poderia ler cada palavra e ainda assim não saber se deve ter medo.

Então existe um vão, e é nesse vão que todo mundo de fato está. Milhões de pessoas chegando a uma porta, com os vendedores de um lado e os especialistas do outro, e ninguém no meio que não esteja vendendo nem se exibindo.

Este é o livro que eu queria quando quem estava parado ali era eu.

O que isto é

Passei anos montando um catálogo de todas as formas documentadas de as pessoas perderem dinheiro nisto — centenas de incidentes, desde 2010, cada um com fonte, checado e cruzado, arquivado por mecanismo, não por drama. É gratuito, é público e não é este livro. É uma obra de referência para profissionais e vai matar você de tédio.

Este livro é o que aquela obra de referência *sabe*, contado como aquilo que de fato é: um conjunto de histórias sobre pessoas — a maioria das quais não fez nada de errado.

Não é um alerta. Não é um pitch de venda. Não é um curso. **É a coisa que eu queria que tivessem me entregue inteira, na porta, antes de eu sair inventando tudo pelo caminho.**

O trato

Aqui está o que estou prometendo, e você deve me cobrar cada item, porque um livro como este vale exatamente o que vale a pior frase dele.

Todo número aqui é verificável, e os que não são vão para o lixo na sua frente. Você vai me ver descartar minhas melhores evidências mais de uma vez, porque tenho à mão alguns números espetaculares que ganhariam qualquer discussão e que eu não posso sustentar. Se eu usar um número que uma empresa inventou porque me favorece, você não tem motivo para acreditar em nenhum outro número do livro — e estaria certo.

Todo capítulo tem um veredicto, e os veredictos não caem todos para o mesmo lado. Este é o mecanismo que faz o livro inteiro funcionar, então aqui vai ele de antemão: pego um perigo do mundo cripto, coloco ao lado da versão desse mesmo perigo que já opera na sua vida financeira comum e digo com

franqueza qual é pior. Às vezes a resposta é cripto. É cripto no capítulo dois, no capítulo sete e — feio — no capítulo oito. Se todo veredicto caísse para o mesmo lado, você deveria fechar o livro — e eu também.

Nada aqui é reconstruído. Quando não sei alguma coisa, eu digo. Há neste livro um roubo de US$ 282 milhões — maior do que qualquer outra coisa nestas páginas — em torno do qual me recuso a construir um capítulo, porque ninguém consegue estabelecer como aconteceu, e uma história com as partes interessantes inventadas não é uma história: é uma mentira com notas de rodapé.

E não vou dizer o que fazer com o seu dinheiro. Nenhuma vez. Não conheço a sua situação, não sou seu consultor, e a indústria inteira de gente que *vai* dizer é o motivo de você ter precisado deste livro.

O que você leva

Ao final, você vai saber o que uma carteira realmente é e por que a palavra é uma mentira. O que é uma chave privada, e por que doze palavras podem ser um quarto de bilhão de dólares. O que é uma stablecoin e o que acontece quando o tipo engenhoso deixa de ser engenhoso. Por que querem o seu passaporte, e o que o sistema que o exige de fato pega. Como uma memecoin é construída, segundo a segundo, para tirar dinheiro de você legalmente. O que quer dizer "limpa", e por que nenhuma moeda é.

E você vai conhecer o formato da coisa, que é a parte que não se encontra em nenhum outro lugar: **quase nada disso é novo.** O telefonema que levou US$ 243 milhões é o telefonema que o seu banco combate há trinta anos. A carteira de hardware falsificada é o chupa-cabra do posto de gasolina. A memecoin é uma

boiler room — a velha sala apinhada de vendedores empurrando ações que não valem nada —, e boiler rooms são mais antigas que o telefone. As fraudes não chegaram com a cripto. Chegaram com o dinheiro, e vêm operando, em grande escala, no lugar onde você já guarda o seu, o tempo todo.

O que a cripto fez foi colocá-las por escrito.

Esse é o argumento. Todo o resto é evidência — são duzentas páginas dela, e você pode conferir cada linha.

Uma coisa, antes do capítulo um

O medo que trouxe você até aqui está correto.

Não vou tentar tirá-lo de você e não vou dizer que isto é seguro. Os três primeiros capítulos são as piores coisas do livro e estão na frente de propósito: um homem perdendo US$ 243 milhões para um telefonema, um sistema sem botão de desfazer e uma década de corretoras que se revelaram um número no banco de dados de alguém.

Leia esses primeiro. Se você fechar o livro depois deles, é um desfecho legítimo — e o livro terá valido o que você pagou.

Mas, se você ficar, a pergunta deixa de ser *isto é perigoso* — é — e passa a ser a que ninguém faz, a única pergunta útil que já se fez sobre tudo isto:

Comparado com o quê?

1
O Telefonema

A PRIMEIRA LIGAÇÃO VEIO do Google.

Não de alguém se passando pelo Google no sentido usual da frase — a ligação ruim, o número estranho, o link que leva a algum lugar errado. O número na tela era do Google. A voz sabia do que estava falando. Havia um problema com a conta, e o homem estava ligando para ajudar a resolver.

Ao fim daquela ligação, eles tinham o e-mail e o armazenamento em nuvem dele. Ou seja: tinham tudo o que ele já havia anotado sobre o próprio dinheiro.

Uma hora depois veio a segunda ligação, e esta era da Gemini — uma corretora de criptomoedas que ele de fato usava. O homem desta ligação sabia coisas. Sabia quais contas existi-

am. Sabia mais ou menos o que havia nelas. Sabia detalhes que ninguém ligando a esmo poderia saber e que golpista nenhum tinha por que saber — e todos eram verdadeiros, porque uma hora antes as mesmas pessoas os haviam tirado da caixa de entrada da vítima.

Esse é o mecanismo inteiro, e vale a pena nomeá-lo, porque é a diferença entre um golpe que qualquer um perceberia e um que ninguém percebe: **cada etapa rouba as credenciais que autenticam a seguinte.** A primeira ligação é frágil e consegue pouco. O pouco torna a segunda ligação sólida. A segunda ligação consegue tudo.

Em algum ponto da segunda hora, no dia dezenove de agosto de 2024, eles o conduziram passo a passo pela redefinição da autenticação de dois fatores e pela transferência dos fundos para uma carteira que eles controlavam. Quatro mil e sessenta e quatro bitcoins saíram numa única transação. Duzentos e trinta e oito milhões de dólares, um clique. O total chegou a cerca de US$ 243 milhões.

É a maior soma de dinheiro já tirada de uma única pessoa na base da conversa.

Carteira não é carteira

Duas palavras naquele parágrafo — *carteira* e *saíram* — estão fazendo, em silêncio, um trabalho enorme, e, se você é novo aqui, as duas estão mentindo um pouco para você. Vamos corrigi-las agora, porque tudo neste livro depende delas.

Uma carteira não guarda nada. Nada entra nela e nada sai dela. Ela não é um recipiente. O que ela guarda é uma *chave* — um número secreto —, e o que essa chave faz é autorizar a movimentação de moedas registradas em outro lugar. Pense menos numa carteira de bolso e mais num anel de sinete: o anel

não é o patrimônio, é o que prova que uma ordem partiu de você. Perca a carteira de bolso e você perde o que está dentro. Perca o anel, e outra pessoa pode mandar vender o patrimônio inteiro.

E as moedas nunca "saíram" de lugar nenhum. Elas estão no registro, e o registro é onde a segunda mentira se desfaz.

Imagine o livro mais entediante do mundo. Cada página é uma lista de transferências — tanto, daqui, para lá, neste segundo. Quando alguém envia dinheiro, uma linha é acrescentada. Só isso. Essa é a invenção inteira. Não há contas no sentido que você conhece, nem nomes, nem agências, nem horário de fechamento. Há uma lista de quem moveu o quê para onde, e o seu saldo não é um número guardado em lugar algum; é o que você obtém quando soma todas as linhas que já mencionaram você.

Três coisas sobre o livro, e a terceira é o motivo de esta história terminar como termina.

Ninguém é dono dele. Não há empresa que o mantenha. Milhares de computadores guardam cópias idênticas e concordam, o tempo todo, sobre o que diz a próxima página. Esse acordo — alcançado por máquinas que não se conhecem e não precisam se conhecer — é o que as pessoas querem dizer quando falam "blockchain", e é genuinamente a parte engenhosa.

Nada jamais é apagado. Não se pode arrancar uma página. Não se pode emendar uma linha. Um erro não é corrigido; uma *linha nova* é acrescentada devolvendo o dinheiro — se quem o tem concordar em devolver. Ninguém alcança o passado.

Qualquer um pode lê-lo. Não "qualquer um autorizado". Não "qualquer um com mandado". Qualquer um. Agora mesmo, do seu celular, você pode assistir a cada transferência do planeta enquanto acontece — incluindo as que acabaram de roubar alguma coisa. O livro é escrito em público, permanentemente, e sempre foi.

Essa última é a propriedade mais estranha de todas as finanças, e este capítulo está prestes a mostrar os dois gumes dela de uma vez.

Porque é por causa dela que o dinheiro saiu e nunca poderia voltar — e é por causa dela que sabemos os nomes dos homens que o levaram.

O homem que perdeu

Ele era credor na falência da Genesis Global Capital e morava em Washington, D.C.

O primeiro fato não é acidental — é o motivo de ele ter sido escolhido, e inverte o que a maioria das pessoas acredita sobre como isso acontece. Ele não foi descuidado. Não era um alvo fácil. Não tinha entrado nisso porque um vídeo mandou. Era uma contraparte institucional sofisticada, que havia emprestado em grande escala a uma empresa de crédito, e, quando essa empresa quebrou, o que ele tinha a receber virou registro público.

Eles não toparam com ele. Eles o pesquisaram.

Esta é a parte mais difícil de aceitar, e o livro volta a ela: **encontrar uma vítima é um problema de pesquisa, e a pesquisa é pública.** Os autos da falência diziam quem tinha a receber. A blockchain dizia o que estava guardado e se havia se movido. Em outro caso documentado da mesma forma, os atacantes montaram sua lista de alvos varrendo o registro atrás de grandes saldos parados havia anos — uma fortuna adormecida é legível de fora, e o dono dela é um nome preso a ela em algum lugar.

A transparência que permite a um investigador rastrear um roubo é a transparência que permite a um atacante montar uma lista de alvos. Ninguém tem uma sem a outra. Isso não é uma falha do projeto; é o projeto — e este capítulo é onde a conta chega.

Todos os sistemas funcionaram

Eis o que não aconteceu no dia dezenove de agosto.

Nenhum contrato inteligente foi explorado. Nenhuma criptografia foi quebrada. Nenhum firmware de carteira foi comprometido, nenhuma corretora foi invadida, nenhum protocolo falhou, nenhum bug foi encontrado, nenhum zero-day foi queimado. Nada na tecnologia deu errado em momento algum das duas horas que levou para mover um quarto de bilhão de dólares.

Cada componente fez exatamente o que foi especificado para fazer. A carteira assinou uma transação corretamente formada, porque foi uma transação corretamente formada que puseram na frente dela, e assinar transações assim é todo o seu propósito. A rede a confirmou, porque era válida. A blockchain a escreveu em caráter permanente e a mostrou a qualquer pessoa na Terra em segundos — que é exatamente *para isso* que a blockchain serve.

Não há componente nessa pilha que tenha falhado. Há um homem ao telefone, e tudo depois dele funcionando perfeitamente.

Esta é a concessão que o livro deve antes de argumentar qualquer coisa: **existe aqui uma camada que engenharia nenhuma alcança, e é a camada à qual todo o resto está aparafusado.** Você pode guardar as próprias chaves, recusar todo custodiante, comprar o hardware, nunca tocar num site que não digitou — e o edifício inteiro ainda termina numa pessoa, que pode ouvir uma mentira de alguém que soa legítimo e conhece o saldo dela.

Os homens que levaram

Eram garotos.

Malone Lam tinha vinte anos. Nasceu em Singapura em julho de 2004 e cresceu em Choa Chu Kang, uma cidade de conjuntos habitacionais no oeste da ilha. Estudou na Unity Secondary School e largou a escola ainda adolescente para passar o tempo negociando cripto e vivendo nas comunidades online que o criaram — servidores de Minecraft e o Discord.

Com os amigos com quem dividia uma casa no Texas, ele cofundou, segundo a denúncia federal, uma coisa que eles chamavam, sem ironia aparente, de **Social Engineering Enterprise** — a "Empresa de Engenharia Social". Chegou a catorze pessoas, espalhadas por vários estados. Trabalhavam com bancos de dados hackeados, dados da dark web e e-mails de phishing, e o que faziam não era hacking. Era ligar para as pessoas.

Jeandiel Serrano tinha vinte e um anos, era de Los Angeles e atendia por "VersaceGod". **Veer Chetal**, que atendia por "Wiz", era mais novo ainda — um adolescente.

Um rapaz de vinte anos que trocou a escola pelo Discord tirou duzentos e quarenta e três milhões de dólares de um credor institucional em Washington por telefone, em cerca de duas horas, sem quebrar uma única coisa.

É essa a frase que este capítulo existe para dizer, e nenhuma parte dela é exagero.

Depois eles filmaram

Eles transmitiram o assalto ao vivo para os amigos.

Não como prova. Pela plateia. Existe uma gravação dos homens que acabavam de tirar US$ 243 milhões de um desconhecido, vendo as notificações chegarem — os alertas, as confirmações, o dinheiro entrando —, comemorando e conversando so-

bre o que viria em seguida. Foi feita por eles e para eles, pelo motivo que faz quem acabou de fazer algo enorme querer guardar o momento.

Então a gravação vazou, e virou a coisa que os identificou.

O que se seguiu foram trinta e três carros de luxo. Relógios. Boates. Viagens. Não foi uma tentativa de escapar impune; foi uma farra de gastos em público, por gente que não parecia ter pensado além daquela semana.

O FBI prendeu Malone Lam em Miami no dia dezoito de setembro de 2024, um mês depois do roubo. Um policial de folga o havia avisado de que seria preso, e, no caminho, ele jogou o celular na baía de Biscayne.

Veer Chetal se declarou culpado. Entregou para confisco quase trinta relógios de grife, um guarda-roupa inteiro e mais de US$ 36 milhões em ether. Depois, em liberdade sob fiança à espera da sentença pelo que era então o maior roubo de cripto de vítima única já registrado, teve a fiança revogada quando a promotoria disse que ele havia participado do roubo de mais dois milhões de dólares.

Ponha tudo isso ao lado do resto do capítulo, porque é a única luz aqui dentro. Este é um livro que vai gastar a maior parte das páginas com pessoas que perderam dinheiro e nunca souberam o que foi feito dele. Esta história tem nomes, idades, um vídeo, três processos criminais e um celular no fundo de uma baía.

O motivo de ela ter essas coisas é o livro de algumas páginas atrás.

Eis o que "seguir o dinheiro" realmente significa, porque não se parece em nada com o que a expressão sugere e é a coisa mais útil que um recém-chegado pode entender.

Quando os US$ 238 milhões se moveram, uma linha apareceu: *tanto, deste endereço, para aquele endereço, neste segundo*. Pública. Permanente. Os ladrões então fizeram o que ladrões fazem — dividiram em três partes e saíram correndo. Quinze corretoras ou mais. Bitcoin trocado por litecoin, litecoin por ether, ether por monero, cada vez mais rápido, cada salto feito para apagar o rastro.

Cada salto escreveu mais uma linha.

Essa é a armadilha, e ela não tem fundo. No mundo que você conhece, seguir dinheiro roubado significa pedir. Pedir a um banco, o que exige um motivo; pedir a um banco de outro país, o que exige um tratado; esperar; ouvir um não; pedir de novo. Cada salto é uma porta, e cada porta tem uma pessoa atrás que pode dizer não, e portas demais esgotam qualquer um.

Aqui não há portas. O registro não tem permissões. Um ladrão movendo dinheiro por quinze corretoras não está cobrindo quinze rastros — está escrevendo mais quinze linhas num livro que todo mundo já pode ler, e ele não pode parar de escrever, porque mover *é* escrever aqui. Ele pode tornar o caminho complicado. Não pode torná-lo privado, e não pode fazer com que ele deixe de estar lá amanhã.

Então alguém leu.

Ele não usa o próprio nome, e isso é deliberado, então usaremos o que ele usa: **ZachXBT**. Seu avatar é um ornitorrinco de desenho animado vestindo um sobretudo de detetive. Ele não é policial. Não é regulador, agente, analista de empresa nem funcionário de ninguém. Não tem treinamento algum em investigação — nenhum: nem um curso, nem um distintivo, nem um dia. Ele mesmo já disse isso.

O que ele tem é uma conta a acertar.

Ele chegou em 2017, durante o boom em que qualquer um podia vender um token escrevendo um documento a respeito, e fez o que todo mundo fazia: comprou os tokens da moda. Viu todos desaparecerem. Então, em 2018, alguém invadiu a carteira dele e levou cerca de quinze mil dólares — o que era, na época, boa parte do dinheiro que ele tinha.

E em algum ponto do rescaldo disso — o rescaldo específico que este livro passou um capítulo descrevendo, aquele sem departamento de fraude e sem ninguém para quem ligar —, ele fez algo que quase ninguém faz.

Ele foi olhar.

Não o próprio roubo. O *registro*. E o que encontrou lá foi a coisa que todo mundo tinha ouvido e ninguém tinha entendido: estava tudo lá, ainda. Cada salto que o ladrão dera, parado em público, não apagado, à espera. Ninguém tinha tirado aquilo do ar porque ninguém podia. Ninguém tinha escondido porque ninguém podia. Estava simplesmente *lá*, e estivera o tempo todo, e quase ninguém estava lendo.

Esse é o momento Michael Lewis, por assim dizer — uma pessoa percebendo algo verdadeiro sobre um sistema antes das pessoas pagas para perceber. Só que não era um insight sobre títulos hipotecários. Era mais como entrar numa biblioteca que todo mundo dizia ser um cofre.

Começou a publicar em 2021. Quando os homens daquele telefonema tiraram US$ 243 milhões de um desconhecido em Washington, ele era o motivo de ter levado um mês para nomeá-los — em vez de nunca.

Em 2025, um cofundador da Paradigm estimava o valor que ele havia ajudado a recuperar para vítimas em **mais de trezentos e cinquenta milhões de dólares**.

Um homem que perdeu quinze mil e não tinha ideia do que estava fazendo já arrancou de volta trezentos e cinquenta milhões para pessoas que nunca viu.

Sem distintivo. Sem intimação. Sem mandado. Sem a permissão de ninguém. Ele leu o que já era público — e o que ainda será público daqui a cem anos.

Ele vai voltar. O resto deste livro continua girando, discretamente, em torno do que ele descobriu.

(Uma nota, já que este livro está prestes a passar duzentas páginas nomeando pessoas. O nome verdadeiro dele consta de registros públicos — apareceu numa peça judicial, porque alguém que não gostou de ser investigado o processou. Não vai aparecer aqui. Ele pede para não ser identificado, o livro não precisa disso, e há uma certa simetria nisso: o homem que tornou visível o dinheiro de todo mundo é a única pessoa nestas páginas cujo nome não vou imprimir.)

O que este capítulo não é

Seria fácil, daqui, escrever a frase que torna isto suportável. Que ele deveria ter desligado. Que havia uma regra, e ele a deixou passar.

Ele não a deixou passar. Não houve momento em que uma pessoa cuidadosa teria percebido, porque, quando a segunda ligação chegou, ela *vinha com provas* — provas tiradas dele uma hora antes, e era exatamente por isso que estavam corretas. Ele não foi enganado por um desconhecido que chutou bem. Foi enganado por um desconhecido que tinha lido o e-mail dele.

E, quando acabou, não havia nada a fazer. Sem recurso, sem reversão, sem autoridade acima da transação, porque a transação era válida, corretamente formada, e fez precisamente o que

dizia. Ele viu US$ 243 milhões saírem de uma forma que não tem desfazer, e era justamente porque o sistema estava correto que ela não podia ser desfeita.

Uma parte foi recuperada depois — apreensões, confiscos, um guarda-roupa, uma pilha de relógios e trinta e três carros. A maior parte, não.

Esse é o medo, e o medo está correto. Não é superstição e não é invenção da mídia, e este livro não vai dissuadir ninguém dele. **Quando o dinheiro vai embora aqui, vai embora permanentemente; permanência é uma propriedade real, com um custo real, e o custo é exatamente o que parece.**

Fique com isso por mais um capítulo antes de qualquer argumento. O medo fez por merecer esse espaço.

Mas leve duas coisas adiante, porque o resto é construído sobre elas.

A primeira é que **nada quebrou.** Nem uma linha de código, nem uma chave, nem uma blockchain. O que falhou foi um homem acreditando numa voz que sabia o saldo dele.

A segunda é que sabemos os nomes das pessoas que ligaram para ele, a idade que tinham, o que compraram e onde o celular afundou.