

JAVIER FADÓN MARTÍNEZ



LA PENA DE LA ESTAFA CRIPTO



PARTE I

EL ENGAÑO DIGITAL

En un entorno donde la sofisticación del fraude escala al ritmo de la tecnología, el engaño digital deja de ser un incidente aislado para consolidarse como un sistema estructurado, diseñado para explotar vulnerabilidades humanas y tecnológicas con precisión industrial.

EL INICIO DEL RASTRO

Cómo comienza una estafa cripto y qué mueve al detective a seguirla

Toda estafa cripto comienza mucho antes de que exista una *wallet*, una transacción o un contrato inteligente. Empieza en un lugar más silencioso, más humano y, por eso mismo, más eficaz: la construcción de la confianza. No nace del caos ni de la improvisación. Nace de una arquitectura precisa, diseñada para convencer sin levantar sospechas, para parecer lógica sin ser verdadera, para ofrecer seguridad justo donde después aparecerá el daño. El fraude no entra rompiendo puertas. Entra con buenas formas, con lenguaje técnico, con estética corporativa y con una promesa que parece razonable dentro del contexto adecuado. Ese es el verdadero punto de partida. No el movimiento en *blockchain*. No el rastro económico. No la pérdida. El inicio real es una idea sembrada con precisión: esto encaja, esto tiene sentido, esto parece serio, esto podría ser una oportunidad legítima.

El gran error de quien observa una estafa desde fuera es imaginar que todo comienza con la avaricia de la víctima o con la torpeza del engaño. En realidad, las estafas más eficaces rara vez apelan a la codicia burda. Ese sería un enfoque demasiado primario. El fraude sofisticado trabaja con materiales más elegantes y más peligrosos: seguridad, oportunidad, visión de futuro, automatización, arbitraje, inteligencia artificial, comunidad, acceso anticipado, diversificación, protección frente a la inflación, pertenencia a un grupo selecto. No vende humo de manera grosera. Vende una historia que encaja con el momento del mercado y con la psicología de quien la recibe. Cuando el mercado sube, la estafa se disfraza de oportunidad. Cuando el mercado cae, se presenta como refugio. Cuando reina la incertidumbre, se ofrece como método. Y cuando la complejidad domina la conversación, el fraude se convierte en una falsa traducción accesible de un ecosistema que muchos no terminan de comprender del todo, pero al que no quieren llegar tarde.

Por eso el primer contacto rara vez resulta agresivo. No llega como una imposición, sino como una compatibilidad. Puede aparecer por redes sociales, por *Telegram*, por *WhatsApp*, por *LinkedIn*, por correo electrónico o a través de una recomendación que parece indirecta y orgánica. El mensaje inicial suele estar diseñado con precisión quirúrgica. Tiene tono profesional, pero no distante; cercanía, pero no invasión; tecnicismo, pero no oscuridad. Si el lenguaje fuese demasiado complejo, generaría rechazo. Si fuese demasiado simple, transmitiría amateurismo. El punto exacto consiste en parecer experto sin obligar a la otra parte a sentirse ignorante. De ahí el uso calculado de determinadas palabras: *blockchain*, trazabilidad, nodos, liquidez, auditoría, *compliance*, *smart contracts*, inteligencia artificial, protocolos, automatización, ecosistema. No importa tanto que quien escucha comprenda todos los conceptos.

Basta con que perciba estructura. Basta con que piense, aunque sea de forma intuitiva, que detrás de ese lenguaje hay conocimiento real. Ahí se produce uno de los primeros desplazamientos clave del fraude: la víctima deja de preguntarse si aquello está verdaderamente demostrado y empieza a preguntarse si aquello parece suficientemente profesional.

Superado ese umbral, la operación entra en una segunda fase: la normalización del entorno. El objetivo ya no es solo despertar interés, sino construir un escenario en el que invertir parezca una conducta razonable, casi natural. Aquí es donde la estafa se profesionaliza de verdad. Aparecen plataformas bien diseñadas, paneles de usuario impecables, *dashboards* con supuestos rendimientos en tiempo real, balances crecientes, históricos de operaciones, atención rápida al cliente, notificaciones, mensajes de seguimiento y una estética tan pulida que, en muchos casos, supera incluso a la de plataformas legítimas. Ese detalle no es menor. Durante demasiado tiempo se pensó que una buena presencia digital era un indicio de fiabilidad. Hoy sabemos que también puede ser la coartada visual del engaño. La interfaz no prueba nada, pero persuade muchísimo. Un panel limpio transmite orden. Un gráfico ascendente transmite estabilidad. Un soporte que responde rápido transmite solvencia. Un diseño elegante transmite estructura. Y cuando una persona percibe estructura, relaja parte de su sospecha. El riesgo no desaparece, claro, pero empieza a parecer gestionado.

En paralelo, se activa uno de los mecanismos psicológicos más eficaces del fraude: la prueba social. Testimonios, capturas de ganancias,

rankings de usuarios, comunidades privadas, supuestos clientes satisfechos, perfiles que recomiendan prudencia y precisamente por eso parecen aún más auténticos, comentarios que refuerzan la sensación de que otros ya están dentro y de que a esos otros les va bien. El cerebro humano baja la guardia cuando percibe repetición y grupo. Si muchas personas parecen participar, el sistema parece más legítimo. Si hay una comunidad, la decisión parece menos arriesgada. Si otros ya han ganado, la duda individual pierde fuerza. El estafador lo sabe y lo explota con enorme inteligencia. No necesita demostrar legalidad. Le basta con escenificar normalidad.

La primera inversión nunca suele ser alta, y no lo es por casualidad. Tampoco por generosidad. Es pura estrategia. El objetivo inicial no es maximizar captación, sino ganar adhesión. Se invita a empezar con una cantidad cómoda, moderada, casi simbólica. Lo justo para que parezca una prueba razonable. Esa primera entrada tiene una función psicológica enorme: convertir a la víctima en participante. A partir de ese momento, ya no observa desde fuera. Ya no evalúa una hipótesis. Ya ha tomado una decisión. Y cuando alguien toma una decisión, necesita que esa decisión tenga sentido. Por eso muchas estructuras fraudulentas muestran en esta fase beneficios visibles o incluso permiten una pequeña retirada. Ese gesto, aparentemente menor, es en realidad una obra maestra de manipulación conductual. La retirada parcial no debilita el fraude. Lo fortalece. Le da a la víctima una experiencia que parece verificable. Una prueba empírica. Una confirmación íntima de que el sistema funciona. Desde ese instante, la última gran barrera de desconfianza cae. La pregunta ya no es si el proyecto es real. La pregunta pasa a ser cuánto conviene escalar.

Y ahí comienza la fase de monetización verdadera. El discurso cambia. Ya no se habla de prueba. Se habla de estrategia. De eficiencia. De aprovechar mejor la oportunidad. De no quedarse corto. De no infrutilizar una herramienta que ya ha demostrado resultados. Aparecen mensajes del tipo «si con esta cantidad has obtenido esto, imagina con una posición mayor», «hay una ventana concreta», «ahora estás entrando, pero aún no estás aprovechando el verdadero potencial», «los rendimientos óptimos exigen cierto volumen». Todo está diseñado para desplazar a la víctima desde la verificación hacia la expansión. Lo más importante aquí es que el fraude sigue sin sentirse como presión. El estafador no

suele ordenar ni imponer ni empujar de forma visible. Sugiere. Recomienda. Acompaña. Mantiene la ilusión de que el control sigue en manos de la otra parte. Y esa es precisamente una de las mayores sofisticaciones del engaño: que la víctima sienta que decide libremente lo que ya ha sido inducida a decidir.

A partir de ese momento entra en juego otro factor decisivo: el compromiso acumulado. La persona ya no evalúa solo una inversión. Evalúa el tiempo que ha dedicado, la confianza que ha entregado, la esperanza que ha proyectado, la imagen de sí misma como alguien capaz de valorar una oportunidad y, en muchos casos, la relación personal o profesional que se ha construido con quien le presenta el proyecto. Retirarse no sería solo apartarse de una operación. Sería aceptar que algo no encaja. Y aceptar eso tiene un coste emocional mucho mayor del que suele reconocerse. Por eso tantas víctimas no ignoran las señales de alerta por falta de inteligencia, sino por la dificultad psicológica de asumir que su criterio ha sido colonizado. El estafador cuenta con ello. Lo necesita. Y lo explota sin necesidad de elevar la voz. Le basta con mantener la lógica interna del sistema y permitir que el propio peso del compromiso arrastre a la víctima un paso más.

Toda estafa necesita, sin embargo, un punto de ruptura. Un momento en el que el dinero deja de circular hacia la víctima y empieza a desaparecer de forma definitiva. Ese quiebre rara vez llega de golpe. Sería demasiado evidente. Primero aparecen pequeños obstáculos que parecen razonables dentro del universo cripto: mantenimientos, verificaciones adicionales, cambios regulatorios, revisiones de seguridad, congestión de red, incidencias técnicas, bloqueos temporales, validaciones KYC, auditorías internas. Nada de eso suena absurdo para quien se mueve, aunque sea superficialmente, en el entorno digital o financiero. Al contrario: todo suena creíble precisamente porque el ecosistema real ya es complejo por naturaleza. Luego llegan nuevas condiciones: comisiones inesperadas, impuestos ficticios, depósitos para desbloquear fondos, garantías adicionales, tasas de certificación, costes de liberación. Cada nuevo pago se presenta como el último. Cada nueva traba se justifica como algo puntual. La víctima entra en una fase especialmente cruel: ya no paga para invertir, paga para recuperar. Ya no pone dinero para crecer, lo pone para rescatar lo que considera suyo. Esa transición es devastadora porque transforma el criterio económico en reflejo emocional. La persona no quiere ganar más.

Quiere evitar asumir la pérdida. Y ahí el fraude ya ha colonizado por completo la lógica de la decisión.

El cierre real llega con el silencio. Un día la plataforma falla. Los mensajes dejan de contestarse. El contacto desaparece. El soporte se diluye. Los perfiles se esfuman. Los canales dejan de responder. Todo lo que parecía un sistema activo, eficiente y acompañado se convierte en un vacío. Ese silencio produce un impacto que va mucho más allá del dinero. Porque no solo confirma la pérdida económica. Confirma también que toda la estructura relacional era una ficción. Para muchas víctimas, el golpe más duro no se formula como «me robaron», sino como «todo era mentira». Y ahí se abre una herida que rara vez se ve desde fuera: no solo se ha perdido patrimonio, se ha roto la confianza básica con la que una persona interpreta el mundo, sus relaciones y su propio criterio.

Por eso es un error monumental reducir una estafa cripto al importe perdido. El perjuicio económico es solo una capa. Debajo aparecen otras mucho más difíciles de medir: vergüenza, culpa, aislamiento, ansiedad, deterioro de vínculos, pérdida de confianza en terceros y un daño serio a la imagen que la víctima tenía de sí misma. Muchas de estas personas se consideraban prudentes, analíticas, formadas, incluso expertas en determinados ámbitos. Haber sido atrapadas por un fraude sofisticado no solo les afecta financieramente. Les hiere la identidad. Y esa es una de las razones por las que tantas víctimas callan. No porque el daño sea menor, sino porque les resulta insoportable exponerlo. El relato social, además, suele ser cruelmente simplista. Se tiende a ridiculizar al estafado, a juzgar desde fuera, a decir que las señales eran evidentes, como si observar una estructura ya colapsada otorgara retrospectivamente una lucidez que nunca se tuvo en tiempo real. Pero la realidad es otra: las mejores estafas no atacan la ignorancia. Atacan la confianza. Se apoyan en deseos legítimos, en narrativas plausibles, en contextos verosímiles y en mecanismos psicológicos que afectan a perfiles muy distintos. Nadie está completamente blindado frente a una operación bien diseñada.

Es exactamente en ese punto donde aparece la figura del detective especializado en criptomonedas. No como un salvador cinematográfico ni como un tecnólogo fascinado por los gráficos, sino como alguien que entra cuando ya no sirven la intuición, la rabia ni las explicaciones simples. El detective no entra para consolar. Entra para ordenar el caos. Su trabajo comienza allí donde otros solo ven confusión. Donde

unos observan alfanuméricos, él busca conducta. Donde otros ven complejidad, él busca secuencia. Donde otros concluyen que no se puede hacer nada, él parte de una premisa distinta: el fraude puede ocultarse, pero no desaparece. Se fragmenta, se desplaza, se mezcla, se disfraza, cruza cadenas y jurisdicciones, pero deja rastro. Y mientras exista rastro, existe posibilidad de reconstrucción.

Una de las investigaciones del despacho no comenzó con una exportación de transacciones, ni con un informe técnico, ni siquiera con una *wallet* concreta. Comenzó antes, en un lugar más incómodo y menos cuantificable: la confianza depositada por un buen amigo y empresario, Iván Collado. Iván no acudió en busca de consuelo ni de frases tranquilizadoras. No quería una evaluación difusa ni una esperanza empaquetada. Tampoco buscaba únicamente recuperar el dinero perdido, aun siendo la cuantía relevante. Su objetivo era otro, más preciso y más exigente: la entrada en prisión del presunto estafador. No por venganza, sino por convicción. Porque había entendido algo esencial: cuando la impunidad se tolera, deja de ser una anomalía y se convierte en modelo de negocio.

Cuando Iván expuso los hechos, lo hizo sin dramatismo. Y esa ausencia de dramatismo era, en sí misma, una señal importante. Quien ha sido golpeado por una estafa sofisticada y ya ha atravesado la primera fase del impacto rara vez sobreactúa. Habla más bajo. Mide palabras. Ordena los hechos con una serenidad extraña, como si al controlar el tono intentara no desbordarse por dentro. Iván no preguntó qué posibilidades había. No pidió «ver qué se podía hacer». Fue directo al objetivo crítico del encargo: «Quiero que este individuo entre en prisión. Lo demás es secundario». Esa frase cambia completamente el marco. Porque una investigación orientada a condena penal no se construye igual que una investigación orientada a recuperación económica o a simple informe privado. Cambia la lógica del caso, la selección de pruebas, el ritmo, el lenguaje y la ética operativa. En ese momento deja de bastar con saber. Hace falta probar. Y no probar de cualquier manera, sino de una forma que resista un juzgado penal, un fiscal escéptico y una defensa agresiva.

Ahí es donde entra en escena el *DetectiveCripto*. No como un mero analista de *blockchain* ni como un investigador tradicional con curiosidad digital, sino como una figura híbrida, situada en la intersección entre investigación privada clásica, análisis forense digital, comprensión

profunda del ecosistema cripto y orientación probatoria judicial desde el primer minuto. Su función no es descubrir qué pasó. Eso es demasiado poco. Su función es reconstruir lo ocurrido de forma cronológica, verificable y jurídicamente utilizable. No trabaja para tranquilizar al cliente. Trabaja para que cada conclusión esté sostenida por evidencia y pueda sobrevivir a contradicción. Hay una verdad incómoda que cualquier profesional serio aprende pronto: en los tribunales no gana quien más sabe, sino quien mejor prueba.

Por eso, uno de los primeros movimientos correctos en un caso así suele ser paradójico: no hacer nada. Nada impulsivo, al menos. No escribir más al presunto estafador. No mover fondos residuales. No reenviar mensajes sin control. No improvisar una denuncia sin arquitectura. No recopilar capturas sin método. Parece antinatural, pero es esencial. En *blockchain*, cada gesto deja huella. Y cada huella mal gestionada puede contaminar el valor probatorio del caso. Una investigación seria necesita preservar integridad, contexto y secuencia. No se trata de hacer mucho. Se trata de hacer bien lo necesario.

Toda investigación con vocación penal sólida necesita responder, al menos, a tres preguntas esenciales: qué ocurrió exactamente, quién se benefició de ello y qué intención criminal puede acreditarse. Esa triple estructura obliga a trabajar en capas. La capa humana: relación previa, generación de confianza, promesas, evolución del contacto, comunicaciones. La capa técnica: *wallets*, rutas de fondos, *exchanges*, bridges, servicios intermedios, contratos, cronología transaccional. La capa jurídica: tipificación penal, dolo, ocultación, reiteración, beneficio, nexo causal. Nada se analiza de forma aislada. Todo se conecta. Porque una estafa sofisticada no se sostiene por una sola pieza. Se sostiene por convergencia.

Aquí conviene desmontar otro mito: el del anonimato absoluto. El estafador cripto no es invisible. Está oculto, que no es lo mismo. Y ocultarse exige operar. Cada operación deja un patrón. Cada intento de anonimato genera una firma conductual. Cada reutilización de infraestructura, cada salto, cada conversión, cada horario, cada secuencia de fragmentación, cada paso por un servicio concreto habla de una lógica humana. El *DetectiveCripto* no empieza necesariamente persiguiendo un nombre. Empieza persiguiendo rutina. Busca repeticiones, simetrías, errores humanos, correlaciones temporales, puntos de consolidación, infraestructuras que reaparecen. El criminal financiero moderno rara vez

cae por una gran torpeza cinematográfica. Suele caer por la suma de pequeñas costumbres. El trabajo está en saber leer costumbre donde otros solo ven complejidad.

Iván comprendió pronto una lección dura pero decisiva: saber o sospechar quién es alguien no equivale a poder demostrarlo en sede judicial. Esa diferencia separa la intuición del caso ganador. El objetivo no era convencer a Iván. Ni siquiera convencer al equipo técnico. El objetivo era convencer a un juez que no conoce a nadie de la historia, que llega con distancia institucional y que necesita ver una secuencia probatoria clara, reproducible y defendible. Por eso cada decisión se filtró por una sola pregunta estratégica: ¿esto acerca o aleja el caso de una condena penal efectiva? Si no sumaba, se descartaba. Si era neutral, se posponía. Si reforzaba, se documentaba con obsesión. En una investigación seria no hay espacio para el ego del investigador. Solo para el resultado.

Aceptar un encargo cuyo objetivo explícito es la entrada en prisión de otra persona exige, además, una ética operativa muy clara. El *DetectiveCripto* no actúa como juez ni como verdugo ni como amplificador emocional de la indignación de la víctima. Actúa como arquitecto de verdad probatoria. Si los hechos sostienen una acusación penal robusta, se avanza. Si no la sostienen, no se fabrica. La justicia no se inventa. Se demuestra. Esa disciplina es la que separa la investigación seria del activismo impulsivo. Y en casos complejos, esa diferencia lo es todo.

A medida que la reconstrucción del caso de Iván avanzaba, se hizo evidente que la verdad técnica por sí sola no bastaba. Las transacciones mostraban más que dinero: mostraban estructura. Las comunicaciones no revelaban solo engaño: revelaban método. Y el patrón empezaba a adquirir una densidad claramente penal. En ese punto apareció una necesidad estratégica nueva: convertir esa verdad técnica en una querella penal robusta. Porque la *blockchain* no miente, sí, pero los tribunales no leen hashes. Un explorador de bloques no convence por sí mismo a un juez. Un informe técnico brillante, sin arquitectura jurídica, puede quedarse en un relato interesante. La verdad técnica necesita traducción legal.

Fue entonces cuando se consolidó la colaboración con Julio Sánchez Abogados. No para «revisar» la investigación a posteriori ni para dar forma jurídica a algo ya cerrado, sino para co-diseñar la querella desde la médula del caso. La elección no fue casual. Se buscaba un despacho con tres atributos no negociables: experiencia penal real, comprensión