Case study
A client needed help with a bribery investigation involving cryptocurrency payments made to government officials. Using EY Blockchain Analyzer and EY Blockchain Forensic Investigations, the team analyzed efforts by the targets of the investigation who had disassembled and reassembled digital wallets to obfuscate payments and established profiles of parties of interest (POIs) related to possible bribes. The team also produced detailed case findings of POIs and related cryptocurrency activities that enabled targeted remediation aimed at recovering misappropriated funds.

EY Blockchain Analyzer
The explorer and visualizer tools of EY Blockchain Analyzer provide a simplified and integrated platform to review and analyze transactions on public and private blockchains. It integrates search functionality with visualization technology, allowing users to look for specific transactions, addresses and blocks to gather relevant information and to spot and track in-depth patterns and trends for on-chain data.

Working with EY Forensic & Integrity Services
• Decades of experience conducting complex financial crime investigations in 150+ countries
• Award-winning innovation leader recognized by our clients

Contacts
Todd Marlin
EY Global Forensic & Integrity Services Technology & Innovation Leader, Ernst & Young LLP
todd.marlin@ey.com

Alex Perry
Managing Director, Forensic & Integrity Services, Ernst & Young LLP
alexander.perry@ey.com

EY Blockchain Forensic Investigations
Managing financial crime risks in the cryptocurrency era
Complicating the financial crime landscape

With businesses increasingly turning to blockchain-enabled transactions, the ability to investigate wrongdoing in public and private blockchains has never been more critical. Leading-edge technologies are needed to help deliver confidence in financial reporting and identify anomalies in operational activity and performance.

Cryptocurrencies are often used in financial crimes, such as money laundering and embezzlement, making it highly challenging to detect fraud and conduct investigations. Scams made up 54% of all cryptocurrency-related crime in 2020, costing roughly $2.6 billion, according to the Chainalysis 2021 Crypto Crime Report. Ransomware payments made in Bitcoin and other digital currencies tripled in 2020 as the COVID-19 pandemic brought new security vulnerabilities to a remote workforce. Between 2019–2020, the volume of cryptocurrency transactions as a whole nearly tripled. At the same time, according to the Chainalysis report, criminal transactions were only 0.34% of all cryptocurrency activity.

As cryptocurrency use becomes more mainstream, organizations must be able to investigate suspicious transactions just as effectively as they do for traditional currencies. A case management tool that tracks and documents on-chain data systemically enables nontechnical users to identify high-risk transactions, investigate them efficiently and properly document their findings.

Challenges in conducting cryptocurrency investigations

While it’s possible to analyze cryptocurrency flows in the same way as traditional money flows, few investigators are equipped to do so. Limited access to data, lack of understanding of how cryptocurrency works and technological barriers all pose challenges. Knowledge in blockchain technology is critical to pinpoint, investigate and document suspicious transactions. Investigators need to understand the technical process and transaction method used by each cryptocurrency algorithm in order to capture and analyze relevant data.

Investigators also must work with legal and business stakeholders to carefully balance privacy requirements with the need for forensic data. A standard methodology should govern all investigative activities, information flow, stakeholder communication and documentation.

Introducing EY Blockchain Forensic Investigations

EY Blockchain Forensic Investigations, which is designed to be used with EY Blockchain Analyzer, makes it possible for internal audit teams and forensics accountants to search for specific transactions, addresses and blocks to gather relevant information. Importing on-chain data from EY Blockchain Analyzer, EY Blockchain Forensic Investigations gives investigators the ability to analyze, track and document suspicious activity in on-chain data transactions.

EY Blockchain Forensic Investigations uses a proprietary case management tool specifically configured for cryptocurrency investigation. By highlighting trends and anomalies, it helps investigators improve their capabilities to uncover and analyze potential outliers in on-chain data, some of which may be fraudulent or raise other red flags for analysis.

Built in EY Virtual Analytics Infrastructure (EY Virtual), EY Blockchain Forensic Investigations benefits from EY Virtual’s security- and privacy-by-design methodology. It has the flexibility to be deployed on premises or via the cloud, and the scalability to be implemented in multiple locations. It allows nontechnical investigators to:

- Organize transaction-based investigative processes using “case branches” that systematically track and document on-chain data for suspicious activity
- Document each case branch with contextual information while linking subsequent transactions
- Analyze on-chain data with built-in algorithms to detect linkages to suspect addresses provided by the client or contained in our proprietary fraud library
- Generate consolidated case reports, including hits to known malicious addresses and transaction inputs and outputs

How EY Blockchain Forensic Investigations works

- Gather on-chain data
- Perform analysis
- Build cases
- Consolidate case findings

EY Blockchain Forensic Investigations

- EY Blockchain Analyzer
- EY Blockchain Forensic Investigations

Case branch 1
- On-chain data
- Branch notes
- Subsequent branch link

Case branch 2
- Analyze movement of cryptocurrency assets
- Identify suspicious addresses that are associated with known hacks, third-party watchlists and the EY proprietary fraud library
- Document findings by case branch
- Identify relationships between transactions by linking case branches

Case branch X
- Aggregate case findings
- Generate case reports that show transactions’ movements using case branches

- Isolating parties and transactions of interest using EY Blockchain Analyzer
- Export transaction details into EY Blockchain Forensic Investigations for investigative analysis
- Analyze movement of cryptocurrency assets
- Identify suspicious addresses that are associated with known hacks, third-party watchlists and the EY proprietary fraud library
- Document findings by case branch
- Identify relationships between transactions by linking case branches
- Aggregate case findings
- Generate case reports that show transactions’ movements using case branches