Chainalysis
GOVERNMENT SOLUTIONS

Declaration of Elizabeth A. Bisbee

Chainalysis
GOVERNMENT SOLUTIONS

My name is Elizabeth (Beth) A. Bisbee. I am the Director of Investigation Solutions for Chainalysis Government Solutions, a wholly owned subsidiary of Chainalysis Inc., a blockchain analytics and forensic investigative firm.

Prior to joining Chainalysis in January 2021, I was the Drug Enforcement Administration's national subject matter expert for virtual currency investigations, practices, and policies. In that role, I served as the DEA's lead expert witness for virtual currency and was involved in over 400 virtual currency investigations, including work on covert operations, blockchain analysis, suspect interviews, seizure of cryptocurrency, and trial preparation and testimony. I developed the DEA's training curriculum related to virtual currency and blockchain analysis, and I have taught numerous classes on virtual currency and virtual currency investigations. This declaration is based on information that has been relayed to me by Chainalysis data engineers and data scientists. If called as a witness I could and would competently testify to the matters stated herein.

This declaration is in response to the request from the Court on June 23, 2023 for additional context as it relates to Chainalysis clustering methodology. This report also provides information related to the Chainalysis error rate.

Chainalysis Clustering Methodologies

Chainalysis clustering methodologies have not been peer-reviewed in the sense that an academic paper would get peer-reviewed with data and methodology(ies) reviewed in a separate study by other scientists. However, every single clustering heuristic in the system has been reviewed by numerous Chainlaysis data scientists, intelligence analysts, and investigators that specialize in blockchain analytics. Chainalysis clustering algorithms are based on deep scientific research in cryptography, blockchains, distributed systems, and computer science. For example, the co-spend heuristic was originally developed by Sarah

Chainalysis
GOVERNMENT SOLUTIONS

Mieklejohn, a professor of cryptography in the information security group in the computer science department at University College London[1].

Chainalysis clustering heuristics are also deterministic which means there is no randomness (i.e., the algorithm[2] will produce the same result every time); the data supporting each independent heuristic result reached in this case can be independently verified and reproduced via the blockchain. This is similar to how Chainalysis creates other clustering heuristics where a combination of facts can only lead to a single conclusion. For example, if Chainalysis conducts transactions with Exchange A on the blockchain, Exchange A must provide deposit addresses for Chainalysis to send funds. Once funds have been sent to Exchange A, the deposit addresses then sweep their funds into a single address. On the blockchain, that single address receives from thousands of other deposit addresses with no other counterparty on the sending side. This means that this address is a consolidation address for Exchange A because deposit addresses of an exchange only send funds to the internal infrastructure of the exchange[3]. Since Exchange A consolidation address has been identified, that also means that the thousands of other deposit addresses also belong to Exchange A. This conclusion is not probabilistic and the transaction pattern can be validated on the blockchain. This is also represented as an intelligence based heuristic.

The co-spend heuristic is also deterministic. If two UTXOs are spent in the same transaction, either they are controlled by the same private key or the two private keys are accessible by the same person. There are scenarios where the algorithm determining the co-spend heuristic identifies an outcome that doesn't fit this logic. This occurs when there an obfuscation technique implemented, such as CoinJoin[4]. Chainalysis has controls in place to detect CoinJoin and can skip the CoinJoin co-spends so the addresses are not clustered/associated.

[1] Meiklejohn S, Pomarole M, Jordan G, et al. A fistful of Bitcoins. *Communications of the ACM*. 2016;59(4):86-93.doi:https://doi.org/10.1145/2896384. This seminal paper has been peer reviewed and been cited by over 1,600 other papers.
[2] One way to describe an algorithm: set of rules that can only lead to a single conclusion.
[3] This is similar to a financial institution consolidating daily deposits into the bank's treasury account.
[4] CoinJoin is an obfuscation technique for combining multiple Bitcoin payments into one transaction in such a way that ownership of coins is unclear.

Chainalysis also validates the clustering and identity of named services that actually belong in the real world. This verification occurs every day hundreds of thousands of times. Chainalysis clusters centralized exchanges and other services on the blockchain that are our own customers, independent of the data they provide. For example, KYT (Know Your Transaction) customers send Chainalysis their transactions for transaction monitoring. As part of the transactions, they are provided with addresses that are controlled by them on the blockchain. Chainalysis then cross-validates the information the customer is detailing against what Chainalysis found independently through clustering and attribution.

There is also validation that occurs with other named entities that are not Chainalysis customers. Every day law enforcement agencies around the world send legal processes to exchanges identified in Chainalysis tools. If the information were incorrect, the exchange receiving the legal process would respond that the address does not match or be controlled by them. Chainalysis does not know how often this happens but this is extremely rare otherwise law enforcement customers would not be able to use Chainalysis tools to further their investigations.

Margin of Error / False Positive / False Negative

Historically, Chainalysis has not gathered and recorded in a central location false positives /false negatives because there is design to be more conservative in the clustering of addresses. In response to the Court's inquiry, Chainalysis is looking into the potential of trying to collect and record any potential false positives and margin of error, but such a collection does not currently exist.

Chainalysis
GOVERNMENT SOLUTIONS

Declarant Signature

Elizabeth Bisbee Digitally signed by Elizabeth Bisbee
Date: 2023.07.18 18:06:22 -04'00'

Elizabeth A Bisbee

