

A proposed bitcoin blockchain investigation methodology: Based on a case study approach

Botha, Johannes G; Singh, Kreaan D; Leenen, L

**Abstract**

Criminal investigations involving cryptocurrencies are still premature with no standard investigative process to follow. This paper proposes a high-level methodology using open-source and analysed data to perform such investigations. It focuses on situations where Bitcoin is involved, but where other similar blockchains are concerned, the technical investigator should apply this methodology only after careful consideration. A case study approach is used to illustrate a cryptocurrency scamming platform, a giveaway scam, and divorce fraud. In all the cases, one needs to follow or trace the funds on the blockchain, referred to as on-chain analysis. The end goal of on-chain analysis is to find a destination address linked to identifiable information obtained from open-source data platforms—such as websites, social media, or a cryptocurrency exchange. Law enforcement can then be engaged to instruct the exchange to reveal all personal and transactional information linked to the address through a subpoena. A successful investigation will result in criminal prosecution and a potential recovery of funds. To maintain familiar investigation processes, the researchers looked at traditional (or non-technical) as well as technical investigation techniques.