

*Bitcoin is a well-known cryptocurrency that is being utilised for more and more illegal transactions, making it difficult to identify money laundering activities due to its decentralised and anonymous character. Criminals use cryptocurrency to send large amounts of money while hiding their identity. It is challenging to discover illicit transactions on the blockchain due to its intrinsic anonymity and methods like mixers. Mixing services mix cryptocurrencies to hide their source, which has led to an increase in cryptocurrency-related cybercrimes. It is imperative to use a machine learning-based strategy to address these problems. The largest labelled dataset in the world, the "Elliptic Bitcoin Dataset," provides insightful information on Bitcoin transactions. Utilizing node and edge data with timestamps helps to understand the temporal dynamics of the blockchain, which is necessary for detecting criminal activity. In order to address class imbalance and overfitting, this paper presents a two-architecture framework that makes use of Temporal Embeddings and an augmentation technique. Patterns are captured via Temporal Embeddings, and class distribution is balanced by augmentation. The Temporal Node2Vec with SMOTE implementation yields a 95% accuracy rate. To sum up, this study provides a useful method for locating rogue nodes that are involved in money laundering in Bitcoin transactions. To improve accuracy and correct for class imbalances, temporal analysis is combined with augmentation approaches.*