Chapter 8

DIGITAL FORENSIC IMPLICATIONS OF COLLUSION ATTACKS ON THE LIGHTNING NETWORK

Dmytro Piatkivskyi, Stefan Axelsson and Mariusz Nowostawski

Abstract

The limited size of a block in the Bitcoin blockchain produces a scaling bottleneck. The transaction scalability problem can be addressed by performing smaller transactions off-chain and periodically reporting the results to the Bitcoin blockchain. One such solution is the Lightning Network.

Bitcoin is employed by lawful users and criminals. This requires crimes against lawful users as well as the use of Bitcoin for nefarious purposes to be investigated. However, unlike Bitcoin, the Lightning Network enables collusion attacks involving intermediate nodes and recipients. In such an attack, regardless of a sender’s actions, money is received by an intermediate node that colludes with a dishonest recipient. Since the dishonest recipient does not “actually” receive the money, it does not provide the goods/service to the sender. Thus, the sender pays for the unprovided goods/service, but the recipient can prove that the payment was not received.

This chapter discusses the forensic implications of collusion attacks with regard to lawful users because no discernible traces of attacks remain, as well as for law enforcement, where the attacks can target parties as a form of forfeiture, analogous to law enforcement “sting” operations. This chapter also discusses the potential of the Lightning Network to be used for money laundering activities.

Keywords: Bitcoin, Lightning Network, audit trail

1. Introduction

Digital currencies are increasingly being leveraged by criminal entities. Therefore, it is important for digital forensic investigators to have
detailed knowledge of how these currencies work and how they can be exploited.

Bitcoin has emerged as the de facto standard for peer-to-peer value exchange in decentralized systems. However, a key problem with the Bitcoin blockchain technology is its scalability. Several solutions have been proposed to address the scalability problem. One solution is the Lightning Network, a peer-to-peer payment system that performs smaller transactions off-chain and periodically reports the results to the Bitcoin blockchain. This chapter discusses the design of the Lightning Network and demonstrates a fundamental flaw that facilitates collusion attacks. Such an attack enables money to go astray between a sender and a dishonest recipient who colludes with an intermediate to claim non-receipt of funds. This chapter discusses the forensic implications of collusion attacks with regard to lawful users and law enforcement, along with the potential of the Lightning Network to be used for money laundering activities.

2. Related Work

Decentralized crypto-currencies is a new research field. Off-chain transactions, as used in the Lightning Network, is an emergent trend that has not been investigated adequately. However, there is no published research on the security of the Lightning Network nor is there any discussion of the digital forensic implications of its use.

The concept of a collusion attack is not new. Conspiracies involving actors in a system have been investigated before. For reasons of space, it is not possible to discuss the topic in detail; instead, a few examples are presented from the literature.

Distributed systems such as wireless sensor networks rely heavily on their key management infrastructures. If the keys are not managed properly, network nodes can collude and reveal the keys [5].

In the case of fingerprinting digital data, when users collude, fingerprints can be removed and the data can be distributed freely [1]. Another example is a collusion attack on an Android device where two applications can collaborate to escalate their access rights [2].

In the financial sector, collusion can be used to manipulate stock prices or to secure loans despite having bad credit. With so many varied examples of collusion attacks, it is important that designers of new methods of collaboration, such as the Lightning Network, understand and guard against collusion.