ARTICLE

Squid Game on the Blockchain:

Leveraging Data Analytics to Enhance Cryptocurrency Investigations

With the Netflix series "Squid Game" becoming a global phenomenon, many businesses are attempting to ride on the hype and the crypto market is no exception. Launched in late October 2021, the Squid Game crypto project gained instant popularity, and its value (SQUID) rose by more than 23 million percent, from just over a cent to $2,861.80 in three days.[1] Although the Squid crypto had plenty of red flags, including bizarre spelling and grammatical errors on its website, the price of Squid continued to swell astonishingly. However, a few days later, the Squid price collapsed from a high of just over $2,860 to effectively zero as the Squid token creators, whose identities are still unknown, pulled the rug out from their investors and made off with about $3.3 million.[2]

This type of scam, called "rug pull," occurs when developers of a crypto token attract investors, then abandon the project, and make off with the investors' money. The developers "quickly drain liquidity from the product, effectively driving the coin's value to zero."[3] Even though blockchain, which is the core mechanism for most cryptocurrencies, is advancing along with smart technology, cryptocurrency trading is not free from fraud. In fact, there are various types of risks inherent in the cryptocurrency market besides the rug pull fraud. Individuals and organisations have taken advantage of the cryptocurrency phenomenon to carry out fraudulent activities such as ICO fraud, price manipulation and Ponzi schemes. A public report shows that around $5 billion worth of cryptocurrency was associated with fraudulent activities in 2020.[4]

The growing risk of financial fraud and money laundering in the cryptocurrency market has already gained attention from regulators around the world. In Hong Kong, the financial regulators including The Securities and Futures Commission (SFC) and the Hong Kong Monetary Authority (HKMA) are reviewing regulations that govern cryptocurrency transactions as there has been increasing adoption of virtual assets in mainstream finance.[5]

[1] Cheng., Amy, "'Squid-Game'-inspired cryptocurrency that soared by 23 million percent now worthless after apparent scam", The Washington Post, Nov 2, 2021. https://www.washingtonpost.com/world/2021/11/02/squid-game-crypto-rug-pull/

[2] Ibid.

[3] Ibid.

[4] The 2021 Crypto Crime Report, Chainalysis, Feb 16, 2021.

[5] Yiu, Enoch, "Hong Kong to review rules on whether to allow retail investors trade cryptocurrency ETFs, regulator says", South China Morning Post, Nov 3, 2021. https://www.scmp.com/business/banking-finance/article/3154725/hong-kong-review-rules-whether-allow-retail-investors

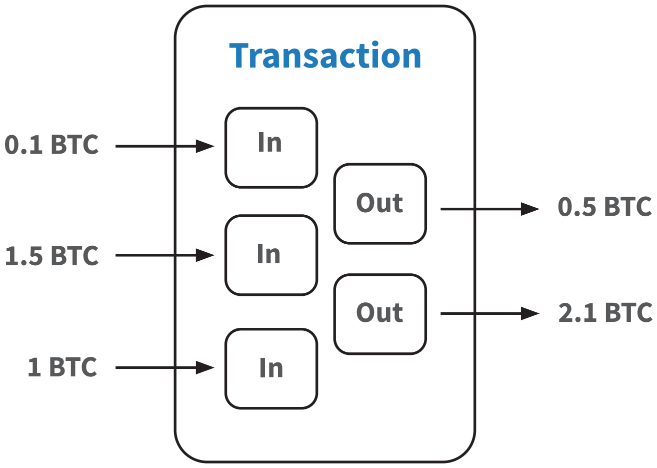
Fortunately, the accessibility of cryptocurrency and blockchain data can enhance cryptocurrency investigations. Most cryptocurrencies including Bitcoin and Ethereum are open-source, and all transactions are recorded in a publicly accessible blockchain. In regular transactions that involve fiat currencies, it is difficult to trace fund flow regardless of whether transactions were made by cash or through financial institutions. Cash is hard to trace due to its nature, and even if records exist for transactions that have been made through financial institutions, it is often hard to access the data due to authorisation issues. It is more complicated to trace funds when transactions involve multiple financial institutions due to the complexity of sharing data among institutions. However, anyone can access cryptocurrency transaction data in real-time and trace fund flows in blockchains. Although some limitations remain, such as the inaccessibility of off-chain transaction data, investigators can take advantage of public blockchain networks for cryptocurrency investigations.

Leveraging Data Analytics to Enhance Investigations

With real-time transaction data in hand, various types of analysis can be performed. In this article, we draw on three such examples, and outline the challenges and benefits of each type of analysis.

Network Analysis

Network Analysis, also known as link analysis, is a technique used to analyse and explore the association between parties. It is particularly useful for identifying hidden relationships between parties and uncovering certain anomalous transaction flows in a network. Performing network analysis with cryptocurrency transaction can be tricky due to the unique characteristics of the data. In the case of Bitcoin, unlike fiat currency, multiple simultaneous inputs and outputs are allowed in a single transaction. For instance, a single transaction can have three input addresses which contribute 0.1 BTC, 1.5 BTC, and one BTC respectively, and two output addresses that receive 0.5 BTC and 2.1 BTC respectively.



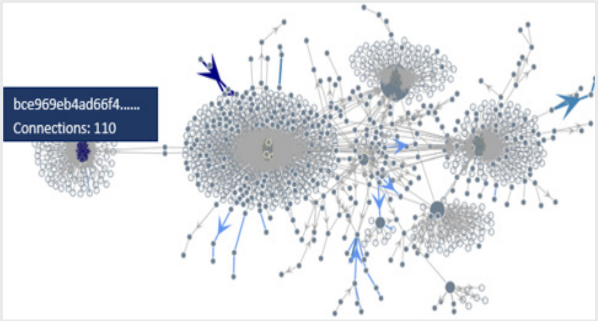
It is hard to determine, in this case, how the Bitcoin from the three input addresses were distributed to the two output addresses. This is simply one feature of Bitcoin data and each cryptocurrency has their own unique characteristics, and therefore investigators should always come up with appropriate assumptions based on the case background and their professional knowledge.

CASE STUDY

Visualising the Bitcoin Transactions

FTI Consulting analysed the most recent 10,000 Bitcoin transaction data and identified all transactions that were both directly and indirectly related to the selected transaction: ‘bce969eb4ad66f496ef9bb73b19991a8 973a692694900ff43715b0ce2e472381’. The transaction had over 1039 direct and indirect connections.

We developed an interactive visualisation graph that allows users to drill down into the transactions. The nodes represent the transactions in the network while the edges represent input/output addresses. The size of the nodes is proportional to the total number connections and the colour of the edges represents the total transaction amount. The darker the edge, the larger the transaction.



Fraud Detection with Artificial Intelligence

Cryptocurrencies are still relatively new to mainstream investors and many popular crypto exchanges have grown rapidly over the past few years. Their system may not be well-developed or compliance-centric and therefore, could be more vulnerable to fraudulent risks compared to that of traditional financial institutions. Criminals can also benefit greatly from this new sector due to the inconsistent supervision and regulations across different jurisdictions. Therefore, it is essential to identify main indicators of fraudulent crypto transactions and actively monitor them.

However, the patterns of fraudulent cryptocurrency transactions can be quite different from fiat money transactions and our previous knowledge on identifying suspicious transactions may not be applicable. Moreover, given the huge volume of cryptocurrency transactions data, human review may not be an efficient method.

Artificial intelligence can be a powerful solution for detecting fraudulent transactions in cryptocurrency networks. For example, it is possible to design supervised or self-supervised (e.g. GANs) algorithms with a relatively short list of fraudulent crypto wallet addresses in order to discover distinctive patterns fraudulent crypto transactions possess. Once specific fraudulent patterns are revealed, investigators can apply the same logic to much bigger transaction datasets to actively monitor crypto transactions that have a potential risk of fraud.

Smart Contract Review

Smart Contract, unlike what the name suggests, has nothing to do with the contract itself, but instead, is a set of computer code that runs on the blockchain. Although in theory, Smart Contract can be designed for any purpose, it is very often used to issue crypto coins or tokens. For instance, some famous crypto coins such as Tether USD (USDT) and USD Coins (USDC) were issued using Smart Contract running on Ethereum. Reviewing the source code of a smart contract can tell us whether the contract is performing what the author originally intended or whether there is hidden logic behind the contract, which gives advantages to a specific group of people. One unique feature of Smart Contract is that, combined with other techniques such as fund flow analysis, a fraud scheme can easily be revealed. Moreover, due to the nature of blockchain, the source code is immutable once it's uploaded, which could act as strong evidence in cryptocurrency investigations.

CASE STUDY

Squid Game Token

In the Squid Game token case, the smart contract associated with the token had a built-in anti-dumping mechanism that blocks users from selling their tokens. However, reviewing the source code reveals that the mechanism only allows the developers to exchange their tokens to BNB, which is a popular token with enough liquidity, so that the developers can cash out.[6] This could be evidence that the developers behind the Squid project deliberately planned to defraud their investors.

[6] Source: https://www.coinfights.legal/squid/

As cryptocurrencies are edging ever closer to the mainstream by attracting a large number of big and small investors, the fraud and financial crime risk of the entire cryptocurrency market has increased significantly. In order to fully benefit from the decentralised cryptocurrency services, it is fundamental to establish fraud investigation standards and develop forensic tools that proactively monitor high-risk activities. The creators of the crypto Squid Game wrote "[y]our experience will only reflect on the joy of winning rewards and sorrow of losing money" in their white paper[7], telling their investors that their games do not provide deadly consequences.

Regardless of whether cryptocurrencies turn out to be the digital equivalent of gold in the long run, today they are providing fraudsters with a rich hunting ground. If the risk of fraud is not reduced, it will certainly present a number of challenges for investors.

[7] Squid Game Whitepaper. https://squid.ws/SquidGameWhitepaper.pdf

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals.

FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.

ALEX WONG
Senior Director
+852 3768 4567
alex.wong@fticonsulting.com

HANNAH KOH
Consultant
+852 3768 4772
hannah.koh@fticonsulting.com