Quadriga Initiative: Recovering from a Collapsed Exchange

Matt M
matthewcomp@hotmail.com
www.quadrigainitiative.com

Abstract: The issue of collapsing exchanges is one of considerable concern in the cryptocurrency space. From the early days of Mt. Gox to modern debacles earlier this year from exchanges including the Quadriga Coin Exchange and Cryptopia, the issue of how to effectively deal with the collapse of exchanges no longer able to pay back customers is one of concern, with wide-reaching consequences. One objective of decentralized currency is operation without needing a centralized authority such as a government or court system. The use of centralized exchanges continues to be prevalent and widespread, and present methods fall short in terms of recovery speed and level of possible recovery. This paper proposes a way to resolve from the total collapse of a centralized exchange, through representation and decentralized recovery of the loss over time, given only a reliable system of validating initial claims.

1. Introduction

The adoption of cryptocurrencies has faced an explosion from their initial conception in 2008. However,

- managing cryptocurrency wallets presents a highly risky technical challenge,
- other means of obtaining cryptocurrency are prohibitively expensive (ATMs), perceived as dangerous and inconvenient (bringing cash to buy from a stranger), or technically impractical (mining), and
- most cryptocurrency users intend them as a profit vehicle that they will regularly need to buy and sell into their national currency.

As a result, new users to the cryptocurrency space typically interact with centralized exchanges as their first point of contact. Properly run and managed exchanges should in theory be able to better secure the digital assets as they are more knowledgeable and have additional resources available, however due to the large volume of currency stored there, they form effective targets for theft, both from inside and outside the organization. There are a wide range of measures which can be taken to mitigate and reduce this risk; however a complete elimination is by its definition impossible. Decentralized exchanges presently require additional technical knowledge, are more costly, and do not meet the needs of most cryptocurrency users who need a fiat gateway from their national currency. As regulation and

technology both improve, achieving a mean time between failures that exceeds the lifetime of most people is a reasonable outcome; however as long as centralized exchanges exist, this only increases the importance of an effective procedure for handling their inevitable collapse.

The traditional model of recovery centers on returning assets to their rightful owner. Part of the challenge in dealing with theft in the cryptocurrency space is that an actual recovery of the stolen assets is often not possible. Even in cases where such a recovery is possible, the costs of doing so often measure up to a large portion of the amount lost, leaving all customers with a still sizable loss. To date, there has not been a single case of theft which has been recovered in full.

What is needed is a new and decentralized approach to the recovery effort, focused on leveraging the economic power of the affected individuals and the wider community to rebuild what was lost and move forward. This approach provides for faster initial relief and an eventual full recovery.

2. Economic Power

Individuals who act in a collective manner and make group decisions towards a common goal have the power to enact considerable change. Throughout history, this has always been a considerable source of progress in humanity. Examples include unions fighting for safe working conditions and higher wages, nations fighting wars to ensure their freedom, and boycotting the use of buses in the civil rights movement. When a large number of people set their sights on a common goal and have a reasonable method to achieve that goal, it typically happens.

In situations where an exchange has collapsed, a large group of people are left in the same situation, and generally desire the same outcome of recovery. The group includes not just those directly affected but also friends and family, and empathetic individuals across the cryptocurrency community. These individuals are players in the wider market, and collectively they have a massive degree of economic power. The decision to increase or decrease interaction with other economic players can stand to massively impact the profitability of those economic players.

3. ERC20 Token Representation

A new development since the fall of Mt. Gox has been the ethereum blockchain, which allows the creation and operation of distributed application. Such applications are enormously powerful and flexible, with a key feature of creating new tokens which are guarded against 51% attacks.

An ethereum smart contract can be programmed to represent the assets lost in the collapsed exchange, enabling affected individuals to have a virtual representation of what they lost. The smart contract acts as a claim which can be recovered over time. It allows others in the wider community to identify the victim supporter community, and honour the underlying claim. Those who act in a manner consistent towards honouring the claims benefit from increased interaction with this group. This becomes a tradable token which can be bought and sold, expanding the size of the victim support community and providing liquidity for victims during the recovery process.

4. Primary Exchange

The process of determining the proper claim amounts is not covered in this paper. We assume that the amounts have been determined, whether through a court, review of a database, or some other knowledgeable body, and that all victims have had the proper chance to dispute any incorrect amounts.

The token distribution process is handled through a primary exchange. This exchange can be newly formed from among the victim community, the wider community, or be an existing exchange already in operation. The benefits to the primary exchange come from a massive boost of publicity and a large influx of new customers to use the exchange. For these benefits, the exchange has the responsibility to properly distribute tokens to victims who sign up to the exchange and file a claim, as well as facilitate trading pairs between token assets and fiat or crypto.

A democratic selection decision could be undertaken by the victim community for determining which exchange to function as the primary exchange. Depending on the size of the exchange, it may appeal to a higher degree by offering to accept tokens towards trading fees, boosting the recovery. A careful consideration of stability, transparency, and matching features should be done.

Once the primary exchange is set up, all victims have the opportunity to receive tokens representing their claim through a registration process on the exchange.

5. Decentralized Recovery

The decentralized recovery process takes place through interaction between the victim community and businesses which provide products and services. Businesses wishing to appeal to the target market of victims and supporters will accept the tokens towards purchases. This has several advantages over a traditional discount model (ie 20% off):

- Price segmentation increases revenue. As additional effort is required to complete the deal, the business retains revenue that would have been lost from customers who happily pay full price.
- Product/service value perception is maintained. The business is still “charging full price”. With a traditional discount, it is easier to see the product value as diminished.
- Brand reputation is enhanced. By focusing on the community, it represents that this business is giving back and trying to create a better future, particularly to victims.

Outside customers wishing to take advantage of the deals have the opportunity to purchase the tokens on the primary exchange, thereby providing liquidity to victims and obtaining for themselves a better deal on the product or service. The time and knowledge involved in doing this provides an effective price segment for the business, enabling it to increase revenue. Businesses can also directly measure the effectiveness of this form of promotion.

Tokens which are recovered in this way are burned, decreasing the supply over time.

6. Recovery Leaderboard

A key part of the ethereum contract is a burn function which can be invoked once a token has been recovered. This information indicates which business is responsible for the recovery and is publicly accessible via the blockchain.

One simple implementation of the burn function is to have the tokens sent to a vanity address which is zero-padded and impossible to generate a private key for. This address can be obtained by applying a custom base 38 to base 16 (hex) function to the domain name, with the digits 0-9, then a-z, then period (.), and then slash (/) as the digits to be converted. For example, the domain “example.com/hello” would send to ethereum address:

0xE89A9ADCD67E29CE834BEA000000000000000000

Leaderboard clients could then decode the business name to determine which domain is behind the promotion. A maximum length requirement would be established to allow clear recognition of burn addresses and prevent their likelihood to have associated private keys.

By maintaining a leaderboard, this information can be made easily accessible to the general public, rewarding those businesses which take leadership towards the recovery with increased business and recognition going forward. Victims can use this leaderboard when making future purchasing decisions, taking advantage of their tokens to obtain the best discounts.

The leaderboard information is publicly visible on the blockchain, allowing for independent analysis and verification. Multiple websites can maintain leaderboards, providing a competitive advantage to increase the usefulness of the information.

7. Deliberate Token Burn

One of the limitations of the approach is that businesses wishing to appear to have recovered large sums of money may do any of the following:

- Purchase the cheap tokens on the exchange and burn them directly without running any promotion.
- Accept tokens at a value other than face value. For example, charge 100 BTC worth of victim tokens to purchase a $10 item.
- Encourage victims to directly burn tokens.

It is important to note that such actions still decrease the supply of tokens, thereby increasing the value of all tokens towards face value. In every case, some individual or entity is letting go of their claim for the full amount. However, it does pose a threat to the usefulness of the leaderboard. The system is most effective if all businesses accept tokens at face value.

As the leaderboards are privately maintained, it is up to the discretion of each leaderboard to decide their rules for inclusion, and what best meets the needs of their users. Leaderboards can maintain lists of active and useful offers, filtering out known or detected businesses that aren’t providing ongoing value, which will increase their usefulness and following. As the primary benefit to businesses is towards their reputation and getting their brand out, there is a significant benefit to following rules which are maintained by the leaderboards.