GenesisEX: Next Generation Digital Currency Exchange

http://GenesisEX.com/
contact@GenesisEx.com

Abstract

GenesisEX builds the next generation digital currency exchange. It offers several new features to improve the security and transparency. In addition, robo-advisors allow automatic digital currency portfolio rebalancing, and social trading allows investors to trade with traders.

1. Introduction

World's first and most traded digital currency bitcoin was invented by an unknown programmer, under the name Satoshi Nakamoto. Since then, the digital currency marketplace grows to a 150 billion US dollar market capitalization as of 2017. Many new and promising digital currencies appear, such as Ethereum, Ripple and Monero.

Digital currency exchanges appeared since 2010. However, they often fail due to various security breach. In essence, digital currency is hacked when hackers steal private keys. In other cases, digital currency could be lost if a deposit address is replaced by hacker's own address.

2. Security

2.1 Depositing address file MD5 hash

No website is 100% secure if it is connected to the Internet. When user deposits the digital currency, exchanges are providing a deposit address and control the private key. But if the website is hacked, the hacker could change the source code and replace the deposit address.

Deposit address file contains all pre-generated deposit addresses. When a user requests depositing, one unused address is provided. Users can verify if the provided address is in the deposit address file. The MD5 hash of the deposit address file is published on our website. Users can download the deposit address file and calculate the MD5 hash to verify the integrity. A custom software monitors the web page which publishes the MD5 hash. If this hash is changed, the website will be shut down for safety.

2.2 No private keys on the public server

At GenesisEX, no private keys are stored on the public server, and hence no digital currency will be lost. Deposit addresses can be considered as cold wallets. All private keys are stored offline. The deposit and withdraw information are pulled from websites and processed offline.

The goal here is to make digital currency safe even if our online servers are compromised. Deposit and withdraw actions are not time critical, as transactions themselves need to be confirmed for several blocks. It is not necessary to maintain hot wallets to achieve the deposit and withdraw feature.

2.3 Circuit breaker mechanism

Digital currency exchanges often suffer DDoS attack. Just before the website becomes inaccessible, if a large sell order is replaced, it could trigger a cascade of liquidations. On May 7, 2007, Kraken was attacked. The Ethereum price went from around $90 to a bottom of $26, in effect liquidating everyone with a long position. On June 21, 2007, Coinbase was attacked. Ethereum's order book at Coinbase's GDAX was completely obliterated as someone sold millions of dollars worth of Ethereum at market price, leading to a cascade of 800 stop orders and margins, sending Ethereum's price to ten cent.

Circuit breaker is used to prevent market flash crashes. It prevents both speculative gains and dramatic losses within a small time frame. As a result of being triggered, circuit breakers stop trading for a small amount of time.

For example, 10% change in price within a 5-minute window will trigger a trading stop for 5 minutes.

2.4 Simulated market order only

A large market order is devastating to the market if the trading engine blindly takes the market. GenesisEX's market order is a simulated market order. It only hits the best bid and offer, keeps the remaining order on the order book and pauses the order sweeping for a fixed amount of time, e.g, 100 ms. This time interval allows other market participants to submit their new orders.

2.5 Capped limit order only

A large limit order is devastating to the market if trading engine blindly takes the market. GenesisEX only accepts capped limit order with limit price crossing the best bid and offer within, e.g. 5%, of the last trading price. For example, if the last trading price is 10, the limit buy price cannot higher than 10.5 and the limit sell price cannot lower than 9.5.

3. Transparency

3.1 Real time total user balances and published cold wallet address

Digital currency exchanges often fails.

In February 2014, Mt. Gox suspended trading, closed its website and exchange service. Mt. Gox announced that approximately 850,000 bitcoins belonging to customers and the company were missing and likely stolen, an amount valued at more than $450 million at the time. The amazing thing about the Mt. Gox incident was not just the number of lost bitcoin, but by the extent of negligence by the company. Investigations into the company showed that it had been losing bitcoins since 2011 in minor failures. In fact, it was not a single hack that led to the loss of the bitcoin, but small amounts being stolen by hackers since 2011. It is not possible to know whether Mt. Gox knew of this, but the company did not have as many bitcoins by 2013 as it thought it had. It was only the mass panic and withdrawals by clients in 2014 that made people aware of the fact.

Bitfinex, which replaced Mt. Gox as the world's largest bitcoin exchange, lost $72 million in bitcoin in 2016.

Study (http://fc13.ifca.ai/proc/1-2.pdf) shows that online bitcoin exchanges have a failure rate of 45 percent, with customer balances often wiped out.

We aim to build world’s most secure and trustable digital currency exchange. In case a security breach happens, this information will be delivered to the public in real time by publishing the real time total user balances and our cold wallet address.

4. Insurance Fund

Although security is our first priority to run GenesisEX, we still cannot guarantee it is a 100% secure. GenesisEX plans to set up its own insurance fund in case of the loss of client funds. 20% of the transaction fee will be reserved for our insurance fund. The cold wallet address of the insurance fund is open, so everyone can check the account balance on the blockchain.

5. Robo-advisors

Robo-advisors provide portfolio management online based on mathematical rules or algorithms. These algorithms are executed by software and thus financial advice do not require a human

advisor. The software utilizes its algorithms to automatically allocate, manage and optimize clients' assets.

GenesisEX continuously monitors our Clients' portfolios and periodically rebalances them back to the Clients' target mix in an effort to optimize returns for the intended level of risk.

6. Social Trading

GenesisEX allows Members to

- Share their investment activity with others, or
- Utilize the investment activity of others in their own investment portfolio.

Registered users ("Members") can choose to share their personal investment activities by becoming a Manager ("Managers" or "Traders"). Managers license their portfolio holdings and trading record ("Trade Data") to GenesisEX. Members may choose to subscribe to Manager's Models as a client of GenesisEX's investment management services ("Client" or "Investor"). Under such a relationship, when a Manager places an order, GenesisEX automatically places orders for the subscribing Client. One aggregate order across the Manager and all subscribing Clients is sent to the trading engine. In such event, the average price of the digital currencies purchased or sold in such a transaction may be determined and a Client may be charged or credited, as the case may be, the average transaction price. GenesisEX uses its proprietary computer algorithms to assess the risk of the order and approve/reject the order.

7. Free Independent Report

GenesisEX accepts digital currencies traded on our platform independently. GenesisEX will not accept any compensations to list a currency. We publish free independent report from our analysts. Only the most promising and interesting digital currencies will be listed. We stand out as the first screen for your investment. We plan to list Bitcoin, Ethereum, Ripple and Monero during our beta test.