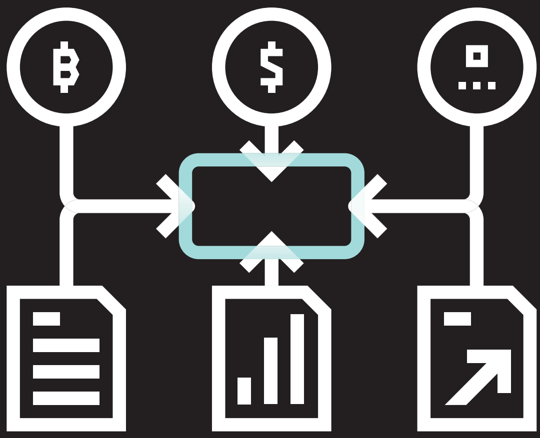
CYBERIAN
Trustless matching of digital assets

Off exchange liquidity venues Crypto Trading with Zero Information Leakage, Guaranteed



INTRODUCTION

Off-exchange liquidity venues have been widely used by institutional investors to keep large trades confidential. Although they are not perfect and can be gamed by high frequency traders, off-exchange alternative trading systems (ATSs) remain popular in equities. They are starting to see traction in the cryptocurrency sector, prompting industry participants to seek out more advanced, institutional-grade tools to most effectively trade “in the dark”. For investors concerned with order information leakage, there are platforms that are engineered to prevent this critical pain point.

OFF-EXCHANGE USE IS ON THE RISE

Recent data from Tabb Group reveals that the share of US equities trades off-exchange ticked up from 34.7% in December 2018, to 38.6% by April 2019. This trend is also being mirrored in Europe where trading within off exchanges accounted for 9.6% of all on-exchange activity for the same period . According to a report in The Trade this is the highest it has been since October 2017, before MiFID II implementation, and a jump from April where off-exchange trading volumes accounted for 9.1% of activity.

In the burgeoning crypto sector, take-up is also increasing. Research firm Aite Group estimates that 65% of all cryptocurrency trading volume will happen in the OTC market in 2019. This is a significant increase from 2016 where OTC activity only made up 32% of trades.

WHY OFF EXCHANGE?

For hedge funds and institutional investors, off-exchange liquidity venues have been traditionally used to make large block equity trades private until that trade is executed. This allows for optimal pricing to be achieved and provides safeguards against impacting the market by signaling an intention to trade . There are now around 30 equity off-exchange venues in operation with some of the biggest being run by big-name banks including UBS Group AG and JP Morgan and a growing group of crypto off-exchange pools are emerging to meet demand from investors.

Despite their expanding popularity for both crypto and equities, there is a trade-off that comes with using off-exchanges which investors must consider. The lack of transparency that is associated with these private platforms is often cited as a potential problem because it is perceived to affect the ability to get the best price. In his bestseller “Flash Boys: A Wall Street Revolt” author Michael Lewis lays out some of the predatory tactics used by HFTs to front-run large block trades performed in off-exchanges.

Order information leakage is another perennial concern for institutional investors and the use of off-exchange pools has been touted as one solution to this. However, even here problems can arise as off-market trading still requires investors to expose their order flow to one or more third parties who may either intentionally or unintentionally leak the information or act upon it.

SOLVING THE PROBLEM OF INFORMATION LEAKAGE

With the intention of solving this problem, TORA, the provider of the industry’s most advanced cloud based trading technology has partnered with Partisia, a world leading provider of multi party computation solutions (MPC) to create a new firm called Cyberian. Cyberian enables institutional investors to trade cryptocurrencies such as Bitcoin (BTC), with zero information leakage at superior prices to what could be achieved on exchanges or with OTC desks.

What sets Cyberian apart from other crypto trading venues on the market is that no single machine or entity is trusted with an order’s data. When you send an order to a third party for matching, you can never really be sure who’s looking at, analyzing, or talking about it. You are forced to trust the third party and take a leap of faith that all the proper controls are in place and working to prevent both intentional and unintentional leakage of information about your order. With Cyberian, this becomes a problem of the past.

Cyberian leverages Multi Party Computing , a field of cryptography first developed in the 1980’s. Using MPC, Cyberian breaks order data into fragments and distributes them to Cyberian nodes. Collectively, Cyberian nodes operate off-exchange pools using an MPC protocol called MACE to perform the matching of orders without having to reveal their own data to each other, ensuring that it stays private even if a node is compromised or doesn’t follow protocol.

As part of its value proposition the MACE protocol employs active security which checks every low-level operation executed for “cheating,” without revealing the results of that operation. If cheating is detected the protocol aborts and the pool operator is alerted. Additionally, the MACE protocol has built-in fault tolerance and can continue to function when a node goes down and resume seamlessly when the node comes back up.

HOW DOES CYBERIAN WORK?

Cyberian's workflow covers three activities: matching, settlement and post-trade.

For matching, investors send encrypted and digitally signed orders to Cyberian nodes. Since the order data has been broken into fragments, individual nodes are unable to glean any information about the orders such as quantity or limit price. The Cyberian nodes collectively operate the matching engine where orders are matched at benchmark prices such as the market midpoint. Nodes are operated by partners who are vetted by Cyberian and receive a share of system revenue in exchange for running a node. Orders are matched at random intervals making them less susceptible to gaming and adverse selection.

In another key point of difference from other off-exchanges, Cyberian users can choose their own settlement parties when submitting an order. This could include OTC desks, exchanges, or brokers with whom they have an account, and orders will only be matched with other orders that have at least one designated settlement party in common.

A key criticism of off-exchange venues has been their inherent opacity. To provide our clients the best possible platform for trading blocks of digital assets, using blockchain technology Cyberian makes a tamper proof record of all price and trade data available, Independent analytics providers can use this data to post-trade analytics and perform toxicity or reversion analysis to demonstrate Cyberian fill quality.

CONCLUSION

While off-exchange pools have been used in equities since the 1980s, crypto investors are now seeing their value as the sector rapidly evolves. While OTC trading desks and off-exchange venues have become a boon for those wanting to execute large block crypto trades, it remains important that institutional investors use tools that have the proper controls in place to prevent information leakage and guarantee data safety.

The new off-exchange platform starts to address some of the industry's most important liquidity and data privacy issues. With the launch of Cyberian, institutional investors now have a secure place to execute their large trades in an environment that not only meets their infrastructure standards but also enhances liquidity.

CYBERIAN

To arrange a demonstration, or for more information,
contact a sales representative at sales@cyberian.digital