RouteCoin

Collateralized, blockchain enabled, aggregation of hidden liquidity

Ian Weisberger, David Weisberger
(ian, dave @coinroutes.com)
Draft 1.0, January 18, 2018

Abstract

The market for trading crypto-assets is fragmented and institutions seeking to trade in large size can either pay significant costs trading with market makers, or risk significant price impact when their orders are seen by other traders in the market. As a result, institutions will adopt strategies that attempt to hide their full trading interest and utilize hidden and reserve order types. This is how institutional traders in the equity market evolved after that market went fully electronic. In the equity market, however, that evolution led to a proliferation of both hidden order types on displayed markets as well as dark pools. The result has been that finding liquidity has remained challenging, particularly for less liquid assets.

CoinRoutes is building a network[1] that will re-aggregate hidden liquidity, where institutions using the smart order router (SOR) will be able to optimally find the other side of trades. Once the CoinRoutes network has developed a critical mass of participants, it will be opened up and a new blockchain will be introduced to log all routing messages. The network will be made available to any firm running an SOR that is willing to stake the required amount of RouteCoin as collateral and agree to the rules of the network. Failure to comply with those rules, which are designed to prevent the leakage or abuse of market moving information, would trigger forfeiture of some or all of the RouteCoin stake, with the proceeds distributed to the participants that detected the breach of compliance. We believe that the use of an immutable, distributed blockchain to create an audit trail along with the incentives created by the RouteCoin should create a superior network. Critically, network participants on both sides of the market can find more liquidity with confidence that their trading interests will remain confidential, except when a trade can result. This would be a superior market structure, that would be a model for all electronically traded assets.

[1] See CoinRoutes: Distributed, Intelligent Network Services for Trading Cryptocurrencies

Introduction

The development of electronic markets in other asset classes is instructive to the likely future for trading crypto-assets. While there is a clear opportunity for blockchain technology to improve trading, it is equally true that the evolution of a robust market requires the interaction of disparate investor and trader types. It is no longer required for such interaction to take place in the same physical place (such as under a tree in the southern tip of Manhattan), but there is a need for buyers and sellers to interact on an informed basis, without fear of market manipulation. The structure of modern markets includes different modalities of price dissemination, anti-manipulation supervision, and an array of order types across linked markets to provide different trading methodologies. It is important, therefore, to understand basic market structure principles before explaining how the RouteCoin network can improve those markets.

Order vs Quote driven markets:

In the case of non-unique financial assets, whether crypto, equities, fx, or bonds, there are two basic ways markets are organized: Order and Quote driven markets. In order-driven markets, such as the dominant platforms for equities, futures, listed options, on-the-run-treasuries, and new FX platforms, there are displayed order books where trades occur when orders interact. In dealer markets, such as the dominant corporate bond markets, big bank platforms in FX, OTC equity platforms, and the majority of ETF trading in Europe, either quotes are displayed for “standard” sizes or they are requested by clients on demand. All trading happens with dealers and orders do not interact, except when dealers choose to match them as a service.

What is interesting about these market types is that they can and do co-exist in many cases. Dealer markets for larger than normal sizes exist to support institutional demand for immediacy, but, in general, when there is sufficient investor two sided interest, order based markets tend to win out. The reason for this is simple; matching orders is a relatively inexpensive thing to do, and has little risk to the platform. Dealers, however, who must commit their own capital to provide liquidity to customers that demand it, must charge for the market risk that they take. As a result, in traditional financial markets, it is relatively straightforward to understand why market structures have evolved the way

they have. In crypto trading, however, there are other considerations, notably about security.

Crypto investors should care a lot about security, as their assets are much more vulnerable to theft than other financial assets, most of which are “protected” by the institutions that trade them or the settlement mechanisms in use. Crypto assets, however, can be stolen, and once taken, the investor typically has little recourse. Thus, the fact that many individuals have chosen to “trust” large firms like Coinbase with their assets is understandable. This is particularly true with news of exchange hacking events. Coinbase, however, only runs one order book, on their affiliate exchange called GDAX, and that market does not necessarily offer the best price to transact at any point in time. There are other exchanges that provide a similar service to GDAX, with five others offering US residents the ability to transact in BitCoin vs US Dollars, for example.

Accessing those six exchanges, before CoinRoutes, is not something that most investors have the capability of managing, however. Thus, in addition to the ease of using Coinbase as a sole provider, dealer platforms are emerging such as Cumberland, OmegaOne and others. They offer a service to institutions who want to transact in larger size and want an immediate execution. They charge a fair premium for that service however, so institutions seeking to lower their cost of trading will need to evolve with the market structure.

Price Discovery vs Cost Control

Many academics like to argue that the primary function of markets is price discovery, defined as determining the price of an asset by matching supply and demand at every point in time. We, however, prefer to say that the most important function of secondary markets is the efficient matching of buyers and sellers, where both can minimize their cost of transacting. The difference between the those views is that price discovery is a worthwhile goal of markets, but it depends upon one’s point of view. To illustrate, consider the following example:

> An investor decides that their portfolio should increase their holdings of BitCoin by 2000 BitCoins. At the time they make this decision, there are roughly 10 BitCoin available on all displayed markets within .05% of the current offer price.

> If, for example, the investor were to bid for all 2000 BitCoin at the prevailing price, the most likely outcome would be that the price would move higher without buying much. A subsequent attempt to buy would then cost more, regardless of the method employed.

In that example, the investor telling the market that they were planning to buy 2000 BitCoin made it more expensive to trade, but the function of price discovery worked well. The increased demand, was reflected quickly in the price, but that did not help the investor.

In real world trading situations, however, investors seek to conceal their trading intent, in order to reduce the market impact such information could cause. As a result, investors, their agents, and markets invented new ways for them to do so, including dark pools and hidden and reserve orders.

Evolution of Dark Liquidity & Fragmentation

When electronic trading started to evolve in the US equity market in the 1990s, the dominant market players had large sales and trading desks which attempted to match buyers and sellers using their relationships and were heavy users of the telephone to negotiate trades. As electronic trading volumes increased and the pace of trading quickened, it became very difficult to combine electronic trading with telephone negotiation. The result was that most brokers developed their own crossing networks, which became the first dark pools. Over time displayed markets in the US also added hidden order types and independent dark pools were formed in order to service the institutional demand. Most of these pools registered as Alternative Trading Systems (ATSs), which is a less regulated form of market. Lastly, market makers decided to offer their own liquidity electronically, although such systems are not typically registered as ATSs. The result is that, in equities, there are over 50 markets for trading US equities with 13 exchanges, several market maker systems and a host of ATSs.

In order to overcome the fragmentation of the market, many firms have tried various strategies for aggregating dark liquidity, but with limited success. Algorithms are used to guess which pools have orders, and some of these are better than others, but none are close to perfect. The problem is that investors placing orders in dark pools only want to interact with bona fide orders on the other side of the market, and don't want their trading interest to become widely known, lest that knowledge create market

impact. The result, of course, is that many potential trades never happen in the dark, and both sides experience higher costs of trading. There was one solution to this problem that showed a lot of promise, but it only operated for a few years.

The idea, created by a company called Lava Trading in the middle of the last decade, was internally called “darkbook” and it relied upon the fact that the Lava Smart Router had a “memory.” The system, which in its heyday, handled over 10% of aggregate trading volume, remembered the full size of orders posted to exchanges and dark pools and used that knowledge to route subsequent orders on the other side against them. The result was that the Lava Router achieved much better execution rates than other routers. Unfortunately, due to a number of reasons, Lava lost market share steadily and there were issues with regulators, caused primarily to an inability to prove that the router memory was *only* used for the purpose of subsequent routing. The RouteCoin concept borrowed from that experience, and, with the introduction of new incentives, the ability to audit the process, and, most important, the availability of the network to any SOR that wants to join, should form a lasting solution to the dark trading and liquidity fragmentation conundrum.

The RouteCoin Enabled Network

The key to the RouteCoin enabled network is a combination of incentives and the ability to verify proper behavior. As explained in the CoinRoutes whitepaper[2] the vision is to build an informed network to facilitate the interactions of investors and exchanges in a distributed manner. The design of this network is such that trading firms, asset managers and software providers will want to participate in order to garner the network effect benefit of matching undisplayed interests of firm counterparty orders. This benefit will dramatically reduce the cost of trading institutional sized orders and can only be enabled by the use of a proof of stake, blockchain enabled protocol, with the appropriate incentives as described below.

To accomplish this, CoinRoutes will create an open source blockchain to document the audit trail among components in the network, and establish a protocol for distributed operators of enhanced market data. Operators of enhanced market data nodes, which

[2] CoinRoutes: Distributed, Intelligent Network Services for Trading Cryptocurrencies, Jan 15, 2018

will be limited to firms that attest to not running a trading operation[3], will be required to stake routecoin to operate the node, but will collect "gas" in routecoin for handling the data requests and performing the audit trail and TCA functions that ensure that SOR operators remain in compliance. The individual market data nodes, however, will not have all order information, as the new order function will be allocated based on individual SOR preferences. While SORs will request information from aggregator nodes, which will request market data from all nodes hosting the book of the product being traded, they will only send the specific order details to one or more of the aggregator nodes. This separation will facilitate the ability of participants, with access to the audit trail to statistically analyze if particular nodes are creating excess market impact from knowing about hidden orders. That will be a basis for voting on the penalization of the RouteCoin stake of those operators.

When both the SOR and aggregator nodes request market data from all nodes, however, the market data request protocol will always ask for both sides of the market for the quantity requested. This will make it unprofitable for enhanced market data node operators to front run the orders making the request. The request, however, will be logged to the blockchain with a delay (sufficient to make the information not able to impact the market), and will be for the actual quantity. If nodes detects that the request was for a quantity larger than the logged quantity on the order, that would also be indicative of out of compliance behavior.

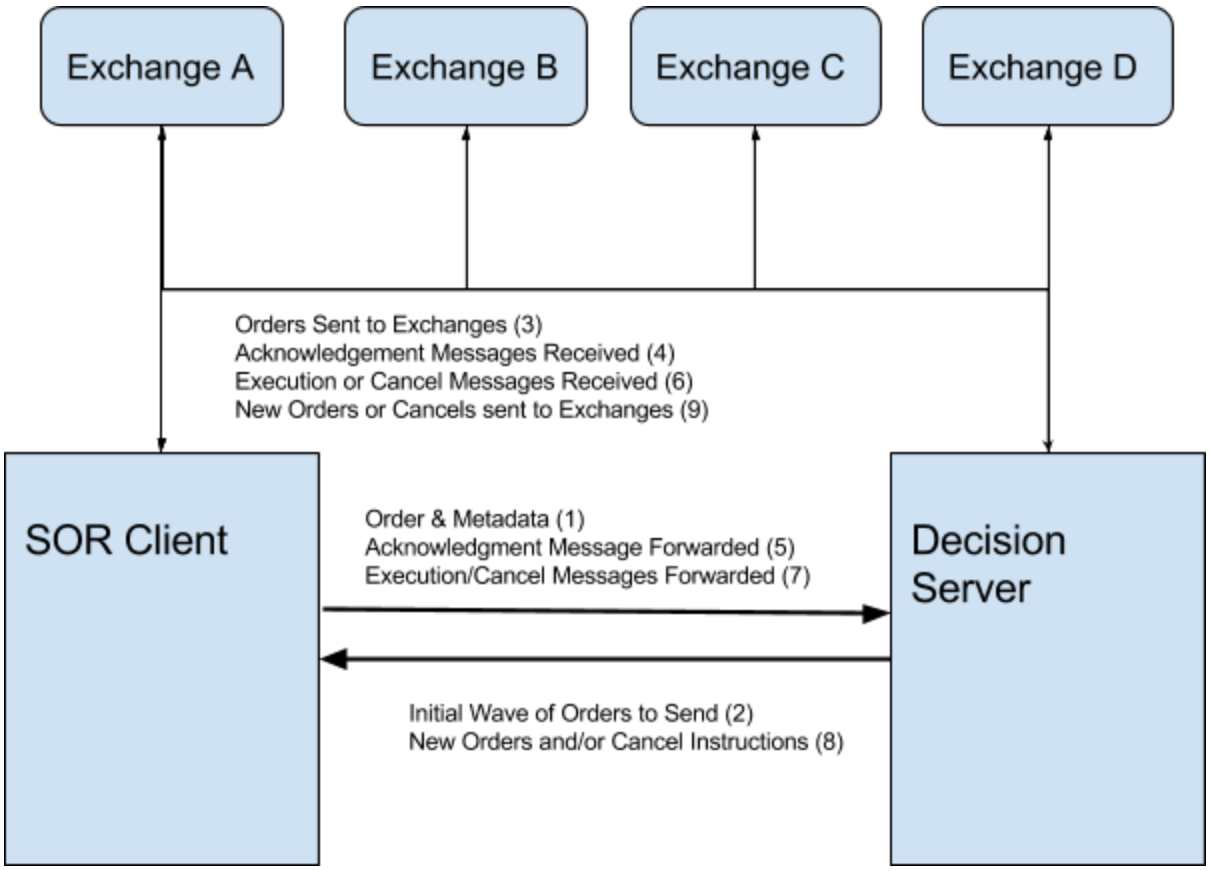
SORs will also need to post a required amount of RouteCoin to the network to gain access to the distributed enhanced market data service described above. This, however, requires that all SORs, with or without separate Decision Services on the network document all relevant transactions to the new blockchain, in order to prove compliance. The goal is to ensure that all orders submitted to the market data service that *could* show where there might be dark liquidity, are bonafide orders that were actually sent to the markets as instructed.

In order to facilitate this, CoinRoutes will develop basic TCA logic to be executed by all nodes on the network to detect front-running or bad behavior. If front-running is detected and successfully voted on, the cheating nodes stake will be slashed and distributed to the honest nodes as well as the node(s) that detected the behavior. This is the unique value proposition of the RouteCoin token, as the network it enables should be able to maximize price discovery and routing efficiency while also self-policing "bad"

[3] This attestation essentially means that enhanced market data nodes can only be operated by agents and not those firms operating SORs for their own use. This mechanism is intended to be enforced via voting, but will also be subject to regulatory directives.

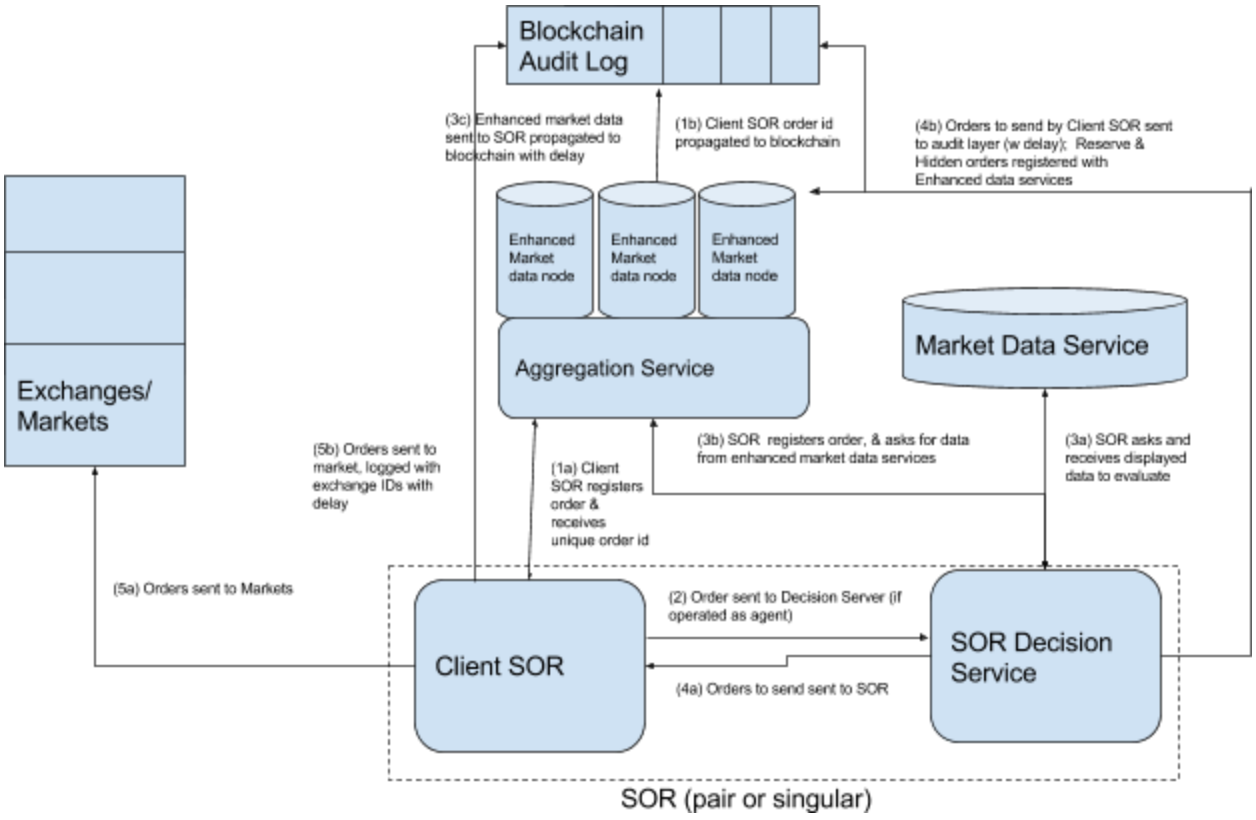
behavior. There is no reason to limit this methodology to trading of crypto-assets exclusively, although that will be the focus of the network for the first few years.

To illustrate how this will work, consider first a simple overview of the message traffic in the CoinRoutes system.



In this diagram, one can see that the SOR client must send a client order to the decision server in order to be told what orders to send, and that each step of the process includes synchronization between the two components. The market data for the dark liquidity, in this system, only gets communicated to the SOR in the form of instructions of orders to be sent to exchanges & markets. Thus, if all market data requests for dark liquidity were also synchronized and logged, the system would have enough information for parties on the network to detect possible bad behavior.

To accomplish this, the system flow for the RouteCoin enabled network will add to the functions of the coinroutes network, a blockchain recorded audit trail, as well as a aggregation layer for the enhanced/distributed market data, as depicted in the following diagram:



An example of dark routing in action

An order is sent to SOR-A to buy 100 BitCoin via a method that prioritizes posting rather than taking liquidity and the SOR determines that the best way to do so is by posting 10 to buy on an exchange and posting 90 on a crypto dark pool. These orders are sent to the market and the 90 BitCoin sent to the dark pool is registered with an enhanced market data node.

Some time later, an order to sell 50 BitCoin is received by a SOR that is on the network. It decides to aggressively sweep the market and requests both displayed and enhanced market data. Since the 90 on the crypto dark pool would be the optimal, it routes all 50 to the dark pool for immediate execution. Once executed, the SOR would finish the logging of its order and market data request history.

At this point, the original buy order gets filled on the displayed exchange and the router, having 40 BitCoin left to do, determines to post another 10 on the displayed venue. Before doing so, it must either cancel or reduce the remaining quantity on the dark pool. This logic continues until the order is complete.

How does the RouteCoin Network Incentivize Good & Punish Bad Behavior?

We believe that there are 6 key "bad" behaviors that need to be disincentivized:

1) SORs that request enhanced data and don't sent orders (a.k.a. Spoofing the system to learn about hidden liquidity)
2) SORs that request enhanced data and change the order they are routing after receiving the data by using misleading timestamps (a.k.a. Using the data to influence the buy sell or quantity decision)
3) SOR colluding with Enhanced Market Data Nodes (EMDNs) to falsely log orders so that the SOR can do either 1 or 2.
4) EMDNs that leak info about hidden orders to trading firms so they can trade on that information.
5) EMDNs leak initial orders when registered to trading firms so those orders could be front run
6) Enhanced Market Data Aggregators disseminating overage quantities to trading firms so they can trade on that information.

To handle numbers 1 and 2, the EMDNs can do both real time TCA to detect this type of behavior and other network participants can compare market data to the logs on the blockchain. The SORs, if they don't log their behavior and the EMDNs do, will be clearly judged guilty, and the same goes for mis-logging.

In order to prevent collusion, the network will require that SORs register their orders with multiple EMDNs. The number of EMDNs required for this will grow with the size and number of participants on the network.

To prevent EMDNs from leaking hidden order information or from leaking real time information, the SORs have an incentive to perform TCA on their flows and the fact that the EMDNs do not all receive the same information means that statistically, EMDNs that are doing this will look far worse in that analysis.

The EMD aggregators who will have access to excess hidden market data when combining node information can be monitored in the same way once there are multiple aggregators. Each will also be incentivized to do TCA on the orders that they are aggregating. Those nodes will be separately collateralized.

RouteCoin Network Component Protocols

The SOR nodes which connect to the network can consist of either a single SOR process for clients who operate the SOR on their own behalf or dual SOR and Decision Service processes, for clients that operate as an agent for other clients. When the SOR client and the Decision Service are operated separately, they will often be distributed across different physical networks,. These components, will interact with both the traditional and enhanced market data services as well as a new aggregation layer. Note that an individual SOR decision service could support multiple SOR clients, in the case that the operating entity is acting as an agent for multiple clients. This is particularly relevant, as the operator of the gateway node will need to know that their own clients are not operating in a way that jeopardize the integrity of the system. Thus, while the SOR node is required to stake RouteCoin to be part of the network, we would envision that agent routers may require operators of client SORs that use the API to post collateral as well, in order to guarantee performance.

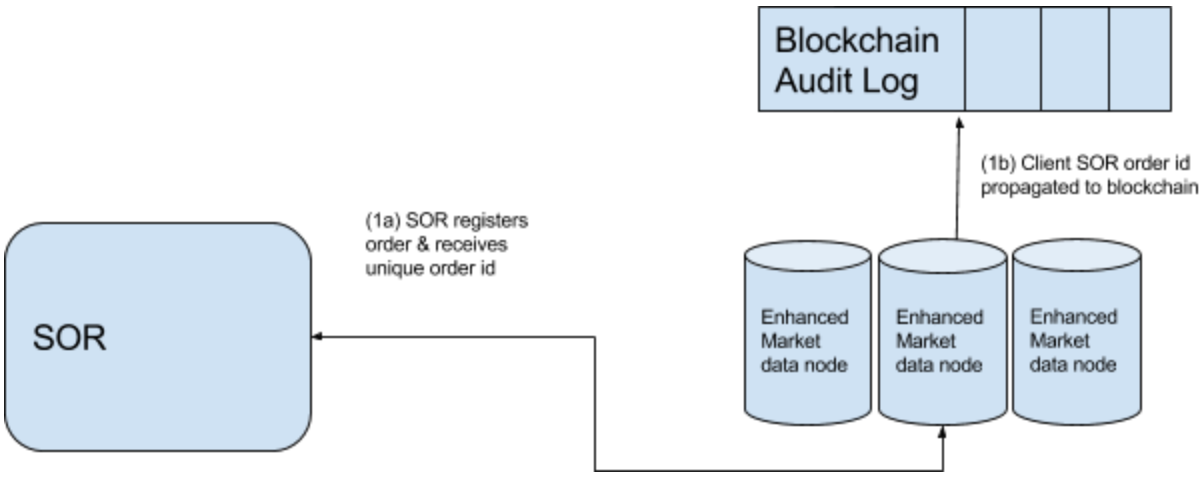
As diagrammed above there are three[4] key protocols that need to be documented to the blockchain:

1. Client Register Order with Network
2. Market Data Request(s)
3. Orders sent to Markets

Client Registration of Order Protocol

This is the first message sent by the Client SOR to initiate an order in the system. It identifies the order as well as communicating the parameters of that order and is sent to multiple Enhanced Market Data Nodes, where the first one will return the id, which the SOR will include in subsequent messages to other EMDNs .

[4] In the case of a agent such as CoinRoutes operating a separate decision server from the SOR client, there will be a fourth and fifth protocol, (new order to decision server) described under “agent protocols” that are not part of the RouteCoin network.



The API for connecting to this service will be require that the SOR provide the following fields:

- Product Pair
- Buy Sell
- Quantity
- Limit Price
- Route Type
- Route Aggression Level

Example: I want to buy 15 BitCoin in US Dollars up to 12,000, using the most aggressive order

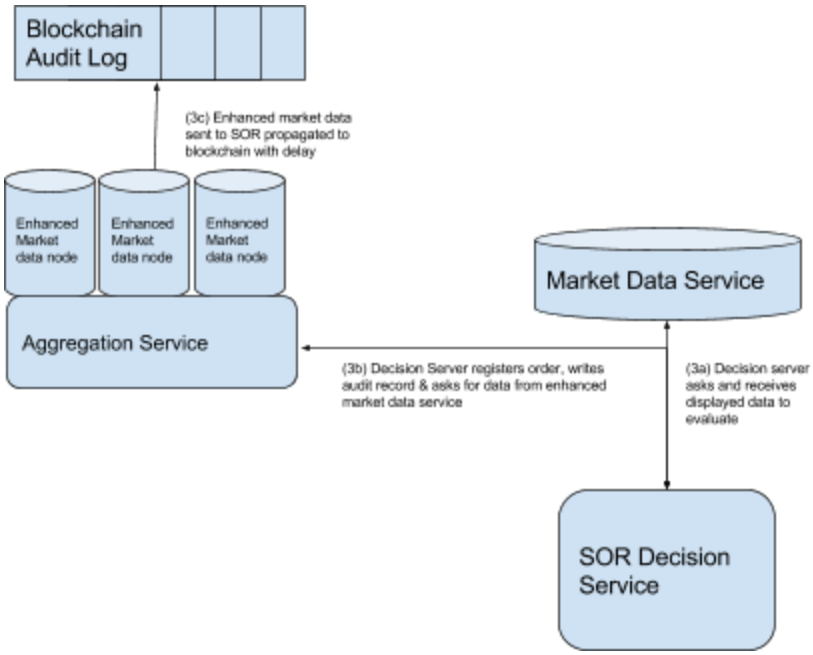
newOrder (15, ‘BTC-USD’, ‘B’, 12000 , ‘sweep’, ‘aggressive’)

The service will return an acknowledgement message or a reject (if there is a problem) with the unique order_id assigned by the distributed system. That order id is constructed by concatenating the client SOR id, Enhanced Market Data Node (EMDN) id, and a sequence number. The system will enforce uniqueness of Client SOR ids.

Market Data Request Protocol

There are two types of market data requests in the system. The first, is a request of the displayed order books from all eligible exchanges, which the system will use to return a consolidated book of all bids or offers to the limit price specified. The second, is a request of all

the hidden or reserve orders and where they are situated up to the limit price and quantity in the order making the request. To ensure that the enhanced data nodes do not have the ability to disseminate these requests to potential front running clients, the protocol will always ask for the book information on both sides of the market and will, therefore mirror the limit price around the midpoint in order to disguise the real order from the operators of the enhanced market data nodes.

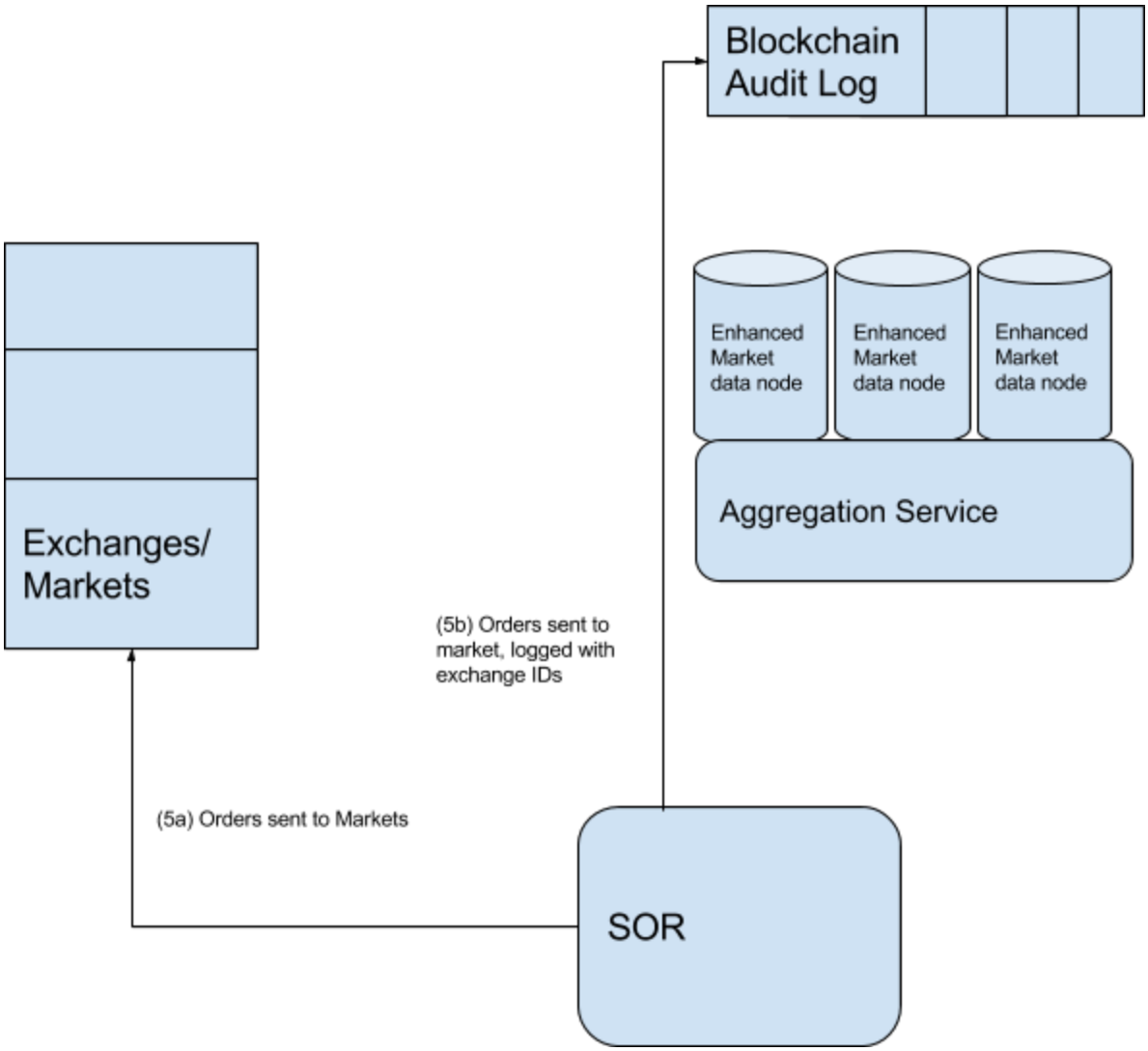


The SOR will send to a set of Aggregator nodes messages that request enhanced market data from all EMDNs, but the aggregator nodes function to limit the quantity returned to the SOR to be no more than the quantity on the order. To do so, it will send:

- Product Pair
- Quantity
- Buy Limit Price (either the actual limit price or the reflection of the sell limit price around the mid price at time of order)
- Sell Limit Price (either the actual limit price or the reflection of the buy limit price around the mid price at time of order)
- Eligible venues from client metadata (needed for determining available liquidity to that order)

Order Send to Market Protocol

This is the actual messages sent to exchanges by the client SOR. The format of these messages will vary based on the order API for each exchange.



BlockChain Process

All components will log their sent and received messages to the public blockchain with a substantive delay. This delay is necessary, due to the potential for such order information, before the order is executed fully or cancelled, to move the market against the client placing the order. This information is written to the blockchain for the purpose of providing network participants information to be used for the purpose of verifying compliance with the rules of the network. Primary among the network rules are:

- The only way to request enhanced market data will be disclosed is in response to a bonafide orders from a SOR or Decision Service
  .
- If sending an order with hidden or reserve quantity, always register that quantity with the system.
    - This requires that all orders be sent to the enhanced market data network. Withholding orders would potential gain advantage to individual SORs.

- Enhanced Market Data Nodes need to be guardians of their ordre data and only distribute it to SORs communicating bonafide orders.

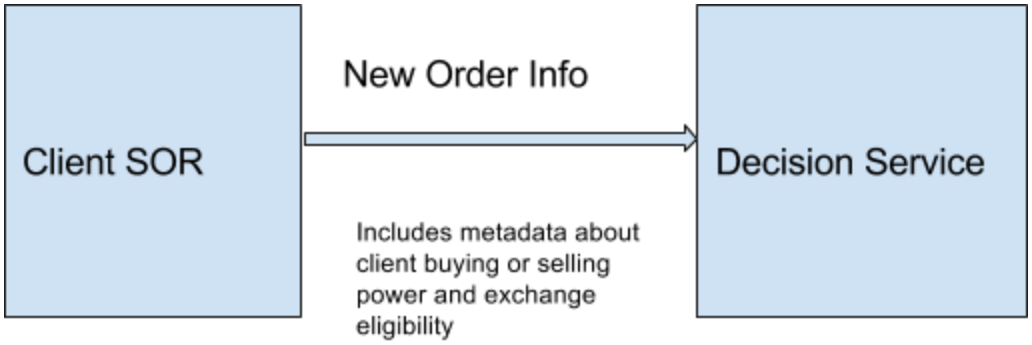
These rules ensure that there is no use for the enhanced data other than to efficiently trade against those orders. Note that there is no way to know the full size of hidden orders without sending a bonafide order of that size or greater, so there is no way to extract information without trading.

Agent Protocols

(these are the protocols used inside of the CoinRoutes System, and would be needed for other agent routers to conform to the network)

New Order Protocol

This is the second step in the order process and includes the order parameters sent to the registration process as well as the descriptive meta-data which identifies the client buying/selling power in the instrument at each exchange in addition to the order information.



The API includes the following fields on the order itself:

- Product Pair
- Buy Sell
- Quantity
- Limit Price
- Route Type
- Route Aggression Level
- Client Order ID (from the registration process)

In addition, the metadata is presented in a table with either the buying or selling power (in pricing currency) associated with all exchanges the client is eligible to trade on.

Example: I want to buy 15 BitCoin in US Dollars up to 12,000, using the most aggressive order

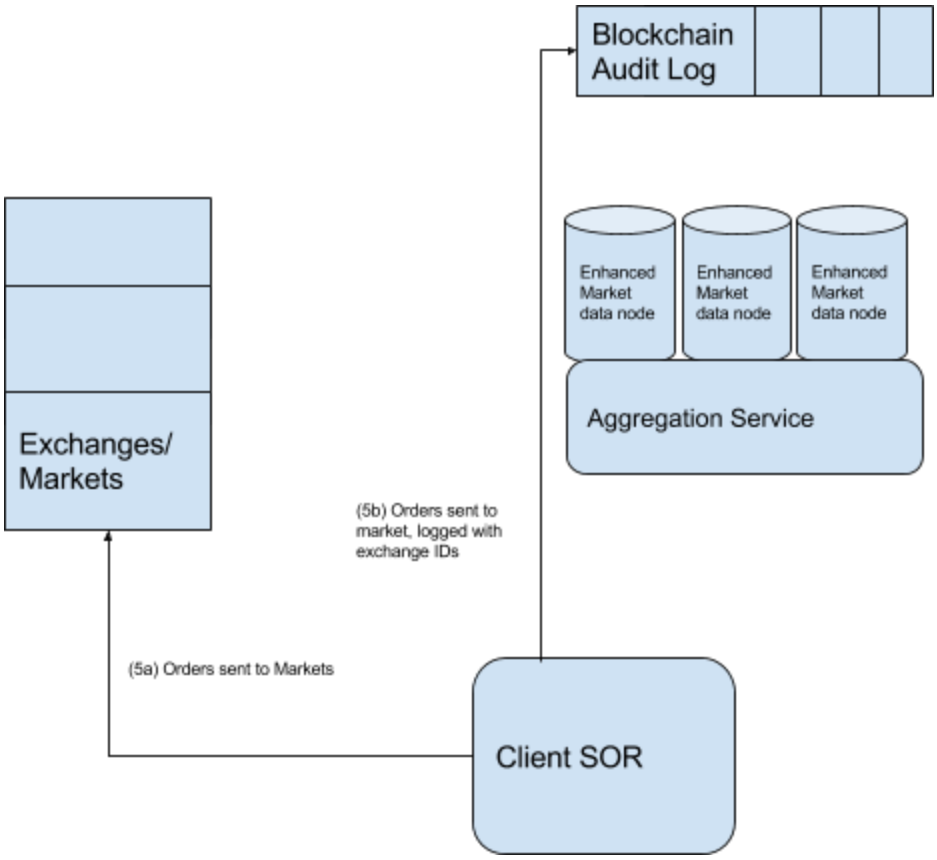
newOrder (15, ‘BTC-USD’, ‘B’, 12000, ‘sweep’, ‘aggressive’, xyzfund10000000ae123)

Metadata:

GDAX	1500000
GEMINI	400000
BITFLYERUSA	20000
KRAKEN	24000
BITSTAMP	15000

Order Package Delivery Protocol

The order package is the specific orders that the decision server instructs the Client SOR to send to the individual markets.



The decision server will communicate the following information to the client SOR:

- **Product Pair**
- **Decision Engine Sequence Number (Decision Engine Sequence number, so that the client knows if it missed a Decision Engine message)**
- **Client Sequence Number (last client sequence number received, so that the client knows if this instruction is stale)**
- **Buy Sell**
- **Quantity**
- **Exchange**
- **Order Type**
- **Limit Price**
- **Cancel messages**

- **Client Order ID**

The reason that the sequence numbers are important is that, while this paper shows the original order entry, there are many situations where the decision server will need to iterate with the Client SOR. In those situations, it is important to keep track of modification, cancel and replacement orders.

Summary

The RouteCoin enabled network for trading cryptocurrencies is an innovation that establishes a self-regulating mechanism for aggregating hidden liquidity. It will establish a more efficient routing platform and could also be used to re-aggregate the fragmented liquidity in other asset classes such as equities.