MONITOR
CHAIN

MonitorChain Marketing Plan

by Zenchain Inc.

Unique Selling Proposition

The unique value and selling proposition in MonitorChain is that it is the first blockchain analytics service that focuses specifically on detection of hacks and exploits. It is the first and only blockchain monitor designed for use as an oracle for Ethereum exchange and token smart contracts.

While other block explorers and analytics platforms may record and display more data, MonitorChain is alone in using this data in a focused manner to solve a massive real-world problem and present the information in a way that enables clear actionable triggers for its customers.

Given the severity of theft and code exploits in cryptocurrency in general, and on Ethereum tokens in particular, MonitorChain provides a simple, ready made solution to a major problem with severe financial and legal costs that most prospective customers will be very aware of and eager to find a solution for.

Customer Type Segmentation

Decentralized Exchanges

The primary customer for MonitorChain. DEXes stand to benefit the most from using MonitorChain due to their anonymous self-serve platforms bring highly vulnerable as destinations for stolen or counterfeit tokens. Given that their exchanges also run on Ethereum smart contracts themselves, they can directly utilize MonitorChain as an oracle to suspend deposit/withdrawal/trading of a token when an alert is received automatically.

Sales pitch to DEXes can be highly technical and will highlight the use of the oracle as the primary selling point. They will be suitable for the higher pricing tiers, especially enterprise level custom hands on integration with their smart contracts. All the core selling features and pain points can be used with them, as they will already fear being used to launder hacked/stolen tokens, and most will be easily convinced of their own financial, legal, and reputational risks. The primary pushback from these potential customers will likely be on price, as there are few decentralized exchanges with significant volume at this time. Acquisition of these customers will come primarily from direct outreach.

Centralized Exchanges

A strong enterprise level customer base, the centralized exchanges have fallen victim to numerous hacks and been involved in several of the major incidents cited in MonitorChain's historic use case examples (OKex with Beauty Token, Huobi with SmartMesh, CoinExchange.io with Monero Gold, Binance with SysCoin).

Since their exchanges are not on the Ethereum blockchain, the oracle function is of no benefit to them; however, they can still become enterprise clients by having us help assist them in integrating alerts within their own offchain proprietary systems. Some of the centralized exchanges have incredible amounts of money so I would expect very low-price sensitivity from them.

The primary selling features for centralized exchanges will be on financial loss prevention, as well as branding/reputation benefits associated with the trust badge, press release and other marketing uses. Legal and regulatory concerns should be a major selling point to the centralized exchanges, though we expect some pushback and underestimation of these concerns by many of the exchanges as they are often based in offshore locations well away from Western government regulators and based on the history and type of personalities who run centralized exchanges, many have a cavalier attitude to the law.

Another expected response for centralized exchanges is that we expect some of them to already have their own rudimentary monitoring systems in place already. We can overcome such issues by reiterating the incredible severity and risk of theft/exploit, to convince them of the value of MonitorChain even if it is only supplementary to their own in house antifraud systems. Acquisition of these customers will come primarily from direct outreach.

Token Creators and Future ICOs

Companies who have or are in the process of creating Ethereum tokens cover the full range of pricing and service tiers, the common element being that their subscription and sales pitch should be focused on intensive monitoring of a single token – their own. All the major core selling points can and should be used with these users: financial loss, legal liability, and reputational damage.

For existing tokens, the larger market cap ones are suitable for enterprise level monitoring, specifically, on the upcoming roadmap features of smart contract specific alerts (such as an alert if a major account holding the developer's time locked vesting reserve suddenly transfers all its tokens). Price sensitivity should not be a major problem with larger tokens, as many of them have funds earmarked for 'supporting the Ethereum ecosystem' which is another selling pitch to include. Smaller existing tokens

should have similar values, pushback and concerns, but with the addition of being more price sensitive. Discounts can be given to persuade these tokens.

A key question to ask existing token creators is whether their token has a freeze function (or in due diligence we can try to identify these ourselves programmatically). If they do, then the oracle has additional value since they can use it to temporarily lock their token when an alert is received.

A major consideration for token creators will be whether we are also supported by the exchanges their token trades on. In sales pitches highlight any exchanges of theirs who already subscribe, and promise increased adoption coming soon. Once we have secured the token as a client, we can attempt to leverage them by having them ask their exchanges to use MonitorChain in order to boost their own value.

For future ICOs who have not yet deployed their token smart contract, we have an additional value proposition, which is to build custom integration pre-deployment – to allow them to have a freeze function tied to MonitorChain alerts under their own control, enabling them to realize full benefit of all MonitorChain features.

Acquisition of these prospective users to the sales funnel will come from several sources. For established existing tokens, direct outreach will be a significant portion. For upcoming tokens, strategic partners such as smart contract auditors and community management companies will be the primary source.

Algorithmic Traders and Private/Academic Institutions

In most cases, this category of users will be the most price sensitive and most difficult to sell, given that they have the least benefit from MonitorChain's features. Traders primary use case for MonitorChain is in integration with their trading bots, to prevent from accidently buying into the hectic price swings and volume that typically follow a major theft or exploit. The value to them is in avoiding being stuck 'holding the bag' with stolen/counterfeit tokens. We expect a high degree of price sensitivity, and these users will likely not be suitable for enterprise plans. To gain subscribers in this group, some discounting will be required. Most initial marketing strategy places a low priority on this class of customer.

Customer Pain Points

Financial Loss

The most direct measurable damage in cryptocurrency theft and exploits, is the loss of fiat or satoshi equivalent funds. The overall impact in losses can manifest in numerous forms, some of which are easier or harder to accurately measure:

- In the case of directly stolen tokens, there is the value of the tokens at the time of theft, which is the benchmark normally used. Pushback from prospective clients may state that if the theft is 'undone' by a fork, that the damage is erased, however, that neglects:
    - These stolen tokens are typically dumped at exchange, converted to a different cryptocurrency and then withdrawn, leaving the losses spread amongst those who were unlucky enough to trade for them before the halt of trading
    - When stolen tokens are dumped on exchange, the value drops significantly. In most cases, the value does not promptly return to the value prior to the theft/hack, spreading additional losses across all holders
- Reputational damage lowers the overall impression of a cryptocurrency, which although hard to accurately measure, causes a drop in value.

When theft and hacks occur, *someone* is always left with a financial loss. In some cases, the token creator can afford to make whole the losses for traders (eg. SmartMesh, at a cost of $1.4m USD). Other times trade rollbacks or token contract forks restore the damage but fail to undo the full losses, as it is impossible to 'put the cat back into the bag'.

While financial losses certainly hurt, many exchanges, and some token creators consider them a cost of doing business. They may push back saying they can afford to repay losses due to hacks. This stance neglects far greater and long lasting negative impacts that tend to occur in the weeks and months following these incidents.

Reputational Damage

When large sums of money are lost or stolen, it attracts all sorts of negative attention. Those who suffered direct losses will very often leave the exchange in question or permanently sell and given up on the token. Whether fairly or not, they tend to blame others and no excuse or company PR push can appease them. This all leads to a torrent of negative news that will haunt Google and social media results for years. Human nature tends to lead to piling on and starting a witch hunt, meaning any other skeletons in the closet of the exchange/token are likely to come out – and to a much more receptive audience than they normally would. While an exchange may be able to brush off the loss of a few million dollars in the context of their balance sheets, reputational damage can destroy even a billion-dollar business. The crypto space is littered with formerly booming companies who have been relegated to the trash heap following a single hack or exploit.

Legal Civil/Criminal Liability

Most terrifying of all, is a specific type of negative attention that comes along with the post theft spotlight, that of lawyers and regulators.

Regulation is a serious concern for most exchanges and ICOs. Given the ambiguous legal grey area that most operate in, a single law could have devastating impact on their businesses. In practice, most regulation to date has been minimal and focused on the most egregious violators. Typically, regulators leave individual exchanges and token creators alone while they work on industry wide long-term regulations. The exception to this rule comes in light of major financial losses. There is no easier way to end up the target of an SEC investigation into every aspect of your business practices than to have investors suffer major financial loss because of theft/exploit of your token or exchange. This prospect should terrify any exchange or ICO, as it threatens not only their business and money – but also the freedom of the operators themselves.

Anyone ignoring this risk is incredibly naïve. Should a prospective customer try to dismiss the risk by claiming they aren't guilty of any crimes, they can be reminded that the average person inadvertently commits 3 felonies per day. Motivated prosecutors will look through their entire history with a fine-toothed comb for anything they can use to charge. Did your Telegram admin once give advice that could be considered encouraging a pump and dump? Did you hire an offshore lawyer to claim your token was a utility while internally your management team discussed it as a security? Did you use any funds from ICO in even slightly different fashion than described in whitepaper? Is there text on any of your web/social properties that could be construed as promotion of an investment? Regulators will find it, and they will prosecute aggressively.

Those who claim to be beyond the reach of Western governments and regulators can be reminded of the United States long-arm jurisdiction, and how you can fall under US laws simply by having Americans use your service, hosting a server in the US, or dealing with any bank that relies on the US banking system.

Beyond criminal prosecution by law enforcement and regulators, is a less commonly discussed by far more common occurrence – class action lawsuits. In the case of a major blockchain theft or exploit, the chances of a class action lawsuit against you are a near certainty.

Pricing/Service Tiers

Pricing is divided into two main categories, Exchanges, and Token Creators (at a later date we may add better support for the Trader category as a SaaS but they are not a major target segment for initial launch).

The primary difference is in number of tokens covered. For Token Creators, it is singular token based, for their own, while for exchanges it is all Ethereum tokens, or at least access to all they trade and ability to add others in future as they list them. Even at the SelfServe/Basic subscription tier, MonitorChain is a higher end B2B service, and should be above the standard price range for SaaS services.

Enterprise customers will be priced on more of a boutique pricing scheme, depending on what custom features and dev work they require, as well as on the size/revenue of their business. We can establish some general price guidelines, but it is likely preferable not to publicly list enterprise pricing on the website. Since most customers are recent ICOs, or exchanges whose profits are in crypto, coupled with the fact that MonitorChain is itself an Ethereum based feed, pricing is set in ETH rather than USD, as it is theorized that psychologically subscribers will be willing to pay slightly higher prices as a result.

With this scheme there would be only 2 columns for the pricing pages for Token Creators and for Exchanges. As discussed as a strategic decision, the basic 'Trader' category will not be listed on the pricing pages, or if listed, as a small font footnote, and not directly marketed to in the funnel. Offchain SaaS style subscriptions and alerts can and likely will be added for this Trader category, along with the added feature that should benefit them directly – notifications of any transaction from a specified list of addresses (so they can know instantly if any of their personal wallets are hacked), but this is not a launch feature of offering as none of it has been developed yet.

Sales Pitch

The sales pitch for MonitorChain will vary somewhat depending on the segment of the prospective market being targeted but will always include elements of a common theme: blockchain theft and exploits are an unavoidable risk that carries immense consequences, and by using MonitorChain the subscriber can greatly reduce the size and scope of their damages and liability when disaster strikes.

The first stage in the sales cycle is to convince the customer that the pain points above are real and extremely severe. In many cases, it will be clear the customer already realizes this, in which case we can move to the next stage in the process. For others, the goal will be to instill a healthy degree of fear by showing them just how much jeopardy they potentially face, by providing examples and illustrating historical and hypothetical scenarios.

The second stage in a sales pitch is to demonstrate MonitorChain as a solution and highlight its problem mitigating capabilities. Depending on the technical affluence and knowledge of past blockchain exploits, this will be done in one of two ways:

- For those who understand smart contracts, oracles, and are aware of the major past incidents, a live demonstration breaking our 'not so smart' contracts where a hypothetical hacks attempts to launder stolen/counterfeit tokens on exchange but is stopped by MonitorChain with real time split screen blockchain activity shown onscreen should be sufficient to provide full education and will lead into specific questions that can be used as jumping off points to close a sale and upsell to higher subscription tiers
- For those with lesser technical knowledge, the pitch can focus on a more succinct pitch deck filled with hard statistics and a clean explainer sales video. Anecdotes can be used as needed to convey more complex technical topics. MonitorChain can be referred to as a 'home alarm system' for exchanges/tokens; or to those who come from a traditional business/finance background 'the crypto equivalent of the insider trading/fraud monitors for NYSE/NASDAQ'

By the conclusion of the second stage, customers should have at least moderate interest, and the goal becomes to close a deal 'can you really afford to wait, knowing the next big hack could happen tomorrow', and upselling to higher price tiers 'Are you sure you only want email alerts and not smart contract integration – what happens if your sysadmin is asleep and you miss an alert'.

In the early sales pitches, it is expected that there will be requests for additional features and custom integrations beyond what is in the current product roadmap. For enterprise clients, this is a business decision, and should their willingness to pay be high enough, we can prioritize anything that is technically possible. For others, we want to listen to their questions and reservations, but firmly encourage them to subscribe now and wait for the product to grow into their full needed feature set. Locking in grandfathered lifetime discounts for early adopters can be used to encourage such users.

Additional Customer Benefits and Services

To add value to Enterprise subscribers, and for early adopters, basic subscribers also, a handful of additional benefits can be included.

- Cobranded Press Releases
- Social/blog mentions
- Listing on MonitorChain.com client list
- MonitorChain Trust Badge

Similar to Norton/McAfee site seal badges, the MonitorChain Trust Badge is a code snippet placed on the website(s) of a subscribing Token/Exchange that displays a visual badge demonstrating that they are valid MonitorChain subscribers who protect their investors and traders from loss by utilizing our security services. Clicking the badge will load a verification popup that displays additional information on their subscription validity and protection levels. This badge has the added benefit of giving MonitorChain brand exposure and some SEO link juice. The badge can either be given exclusively to Enterprise subscribers, or alternate versions of it can be made so that this badge can be used by all subscribers. The badge can be further segmented and utilized should MonitorChain partner with a smart contract auditing firm in a great case of mutual benefit – MonitorChain assures that if a hack/theft occurs the damage should be minimized; while the smart contract auditor's certification ensures the chances of such an event happening in the first place is lower.

Acquisition Channels

Direct Email/Social Outreach

As MonitorChain is a B2B product with a well defined but narrow target market, the core marketing and sales will be via direct outreach to strategically selected key decision makers at primary userbase companies, namely Ethereum token creators and exchanges that trade in Ethereum tokens. The goal of initial outreach will be the generate enough interest that the potential customer views either a live sales demo or a recorded MonitorChain hack prevention video (~15mins).

Cold outreach tends to perform poorly, especially for a relatively unknown startup. To help overcome this issue, we have created the Telegram Anti-Phishing Admin Bot, which can be offered for free as an ice breaker to generate goodwill and demonstrate value to potential customers. The bot can be further used in outreach by contacting admins on the token/exchange Telegram channels and offering it there to open a conversation that can later be shifted to MonitorChain.

Revshare Partnership with Security/Audit and Community Management Agencies

MonitorChain is a 'picks and shovels' type of service, in that it provides support for the major players in cryptocurrency, which are currently composed almost exclusively by ICOs and exchanges. While MonitorChain is a new product that is essentially creating its own niche, there are several categories of established companies that happen to have largely identical customer sets and offer complimentary services that make them excellent distribution partners for MonitorChain.

Smart Contract Auditors – These security and testing firms that check smart contracts for vulnerabilities are a perfect match for MonitorChain. Those tokens and firms who have utilized smart contract auditors are ideal MonitorChain customers for several reasons: it shows a willingness to spend money on security services (contract audits typically cost $10,000 - $60,000 each), it demonstrates their commitment to protecting their users, and also presents a natural sales pitch 'The smart contract audit reduced the chance of your token being hacked – MonitorChain will take your protection to the next level by reducing the damage in the case you are hacked anyways.' Further to the direct benefits, a partnership with a reputable contract auditor would serve to boost the trust and reputation of MonitorChain itself. Securing at least one major contract auditor partnership quickly after launch is a primary goal for MonitorChain. For the contract auditors, a partnership presents an opportunity for them to offer MonitorChain as an upsell to their customers at significant revshare, generating them a considerable additional revenue stream. Likewise, a referral system could work both ways, with future MonitorChain clients whose contracts aren't professionally audited being very hot leads for the contract audit firm.

ICO/Crypto Community Management Firms – These companies run certain public facing aspects of token and exchange's businesses, primarily social media and user engagement. As with smart contract auditors, they have a customer base of tokens and exchanges willing to pay significant sums (prices for these management companies start at $10,000 and go up significantly) for the benefit of their users. There is a strong revshare referral incentive here. The Telegram Bot is a solid additional benefit also, as it solves a major need for the community management firms that don't have their own internal solution.