STRATUS CYBER

ICO PRE-SALE

SECURITY CONSIDERATIONS AND BEST PRACTICES

Introduction

At its core an ICO is a piece of code, a “smart contract” on the public Ethereum blockchain. Most of what surrounds an ICO though, is a non-exhaustive list of endeavors pertaining to early-stage startup initiatives. Nevertheless, owing to the uniqueness and intricacies of the underlying blockchain technology that powers an ICO, certain fundamental measures are essential to its successful execution-measures that fall into the categories of security, legal regulation, digital marketing, and strategic planning of operations.

Recently, there has been considerable focus by blockchain startups on conducting a “Pre-ICO Sale” or “Pre-Sale”. For the entire ICO to run smoothly, the pre-sale, the “main” sale, and the post-sale activities have to gel together into a unified whole which reflects a well thought out strategy that addresses the categories of importance mentioned above.

Pre-Sale

Essentially, a pre-sale is a small-scale ICO, conducted prior to the main ICO event. As such, many of the general guidelines that are pertinent in the context of an ICO, are applicable to the pre-sale as well.

Assuming a company decides that an ICO makes perfect sense for its business and product, a pre-sale can be useful in a number of ways. It can:

- Help test the ICO infrastructure at a smaller scale
- Raise capital for the main ICO
- Generate investor interest by offering limited time discounts and perks
- Reward the community of early supporters

Guidelines

To effectively execute a pre-sale (and to decide whether you need to do one at all), the following list of guidelines is a good place to start. Note that these guidelines are suggested best practices to securely and smoothly run a pre-sale, and in no way embody guarantees of successfully raising arbitrary investment goals.

Token Value Considerations

While a pre-sale has a number of benefits, a known disadvantage relates to token valuation. A pre-sale that is followed by an ICO which ultimately lists the tokens on public exchanges, incentivizes pre-sale investors to immediately sell their tokens at higher ICO prices, flooding the market and lowering the token value. Given a company's priorities in the light of its business strategy, pre-sale/ICO pricing mechanics, long-term token utility, and community goals around its product, considering the market behavior around pre-sales is an essential item on the checklist.

Security

ONLINE IDENTITY

When it comes to ICOs and pre-sales,a company's digital identity could be the weakest link in the chain of security. Owing to the fact that the entire fundraising rests upon an Ethereum smart contract address, any malicious party pretending to be linked to the original company, can easily advertise a different address to redirect funds - for example, the CoinDash ICO was infiltrated by hacking into the main website and changing the smart contract address.

Given this delicate security situation, the following is a non-exhaustive list of guidelines towards securing your company's digital presence:

- Hackers will try to use domain names that resemble the target name. It is a good idea to buy-off (especially if they are available at a cheap price) domain names that are similar or closely related to the original domain name

- It is imperative to get an SSL certificate from a Certificate Authority like Verisign. Apart from presenting your online audience with a feel-good HTTPS green padlock in their browsers, a valid certificate not only legitimizes your online presence but also links your company's real-world identity to particular domains

- Incorporate solutions such as Cloudtlare and two-factor authentication to maximize security around your websiteReward the community of early supporters

- Follow similar caution with regards to your social media presence. Attackers can spoof social media accounts just as easily. Link to social media through your CA validated website

- Login credentials to social media accounts and website management should remain within a tight circle in the company

- Audit your digital footprint through a general online investor's perspective. Google for your company and pre-sale, see what comes up. This is by far one of the best methods to weed out potential attackers and fake ads

SMART CONTRACT AND TOKEN CONTRACT AUDIT

As mentioned earlier, the smart contract (and the associated token contract referenced within it) is at the core of your pre-sale and ICO. To maximize the probability of having a secure and trustworthy piece of code on which you can rest the reputation of your ICO, it is vital that you:

- Ensure the transparent and understandable reflection of your token distribution strategy (as outlined on your website and white paper) within the smart contract. A good practice is to publish the source code for the contract as well

- Have multiple independent security audits of the smart contract and token contract code. This is a fundamental requirement which addresses code vulnerabilities such as re-entrancy attacks, loops, gas-limit related concerns, token lock-ups, and refund mechanics

- Take the safest route to secure ownership of the ICO contract: paper based records of your public and private keys. Offline hardware storage such as Ledger Nano are better than on-device wallets, but a piece of paper with your keys written down is the most secure way to go

- Dispense similar advice to the participants of your ICO. While the easiest method for ICO participants is to use a well-respected online wallet such as MyEtherWallet, more sophisticated methods of securely storing and trading tokens exist in which both offline (for digital signatures) and online (for sending out transactions to the network) programs are used. Another factor that influences the choice of wallets, is the amount of cryptocurrency/tokens to be stored and the frequency of conducting transactions

- Choose a software wallet which has proper security in place regarding calls to its public functions in shared contract code. The Parity Multisig Wallet had a security flaw in its public contract code, which resulted in a substantial amount of ether being stolen

- Test your solution. The entire pre-sale can be tested with simulated traffic on Ethereum test networks, before going live on the public chain

Legal

The regulatory framework around ICOs is in its nascent stage. Regardless, legal counsel is essential. There is major disparity between each country's legal approach towards ICOs and cryptocurrency. For example, in USA, regulation is predominantly treating tokens as securities (the "Munching Munchees" ICO was recently stopped by the SEC under the legal pretext of unregistered trading of securities). This can fundamentally change a company's approach towards modelling its token economy. You can choose to geographically limit the distribution (by enforcing IP filtering), or find a legal foundation which helps enforce your original token model. Either way, you must have an expert on ICO law, relevant to the region you intend to operate in, on-board.

Misc. Best Practices

- Do you need an ICO at all? Discuss with experts regarding the relevance of your product and business model in the context of blockchain technology. "Tokens have their place, and what Iam against is protocols that really do not need to have their own tokens for any technical reason shoving a token into their protocol in order to be able to ICO it." Vitalik Buterin

- Educate your audience regarding the ICO.As this domain is still relatively new to people, the importance of reiterating the basics regarding security of public/private keys, software/hardware/paper wallets, and trusting exchanges with your tokens, cannot be overstated

- Exercise full-disclosure and transparency. List details of each core member

- Be readily available on slack and social media

- Clearly define the goals of the pre-sale, and of the utility of the token

As a rough road-map, begin with finalizing the white paper (extensive details on the product and the team), decide whether an ICO makes sense (and if it does, is a pre-sale best suited to your goals?), clearly define token utility and distribution, develop pre-sale contracts and token contracts that transparently reflect the outlined details regarding the ICO (publish source code), have several independent security audits performed on contract code, simulate the pre-sale on a test network (preferably with a team dedicated to hack the sale), secure your online presence, and finally announce your contract address - a contract that is owned by a public-private key pair backed up on paper, and only in the hands of a few trusted team members.

STRATUS CYBER

GENERAL INQUIRIES

✉contact@stratuscyber.com ☎443-292-2966

TECH SUPPORT

✉support@stratuscyber.com ☎602-900-9321