How are you going to make sure your nodes operate securely?

We take security of our nodes extremely seriously. It is our expectation that as Factom grows in popularity the network will be attacked (particularly as it is possible to open leveraged short positions on the Factoid token), similar to how the Ethereum network has been attacked over the years. It is therefore incumbent on ANOs to be at the top of their game to ensure the network remains functional and stable.

The first step in ensuring our operation is secure actually starts at the setup of the operators' workstations. All of our system administrators will use Purism laptops running Qubes OS as their primary system. These are built with security in mind and come with hardware kill switches for cameras, microphones and wireless radios as well as open source Firmware that has the Intel Management Engine disabled. They can also come configured with a Trusted Platform Module (TPM) that utilises Heads firmware which can detect unauthorized tampering with the system's boot files.

Qubes OS is a security oriented distribution that easily allows the user to establish specific virtual machines (VMs) with read only file-systems for different purposes. System administrators will utilize separate VMs for different tasks, including SSHing into servers, accessing datacentre control panels via a website, Discord communications and Email.

The use of separate VMs means that, for example, in the instance a malicious payload is included in an email it will only affect the email VM and not the other VMs that may be accessing our servers. In the event of any such incident it is trivial to shutdown the VM and restore from an earlier known-good image.

In addition to the laptop, each system administrator will have a dedicated SSD with an encrypted linux install that they can use with their desktop system to administer the servers in the event of a laptop failure.

We will use Ledger Nano S's to manage system administrators' SSH (Secure Shell) keys with each system administrator having two devices, one a primary and one a backup. The Ledger Nano S ensures that the actual SSH private key remains in its secure processor and does not leave the device.

We will undertake a risk assessment to decide whether we should also implement additional 2FA (2 Factor Authentication) on our servers through the use of OTP (One Time Password) codes linked to the current time. If deemed necessary, we will ensure each system administrator has access to a minimum of 2 devices that can generate their 2FA codes so they can still access the servers if one device fails.

We have a number of standard security practices we implement as soon as we take custody of a server. We set up our administrative users with sudo access and a strong password policy that has sufficient entropy that it cannot be brute-forced with modern day computation and we disable root logon via SSH.

We are in the process of switching to SSH keypairs for remote administration and, at this point password logons for SSH will be disabled. We also switch the SSH port to a non-standard port and deploy a customised iptables firewall that has strict ingress and egress rules. Anything that doesn't match is logged and then dropped. We test these rules to ensure they do not interfere with the normal running of the server. We check which services are running and disable any that are not 100% necessary. At present we disable any ipv6 network interfaces and set ip6tables to drop all packets. All of the above actions are being built into a script to ensure none will be missed when we have to deploy new servers from scratch.

All our servers will have coded hostnames and we will maintain an internal directory that clearly links these to purpose and IP addresses for system administrator's eyes only. None of this will be

bound to any public DNS (Domain Name System) for security reasons. We are aware of the community's historic plans for guard nodes and would be ready to implement best practices when the time arises.

In order to verify that our security procedures are working correctly we run external port-scans of the server via nmap to confirm that everything is locked down as much as possible.

Each of our system administrators will have a unique user account and we will maintain a separate centralized logging server in a distinct data centre with completely different user access credentials.

All of our nodes will be configured to send all relevant logs to this centralized server via TCP and this will be invaluable in the hopefully unlikely event there are any attempts to hack into our servers. We will undertake a research project to identify the best techniques to store and analyze these logs in a way that provides us the clearest visibility of what is happening on our servers and networks. We will also undertake a research project to evaluate the best methods of evaluating unauthorized server intrusion, for example using tools such as Tripwire that regularly audit the filesystem. We will pay close attention to ensuring that use of these tools does not in any way hinder the reliability and operation of the Factom node.

We will also develop a clear incident response policy to detail how our admins will respond in the event of a security breach. This will focus on two key areas, bringing back online a second redundant server as quickly as possible to minimize any effect on the network and secondly preservation of evidence so a proper audit and review can be conducted to determine how the server was attacked and how it can be prevented in the future.

The security of our servers will not stop at just these processes, we see operational security as a continuous improvement process and are always prepared to undertake further research efforts to identify new techniques that can bolster our activities in this area. Finally, we are subscribed to popular security bulletins to ensure awareness of what is happening in the broader IT ecosystem and in particular anything that affects the specific hardware and software configurations we are using. This will enable us to be aware of all the necessary security updates for the particular Linux distributions we are using and ensure they are applied in a timely manner with an understanding of what they are affecting.

Cube3 is committed to ensuring our network is hardened against intrusion. To independently assess our overall vulnerability, we plan to procure assessment from a reputable company involved in cyber security. This will initially just cover testing our servers for vulnerabilities but we will also seek to engage them with a full audit of our company at a later date, commonly known as a PenTest (Penetration Test). This will include attempting to access our systems via social engineering. Given the expense of running a PenTest, and the general benefit to all, this may be extended to a wider evaluation of multiple Factom ANOs. Ideally, this could be the subject of a development grant, which Cube3 would be happy to take the lead on.

As a number of team members have been involved in cryptocurrency for several years, we are well aware of the use of social engineering to gain unathorized access to systems and will pay close attention to the security of all accounts used to access any 3rd party services that we rely on. For example we will set up 2FA for all web portals for the datacentres and email providers we are using. In addition we will ensure that all mobile phone numbers that are used for team and company purposes are explicitly setup with additional authorization passwords and account locks at the provider’s end to prevent someone from taking custody of these as a springboard to access deeper in to our systems.