Factom Authority Node Operator Proposal

CUBE Technologies

Contents

1 CUBE3 TECHNOLOGIES

We are Cube3 Technologies Ltd (Cube3), a small UK-based team with demonstrable capability and experience in business, commerce and academia. Collectively, we have been involved with Blockchain related technology since 2016 and we have a real passion to improve the integrity of information.

We believe that business and political decision making must be improved. Having personally suffered from poor decisions at governmental level (particularly with regard to health issues), we are certain that greater confidence in the fidelity of information would make a real difference. Because of this, one of our primary motivations is to help protect the truth of research; ensuring that information is readily and promptly available to benefit society, without the encumbrance of commercial exploitation or political restrictions.

Blockchain technology is one of the newest tools in our armoury to make this difference. Factom, in particular, is well placed to be truly significant. As such, we appreciate the opportunity to present our credentials to the Factom community and aim to demonstrate our capability and readiness to participate as an Authority Node Operator; running a robust, resilient and secure node.

In addition to node operation, we are also capable of and very interested in exploring opportunities to benefit the extended ecosystem. Should we be successful, we would like to pursue additional activities through grant applications, to ensure Factom gets real value for money through discrete measured projects. However, as it is most important to ensure the fundamental development of Factom during this early formative stage, our proposal solely focuses on our current commitment to providing infrastructure.

1.1 FOUNDING PRINCIPLES

Our company is based on eight founding principles:

Integrity	-	Our foundation
Share and be shared	-	We cannot change the world single-handedly and are very interested in the work of others in the Factom community. We will also build on strong networks in UK commerce, industry and academia.
Organisation	-	Using a sound framework to tackle the responsibilities, challenges and issues that being a Factom node operator entails.
Technical competence	-	Capitalise on our capabilities to do the job and always develop further.
Operational excellence	-	Through standardisation with cautious continuous-improvement.
Flexible and responsive	-	Relying on the stability our framework gives us to address real needs.
People based	-	Because we only achieve results through people.
Long term	-	We look to the future and take a long term view of our involvement in any project.

1.2 ORGANISATION AND TEAM

Cube3 Technologies Ltd is a UK based business operating from the Oxford area. It has 4 founders: Pete, Tom, Will and Mike. We intend to continue with a small core team and will add other resources on a contract basis as the business develops. Responsibilities within the company are delegated as follows:

CEO: Governance (including business processes), regulatory compliance, finance, strategic direction and programme & project management discipline.

COO: Operations, business measures, continuous improvement and the management of 3rd parties.

CTO: Technical standards, server administration development, change control for technical standards and development projects.

MIKE - CHIEF EXECUTIVE OFFICER

Michael (Mike) was a Chartered Engineer having gained a Bachelor of Technology from Loughborough University in the 1970s. His early career was in the challenging environment of Automotive Manufacturing where he was responsible for changing the manufacturing operations of a number of UK household names culminating in recognition in the Institution of Mechanical Engineers award for Manufacturing Effectiveness. His career switched into Logistics and Supply Chain activities where he worked in both operational and strategic roles before taking up consultancy. Here he has delivered the design, modelling and project management of business solutions for public and private sectors covering health, utilities, automotive, construction, agricultural equipment, cellular telephones, clothing and electronics. Expertise includes: Programme & Project Management, Process re-engineering, Logistics design and Manufacturing Engineering. He is a registered Managing Successful Programmes Practitioner, a Prince2 Practitioner and a Six-Sigma Black Belt who firmly believes in the people, process and systems approach to transformational change and that such results are achieved by building capable teams based on trust, respect and honesty. He is now largely retired.

TOM - CHIEF OPERATING OFFICER

Thomas (Tom) was awarded his PhD in Intelligent Automation in June 2018 and holds a Masters degree in Aeronautical Engineering. In 2012 he joined BAE systems as a Student Research Engineer, working on Prognostic Health Management solutions. Following this he became a Research Associate working on Hybrid Strategy for Hydrogen Fuel Cell Vehicles, before joining the Engineering and Physical Sciences Research Council (EPSRC) Centre for Innovative Manufacture in Intelligent Automation at Loughborough University, where he currently works as a Research Engineer. Here he helps manage the group's PLM server, network storage servers and assists with the two Deep Learning computers, whilst developing custom mechatronic solutions for a number of large aerospace companies. He is the author of 9 publications and is the recipient of 4 Honours & Awards including one contribution which helped Loughborough University gain *The Queen's Anniversary Prize for High-Value Manufacturing*.

WILL - CHIEF TECHNICAL OFFICER

William (Will) was awarded his PhD in October 2017 having received both undergraduate and graduate degrees at Loughborough University. His primary research interests include robotics, unmanned vehicles and machine vision, with his PhD thesis focussing on automated aircraft taxiing. Since graduating, Will continues at Loughborough University as a Research Associate in mechatronics, working on robotics and deep learning. Much of his work involves industrial and mobile robotics, predominantly using the Linux based Robot Operating System (ROS). His primary experience in server management comes from the setup and administration of deep learning servers, used to train robots for human interaction. Will has also been involved in several large European projects, including the Open-Manufacturing-Operating-System (openMOS), which focuses on Industry 4.0 and Intelligent Cyber Physical Systems.

PETE - TECHNICAL AND STRATEGIC ADVISOR

Peter (Pete) has an MEng in Computer Science and worked as a data analyst and programmer for a logistics consultancy during University vacations. Upon graduation he secured a position with one of the Big 4 Accountancy firms. Unfortunately, he developed a serious long-term health condition before he could start this role and has been unable to work since that point, over a decade ago. Since then he has kept up with developments in computing and technology as his health has permitted. He developed an interest in running an enterprise grade server set-up on his local network so that media centres could feed multiple TVs. Driven by a desire to do things right and a thirst to learn new skills this has evolved to encompass two servers running the Proxmox hypervisor with redundant mirrored ZFS storage and UPS backup, it currently provides local shared storage, personal cloud and calendar management facilities for his household. He began to follow cryptocurrency in 2016, starting with a small mining operation focussed on Ethereum as well as some direct investments. He also runs nodes for a number of projects including Particl, HEAT and Ethereum. He purchased his first Factoids in 2016 and has since kept a keen eye on the project. Whilst his health condition will primarily limit him to largely an advisory role in this venture, his technical experience and understanding of the blockchain space will be invaluable.

1.3 VISION AND MISSION

Cube3 aims to be recognised as a successful company that, by respectfully engaging and rewarding all stakeholders, brings innovative solutions to bear on today's problems for the benefit of current and future generations. We aim to do this by promoting integrity, honesty and openness as the business, cultural and political norm. Our vision for working with Factom is to capitalise on the "Honesty is subversive" belief of Paul Snow and by working together encourage the use of Factom to increase geometrically as people adopt it; disrupting the inefficiency of traditional record keeping, disparate information and legal tussles over who actually said what. One of our CEO's key reflections on his long business career was how integrity in an audit trail can be so hugely beneficial when things go wrong. The challenge has always been how to get this without suppressing spirit. Factom can do this!

As a small company, our mission is to make a big impact by searching out, designing, developing and capitalising on technological developments. Working with Factom, we intend to:

- Support the Testnet in a way that we all learn and get better at operating this reliably and effectively. Do this by:
  - Running a minimum of two testnet nodes at two geographically separate locations.
  - Use this experience to design, build and operate processes, capable of being used with confidence if we are appointed to run a Mainnet node.
- Research and select two geographically discrete and robust providers of mainnet servers plus at least one provider of redundant/back-up servers.
  - Commission, configure and test these servers and monitoring equipment.
  - Operate the servers using the standard processes developed during Testnet.
  - Monitor performance and cautiously improve processes on a continuous basis.
- Initiate and manage a development programme that researches and implements methods of ensuring reliable, fault tolerant server operations that enable Factom to build on solid foundations in order to achieve its fullest potential.
- Share the above with the Factom community so that we can all learn from each other.
- Do the above within the available resources, including any grants so that the business is resilient enough to withstand sporadic low income levels.

1.4 PRIOR EXPERIENCE

Although Cube3 is a new company, our team members already have a wide range of experience in operating servers for many different applications. This includes:

- Product Lifecyle Management (PLM) server implementation and administration for research at a large university. (5 years)
- Server administration and data policy implementation for Intellectual Property (IP) sensitive material, specifically relating to Non-Disclosure Agreements (NDA) covering reception, storage and disposal of sensitive data. (3 years)
- Management of network storage servers for critical and secure data. (2 years)
- Set up and administration of deep learning servers, used to train robots for human interaction. (2 years)
- Distributed simulation using a large cluster of embedded computers, intended to simulate workstation interaction within a future manufacturing environment. (2 years)

1.5 FACTOM EXPERIENCE

Our interest in the Factom community began in 2016, when Pete and Mike started a diversified long-term (10 year+) crypto investment portfolio, identifying Factom as not only a potential financial investment, but also a credible contribution to future information fidelity. Since this time, Pete has remained a keen follower of developments with this project, having joined the Slack back in 2017. Having carefully considered the options for fulfilling a role as an Authority Node Operator, we have decided that we should initially try to add the most value in the short-to-medium term. This will be achieved by focusing on the technical business of operating reliable node servers. Prior to any involvement with the Mainnet, we have been using the Factom Community Testnet, since June 27 2018, to help build operating experience across the team. So far we have:

- Evaluated appropriate VPS hosting providers for Testnet (see Attachment 1).
- Deployed two Testnet servers; one in the Authority set and one as a Follower node.
- Implemented our initial server-hardening strategy.
- Conducted a successful "Brain-Swap" on the Testnet.

Following submission of this application, we intend to add two more servers to provide a total of four Cube3 servers on the testnet. In addition we have setup a separate centralized logging server using an OVH VPS, to record all Linux authentication logs. This will also be used for the first test of our remote monitoring system; providing centralized logging and configured to monitor the uptime of the other servers and send alerts via phone/sms upon testnet server malfunction.

2 SERVER HOSTING OPTIONS

As each Authority node will be running the same core software, the differences between Authority Node Operators are largely down to the servers hosting each node. For our proposal to be convincing, we feel that an exploration of the available hosting options is necessary. Prior to any specifics, the first decision is whether to self-host the server, or rely on an external provider.

As the Cube3 team has several years of experience running servers, networks and mining rigs (including a considerable degree of redundancy) it would be feasible to run the servers ourselves. To determine if self-hosting would be a sensible option, we conducted a risk analysis comparing self hosting to using an external provider. From the risk assessment we have determined that self-hosting incurs four times more risk than using a capable data centre, due to the multiple single-points of potential failure that would exist. Therefore, for the Factom Mainnet we have discounted self-hosting.

2.1 SELECTING A SERVER HOST

Having decided that the authority node is best supported by a competent data centre, the next task is to identify a suitable hosting provider. The selection criteria for a hosting provider can be divided into three primary factors, each of which will be addressed below:

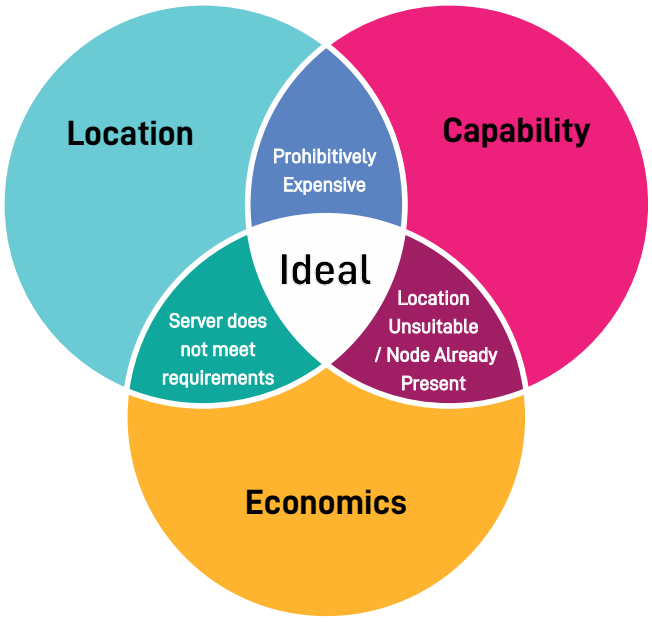

FIGURE 1: PRIMARY FACTORS IN SELECTING A HOSTING PROVIDER.

2.2 LOCATION

Of the three factors indicated above, economic cost and server capability are typically correlated. Therefore the most independent factor is *location*. The location of the provider will be governed by:

1. Global network access
2. Political volatility
3. Potential for natural disaster including geological stability considerations

The geographic proximity to other ANOs is also a factor to consider, as co-locating would increase risk for the Factom network. Figure 2 shows the global locations of existing ANO nodes [1], with numbers signifying locations with multiple nodes.

FIGURE 2: WORLDMAP OF CURRENT ANO LOCATIONS

From Figure 2 it is clear that the greatest concentrations of existing ANOs are in North America and Europe. From our UK base, we would prefer our servers to be in Europe to make access as easy as possible. Although there are already many ANOs in Europe, Figure 3 shows that most European countries do not currently host an ANO.

[1] A more detailed interactive Google map can be found here.

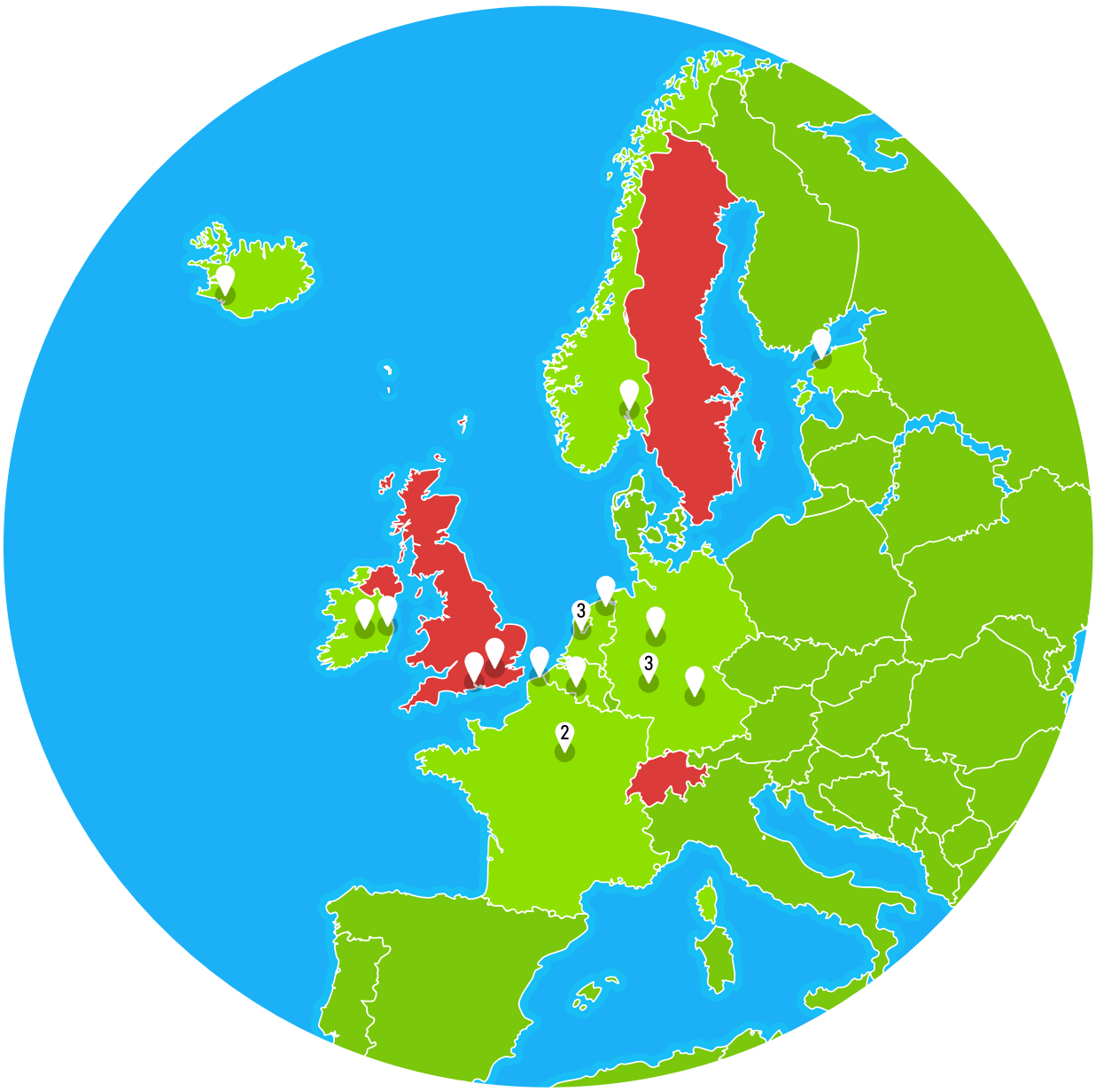

FIGURE 3: MAP OF CURRENT ANO LOCATIONS IN EUROPE

Of the countries without Factom data centres/servers, a number are quite suitable. In particular, Sweden and Switzerland are incredibly desirable countries to host servers, due to their strong stance on personal privacy and excellent infrastructure. The analysis of this can be seen in Attachment 2.

Despite the UK already having ANOs, we feel that the UK still represents a suitable site for backup and testnet servers, given that Cube3 is a UK company. Therefore, our preferred geographic locations are Sweden, Switzerland and the UK. The next stage is to select data centres in these regions based on their capabilities, and cost.

2.3 ECONOMICS AND CAPABILITY

Due to the correlation between server costs and capabilities, it is easiest to cover these factors simultaneously. Prior to selecting a specific host, we investigated whether virtualisation or dedicated hardware would be the best option.

2.3.1 DEDICATED HARDWARE

For most server applications, a virtual installation offers many advantages. However, there are drawbacks to this approach, with dedicated hardware being more suitable for certain applications. Despite using VPS for our testnet nodes, we have considered the advantages and disadvantages of virtualisation and concluded that we should use dedicated servers for the following reasons:

Surety of resources	-	No risk an unscrupulous provider can over-allocate resources leaving us underpowered when we need to scale in performance.
Surety of access	-	Direct access to the administration of the server. An administrative error with the general hypervisor could jeopardize our uptime and this can't happen with a dedicated system under our control. Attacks based on branch prediction timing such as Meltdown and Spectre could theoretically enable unscrupulous code to break out of a VM and potentially damage other VMs and the host system. With complete control of the dedicated system no one else could be running potentially malicious software on another part of the system, something quite possible with a VPS.
Complete control of when resources are restarted	-	With the current implementation of factomd it is important to be in control of when any nodes come online with a server identity. If an automatic failover protocol was implemented that switched the server identity to a remote backup server when the primary failed there could be serious problems if a VPS provider automatically or arbitrarily restarted the primary VM and caused identical server identities to exist at the same time. The Factom protocol is currently designed to terminate any node that comes online with an existing identity but there is a risk that both come on at the same time and both are terminated or the secondary backup server gets terminated only for the Primary to fail again because the initial fault was not rectified.

From this analysis we concluded that a dedicated server, hosted at a competent data centre, is the appropriate choice for Mainnet.

2.3.2 PROVIDER COMPETENCES

Aside from the technical capabilities of a host provider, the capability of host data-centres can be measured by assessing other characteristics.

Security	- Information security policies. - Organization of information security. - Human resource security. - Access control. - Cryptography. - Physical and environmental security. - Operations security. - Communications security. - Information security incident management. - Information security aspects of business continuity management.
Systematic processes	- Asset management. - System acquisition, development and maintenance.
Relationships	- Suppliers. - Customers. - Reputation.
Compliance	- Internal policies. - Customer specifications. - Laws.

These are embodied in the standards below, which are further assessed in Attachment 3:

- ISO 27001
- ISO 27002
- ISO 270017
- CloudControls

However there are no globally adopted standards meaning that conformance to a particular standard is strongly influenced by geography. Consequently other standards have been accepted as having a degree of equivalence. These include:

- PCI DSS
- SOC 1
- SOC 2
  - ↳ Type 1
  - ↳ Type 2
- SOC 3
- EU-U.S. Privacy Shield

How well a data centre adheres to these standards is typically reflected in uptime tier performance, where we are targeting either Tier 3+ or Tier 4.

We have measured data centre competency by establishing which providers data centre(s) comply with these standards. As exact standards vary by nation, we have attempted to establish a degree of equivalence about the Tier 3+ rating, and provided each data centre with a score. Figure 4 shows these results, with the greater scores being more desirable:

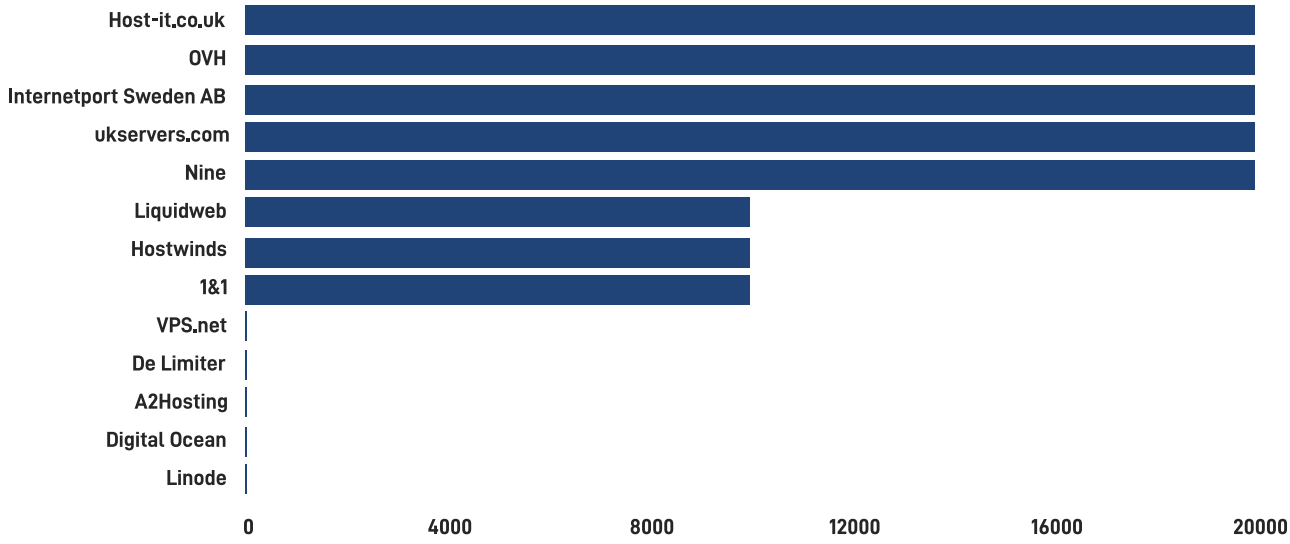

FIGURE 4: DEDICATED SERVER PROVIDER ASSESSMENT

Of note, a number of providers could not provide a dedicated server that met our minimum technical specification and were therefore awarded a zero score.

2.4 OUR SELECTED SERVER HOSTS

Taking the above factors into account, we have opted for two flagship primary servers:

- nine.ch in Switzerland
- Internetport Sweden AB in Sweden

However dedicated servers cost in excess of $300 per server per month, which represents a significant cost. Therefore we have decided on an approach which differs to the existing ANOs. We propose to colocate our own hardware in a competent UK datacentre, that will host 2 backup nodes and several testnet nodes. Currently, we are still reviewing out options but have preliminary identified two providers:

- host-it.co.uk (Tier4 datacentre)
- ukservers.com (Tier3 datacentre)

This server arrangement will form the basis of our chosen approach, described in the next section.

3 THE CUBE3 PROPOSED APPROACH

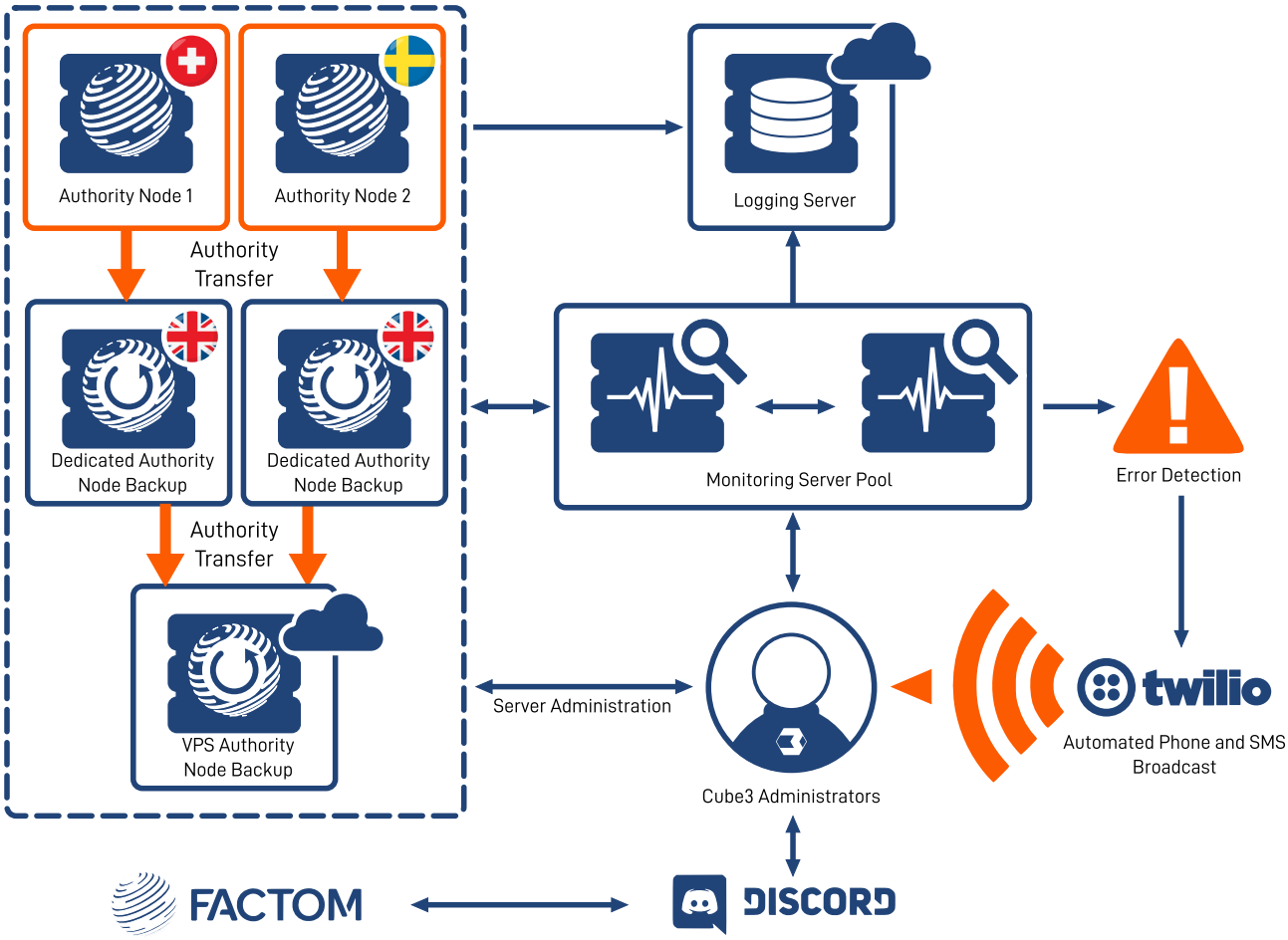

FIGURE 5: PROPOSED CUBE3 NETWORK TOPOLOGY DIAGRAM

It is our intent to operate 2 Mainnet Nodes as dedicated servers, in geographically separate locations. Our preferred locations are northern and central Europe, where we have selected server providers in both Switzerland and Sweden. Each Mainnet node will be paired with a fully functioning 'back-up node', situated in the UK. These 'back-up' nodes will be virtualised machines, running on colocated servers which Cube3 Technologies will procure, own and maintain, at a datacentre providing Tier 4 capability. They will have local full time staff and are located within 45 minutes driving time of our operations team.

3.1 PRIMARY SERVER SPECIFICATION

The significant drivers for selecting our server specifications are:

- Factom formal specification for mainnet servers.
- Appropriate headroom.
- Adequate redundancy (including mirrored drives and dual redundant PSUs).

Although we have taken great effort in selecting our chosen provider, their current server offerings do not include sufficiently new quad core CPUs to meet our requirements. As such, we have opted to use the latest 10 core CPUs instead. As this type of CPU is primarily designed for virtualisation, it has a lower base-clock than performance CPUs with only four cores. Therefore, to mitigate any potential problems, we intend to employ our servers using a bare-metal Linux install, with the Factom node software as the only workload. This ensures that there will not be any other computational demands on the system, leaving plenty of thermal headroom for the CPU to reach its Turbo clocks on the cores in use. We believe that this setup will not be disadvantaged compared to a basic Quad core with a faster base clock, should Factom software updates require increases in single-threaded CPU performance.

Further negotiations may yield a more recent Quad core that still meets the maximum ANO scoring criteria but at a slightly reduced cost; if not the option we have picked is completely capable of providing the service the Factom network needs with plenty of headroom. For now, the specification of our primary server in Switzerland is as follows:

Type of node/server	Dedicated
CPU number of cores	10
CPU type & clock speed	Intel XEON E5-2630v4 2.2GHz base clock 3.1 GHz Turbo frequency
Amount of RAM	32Gb DDR4 ECC
Whether memory is scalable	N/A dedicated RAM
Storage, raid type	Raid 1 mirror
Storage disk type	2 x 400Gb Enterprise SSDs in a HW RAID1 mirror
Storage (free size in GB for databases)	340Gb
Factom volume/disks	Separate volumes for root, var and Factom database
Connection and uplink speed	1Gbps

For all Cube3 servers we have elected to use Ubuntu 18.04 as our operating system. As the latest long-term support release, it is guaranteed to receive the latest security updates over the next few years. In addition, Ubuntu is already a popular choice for existing ANOs, providing plenty of experience within the community to draw upon.

3.2 BACKUP SERVER SPECIFICATION

The initial specification for the backup server is a high performance AMD EPYC processor system with 24 cores and 128 Gb RAM. By running this with the open-source Proxmox hypervisor our nodes will be allocated guaranteed resources that meet or exceed the maximum specifications detailed in the Factom Governance documents. This provides all the advantages of dedicated servers but with the flexibility of using virtual machines (VMs). Cube3 suspects that the flexibility of using VMs with snapshots could be gained without sacrificing the reliability afforded by our bare-metal flagship servers and we will conduct structured trials to validate this prior to use on mainnet.

This setup provides significant hardware scaling capability without requiring additional purchases, allowing us to easily respond should the Factom network suddenly see step increases in usage. Purchasing our own servers for the UK datacentre makes it significantly more affordable to continue supporting the Factom nodes in Sweden and Switzerland over the long-term, even if the Factoid market remains depressed for a period in excess of 18 months. There is just one up-front cost and the colocation fees are significantly cheaper than renting the hardware. We have identified at least 2 UK datacentres that meet our strict specifications, one a tier 3 the other a tier 4 and we are scheduling visits to assess them in person within the next month.

3.3 REDUNDANCY

All servers, both primary and backup, will feature local redundancy through the use of mirrored SSDs and redundant power supplies. In addition, the datacentres selected have sufficient redundancies for power, network and cooling.

To ensure that Cube3 is capable of providing continuous uptime, we also intend to operate an additional node using a VPS service. This will use the same hardware specifications as the two dedicated servers, but will only function when the integrity of another server is in question. This strategy of having a standby VPS ensures that even with a significant incident at one of our other Datacentres, Cube3 will have at least 3 independent locations with servers up and running. Even if we suffer a further datacentre or server outage we will still be able to provide 2 Authority nodes to the Factom network.

When not in use, the server will only be operated for updates and periodic synchronisation. It will be operated by a "pay as you go" VPS provider. Provisionally this is DigitalOcean; we are in negotiations with another "pay as you go" provider who operates in a Tier 4 Luxembourg datacentre. We feel that this extra layer of redundancy justifies the relatively small costs and upkeep time it requires.

3.4 MONITORING, MAINTENANCE AND EMERGENCY SUPPORT

To ensure that we are always able to respond quickly to any problem, a systems administrator will be available on a 24/7 basis. This team member will be responsible for monitoring servers, responding to service calls and rapidly implementing upgrades if required. The sites at which our systems administrators are based will have redundancy through secondary machines, uninterruptible power supplies as appropriate and back-up internet access. We will also ensure that our contact details are always up to date so that we can be reached easily by the community.

In the event of an unscheduled restart we will be alerted first by our own monitoring servers. We will maintain two independent VPS, solely for monitoring our primary servers:

- Each monitoring server will supervise both primary servers, as well as the backup servers, using dedicated monitoring scripts.
- Different software will be used on each server, to minimise the chances that a single event could take both monitoring servers off-line simultaneously.
- These servers will also monitor each other, eliminating the risk of monitoring failure.
- If the monitoring scripts detect an issue, they will automatically alert an on-duty system administrator via SMS or phone call.

Should an alert trigger, the monitoring servers require the on-duty system administrator to confirm they have received and are acting on the alert. Without confirmation the automated system will call additional system administrators after a pre-determined time. Following an alert from either our own monitoring systems or a centrally issued notice, the on-duty system administrator will follow the the processes we will develop for a range of scenarios. These will include the following activities:

- Logging on to the community Discord to assist in determining the cause of the problems and ensuring we can rapidly implement any necessary action.
- Logging on to the relevant servers to assess their status and accessing their logs.

In the event of any incidents that indicate a potential datacentre or server fault, we will start up one of our secondary backup on-demand services to ensure we have an additional node ready to go as soon as possible (This is not to be confused with our primary backup follower nodes of which two will always be permanently on and synchronised). To ensure all members of the team get regular experience administering the Factom node software, we will continue to run four Testnet servers and use them for regular training.

3.5 SECURITY

Similar to how other blockchain networks have been attacked over the years (such as Ethereum), it is our expectation that as Factom grows in popularity, it will also come under attack (particularly as it is possible to open leveraged short positions on the Factoid token). As it is the responsibility of ANOs to ensure the network remains functional and stable, we take the security of our nodes extremely seriously. As part of this, we intend to 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:

1. Bringing a second redundant server online as quickly as possible to minimize any effect on the network.
2. 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.

3.5.1 SECURITY: ADMINISTRATOR EQUIPMENT

Our approach to security begins with how our operators access the Cube3 network. All of our system administrators will be issued with a Purism laptops, which are built with security in mind. These feature:

- Hardware kill switches for cameras, microphones and wireless radios.
- Open source Firmware that has the Intel Management Engine (IME) disabled.
- A Trusted Platform Module (TPM) that utilises Heads firmware, which can detect unauthorized tampering with the system's boot files.

In addition to a laptop, each system administrator will also have an encrypted linux install on a dedicated SSD, allowing them to administer servers in the event of a laptop failure.

To compliment this level of hardware security, all administrators will be using Qubes OS as the primary operating system. 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. Cube3 system administrators will utilize separate VMs for different tasks, including:

- Using Secure Shell (SSH) to access servers.
- Accessing datacentre control panels via a browser-based web interface
- All communications, including Discord and Email.

Segregating tasks using specific VMs makes it trivial to shutdown a VM and restore from an earlier known-good image, if a VM is compromised. In the event of any malicious incident (such as a targeted payload included in an email) only the exposed VM will be affected, protecting the other VMs that may be accessing our servers.

3.5.2 SECURITY: REMOTE CONNECTIONS

As soon as we take custody of a server, we set up our administrative users with *super user* access and a password policy that has sufficient entropy that it cannot be brute-forced with modern day computation. Each of our system administrators will have a unique user account, to allow their access to be reviewed, and access is only possible via a hardened SSH connection:

- Root logon via SSH is disabled.
- Password logons via SSH are disabled, instead requiring SSH keypairs for remote administration.
- SSH access only via a non-standard port.

As part of our standard server hardening protocol we deploy a customised iptables firewall that has strict ingress and egress rules. Any external connection which doesn't obey these conventions 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 also disable all 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.

To ensure that system administrators' SSH (Secure Shell) keys remain private, we are implementing hardware based key storage using Ledger Nano S secure wallets. The Ledger Nano S ensures that the actual SSH private key remains in its secure processor and does not leave the device, with each system administrator having two devices, one a primary and one a backup.

In addition, 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.

3.5.3 SECURITY: NETWORK TOPOLOGY

The topology of our network is also intended to help protect against intrusion with each of our servers using coded hostnames to conceal their role. An internal directory of hostnames and IP addresses will exist (for system administrator's eyes only) but 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. We will maintain a separate centralized logging server in a distinct data centre with completely different user access credentials and each of our servers will be configured to send all relevant logs to this logging server via TCP. In the (hopefully) unlikely event there are any attempts to hack into our servers, this information may be invaluable in determining how best to respond.

3.5.4 SECURITY: ONGOING REVIEW

The security of our servers will not stop at just these aforementioned activities. We see operational security as a process of continuous improvement and are always prepared to undertake further research efforts to identify new techniques that can bolster our activities in this area.

As part of this approach, we are already 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 enables 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.

We intend to undertake a research project to identify the best techniques to store and analyse the logs stored in our centralized server in a way that provides us the clearest visibility of what is happening on our servers and networks. We also wish to establish 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.

3.5.5 SECURITY: VULNERABILITY ASSESSMENT

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.

3.6 DEVELOPMENT AS AN ANO

Although our team already consists of competent system administrators, there is still some research required in certain areas to identify best-practices. This includes implementing a robust centralized logging solution, as well as determining auditing techniques appropriate for identifying unauthorized access to any of our servers.

As we recognize it is in our best interests for all Factom nodes to be run as securely and professionally as possible, we would be happy to publish these findings should the community be interested. This could include being subject to peer-review by other experienced infrastructure ANOs, if required.

3.7 DEVELOPMENT PROJECTS

We intend for our business to operate cautiously, with risk management as a core tenet. However, we also embrace an ethos of continuous improvement and seek to both improve ourselves and Factom as a whole. Our backgrounds in both academia and industry place us in a strong position to undertake research projects, with the Cube3 team already identifying areas that we would be interested to pursue. (Our initial ideas include the verification of research and research data which we are happy to expand upon).

If it is seen a viable option, we will probably approach Factom for Grant support, intending for any research to occur as a self contained and justified package of work, with clear deliverables. However, we do not plan to begin any research projects at this early stage, and would only undertake such work after due deliberation and involvement with the Factom community.

4 IMPLEMENTATION PLAN

To bring the Cube3 proposal to fruition, the company has been following an implementation plan. As of the submission of this proposal, our current progress includes:

1. Setting up the company: (Cube3 Technologies Ltd. was established **June 26, 2018**).
2. Establishing a budget and appointing an accountant.
3. Designing and implementing our business processes.
4. Researching and appointing data centre providers.
5. Specifying and procuring hardware and software.
6. Participating in Factom Testnet. (Our first Testnet servers went live **June 2018**).
7. Preparing and submitting our Factom ANO proposal.

Going forward, most of the remaining Cube3 implementation plan will occur only if we are approved for onboarding:

8. ANO approval of onboarding to Mainnet.
9. Implementation of our monitoring and support infrastructure.
10. Periodic business reviews every few months.
11. Continuous ongoing development.

Cube3 has built this plan based on a number of assumptions. The most significant being a **3 month** onboarding timeline. Our capability to run servers on Mainnet is based on conservative estimates and could be brought forward if required. The salient features of the plan (albeit subject to controlled revision) are as follows:

- Capability to run fully functioning servers live on Mainnet by **November 2018**
- Fully functional servers onboarded by **December 2018**

The following Gantt chart explains our intentions in more detail.

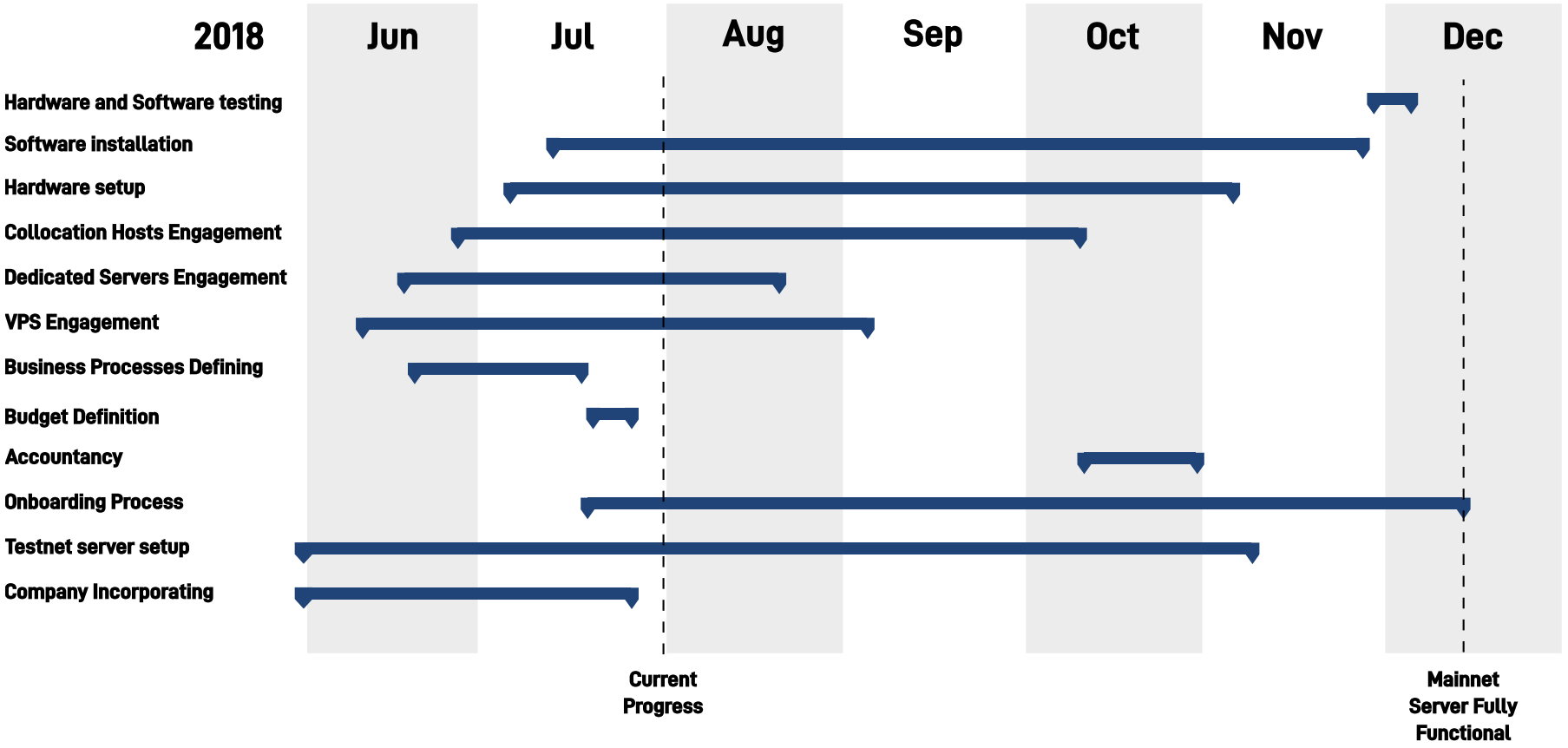

FIGURE 6: GANTT CHART OF TIMELINE FOR FULLY FUNCTIONING SERVERS ON MAINNET.

5 ECONOMICS AND BUDGET

We have estimated the salary of one system administrator at £26,000 ($34,000) per year and assessed the number of administrators required to operate 21 eight hour shifts per week as 4.65, thus accounting for weekends and holidays etc. and providing 24/7 cover. We have not made any charges for the design and implementation of our systems because we are providing this free of charge.

Assuming the FCT price stays in its current region of $10, which it may do for another 12-24 months and the markets become sufficiently liquid that conversion to fiat becomes feasible then theoretically we would need to operate at an efficiency of 25% to fully pay for our resources and show a break-even with 2 years, as shown in Figure 7.

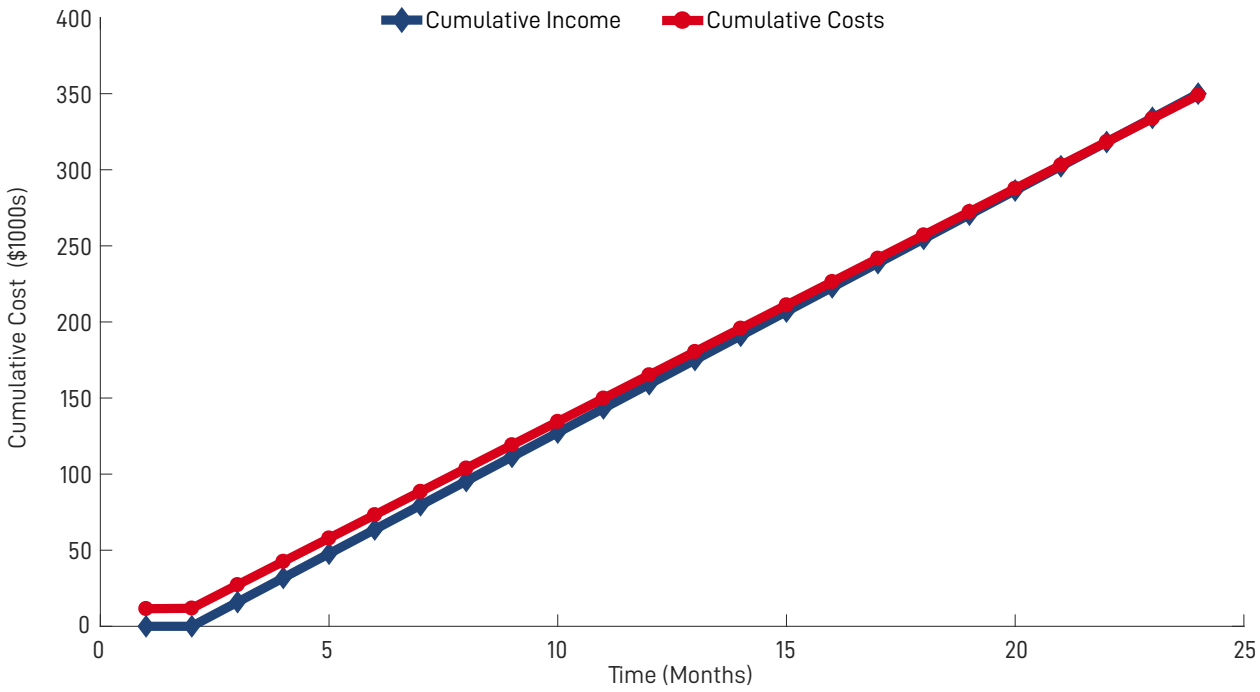

FIGURE 7: CUMULATIVE COSTS AND INCOME AT 25% EFFICIENCY

Given our long term ethos we have positively chosen not to do this. We believe it is in our and the network's best interests to operate at an efficiency of 70%, thus diverting a significant portion of the node payout into the grant pool to help grow the Factom ecosystem. This gives all of us the best chance of seeing a FCT price significantly and sustainably above current market rates, as shown in Figure 8.

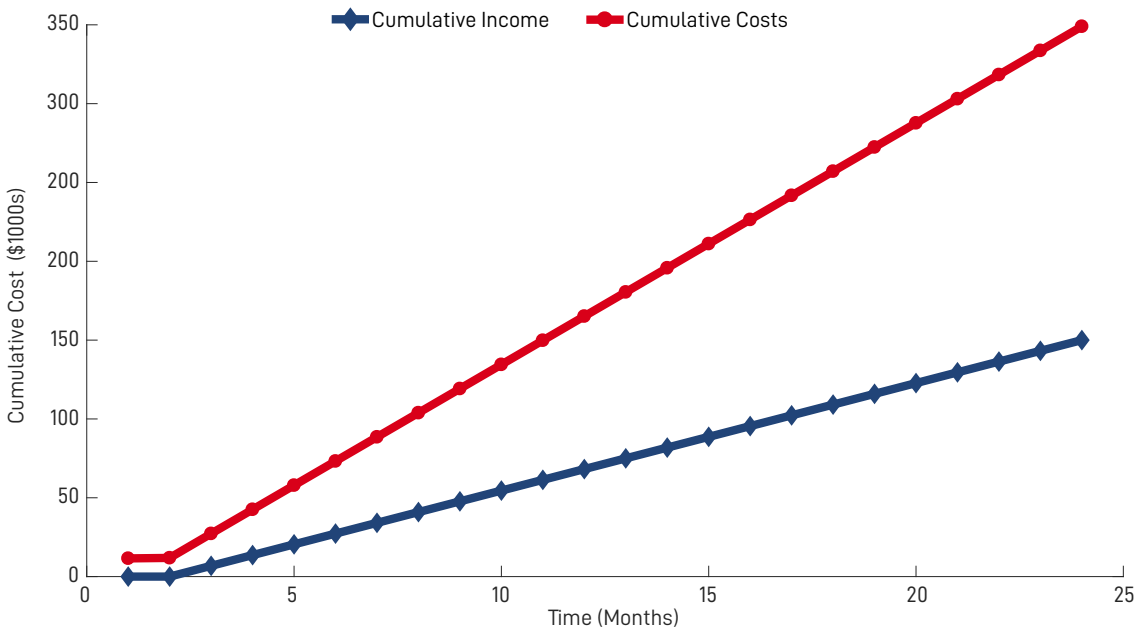

FIGURE 8: CUMULATIVE COSTS AND INCOME AT 70% EFFICIENCY

We are opting to initially forego any salary component and provide these system administrator services for free until market conditions improve. This is clearly seeking a balance of risk and reward. Our intent, other than paying UK Corporation Tax and certain direct costs is to accumulate funds in the company for re-investment subject to formal advice from our accountants.

If our assumptions about the viability of the Factom network are wrong, FCT will not grow in price, we will not recover our costs and our system design and system administrator work will see no remuneration, as shown in Figure 9.

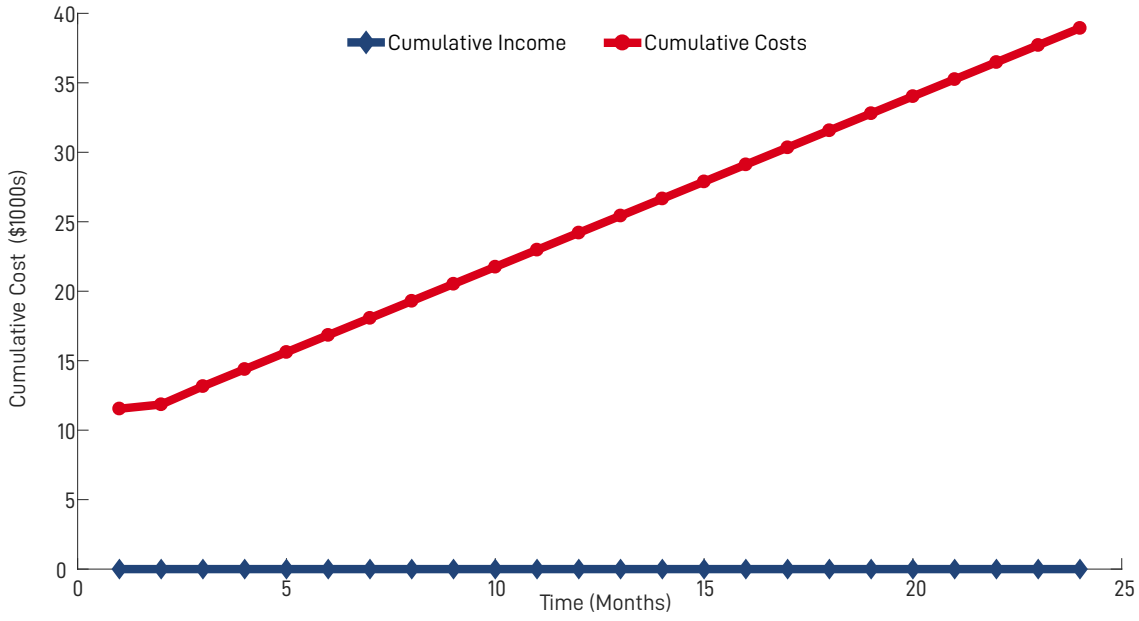

FIGURE 9: CUMULATIVE COSTS AND INCOME AT ZERO-VALUE FCT AND NO WAGE PAYOUT.

However, if we are right we will have sufficient funds when the price of FCT picks up. This will fairly compensate us for the time and risk we have taken. Crucially it will also be used by Cube3 to create a "war-chest" to enable us to meet future scaling demands of the network involving potentially significant hardware and personnel costs. It will also better position us to weather potential future volatility in the FCT market. This is true even if the value of Factom falls. If Factom were to drop to 25% of it's current value (approximately $2.70) we would still expect a recovery of costs within 24 months, as shown in Figure 10.

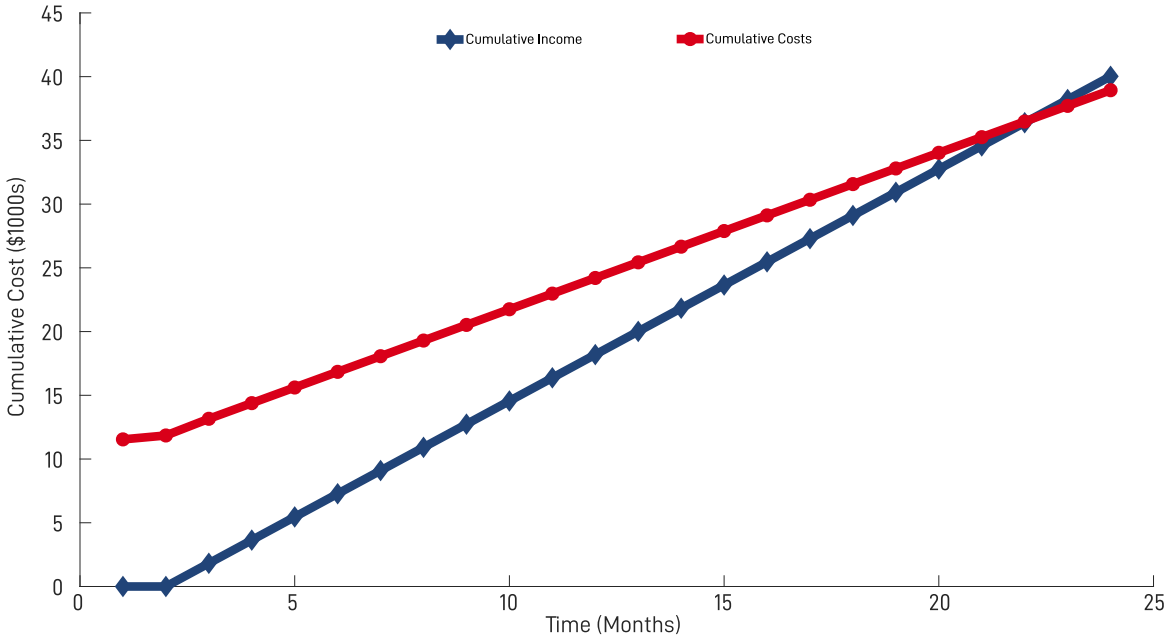

FIGURE 10: CUMULATIVE COSTS AND INCOME AT $2.70 VALUE FCT AND NO WAGE PAYOUT

6 SWOT ANALYSIS

FIGURE 11: SWOT ANALYSIS

7 OUR COMMITMENT TO THIS WORK

Our commitment to this work derives first and foremost from the deep belief, jointly held by the co-founders that trustworthy information is fundamental to humanity's future welfare. We are motivated by a bitter experience of poor, inaccurate and politicised information impacting on our lives. We are encouraged by the innovation of Factom in providing the world with the very first precise, verifiable, and immutable audit trail. The decentralised Factom community are making great progress in both development and application of this and we would like to be a strong part of this community and play our role.

We demonstrate our commitment by:

- Community involvement on Discord.
- Investing in Testnet servers.
- Setting out to run dual servers (geographically and commercially separate) as Factom Authority nodes.
- Budgeting $28,000 for set up & early operating costs which may not be recoverable
- Setting up a separate limited company to make the above happen
- Returning 70% of the originally intended Node support fees to the community to foster other developments

We look forward to dialogue with the community about our application.