LAOCON PLATFORM

Accelerate innovation of cyberspace

Version 1.0
# CONTENTS

1. Our Vision ......................................................... 4

2. Executive Summary ............................................. 5

3. Disclaimer, Terms, and Conditions for Cloud Sale ............ 6

4. Project Description ............................................. 8
   4-1. Background .................................................. 8
   4-2. Issues to Solve ........................................... 9
   4-3. LAOCON PLATFORM ...................................... 12

5. Business Model（Why LAOCON？） .......................... 14
   5-1. Target Market/Customer .................................. 14
   5-2. Service Flow ............................................... 15
   5-3. Monetization Model ....................................... 19
   5-4. Technical Feasibility .................................... 21
   5-5. LAOCON Technical Architecture ..................... 22
   5-6. LAOCON Product Roadmap .............................. 22
   5-7. Growth Potential ......................................... 23
   5-8. LAOCON’s Differentiator ................................. 24

6. Business Growth Strategy ..................................... 26
   6-1. Our Growth Strategy ...................................... 26
   6-2. Marketing Strategy (for Business Growth) ............. 27
   6-3. Growth Forecast for Platform Enrollment .............. 29
   6-4. Sales forecast based on growth strategy .............. 30

7. LC Token Sales .................................................. 31
   7-1. LC token ..................................................... 31
   7-2. Token Description ........................................ 32
   7-3. Token Allocation ......................................... 33
   7-4. Use of Proceeds ......................................... 34
   7-5. Token Economy .......................................... 35

8. Our Team ......................................................... 36
   8-1. Project Team ............................................... 36
   8-2. Advisors ................................................... 37
CONTENTS

9

Project Road Map ......................................................................................... 33
  9-1. Project Roadmap and Schedule .......................................................... 36

10

Legal opinion .................................................................................................. 38

11

Source ............................................................................................................ 52
In times when new value has been created by innovations in IoT, big data, AI, and virtual currencies, the need for a more adaptive cybersecurity has become critical. The decentralized accumulation of cybersecurity knowledge by people from around the world will make cyberspace better in the future. This is our mission.
Executive Summary

LAOCON develops a platform that accumulates and verifies all sorts of cyber-related knowledge against the malicious attacks and methods increasing in cyberspace.

Every minute, someone, somewhere in the world can be exposed to cyber attacks seriously. In respect to the cryptocurrency industry, thefts at the exchange have been increasing, with coins and tokens laundered through the dark web and personal PCs hacked for illegal mining purposes. We must be aware that we have got threats even closer since many devices and machines such as smartphones, watches, cars, homes, and home electronics have connected to the web and make our life more convenient.

To protect data - the asset and resource of the next generation - we must encourage cyber security experts to share their ideas and information on an open and safe platform as well as unite the powers of efficient white hat hackers who do not belong to a particular organization. LAOCON believes that it can resolve these issues through block-chain and token technology.

We hope you would understand the scheme and agree with our mission, feasibility, and technical capabilities by reading this white paper.
Disclaimer, Terms, and Conditions for Cloud Sale

This is not a solicitation for investment

This document was written for the purpose of providing information on LAOCON’s service and does not constitute a solicitation for investment or sale of the respective token.

LC is not considered a security for investment

LC is not considered a security in any jurisdiction - nor have properties similar to it. LC is a utility token that can be used on the LAOCON platform as well as cooperating enterprises and applications.

Necessity of the Entire Agreement

This document constitutes entire agreements between parties regarding matters in this Agreement. All previous agreements, discussions, argumentations, conditions of warranty, and warranty clauses are integrated in this document. No conditions of warranty, announcement of intention, warranty clause, or agreement exists between parties, express or implied, except as expressly referred to in this Agreement. This Agreement may be amended or altered only in writing signed by either party.

Only those who fully agree to the following terms and conditions should purchase LC tokens (LCs):

- You agree fully to the Terms and Conditions set out in the Whitepaper and understands that it has legal binding power.
- Pursuant to the law applicable to the place of your residence, you are entitled to purchase LCs
  - Residents of the United States of America or residents of the People's Republic of China may never purchase this token
- You will not purchase LCs for speculation or investment purposes
- You shall carefully review and understand the risks involved before purchasing LCs
- You do not use LCs for the any illegal activities such as money laundering and financing for terrorists.
Risk

We cannot guarantee the recovery of capital used to purchase LAOCON tokens (LCs) in any way. “LAOCON Inc.” is not liable for capital lost from purchasing LCs.

- **Devaluation Risk**
  As LCs are subject to market supply and demand, LCs may depreciate from your initial purchase price. Changes to cryptocurrency regulations as well as technical issues on the LAOCON platform are some reasons that may cause LCs values to fall.

- **Regulatory Risk**
  Restrictions such as the use or possession of the LCs – or the possibility thereof – could negatively impact LC value as well as liquidity, increasing the cost of transaction.

- **Ethereum Platform Risk**
  Because LCs will be issued on Ethereum, any issue such as a failure or malfunction of the Ethereum protocol could have an adverse impact on the ability to exchange LCs for fiat currencies.

- **Technological Risk**
  Due to technological innovations such as quantum computing and high-speed calculation algorithms, our encryption technology may become targets for cyberattacks and be subject to security breach.

- **Serviceability Risk**
  There is the possibility that the start date for the provision of services may be delayed or that the expected function cannot be implemented.
4-1. Project Background

In 2017, the global cybersecurity market stood at $1,378 billion in revenue. By 2022, the market is expected to be almost double up to $2,319 billion.

The two biggest sources of growth will come from increasing data volume and cyberattack methods (or entry points). As more devices become connected to the Internet, as more companies allow employees to use their own devices for work or access the company network, and as more cloud-based applications become available, the need for cybersecurity will only grow. Nonetheless, a lack of cybersecurity personnel remains a severe issue.

According to a report that was released by ITU (International Telecommunication Union) in 2017, Singapore came above United States as the number 1 country (out of 134 countries reported) to tackle the shortage issue by helping develop cybersecurity experts. As a proof of its leading position, the Innovation hub "Cybersecurity Ecosystem @ block71 (ICE71) " was launched in April 2018 to support entrepreneurs and startups in the field of cybersecurity with know-how and financial support, with plans to help develop 100 entrepreneurs and 40 start-ups over the next two years.

In addition to the overall growth of cyber security industry, there is no doubt that Singapore will be the most potential market in the world in present and future, and we need a system for its large demand.
4-2. Issues to Solve

The aim of this project is to construct a platform that solves three issues of cybersecurity.

Rising complexity and cost of cybersecurity

In recent years, the cybersecurity market has grown at an annual rate of above 10%, driven by the increase in cyberattack-tactics employed by hackers as well as the expansion of cyberspace infrastructure. Today, security measures are required for software and applications in not only computers, but also in smartphones, watches, cars, and home appliances.

In addition, while IT users and operators’ main concerns used to be limited to computer viruses, they now must deal with the rising threat of spywares and malwares used to steal private information. Websites also face specific challenges known as DoS (Denial of Service) and DDoS (Distributed Denial of Service), in which sites are bombarded with large amounts of data/requests to render them unusable for the intended target customers.
Shortage of human resource for cybersecurity

Despite the growing need for cybersecurity, a lack of security experts has become a serious issue. Japanese companies, for example, lacked an estimated 161,140 persons in 2018, according to the “Trends and Outlook of IT Personnel Report” conducted by the METI. By 2020, the demand for cybersecurity will only increase and the shortage is forecasted to rise to 200,000. Globally, BCG estimates the world would face a shortage of approximately 1,800,000 persons by 2022.

In addition to the shortage of cybersecurity experts, the current market makes it difficult for clients of cybersecurity personnel’s services to find experts with appropriate qualifications. Given that cybersecurity experts must stay abreast with the everchanging landscape of Information Technology and cybersecurity, conventional measures such as a professional license or certificate have limited reliability. This makes it difficult for companies to hire successful candidates. Consequently, the average success rate in hiring qualified cybersecurity experts is estimated at just 25%, resulting in high employee turnovers as well as unclear career paths for cybersecurity experts. According to a survey conducted by ISSA (Information System Security Association), about 65% of cybersecurity personnel did not believe they had a clear career path. As such, there is significant demand for a service that matches cybersecurity personnel’s services with appropriate companies.

Increased Demand for Security Personnel Causes Shortage of Human Resources

![Graph showing increased demand for security personnel causes shortage of human resources.](http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf)
Vicious Cycle caused by the accumulation of Cyber Security Knowledge

As previously described, cybersecurity has become more complicated because of an increase in the number of cyberattack-methods used by hackers as well as an increase in the number of cyber-connected devices (i.e. expansion of cyber infrastructure). Ideally, preventive measures against cyberattacks should be incorporated in the planning stage of a software / application development process, as it significantly reduces the cost of cybersecurity. Unfortunately, most companies take supportive measures – tackling cybersecurity issues after problems have surfaced.

The Internet was not originally invented for business-application in mind. Nonetheless, companies have used the Internet as a platform to build websites, e-commerce, cloud, and many other IT infrastructures. And as companies grew, the number of confidential, private, and personal information that require protection has increased. Because companies tackle cybersecurity after systems have been developed, companies end up facing complex incidents and accidents, raising calls to review cybersecurity measures.

The number of methods that can be used to attack a system has also become more varied. In 2017, for example, a malicious ransomware named Wanna Cry, which encrypts private files and hold them to ransom, had a wide-spread impact on countless devices worldwide. To protect devices from the more crafty and ingenious attacks, companies have strengthened their protection measures by use of AI (Artificial Intelligence) and multi-layered defensive systems. Yet, these still are not able to offer 100% protection; and as attacks grow in methods, so must defensive technologies.
4-3. LAOCON PLATFORM

The LAOCON PLATFORM will help provide a blockchain technology enabled version of a bug bounty program. An application developer (whether enterprise or individual) would publish the information about their web service or application onto the platform with a reward (LAO tokens) that incentivize white hat hackers to conduct security tests. White hat hacker(s) that succeed would provide a report on the LAOCON platform, documenting the vulnerabilities of the web service/application. The developer may decide to view the report by distributing the reward.
We believe LAOCON platform will be able to provide the following benefits to its stakeholders:

1. **Access to higher-quality service at lower cost**

Because of LAOCON’s global reach and consequently access to a greater pool of talent, removal of the middleperson, and result-based compensation structure, developers would be able to receive comparatively higher quality of service at a lower cost than they would via traditional methods. Under traditional methods, cybersecurity services are provided under “time-based” or “fixed” compensation structures, in which payments are made regardless of vulnerability discovery or security improvement. By allowing developers to set the price of cybersecurity service (as LAO token rewards), we also believe developers would be better able to manage their costs.

2. **Matching Cybersecurity Supply and Demand**

Under the circumstance that there is a shortage in cybersecurity personnel, the LAOCON platform will match supply and demand via two means. In the first method, LAOCON will help connect developers with cybersecurity personnel around the world through a bug bounty program model. In the second method, LAOCON will provide talent-acquisition (recruiting) service to developers by harnessing platform data such as user profiles, cybersecurity expertise, and performance records.

3. **Sharing the latest cybersecurity knowledge globally**

As white hat hackers test their methods against web services and applications uploaded onto LAOCON, our platform will accumulate the latest information on application vulnerabilities and cyberattack methods. By harnessing these information and providing consulting services to independent and enterprise application developers, we can help strengthen their programs to cyberattacks.
5-1. Target Market/Customer

The LAOCON PLATFORM business will target cybersecurity users (IT companies, independent developers, and etc.) and providers (white hat hackers) globally, starting with Asia. The global cybersecurity testing market for enterprise/desktop, mobile, web, and cloud applications has grown at a CAGR (compounded-annual-growth rate) of 19.9%. By 2020, it is forecasted to reach 7.8 billion dollars, with Asia accounting for a third (2.4 billion dollar) of the global market size. Starting with a headquarter in Singapore, where there’s significant support for setting up cybersecurity businesses and developing cybersecurity talent, we plan to expand our business worldwide.
# 5-2. Service Flow

![Service Flow Diagram]

## 1. User Registration

To begin using the LAOCON service, users (developers and white hat hackers) must first register on the platform. Registration will be free; but registrants must provide some basic information (see table attached below) that will help us identify users when disputes arise and strengthen the trustworthiness of the platform.

### User Registration Details

<table>
<thead>
<tr>
<th>Developers</th>
<th>White Hat Hacker</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Individually</strong></td>
<td><strong>Company / Org.</strong></td>
</tr>
<tr>
<td><strong>Platform Registration</strong></td>
<td><strong>Name</strong></td>
</tr>
<tr>
<td><strong>Service Registration</strong></td>
<td><strong>Email Address</strong></td>
</tr>
</tbody>
</table>
2 Requesting Security Tests

Upon completion of user verification, developers will be able to use the platform to conduct security tests. The following four points list the activities that users must undertake before a successful request can be made:

1. Submission of a more detailed user information
2. Payment for LC token that will be used as bounty rewards
3. A detailed explanation of the request - for example, the kind of tests that the developer would like to be conducted as well as the link(s) to applications, and the deadline
4. Sign an NDA (non-disclosure agreement) on the occasion of security test

To request a security test, developers will first have to pay the bounty award to LAOCON in the form of a deposit. Should they later request to see reports that white hat hackers have submitted, LAOCON will make payments to relevant white hat hackers. If the developer decides not to conduct the test, the deposit will be refunded.

Upon successful completion of the afore-mentioned activities, the request will be published on the LAOCON platform. Developers (requestees) are allowed to perform updates to their requests, such as raising the reward amount, extending the project duration, and modifying the content upon viewing the summaries and the number of reports that white hat hackers submit.
Assigning Security Tests

From a list of available requests, white-hat hackers can view a quick description of each request as well as the associated bounty reward. At this stage, sensitive information such as links to relevant applications will not be disclosed. If a white hat hacker wishes to be assigned to a request, he/she will take the following steps:

1. Provide a more detailed information regarding their backgrounds
2. Sign an NDA (non-disclosure agreement)

To uphold our quality of service and ensure that tests are done by trustworthy white hat hackers, LAOCON will conduct background checks on their past experiences before deciding whether to assign the work or not. In some circumstances, we may confirm our decisions with relevant developers. Once a white hat hacker is assigned to a project, details such as links to applications will be provided.

Payment Reward

White hat hackers who are assigned to projects must complete security tests by the end of their respective project duration/expiration dates and submit relevant analysis reports. These reports should contain a summary of the tests that were conducted and their results - such as the number of issues identified, a sample of the issues identified, and contents that would be made available in the full document. Upon viewing documents, the developer (requestee) may decide whether to purchase and receive the full-version. The full-version document will likely include – but not limited to - the following items:

- A list of identified issues
- Procedures that will allow the developer to reproduce the issue
- The negative impact the identified issues can have
- The severity and importance of resolving such issues
- Basic guidance on how to resolve those issues
The report quality will naturally be affected by factors such as the amount of bounty reward, completion tightness, and the number of assigned white hat hackers. Consequently, if developers/requestees decide not to purchase any of the reports after viewing them, they may cancel the request. While developers/requestees will still be charged a platform usage fee (see information on “Monetization Model”), the remaining deposit will be returned. On the other hand, if not a single report were submitted by the project completion date, there will be no platform usage / cancelation fee.

As some developers may have clarifying questions regarding the submitted documents, developers may initiate conversations with the respective white hat hackers through a chat box interface on LAOCON platform. To protect each user’s identity, the chat community will only adopt each user’s nickname and LAOCON will continuously monitor conversations to ensure that no information that can help identify a person is being communicated.

If a developer decides to purchase a report, the LAOCON platform will first deduct its portion from the bounty reward (called the platform usage fee) before the remaining amount is given to the relevant white hat hacker. If a user wishes to purchase more than one report, he or she may pay extra tokens for them, based on the bounty reward that was initially set. The following table sets out the pricing for additional reports:

<table>
<thead>
<tr>
<th>Report Number</th>
<th>Bounty Reward</th>
<th>Platform Usage Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100% of Initially Stated Bounty Reward</td>
<td>5% of Bounty Reward</td>
</tr>
<tr>
<td>2</td>
<td>50% of Initially Stated Bounty Reward</td>
<td>3% of Bounty Reward</td>
</tr>
<tr>
<td>3</td>
<td>30% of Initially Stated Bounty Reward</td>
<td>3% of Bounty Reward</td>
</tr>
<tr>
<td>4</td>
<td>15% of Initially Stated Bounty Reward</td>
<td>3% of Bounty Reward</td>
</tr>
<tr>
<td>5</td>
<td>10% of Initially Stated Bounty Reward</td>
<td>3% of Bounty Reward</td>
</tr>
<tr>
<td>6～</td>
<td>5% of Initially Stated Bounty Reward</td>
<td>3% of Bounty Reward</td>
</tr>
</tbody>
</table>

**Hacker Evaluation**

After the developer has purchased the report and payments have been made to white hat hackers, the developer can rate and review the white hat hacker’s level of service (for example, based on the quality of report or helpfulness over the LAO chat). These reviews, along with information that the white hat hacker has received payments will be collected in the LAOCON data base (Security Experts Data Base) and later be used by LAOCON (or developers) to determine whether to assign white hat hackers to future projects, and to provide recruiting service (see “Revenue Model” for more details).
5-3. **Revenue Model (Source and Flow)**

The following diagram depicts LAOCON business’s revenue flow

The company’s expected revenues will derive from its 1) platform service, 2) cybersecurity consulting service, 3) cybersecurity recruiting service, and 4) other support service.
Platform Service Fee

Under the platform service, we will charge developers a service fee equivalent to 5% of the quoted token reward, if at least one white hat hacker successfully submits an assessment report. In other words, unless no white hat hacker can successfully hack/find bugs and submit an assessment report, each security test will incur a platform usage fee in the form of tokens. These tokens will subsequently be converted into fiat currencies before revenue can be recognized. Consequently, our platform service revenue depends on the number or security tests requested, token reward, assessment reports submitted, service fee, and token-to-fiat exchange rate.

Consulting Service Fee

We believe we can accumulate material knowledge on latest cybersecurity issues through the LAOCON platform as more white hat hackers and developers use the service. To provide a more comprehensive cybersecurity offering, we plan to offer consulting services to developers and cybersecurity companies such as IT security and anti-virus software developers.

Recruiting Service Fee

By leveraging the large amount of data (user info, field of expertise, performance record, and etc.) we accumulate over time on the LAOCON platform, we believe we will be able to provide a competitive cybersecurity personnel recruiting service for developers (enterprises, start-ups, independent, and etc.) globally.

Other Support Service Fee

As we grow our LAOCON platform, we plan to grow a line of support services that will help users (both developers and white hat hackers) maximize their utility on the LAOCON PLATFORM. These will include, but would not be limited to, products such as security test cost assessment service, priority testing service, and translation service for submitted reports into foreign languages other than English. Payment under this category will be made in LAO tokens, which will be converted into fiat-currency for revenue recognition.
5-4. Technical Feasibility

For each developer request (hereon described as “project”), LAOCON will produce one smart contract. Each smart contract will contain the following information:

- Project Name
- Requestee’s Name
- Deposited Token Numbers
- Project Duration
- Hacker’s Report
- Requestee’s Review of Hacker’s Performance

In addition, each smart contract will have the following functions:

1. **Deposit**
   A function that stores LC tokens provided by the requestee over the duration of the project

2. **Project Start**
   A function that allows receipt of white hat hacker’s report over the duration of the project

3. **Finalize**
   A function that allows the requestee to view the hacking report and to review the hacker’s performance when project is finished

4. **Self Destruction**
   A function that allows the requestee to cancel the project and return a portion of the deposited LC tokens back. If the “Finalize” function has already been carried out, the “Self Destruction” function cannot be executed.

Through smart contracts, hackers will submit the script and evidence of their hacking success and receive reviews from requestees. Project information that have been modified or executed by smart contracts will be written and stored on the blockchain and be able to be viewed by everyone, resulting in the inability of the smart contract or project information to be modified. This blockchain will be developed in-house based on a similar technology to Ethereum.
5-5. LAOCON Technical Architecture

Cloud Service

Cloud DNS ➔ Cloud Load Balancing ➔ Web Server ➔ Lacon Server (Blockchain Node)

Storage ➔ Sync

Laocon Minner (Blockchain Node)

5-6. LAOCON Product Road Map

2018,10
2019,2
2019,9
2019,10
2020,1

APP

Closed Beta (β) Release
- Begin hacking event
- Collect hacking reports

Closed Beta (β) Updates
- Complete report and activity evaluation on Closed Beta version
- Update and improve application as necessary

LAOCON Chain

Begin Chain Development
- Complete LAOCON chain
- Begin miner recruitment

Complete Chain Development

APP Integration
- Begin app integration with LAOCON chain

Platform Release
- Release LAOCON Platform
5-7. **Business Growth Potential**

**Growth in Internet, Web, and Data**

As ICT advances in technology and IoT equipment become more widespread, consumer’s life becomes more convenient. However, this also brings about a surge in private and sensitive data that become exposed to theft. Between 2010 and 2020, IDC expects digital data volume to grow 45-fold.

*source*: IDC 『The DIGITAL UNIVERSE of OPPORTUNITIES』

**Growth in Cyberattacks**

On the other hand, there is an increase of the damages caused by a cyber attack on the backyard of such innovations. The number of data leaked in the United States is exceeding 1,500 in 2017, and the damage is up to 12 trillion yen. This kind of attacks to the servers will continue to increase in the future, and the loss will not only be monetary, but it also causes deterioration of the corporate brand image, so that concerns about cyber security for companies and periods are becoming bigger gradually. In fact, according to the results of research conducted by A.T. Kearney for the 400 top executives of the world's leading companies cited the risk of cyber security, which is increasing by about 43%, as a problem of their workplace.

*source*: 『Adapting to Disruption』
https://www.atkearney.co.jp/paper/-/asset_publisher/dVxv4Hz2hbS/content/id/13580677

**Market Growth**

Strengthening cybersecurity measures is an urgent matter that even governments are getting involved. In the EU, for example, the General Data Protection Regulations (GDPR) was implemented in May 2018 to protect its citizens’ private information. Companies that provide services to EU residents need to deal with GDPR even if they do not have a business office in the EU.

Other countries are also considering strengthening their regulations around private information, which will ultimately result in higher cybersecurity spending going forward. In Japan, for example, after accounting for cybersecurity budgets allocated for Tokyo Olympic / Paralympics and growth in IoT security, cybersecurity spending will reach a record of 73 billion yen in 2018. This was twice the budget reported 3 years ago. Naturally, one can also expect cybersecurity demand to grow in Asia as well.

In 2017, the amount of capital that poured into cybersecurity reached ~$138 billion. By 2022, this is expected to almost double to $232 billion dollars. Investors forecast cybersecurity companies to continue to report double-digit growths in revenues and expect them to outperform the overall IT industry on a per-share basis.
5-8. LAOCON’s Differentiator

We believe LAOCON PLATFORM’s model of security testing service by bug bounty will compete directly with existing cybersecurity offerings. These current offerings can be categorized into security testing, cyber insurance, and bug bounty services. Nonetheless, we believe these products have drawbacks that the LAOCON PLATFORM can fill.

Product Comparison

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Security Testing</th>
<th>Cyber Insurance</th>
<th>Bug Bounty</th>
<th>LAOCON</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Structure</td>
<td>Time-Based</td>
<td>Time-Based</td>
<td>Performance-Based</td>
<td>Performance-Based</td>
</tr>
<tr>
<td>Cost</td>
<td>Initial</td>
<td>□ (Incurs at start of service)</td>
<td>□ (Incurs at start of insurance date)</td>
<td>○ (Does not apply)</td>
</tr>
<tr>
<td>Intermediary</td>
<td>△ (Does not apply unless provider is a broker or agent)</td>
<td>○ (Does not apply)</td>
<td>□ (Incurs brokerage fee)</td>
<td>○ (Does not apply)</td>
</tr>
<tr>
<td>Total</td>
<td>△ (Depends on service quality)</td>
<td>□ (Only insurance premium)</td>
<td>△ (Depends on service quality)</td>
<td>△ (Depends on service quality)</td>
</tr>
<tr>
<td>Service Quality</td>
<td>Security Improvement</td>
<td>△ (May finish without finding problems)</td>
<td>□ (Does not prevent cyberattacks)</td>
<td>○ (Depends on compensation)</td>
</tr>
<tr>
<td>Speed</td>
<td>○ (But depends on provider’s skills)</td>
<td>□ (Does not resolve issue)</td>
<td>□ (Depends on compensation)</td>
<td>○ (Depends on compensation)</td>
</tr>
</tbody>
</table>
1 | Security testing

A cybersecurity professional will be provided by the service company to test a developer's web application or system or vulnerabilities. Under this model, the developer will pay a time-based fee regardless of whether the service provider can uncover issues or bugs. Service quality is highly dependent on the service provider’s talent pool.

2 | Cyber insurance

Similar to a common insurance, the insured will pay monthly premiums to an insurer in exchange for protection or reimbursement against losses due to cyberattacks. While the cost may be minimal, it does not prevent cyberattacks. In addition, these reimbursements often only cover direct expenses (lawsuits for example) - they do not cover damages that arise from the loss of creditworthiness and information outflow – and are only distributed after the damages have been done.

3 | Bug bounty

Traditionally, a bug bounty program will use a middleperson to help a developer find white hat hackers to conduct hacking tests and facilitate communication. While these services offer access to competent white hat hackers nationwide, they are comparatively more expensive than the P2P/platform model that LAOCON plans to offer, as a charge (intermediate exploitation) occurs.
Comparison with competitive services by use case

The superiority will be clarified when comparing the competitive services mentioned in the previous section with the LAOCIN platform service by using the use case. As a use case, we assumed a medium-sized web application that the number of development is increasing year by year, evaluates the advantage for each service flow to go.

**Service Flow**

**Existing service** (Security test service)

- Application developers
  - Pick up the test request destination
    - Collect information on customers from the net, word of mouth, existing network, individual negotiations

- For each target application
  - Estimate test cost / duration
    - The test cost varies depending on the target and content. The cost and the required time for the test are unknown until receiving the estimation

- Depending on the requested engineer
  - Test is conducted within the period
    - Engineers owned by the client (usually 3 to 5 people for each case) are tested
    - Test quality depends on the requested engineer

- From the testers
  - Receiving the report of test result
    - The effect of test and the quality of the report contents depend on the testers, the cost accrues regardless of the quality

**LAOCIN PLATFORM**

- On the LAOCIN platform
  - Post security test request
    - By submitting request, we can ask all white hackers of platform

- When test is requested
  - Setting the cost and the time for test by oneself
    - It is possible to set up a test cost in the form of bounty at the time of request, never going over budget or schedule delay

- On a scale that was evaluated and set by oneself
  - Operating security test
    - Number of white hacker staff who conducts the test · Quality can be judged and set by oneself
    - Secure the reliability of white hackers on the platform management side separately

- Offered by White Hacker
  - Receiving necessary from multiple reports
    - Confirming the test overview and receiving report report or selectable
    - Multiple reports can be acquired if required
Advantage in security test request

Conventionally, when requesting a security test, it is necessary to extract the service provider companies by collecting information and individually evaluate the reliability of the test work or the risk of information leakage, etc. Then choosing the one to request test after reviewing, or choosing an existing fixer without evaluating the quality and the cost validity of the test work appropriately and asking for a security test.

On the LAOCON platform, we can request tests to all white hackers registered on the platform by submitting a test request from the request form. And the quality and the reliability of test are based on their past achievements and history (knowledge of the target application, etc.) of white hacker.

Advantage in preliminary confirmation of test requirements (cost estimation)

In the case of the conventional security test, the test difficulty level is determined according to the number of screens of the target application and the number of requests to be tested, etc., and the cost and the period of security test are determined. Therefore, the costs and the periods of test are not presented unless estimates are actually received from the testers by individual negotiation or confirming requirement. As a result of carrying out the test, sometimes it is not capable to obtain expected test results due to overlooking of the preliminary confirmation of the requirement, additional costs may occur, and problems such as excessive budget and delay of the application release schedule can happen. On the LAOCON platform, since it is possible for the user (developer) to set the test period (the deadline for reward) and the test cost (reward: bounty) at the time of requesting the security test, it is assumed that the possibility of having this type of problems above is low. In this use case, the total number of screens is 20 and the number of requests is 80 (20 screens × 4 requests).

According to the survey of this project team, the test costs $30,000 to $40,000 per month ($400 per screen, $300 per request, + Additional option fee). But the LAOCON platform can post a request such as $10,000 in 2 weeks (In case you could not have the report with high quality test result, you can change the fee and the period and re-request it).

Advantages in conducting security tests

The quality of the security test depends on the experience and know-how for the target application system by the testers. Therefore, in the cases of existing services, it depends on the engineers who belong to the testers (except the case where the test requester has re-entrusted the test implementation, although the cost increases)

In the LAOCON platform, as it can judge the engineers who has experience and know-how from among the registered white hackers, it is can conduct higher quality tests according to the target test case.

 Especially, in recent years, the advances in IT technology are remarkable. And various applications and systems using new technologies are developed. So it is very important to pick up right test practitioners according to the target test case.

Advantage in reporting of test result (by the report)

Conventional reports of test result are generally is provided in the report by testers or having meeting for the report in face to face, but the quality in the implementation of test result depends on the engineer of the testers as described above. Therefore, although it is assumed there is some risks of providing low-quality reports of test result, even in that case, the test cost will be charged on the user (developer side) fully (and it need additional costs in the case of retest).

In the case of the LAOCON platform, when a test result is provided by a white hacker, it can check the outline of the report contents (test contents, operation menu, etc.), and if the test quality is low, it is possible not to receive the test result. In that case no cost will be charged, except platform usage fee. Also, if there are multiple test results that you want to receive, you can receive it by presenting additional rewards, so the possibility of getting a high quality test result is very high.
6-1. Our Thoughts on Growth Strategy

LAOCON Inc.’s revenue (see above for revenue model) depends primarily on the number of test requests that registered users (developers) make on the platform. Growth in test requests will not only result in higher platform service revenues, it will also result in higher white hat hacker, test, and report counts. By harnessing the wealth of cybersecurity knowledge and user information accumulated, LAOCON would then be allowed to offer other services such as cybersecurity consulting and cybersecurity personnel matching service. As the number of test request is dependent on the number of users on the platform and the number of requests made per user, we believe focusing on these two factors will drive LAOCON’s growth.
6-2. Marketing Strategy (for Business Growth)

We will implement two measures aiming at increasing the number of registered users (developers) and the request rate (the number of requests made per user)—the two key metrics that will drive LAOCON’s growth.

1 Cybersecurity Event Participation & Sponsorship

The number of registered users (developers) and request rate will ultimately depend on the quality of test report and volume that LAOCON platform is able to provide. The higher the quality and the cheaper LAOCON can provide reports to developers, the more developers would want to register and use LAOCON’s service more frequently. In order to ensure the quality of test reports, LAOCON must attract trustworthy and quality white hat hackers to register and offer their services on the LAOCON platform.

We plan to raise LAOCON’s awareness among white hat hackers and relevant cybersecurity companies by sponsoring and participating in cybersecurity events globally. While our options would be limited to existing cybersecurity events, we plan to organize and hold a few events of our own every year once we are on solid footing. As part of our growth strategy, we plan to attend the following events listed below (Step 1).

<table>
<thead>
<tr>
<th>#</th>
<th>Host Country</th>
<th>Event Name</th>
<th>Number of Participants</th>
<th>Duration (Planned)</th>
<th>Organizer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>JAPAN(Tokyo)</td>
<td>Trend Micro CTF</td>
<td>1,431 Teams</td>
<td>2019.09~2019.12</td>
<td>Trend Micro</td>
</tr>
<tr>
<td>2</td>
<td>JAPAN(Tokyo)</td>
<td>Code Blue</td>
<td>N.A</td>
<td>2019.11</td>
<td>HITACHI, NEC, IIJ, Deloitte, and etc.</td>
</tr>
<tr>
<td>3</td>
<td>Singapore (Ayer Rajah Crescent)</td>
<td>Cross CTF</td>
<td>N.A</td>
<td>2019.06</td>
<td>Vantage Point, Cyber Test Systems, and etc.</td>
</tr>
<tr>
<td>4</td>
<td>Singapore</td>
<td>HACK and ROLL</td>
<td>N.A</td>
<td>2019.01</td>
<td>Sea, Visa, Google</td>
</tr>
</tbody>
</table>

We plan to use part of the proceeds obtained from the ICO to attend events listed above not only to build awareness of the LAOCON platform, but also build connections with cybersecurity companies for potential partnerships as well as to recruit talented white hat hackers and engineers (see next page for more information on recruitment). Once we have secured a solid LAOCON platform management team, we will attend and actively participate in larger international events (Step 2, see below).

<table>
<thead>
<tr>
<th>#</th>
<th>Host Country</th>
<th>Event Name</th>
<th>Number of Participants</th>
<th>Duration (Planned)</th>
<th>Organizer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>America(Las Vegas)</td>
<td>Black Hat USA</td>
<td>17,000</td>
<td>2019.08</td>
<td>Accenture, Confense, IBM, RSA</td>
</tr>
<tr>
<td>2</td>
<td>America(Las Vegas)</td>
<td>DEF CON</td>
<td>23,000</td>
<td>2019.08</td>
<td>Village, Karamba Security, and etc.</td>
</tr>
<tr>
<td>3</td>
<td>America(Atlanta, GA,)</td>
<td>Global Cyberlympics</td>
<td>2,100 (2012年～)</td>
<td>2019.04</td>
<td>IBM, ISACA, CERT, PROMETRIC, MITRE</td>
</tr>
</tbody>
</table>

By participating in events listed above in Step 2, we would not only be able to raise LAOCON’s awareness among white hat hackers, engineers, and cybersecurity companies internationally, we would also be able to accelerate LAOCON’s growth by securing users (developers and white hat hackers) along the way.

Once LAOCON platform has become well-known within the cybersecurity community through Steps 1 and 2 mentioned above, we plan to organize and hold hacker (cybersecurity) events of our own (Step 3). By regularly hosting these hacker (cybersecurity) events, we plan to make aware of LAOCON’s presence to up-and-coming white hat hackers and be able to stay current with the latest technological developments.
2 Cybersecurity Team

For the LAOCON platform to grow, it is necessary to build a team of talented in-house white hat hackers and engineers. The team will be in charge of upholding the level of service that LAOCON platform is able to offer to its users (developers) as well as managing and planning cybersecurity events.

As shown in the service flow diagram previously, LAOCON Inc. will manage and check assignment requests and reports submitted by white hat hackers on the platform. Our in-house cybersecurity team will be in charge of this function and ensure the quality of service is up to standard for its users (developers).

As part of its role, the cybersecurity team will also be in charge of planning and managing cybersecurity events. These events will be carried out with the aim of growing the number of independent and corporate users (both developers and white hat hackers) on the platform.

We plan to build our in-house cybersecurity talent pool by attending or sponsoring cybersecurity events.
6-3. Growth Forecast for Platform Enrollment

(User - White Hacker)

We are planning to expand the LAOCON platform business by extending the number of users and white hackers in the platform through advertisement and promotion, plus the marketing strategy based on the 3 steps above. In the current plan, we will start the LAOCON platform business from August 2019. Until the start of the project, we will support existing cyber security events as sponsor (STEP 1), participate in cyber security events (STEP 2), place the web advertisement, participate in other security community, promote to increase enrollment of users and white hackers.

As the numerical goal until the start of business, we plan to have 500 users (participation / sponsorship for 5 events, 50 enrollments by each event, additional enrollements by other advertisement), 50 white hackers (participation / sponsorship for 5 events, 10 enrollments by each event: 10 people, additional enrollements by other advertisement).

After the start of the project, we plan to host cyber security events, and participants need to sign up in the LAOCON platform as the entry condition. That will accelerate the number of enrollments of white hackers.

Until August 2021 (two years from the start of the project) we plan to achieve the numerical goal of 5000 user enrollment and 500 white hackers. According to the degree of attainment in the numerical goal of enrollments, we will add more promotional advertisements and promotional activities.
6-4. Sales forecast based on growth strategy

In the LAOCON platform business, the gain on disposal at the exchange from the sale of the LC tokens collected from three types of the fee, the commission fee for platform (and other optional service fee), the consulting service fee for cybersecurity, and the HR matching service fee for cybersecurity will be the main profit.

By executing on this growth strategy, we will expand annual revenue by increasing the number of enrollments of users and white hackers in the platform and sorting out company structure (cyber security team and consulting team).
7-1. LC Token (LCs)

This token is used on the LAOCON platform. Developers will offer tokens as rewards for successfully conducting hacking tests on applications and programs. White hat hackers who found the vulnerability of the application would submit test reports to their respective clients. If clients find white hat hackers’ reports to be valuable, the rewards (LC tokens) will be released to relevant white hat hackers.
7-2. Token Description

The following content contains detail of the LAOCON Token

<table>
<thead>
<tr>
<th>Token Name</th>
<th>LC Token</th>
</tr>
</thead>
<tbody>
<tr>
<td>Token Code</td>
<td>LC</td>
</tr>
<tr>
<td>Token Sale Price</td>
<td>0.1 USD/LC, 0.0005 ETH/LC</td>
</tr>
<tr>
<td>Particulars</td>
<td>ERC-20 (Ethereum-Based Token)</td>
</tr>
<tr>
<td>Maximum ETH raised</td>
<td>200.000 ETH</td>
</tr>
<tr>
<td>Soft cap</td>
<td>10,000,000 USD</td>
</tr>
<tr>
<td>Hard cap</td>
<td>100,000,000 USD</td>
</tr>
</tbody>
</table>

- **Distribution Timing**
  Except for tokens that are subject to lock-up periods, all tokens will be distributed to token buyers prior to LAOCON token’s initial listing. Tokens that are subject to lock-up periods will be distributed after the lock-up period. Tokens will be distributed to wallet addresses provided by buyers.
  ※Token buyers should not provide wallet addresses from coin/token exchanges. Instead, please provide wallets that were created from services such as MEW (MyEtherWallet).

- **Roadmap**
  The following share of token purchased (or received via compensation or bonus) will be subject to a lock-up period of 3 months from the token listing date
  - Founder : 100%
  - Advisor : 80%
  - Secret-sale period : 80%
  - Pre-sale period : 50%
  - Cloud-sale period : 0%

- **Minimum Purchase Amount**
  The minimum purchase amount will vary across three sales periods
  - Secret-sale period : 3ETH
  - Pre-sale period : 1.5ETH
  - Cloud-sale period : 0.1ETH

- **Bonus Coins**
  Bonus coins that are offered to token buyers will vary across three sales periods
  - Secret-sale period : 100% of purchased amount
  - Pre-sale period : 50% of purchased amount
  - Cloud-sale period : No bonus

- **Token Ban**
  Upon completion of token sales, LAOCON Inc. may “ban” unsold quantities

- **Sales Process**
  1. A LC token will be issued whenever a user purchases a token (mintable token)
  2. Any purchase order cannot be withdrawn or cancelled once it is submitted
  3. LAOCON Inc. will not provide a generic funding address through any social media, messaging services, bulletin boards, etc., as most ICO hacks happen this way
  4. Sales will commence at 00:01 on October 1st, 2018 and end at 23:59 December 31th, 2018.
7-3. Token Allocation

- **5%** founder
- **5%** team
- **10%** other
- **40%** reserve for service
- **40%** offered for public sales
7-4. **Use of Proceeds**

- **Marketing** 20%
  - SEO
  - Advertisement
  - Community management
  - Social media
  - Attract business
  - Security contest
  - Other events

- **System Development** 25%
  - Platform development
  - Chain development
  - Smart contract development
  - Engineer labor cost

- **Legal** 5%
  - Lawyers
  - Accountants
  - Law, compliance, and etc.

- **Founders** 8%

- **Management** 10%
  - Personnel
  - Office, rent
  - Transportation, and etc.

- **Team • Advisor** 15%

- **Tax** 17%
  - According to Singapore tax law
7-5. Token Economy

LC Tokens that are used on the LAOCON platform should appreciate in value over time as LAOCON business grows. The LAOCON management team will execute growth strategies (discussed under point 6 of this whitepaper) and seek to grow the number of white hat hackers, developers, and (security-test) requests transacted on the platform over time. As more people use the platform and more transactions are made, demand for LAOCON tokens should rise, resulting in higher prices and greater liquidity.

LAOCON Mgmt. Team
- Participate and Sponsor Cybersecurity Events
- Responsible for Building a Talend Cybersecurity Team

Grow user (developer) count & request rate by raising service quality and attending events

High test report quality ensured by in-house cybersecurity team

Acquire white hat hacker sign-ups by participating and sponsoring events

USER

LAOCON Platform Service

WHITE HACKER

Coin / Token Exchange
ICO Team Members & Their Relevant Business Background

8-1. ICO Team Members

CEO/FOUNDER

TAKAOMI UEMATSU

10+ years of experience in real estate transactions and advisories. A highly skilled professional in developing trading strategies and building investment portfolios. Over the course of his career, he managed complex projects and was actively engaged in business dev. Responsible for securing personnel necessary for marketing, platform creation and operation.

CIO

DONGYING LI

Arteryex, Inc CEO

Joined IBM Japan as a new graduate and engaged in a wide range of IT projects, such as ERP implementation, business transformation, system development and so on. In 2016, participated in launching a friend’s blockchain startup, experienced business plan and system design utilizing blockchain. In 2017, joined KPMG Consulting and provided the latest ICT strategy for government agencies and ICO consulting services for general corporations. In 2018, established Art.

CTO

TIANQI LI

Engineer

Machine learning expert with a deep-learning specialization and software development background. Responsible for platform RD & concept demonstration and project / marketing. Joined a major Japanese IT company as a new graduate, He has a deep knowledge in computer vision and AI system, including achievements at the top international conference.

CFO

KIMITO HORI

TOKYO UNITED Integration office
TOKYO UNITED Accounting & Tax Department Manager. CPA

In working Tax office of Tokyo National Taxation Bureau, he was conducting a corporate tax inspections. In working for Ernst & Young ShinNihon LLC, he was in charge of accounting audits of listed companies such as major manufacturers and department stores. In addition, he was engaged in Initial Public Offering, FAAS (financial accounting advisory service). TOKYO UNITED Integration office.

CMO

TAIKI HIGASHI

Business Consultant

Joined IBM Japan as new graduate, and engaged in Business(ERP) and IT consulting. He experienced various projects such as requirement definition of core system, design / development, marketing strategy and new business development. In October 2017, he moved to a foreign-affiliated consulting firm and engage in projects such as M & A strategy planning, business DD, business value evaluation and marketing support.

LEGAL ADVISOR

RESSOS LEGAL PTE. LTD.

International law firm with offices in Singapore, Malaysia, China, Hong Kong. A highly skilled professional in ICO. Responsible for planning legal opinions on the legal nature of tokens, countermeasures against money laundering on utility tokens, securing AML manuals and compliance policies.
8-2. ADVISOR

Nikolay Shkilev

Shkilev Nikolay is an entrepreneur, owner and co-owner of dozens of successful business projects, ICO advisor and blockchain expert. Nikolay has 20 years of experience in large-scale transaction projects. Has many awards and titles in the IT business: Self-Made Russia award, Tech guru, Super TOP award. His Holding received "Enterprise of the Year" award in the Kremlin. Has a business in various directions. Crypto enthusiast and mentor. Advisor in marketing, platform creation and management.

Vladimir Nikitin

Professional legal consultant/financial advisor with over ten years of experience in legal, finance, retail, and IT industries. Well-known cryptocurrency expert and ICO advisor. As an active supporter and advocate of blockchain technology, Vladimir Nikitin provides consulting services to select ICOs in the CIS region. His network in the crypto community tops over 31,000 followers.

JASON HUNG

Jason is a serial entrepreneur and inventor in mobile business, blockchain, digital marketing, AI and ERP related business. He is a co-founder of GFOB (Global Federation of Oxford Blockchain) and Keyman Technology Ltd, and an advisor at IDACB (International Decentralized Association of Cryptocurrency and Blockchain). He is the world’s top 3 expert ranked by ICOBench, helping more than 40 projects include IOTW, Gemstra, NHCT, Buying.com, DEPO, CyClean, INTRO, ICOMax, BitRewards, DateCoin, eCoinomic, USAT, EVENFOUND, and AllSporter. He has more than 20 years of proven track record on managing RD, IT, sales, consulting service with 9 patents which are being used at more than 2000 Apps.
LAOCON Inc. will begin development of the LAOCON platform in the beginning of 2019, with plans for official release in August 2019. A more limited version, the β (Beta), will be released prior to the official release date - and in-line with the Initial Coin Offering - in order to conduct further market research, product tests, business feasibility studies, and business appraisals.

### Project Roadmap (2018)

<table>
<thead>
<tr>
<th>Month</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>April</td>
<td>◯ Establishment of a company “CRYPTOSK”</td>
</tr>
<tr>
<td></td>
<td>◯ Market research &amp; business basic Research</td>
</tr>
<tr>
<td></td>
<td>◯ Establishment of business structure &amp; project team</td>
</tr>
<tr>
<td>August</td>
<td>◯ Issuing a token as “LC token”</td>
</tr>
<tr>
<td></td>
<td>◯ Publication of LP (<a href="https://laocon.io">https://laocon.io</a>)</td>
</tr>
<tr>
<td></td>
<td>◯ Publication of whitepaper (1st edition)</td>
</tr>
<tr>
<td></td>
<td>◯ Commencement of LAOCON Platform system (β version) development</td>
</tr>
<tr>
<td></td>
<td>&lt;&lt;Requirement definition&gt;&gt;</td>
</tr>
<tr>
<td>September</td>
<td>◯ Commencement of LAOCON Platform system (β version) development</td>
</tr>
<tr>
<td></td>
<td>&lt;&lt;UI &amp; system design&gt;&gt;</td>
</tr>
<tr>
<td></td>
<td>◯ Publication of whitepaper (2nd edition)</td>
</tr>
<tr>
<td>October</td>
<td>◯ Start of LC Token Sales &lt;&lt;Secret Sales&gt;&gt;</td>
</tr>
<tr>
<td></td>
<td>- Sales target : $ 50 million</td>
</tr>
<tr>
<td></td>
<td>- Sales period : 3 month</td>
</tr>
<tr>
<td></td>
<td>◯ Commencement of LAOCON Platform system (β version) development</td>
</tr>
<tr>
<td></td>
<td>&lt;&lt;System development&gt;&gt;</td>
</tr>
<tr>
<td>December</td>
<td>◯ Publication of whitepaper (Final edition)</td>
</tr>
</tbody>
</table>
Project Roadmap (2019)

2019

January
- ◎ Launch of LAOCON Platform system (β version)
- ◎ Start of LC Token Sales <<Pre Sales>>
  - Sales target: $40 million
  - Sales period: 2 month
- ○ Commencement of LAOCON Platform system (product version) development <<Requirement definition>>
- ○ Start of Building cyber security team & recruitment
- ○ Start of Event Preparation “LAOCON Hacking party”

April
- ◎ Start of LC Token Sales <<Public Sales>>
  - Sales target: $30 million
  - Sales period: 5 month
- ○ Commencement of LAOCON Platform system (product version) development <<UI & system design>>
- ○ Commencement of LAOCON Platform system (product version) development <<System development>>

June
- ★ Listing on exchange
- ◎ Launch of LAOCON Platform system (product version)
- ○ LC token distribution

August
- ★ Laocon business start
Dear Sirs

LEGAL OPINION ON THE INTENDED ‘INITIAL COIN OFFERING’ OF THE LAOCON PLATFORM TOKEN (LC) UNDER SINGAPORE LAW.

1. We refer to the Laocon Official White Paper provided by you to us on 4 September 2018 related to the proposed Laocon Platform token (the "White Paper").

A. INSTRUCTIONS

2. We are instructed that Laocon Pte. Ltd., a private limited company incorporated under the laws of Singapore (hereinafter referred to as the “Issuer”) intends to undertake an issue and sale (the "Token Sale") of a digital token known as Laocon Token (LC) (hereinafter referred to as the “Token” or “Tokens”). As requested, we set out herein our legal opinion on whether the Token will be deemed a ‘utility’ or a ‘security’ pursuant to the Securities and Futures Act (Cap. 289) and related subsidiary legislation.

3. We are further instructed that the key parameters of the Token Sale are as follows.
   a. The Issuer plans to develop, in its capacity as a technology services company, a decentralized, peer-to-peer cyber security platform featuring smart contract functionality (the “Laocon Platform”) based on blockchain technology networks employing the Tokens, where cybersecurity clients can use the platform to conduct security tests on their websites, systems or applications to identify any vulnerability to cyber-attacks.
   b. The Tokens will function as utility tokens and allow users to submit their web applications and systems for security testing by white hat hackers registered on the Laocon Platform, who will perform security tests based on the client’s requests and submit a report of their analysis on the platform.
   c. The White Paper states that the Tokens can be used by clients to pay for platform usage fees and to purchase the relevant test reports submitted by white hat hackers assigned to a client.
d. The Issuer has not apprised us on whether the Tokens will be utilised for any purpose other than for the purposes enumerated under paragraph 3b and 3c above.

e. We are further advised that the Issuer will issue a fixed amount of Tokens for sale during a specified period and that the Tokens may subsequently be traded on independent cryptocurrency exchange(s).

B. ISSUE

4. The specific issue that we have been instructed to opine upon and to render our legal advice on is whether the Token is a ‘strict utility’ token that will not be regulated by the Monetary Authority of Singapore ("MAS") or whether the offer or issuance of the Token is to be regulated by MAS because the Token has been deemed a capital markets product and/or collective investment scheme (CIS) under the definition section of the Securities and Futures Act ("SFA") and any other related subsidiary legislation.

5. We have not been instructed to opine on, or provide any advice, on any query or matter other than that set out in the preceding paragraph.

C. EXECUTIVE SUMMARY

6. Based on the instructions you have provided to us and as set out above, we are of the opinion that:

   a. The offer or issuance of the Tokens will likely not be deemed a capital markets product for purposes of the SFA nor will the offer or issuance of the Tokens be deemed an ownership of a unit in a CIS or an option to acquire an interest in a CIS. The MAS issued a Guide to Digital Token Offerings on 14 November 2017 (the "DTO Guide"). Based on our review of the (non-exhaustive) DTO Guide (including the case studies in the DTO Guide) and assessment based on our specific fact pattern, the SFA and related subsidiary legislation will likely not apply to the offer or issuance of the Tokens.

   b. It is also likely that the Issuer’s proposed Token Sale or intended model will not constitute a Stored Value Facility within the meaning of the Payment Systems (Oversight) Act (Cap. 222A) ("PSOA").

   c. The Issuer is advised to undertake robust due diligence measures in relation to anti-money laundering ("AML") and countering the financing of terrorism ("CFT") regulations and adhere to the MAS Notices on Prevention of Money Laundering and Countering the Financing of Terrorism.

   d. The Issuer is obliged to report suspicious transactions pursuant to section 39 of the Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A) and to strictly adhere to the Terrorism (Suppression of Financing Act) (Cap. 325) and all prevailing United Nations Security Council Resolutions.

D. ANALYSIS
MAS’ Clarification and the DTO Guide

7. On 1 August 2017, MAS issued a press release "MAS clarifies regulatory position on the offer of digital tokens in Singapore" (the "MAS Clarification") stating:

"[MAS] clarified today that the offer or issue of digital tokens in Singapore will be regulated by MAS if the digital tokens constitute products regulated under the Securities and Futures Act (Cap. 289) (SFA).

... MAS has observed that the function of digital tokens has evolved beyond just being a virtual currency. For example, digital tokens may represent ownership or a security interest over an issuer’s assets or property. Such tokens may therefore be considered an offer of shares or units in a collective investment scheme under the SFA. Digital tokens may also represent a debt owed by an issuer and be considered a debenture under the SFA.

Where digital tokens fall within the definition of securities in the SFA, issuers of such tokens would be required to lodge and register a prospectus with MAS prior to the offer of such tokens, unless exempted. Issuers or intermediaries of such tokens would also be subject to licensing requirements under the SFA and Financial Advisers Act (Cap. 110), unless exempted, and the applicable requirements on anti-money laundering and countering the financing of terrorism. In addition, platforms facilitating secondary trading of such tokens would also have to be approved or recognised by MAS as an approved exchange or recognised market operator respectively under the SFA.

Examples of schemes falling under the revised definition of a collective investment scheme are found in Section 3 of the Consultation Paper on Proposals to Enhance Regulatory Safeguards for Investors in the Capital Markets, July 2014. [Emphasis added.]

8. It is clear from the MAS Clarification that MAS will look into the substance of the arrangement to consider whether it would amount to securities or collective investment schemes presently regulated by MAS, and not merely the labels or mode of arrangements.

9. The approach undertaken by MAS is to assess the underlying nature and characteristics of the Tokens to ascertain if there is any underlying security or ownership interest or right to acquire an ownership interest in the Tokens.

10. Then on 14 November 2017, MAS issued the DTO Guide. It stated that it would examine the structure and characteristics of, including the rights attached to, a digital token in determining if the digital token is a type of capital markets products regulated under the SFA. Capital markets products means "any securities, futures contracts, contracts or arrangements for the purposes of foreign exchange trading, contracts or arrangements for the purposes of leveraged foreign exchange trading, and such other products as MAS may prescribe as capital markets products".

11. In particular, MAS highlighted that a digital token may constitute a share, a debenture or a unit in a collective investment scheme ("CIS").
Offer of Securities under the SFA

12. Generally, when a person wishes to make an offer of investments or securities to the public, he would need to comply with certain rules and regulations, including the issuance of a compliant prospectus. Under section 240 of the SFA:

“No person shall make an offer of securities unless the offer — (a) is made in or accompanied by a prospectus in respect of the offer — (i) that is prepared in accordance with section 243; (ii) a copy of which, being one that has been signed in accordance with subsection (4A), is lodged with the Authority [the Monetary Authority of Singapore (MAS)]; and (iii) that is registered by the Authority; and (b) complies with such requirements as may be prescribed by the Authority. [Emphasis added.]”

13. Section 239(1) of the SFA defines the following terms:

“securities means —
(a) shares or units of shares of a corporation;
(b) debentures or units of debentures of an entity;
(c) interests in a limited partnership or limited liability partnership formed in Singapore or elsewhere; or
(d) such other product or class of products as the Authority may prescribe,
but does not include such other product or class of products as the Authority may prescribe as not being securities; …
“debenture” includes debenture stock, bonds, notes and any other debt securities issued by a corporation or any other entity, whether or not constituting a charge on the assets of the issuer but does not include —
(a) a cheque, letter of credit, order for the payment of money or bill of exchange;
Section 2(1) of the SFA.
(b) subject to the regulations made under this Act, a promissory note having a face value of not less than $100,000 and having a maturity period of not more than 12 months; or
(c) for the purposes of the application of this definition to a provision of this Act in respect of which any regulations made thereunder provide that the word "debenture" does not include a prescribed document or a document included in a prescribed class of documents, that document or a document included in that class of documents, as the case may be”.

14. Section 239(3) of the SFA further provides:

"(3) For the purposes of this Division —
(a) any invitation to a person to deposit money with or to lend money to an entity shall be deemed to be an offer of debentures of the entity; and
Offer of Securities under the SFA

12. Generally, when a person wishes to make an offer of investments or securities to the public, he would need to comply with certain rules and regulations, including the issuance of a compliant prospectus. Under section 240 of the SFA:

“No person shall make an offer of securities unless the offer — (a) is made in or accompanied by a prospectus in respect of the offer — (i) that is prepared in accordance with section 243; (ii) a copy of which, being one that has been signed in accordance with subsection (4A), is lodged with the Authority [the Monetary Authority of Singapore (MAS)]; and (iii) that is registered by the Authority; and (b) complies with such requirements as may be prescribed by the Authority. [Emphasis added.]”

13. Section 239(1) of the SFA defines the following terms:

“securities means —
(a) shares or units of shares of a corporation;
(b) debentures or units of debentures of an entity;
(c) interests in a limited partnership or limited liability partnership formed in Singapore or elsewhere; or
(d) such other product or class of products as the Authority may prescribe, but does not include such other product or class of products as the Authority may prescribe as not being securities; …
“debenture” includes debenture stock, bonds, notes and any other debt securities issued by a corporation or any other entity, whether or not constituting a charge on the assets of the issuer but does not include —
(a) a cheque, letter of credit, order for the payment of money or bill of exchange;

Section 2(1) of the SFA.
(b) subject to the regulations made under this Act, a promissory note having a face value of not less than $100,000 and having a maturity period of not more than 12 months; or
(c) for the purposes of the application of this definition to a provision of this Act in respect of which any regulations made thereunder provide that the word "debenture" does not include a prescribed document or a document included in a prescribed class of documents, that document or a document included in that class of documents, as the case may be”.

14. Section 239(3) of the SFA further provides:

"(3) For the purposes of this Division —
(a) any invitation to a person to deposit money with or to lend money to an entity shall be deemed to be an offer of debentures of the entity; and
(b) any document that is issued or intended or required to be issued by an entity acknowledging or evidencing or constituting an acknowledgment of the indebtedness of the entity in respect of any money that is or may be deposited with or lent to the entity in response to such an invitation shall be deemed to be a debenture."

15. Based on our assessment of the business model presented in the White Paper, it is unlikely that the proposed Token Sale will be deemed to be an offer of shares or debentures under the SFA and related subsidiary legislation because the Tokens are strictly used for supporting services and functionalities as well as making payments on the Laocon Platform as well as on co-operating enterprises and applications. The White Paper does not state that the Tokens provide the buyer of the Tokens with a share or stake in the Platform or in the co-operating enterprises and applications.

16. Based on the functions of the Tokens described in paragraph 15 above, the value of the Tokens is not based on the market acceptance of the Tokens or on buyers’ interest in any share, benefit or security interest in the Issuer’s cryptocurrency project. The Token is therefore not a security, but a token with utilitarian value only, i.e. a ‘utility token’ for consumptive use, including for accessing the services on the Platform and as a means of payment for those services and used as bounty rewards.

17. We are further instructed that although the Distributor (as defined in the White Paper) will deploy all proceeds of sale of the Tokens to fund the Issuer’s cryptocurrency project, business and operations, the buyer of the Tokens will not have any stake in the Issuer’s cryptocurrency project, business and operations by virtue of acquiring the Tokens. Although it is expressly stated in the White Paper (pages 10-11) that the Laocon Platform will provide benefits to its stakeholders including providing access to higher quality service at lower cost, matching cybersecurity supply and demand as well as strengthening cybersecurity, Token holders will nevertheless, not have any ownership rights or stake in the architecture or platform. The Tokens will thus not confer any other benefit or security interest in any capital markets product as defined in the SFA nor do the Tokens provide the buyer of the Tokens with a right or interest in a CIS or an option to acquire a right or interest in a CIS. The Tokens also do not provide the buyer with any equity interest or otherwise in the shares of the Issuer.

18. According to the White Paper, the Issuer plans to maximize utility of the Laocon Platform in the future by offering further consumptive uses including providing cybersecurity personnel recruiting services, consulting and other cybersecurity support services. It is clear that the addition of these future services will not change the nature of the Tokens which will remain as ‘utility tokens’.

19. It is also clear from the White Paper that the value of the Tokens is dependent on the health of the platform and the adoption of its use by its users and the value of the Tokens is not dependent on any ownership interest in shares or any investment.

20. The DTO Guide suggests that a share "confers or represents ownership interest in a corporation, represents liability of the token holder in the corporation, and represents mutual covenants with other token holders in the corporation inter se" (DTO Guide at 3).
21. The leading Singapore law treatise on company law (Walter Woon on Company Law (3rd Edition, 2009) at 424) states:

"A share is the interest of a shareholder in the company measured by a sum of money, for the purpose of liability in the first place, and of interest in the second, but also consisting of a series of mutual covenants entered into by all the shareholders inter se in accordance with s 39(1) of the CA": per Farwell J in Borland's Trustee v Steel Brothers & Co Ltd. Shares are 'a right of participation in the company on the terms of the articles of association': per curiam, Prudential Assurance Co Ltd v Newman Industries Ltd (No 2). 'Primarily a share in a company is a piece of property conferring rights in relation to distributions of income and of capital': per Dixon J in Peters' American Delicacy Co Ltd v Heath”.

22. The Tokens will most likely not be characterised as shares. While "shares" is not expressly defined in the SFA, it is assumed to refer to "shares" as defined in the Companies Act. Section 2(1) of the Companies Act defines it as follows: "A share in the share capital of a corporation and includes stock except where a distinction between stocks and shares is expressed or implied". Based on what has been set out in the White Paper, Tokens would not constitute share capital of any corporation. It is expressly stated that Tokens will only be used by users for accessing the Issuer’s platform and to pay for cybersecurity testing and analysis as well as used on cooperating enterprises and applications. Nowhere does it propose that Tokens will grant users any rights of participation, income, profit or returns in the Issuer's assets.

23. To be prudent, the Issuer should expressly state in marketing materials, the terms and conditions of the Token Sale and/or relevant white paper that Tokens will have no rights or functions attached to them, and will not grant token holders any ownership, voting or management right or interest in the Issuer, or any right to receive profits, income, or other payments or returns arising from the acquisition, holding, management or disposal of, the exercise of, the redemption of, or the expiry of, any right, interest, title or benefit in the Issuer, the Issuer’s property, or the Issuer’s platform.

24. The Tokens will thus not be deemed to be shares nor constitute securities under the SFA.

25. It is also unlikely that the Tokens would be deemed by MAS to be "debentures". The definition of "debentures" includes "any other debt securities".

a. Essential to debentures is indebtedness. The proposed Token Sale envisages a sale of Tokens. Nowhere in the White Paper does it suggest that Tokens will be exchanged for repayment of money as a matter of legal right. Nonetheless, to be prudent, the Issuer should expressly state that holding Tokens will not grant token holders any right of repayment by the Issuer in respect of any value paid for the Tokens or indeed any return on investment.

b. Further, there is no promise or guarantee by the Issuer to buy back Tokens at any time from any person or to exchange Tokens for money or money’s equivalent.
c. The fact that Tokens may subsequently be traded on independent cryptocurrency exchanges does not make Tokens some form of debenture. The onus will be on the cryptocurrency exchange or operator of the platforms to be regulated. In such a scenario, any exchange of Tokens for money or money’s equivalent will be on a secondary market with third parties on a willing buyer willing seller basis, and not as a matter of legal right or obligation.

26. Further, the MAS has not prescribed cryptocurrency or similar things as “such other product or class of products” as “securities” within the meaning of section 239(1) of the SFA. It is therefore unlikely that the Tokens would be caught by this Division in the SFA.

Collective Investment Schemes under the SFA

27. The SFA and its subsidiary legislation, the Securities and Futures (Offers of Investments) (Collective Investment Schemes) Regulations ("CIS Regulations"), also regulates CIS. The CIS Code will apply if an arrangement falls within the meaning of a CIS. A CIS must be authorized (if constituted in Singapore) or recognised (if constituted outside) by MAS.

28. A CIS is defined in section 2(1) of the SFA as follows:

“collective investment scheme’ means —

(a) an arrangement in respect of any property —

(i) under which —

(A) the participants do not have day-to-day control over the management of the property, whether or not they have the right to be consulted or to give directions in respect of such management; and

(B) the property is managed as a whole by or on behalf of a manager;

(ii) under which the contributions of the participants and the profits or income from which payments are to be made to them are pooled; and

(iii) the purpose or effect, or purported purpose or effect, of which is to enable the participants (whether by acquiring any right, interest, title or benefit in the property or any part of the property or otherwise) —

(A) to participate in or receive profits, income, or other payments or returns arising from the acquisition, holding, management or disposal of, the exercise of, the redemption of, or the expiry of, any right, interest, title or benefit in the property or any part of the property; or

(B) to receive sums paid out of such profits, income, or other payments or returns; or

(b) an arrangement which is an arrangement, or is of a class or description of arrangements, specified by the Authority as a collective investment scheme by notice published in the Gazetto..."
29. The proposed Token Sale is not likely to constitute a CIS. Under the proposed Token Sale, the White Paper does not suggest that the Token purchasers or holders will be able to "participate in or receive profits, income, or other payments or returns arising from the acquisition, holding, management or disposal of, the exercise of, the redemption of, or the expiry of, any right, interest, title or benefit in the property or any part of the property" or "to receive sums paid out of such profits, income, or other payments or returns".

30. The Issuer is advised to expressly state in commercial/legal documentation that Tokens will not grant token holders any right to receive profits, income, or other payments or returns arising from the acquisition, holding, management or disposal of, the exercise of, the redemption of, or the expiry of, any right, interest, title or benefit in the Issuer, the Issuer's property, or the Issuer's platform, or to any return on investment.

Case Study 1 in the DTO Guide

31. Our analysis above is buttressed by the case study 1 set out in the DTO Guide at page 8. The case study hypothetical states:

"Company A plans to set up a platform to enable sharing and rental of computing power amongst the users of the platform. Company A intends to offer digital tokens ("Token A") in Singapore to raise funds to develop the platform. Token A will give token holders access rights to use Company A's platform. The token can be used to pay for renting computing power provided by other platform users. Token A will not have any other rights or functions attached to it. Company A intends to offer Token A to any person globally, including in Singapore.

Application of securities laws administered by MAS in respect of an offer of Token A

• A holder of Token A will only have rights to access and use Company A's platform, and the right to use Token A to pay for rental of computing power provided by other users. Token A will not provide its holder any other rights or functions attached to it. Hence, Token A will not constitute securities under the SFA.

• Company A's offer of Token A will not be subject to any requirement under the SFA or the FAA".

32. The proposed Token Sale and envisaged Tokens are substantially similar to the aforesaid case study. Tokens, like Token A in the case study, "will give token holders access rights to use ... [a] platform" developed and operated by the Issuer. Tokens, like Token A, "will not have any other rights or functions attached to it". On these premises, MAS has indicated that such digital tokens "will not constitute securities under the SFA".
Stored Value Facility

33. The envisaged Tokens would not be likely to constitute a Stored Value Facility within the meaning of the PSOA.

34. Section 2(1) of the PSOA defines "stored value" and "stored value facility" ("SVF") as follows:

"stored value", in relation to a stored value facility, means the sum of money that—

(a) has been paid in advance for goods or services intended to be purchased through the use of the stored value facility;

(b) is available for use from time to time for making payment under the terms and conditions applying to the stored value facility; and

(c) is held by the holder of the stored value facility;

"stored value facility" means —

(a) a facility (other than cash), whether in physical or electronic form, which is purchased or otherwise acquired by a person (referred to in this Act as the user) to be used as a means of making payment for goods or services up to the amount of the stored value that is available for use under the terms and conditions applying to the facility, and payment for the goods or services is made by the holder of the stored value in respect of the facility (rather than by the user); or

(b) all the facilities referred to in paragraph (a) provided under the same terms and conditions; …

"holder", in relation to a stored value facility, means the person who holds the stored value and makes payment for goods or services referred to in the definition of "stored value facility"; …"

35. MAS’ Stored Value Facility Guidelines (June 2008) ("Guidelines") sets out an explanation of SVF:

"A stored value facility ("SVF") is a facility that is used for payment of goods or services up to its stored value. A person who wishes to use an SVF ("user") will purchase the SVF containing a certain stored value. This stored value amount is paid in advance to the stored value holder of a SVF ("holder"). Thereafter, the user will be able to use the SVF to purchase goods or services from merchants who accept the stored value in the SVF as payment ("merchants"). These merchants will redeem from the holder the stored value that they have accepted from users. SVFs can be provided in different forms, such as smart cards, contact-less cards, magnetic stripe cards, paper vouchers, micro-chips and internet accounts. Certain forms of SVFs allow for the "topping up" of additional stored value in consideration of cash or other means of payment."
36. In the 2nd parliamentary reading of the Payment Systems (Oversight) Bill on 16 January 2006, then Minister for Education Tharman Shanmugаратnam defined "stored value facility" as "prepaid payment instruments, most commonly used for low value retail payments".

37. There are no reported court judgments on the meaning of "stored value facility".

38. Applying the definitions, including those in section 2(1) of the PSOA and the Guidelines, set out above, we are of the opinion that the envisaged Tokens will not constitute a "stored value facility".

39. While the Tokens will likely be deemed to be "a facility (other than cash), whether in physical or electronic form, which is purchased or otherwise acquired by a person … to be used as a means of making payment for goods or services", the key distinction between the Tokens and a stored value facility is that for Tokens, the Issuer will not be making payment for the goods or services up to the amount of the value of the tokens. Instead, when customers exchange with merchants Tokens for goods or services, the merchants will not look to the Issuer to further exchange the tokens for money. The merchants may use the tokens to pay for services on the platform or trade them on an independent exchange. In contrast, a stored value facility requires that "payment for the goods or services [be] made by the holder of the stored value in respect of the facility".

AML/CFT

40. MAS has stated in the DTO Guide that digital tokens which may not be within MAS' regulatory purview may nonetheless be subject to other legislation for combating money laundering and terrorism financing, and in particular the following (DTO Guide at 7):

a. Obligations to report suspicious transactions with the Suspicious Transaction Reporting Office, Commercial Affairs Department of the Singapore Police Force pursuant to section 39 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A) ("CDSA");

b. Prohibitions from dealing with or providing financial services to designated individuals and entities pursuant to the Terrorism (Suppression of Financing) Act (Cap. 325) ("TSOFA") and various regulations giving effect to United Nations Security Council Resolutions.

41. The proposed Token Sale will be similar to the operation a stored value facility, although it will not be identical to or amount to a stored value facility. As such, it is apposite to consider the MAS Notice PSOA-N02 "Notice on Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Stored Value Facilities" for AML/CFT guidance.

42. Paragraph 6.2 of PSOA-N02 states that where the organisation "has any reasonable grounds to suspect that the assets or funds of a customer are proceeds of drug dealing or criminal conduct as defined in the CDSA, or are property related to the facilitation or carrying out of any terrorism financing offence as defined in the TSOFA, the relevant holder shall—(a) not establish business relations with, or undertake a
transaction for, the customer; and (b) file an STR [suspicious transaction report], and extend a copy to [MAS] for information”.

43. Do note that the failure to file an STR would constitute a criminal offence under the CDSA. Section 39(1) of the CDSA states:

“Where a person knows or has reasonable grounds to suspect that any property—

(a) in whole or in part, directly or indirectly, represents the proceeds of;
(b) was used in connection with; or
(c) is intended to be used in connection with,

any act which may constitute drug dealing or criminal conduct, as the case may be, and the information or matter on which the knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment, he shall disclose the knowledge or suspicion or the information or other matter on which that knowledge or suspicion is based to a Suspicious Transaction Reporting Officer as soon as is reasonably practicable after it comes to his attention.”

44. It is therefore important that the Issuer conducts the necessary due diligence measures to verify the identity of Token purchasers before executing a sale of tokens with the customer. To this end, the Issuer should obtain at least the following information (cf. Paragraph 6.6 of PSOA-N02):

a. full name, including any aliases;

b. unique identification number (such as an identity card number, birth certificate number or passport number, or where the customer is not a natural person, the incorporation number or business registration number);

c. the customer’s:
  i. residential address; or
  ii. registered or business address, and if different, principal place of business, as may be appropriate;

d. date of birth, establishment, incorporation or registration (as may be appropriate); and

e. nationality, place of incorporation or place of registration (as may be appropriate).

45. Where the token purchaser is a legal person or legal arrangement, the Issuer should, apart from identifying the purchaser, also identify the legal form, constitution and powers that regulate and bind the legal person or legal arrangement (cf. Paragraph 6.7 of PSOA-N02).

46. Where the token purchaser is a corporate entity or arrangement (as opposed to an individual), the Issuer should identify the connected parties of the purchaser, by
obtaining at least the following information of each connected party (cf. Paragraph 6.8 of PSOA-N02):

a. full name, including any aliases; and

b. unique identification number (such as an identity card number, birth certificate number or passport number of the connected party).

47. the Issuer should verify the identity of token purchasers using reliable, independent source data, documents or information. Where the token purchaser is a corporate entity or arrangement, the Issuer should verify the legal form, proof of existence, constitution and powers that regulate and bind the customer, using reliable, independent source data, documents or information (cf. Paragraph 6.9 of PSOA-N02).

48. Where a token purchaser appoints one or more natural persons to act on its behalf in establishing business relations with the Issuer or the purchaser is not a natural person, the Issuer should (cf. Paragraph 6.10 of PSOA-N02):

a. identify each natural person who acts or is appointed to act on behalf of the customer by obtaining at least the following information of such natural person:

   i. full name, including any aliases;

   ii. unique identification number (such as an identity card number, birth certificate number or passport number);

   iii. residential address;

   iv. date of birth;

   v. nationality; and

b. verify the identity of each natural person using reliable, independent source data, documents or information.

49. the Issuer should verify the due authority of each natural person appointed to act on behalf of the token purchaser by obtaining at least the appropriate documentary evidence authorising the appointment of such natural person by the token purchaser to act on his or its behalf (cf. Paragraph 6.11 of PSOA-N02).

50. the Issuer should also verify whether any potential token purchaser is named in MAS’ lists of designated individuals and entities before engaging in any sale or purchase activity with them to prevent violation of the MAS Act, United Nations Act, and TSOFA. The URL is as follows:


51. The aforesaid measures and guidelines are not exhaustive. You should refer to the entire PSOA-N02 and any other relevant MAS Notices and guidances to ensure your compliance with AML/CFT measures.
52. You should also note that MAS intends to establish a new payments services framework which would address, among other things, virtual currencies. This is a work-in-progress presently but may impact the Issuer in the future.

E. DISCLAIMERS

53. This legal opinion is based on Singapore law as it stands on the date of this opinion, and is based solely on the instructions, information and documents which have been provided by you to us and set out above, the veracity of which we shall not be held responsible for. For the purpose of this opinion, we have assumed that the information you have provided to us are complete, up to date and accurate.

54. This legal opinion is strictly based on the fact pattern enumerated in the White Paper that has been provided to us. We have not been apprised of any other information, facts nor have we sighted any legal documentation or any other information memorandum or details that would affect our legal assessment.

55. We express no opinion on any other law as it affects or would be applied in any jurisdiction other than Singapore. We have not made any investigation of, and do not express any opinion on, any other law. You are advised to obtain legal advice from other jurisdictions as applicable.

56. This legal opinion is intended solely for you only and shall not be relied on by any other party for any purpose.

Yours faithfully

KGP Legal LLC
11

source

   https://www.marketsandmarkets.com/PressReleases/cybersecurity.asp

2. ICE71 - Cyber Security Agency of Singapore
   https://ice71.sg/

3. Accenture 「2017 COST OF CYBER CRIME STUDY」

4. NPO Japan Network Security Associate 「2016年度国内情報セキュリティ市場調査」

5. METI 「IT人材の最新動向と将来推計に関する調査結果」

6. IDC 「The DIGITAL UNIVERSE of OPPORTUNITIES」

7. 「Adapting to Disruption」
   https://www.atkearney.co.jp/paper//asset_publisher/dVxv4Hz2h8bS/content/id/13580677
THANK YOU
by LAOCON