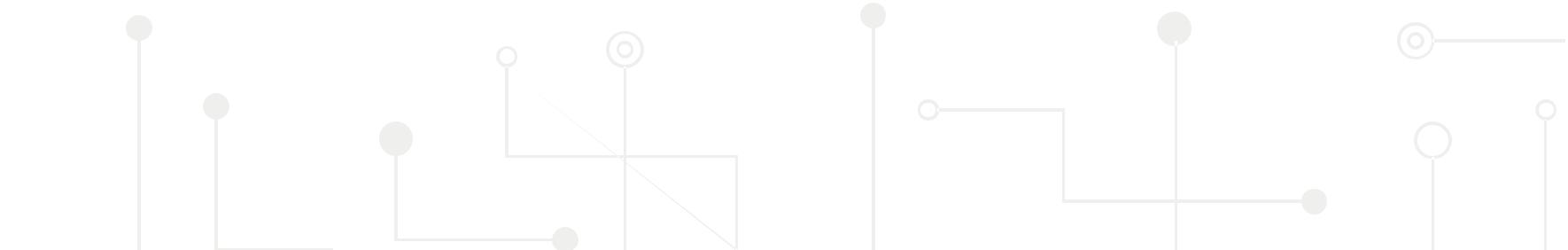


1



**Table of Contents**

|  |  |
| --- | --- |
| **Legal Disclaimer** | 3 |
| **Executive Summary** | 4 |
| **Business Strategy Overview** | 5 |
| **Background** | 6 |
| **ROLE OF THE White Hat Hackers** | 6 |
| Increasing cybersecurity threats | 6 |
| Increasing shortage of skilled cybersecurity personnel | 7 |
| **WORKING WITH White Hat Hackers** | 9 |
| Penetration Testing versus Ethical Hacking | 10 |
| Market Size | 11 |
| Market Opportunity | 11 |
| **WHY White Hat Hackers FAIL TO CONNECT** | 12 |
| **AntiHACK.me’s Solution** | 13 |
| Proof of Authority | 14 |
| Hacker Identity and Data Management(HIMS) | 15 |
| **AntiHACK.me AS A SERVICE** | 15 |
| Business Strategy Overview | 16 |
| Core features of AntiHACK.me | 17 |
| Defining the bug bounty security parameters | 18 |
| 1. Maturity assessment tool | 18 |
| 2. Vulnerability reports | 18 |
| 3. The AntiHACK.me Fixer | 18 |
| 4. Mediation | 18 |
| 5. AntiHACK.me AI | 19 |
| 6. Hackers Hall of Fame | 19 |
| 7. Multi-Signature Wallet | 20 |
| Overview of Hall of Fame | 21 |
| **LEADERBOARD** | 22 |
| **WALKTHROUGH** | 23 |
| Penetration Testers | 23 |
| Validation and Payment | 24 |
| **THE ATH TOKEN** | 25 |
| Tokenomics | 25 |
| **THE ANTIHACK.ME ACADEMY** | 26 |
| **FACT SHEET** | 27 |
| **MARKET SUPPLY** | 28 |
| **ROADMAP** | 29 |
| **COMPANIES THAT OUR HACKERS WORKED WITH** | 30 |
| **OUR PARTNERS** | 31 |
| **TEAM PAGE** | 32 |
| Business Advisors | 35 |
| ICO Advisors | 37 |
| Cybersecurity Advisors | 39 |
| Security Experts | 40 |
|  | 2 |



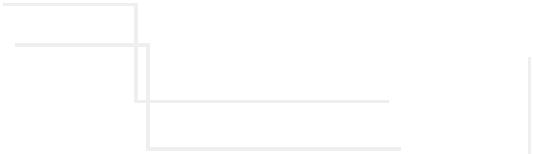
**Legal Disclaimer**

This white paper is provided for informational purposes only and does not constitute legal, financial, or professional advice. The content contained herein is based on the author's research, analysis, and interpretation of available information and industry best practices.

Readers are advised to consult with qualified legal, financial, or accounting professionals before making any decisions or taking any actions based on the information presented in this white paper. The author and publisher make no representations or warranties of any kind, express or implied, regarding the accuracy, completeness, reliability, suitability, or timeliness of the information contained herein.

Furthermore, the author and publisher disclaim any liability for any loss, damage, or inconvenience caused as a result of reliance on the information provided in this white paper or any errors or omissions therein. The views and opinions expressed in this document are those of the author and do not necessarily reflect the official policy or position of any organization or entity mentioned herein.

The content of this white paper may be subject to change without notice, and the author and publisher reserve the right to modify, update, or revise the information contained herein at any time. By accessing or using this white paper, readers agree to release the author and publisher from any and all liability arising from or related to their use of the information presented herein.

 3

# INTRODUCTION

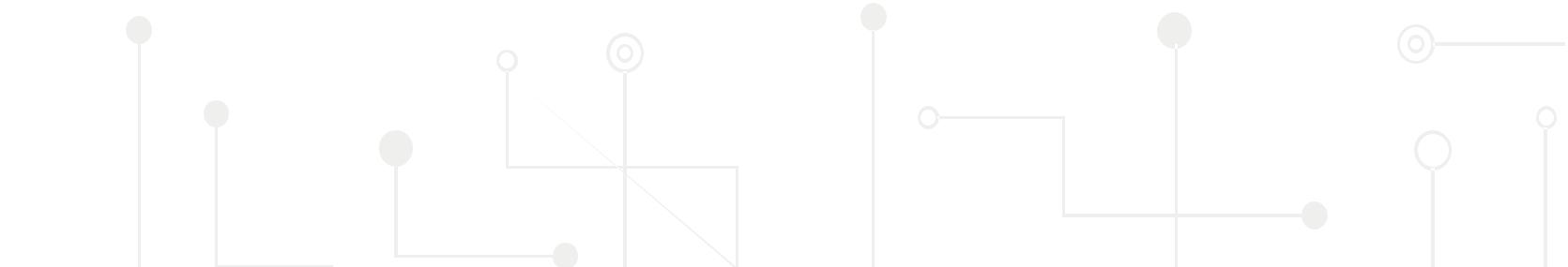
## Executive Summary

Cybersecurity has become increasingly essential to businesses in their daily operations. The majority of big corporations have adjusted well to the growing cyber threat given their budget surplus and muscles to hire top cybersecurity firms. On the other hand, smaller-sized businesses find themselves daunted by the expertise and budget required to properly secure their cyber operations. This has created a David versus Goliath battle between hackers and firms, where the latter finds himself encumbered from all sides. Bug bounty programs, initiated by Netscape in 1995, offers a decentralized and cost-effective method to source for code vulnerabilities. AntiHACK.me is disrupting, democratizing and expanding the White Hat Hacking ecosystem by building a blockchain-powered hacker network (HacketNet). It leverages on anonymous transactions and a private, highly secured testing environment to solve the existing challenges in the cybersecurity industry and fulfil the ever-growing demand for penetration testing.



4

## OVERVIEW

****

Framework for detecting, mitigating, and preventing financial statement fraud

Interdisciplinary expertise

Overview of financial statement fraud

Transparency and Accountability: Advocating for greater transparency, accountability, and integrity in financial reporting practices within the insurance industry to foster trust and confidence among stakeholders.

Practical Guidance: Offering actionable recommendations and guidance for implementing robust internal controls, risk management frameworks, and fraud detection systems tailored to the insurance sector.

Detection and Prevention Strategies: Providing insights into effective methodologies, techniques, and best practices for detecting, mitigating, and preventing financial statement fraud within insurance companies.

Understanding Financial Statement Fraud: Exploring the definition, types, and common red flags of financial statement fraud in the insurance industry.

WHAT

HOW

WHY

Intent: The intent of this white paper is to serve as a definitive resource for insurance professionals seeking to enhance their understanding of financial statement fraud and implement robust fraud detection and prevention measures

Mission: Our mission is to provide comprehensive insights, practical guidance, and actionable recommendations for detecting, mitigating, and preventing financial statement fraud in insurance companies

Vision: The vision of this white paper is to empower insurance industry professionals with the knowledge, tools, and strategies necessary to combat financial statement fraud effectively

**Introduction**

**Overview of**

****

**Financial Statement Fraud in the Insurance Industry**

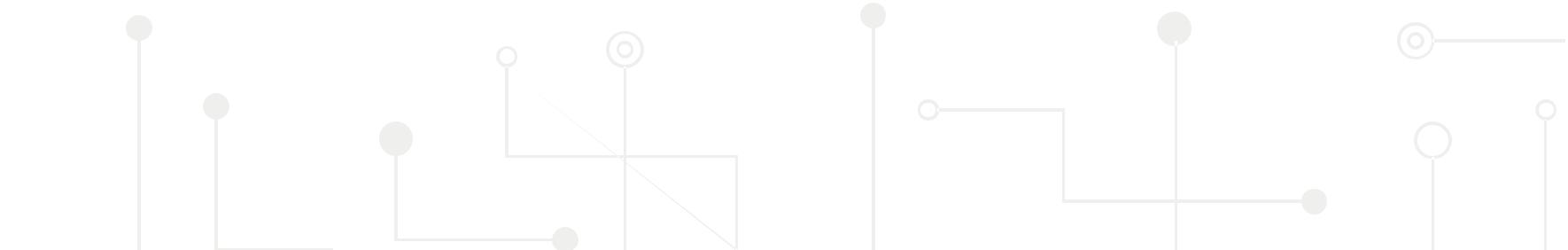
***“Financial statement fraud can take many forms, including revenue recognition manipulation, understating or overstating expenses, manipulating cash flow statements, and misrepresenting assets or liabilities. Such fraudulent activities can have devastating effects on companies' reputations and lead to significant losses for investors and other stakeholders.” (Xiaoyu et al., 2018)***

**Threat of Financial Statement Fraud**

Financial statement fraud poses a significant threat to the stability and integrity of the insurance industry. As entities entrusted with managing substantial financial assets and liabilities, insurance companies are vulnerable to various forms of fraudulent activities that can distort their financial statements, mislead investors, and undermine public trust. Understanding the nature, causes, and implications of financial statement fraud in the insurance sector is crucial for implementing effective detection and prevention measures.

**Why Detect and Prevent Fraudulent Activities?**

1. Fraud can result in significant financial losses for individuals, businesses, and organizations.
2. Fraud can damage an organization's reputation and erode customer trust.
3. Detecting and preventing fraud helps organizations comply with legal and regulatory requirements.
4. Fraud prevention helps safeguard sensitive information, such as personal data and financial information.
5. Fraud can disrupt business operations, making prevention crucial for continuity.
6. In some cases, fraud can be linked to criminal organizations or terrorist financing, making detection and prevention a national security concern.
7. Proactive fraud prevention reduces the costs associated with investigating and prosecuting fraud cases.
8. Fraud prevention protects stakeholders, including employees, customers, and investors.

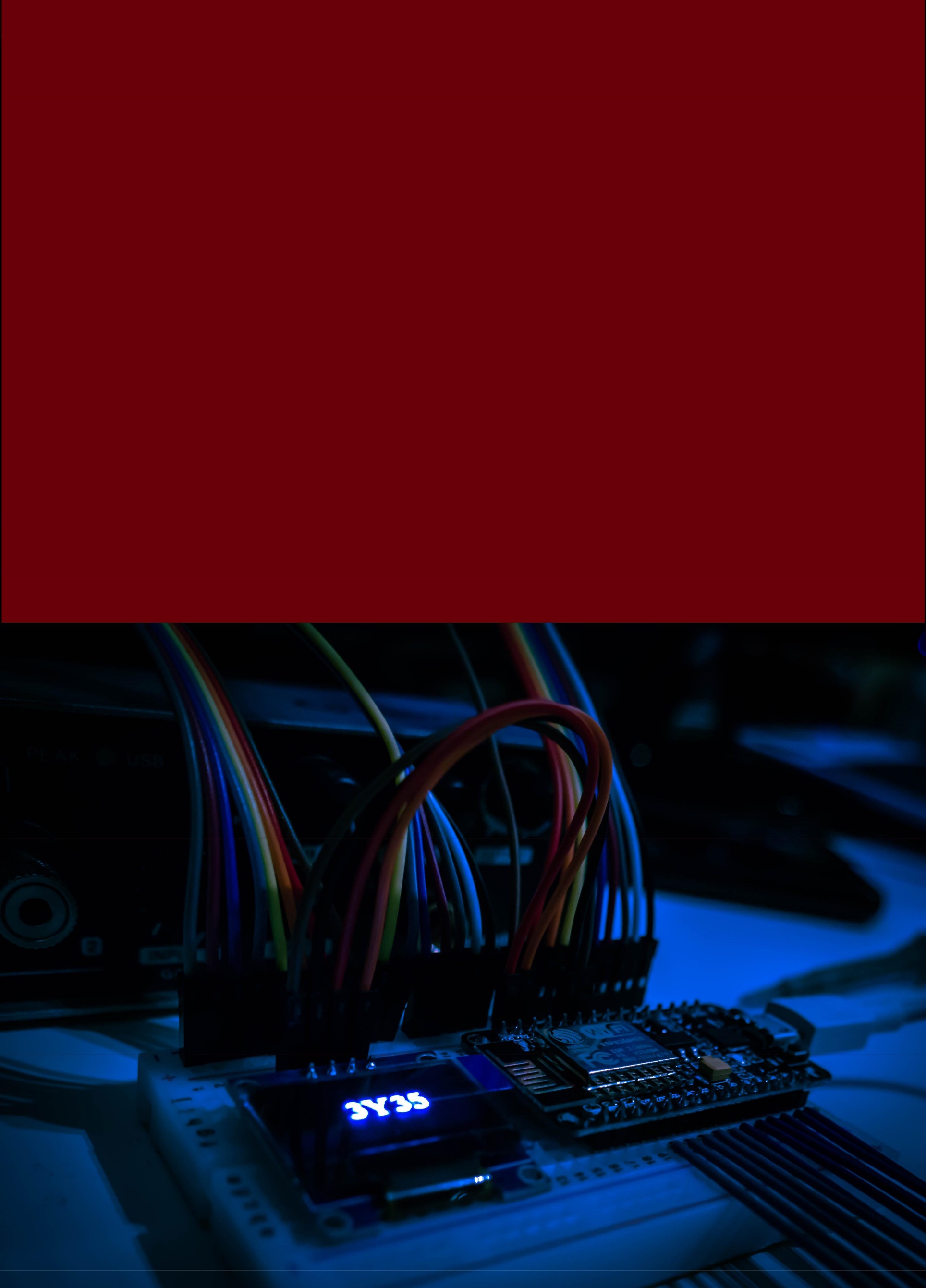


**OBJECTIVES**

**FINANCIAL STATEMENT FRAUD DETECTION**

* Outline effective methodologies, techniques, and best practices for detecting, mitigating, and preventing financial statement fraud within insurance companies, focusing on data analysis, modeling, and statistical analysis approaches.
* Equip insurance professionals with the knowledge, tools, and resources necessary to enhance their fraud detection capabilities, enabling them to identify and address potential red flags and indicators of financial statement fraud proactively.
* Provide comprehensive insights into the nature, causes, and implications of financial statement fraud in the insurance sector, enhancing awareness and understanding among executives, managers, auditors, and analysts.
* Stimulate further research, innovation, and interdisciplinary collaboration in the fields of forensic accounting, data analytics, machine learning, and risk management, advancing the state-of-the-art in financial statement fraud detection and prevention methodologies.



**Understanding Financial Statement Fraud**

Financial statement fraud comprises of various deceptive practices with the goal presenting a misleading perspective of a company's financial health. There are cases of revenue recognition fraud which involves recording sales before they are actually earned or recognizing fictitious sales, thereby inflating the company's revenue figures. Some companies do expense manipulation, this includes practices like understating expenses or delaying their recognition to make profits appear higher than they actually are. Both these methods aim to artificially boost the company's financial performance, misleading stakeholders about the true economic condition of the business.

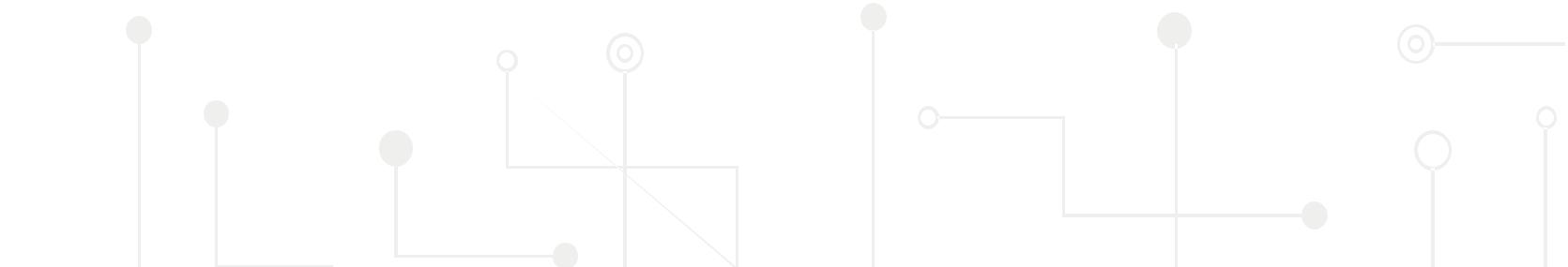
Companies also carry out asset misrepresentation where they inflate the value of company assets or fabricating nonexistent assets to enhance the balance sheet. There is also liability concealment in hiding or understating company liabilities to make the financial position appear stronger and equity manipulation which refers to the improper adjustment of shareholders' equity, often through unauthorized issuance or repurchase of shares. These fraudulent activities misrepresent the true financial condition and performance of a company, potentially leading to severe consequences for insurance companies and the broader financial market.

10

**Common Indicators**

1. Unusual or unexplained changes in financial statements
2. Inconsistencies in accounting records
3. Unusual or excessive transactions
4. Lack of transparency or disclosure
5. Unusual or unexplained payments
6. Changes in accounting policies or procedures
7. Unusual or unexplained relationships between management and third parties
8. Unusual or unexplained changes in management's compensation.

**Impact of Fraud on Insurance Companies**

****

**WHY WHITE HAT**

**HACKERS FAIL TO CONNECT**

****

Unfortunately, the market in which White Hat Hackers participate is currently controlled by cybersecurity firms – and the result is parlous. As one might expect when hackers try to work with cybersecurity firms, there is a certain cultural conflict rather like that of the cat and the mouse. Most hackers are by nature, the ‘off-the-grid’ kind of people, while cybersecurity experts tend to be buttoned-down micromanagers.

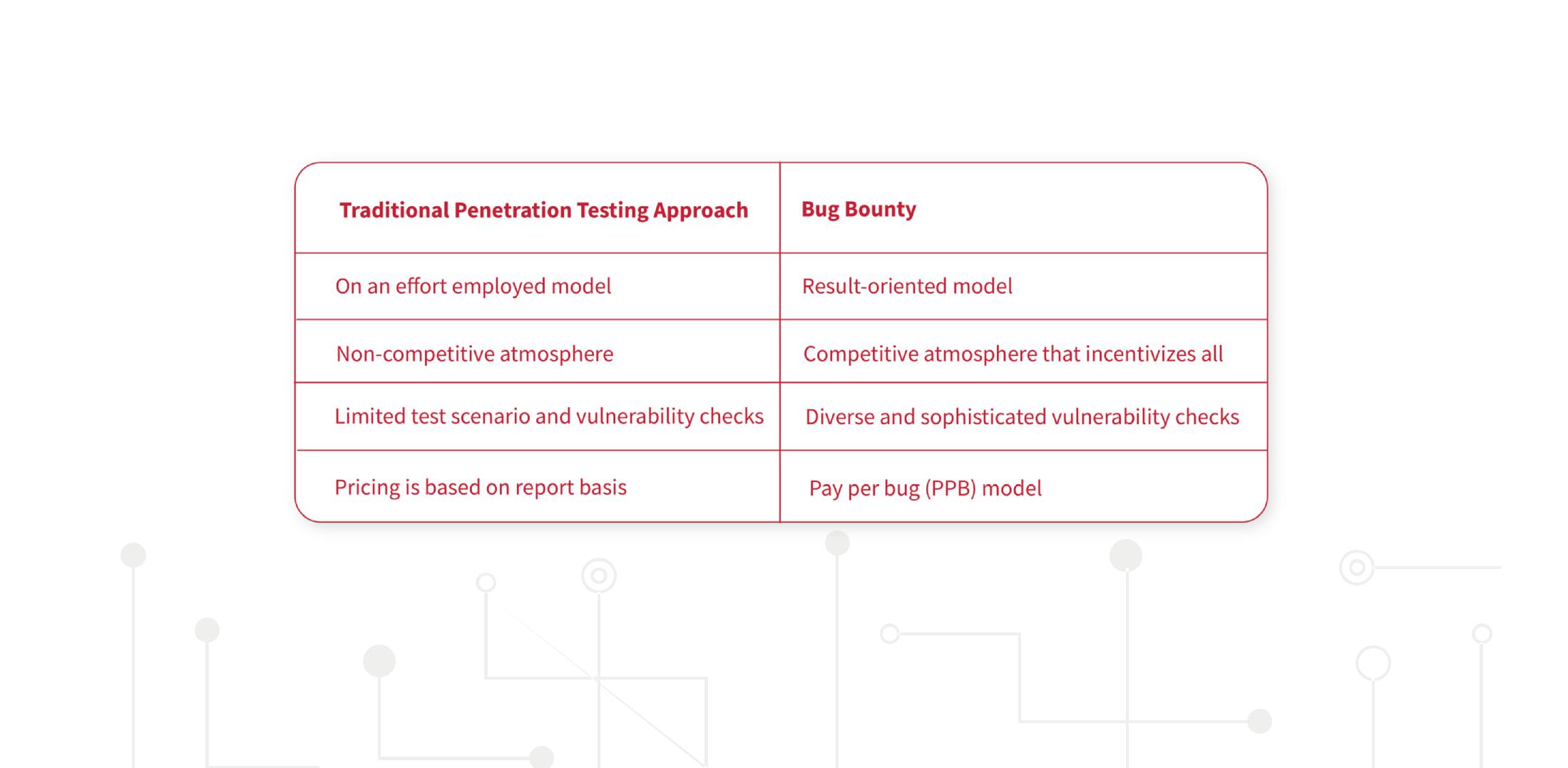
The first issue is as fundamental as identification: Hackers, regardless of the color of their hat, like to work anonymously, or at least pseudonymously. However,thisdoesnotgodownwellwithcybersecurity firms and it becomes particularly complicated for hackers when high-profile organizations like the UN or the IMF are involved. Similarly, cybersecurity firms have trouble validating the skills of hackers, and even in paying them. Because of their unconventional background, many companies, even some cybersecurity firms, are reluctant to work with White Hat Hackers. Most hackers do not always have the traditional finances, or they prefer to operate within a closed circle, protecting their identities. This can make the onboarding process for contract work with organizations problematic. Many White Hat Hackers also work in Eastern Europe, or in other emerging markets, where companies and financial institutions are not necessarily up-to-date.

**Traditional Option**

***“This Bug Bounty Platform, this Hackernet, is built by hackers, and for hackers. I am personally a hacker, and this has given us the unparalleled advantage of building a bug bounty program that specifically suits White Hat Hackers. Years of running AntiHACK.me have given me an unprecedented insight into the mindset of White Hat Hackers, who prefer freelance work to a routine 9 to 5 job at a cybersecurity firm.”***

***- Dexter Ng, Co-Founder & CTO***

Cybersecurity consulting firm: Current offerings in the market are too often provided by cybersecurity firms with in-house teams that conduct penetration testing for companies which have approached them. Typically, a base consultation fee, as well as additional costs, are charged, depending on the number and severity of bugs found and solved. This approach is costly as the base consultation fee is mandatory, even if no bugs are found or any issues are resolved. On top of that, the price increases exponentially for every supplementary solution. The cost can exceed the budget for smaller organizations who then cannot address security lapses.



12

**Bridging the Gap**

It is paradoxical that White Hat Hackers’ talent cannot connect with companies directly, particularly with smaller ones that cannot afford the big cybersecurity firms. Meanwhile, those that do engage the big firms may be overpaying for unnecessary services.



**AntiHACK.me’s Solution: HackerNet - Blockchain-Powered**

**Hacker Network and AI Driven Secured Hacker Testing**

**Environment**

We are disrupting, democratizing and expanding the White Hat Hacking ecosystem.



AntiHACK.me has been created to fill the gap between those who are seeking for White Hat Hackers’ services and the hackers themselves. By sourcing for White Hat Hackers in a decentralized manner and securing it on the blockchain, we are able to offer services transparently, preserving the hacker’s anonymity while ensuring that transactions are completed fairly. We can satisfy the ever-growing demand for penetration testing services with an economical offer that is affordable even for smaller companies.

Given that it is a pay-for-results only service, it comes in at a lower cost than the traditional approach, with guaranteed results and zero “consultation” fees. Rather than relying on a centralized party for extensive cybersecurity support, we instead embrace the philosophy of decentralization. Freelance White Hat Hackers are able to find employment on the AntiHACK via AntiHACK.me. The creation of HackerNet on the blockchain gives a platform to aspiring hackers, across geographical boundaries and time zones, to work together.



13



**Our AI-Driven Private and Decentralized Sandbox (HackerBox):**

The Hackerbox makes it possible for clients to submit a copy of their website/software/system; data is anonymized via machine learning and AI; hackers work with the anonymized and sanitized version to find vulnerabilities. HackerBox is robust and able to dynamically adapt to rules set by owners (clients) of the run-time environment, and also presents an easy-to-use format for White Hat Hackers to conduct penetration testing and send reports.

**Proof of Authority**

HackerBox runs on the Proof of Authority mechanism. Proof-of-Authority is a replacement for Proof-of-Work on the blockchain, where Proof-of-Work is generally used for verification. Instead of solving arbitrarily difficult mathematical problems, Proof-of-Authority uses a set of “authorities” - nodes that are explicitly allowed to create new blocks and secure the blockchain. But the basic principles of the blockchain are maintained: A transparent ledger which securely lists all transactions, and an anonymous environment so that hackers and clients need not make themselves known. Validators are entrusted to secure the network, generating blocks, and updating information on the sandbox.

There will be a total of 10 delegates with 3 running as the backup. A portion of this forged reward will go towards the AntiHACK.me academy and reward hackers who are on the hall of fame list.

**Proof of Authority consensus mechanism**

For the Proof of Authority network to work, these three conditions must be upheld: the validators’ identity must be true, the difficulty in obtaining eligibility and the procedural process of becoming a validator must be consistent for all.



14

**Reputation Score (HackerCred)**

In any consensus mechanism, there runs the risk of errant delegates with malicious intent. AntiHACK.me will verify the credentials of delegates thoroughly beforehand. However, there is no guarantee that these delegates would remain honest in the future. In this scenario, validators in place would access their credibility and the wayward delegate would face reputational repercussion. There is also a need to codify the reputational score to kick out deviant validator.

In the Hackernet, each delegate will be assigned a HackerCred (HC). Owners of ATH tokens are able to downvote HackerCred. The decrease in HackerCred (HC) beyond a certain level will cause the delegate to be booted out and replaced.

**Hacker Identity and Data Management (HIMS)**

HackerNet allows for active verification and secure storage of hacker identities and data on-chain via a number of cutting-edge identification techniques – Accenture identifies a number of high-grade alternatives to the ID and password system and Hackerbox may make use of as many as needed.8 Similarly, hackers will be obliged to provide proof of their skills and experience with a variety of submissions including certification, research credentials and proof of experience, to determine their ranking and expertise level. Clients will be able to get the certification of hackers prior to the engagement.

Beyond that, AntiHACK.me understands that sensitive personal details will be shared therefore, we are also venturing to explore our very own sidechain. A sidechain - essentially allows tokens or other digital assets from one blockchain to be securely used and stored in a separate blockchain and moved back to the original whenever needed. The sidechain developed would be made private to store sensitive identity information, therefore ensuring control on the privacy of data such that the national ID, name, and age are strictly confidential.



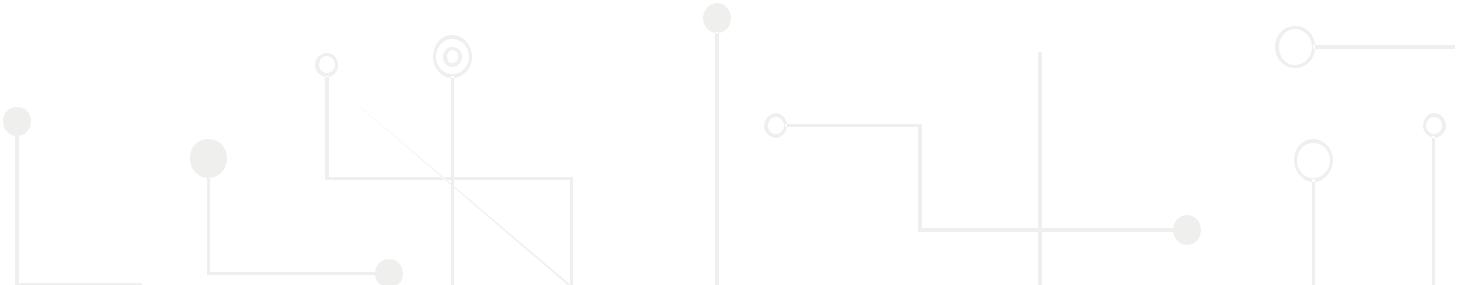
This will serve to establish HackerNet as the largest repository of verified White Hat Hackers.

**AntiHACK.me**

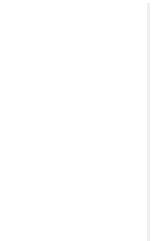
**AS A SERVICE**

AntiHACK.me will be the first Bug Bounty Platform in Asia. It will be built on our own Hackernet system. We are recognized as veterans and thought leaders in the field of white hat hacking. With blockchain and AI technology, AntiHACK.me will be able to increase its business exponentially, as our network attracts both new hackers and exposes mainstream companies to the benefits offered by the bug bounty platform.

8



https://www.accenture.com/\_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub\_9/Accenture-Future-Identity-Banking.pdf



15

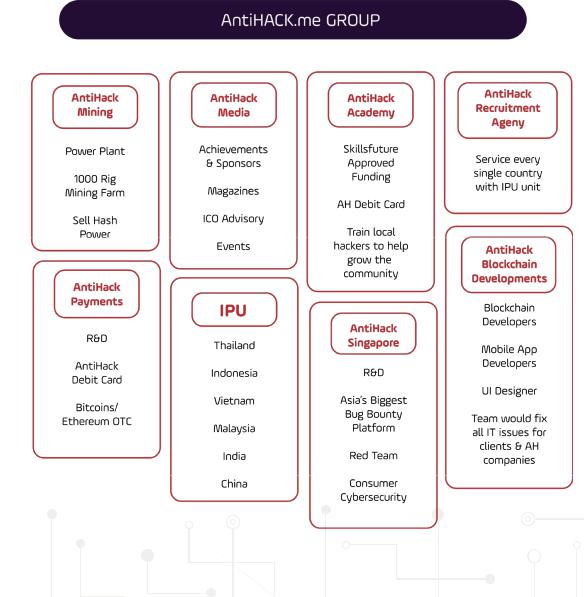


**Business Strategy Overview**

To achieve our objectives, AntiHACK.me first focuses on growth within our current target market, Singapore. We are actively seeking a working partnership with the Singapore government to become an approved vendor for hacking services, which enables our future customers to purchase our services at a subsidized rate.

Our marketing strategy is also based on an aggressive outreach that communicates the solution and benefits in AntiHACK.me’s cybersecurity services to potential customers and hackers. This consists of an integrated marketing approach that includes (but isn’t limited to) strategies related to social media, public relations, online and offline advertizing, content marketing, SEO, and events, and tradeshow marketing.

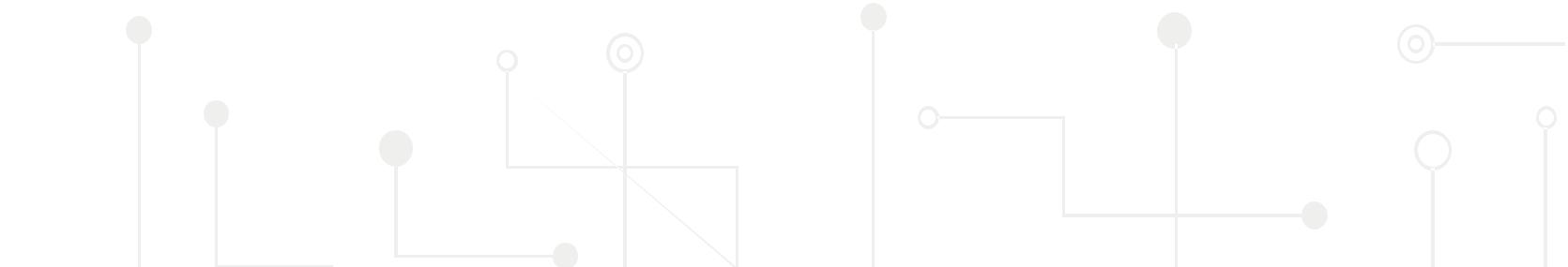
For the consistent and continuous update of our platform, we will publish a monthly cybersecurity e-magazine to allow the layman to be better informed about cybersecurity’s related risks and trends, and to provide up-to-date insights about IT security. Our target audience would range from people who do not have much knowledge of cybercrimes, cybersecurity and hacking to people who are interested in the topics.



16

**Core features of AntiHACK.me**

AntiHACK.me allows any company to utilize Bug Bounty programs to uncover vulnerabilities in their system. We have a three -tiered programme that caters to companies with different needs. Our program is specially calibrated for small to medium sized companies who require professional cyber expertise, ranging from designing the perimeters of penetration testing to patching vulnerabilities in the event of uncovered bugs.



17



**Defining the bug bounty security parameters**

The AntiHACK.me platform will guide clients in creating a customized security program. They will also provide instructions for hackers: Scope of project, types of accepted or unacceptable findings, acceptable behaviors, and an example of an ideal vulnerability report. The company also determines its “bug bounties” - what it will pay for different types of vulnerabilities found based on the severity of the threat level.

**1 Maturity assessment tool** **2 The AntiHACK.me Fixer**

****

The maturity assessment tool is an essential apparatus for penetration testing. With varying assessment criteria and a carefully crafted weightage system, this assessment will be able to determine and suggest the scope of penetration testing required. AntiHACK.me will then be able to suggest a company-specific template to optimize their bug bounty program.



AntiHACK.me will offer its fixer service to companies who require assistance in patching identified software vulnerabilities. Our analysts at AntiHACK. me will offer bug fixes to remedy vulnerabilities in the shortest time possible. Companies can also communicate with pentesters and access reports. These features are essential for smaller firms who do not have their own cybersecurity team, especially when the vulnerabilities and the associated fixes are time sensitive.

1. **Vulnerability reports**

Companies can expect vulnerability reports as quickly as within 24 hours. A customer should receive an average of 3 vulnerability reports or more in the first 2 weeks.



1. **Mediation**

****

Should a client deem the bug report commissioned to be inaccurate or irrelevant, White Hat Hackers can contact the AntiHACK.me team to mediate the dispute.

18

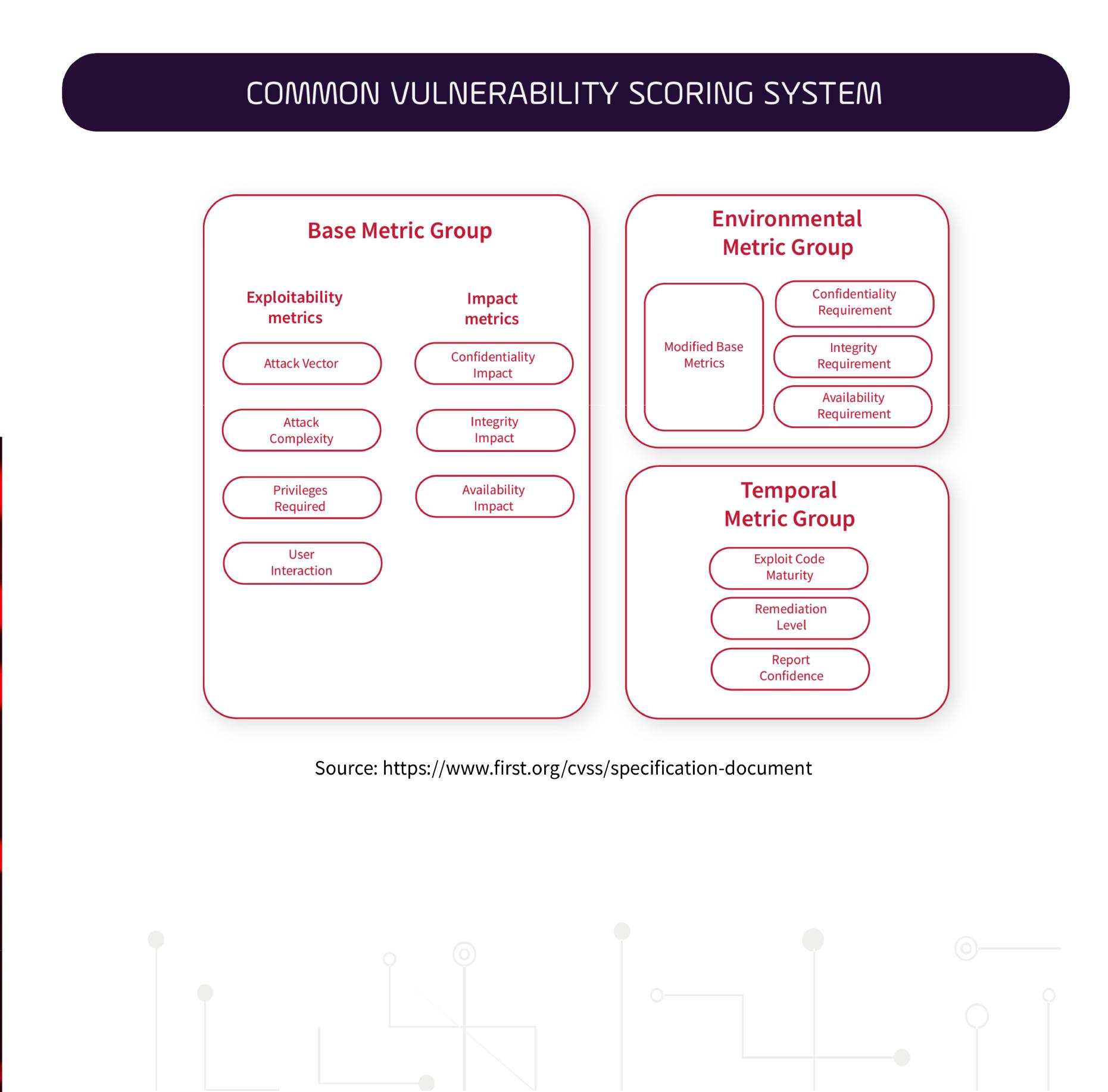
1. **AntiHACK.me AI**

AntiHACK.me AI is a deep learning penetration testing solution that identifies vulnerabilities in web application security through ever-evolving remote AI hacking attacks and then generates detailed vulnerability reports. AntiHACK.me AI makes it accessible and affordable for all businesses to conduct penetration testing and is one of our core features.



1. **Hackers Hall of Fame**

Every single bug report submitted will be evaluated using the Common Vulnerability Scoring System 3 (CVSS3) and the pentesters will be awarded points accordingly.9 The CVSS3 offers an objective, neutral and unbiased way of evaluating the quality of bug reports. The top pentesters will enter the Hackers Hall of Fame, where they will be rewarded with ATH tokens. The token reward encourages White Hat Hackers to partake in Hackerbox on a long-term basis and an additional layer of monetary incentive to find quality bugs.



9 https://www.first.org/cvss/examples  19



1. **Multi-Signature Wallet**

****

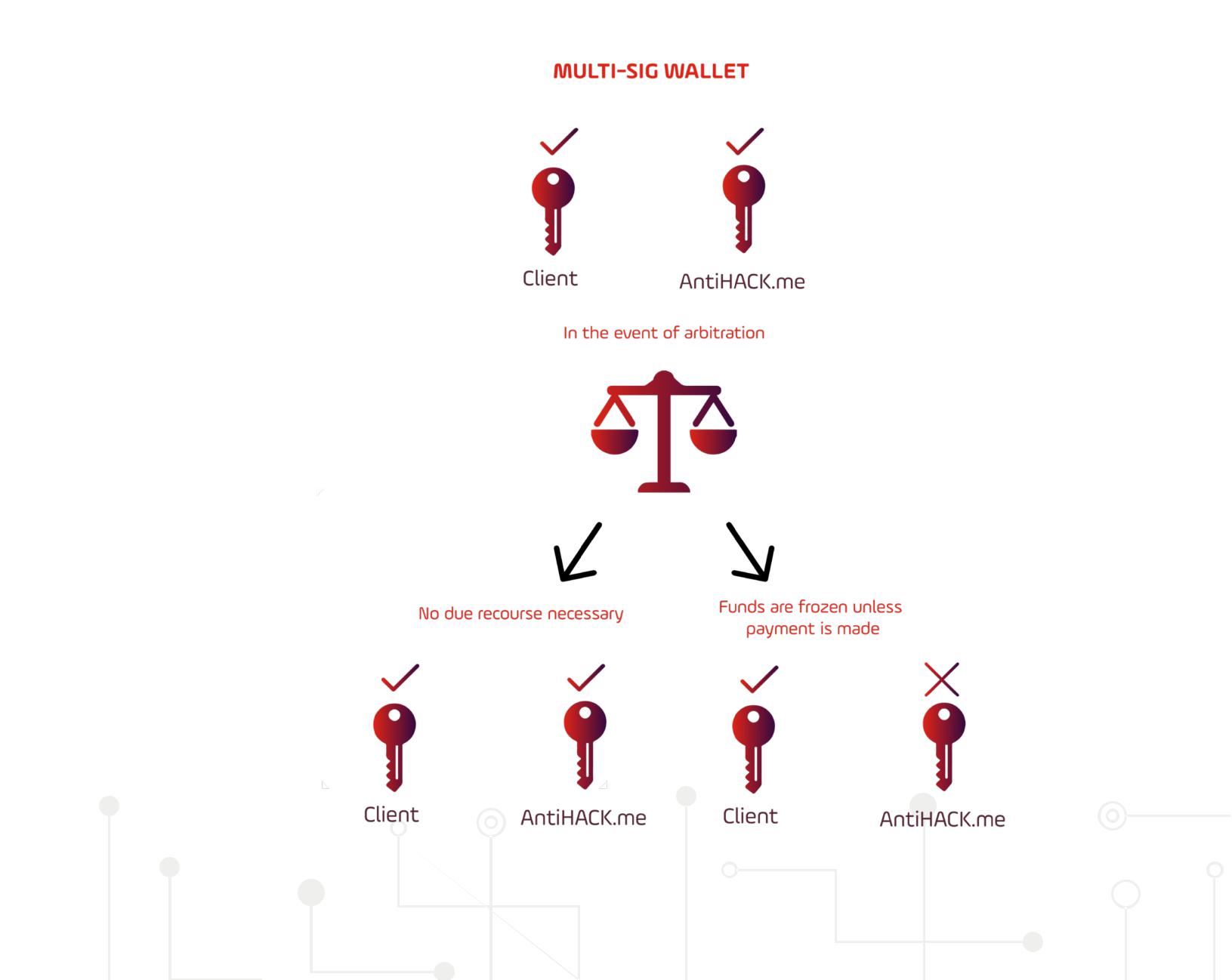
Unfortunately, the tables are stacked against White Hat Hackers in bug bounty platforms. There have been instances where companies refuse to pay out for bug reports. In this instance, White Hat Hackers often find themselves lacking in options to seek remedy when clients refuse to pay for bug submission. During arbitration, bug bounty platforms are usually more accommodating towards clients than White Hat Hackers given their established business ties and the possibility of repeat businesses in the future. This lopsided arrangement makes the bug bounty ecosystem unsustainable and drives away genuine White Hat Hackers.

Multi-signature (often called multi-sig) is used to add additional security for cryptocurrency transactions. It requires another user or users to sign a transaction before it can be broadcasted onto the blockchain. During our onboarding process, clients are to deposit the ATH coins into a multi-sig wallet, where AntiHACK.me and the client company both hold an individual private key. Both private keys are required for any transaction. During mediation, this permission is withdrawn to prevent any outgoing transaction.

Upon arbitration, two things can happen:

1. No due recourse is needed
2. It is determined that the White Hat Hackers should be remunerated and funds are frozen in the wallet unless payment is made.

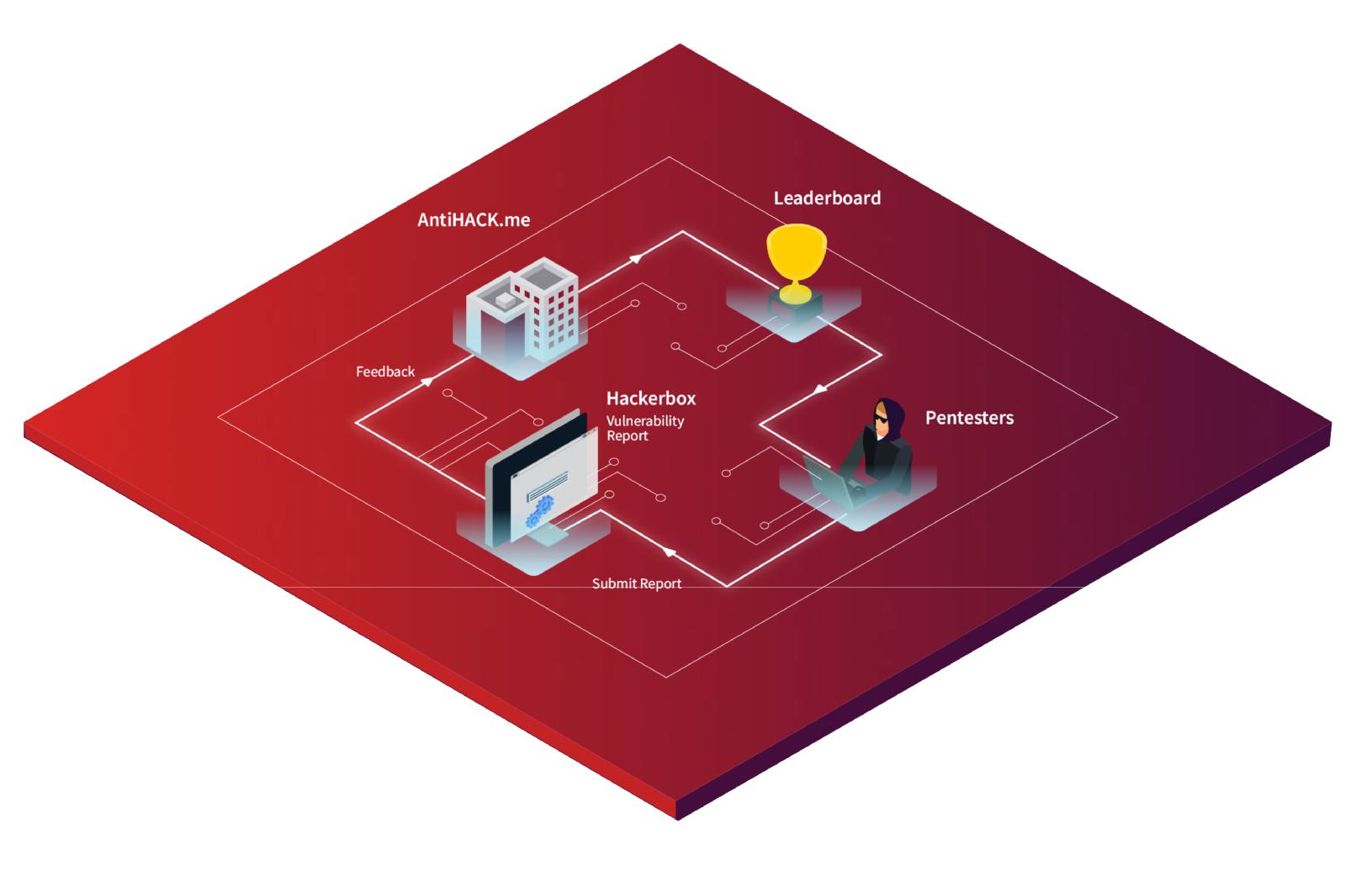
The multi-sig wallet provides the ability to impose a cost on companies who fail to properly remunerate White Hat Hackers. At any given point, AntiHACK.me will never be in total control of the funds in the wallet. This measure gives greater utility to our mediation process, where there can be proper recourse for White Hat Hackers. The establishment of an effective arbitration tool will boost the confidence of White Hat Hackers and build a sustainable bug bounty ecosystem.



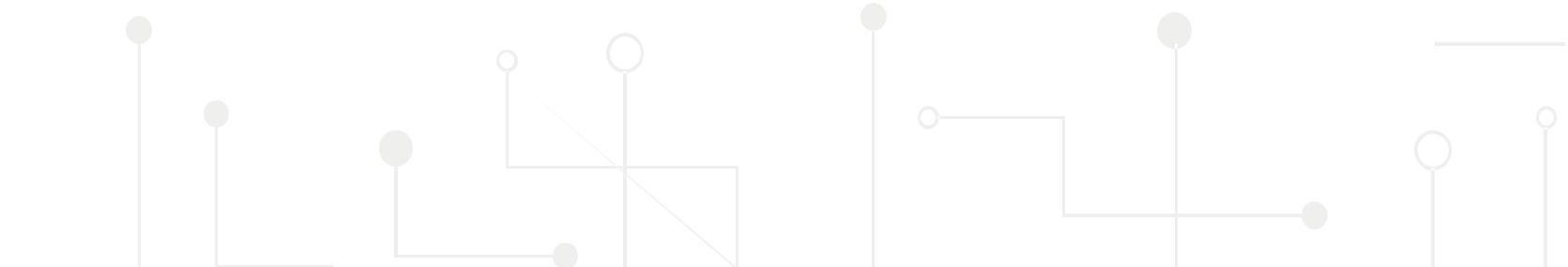
20

**Overview of Hall of Fame**

Induction into the Hall of Fame is a testament to their integrity, expertise, and experience as an Ethical Hacker. This practice is commonly adopted by big companies such as Google10 or Microsoft11 where after the bug bounty is awarded, they often also include these hackers in the Hall of Fame that will be visible to the public.



10https://www.google.gr/about/appsecurity/hall-of-fame/archive/

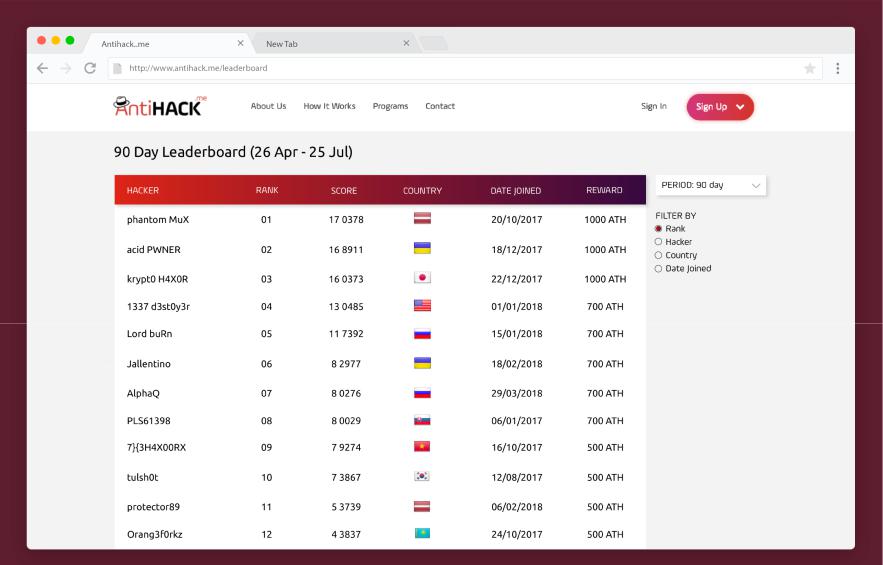
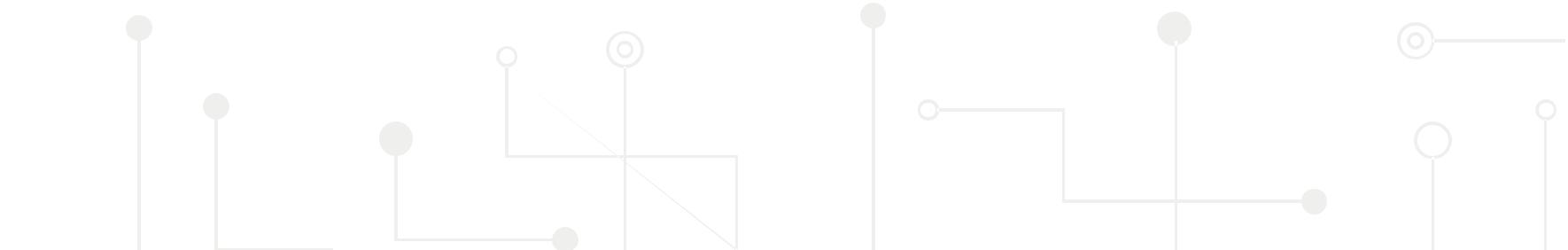


11https://www.independent.co.uk/life-style/gadgets-and-tech/news/microsoft-pays-out-100000-to-hacker-who-exposed-windows-security-flaws-8871042.html

21



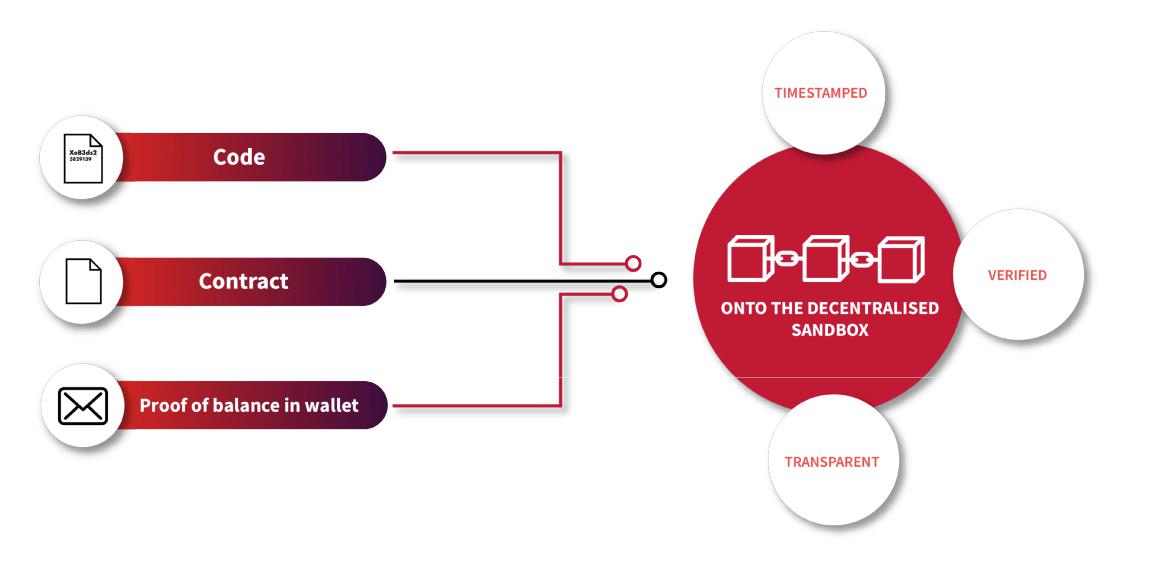
**LEADERBOARD**

****

22

**WALKTHROUGH**

* Clients enrol in the Bug Bounty program and decide on the security and reward parameters.
* The cybersecurity professional team in the Hackernet will then upload the code and contract details onto the Hackerbox. All payment will be made using ATH tokens. Clients will also have to upload their wallet address and concurrently prove the ownership of tokens in their wallet.
* The data will then be uploaded onto the blockchain and timestamped.



**Penetration Testers**

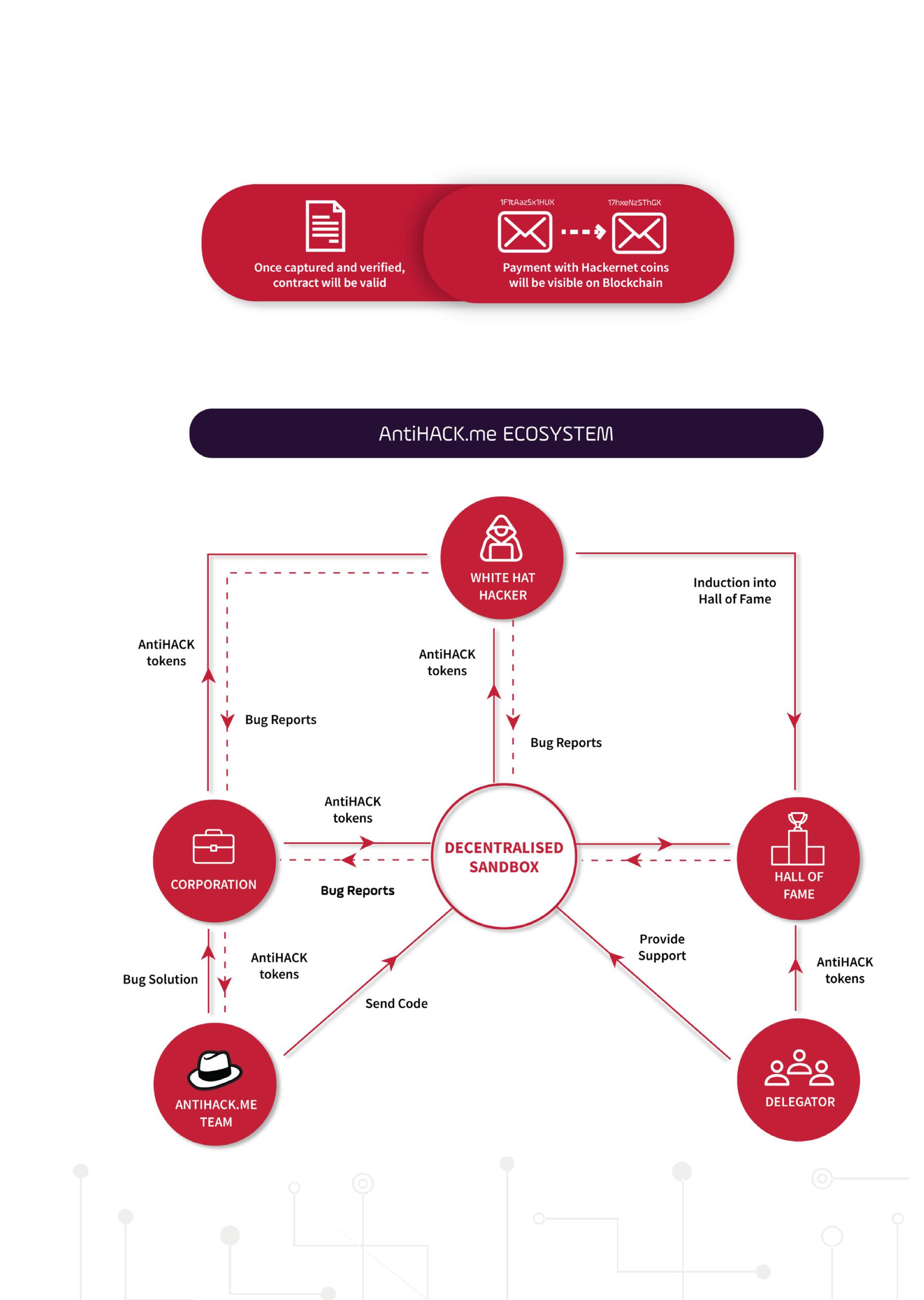
* White Hat Hackers will scour the HackerBox for contracts and work on bug reports.
* Upon submission of the bug report, it will be uploaded onto the HackerBox, where it is timestamped, transparent and visible to all, along with the wallet address where they wish to be paid to.
* In the event of a duplicated report, the blockchain makes it easy to identify the first bug report, so that only the first one will be paid, following the convention in “duplicate” rule of bug bounty.



23



**Validation and Payment**

****

* If the client decides that the bug report is valid, the White Hat Hacker will receive payment in their wallet address.
* The transaction process will be in accordance to the AntiHACK.me bug report process; it will be transparent and visible on the blockchain and anyone can verify the transaction.

24

**THE ATH TOKEN**

**Tokenomics**

The AntiHACK coin(ATH) will be used as the universal transaction unit within the HackerNet and extended AntiHACK.me network, allowing all participants to interact seamlessly and securely. Any services via HackerNet, AntiHACK.me fixer, or bug bounty programs must be purchased in ATHs. ATH is an ERC-20 token. It does not act as a security, because it is entirely integrated into the operations of the platform. Tokens are used to procure services and to pay contractors. Token holders will also receive discounts and advantages related to the operations of the platform. Token purchasers of the TGE will be able to make use of the platform from its first day of operations.

At AntiHACK, we are keen to recognize early adopters of our vision and ecosystem. One of our mission is to also make cryptocurrency readily accessible as a payment method. As a token of appreciation, we are rewarding qualified12 token holders an AntiHACK.me debit card, where they can convert their existing cryptocurrency to fiat and make purchases.

12

Qualified token holders include hackers who have submitted at least 1 verified critical severity bug, our overseas partners and token holders with at least 20,000 AH tokens (1000 USD)

25

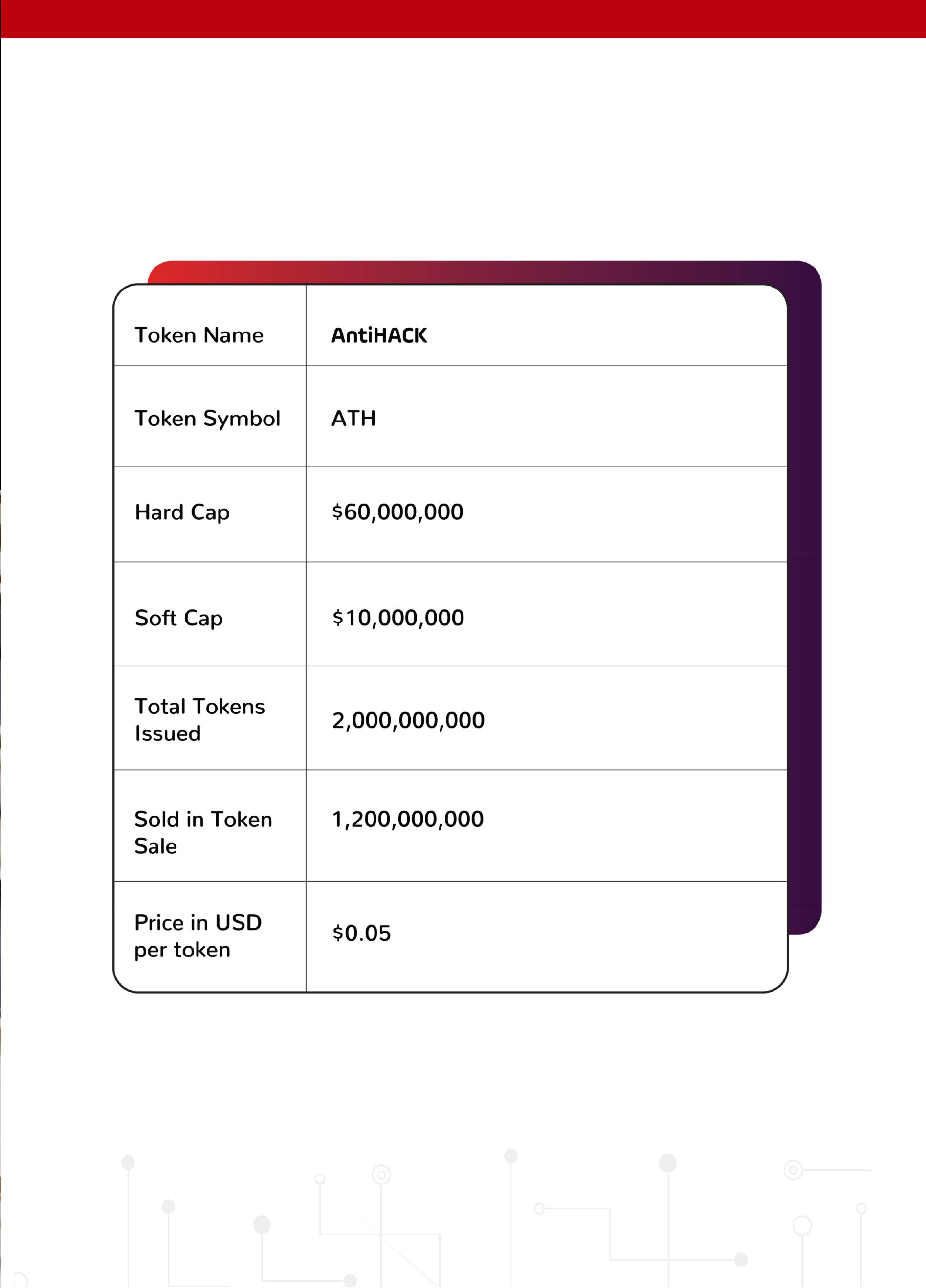
**THE ANTIHACK.ME ACADEMY**

With the ever-increasing digitization of services, it is of paramount importance that companies are equipped in cybersecurity. As part of AntiHACK.me’s efforts to nurture the next generation of White Hat Hackers and to help companies improve their competency in cybersecurity, AntiHACK.me will be providing cybersecurity courses of various levels, namely:

* Pentesting for Beginners
* Pentesting for Advanced learners
* Pentesting for Professionals
* Additional Professional Cybersecurity Certifications

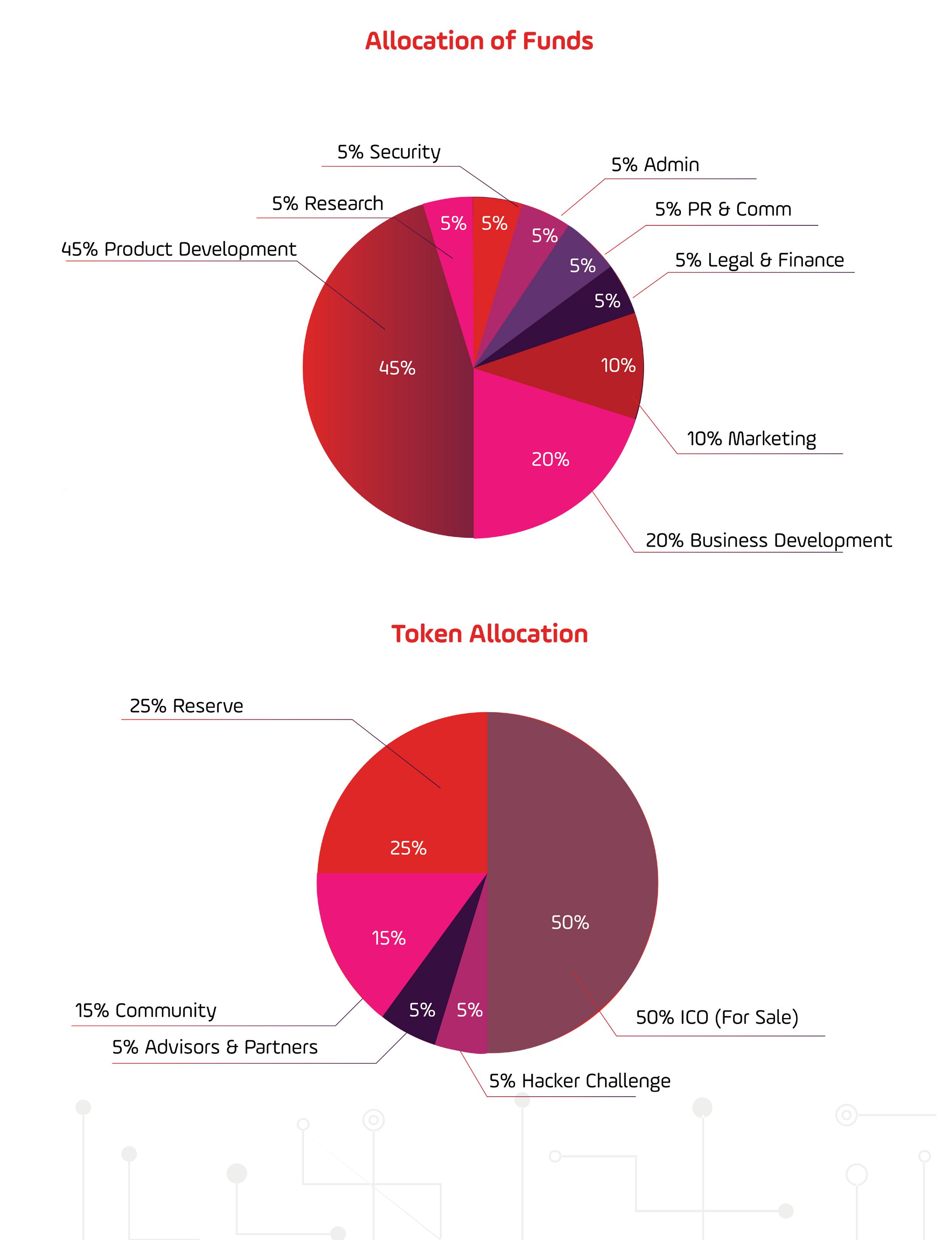
These courses are taught by real hackers, ensuring that the courses are more hands on than courses of traditional academies, which are more theory-based.

26

**FACT SHEET**

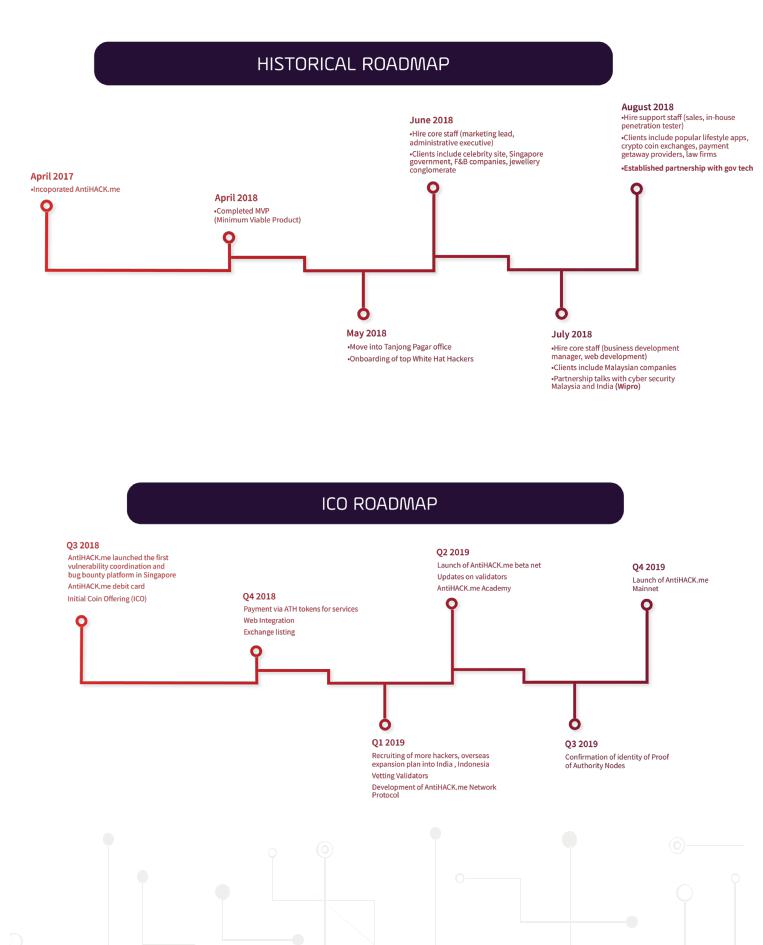
27

**MARKET SUPPLY 2 BILLION**

****

28

**ROADMAP**

****

29

**COMPANIES THAT OUR HACKERS HAVE WORKED WITH**

****

30

**OUR PARTNERS**

****

**Banff Cyber Technologies**

Banff Cyber Technologies (Banff Cyber) is a tech company that specializes in monitoring your website for any cyber attacks and gives you the option of restoring your website with a secure replica in the event of an attack. Founded since 2012, Banff Cyber is based in Singapore, with a growing regional presence (Australia, Philippines, Hong Kong, India, and Indonesia)

Banff Cyber’s flagship product, the Web Orion, utilizes their own patent-pending technologies to provide website defacement monitoring and website restoration services, providing the following features and benefits to their clients:

* Web Security Suite (e.g WAF/CDN, High Fidelity Monitoring, Secure Replica Restoration)
* Countermeasures against Web Hacking (e.g Ransomware, Blackhat SEO, Defacement, etc)
* Powered by Innovative patented technologies & knowhow

Banff Cyber serves a large customer base, serving large enterprises in 5 countries, having worked on 30,000 web pages and counting. They serve a wide range of enterprises, from the government sector (Defence Science and Technology Agency) to telcos (Singtel) and continue to expand regionally.

**Our Customer Base (SG)**

****

**Government**

**Financial/**

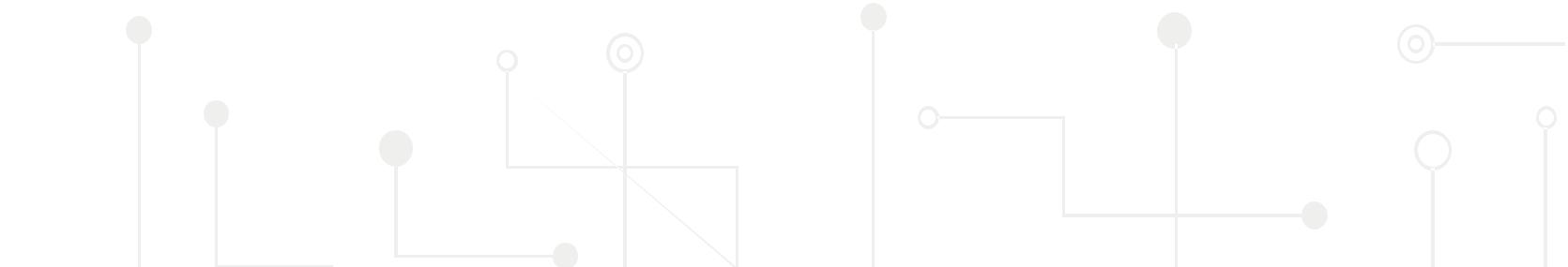
**Telcos/**

**Transport/**

**Utilities**

**Healthcare/**

**Education/F&B**

****

31



**Our Customer Base (Overseas)**

**Regional(India)** **Regional (ANZ)** **ASEAN+HK**

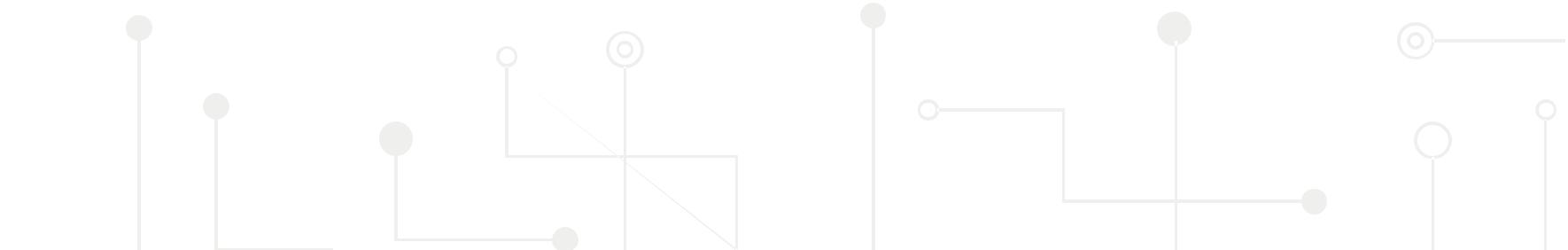
****

**Achievements and Awards**

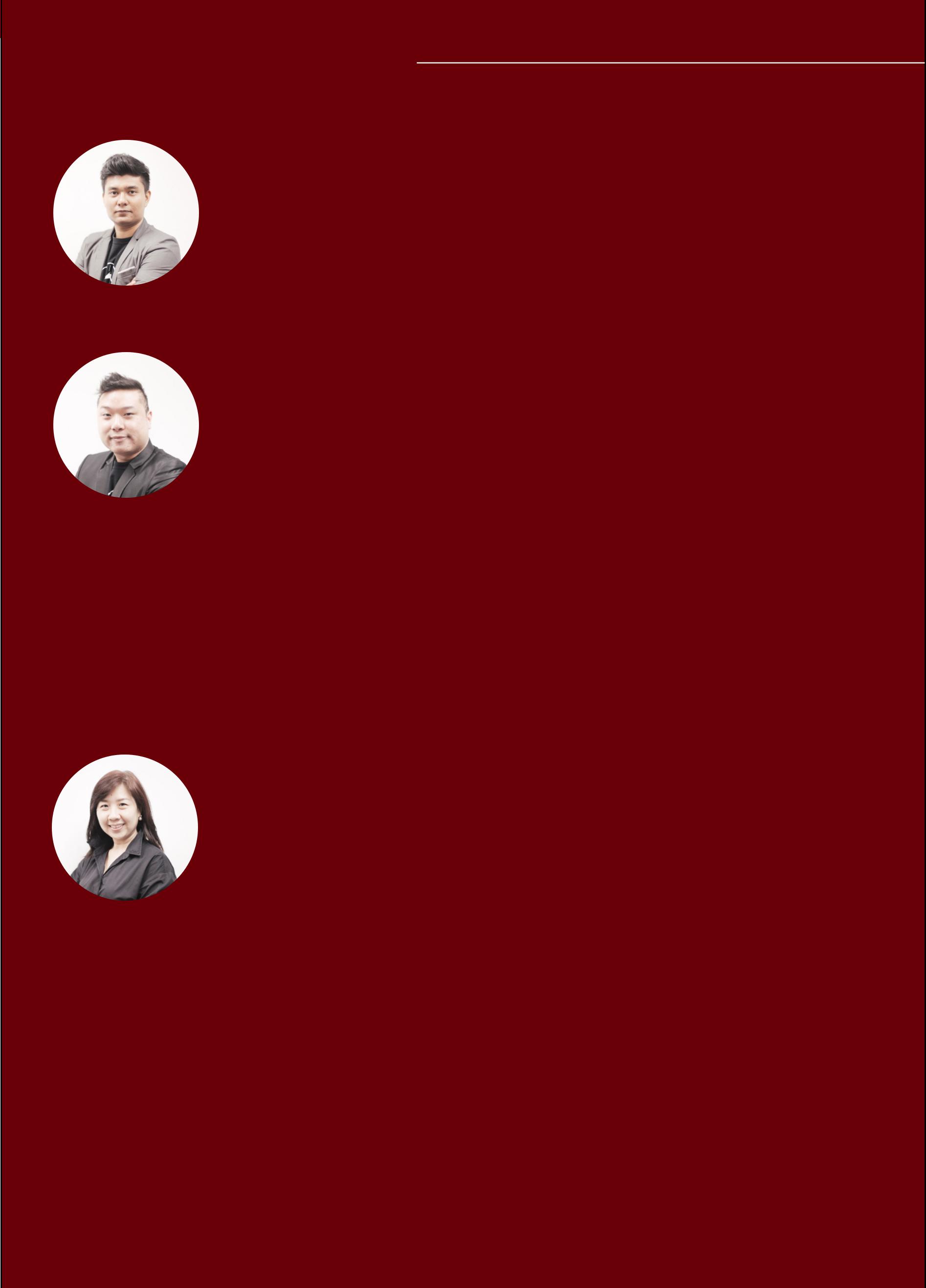
Having been in operation for less than a decade, Banff Cyber has already received multiple accolades and experienced a meteoric rise through the ranks to be amongst the top few companies in cybersecurity. Listed below are a few a few their achievements:

* 2015 Red Herring Top 100 Asia Company
* Listed in “Top 25 Most Promising Enterprise Security Solution Providers” by APAC CIO Outlook Magazine
* Ranked Top 250 in Global Cybersecurity 500 Rankings
* 2016 Frost & Sullivan Asia Pacific Product Line Strategy Leadership Award

**Featured in:**

****

32

**OUR TEAM**

**Andy Prakash**

**CO-FOUNDER & CHIEF OPERATING OFFICER**

A savvy entrepreneur by nature, Andy Prakash is the Chief Operating Officer at AntiHACK. me. He is also one of the founding partners of Singapore’s first crypto-mining company that has been interviewed by numerous media houses. Ever curious, he has a knack for figuring out how things work and constantly producing industry disruptive ideas.

**Dexter Ng**

**CO-FOUNDER & CHIEF TECHNOLOGY OFFICER**

Dexter Ng has a keen eye for the latest trends in the technology space that helps address real-world problems. He created the first iPhone App development company in Singapore and was ranked first in Google for many years. He is also experienced in managing the team of developers, which had key clients such as Starhub, Nebo (NTUC), Health Promotional Board, Club 21 and Hotel 81. Dexter is able to bridge relations between the developers and clients, helping the team to synergize better. He was also the pioneer in bringing cryptocurrency mining to Singapore – Mining.Sg. Mining.Sg was the biggest mining operation in Singapore and was interviewed by BBC, Channel News Asia, Straits Times, Coin Telegraph, Bitcoin.com, Yahoo and many more. He is the brainchild of AntiHACK.me and brought this new cybersecurity concept of crowd-security to Asia, being the first in Singapore to do so. AntiHACK.me helps address the issues of the shortage of cybersecurity talents and rising costs of cybersecurity. Dexter also exited Mining.Sg to work on AntiHACK.me.

**Ruth Yong**

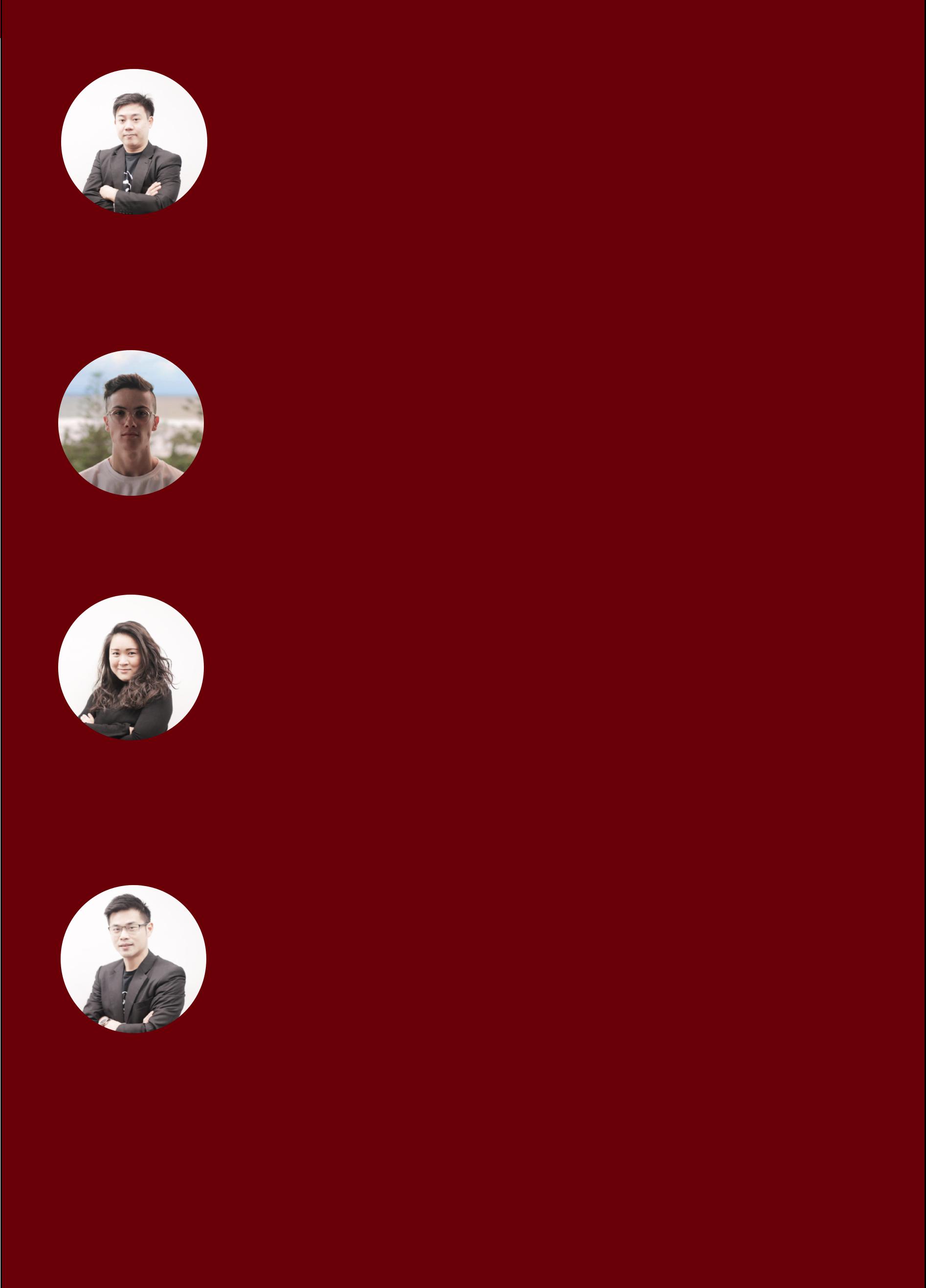
**CHIEF FINANCIAL OFFICER**

Ruth has more than 15 years in leadership roles working with Global Financial Institutions, SMEs and Listed Companies. Her experiences spanned across working in Audit, Controls and Compliance (including Internal Audit practices) with KPMG and Arthur Andersen, HSBC Pte Bank and Vistra Trust (formerly known as Credence) and working with regulators like Monetary Authority of Singapore on business processes and planning.

She also brings with her experiences in Financial Controller roles in the Retail/Trading and Business Consulting Businesses. She is effective working with both emerging and developed markets due to her vast business exposures. Fast paced start-ups are not foreign to her as she has helped set up International Financial Institution (Trust), Retail and Trading and Business Consulting companies. She is quick with understanding the 360 views of businesses and their risk environment, and has a natural affinity and passion for problem solving, with managing finances at the core of driving the company’s success.

While she enjoys having HIIT at the gym, reading and chilling out with good friends, her other passion in her free time includes investing in Options and Equities. 

33

**Cedric Chua**

**CHIEF MARKETING OFFICER**

Cedric Samuel Chua has a decade of corporate experiences networking with various ASEAN countries. Based in Vietnam, he has successfully launched profitable businesses including Sai Gon Von Microfinance, a mortgaging and licensed money-lending company, Vietlott Vietnam lottery franchisee which owns 5 branches, a private property development consisting of 10 privately-held properties and is also the master franchiser (Singapore) of Kiss The Tiramisu café and more.

**Corey Wilton**

**COMMUNITY MANAGER**

With an abundance of experience in community management and customer support, Corey plays a key role in developing, managing and promoting the community surrounding AntiHACK.me. Passionate and versatile, Corey has been involved in several large blockchain projects and only takes part in ventures which he believes will positively impact and bring real value to the end users.

**Jan Leow Jin**

**BUSINESS DEVELOPMENT MANAGER**

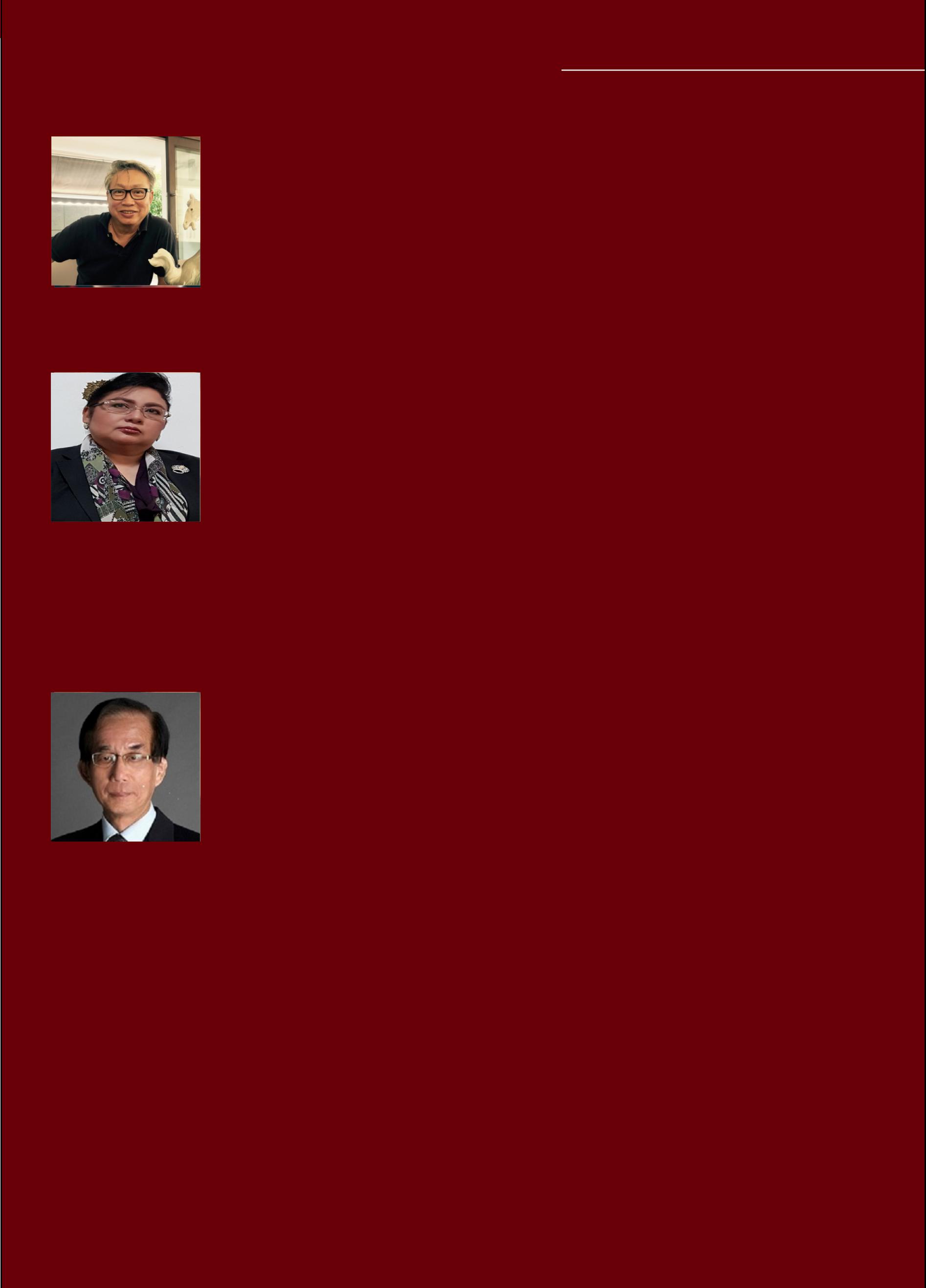
Jan is a tech junkie and a passionate advocate for the limitless possibilities that IT can bring. She has embraced this passion to advise several startups on their strategic developments. In 2013, Jan graduated with a Master’s degree in Business Administration at Murdoch University as the youngest of her cohort. Since then, she has managed and coordinated cross-continental projects including the European and Chinese market. Jan’s naturally inquisitive nature paired with her flare for IT often sees her questioning the status quo and industry boundaries.

**Desmond Tan**

**CHIEF REVENUE OFFICER**

Desmond has managed a few hundred million dollar sales in assets over more than 10 years and has a sales team of 60 under his leadership. His past working experiences involves maintaining excellent relationships with C-level executives of key target clients and high net-worth individuals. He participates actively in the strategic and business unit which plans to develop reasonable and thorough revenue projections for annual budgets and multi-year projections.

34

**BUSINESS ADVISORS**

**Benedict Ng**

**LOGISTICS & SHIPPING ENTREPRENEUR**

Benedict has 35 years experience in the logistics and shipping industry where he has won a good number of accolades. Today, he’s an ardent investor and an active owner with several other blooming ventures spread across different niche industries including development and construction, renewable energy, commodities trading and marine agencies worldwide. He is responsible for chairing the Board of Advisory.

**YBM Engku Nurhuda Binte YBM Engku Abdul Jalil**

**DESCENDANT OF THE ROYAL FAMILY**

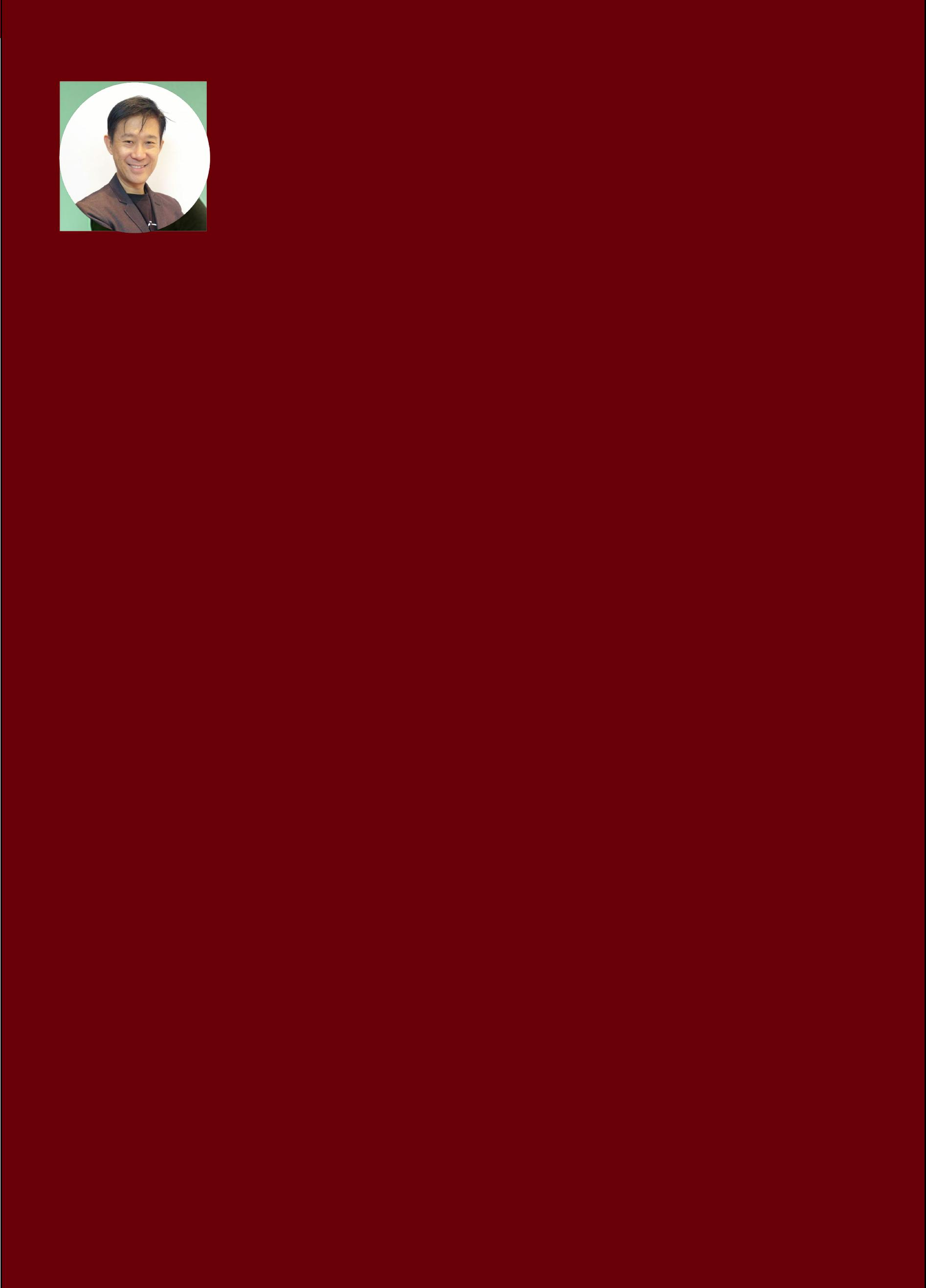
Engku Nurhuda strongly believes in the importance of versed experience and exposures in business strives internationally. Being an expatriate who is based overseas for over 14 years, she values the need to be resourceful, versatile and well-honed in business acumen, thus, inspiring her to keenly pursue achievements in this regard. Her exposure in dealing with various adventurous situations and real life scenario is inimitable. Engku Nurhuda is an active board member and director in her company, where she is a major investor. She currently invests in several other organizations both locally and internationally.

**Michael Ang**

**ICT PROFESSIONAL**

Michael Ang is the President of The Association of the Telecommunications Industry of Singapore (ATIS), and Vice President, Carrier Sales, ANTlabs, a global authentication solutions company. He has bagged four decades of experience in the IT, semiconductor and Telecom markets. He was VP Asia Pacific for a number of companies in the Asia Pacific region such as Fujitsu, Microelectronics Asia, EDS, Alcatel, with start-ups like Xylan, Top Layer and Aventail for the past 27 years. Michael is also a highly reputed speaker and innovative thought leader who has delivered in international conferences like Asia Telecom Industry Exchange (South Korea), Asia Telecom (India), Customer Churn (Malaysia), Cloud Asia and Next Generation Broadband Networks in Singapore.

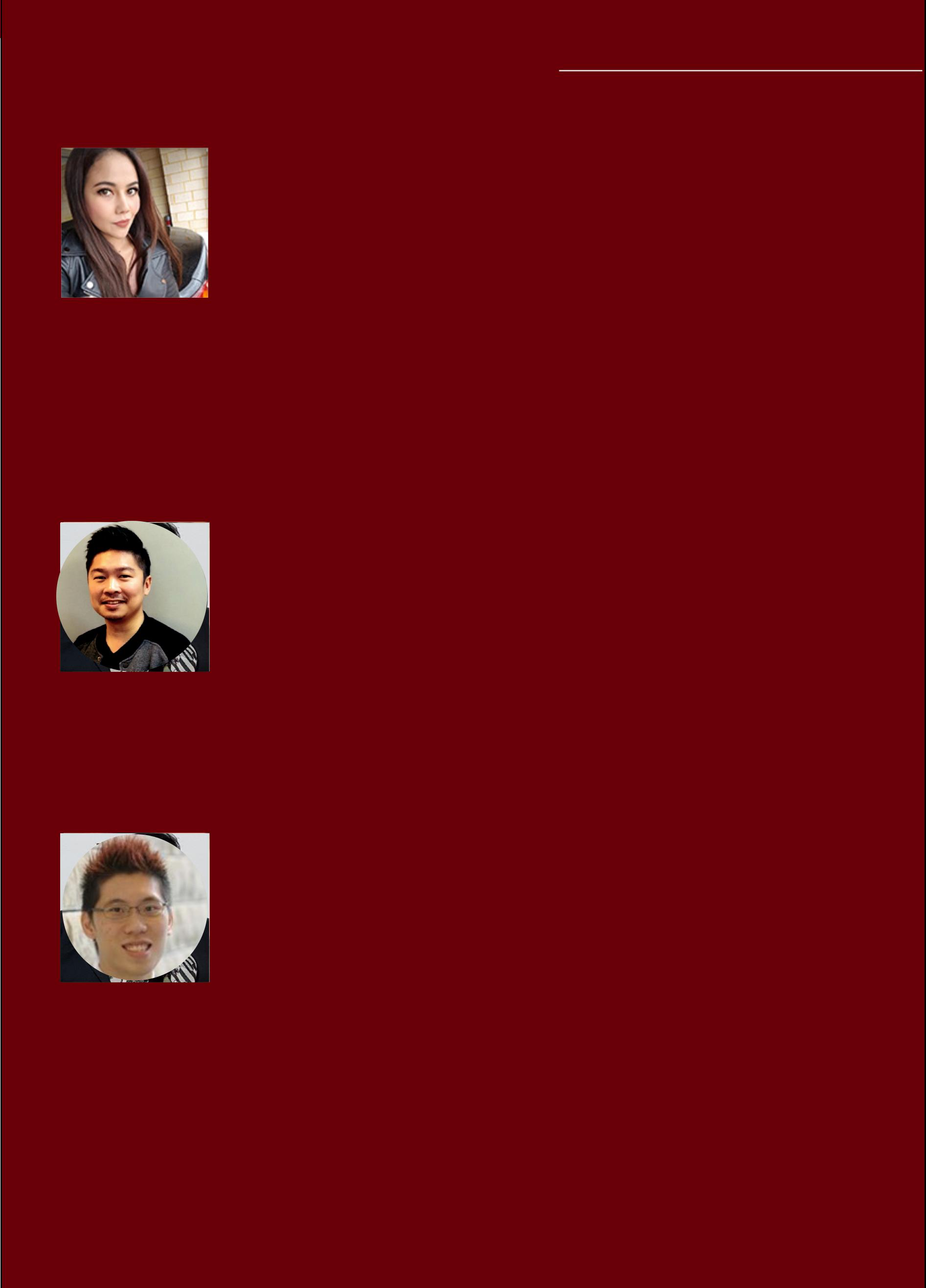
35

**Shane Chiang**

**ADVISOR**

Shane is the Head of Marketing for APAC for HMD Global Oy, a mobile phone company based in Finland that develops Nokia branded phones. The company uses technology to enhance and improve the lives of billions of people around the world and is also a startup that achieved unicorn status within 16 months of launch. The launch reached 80 countries and brought in US$2.5B worth of revenue. Prior to joining HMD, Shane Chiang was previously the VP of Cities and also CMO of Honestbee, a fast pace on demand online groceries, food and lifestyle logistics and concierge services company, delivering within the hour through the use of technology. Shane also spent 5 years at HTC Corporation, a smartphone company as various global and regional lead roles and also part of the Global Marketing & Communications roles based in APAC. He also spent 10 years in China as the EVP of Sales and Marketing for OEM Electric Equipment, a small home appliance OEM/ODM manufacturing company based in China with distribution into Wal-Mart, Kmart, Target, Best Buy, Argos Catalog and Harvey Norman. Shane has over 23 years of sales, marketing and management experience.

36

**ICO ADVISORS**

**Wannipha Buakaew (CryptoJen)**

**DIRECTOR, CRYPTO JEN PTD LTD | U.S BLOCKCHAIN ASSOCIATION**

Known as CryptoJen, Jen has a leading personality and is also a public speaker and voice of progress for the cryptocurrency community and emerging markets. While advising a number of blockchain projects including DRAGON ($320 mil raised) and recently SOLVE. CARE (hard cap successfully achieved), Jen is also on The New Money Systems Board - Lifeboat foundation alongside Vitalik Buterin and Charlie Lee. Jen is also the Board of Directors for the International Decentralized Association of Cryptocurrency and Blockchain (IDACB), at the HQ in Russia. She also is working on a program with Frankfurt School Blockchain Center, Innomine and Alastria association to support SMEs all across Europe engaged in blockchain initiatives. She is one of the most highly regarded female crypto/ blockchain influencers in the world. Currently based in Bangkok-Thailand following the appointment as Advisory Board for Thai Blockchain Association (TBA), Jen has also recently accepted her role as an advisor for the American Blockchain Association.

**Jeremy Khoo**

**GROUP CEO, IFASHION GROUP | VP, MC PAYMENT | MANAGING PARTNER, NOVUM CAPITAL | MANAGING PARTNER, CRC CAPITAL | VECHAIN ICO PARTNER**

Jeremy is an international business operator, founder and blockchain entrepreneur who has successfully exited 3 venture funded companies. He is currently the Group CEO of retail conglomerate iFashion Group and is also co-leading MC Payment’s public listing on the SGX. Jeremy is heavily involved in blockchain projects and has been instrumental in the sale of more than US$100M in tokens for 8 companies.

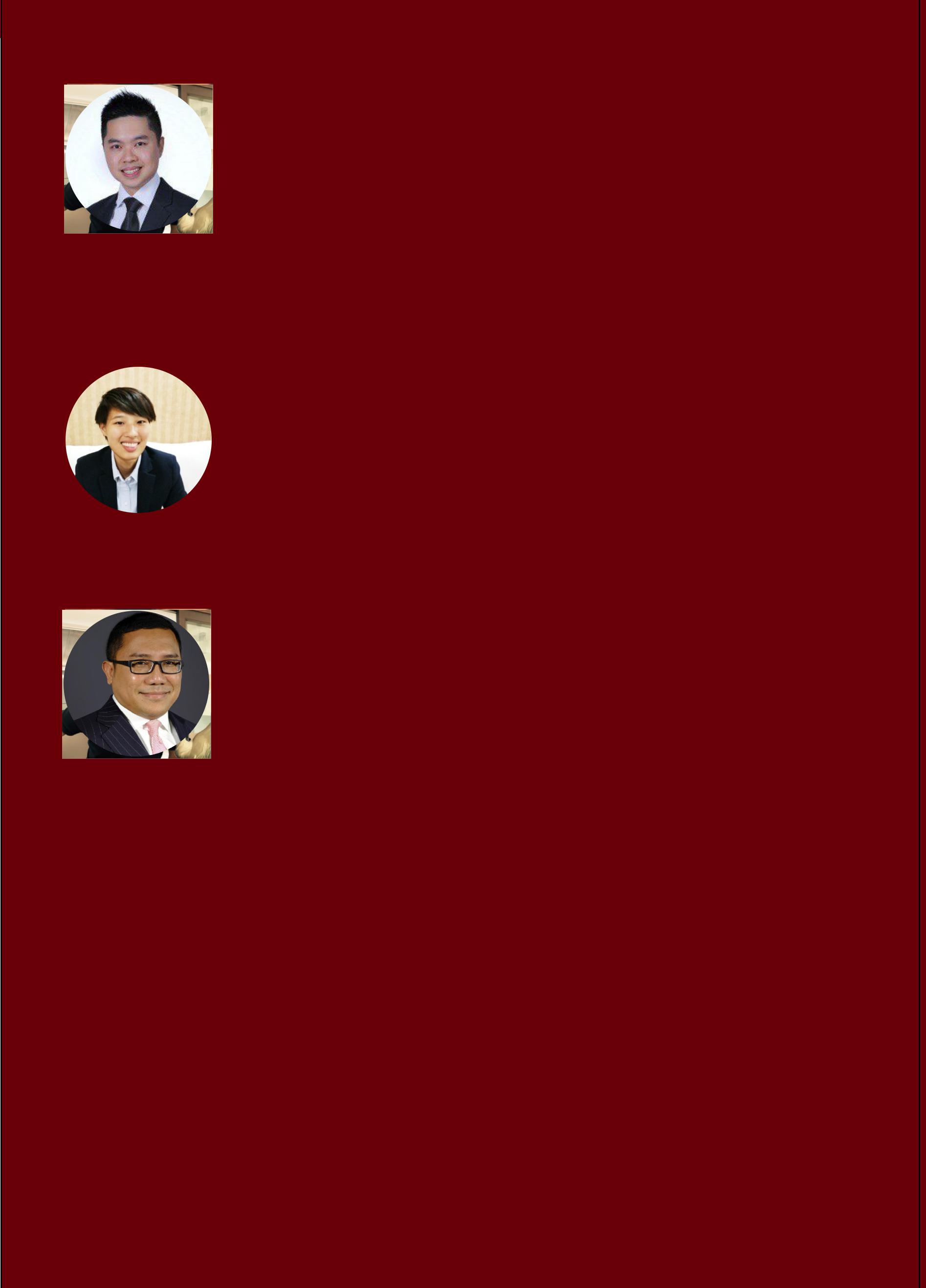
**Mark Cheng**

**BLOCKCHAIN ADVISOR**

Mark has 11 years worth of experience in venture capitalist, social enterprise and commercializing start-ups. He is a partner at CirclesX, an ICO advisory firm that structures ICO for listed companies and mature-stage companies. Mark is also a senior partner at Blockchain Labs, which builds blockchains for the government, crypto exchanges and listed companies. Till date, he has worked and advised for 18 ICO and blockchain deals. He is​the​ chairman​ of​ Start-Up Brunei, a venture builder and an accelerator in Brunei. Mark has a LLM, specializing in corporate law with the University of London (University College London

* Queens University). He was awarded the 2011 JCI Ten Outstanding Young Persons of the World (Singapore) and the first Singaporean awardee of Queens Young Leaders Award 2016.

37

**Ong Jun Hao**

**FOUNDER OF BLOCKCONNECTORS | COMMUNITY AMBASSADOR, HUOBI GLOBAL**

Jun Hao is the founder of BlockConnectors.io, a top blockchain consulting firm based in Singapore which consulted more than 20 Initial Token Offering (ITO) - Token Sale. He also helped grow various groups like CGCX, Strykz, Kinguin, BTU protocol, Lendo, Neoplace, VUtoken, and Axens’s Telegram groups. Up till date, Jun Hao has built a total community of more than 200,000 across multiple token sale projects. He has also raised more than $300 million for all projects collectively.

**Ngeow Jiawen**

**CEO & CO FOUNDER, MEGAFASH**

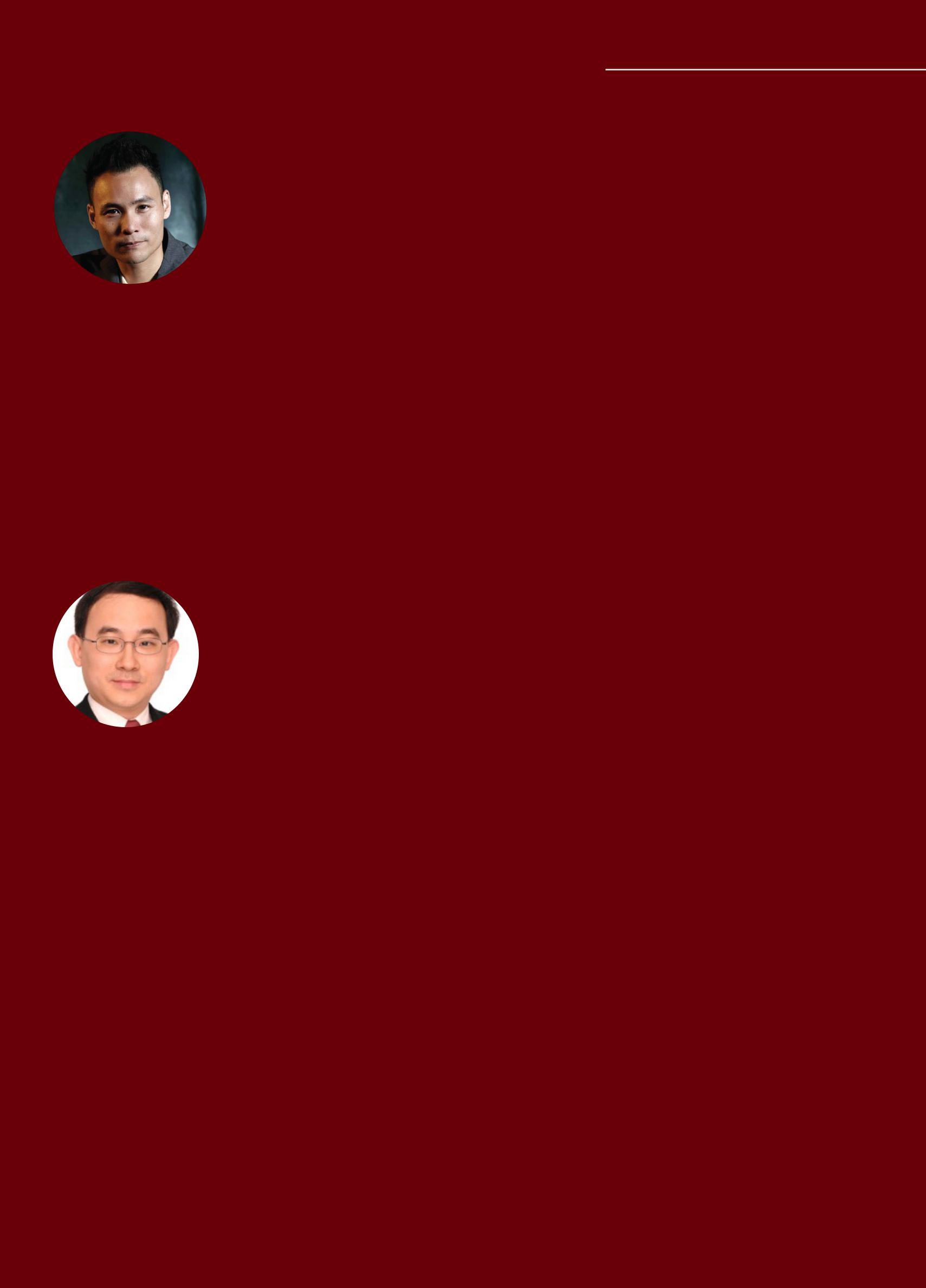
Jia Wen has successfully exited 2 venture funded companies for a total of US$20M combined, with 7 years of experience in marketplaces, e-commerce, retail and brand building. She is rated as one of the top 15 cryptocurrency czar in Singapore by Singapore Business Review. She is presently the Group COO in consumer-group, iFashion, CEO of retail company, Megafash and co-founder of blockchain project Megax.

**Nizam Ismail**

**LEGAL PARTNER, RHTLAW TAYLOR**

NizamspearheadsRHTLawComplianceSolutions,adedicatedfinancialservicescompliance and consultancy/solutions provider in Singapore, Malaysia and Indonesia (PT RHT Solusi Indonesia). He is also leading the Financial Services Practice of RHTLaw Taylor Wessing LLP. Nizam has also worked with regulators, exchanges, markets, banks, broker-dealers, commodities firms, fund managers, trust companies and financial advisers. He has also worked with a variety of FinTech firms, cryptocurrency firms and ICO/TGE issuers.

38

**CYBERSECURITY ADVISORS**

**Benjamin Mah**

**CEO & CO FOUNDER, V-KEY INC.**

Benjamin is the co-founder of V-Key Inc. and serves as its Chief Executive Officer. Benjamin is a proven entrepreneur and has built a distinguished management career in both e-Cop (acquired by a wholly-owned subsidiary of Temasek Holdings) and Encentuate (Acquired by IBM). Over the last 13 years, he also held senior management positions in corporate companies including Oracle, IBM and CA. He played a central role in growing Encentuate Inc, a leading provider of enterprise single sign-on software, until its acquisition by IBM Software. In 2000, he also pioneered e -Cop and grew it into a leading Managed Security Service company until its acquisition. He held key regional leadership positions within Oracle and IBM where he drove a large part of the core security software business and played a key role in establishing new business units. He has more than 10 years of experience in business and IT and is often called upon by the industry to speak on information security issues and entrepreneurship. He has been recognized by several key organizations as one of the industry’s “most influential people on the infocomm Security”.

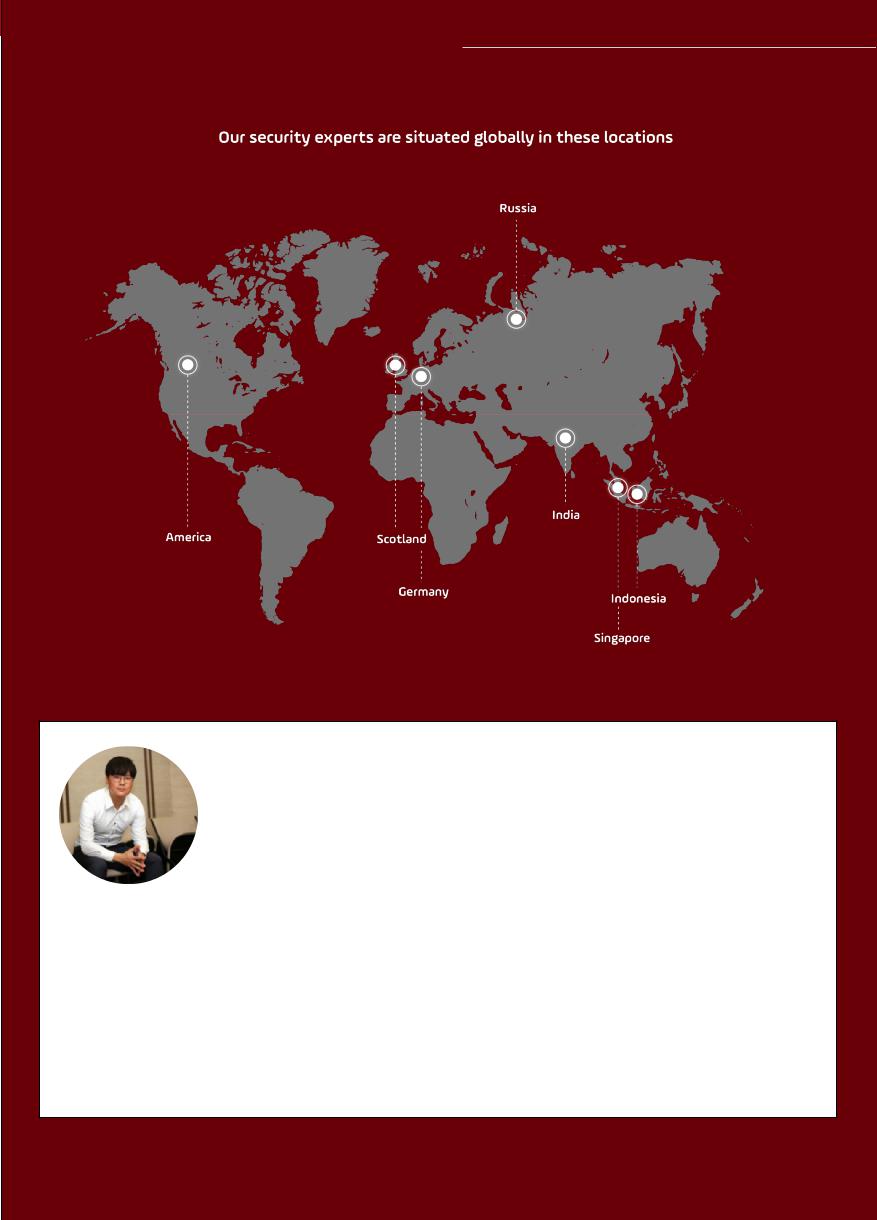
**Liew Hui Ming**

**GENERAL MANAGER & PARTNER, BANFF CYBER TECHNOLOGIES PTE LTD**

Hui Ming has spent the last 20 years in various experiences, from being a technology evangelist of cutting edge technologies in the early years, to programme management of large scale government projects and initiatives, to more recent endeavours in innovation, market research, business process re-engineering and corporate planning. He is also a “Change Activist” and is well apt in Change Management based on the principles of a learning organization.

Hui Ming is currently the business partner and general manager of BanffCyber Technologies (A SG cybersecurity product start-up company), whose key responsibilities include the full operational responsibility and accountability for company, leadership and management of the business spanning sales, marketing, delivery, engineering, support and finance & operations.

39

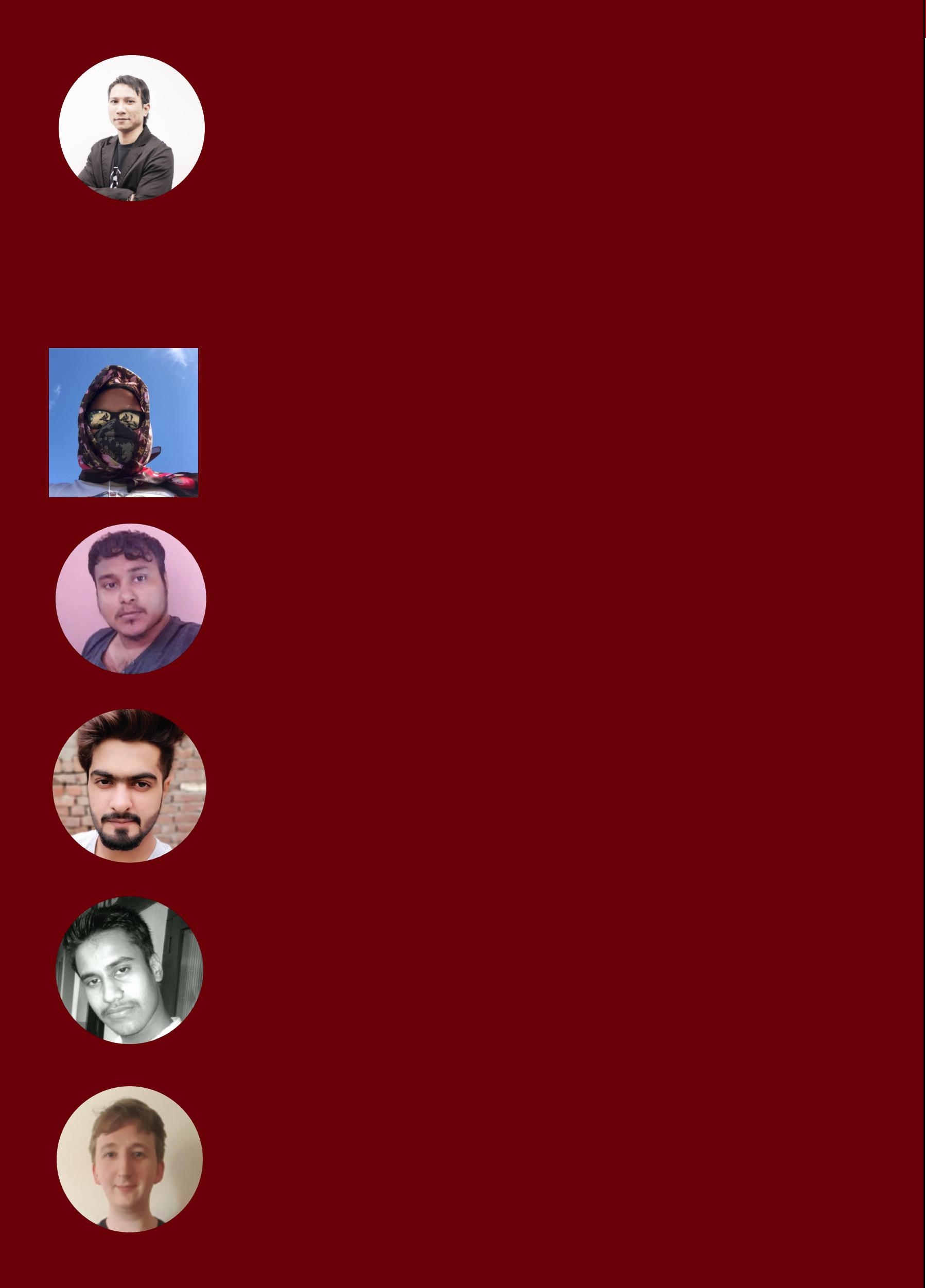
**SECURITY EXPERTS**

**Darrel Shivadagger**

**TOP BUG BOUNTY HUNTER FROM MINDEF’S FIRST BUG BOUNTY PLATFORM**

An IT fanatic and hacker from young, Darrel has been in the IT scene since he was 14 years old, hacking websites, games and online contests. More recently, Darrel emerged as the top hacker amongst a pool of 264 talented White Hat Hackers in the Singapore Ministry of Defence (Mindef) first ever bug bounty program. In this bug bounty program, eight of the ministry’s public facing facing systems (including the National Service (NS) portal) were put through a penetration test and Darrel discovered 9 unique vulnerabilities. He was rewarded with US$5,000 from this bounty program, one-third of the total bounty paid out to all the hackers. Of the US$5,000 Darryl earned, US$2,000 was for one high severity bug, a rarity in the public service systems.

40

**Azhar**

**VULNERABILITY SECURITY RESEARCHER**

Beginning his love affair with computers at a young age, Azhar has always been an ardent techophile and an advocate of experimenting with new ideas. Aside from cybersecurity, Azhar’s experimental nature has led him to various endeavors such as a DJ, cryptocurrency miner, and an avid IOT tinkerer able to build his own smartwatches and other devices. A passion for technology drives Azhar’s ambition to master his craft. Inspired by the movie Hacker (1995) and Iron Man (2008), Azhar understands that technology is a useful tool that can greatly enhance our quality of life and as such is planning his next move 10 steps ahead of everyone else.

**Roy Castillo**

Roy is a bug bounty hunter and in the Google/Facebook Hall of Fame.

**Sreedeep CK Alavil**

Sreedeep is in the Google VRP Hall Of Fame ranked at world top 54. He also entered Microsoft ‘s Hall Of Fame 6 times and also those of Intel, Dell, Oracle, Avira, Eset, Sony, Eccouncil, Belkin, Kaspersky, Flipkart, eBay and American Telecommunication. He is in more than 100 over Hall Of Fame and has the acknowledgement certificate.

**Zeeshan Khalid**

Zeeshan is an ethical hacker listed in the Hall of Fames of: Trend Micro, Google, Dell, Sony, MediaFire, AVG and more

**Sagar VD**

Sagar is an ethical hacker listed in Google and Microsoft.

**Benjamin McEwan**

Benjamin is a bug bounty hunter and in the Google/Facebook Hall Fame.

41

**Christopher Laconsay**

Christopher is an ethical hacker from the Phillipines who is also listed on Facebook and Zoho’s Hall of Fame.

**Mushraf Mustafa**

Mushraf is an ethical hacker from Pakistan with acknowledgement from companies such as:

Oracle, Edmodo, Dell, Intel, Sony, Soundcloud, Buzzfeed and more.

**Abartan Dhakal**

Abartan is a self taught ethical hacker from Nepal skilled in Python, Vulnerability Assessment and Penetration Testing(VAPT), Wordpress Customization and HTML. He is also listed on the Hall of Fame of: Intel, Pixiv, Hubspot, NetGear, Codepen, Sastodeal, Silent Circle, US Department of Defence and more.

**Ariel Marlon Antonio Javier**

Ariel is an ethical hacker thanked by Hackerone and US Department of Defence.

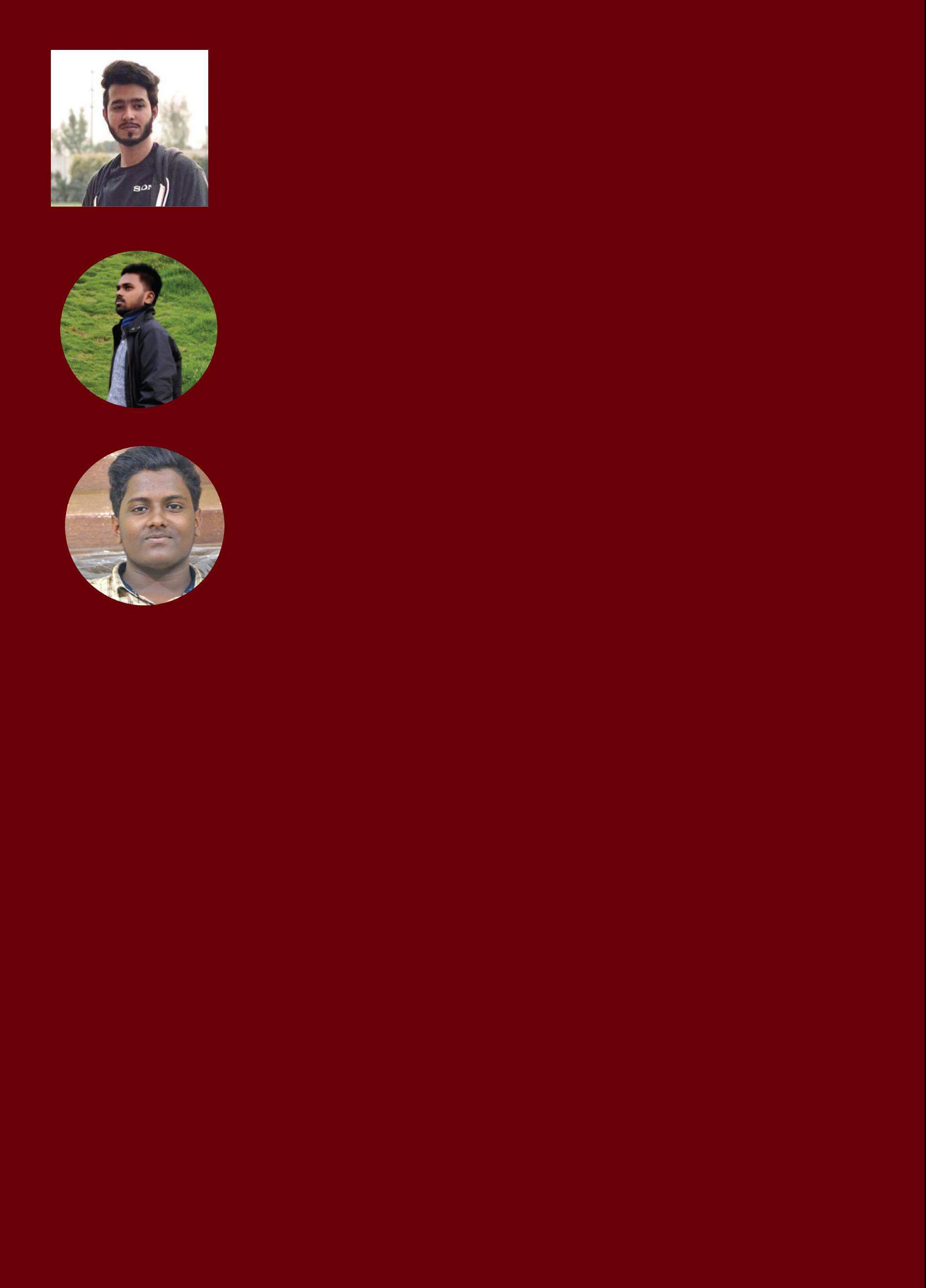
**Mohammed Abdul Raheem**

Raheem is a security enthusiast and bug bounty hunter with an overall 2+ years of experience in bug bounties. He is also anindependent security researcher who loves pentesting web applications and mobile applications and believe in responsible disclosure of the vulnerability to its vendor.

**Vyshnav Nk**

Vyshnav is currently in over 50 Hall of Fames such as Google, Apple, Microsoft, Adobe, AT&T, Sony, Redhat, Dell, Asu and many more. 

42

**Shawar Khan**

Shawar is a bug bounty hunter & in the Google/Facebook Hall Fame.

**Nikhil Sahoo**

Nikhil is an ethical hacker from India listed in the Hall of Fame of Sony, Oracle, Microsoft, Adobe, Dell, AT&T and more.

**Rasis Ras**

43