



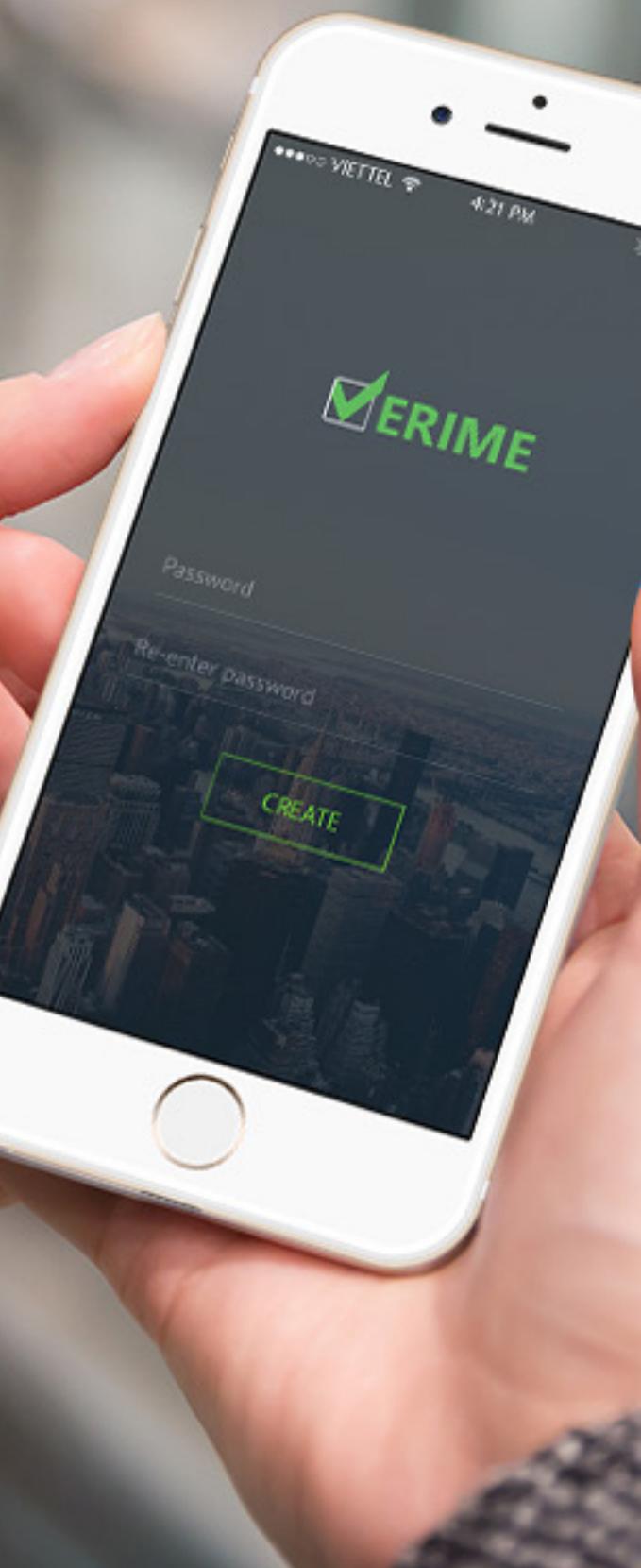
Digital Identification & Authentication Made Easy

WHITEPAPER FOR CROWDFUNDING

21 June 2018
Version 2.1



INDEX



OVERVIEW	3&4
1 SOLUTION OVERVIEW	5
1.1. About Verime	5
1.2. Verime D-KYC	5
1.3. Verime D-SECURE	7
1.4. Verime D-AUTH	9
1.5. Why Verime?	10
2 PRODUCT OVERVIEW	
2.1. Customer Creates Profile & Self-Identify	10
2.2. Customer Performs D-KYC on Partners	11
2.3. Customer Performs D-SECURE on Partners	11
2.4. Record Transaction on Blockchain	12
2.5. VERIME System Architecture	12
3 D-KYC REVENUE MODEL	
3.1 D-KYC Revenue Source	13
3.2 D-KYC Incentive Sharing Scheme	14
4 D-SECURE REVENUE MODEL	
4.1 D-SECURE Revenue Source	15
4.2 D-SECURE Incentive Sharing Scheme	16
4.3 D-KYC & D-SECURE Interoperability	17
5 BUSINESS DEVELOPMENT	
5.1 Our Achievements so far	18
5.2 Sales Strategy	19
5.3 Our Targets, Milestones & Roadmap	19
6 TOKEN ISSUE AND OFFER	
6.1 Token Issuance	20
6.2 Token Reserve Management	21
6.3 Token pricing & Anti-inflation	22
6.4 Use of Proceeds	22
6.5 Value Increase Potentials	23
7 PEOPLE AT VERIME	
7.1 Core Team	24
7.2 Advisory Team	26
7.3 Promoters	27
8 OTHER MATTERS	
8.1 Potential Risks	28
8.2 Legal Statement	29
8.3 Forward Looking Statements	31



OVERVIEW

VeriME is a decentralized Verification-as-a-Service (VaaS) ecosystem operating on Blockchain and Customer's mobile application, using the most advanced biometric technologies and machine learning tools to identify and authenticate the Customer during purchase of goods and services. Customers can verify their identity electronically with the Service Providers (Online/Offline, both Blockchain and traditional applications) who are VeriME's partners in just a few seconds, saving cost for Service Providers and enhancing Customer experience.

VeriME would initially offer two solutions to its partners:

1. D-KYC – Using this product, VeriME's partners would be able to validate potential customers and complete onboarding process with them seamlessly within seconds. Typical partners in this case would be Peer-to-Peer Lending Companies, Resellers/Distributors of Insurance and Financial Products, e-Wallet Providers, Banks, Insurance companies, Government Institutions, Credit Card Issuers, Pre-paid/Private-Label/Loyalty Card Issuers, TelCos, Travel & Ticketing Companies, Payment Service Providers, Independent Sales Organizations, Merchant Service Providers, and last but not the least, Companies raising funds through ICOs!
2. D-SECURE – Using this product, VeriME's partners would be able to seamlessly authenticate customers during the purchase of goods and services. Typical Partners in this case would be Banks, Payment Service Providers, Online Merchants, Marketplaces, Independent Sales Organizations, Merchant Service Providers, Merchants involved in high risk businesses such as Airlines, Luxury Goods, Gaming, Gambling, Mobile carrier billers & aggregators, and all D-KYC Partners who accept payments from their customers for sale of Goods and Services. Apart from authenticating a sales transaction, D-SECURE would also provide dispute/chargeback protection to its Partners.

VeriME's products protect its Partners and ensure their compliance with local, in-country regulations such as prohibition of transmission of confidential or sensitive information of an individual outside its boundaries (also known as Local Data Sovereignty and PDPA laws). VeriME's solutions are designed in such a way that it DOES NOT transmit confidential or sensitive information such as **PCI DSS** [Payment Card Industry Data Security Standards] and **PII** [Personally Identifiable Information] data, during KYC and Authentication processes.

Unlike other projects, VeriME is a ready-to-use product, being researched and developed for the past two years. Since April 2017, VeriME's D-KYC product has been functional with 14 of its partners (including a largest online payment gateway, e-Wallet, ebay.vn and a TelCo), with selected merchants and across 30,000 users in the Vietnamese market. Please refer to Section 5 for more details.

VeriME issues the VME Token, which is the "utility token" of the ecosystem for availing VeriME services. The tokens used as service fee will be distributed among members of the ecosystem to motivate the growth of VeriME and increase value of VME Token in the long-run, facilitating it to become a self-operating ecosystem.

OVERVIEW

Mission: Digitize KYC and Authentication solutions, deliver transparency with Blockchain, provide access anywhere and anytime via personal mobile device, minimize time & cost for Partners, maximize Customer experience.

Vision: VeriME becomes a global, not-for-profit, decentralized VaaS ecosystem in the Blockchain space and beyond saving time and money for partners and end consumers.

Issuer	VeriME DIGITAL PTE. LTD.
Token Name	VeriME
Token Symbol	VME
Token Contract Address	0xC343f099d3E41aA5C1b59470450e21E92E2d840b
Total Supply	400 Million
Platform	ERC20
Official website	https://www.verime.mobi/home

1. SOLUTION OVERVIEW

1.1 ABOUT VERIME

VeriME is an intermediary digital Validation-as-a-Service (VaaS) that allows Service Providers who are its Partners to validate and/or authenticate a potential Customer who has already been verified and approved by VeriME. The verification process can be self-done by the Customer anytime, anywhere within minutes right on the Customer's mobile device thanks to the smart application which uses sophisticated technologies such as Artificial Intelligence, Computer Vision and Cloud Computing. VeriME helps in strengthening the transparency & accuracy of transactions and improving user experience, while saving time and cost for Customer KYC and Authentication processes.

VeriME operates on a Blockchain-based decentralized model. A customer's Profile that has been validated & certified is stored right on his/her mobile device, ensuring privacy and eliminating the risk of data leakage.

VeriME is a complete ecosystem with three parties involved: VeriME Team, Customers and Partners. All are motivated to contribute to the development of the ecosystem through a service fee sharing scheme, unlocking the potential for unlimited expansion.

VeriME will release VME Token on Ethereum ERC20 Smart Contract as the cryptocurrency for the ecosystem. The VME Token is a utility token, meant for usage within the VeriME ecosystem. It is not a security.

Lastly, VeriME is one of those rare not-for-profit ecosystems in the Blockchain space which will reinvest all its revenue from its services in technology upgradation and expansion of the ecosystem to increase the usage of VME Token.

1.2 VERIME D-KYC.

KYC (Know Your Customer), is a process which enables businesses and organisations to identify and validate the identity of their customers. This process is particularly important in the financial services industry to ensure that the customer is as real as the file to avoid potential litigation risks and to assign responsibility if there is a violation of the law in the future.

The KYC process always starts with gathering basic information about the customer and identifying it with a physical person with the following layers of information:

- Contact Information: Email address, phone number etc.
- Personal Identity: Identity proof documents such as identity card, driver's license, passport etc.
- Address: through attested documents such as utility bills (electricity, water, telephone, internet etc.), confirmation of residence by local authority, etc.
- Financial status: Salary slips, Bank statements, Tax certificates etc.

1. SOLUTION OVERVIEW

The traditional KYC process requires that customers and Service Providers to meet face-to-face in order to fill out forms, handover documents which match with the customer. The major issues involved in this process are as follows:

- Inconvenience caused to the customers, increased operation costs for Service Providers;
- Possible risk of error if the employee is unable to identify and match the authenticity of the document with the physical person.
- KYC is an unexciting and expensive task, and it consumes a considerable amount of time. Customers have to go through KYC procedures numerous times with different Service Providers, multiplying the waste of time and cost.

There has been growing focus on KYC in Southeast Asia, largely driven by regulatory changes surrounding Anti-Money laundering (“AML”) and Combating the Financing of Terrorism (“CFT”). This is driven internationally by the Financial Action Task Force (“FATF”), which sets international benchmarks in the form of the 40 Recommendations. The FATF conducts rigorous assessments of member countries in Southeast Asia to ensure robust AML/CFT measures.

With the advent of FinTech and technology-driven services in Southeast Asia, there emerges a very strong demand for digital identity services.

According to Wikipedia, [Regulatory Compliance Technology](#), also known as RegTech, is the application of technology (specifically IT) to meet industry's monitoring, reporting and compliance requirements, especially in financial services. RegTech's businesses focus on finding solutions that meet the challenge of legal compliance through technological innovation to save cost and increase customer experience. Those companies usually use cloud computing infrastructure, Software-as-a-service (SaaS) and more recently, the application of Blockchain technology.

According to a survey conducted by [Thomson Reuters](#) it is estimated that financial Institutions and firms spend up to \$500 million globally on KYC. Also, 13% of the customers who responded revealed that they had changed their financial services provider as a result of bad experience. It is important to note that not only costs, but also customer experience is critical for businesses to retain their clientele.

KYC is legally mandatory for financial service providers. They must adhere seriously to KYC procedures if they want to avoid [billions](#) of dollars in fines. Many other non-financial-service industries also need to KYC their customers for legal compliance. So, the KYC market size is tremendous with up to 3 billion customers and it costs [tens of billions](#) of dollars annually across the globe.

A common characteristic of blockchain is anonymity, which makes it the preferred mode for financial transactions among criminals. In order to be recognized by the governments for its decentralized nature, transparency and immutability, the Blockchain technology must include mechanisms for legal compliance and KYC requirements. This is a booming futuristic opportunity for Digital-KYC industry in general and VeriME in particular.

1. SOLUTION OVERVIEW

Thus, different kinds of organizations across the world are in need of a breakthrough solution which saves the time and cost of KYC processes, and VeriME is already working on such a solution.

VeriME's Digital-KYC [D-KYC] is 'Know Your Customer' in a digital way. It performs KYC processes remotely and completely online without requiring customers to meet, fill out forms and submit documents. D-KYC uses biometric technologies to automatically identify the physical form of customers and match them with authentication documents without the need for a face-to-face meeting, hence maximizing convenience and minimizing cost for Customers and Service Providers.

Once the customer has successfully validated the required data, VeriME would continue to monitor the validity of the data and prompt the Customer to update the data as and when required. In such a scenario, VeriME would also handle updating of the smart contract between the Customers and Partners so that every stakeholder in the ecosystem is up-to-date.

In addition to KYC, VeriME will provide holistic solutions to its Partners by offering **AML** (Anti Money Laundering), **PEP** (Politically Exposed Person) and Sanction Checks. However, these services will be optional for the Partners based on their business needs.

Video on VeriME's D-KYC can be viewed here:

https://www.youtube.com/watch?v=FaFx_Jwl0ro&t=58s

1.3 VERIME D-SECURE

Payment or Transaction Authentication generally refers to a secure online or offline method of identifying a user or buyer through two-factor authentication or three-factor authentication. It involves identifying and validating legitimacy of the user. Many solutions have been introduced in the market by Payment Schemes, e-Wallet providers and Banks, but Payment fraud continues to increase with increase in eCommerce growth. Additionally, with increase in online-to-offline and omni-channel solutions, this **threat** continues to grow.

Below are some of the authentication & fraud challenges faced by the Payment Industry today:

- Market has moved on; Technology and Customer behaviour have changed - Owing to the outburst of smart phones and social media in the recent past, the user base has drastically changed. According **Adyen's report**, in 2015 alone over 27% of global ecommerce transactions were done on mobile devices. However, Authentication and Fraud Detection services available in the market haven't evolved at the same rate, which are costing businesses billions of dollars every year.
- Bad Customer experience & low conversion rates– Most of the Authentication services on the internet involve redirecting a customer to another browser to perform authentication formalities leading to higher drop off and basket abandonment rates.

1. SOLUTION OVERVIEW

- Not fully secure— Current offerings are prone to many security threats such as Man-in-the-middle (MitM) or Man-in-the-Browser (MitB) attacks thus failing to protect sellers and/or buyers.
- Expensive – Implementation of current solutions involves many players. E.g. a **3D Secure** authentication offered for Credit/Debit Card Payments involves the Issuing Bank, Acquiring Bank, Payment Schemes, ACS (Access Control Server) and MPI (Merchant Plug In) providers etc. thus making the solution quite expensive for merchants.
- Limited mobility – According to [Wikipedia](#) when a 3-D Secure confirmation code is required, if the confirmation code is sent by SMS on mobile phone (assuming she/he owns one) the customer may be unable to receive it depending on the country he currently is in (not every mobile network accepts SMS). The system is also not convenient for customers who tend to change mobile numbers from time to time – such as due to travelling (and some banks require a visit to their Branch to change the mobile number on the account). Some Wi-Fi providers who charge for usage by credit card don't actually allow accessing the 3-D Secure site before the payment is completed, so the user is unable to purchase Internet access.
- Not fully compliant with Local Data Sovereignty & PDPA Laws – Global Authentication services are centralized and fail to meet local, in-country regulations (for ex: China, Vietnam, Indonesia etc.)

With rapidly changing technology & growing social media, fraudsters are always one step ahead of traditional authentication and fraud management tools. With global card fraud projected to reach **\$31.67 billion** in 2020, it is more important than ever to consider innovative, secure and most importantly payment instrument agnostic and universal solution to tackle the authentication conundrum without adding friction to the customer experience.

D-SECURE is an authentication service offered by VeriME to its partners. Partners involved in sales of goods and services and/or transaction processing can avail this service as an alternative to traditional authentication tools. The solution would not only authenticate the Customer, but also would provide full chargeback/dispute protection to VeriME partners and their Merchants.

VeriME's D-KYC and D-KYC solutions are designed to ensure VeriME's Partners' compliance with local data sovereignty and PDPA laws.

VeriME believes that D-KYC and D-SECURE solutions combined with Blockchain and Machine learning solutions can truly provide real value to financial ecosystem.

1.4 VERIME D-AUTH

VeriME D-AUTH is a by-product of VeriME D-SECURE solution leveraging most advanced biometric technologies and machine learning tools to identify and authenticate the Customer. Unlike D-SECURE which is designed to provide Payment Authentication and Chargeback protection to VeriME Partners, VeriME D-AUTH solution is designed to provide multilevel User authentication solution to its Partners.

1. SOLUTION OVERVIEW

1.5 WHY VERIME?

a) For Customers

- Create a personal profile only once on your mobile device through the VeriME application, and reuse it for D-KYC and D-SECURE with all VeriME's partners without having to travel or meet up.
- Use VeriME application to scan QR-Codes or authenticate using biometric authentication tools at the website or mobile application of a VeriME Partner for completion of the D-KYC & D-SECURE process in a matter of seconds.
- Receive Usage fee (in the form of VME Tokens into personal wallet) on every transaction with VeriME Partners, which can be traded in world-wide Exchanges.

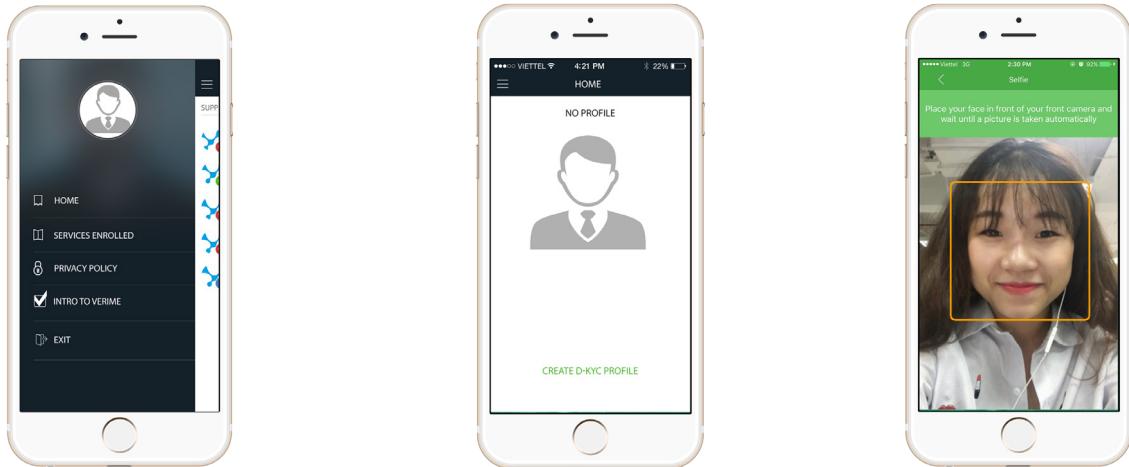
b) For Partners

- Whenever there is a need for KYC or Authentication, just generate a QR-Code using VeriME's APIs and ask the Customer to scan it with VeriME's mobile application to receive the Customer's Verified-by-VeriME profile within seconds.
- Maximize Customer experience, cut costs on KYC & Authentication while maintaining 100% credibility.
- When other Partners request for D-KYC or D-SECURE for customers who have been previously validated & certified by VeriME by Primary Partners, Primary Partners would receive a referral fee in the form of VME Tokens, which can be used for performing D-KYC and/or D-SECURE for new customers, or can be traded in world-wide Exchanges.,

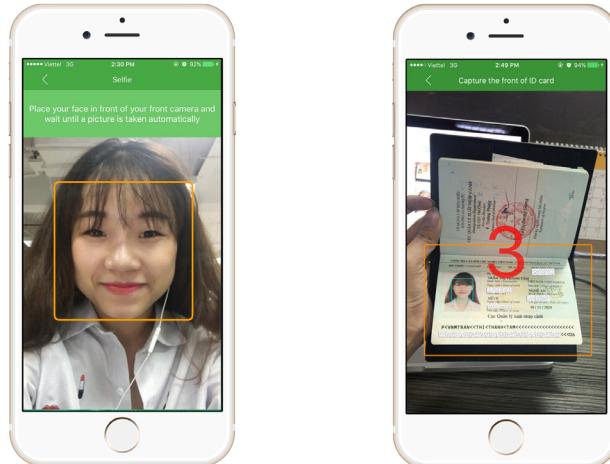
2. PRODUCT OVERVIEW

2.1. Customer Creates Profile & Self-Identify

- Step 1: Customers download VeriME mobile app on personal mobile device; Using camera they make random expressions as requested by VeriME to ensure that he/she is a physical person; VeriME logs their facial identification.



- Step 2: VeriME application automatically takes a selfie picture and then asks Customer to upload the Identity proof document, Payment methods etc. VeriME recognizes, validates and stores the information on the mobile device.



2. PRODUCT OVERVIEW

- Step 3: VeriME application uses computer-vision algorithms in the background to match and verify Customer's selfie picture with the photo on identity proof document, Payment methods etc., with accuracy ratio higher than detecting by human. If the match is a success, VeriME changes Customer's profile status to "Verified". The profile creation and identity verification process is completed in less than 3 minutes. VeriME creates unique identity for verified customer using Blockchain technology.



2.2. Customer Performs D-KYC on Partners

While using a Partner's service, if the customer is required to perform D-KYC, the customer uses VeriME mobile application to scan VeriME QR-Code generated by the Partner.



2.3. Customer Performs D-SECURE on Partners

While using a Partner's service to perform D-SECURE, Customer can verify and authenticate the transaction using options below:

- When a D-SECURE authentication is requested by Partner's Merchant or Merchant through Web, Customer will authenticate using QR code.
- When a D-SECURE authentication is requested by Partner's Merchant or Merchant through Mobile application, Customer will be able to authenticate using biometric means.

In both the scenarios, VeriME will be performing additional checks such as IP/Geo location Check, Velocity Checks, Device fingerprinting, real-time profiling & risk scoring etc. using Machine Learning based tools for fraud prevention, thereby protecting merchants and partners from disputes and chargebacks.

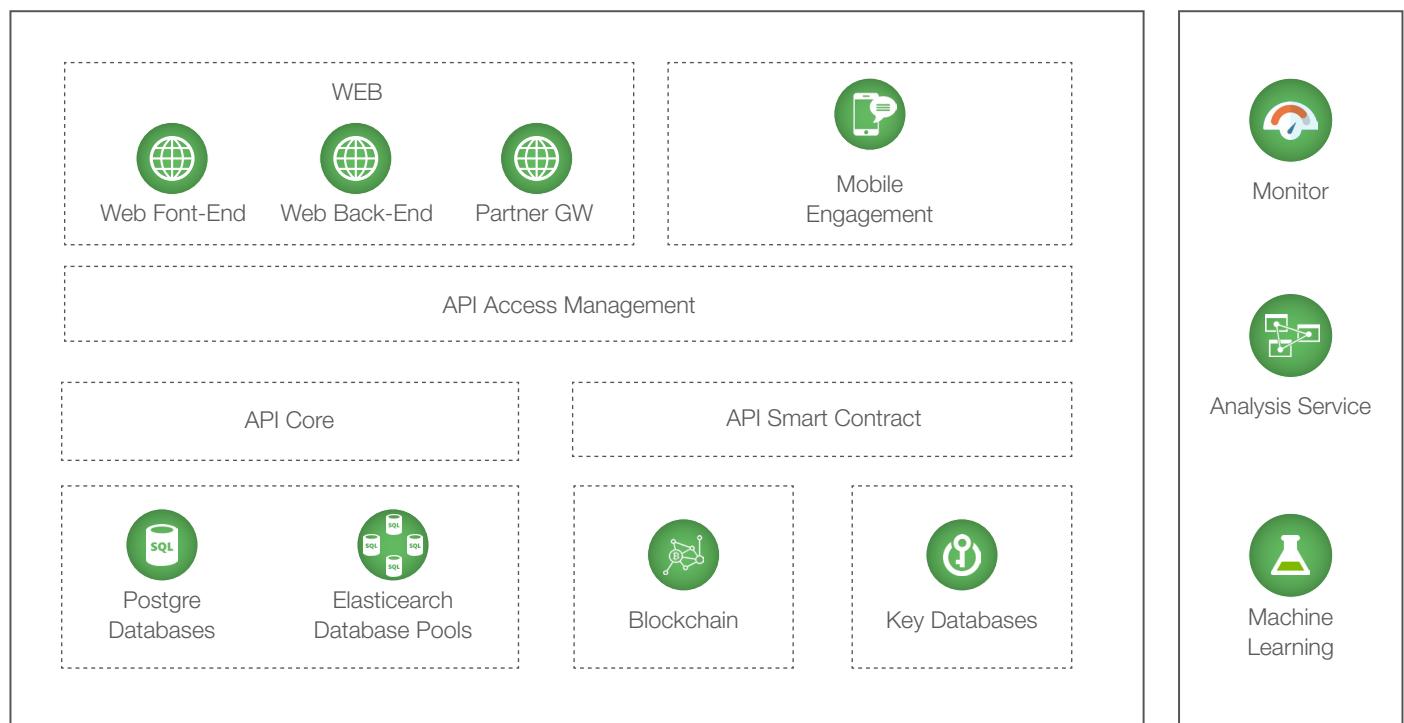
2. PRODUCT OVERVIEW

2.4 Record Transaction on Blockchain

Customer's VeriME application interacts with Blockchain to confirm transactions between members of the ecosystem with the Charge and Sharing scheme as described in Sections 3 & 4.

2.5 VERIME System Architecture

VERIME ARCHITECTURE DIAGRAM



3. D-KYC REVENUE MODEL

3.1 D-KYC Revenue Source

D-KYC will be offered in two service bands as mentioned below. Partners can choose appropriate service during D-KYC request based on their business needs.

Service Description	Checks performed
Basic	Passport, National ID, Driving License, email, Phone number
Advanced	Basic + PEP/AML/CTF Checks + Negative News screening

When performing D-KYC on a Customer, a Partner is required to pay service fee in the following 2 scenarios:

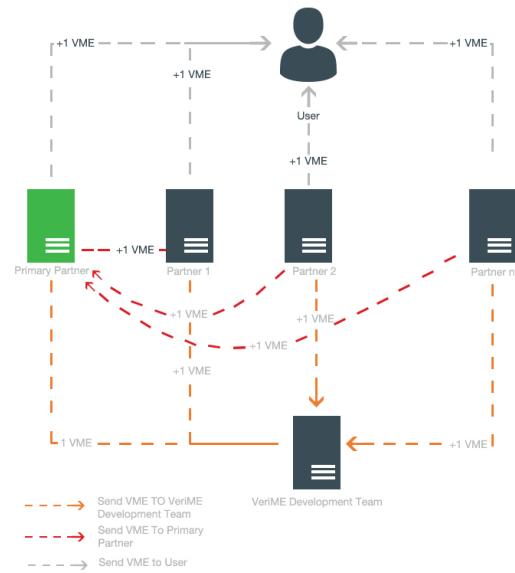
a) This Customer performs D-KYC for the first time through VeriME: in this case, this Partner is called PRIMARY, pays only 2/3 of the service-fee.

b) This Customer has performed D-KYC through VeriME with another PRIMARY Partner in the past: in this case, this Partner is called SECONDARY and will be charged full service-fee.

After careful evaluation of its Partners' needs, VeriME Team have decided to price its D-KYC service in US Dollars. This would enable both Crypto and traditional partners to seamlessly purchase VeriME services using various payment methods.

Partners would have option to purchase number of KYCs to be performed from VeriME in various payment currencies, for ex: USD, VME, BTC, ETH etc. If the partner purchases D-KYC service in a non-VME form, VeriME will convert the payment into VME tokens by purchasing VME from an exchange. When VME Tokens (i.e. Number of D-KYCs) runs out, the Partner (directly or through VeriME) will have to purchase more tokens through Exchanges and load them into VeriME wallet to continue using D-KYC service, thus stimulating the demand for VME Token on the market.

Fee collected is subjected to sharing as described in section 3.2.



Note:

- "Primary Partner" is the Partner with whom Customer/User performs D-KYC with VeriME for the FIRST time;
- "Partner 1-n" are the Secondary Partners where that X Customer/User performs D-KYC with VeriME for the following times;

3. D-KYC REVENUE MODEL

3.2 D-KYC Incentive Sharing Scheme

In addition to the practical benefits described in Section 1.3, members of VeriME ecosystem are also entitled to benefit sharing according to the following specifications:

WHO	BENEFITS	PURPOSE
The first 1,000 Partners to integrate VeriME to D-KYC Customers	Each Partner is rewarded with 1,000 D-KYCs (in the form of VME tokens) in the VeriME Wallet on the Blockchain.	<p>Free "Gasoline" for early Partners to adopt VeriME immediately without having to buy the Token. This reward scheme will activate the VeriME Partners network & grow quickly before reaching the self-growth stage.</p> <p>This rewarded VME Token is not transferrable & it can only be used to pay for D-KYC and D-SECURE services offered by VeriME. This mechanism will prevent bad Partners from signing up just to get reward Tokens and resell them for immediate profit.</p>
Each first customer that PRIMARY Partners get to perform D-KYC through VeriME	(*) A Referral Fee equivalent of 1/3rd of the service fee will be paid for each first Customer performing D-KYC with SECONDARY Partners in the future.	This mechanism will motivate the Partners to accelerate the incorporation of VeriME to D-KYC their customers, in order to become PRIMARY Partner to as many Customers as possible, thereby gaining "referral income" every time those Customers perform D-KYC or D-SECURE with other SECONDARY Partners in the future.
Customers perform D-KYC with VeriME Partners	(**) A Usage Fee equivalent of 1/3rd of the service fee will be paid per D-KYC transaction with a VeriME Partner.	This mechanism will motivate Customers to enthusiastically prioritize performing D-SECURE through VeriME when using online services provided by the Partners.
VeriME Team	(**) A Processing Fee equivalent of 1/3rd of the service fee will be retained per D-KYC transaction.	This mechanism will generate revenue for reinvesting into upgrading systems, adding functionalities and developing VeriME ecosystem on not-for-profit principles.

4. D-SECURE REVENUE MODEL

4.1 D-SECURE Revenue Source

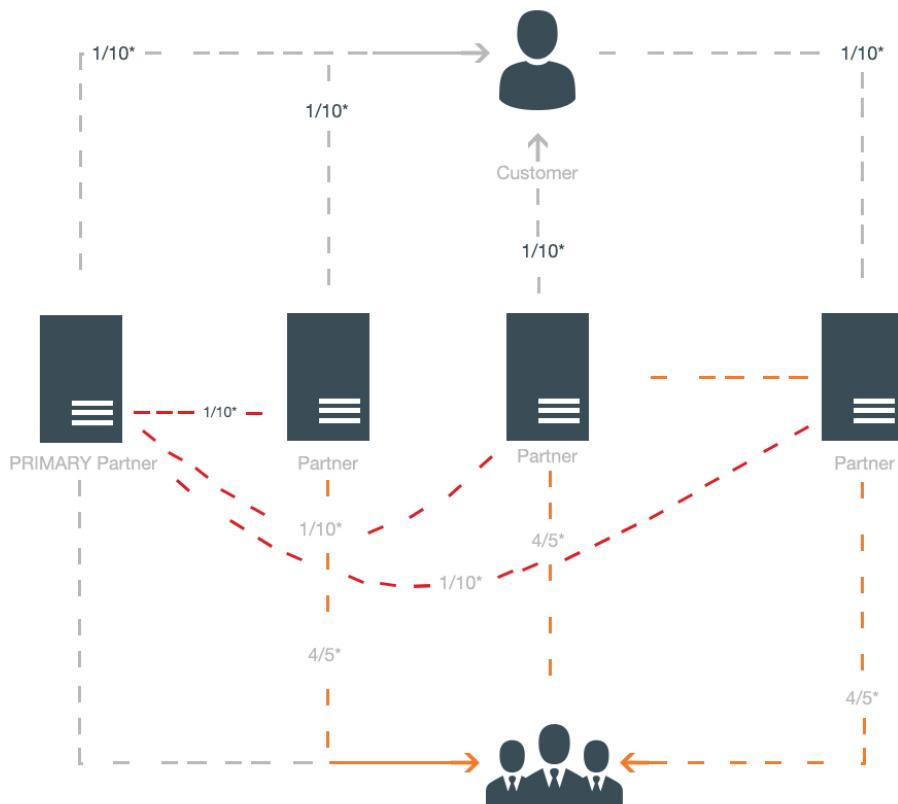
The service fee that the Partner has to pay for each D-SECURE transaction through VeriME would be in percentage of the Sale amount. For example: if the Sale amount is \$100 USD and D-SECURE fee is 1.00%, \$1.00 USD equivalent of VME Token

NOTE: 1.00% is indicative pricing. We expect pricing to be in the range of 0.5%-1.50%

When performing D-SECURE on a Customer, a Partner is required to pay service fee in the following 2 scenarios:

- This Customer performs D-SECURE for the first time through VeriME: in this case, this Partner is called PRIMARY Partner. The Partner pays only 9/10 of the service fee.
- This Customer has performed D-KYC or D-SECURE through VeriME with a PRIMARY Partner in the past: in this case, this Partner is called SECONDARY and will be charged service fee in full.

Fee collected is subjected to sharing as described in section 4.2.



4. D-SECURE REVENUE MODEL

4.2 D-SECURE Incentive Sharing Scheme

In addition to the practical benefits described in Section 2.3, members of VeriME ecosystem are also entitled to sharing of benefits according to the following structure:

WHO	BENEFIT	PURPOSE
The first 1,000 Partners to integrate VeriME to D-SECURE Customers	Each Partner is rewarded with \$1000 of D-SECURE Payment Protection value (in the form of VME Tokens) in the VeriME Wallet on the Blockchain.	<p>Free "Gasoline" for early Partners to adopt VeriME immediately without having to buy the Token -> This reward scheme will activate VeriME Partners network & enable it to grow quickly.</p> <p>This rewarded VME Token is not transferrable & it can only be used to pay for D-KYC and D-SECURE services offered by VeriME. This mechanism will prevent bad Partners from signing up just to get reward Tokens and resell them for immediate profit.</p>
Each first Customer that PRIMARY Partners get to perform D-SECURE through VeriME	(*) A Referral Fee equivalent of 1/10th of the service fee will be paid for each first Customer performing D-SECURE with SECONDARY Partners in the future.	This mechanism will motivate the Partners to accelerate the application of VeriME to D-SECURE their customers, in order to become PRIMARY Partner to as many Customers as possible, thereby gaining "passive referral income" every time those Customers perform D-KYC or D-SECURE with other SECONDARY Partners in the future.
Customers perform D-SECURE with VeriME Partners	(*) A Usage Fee equivalent of 1/10th of the service fee will be paid per D-SECURE transaction with a VeriME Partner.	This mechanism will motivate Customers to enthusiastically prioritize performing D-SECURE through VeriME when using online services provided by the Partners.
VeriME Team	(**) A Processing Fee equivalent of 4/5th of the service fee will be retained by VeriME team per D-SECURE transaction.	This mechanism will generate revenue for reinvesting into upgrading the systems, adding functionalities and developing VeriME ecosystem on not-for-profit principles.

(*) Why is 1/10? If the Customer performs D-SECURE with a PRIMARY Partner, the PRIMARY Partner would pay discounted fee of 9/10 of the total fee. When a Customer performs D-SECURE with a SECONDARY Partner, that Partner must pay service fee in full, then both PRIMARY Partner and the Customer would receive 1/10 of the fee.

(**) Why 4/5? This is because VeriME is providing Chargeback and Dispute protection to its Partners. The funds would be used to cover Risk, build and continuously improve VeriME's risk management based on Biometric and Machine Learning tools.

4. D-SECURE REVENUE MODEL

VeriME supports all fiat currencies. When the currency of Sale is a non-USD currency, US Dollar would be used as Base currency to calculate VME service fee.

Example:

Sale amount = S\$100 (Singaporean Dollar)

Base Amount [USD] = \$74 (using Trusted Foreign Exchange Rate Provider)

VeriME D-SECURE Fee in USD = \$0.74

VME<>USD Rate: 1 VME = \$0.10*

D-SECURE Pricing to Partner = 1.00%*

VeriME D-SECURE Fee in VME = 7.4000

Customer Usage Fee in VME = 0.7400

Primary Partner Referral Fee in VME = 0.7400

VeriME Processing Fee in VME = 5.9200

*sample price. Partner Pricing and Exchange rate may vary.

4.3 D-KYC & D-SECURE INTEROPERABILITY

VeriME is built on a shared ecosystem model where both Partners as well as Customers take active role in building and nurturing VeriME's products and services. Hence, benefits and incentives offered by VeriME products are interoperable.

E.g.: A Customer can perform D-KYC with VeriME's Partner (Eg: a TelCo) for the first time, and can subsequently perform D-SECURE with other VeriME's partners (E.g. a Payment Gateway).

In this scenario, not only does the Customer benefit from Usage Fee (1/3 of service fee) from D-KYC, but he/she would also benefit from subsequent Usage Fees (1/10 of D-SECURE service fee) which can be deemed as rewards in the form of VME Token.

Similarly, PRIMARY Partners (i.e, TelCo) can benefit from passive referral income regardless of VeriME products (D-KYC or D-SECURE) their customers are using with other Partners. This referral income can be originating from any business, irrespective of the business the PRIMARY Partner is in. In this scenario, Telco would earn passive revenue from a Payment Gateway Partner of VeriME!

5. BUSINESS DEVELOPMENT

5.1 Our Achievements so far..

Many other ICO projects are just ideas with no ready product. With VeriME, the research and development of the product has been going on since January 2016, and today, the product is in practical use in Vietnamese market. VeriME's solution is based on a complete product, and not just an idea.

Currently VeriME is being used by many leading FinTech companies in Vietnam with D-KYC performed on more than 30,000 Customers. It will start expanding to other global partners after the ICO campaign. Some of the highlights* of its Vietnam operations are:

#	Partner Name	Business	Customer Base
1	NganLuong.vn	Largest online payment gateway in Vietnam	57,000+ Active Merchants
2	VIMO.vn	Leading mobile e-Wallet in Vietnam	More than 200,000 e-wallet Users
3	VayMuon.vn	First Peer-to-Peer lending network in Vietnam	More than 16,000 Users
4	Weshop.asia	One of the largest marketplaces in Vietnam and ASEAN	Largest Vietnamese marketplace with millions of customers
5	12trip.vn	Online Travel Agency (start-up)	Vietnamese OTA reselling more than 1 million hotels/properties

*partial list as at the time of ICO launch. Full list of partners can be found here: <https://www.verime.mobi/partners>

5. BUSINESS DEVELOPMENT

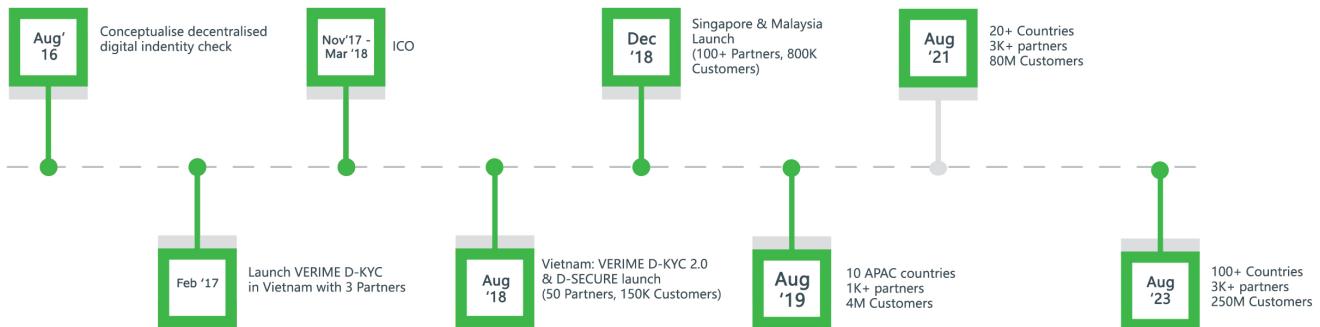
5.2 Sales Strategy

VeriME will employ a high-quality sales force to rapidly acquire Partners who are operating Websites and Mobile Applications (in both Blockchain and traditional space) that require KYC and/or Authentication services, especially in financial services industry.

VeriME Team comprises of domain experts and functionaries from Payment Schemes, Banking and Financial organizations as well as Entrepreneurs who have built Payment Systems and FinTech companies from scratch to multi-million-dollar revenue grossers. Our existing customer and partner base consists of many businesses that can easily adapt VeriME's D-KYC and D-SECURE solutions.

Each qualified Partner is expected to bring about 10,000 Customers. A single Customer can perform VeriME services multiple times with different Partners. It is anticipated that by reaching 10,000 Global Partners and 100 million Customers, VeriME ecosystem would become a large enough network to self-grow with long-term sustainability. The Token reward scheme would then be not necessary to acquire Partners afterwards.

5.3. Our Targets, Milestones & Roadmap



Short Term Goals:

- Support 2-3 APAC countries within 6 months of ICO with 100+ key partners
- Support 10 APAC countries with 1000+ partners within 12 months of product launch
- Support 20+ countries across APCEMEA and Americas with 3000+ partners within 24 months of product launch

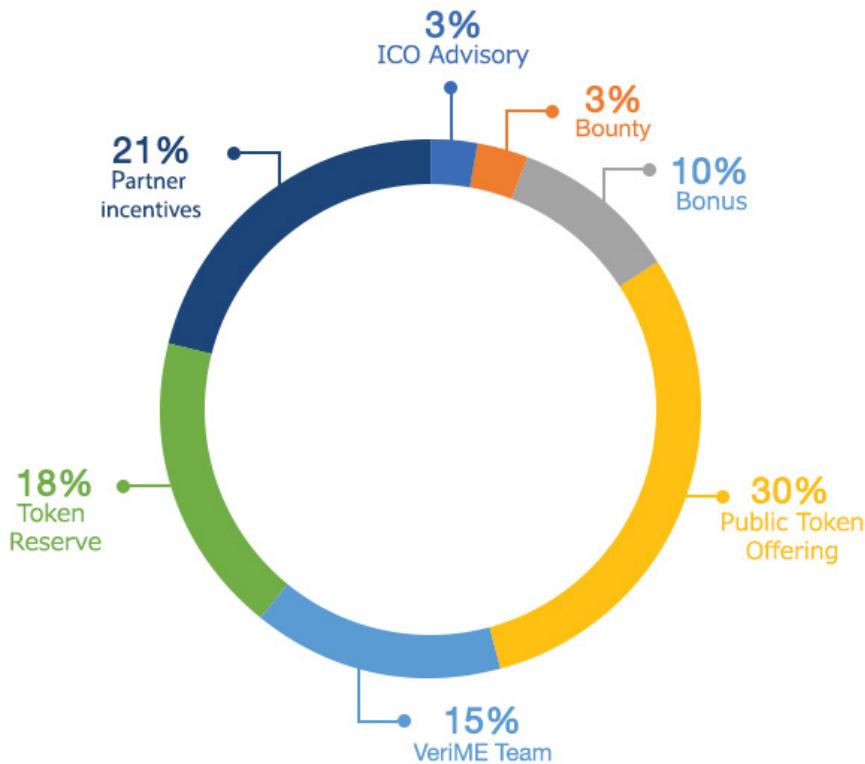
6. TOKEN ISSUE AND OFFER

6.1 Token Issuance

VeriME Team has issued 400 million VME tokens with code name VME to build and deploy its VaaS platform.

- Total Supply: 400 million VME
- Team: 60 million VME. This will be reserved for VeriME Team. These Tokens will be frozen for 18 months (until October 2019).
- Partner & Customer Incentives: 84 million VME. To be used for Partner and Customer Incentives. These Tokens will be part of VeriME Token Reserve and will be released to VeriME Partners and Customers. Please refer to Section 6.2 for more details.
- Reserve: 72 million VME. To be retained for future use as part of VeriME Reserve Management.

VERIME TOKEN ISSUANCE

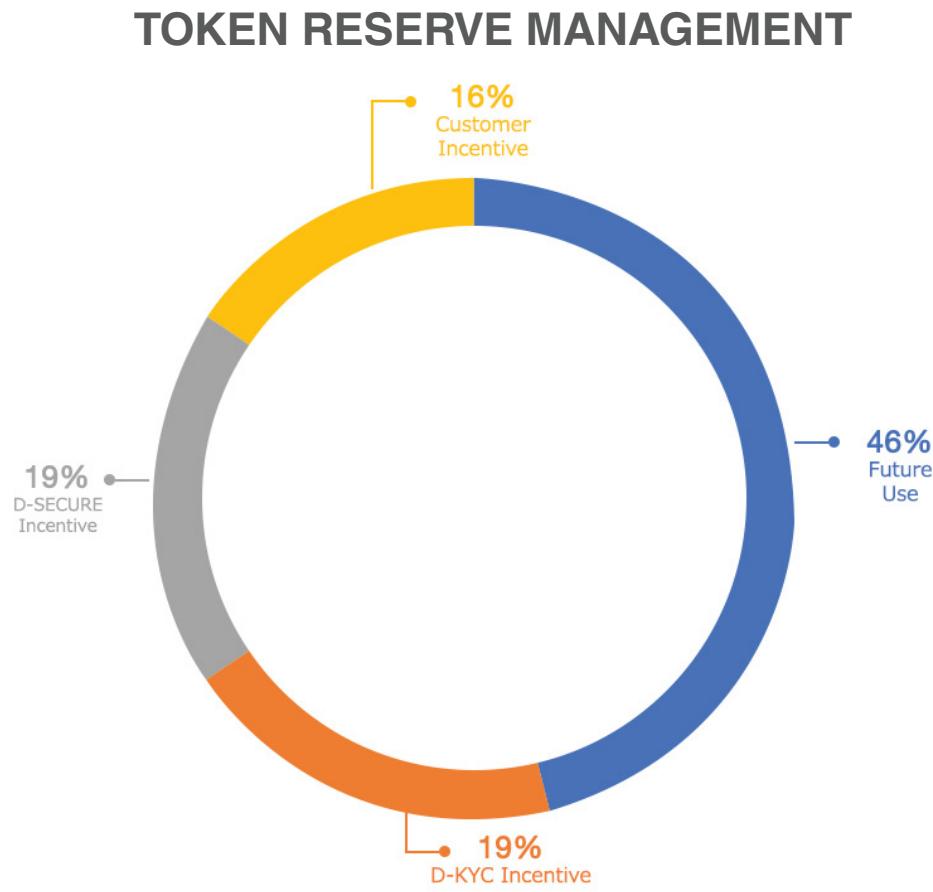


6. TOKEN ISSUE AND OFFER

6.2 Token Reserve Management

156 million VME Tokens will be utilized as below:

- 30 million VME Tokens will be used for D-KYC Partner incentives. i.e, first 1,000 D-KYC Partners will be incentivised as described in Section 3.2
 - 30 million VME Tokens will be used for D-SECURE Partner incentives. i.e, first 1,000 D-SECURE Partners will be incentivised as described in Section 4.2
 - 24 million VME Tokens will be used for Customer Incentives. i.e, first 1 million customers would be incentivised with 25 VME Tokens upon successful registration and first D-KYC or D-SECURE transaction.
 - Remaining 72 million VME Tokens will be frozen till April 2019 & will be used for incentive programs in the future.



6. TOKEN ISSUE AND OFFER

6.3 Token pricing & Anti-inflation

The initial price of VME Token issued in the ICO campaign is calculated as 1 VME = 0.000333333 ETH. Thus:

- 1 ETH = 3000 VME Token

This is the first and only VME Token issuance, after this campaign there will be NO other VME Token issuance. This is to maintain value of the token by ensuring its scarcity.

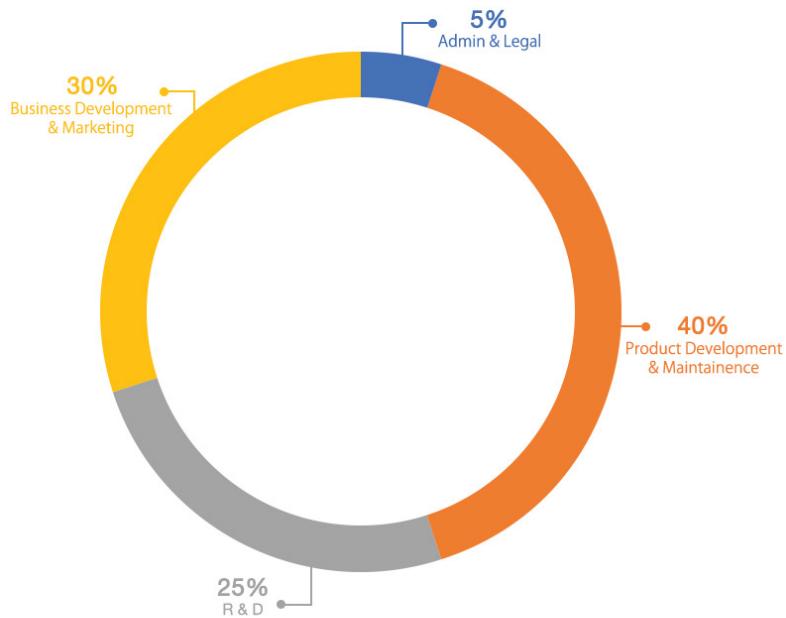
6.4 Use of Proceeds

The funds raised will be used solely for the development of VeriME ecosystem over the next five years (from the beginning of 2018 to the end of 2022) to reach the targets defined in section 5.3, thus increasing value of VME Token.

ICO proceed will be spent as below:

- 40% of the proceeds: Building, developing and maintaining the technology infrastructure for VeriME applications on a decentralized, Blockchain-based model.
- 25% of the proceeds: Researching and developing new forms of D-KYC & D-SECURE based on biometric, machine learning technologies & supplementation of identity proof documents from 150 countries around the world.
- 30% of the proceeds: Business development, Partner acquisition and Marketing of VeriME brand to Customers.
- 5% of the proceeds: Administrative, Office, Legal & other expenses.

USE OF PROCEEDS



6. TOKEN ISSUE AND OFFER

6.5 Value Increase Potentials

The incentive sharing among all stakeholders mentioned in sections 3.2 & 4.2 will create network effects in the VeriME ecosystem, enabling exponential growth of VeriME, leading to a strong value increase for VME Token. This, in turn, opens up great opportunities for those who own VME Token.

As VeriME becomes a popular VaaS platform in the Blockchain and traditional space, many Partners will have to purchase VME Tokens in the open market through the Exchanges to use VeriME services. As demand increases, the value of VME Token will grow sharply, bringing great benefits to the members in the VeriME ecosystem.

Once VeriME ecosystem garners identity data of hundreds of millions of Customers and trusted by thousands of prestigious Partners, this block chain based decentralised data store will be an extremely valuable "capital" asset for developing more services and extensions with the aid of AI and Big Data. This will keep the entire ecosystem growing in the long term.

7. PEOPLE AT VERIME

7.1 CORE Team

NGUYEN HOA BINH: Co-Founder & Chairman



Nguyen Hoa Binh is Group CEO and Founder of NextTech Group of companies, a multi-national group of 40+ companies, pioneering in Digitalization Services with an ecosystem of 20+ businesses in Commerce, Logistics, FinTech with annual revenue over 90 million USD.

Mr Binh has 16+ years of start-up experience in the Internet & Payments industry since 2001 when he was an undergraduate student at Vietnam National University. He holds master degree in Urban Informatics from Osaka City University and has won more than 30 prestigious technology awards during his entrepreneurial career.

For the last decade, Mr. Binh has been pioneering into multiple new technology trends including e-Commerce, e-Logistics and FinTech. Prior to NextTech, he was a well-known young technology entrepreneur in Vietnam as the founder of PeaceSoft group, Vietnam's leader in e-Commerce and e-Payment industry.

SANJEEV KUMAR: Co-Founder & Chief Strategist



Sanjeev Kumar has over 20 years of experience in the Internet & Payments Industry. For the last decade, Sanjeev has been instrumental in rolling out innovative products and solutions across APAC markets with focus on China, ASEAN and Japan. Prior to VeriME, Sanjeev served as Chief Product and Marketing officer at Omise, a Thai Payments start-up. Sanjeev also held various senior leadership positions at Visa, CyberSource, Elavon, Cap Gemini and ANZ Banking Group.

NGUYEN HUU PHU: CEO VeriME Vietnam



Mr Phu is Bachelor of Science graduate in Information Technology, University of Engineering, Hanoi. He has spent many years in FinTech and IT Security space. Under NextTech group, he has spent many years in design and development of ERP systems for Corporate Governance & over the last 3 years on Block chain research. His other areas of expertise include ERP & Big Data.

7. PEOPLE AT VERIME

LE VAN LUONG: CTO VeriME



Mr Luong has 9 years of experience in FinTech, Biometric & Telecommunications and is a Payments & Cryptocurrency veteran in Vietnam. In the past, Mt Luong led Research & Development wing for Vietnam Science Academy, in co-operation with NTU Singapore on 'Study of digital image recognition technology based on low-level characteristics of image (CBIR)'.

PHAM NGOC TRAM ANH: PR – Communication Manager



Tram Anh is a Group PR Manager at NextTech Group. She is a PR and communications expert with more than 10 years of experience. Combining both corporate and agency experience, she has developed and managed execution of variety of brand and corporate communications campaigns. Tram Anh holds Bachelor's Degree in Journalism from University of Social sciences & Humanities, Hanoi.

7. PEOPLE AT VERIME

7.2 Advisory Team

NIZAM ISMAIL (<https://www.linkedin.com/in/nizam-ismail-2a4090b/>)



- Partner & Head of Financial Services, RHTLaw Taylor Wessing
- Co-Founder of RHT Compliance Solutions (leading compliance consultancy in Southeast Asia)
- Former Executive Director and Head of Compliance for Southeast Asia, Morgan Stanley and Lehman Brothers
- Former Deputy Director and Head, Market conduct policy division, Monetary Authority of Singapore [MAS]
- Former Deputy Public Prosecutor, State Counsel, Singapore

Dr INDAKA NAYANAKKARA (<https://www.linkedin.com/in/indy-nanayakkara/>)



- CEO, Lucerne Investment Partners
- Co-Founder & CEO, Piquant Capital
- Former Head of Equities at Henderson Global, Macquarie Group, Credit Suisse

IGOR PESIN (<https://www.linkedin.com/in/igorpesin/>)



- FinTech Investor & Partner, Life.Sreda VC Fund
- Partner & Chief Financial Officer, Based on Blockchain Fund
- Founder & CEO, ECOM Ltd., Russian Federation

Dr KANTH MIRIYALA (<https://www.linkedin.com/in/kanthmiriyala/>)



- CEO and Co-Founder TuringLabs ICO Services, Revelin7 & CryptoKnights Podcast
- Founder / Advisor / Early Stage Investor in Quintant (sold to iGATE), Qik (sold to Skype), Gravitant (sold to IBM), Cicada Resorts (sold to Premji Invest)
- Former Head of Global Business Consulting at iGATE

7. PEOPLE AT VERIME

7.3 Promoters

NEXTTECH GROUP: NextTech (www.nexttech.asia) is a group of 30 businesses spread across Asia Pacific region. The group employs more than 600 staff across 7 markets, under 3 main verticals: Digitized Commerce, Fintech and Digitized Logistics, with FY2017 estimated processing volume of \$500 million USD and \$90 million USD in revenue.

NextTech specializes in Digital innovation, managing a wide range of businesses including Online Store Front & Marketplace, Cross Border Trade, Online Payment Gateway, Mobile Wallet, Mobile Point-of-Sale, Online Lending, Online Payment Gateway, Warehouse & Fulfilment, Last Mile Delivery, STEAM Education, Cross-border remittance, Online Travel Agency etc.

NextTech group has field operations in 8 world-wide offices: Hanoi, Vietnam (HQ), Ho Chi Minh City (Vietnam), Bangkok (Thailand), Kuala Lumpur (Malaysia), Jakarta (Indonesia), Manila (Philippines), San Jose (California USA), and Guangzhou (China).

8. OTHER MATTERS

8.1 Potential Risks

Please carefully read every piece of information, understand and analyse the risks related factors, before deciding to participate in the investments and purchase of VME tokens. By purchasing, anyone holding, owning and using VME Tokens should clearly recognize and presume the risks which are likely to be, including but not limited to:

- a) Risk of losing access to VME Tokens due to loss of Private keys, or any kind of custodial or purchaser errors.
- b) The Partners and Customers need to have a private key, or a combination of private keys, which is necessary to control and dispose of VME Tokens stored in your wallet
- c) The funds raised in the token generation event are exposed to risks of theft.
- d) VeriME, if in any case, is significantly and unfavourably affected, if it fails to efficiently administer its procedures as its business builds up and progresses, which would have a straight blow on its capability to maintain the VeriME platform or even to launch any future platforms.
- e) Risks arising from lack of governance rights or any changes made to put restrictions over the cryptocurrency utilization in Vietnam, Singapore and any other territory all over the world.
- f) Risk of attacks, uninsured losses, from taxation, uncertain regulations and enforcement actions, associated with markets for VME tokens etc.
- g) Risks arising from dissolution of the company, unfavourable fluctuation of BTC or ETH values, hacking, cyberattacks and security weaknesses.
- h) Risks associated with the Ethereum protocol, because VME tokens and VeriME ecosystem are based on the Ethereum protocol, any malfunction, breakdown or abandonment of the Ethereum protocol may have an adverse effect on the platform or VME Tokens.
- i) General global market and economic conditions may have an adverse impact on VeriME's operational performance, results of operations, and cash flows.
- j) VME token holders can lose their investments owing to the VME tokens falls to zero, by any means of market forces.
- k) The risks related to the ICO investments should be carefully analysed and speculated, so as to avoid any hassles after or during the ICO stages.
- l) Regulatory risks: The regulation of tokens such as the VME Tokens is still in a very nascent stage of development in Singapore. A degree of uncertainty as to how tokens and token-related activities are to be treated exists. The applicable legal and regulatory framework may change subsequent to the date of issuance of this White Paper. Such change may be rapid and it is not possible to anticipate with any degree of certainty the nature of such regulatory evolution. VeriME does not in any way represent that the regulatory status of the VME Tokens will remain unaffected by any regulatory changes that arise at any point in time before, during, and after this offering.
- m) No regulatory supervision: None of VeriME or its affiliates is currently regulated or subject to the supervision of any regulatory body in Singapore. In particular, VeriME and its affiliates are not registered with MAS in Singapore as any type of regulated financial institution or financial advisor and are not subject to the standards imposed upon such persons under the Securities and Futures Act, Financial Advisors Act, and other related regulatory instruments. Such persons are required to comply with a variety of requirements and standards concerning disclosures, reporting, compliance, and conduct of their operations for purposes of maximising investor protections. Since VeriME is not subject to such requirements or standards, it will make decisions on those issues at its own discretion. While VeriME will have regard to best practices on these issues, holders of VME Tokens may not necessarily enjoy the same extent and degree of investor protections as would be the case should they invest with regulated entities instead.

8. OTHER MATTERS

n) No fiduciary duties owed: As VeriME is not a regulated financial institution, it does not owe investors in VME Tokens any fiduciary duties. This means that VeriME has no legal obligation to always act in good faith in the best interests of holders of VME Tokens. While VeriME will have regard to the interests of holders of VME Tokens, it is also permitted to consider the interests of other key stakeholders and to prefer these interests over the interests of VME Tokens holders. This may mean that VeriME is permitted to make decisions that conflict with the interests of VME Tokens holders. Not owing any fiduciary duties to holders of VME Tokens also means that holders of VME Tokens may have limited rights of recourse against VeriME and its affiliates in the event of disputes.

o) Tax risks: The tax characterization of VME Tokens is unclear. Accordingly, the tax treatment to which they will be subject is uncertain. All persons who wish to purchase VME Tokens should seek independent tax advice prior to deciding whether to purchase any VME Tokens. VeriME does not make any representation as to whether any tax consequences may arise from purchasing or holding VME Tokens.

p) Risks from third parties: The tokenised nature of VME Tokens means that they are a blockchain-based asset. The security, transferability, storage, and accessibility of blockchain assets depends on factors outside of VeriME's control, such as the security, stability, and suitability of the underlying

blockchain (in this case, the Ethereum blockchain), mining attacks, and who has access to the private key of a wallet where VME Tokens are stored. VeriME is unable to assure that it can prevent such external factors from having any direct or indirect adverse impact on any of the VME Tokens. Persons intending to purchase VME Tokens should note that adverse events caused by such external factors may result in the loss of some or all VME Tokens purchased. Such loss may be irreversible. VeriME is not responsible for taking steps to retrieve VME Tokens lost in this manner.

q) Risks in purchasing VME Tokens: VeriME cannot and does not guarantee or otherwise assure that there are no risks in relation to your purchase of VME Tokens. The purchase of VME Tokens may, depending on the manner in which the relevant purchase is effected, involve third parties or external platforms (e.g., wallets). The involvement of such parties or platforms may introduce risks that would not otherwise be present, such as misconduct or fraud by the third party, or your failure to receive VME Tokens upon duly making payment because of a third-party wallet's incompatibility with VME Tokens. VeriME is not responsible for any risks arising due to the involvement of third parties, including the risk of not receiving (or subsequently losing) any or all VME Tokens you attempt to (or successfully) purchase.

8.2 Legal Statement

a) The presentation of this whitepaper is solely for informational purposes. The participants interested in investing in VME tokens should analyse and consider various associated risks prior to making any kind investment decisions in the VeriME pre-ICO & ICO.

b) The VME Tokens are not securities or units in a collective investment scheme or business trust, each as defined under Singapore's Securities and Futures Act (Cap. 289) ("SFA"). Accordingly, the SFA does not apply to the offer and sale of the VME Tokens. For the avoidance of doubt, this initial offering of VME Tokens need not be accompanied by any prospectus or profile statement and no prospectus or profile statement needs to be lodged with the Monetary Authority of Singapore ("MAS").

c) This White Paper does not constitute an offer of, or an invitation to purchase, the VME Tokens in any jurisdiction in which such offer or sale would be unlawful. No regulatory authority in Singapore, including the MAS, has reviewed or approved or disapproved of the VME Tokens or this White Paper.

d) This White Paper and any part hereof may not be distributed or otherwise disseminated in any jurisdiction where offering tokens in the manner set out this White Paper is regulated or prohibited.

8. OTHER MATTERS

- e) The information in this White Paper is current only as of the date on the cover hereof. For any time after the cover date of this White Paper, the information, including information concerning VeriME's business operations and financial condition may have changed. Neither the delivery of this White Paper nor any sale made in the related initial token offering shall, under any circumstances, constitute a representation that no such changes have occurred.
- f) VeriME does not make or purport to make, and hereby disclaims, any representation, warranty, undertaking, or other assurance in any form whatsoever to any person, including any representations, warranties, undertakings, or other assurances in relation to the truth, accuracy, or completeness of any part of the information in this White Paper.
- g) Whether taken as a whole or read in part, this White Paper is not, and should not be regarded as, any form of legal, financial, tax, or other professional advice. You should seek independent professional advice before making your own decision as to whether or not to purchase any VME Tokens. You are responsible for any and all evaluations, assessments, and decisions you make in relation to investing in the VME Tokens. You may request for additional information from VeriME in relation to this offer of VME Tokens. VeriME may, but is not obliged to, disclose such information depending on whether (i) it is legal to do so and (ii) the requested information is reasonably necessary to verify the information contained in this White Paper.
- h) VME Tokens are intended for use within applications available on the VeriME intermediary digital Validation-as-a-Service (VaaS) ecosystem and VeriME warrants that the VME Tokens are fit for these purposes. However, VeriME is not responsible for compelling any person to accept VME Tokens and disclaims, to the fullest extent permitted by law, all liability for any adverse consequences arising out of or in relation to such rejections of VME Tokens.
- i) Upon purchasing any VME Tokens, you will be deemed to have reviewed this White Paper (and any information requested and obtained from VeriME) in full and to have agreed to the terms of this offering of VME Tokens, including to the fact that this offering does not fall within the scope of any securities laws in Singapore and is not regulated by the MAS. You further acknowledge and agree that the VME Tokens are not securities and are not meant to generate any form of investment return.
- j) The VME Tokens and related services provided by VeriME (if any) are provided on an "as is" and "as available" basis. VeriME does not grant any warranties or make any representation, express or implied or otherwise, as to the accessibility, quality, suitability, accuracy, adequacy, or completeness of the VME Tokens or any related services provided by VeriME, and expressly disclaims any liability for errors, delays, or omissions in, or for any action taken in reliance on, the VME Tokens and related services provided by VeriME. No warranty, including the warranties of non-infringement of third party rights, title, merchantability, satisfactory quality, or fitness for a particular purpose, is given in conjunction with the VME Tokens and any related services provided by VeriME.
- k) VeriME will accept only ETH, BTC, XRP, NEO, LTC, USDT, Singapore Dollar [SGD] and United States Dollar [USD]; Investors from United States are not allowed to invest in this ICO.

8. OTHER MATTERS

8.3 Forward Looking Statements

Certain information set forth in this whitepaper includes forward-looking information regarding the future of the project, future events and projections. These statements may be identified by but not limited to words and phrases such as "will", "estimate", "believe", "expect", "project", "anticipate", or words of similar meaning. Such forward-looking statements are also included in other publicly available VeriME materials such as videos, blog posts, interviews, etc. Information contained in this whitepaper constitutes forward-looking statements and includes, but is not limited to:

- i) the projected performance of the project;
- ii) completion of the campaign;
- (iii) the expected development of the project;

(iv) execution of the project's vision and strategy;
(vii) future liquidity, working capital, and capital requirements.

The forward-looking statements involve a variety of risks and uncertainties. Should any of these risks or uncertainties materialise, the actual performance and progress of VeriME might differ from expectations set by the forward-looking statements. These statements are not guarantees of future performance and no undue reliance should be placed on them. VeriME undertakes no obligation to update forward-looking statements if circumstances change. By acting upon forward-looking information received from the whitepaper, VeriME website and other materials produced by VeriME, you bear full responsibility in the case of forward-looking statements not materialising.

Contact and Support

Reach out to us if you have any questions about anything on VeriME through below contacts:

-  : <https://www.verime.mobi/>
-  : hello@VeriME.mobi

-  : press@VeriME.mobi
-  : contact@VeriME.mobi

Social

Reach out to us if you have any questions about anything on VeriME through below contacts:

-  : https://twitter.com/VeriME_mobi
-  : <https://www.facebook.com/Verime-Digital-Pteltd-484328191950430>
-  : https://www.youtube.com/channel/UC_OE9x12I7lif-ZEzljtC2g?disable_polymer=true
-  : <https://www.reddit.com/user/VeriEMobi/>
-  : <https://medium.com/@verime.mobi>