VAULT

Security You Can Trust

Vault Smart Security Token Knowns as VSS Token

Last Updated: 12 December.2018

Version: 7.0 - English

TheVault Ltd.
(Company Registration No. 201819091D)

Written by: Dannie Francis (dannie@thevault.foundation) and
Marco Baik (mailto:marco@thevault.foundation)

CONTENTS

IMPORTANT NOTICE

Please read this section carefully.

This white paper ("White Paper") has been issued by TheVault Ltd. ("Vault"), and has been prepared by the persons named on the cover page on behalf of Vault.

This White Paper may not be distributed, disseminated or otherwise transmitted to any country where such distribution, dissemination or transmission may be prohibited. Further, no part of this White Paper is to be reproduced, distributed, disseminated or otherwise transmitted without including this entire section titled "Important Notice".

GENERAL DISCLAIMER

This White Paper is a work in progress and will be updated with more details from time to time. Due to the incredible interest in the Vault Platform and the token sale relating to the Vault Smart Security Token ("VSS Token"), this White Paper has been made available for public evaluation.

More details about the Vault Platform and token usage may be added from time to time in a series of updates which will be noted on Vault's official website at http://www.thevault.foundation ("Website"). Whilst more information may be added, Vault does not intend to change its core offering, token structure, token distribution, and use of funds.

Before participating in the token sale, you should consider the information in this White Paper carefully, and consider whether you understand what is described in this White Paper. For more information about the token sale, please visit the Website. Please be cautious of other phishing sites and similar sites. If you are in doubt as to the action you should take, please consult your financial, legal, tax, technical or other professional advisors.

LEGAL DISCLAIMER

This White Paper and the information contained herein, should be regarded as an informative document describing the technical and business aspects of the Vault Platform (comprising the Vault Security Consensus Network, the Vault AI-powered Fraud Detection Solution and the Vault Consumer Protection Layer), the VSS Tokens, the token sale, and the people involved in the Vault Platform. This White Paper is not binding and Vault shall not be responsible for any loss arising from the use, reference, or basing of information from this White Paper.

This White Paper is prepared based on the current views and plans of Vault. Certain statements, estimates and financial information contained in this White Paper can be regarded as forward-looking statements. Such forward-looking statements or information involve known and unknown risks and uncertainties, which may cause actual events or results to differ materially from the estimates or the results implied or expressed in such forward-looking statements. Vault reserves the sole and absolute discretion to revise this White Paper from time to time by posting the updated White Paper on the Website. Such updated White Paper will become effective immediately from the time of posting.

The sole purpose of this White Paper is to provide the recipient with preliminary information regarding the token issue to assist the recipient in deciding whether they wish to buy the tokens issued by Vault and to express their respective interest to Vault in order for Vault to be able to determine the final conditions of the token issue.

Separate terms and conditions will apply to the token sale, and to the use of the tokens. These terms and conditions should be read and consulted before entering into any transaction. A purchaser contemplating acquiring tokens should not make a decision relying solely upon this White Paper.

All statements of opinion and all projections, forecasts, or statements relating to expectations regarding future events or the possible future performance represent Vault's own assessment and interpretation of information available to it currently.

For the avoidance of doubt, the tokens do not qualify as capital markets products, securities or any other financial or investment instrument in any jurisdiction. The tokens cannot be used for any purposes other than those provided in the White Paper, including but not limited to, any investment, speculative or other financial purposes. The tokens are not intended for sale or use in any jurisdiction where sale or use of digital tokens maybe prohibited.

None of the information in this White Paper has been filed with, reviewed by, or approved by any regulatory authority. This Whitepaper does not constitute a prospectus or offer document of any sort. This White Paper is also not intended to constitute an offer of, or a a solicitation for investment in, capital markets products, securities or any other financial or investment instrument in any jurisdiction. This White Paper does not constitute an offer to sell or a solicitation of an offer to purchase the tokens in any jurisdiction in which such offer or solicitation is not authorized or to any person to whom it is unlawful to make such offer or solicitation.

Vault reserves the right, exercisable in its sole and absolute discretion, to review and decide whether to accept (with or without conditions) or reject any offer to purchase the VSS Tokens during the token sale. Please refer to the terms and conditions for the token sale of the VSS Tokens for further information.

The purchasers shall conduct their own investigation as to the potential legal risks and tax consequences related to the issue of and purchase of the tokens.

This White Paper should not be construed as the provision of financial advice or investment advice by Vault. If you are in any doubt as to whether to purchase the tokens proposed to be offered by Vault and described herein, you should consult financial, legal, tax, technical or other professional advisors.

LANGUAGE DISCLAIMER

This White Paper was conceived, designed and written in the English language. The Vault team is currently working with multiple entitles to translate this White Papers to other languages. In the event of any conflict or inconsistency, the English version of this White Paper shall take precedence over the translated version.

1. EXECUTIVE SUMMARY

Cyber security is the #1 issue facing the cryptocurrency sector, and until we establish a universal layer of trust, the sector will never achieve its true potential.

The cryptocurrency sector suffers from an acute lack of trust because exchange and wallet services are primarily centralized, largely un- or self-regulated, and devoid of the standards of consumer protection we expect from traditional financial organizations. In fact, most exchanges and wallet providers go to great lengths to warn consumers they bear zero responsibility for the safety of crypto transactions or the storage of coins and tokens.

If the cryptocurrency sector is to find mass adoption, we must do better. A 2018 global fraud report by Experian that explored consumer trust and fraud links exposes the flaws in the crypto sector's "trustless" subculture.

The Experian report reveals that 75% of merchants businesses want advanced authentication and security measures without disruption to the consumer experience, that 53% of consumers abandoned online transactions for a variety of trust-related security reasons and that 66% of consumers liked visible security measures because "it makes me feel more protected."

Against a background of high profile hacks and consumer skepticism for crypto currencies, the Vault Platform, comprising the the Vault Security Consensus Network, the Vault AI-powered Fraud Detection Solution and the Vault Consumer Protection Layer, will deliver the protection and trust levels, the sector needs and consumer's deserve.

The Vault Platform seeks to eliminate fraud, stop cyber attacks and prevent consumer errors in digital payment transactions and across digital payment networks whether they are crypto currency or traditional banking networks.

Vault will lower transactional costs by replacing expensive, slow trusted third parties with a faster, lower cost decentralized security consensus network and deliver guaranteed consumer protection standards to digital payments whether using fiat or crypto currencies.

Consumers use traditional banks because they trust the security infrastructure banks deploy, and the regulatory mandates that govern them.

But many crypto exchanges, wallets and token providers, have not invested sufficiently in the security processes and fraud management practices to protect their consumer members, nor have they embraced a decentralized security consensus protocol capable of providing consumers, merchants and Governments with a corresponding sufficient level of trust.

Vault has been established to build a security solution that is capable of delivering a level of consumer confidence, that will drive mass adoption of cryptocurrencies and blockchain based digital payments by consumers.

While cryptocurrency industry initiatives such as the Crypto Currency Security Standards (CCSS) has been prepared as a guide for all organizations that provide cryptocurrency services, there is no regulated or self-regulated authority to mandate the implementation of such practices or provide auditing oversight or certification.

If the cryptocurrency sector wants legitimacy, then it must accept the responsibility of putting in place layers and frameworks necessary to maintain the highest levels of security standards. The Vault Security Consensus Network can help deliver a legitimate level of trust.

From its inception, the cryptocurrency sector has been victimized, stalked by hackers and cybercriminals. High-profile cryptocurrency hacks and heists (CoinCheck, Bitfinex, DAO, Mt Gox, NiceHash) have resulted in over 1.2 billion US dollars in crypto coin value being stolen in the past 4 years. ICOs scream opportunity to cyber criminals.

Frauds involving Veritaseum, Enigma, CoinDash, and breaches against Tether and Parity Wallets are well-publicized highlights of an endemic activity.

Whether it is fraud, theft, cryptojacking or the result of phishing, social engineering or ransom attacks, investors and traders at both consumer and institutional levels have lost funds, just as much as the cryptocurrency sector loses its respectability.

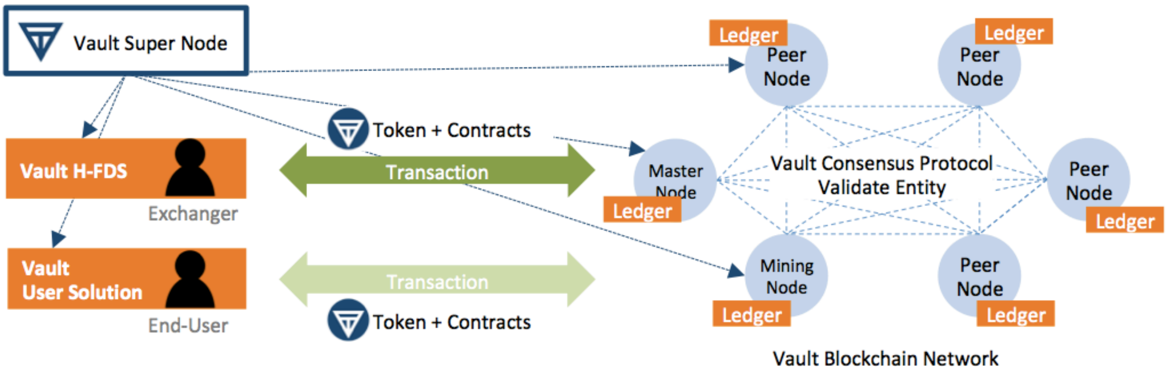
Yet almost none of the major crypto exchanges or wallet providers in operation today are PCI DSS Level 1 compliant (an expectation we as consumers have, and one which government regulators mandate that traditional banks and payment gateways comply with).

With demand at a premium, and without an alternative, consumers, investors, traders and business partners are forced to accept what are in fact “unacceptable” standards of risks to the security of their digital assets.

Against this backdrop of poor security practices, the demand for cryptocurrency continues to grow. More people are participating with each passing day as new coins are being launched and the growth of the industry marches on relentlessly, largely unchecked, under regulated and uncertified.

Vault has a solution to bring this lunacy to an end. Vault’s solution is smart, secure, effective and rooted in the experience of a proven security software and management processes using the world’s premier blockchain technology and powered by the Vault Security Consensus Network, the Vault AI-powered Fraud Detection Solution and the Vault Consumer Protection Layer.

Overview of the Vault Security Consensus Network



Within the Vault Security Consensus Network, each entity acts as follows:

1) Vault Consumer Protection Layer. The end user solution collects the necessary information from various access environments such as PC, mobile, and web.

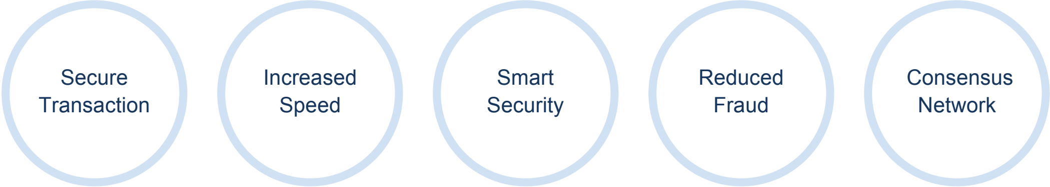
2) Within the Vault Security Consensus Network, cryptocurrency users and exchanges create new blocks, making requests for secure transactions.

3) Each node in the Vault Security Consensus Network is responsible for data processing for Vault's Artificial Intelligence powered-Hybrid-Fraud Detection System (AI-HFDS). The Vault Super Node communicates with each node, performing authentication and verification of each node's role, and serves as a control tower for efficient operation of the network.

The decentralized Vault Security Consensus Network is designed as an improved version of the Practical Byzantine Fault Tolerance algorithm, improving disadvantages such as uncertainty and performance issues, and specifically preventing malicious attacks from any access points throughout the network's eco-system.

This is a decentralized, highly secure eco-system in which trusted nodes join the algorithm in agreement with the blockchain and verified by tokens and smart contracts.

Key Advantages of the Vault Platform



Secure Transaction

Increased Speed

Smart Security

Reduced Fraud

Consensus Network

1. Secure, Error-free Transactions

By deploying the world's first artificial intelligence-powered Hybrid Fraud Detection blockchain Solution (AI-HFDS), we eliminate blacklisted address, fraudulent behavior, identify anomalies and irregularities and even consumer errors from transactions.

2. Increased Speed

The Vault Platform is built on one of the fastest blockchain technologies and when coupled with AI-powered AI-HFDS driving trust relationships with master node operators, result in the capability to process real time transactions in excess 4,000 transactions per second.

3. Smart Security

To guard against various cryptocurrency fraud and hacking scams that target both Exchanges and consumers, the Vault Platform pairs the AI-HFDS with a Consumer Protection Layer providing the data to power the machine learning engine.

4. Reduced Fraud and Risk

The Vault Platform's AI-HFDS significantly reduces the capability of criminal transactions through blacklist management, multidimensional user verification, and deep learning-based fraud transaction sign modeling.

5. Security Consensus Network

Vault’s strategy to empower its partners to arm their customers with the security to protect every end point, every access point throughout their network is coupled with a strategy of cooperation between nodes on the Vault Security Consensus Network..

Even existing non-crypto-focused financial organization such as banks, telcos, government organizations, existing payment gateways and credit card companies will be able to join the Vault Security Consensus Network.

The Vault Security Consensus Network will provide master nodes and operators with access to real time data and shared intelligence to the benefit of all members of the cryptocurrency community while protecting the anonymity of the consumer/user and the trustless state of the blockchain.

2. INTRODUCTION

2.1 Background

Vault is dedicated to the public interest of providing security policies and security solutions to the cryptocurrency industry. The Vault Platform can protect all parties who buy or trade in cryptocurrency from the host of potential risks they face whether it be from cyber criminal activity or the frailties of their own information system infrastructure.

Vault's AI-HFDS and end-to-end security solution offers protection to the entire ecosystem. The efforts of C4 and Cryptocurrency Security Standards (CCSS), have culminated in standards that exchange, wallet and token providers should be observing in building their systems.

They have defined methodologies and provided a matrix to guide in the development of information systems to make them more secure. While we strongly support this initiative, we do not believe it goes far enough to enable cryptocurrency service providers to "guarantee" the safe trade or storage of digital assets.

CCSS defines the use of security practices such as multi factor authentication scheme using TOTP and OTP (time-based and one time passwords), PRNG (pseudo random number generators), multi-signature (multisig) practices on wallet management, the trusted environment of enterprise servers, multi level backup policies etc.

Yet, despite these guidelines, it seems most exchanges and wallet providers have not gone the extra mile to implement these guidelines, or have not done so with independent third party oversight. Government regulators have yet to mandate security levels across the global landscape. Unless the industry embraces the need for a higher level of security, it leaves us all at risk.

As of March 2018, the cryptocurrency market has been growing rapidly around Bitcoin. There are about 1,560 kinds of cryptocurrencies registered by the major cryptocurrency exchanges, and the number of cryptocurrency wallet users is approximately 23.6 million, demonstrating a growth of about 100% over the previous year.

The cryptocurrency market scale is about USD411 billion, with an average daily transaction value of USD16.2 billion. The average number of transactions per month for the past six months is about 8.5 million.

So let's look at some of the potential threats and security problems to end users, traders and exchanges and within the technology of the exchange and wallet providers:

First, problem of cryptocurrency wallet management

Most personal cryptocurrency users (hereinafter “users” or ‘consumers’) are exposed to a host of threats as they manage their cryptocurrency activities by themselves. In particular, they must guard against a wide range of threats from both random and professional attacks such as phishing, malware, and ransomware scams. It is both a burden and risk for these consumers, to establish and manage security policies to prevent such attacks.

In addition, they, especially new users, face risks arising from self-management. For example, if a consumer mistypes or otherwise incorrectly enters the address of a recipient’s wallet, the transaction could be lost forever. A user may not receive the tokens purchased at an ICO if such user accidentally provides the wrong wallet address. These mistakes are commonplace.

Similarly, if a crypto wallet is created and managed directly without going through a wallet provider with password management protocols and the consumer loses his/her wallet's private key, there may be no way to recover it and all coins/assets will be lost.

When a consumer logs into his/her own crypto-currency wallet through a personal (or public) PC, if the user's information (cryptocurrency wallet address, private key) is leaked through a phishing program installed in the PC, hackers can move all the user's coins to the hacker's wallet.

According to statistics in Bitcoin.com, cryptocurrency worth about USD9.1 million per day was stolen of hacked due to the above reasons in the first two months of 2018.

Second, risk factors of the cryptocurrency exchanges.

Many cryptocurrency exchanges are operated relatively autonomously due to the lack of conformity and governing laws and regulations related to exchanges, as the governing laws and regulations vary in each country. Therefore, many exchanges fail to establish and apply effective security policies on their own.

However, if the exchange is hacked due to security vulnerabilities, it may lead to direct damage to the consumers and institutional investors who use them.

For example, if an exchange has unwittingly leaked user information stored in their server through a hacking initiative as with the infamous Coincheck hack, the hacker can transfer the exchange customer’s cryptocurrency to the hacker's cryptocurrency wallet.

Even if authorities can track the address to a destination, retrieval of the customer’s assets may never be achieved.

Likewise, if the exchange's internal personnel leak customer information or pass on the customer's cryptocurrency to their wallet due to poor security management, as with the Bithumb employee’s case in 2017, hackers who obtain customer addresses may steal the cryptocurrency.

In 2014, the world's largest exchange, Mt.Gox, went bankrupt due to the hacking of 850,000 BTC (about USD470 million at that time), and in January 2018, USD524 million worth of NEM coins was hacked from the Japanese exchange Coincheck (now owned by Monex).

While all the specifics as to how the hacking happened are still not clearly identified, it is clear to the security experts that the primary reason is likely to be poor security management.

According to survey data from the University of Cambridge in the UK, for major cryptocurrency exchange operators, the exchange itself believes that IT security processes and the threat of hacking are the greatest risks they face, followed by worsening of relations with banks, and fraud in financial transactions.

These risks are even more acute in small and medium-sized exchanges that are rated at high risk for IT security, hacking and financial transaction fraud.

Exchange Operational Risk Factor Check List (2017, Cambridge University)

1: Very low risk, 2: Low risk, 3: Medium risk, 4: High risk, 5: Very high risk

	Weight average	Small exchanges	Large exchanges
IT security/hacking	3.70	3.93	3.17
Fraud	3.45	3.50	2.08
Regulation (in general)	3.08	2.89	3.50
AML/KYC enforcement	2.68	2.64	2.75

Third, vulnerability of cryptocurrency associated technology.
If a consumer is harmed by the technical vulnerability of a cryptocurrency token or exchange, it is practically impossible for the consumer to prove a loss or claim compensation for the damage.

In addition, many cryptocurrency related technologies are run by non-profit public licenses, and users themselves may be liable for damages caused by using public technology. It is seemingly simple for these organizations to avoid any liability.

Cryptocurrency wallet types can be divided into hardware wallets (Cold Wallet) and software wallets (online for desktop, mobile, and web usage), and there are currently about 135 various software wallets. Many cryptocurrency software wallet providers have potential weaknesses from a technical process and security technology point of view.

However, they have protection by featuring warnings about loss responsibility, or incorrect storing of passwords or phrases etc. or terms stating ‘under development’ and asking users to accept the terms of use even if software bugs are unwittingly built into the code which may cause a loss of the cryptocurrency in the wallet.

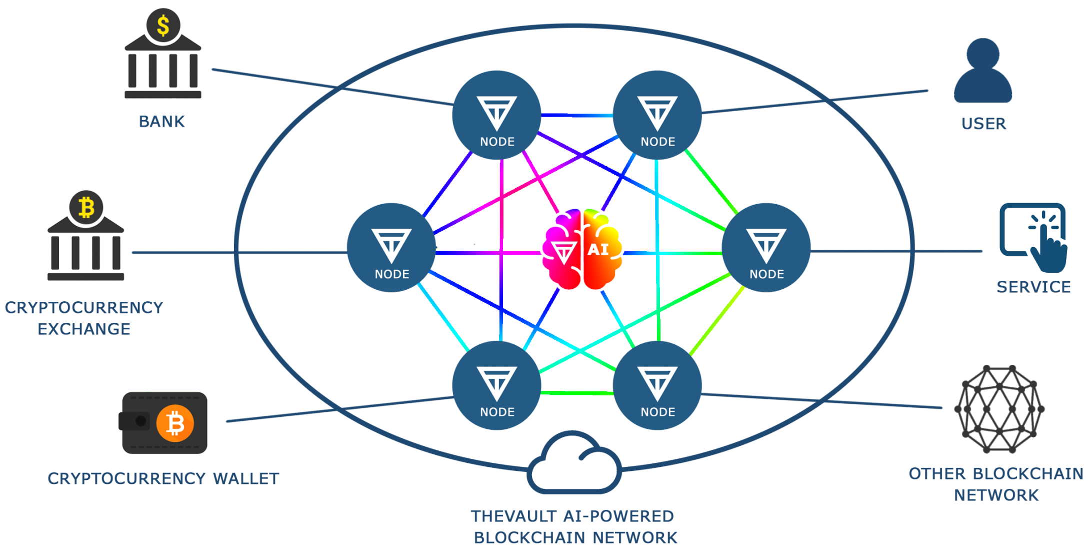
For example, users of Parity Technology's Multisig Wallet suffered damage in November 2017 to its Ethereum assets worth approximately USD280 million when a coding imperfection was set off by an unsuspecting user which wiped out library code and caused all wallets created since July to be frozen, ironically, because of a vulnerability in the Multi Signature security feature.

As you can see from the above description, there is a need for a solution that can guarantee the reliability of both a transaction and storage, whether the transaction came from a crypto source or a fiat source.

2.2 Concept

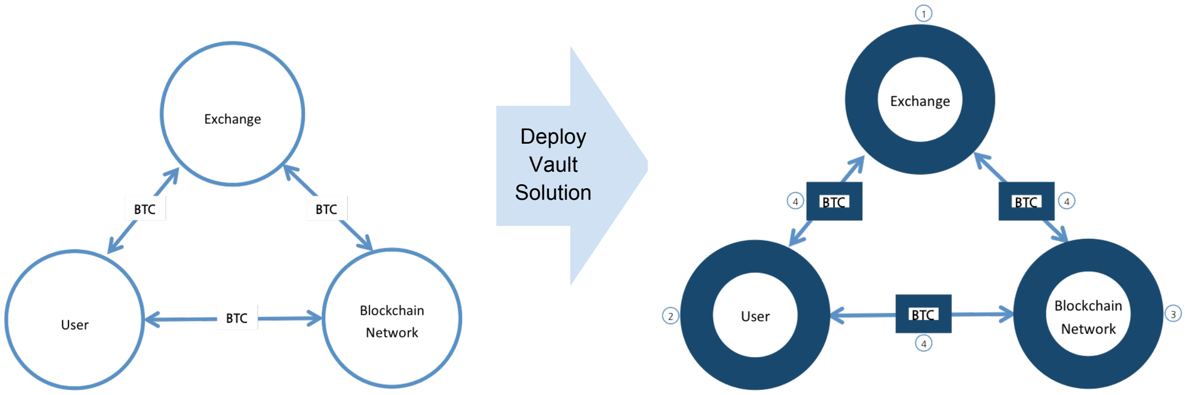
In order to solve the problems of the cryptocurrency industry, we propose the Vault Platform (comprising the Vault Security Consensus Network, the Vault AI-powered Hybrid Fraud Detection Solution and the Vault Consumer Protection Layer), a multi-dimensional security solution for the entire cryptocurrency ecosystem including Exchanges, merchants, users and other service providers and is built to include government departments, banks, telcos etc.

The Vault Platform Ecosystem



The Vault Platform is based on DNA of Vault, to build ‘a bridge of trust’ between all parties from consumer investors to wallet and exchange providers and from both fiat and cryptocurrency sectors.

As shown in the figure below, Vault's security solution with various security functions can be plugged into the services of each service provider to participate in Vault's security network.


Current Cryptocurrency Transaction **Vault Security Transaction**

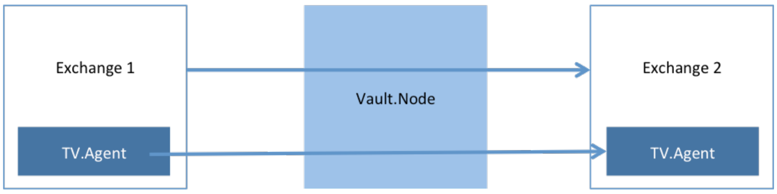
The explanation of how Vault delivers a secure transaction is as follows.

1. By deploying Vault's AI-HFDS, an exchange can be protected against the risk of hacking transactions or abnormal transactions between users and exchanges.

2. By delivering the Vault Consumer Protection Layer to the end user for PC, Mobile or web environments, the end user will be protected from various hacking, phishing, information leaks, and risk of abnormal or erroneous trading.

3. Vault provides an Application Programming Interface ("**API**") to the existing cryptocurrency network to provide secure technology to network users.

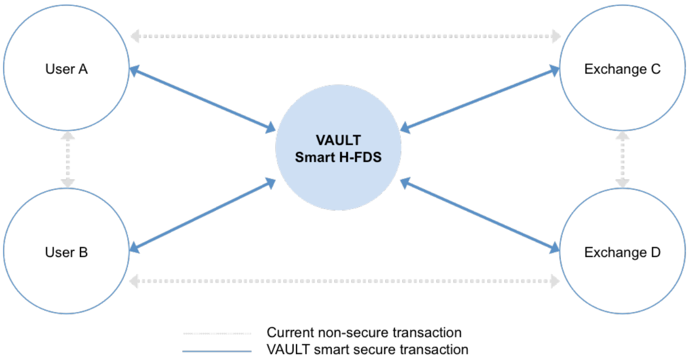
Transaction Flow Between Exchanges



The Vault Agent supports the Smart-Voting function to check the integrity of the cryptocurrency wallet address, to mutually verify the presence or absence of the address of the other party's wallet, to check whether or not the address is activated, to check blacklist registration and to measure the reliability of transaction target.

As shown in the figure below, the Vault Agent plays a role of relaying transactions in inter-personal and inter-exchange transactions

User, Exchange Transaction Flow


User A
Exchange C
VAULT
Smart H-FDS
User B
Exchange D
Current non-secure transaction
VAULT smart secure transaction

1) For example, when a user sends a 1 BTC from his/her Exchange A to a wallet address belonging to Exchange B, Exchange A checks whether the end user security solution of the Vault is installed, and if it is installed, the end user solution is executed.

After verification, transactions between all users and exchanges are protected by Vault's Platform.

When the user enters and transmits the address of the bitcoin wallet to be transmitted, the Vault Agent of Exchange A, is connected to the Vault Agent of the counterpart Exchange B, to perform functions to increase the reliability of transactions such as checking the validity and existence of the wallet transaction destination address, whether or not to register the blacklist, and the reliability of the electronic wallet address.

The Vault Agent of Exchange B will then review the internal database to respond to user-related questions received by the Vault Agent of Exchange A.

If the wallet address to be transmitted to Exchange B is not valid, or if the wallet does not exist, or has some irregularity, the Vault agent of Exchange B sends a message to the Vault agent of Exchange A, and Exchange A stops the user's transfer.

Exchange A then notifies the user that the address does not exist, and the transferring user goes through the process of re-checking the wallet address. This process prevents users from accidentally losing cryptocurrency.

Similarly, if Exchange A verifies that the address of Exchange B is registered in the blacklist via the Vault Agent, Exchange B shares the message with Exchange A.

Exchange A notifies the user that the account is registered in the blacklist and the user, depending on the rules of the Exchange, will act according to the options available.

The Vault Agent evaluates the reliability of the electronic wallet and protects the user from potential risk through the resulting level.

If the reliability is significantly lower, the exchange will notify the user that there is a related potential risk, and when transferring cryptocurrency to the corresponding wallet address, the user will go through additional authentication such as e-mail, phone, biometric or other approved types of authentication.

The Vault Consumer Protection Layer

The Vault Consumer Protection layer is an end user security solution that integrates with the rest of the Vault Platform components and offers a powerful security solution for digital payments cryptocurrency end users.

When a user transacts cryptocurrency from various access environments (PC, mobile device, web etc.), Vault provides security features optimized for each environment to protect users from various hacking, phishing, pharming, and other threats. It can be applied to the following cases.

1) When using a PC device

The end user security solution uses an 'Anti-Virus Engine' to protect the user's PC from all of the latest viruses and to block various cyber threats such as malware, spyware, and ransomware. When making a transaction from an exchange or wallet, the end user can invoke Vault's protection to guarantee the security of a transaction.

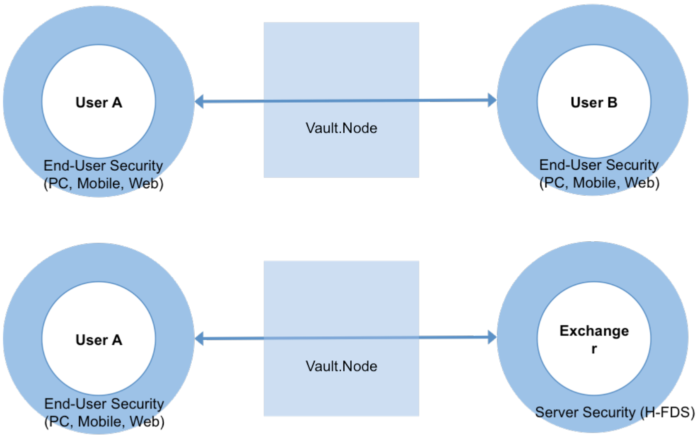
2) When using a mobile device

If a consumer uses a cryptocurrency wallet mobile app on his/her mobile phone, a cryptocurrency wallet app service provider simply plugs in the Vault mobile security module into the program to protect the user.

When a user accesses services through a mobile app protected by the Vault mobile security module, the app protects the user via features such as detection of abnormal execution, executable file encryption detection, app integrity verification, app tampering and payment bypass detection, hacking tool blocking detection etc.

As shown in the figure below, Vault's security layer protects the user, enabling reliable transactions between all users including both consumers and exchanges.

End User Security Method



Artificial Intelligence-Powered Fraud Detection System

By reinforcing security with the Vault AI-HFDS, cryptocurrency service providers (cryptocurrency wallet, cryptocurrency exchange, etc.) can set appropriate actions and business rules to cope with various types of user transaction problems.

For example, Vault's deep learning AI algorithm collects various trading patterns of cryptocurrency users from exchanges that join Vault’s Security Consensus Network.

This collected data creates data sets and finds correlations between data to identify patterns of behavior enabling it to point out irregularities based on established or a growing set of criteria created by the algorithm. Let us discuss some scenarios:

1) Use case of location information

If payment is made by a specific user at a restaurant in London, and then 30 minutes later the same user pays at a (for example), a restaurant in Singapore, the system knows the travel time is not sufficient to be in both places.

As the transaction needs to pass the predefined business rules share by nodes on the Vault Security Consensus Network, it would fail and then the relevant services rules would set in motion actions such as, denying the transaction or temporarily suspending the user's capability to transact until further verifications are made.

2) Use cases of user information and transaction history information

If a user who typically trades less than USD1,000 a day, suddenly initiates a trade of more than USD100, 000,,because of the wide differential from the usual trade pattern, Vault AI-HFDS will carry out the process of confirming the identity and authenticity.

3) Use case of user environment information

If whether there is a concurrent user, or other user environment changes are detected through analysis of connected environments (PC and mobile device, operating system, web browser, IP address) in cryptocurrency service which has the Vault AI-HFDS, the service provider will proceed with the user re-authentication or the identification steps.

2.3 Who We Are

Vault's co-founders and senior management team comprise experienced professionals from Asia’s fintech, marketing and cyber security sectors.

Dannie Francis:	Co-founder: linkedin.com/in/danniefrancis
Marco Baik il Kyoung:	Co-founder: linkedin.com/in/marcobaik

A full list of the management team and advisors can be found on
our official website (http://www.thevault.foundation)

2.4 Organization

Vault is a public company limited by guarantee that is run on a non-profit basis. Vault has a subsidiary, namely, TheVault Lab Pte. Ltd. which will engage global finance and security experts to conduct software development and network operations.

A description of each entity is given below.
1) Non-profit Corporation: Vault is incorporated in Singapore and will be responsible for issuing and managing the VSS Token.

2) Profit Corporation: TheVault Lab Pte. Ltd. has been incorporated in Singapore as a subsidiary of Vault. This corporation will be responsible for conducting research on strengthening security and processes related to cryptocurrency industry and industry-wide security policies. This corporation will also be responsible for maintaining and managing the Vault ecosystem, including developing Vault solutions, managing the Vault Platform, distributing solutions to the user, and updating the software.

3. AI-HFDS SOLUTION

3.1 Server-side Security ‘AI-HFDS’

Vault’s AI-HFDS is a solution to prevent unauthorized, fraudulent, illegal and or mistaken transactions by users, merchants, wallets and Exchanges.

Vault’s AI-HFDS collects and analyzes terminal, access and transaction information (see table for more information). Using a set of criteria for each access level, AI-HFDS is capable of detecting and if appropriate, blocking transactions based on that criteria (such as irregular user behavior patterns, unusual trade purchase or sale requests, location or device usage variations, blacklisted and greylisted addresses etc).

While the CryptoCurrency Security Standards (CCSS) sets out security guidelines for wallet and exchange providers, it is at the end of the day, not a mandatory set of features that must be implemented and audited. AI-HFDS sets policies on top of these guidelines to make security smarter and more secure.

The same can be said of existing banking systems. While many traditional banks emphasize the need for user side security or provide additional hardware solutions and multisig and multi authentication procedures, sophisticated hackers continuously find their way to navigate the many loopholes that exist in both environments.

In this way, Vault’s AI-HFDS solution (whether applied to traditional banking or the cryptocurrency industry) can be said to be a more protective measure than existing systems from both sectors, but especially so for cryptocurrencies.

For example, by collecting and analyzing various information from individuals and companies who are using cryptocurrencies, services can be created or provided to detect and block abnormal transactions. Through mobile devices, online virtual currency transactions are growing dramatically and the risks associated with them are also increasing.

The advantages of configuring a blockchain-based network are as follows:

First, security enhancements

Vault's blockchain network improves the reliability of the underlying data by preventing the data from being forged and tampered with to collect user information.

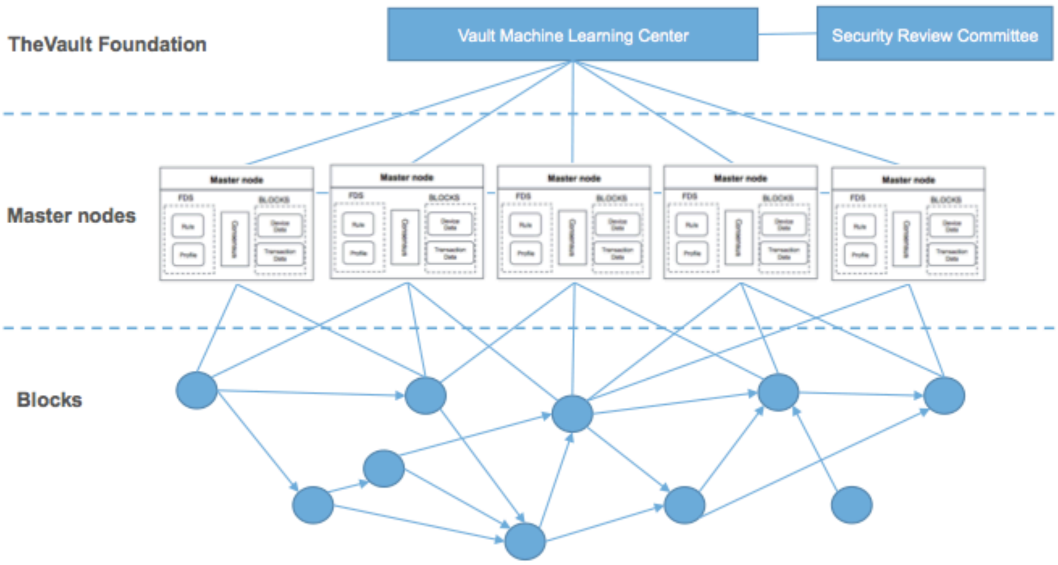
Second, improve compatibility

Because it is a non-translatable public platform, pre-validated systems can be delivered to end users and cryptocurrency service providers.

Third, cost and resource savings

Dependent systems, each deployed and operated by an individual operator, must be validated, and centralized system deployment requires significant cost and resources. Vault's blockchain network centrally manages minimal resources and distributes most of the data, enabling low-cost, highly efficient processing.

Vault Blockchain Network Diagram



Key components of the Vault Platform are described below.

1) Vault Machine Learning Center

We train transaction logs with deep learning to create abnormal transaction detection patterns in Vault's Machine Learning Center.

2) Security Review Committee

A Security Review Committee will establish and manage security policies and will review abnormal transaction detection pattern policies based on the Blacklist and Greylist terminal and Wallet addresses.

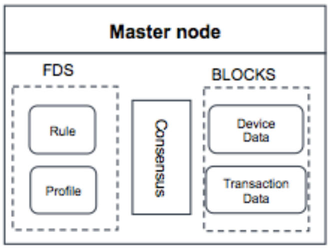
3) Master Node

The master node consists of the Ideal Trade Detection RULE and the Agreement, which uses the Vault Security Consensus Network The mainnet in the Vault Platform consists of a master node and detects any abnormal transactions. The blocks in each blockchain are utilized as a terminal information transaction log and information repository.

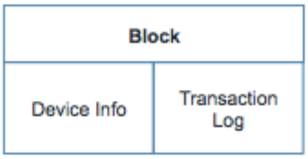
4) The Blocks device information and transaction log will be saved.

In order to prevent and minimize illegal use or fraud that may occur in these online virtual currency transactions, Vault is making efforts to introduce and develop AI-HFDS together with partner companies, government agencies, banks and exchanges.

Master Node Structure



Block Information



Using the AI-HFDS comprehensively determines the user's transaction use environment, transaction pattern, and transaction advance action, and judges whether or not abnormal transaction is performed according to each transaction’s allowance range.

The abnormal transaction detection pattern is composed of rules and scores. It is applied to electronic financial transaction for integrated analysis with a large capacity engine for patterns based on various user device acquisition information and transaction information and then, processes the blocked object information to the business server for abnormal signs.

The more data provided, the more accurate the analysis. Some sample information collected for basic deep learning is shown in the table below.

Sample Data: Access terminal log information collection items

Transaction Information	PC	Mobile device
User identification ID	Connector computer local IP	UUID
Transaction time	Proxy IP	UUID2
Remittance Wallet Address	VPN IP	Mobile OS version
Deposit account address	IP National band	Device manufacturer
Exchange code	MAC Address	Model name
Amount	HDD Serial Number	Voice call status
Channel identification code	CPU ID	Data communication status
Service identification code	OS information	Terminal ID
	Browser information	Terminal phone number
	USB Serial	Network operator code
	Biometric	SIM Card Country code
		SIM Card serial number
		Subscriber ID
		Terminal MAC Address Info
		Routing or escaping

3.2 User Security - PC

Vault's end-user solution is based on ‘Anti-Virus Engine’ (hereinafter ‘AV Engine’) and blocks various cyber threats including malware, spyware and ransomware and safeguards the cryptocurrency user's computer.

By installing Vault’s end user security program on the PC or mobile device, the cryptocurrency user can securely protect his/her systems and important information via real-time monitoring and protection.

Cryptocurrency exchanges or cryptocurrency-related software developers and service providers could protect users from the risk of potential hacking and phishing attacks that may occur in end user devices by installing Vault’s end user security programs.

3.2 User Security - Mobile

Vault's mobile security solution is designed to allow mobile app developers who develop cryptocurrency wallet etc. to quickly and easily apply security features by integrating Vault's security modules within the program.

Developers can protect users from various hacks by encrypting executable files and preventing hacking via Vault's mobile security agent.

3.3 User Security - Web

Vault's online and web security solution is an integrated online security solution that prevents information leaks, keyboard hacking, and various cryptocurrency accidents on your PC using cryptocurrency sites.

It supports various operating systems and web browsers, and is easily installed through HTML and Java Script. A variety of PC security features and regular pattern updates implement a secure PC experience.

4. VSS TOKENS

4.1 Value of the VSS Token

VSS Tokens are issued by Vault and will used to fund all of the components involved in providing smart secure transactions.

All nodes that join the Vault Security Consensus Network will receive revenue share from transaction fees of 0.005%. The remaining amount will be used to fund the organization and research and development into future technologies and partnership to ensure the mission of Vault remains on course to deliver smart, secure transactions.

4.2 VSS Token Acquisition

Users (Exchanges, end users, merchants etc), will need VSS Tokens to use Vault security services on their PCs, mobile devices, and the web.

Users must first create a VSS Token wallet before they can obtain VSS Tokens, and then create a Vault wallet in the following manner. To acquire a VSS Token, a user must create a Vault wallet.

How to Make a Vault Wallet:

1) Create a wallet with the security user program installed

After installing the Vault user security program, the user can create an account and create a VSS Token wallet linked to this account.

2) Create a wallet through a Vault website account

The user can create a Vault wallet after signing up on the Vault website,

3) Create a wallet through a cryptocurrency exchange

User will be able to create a VSS Token wallet through a cryptocurrency exchange where VSS Tokens are listed. After you create an account on the exchange, you can create a VSS Token wallet.

How to Acquire 'VSS Tokens'.

1) How users can acquire tokens

- Exchange using existing cryptocurrency

End user can acquire from any Exchange trading VSS Tokens.

- Participate in Vault's research, public service announcements and surveys

Vault will conduct research for users and businesses over time. Users can earn VSS tokens by participating in these Vault activities.

- Join the Vault bounty network

The Vault bounty programme will reward participants according to the rules of the programme.

2) How businesses / operators (Exchange, Miner, etc.) can acquire VSS tokens

- Participating Exchanges

Participating Exchanges will need to acquire sufficient VSS Tokens to enable their end users to access and protect their transactions with VSS Tokens.

- Token acquisition through operation of Vault master node

The Vault Security Consensus Network specifies proven master nodes by country and region for reliable service. These master nodes play a central role in transaction and AI-HFDS processing. By acting as a master node, an amount of VSS Tokens will be paid to master nodes.

- Token acquisition through mining of VSS tokens

Businesses that mine VSS Tokens are responsible for part of the transaction processing and will be rewarded accordingly.

4.3 Token Use

The scenarios for use are:

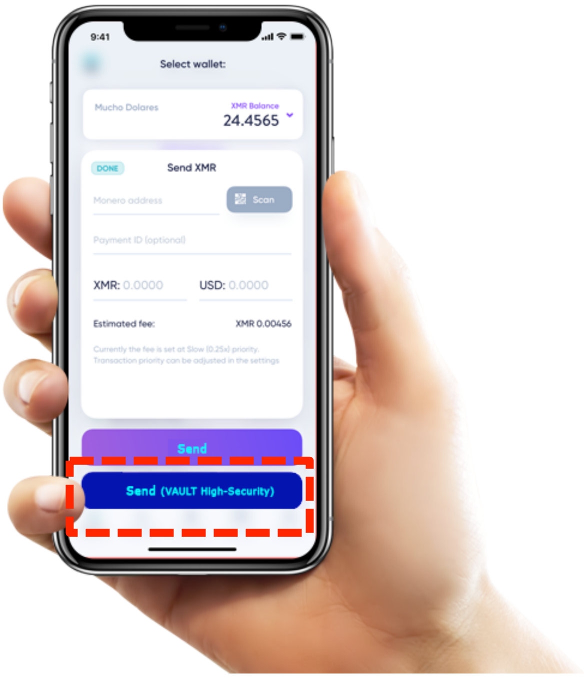
1) End Users

When using the Vault Consumer Protection Layer, the end user security solution that supports various access environments (PC, Mobile, Web), the user must use own VSS tokens.

2) Exchanges

When providing their end users to have access to Vault's Platform, Exchanges will be able to provide their end users with VSS tokens they can then apply to making as transaction safe.

Vault Security Transfer Screenshot



9:41

Select wallet:

Mucho Dolares

XMR Balance 24.4565

Send XMR

Monero address

Payment ID (optional)

XMR: 0.0000 USD: 0.0000

Estimated fee: XMR 0.00456

Currently the fee is set at Slow (0.25x) priority. Transaction priority can be adjusted in the settings

3) Cryptocurrency related business operator using AI-HFDS

If a cryptocurrency related business operator uses Vault's AI-HFDS, the operator can provide a high level of security services to its members.

In particular, Vault AI-HFDS improves accuracy through a variety of user and transaction modeling, and operates independently to provide improved security for each operator.

Operators can use VSS Tokens to operate AI-HFDS for servers with these advantages.

5. ROADMAP

In Q4, 2018, Vault will begin the offering of VSS Tokens until Q1, 2019, and Vault will launch security solutions in stages according to the technical Roadmap outlined below.

5.1 Business Roadmap

Date	Description
2018 Q4	• Start VSS Token token sale and Crowd Funding
2019 Q1	• Master node Partner application start • Roadshow, business development – Asia, Europe, America
2019 Q2	• Open USA HQ • Master node partner appointed
2019 Q3	• Open Europe HQ • Vault partner network event
2019 Q4	• Vault stakeholder event • Global publicity campaign starts
2020 Q4	• The Vault global exhibition

5.2 Technical Roadmap

Date	Description
2019 Q2	• Release open source of ‘Vault Smart Security Token’ (VSS)
2019 Q3	• Launch global developer network • Open source of TheVault.Wallet, developer forum – 1st
2019 Q4	• Launch The Vault tech wiki • Open source of TheVault.Security, developer forum – 2nd
2020 Q2	• Release demo of AI engine for AI-HFDS • Open source of TheVault.AI, developer forum – 3rd
2020 Q3	• 1st release of the Vault Platform (with all components included) • 1st The Vault Global Developer Exhibition
2020 Q4	• 2nd The Vault Global Developer Exhibition

6. CROWD FUNDING

6.1 Token Sales Plan

This White Paper describes how VSS Tokens are applied, the potential benefits of using tokens, and how and when tokens are acquired, the token release date, and the token offer basics.

6.2 Token Sales Offer

Vault intends to sell VSS Tokens (which may be used to pay for the protection of crypto currency and digital payment transactions) in a token sale.

The total number of VSS Tokens issued is 10,000,000,000 (10 billion).
1) 2,000,000,000 (2 billion) tokens are reserved for future use.
2) 900,000,000 (0.9 billion) tokens are held by the founders.
3) 3,100,000,000 (3.1 billion) tokens are arranged for partners, members, advisors and consultants.
4) 4,000,000,000 (4 billion) tokens are for crowd funding, members of the public, individuals and businesses

Type	Description
Reserved (20%)	Reserved tokens for future service and control token value
Founders (9%)	Reserved tokens for future service and control token value
Partners (31%)	Partners, Consultants, Advisors and team members
Token Offer (40%)	Token offer for crowd funding

6.3 Token Type

The VSS Token is a utility token that is to be used to fund transactions protected by the Vault Platform, not a security token. Having a VSS token is not an investment, and Vault does not provide any compensation for future profits to a VSS Token owner.

VSS Tokens are not a profit investment. VSS tokens are required for use by end users to fund the protection of digital payment and crypto currency transactions.

Vault is established based on the jurisdiction of Singapore prior to token sale and applies only the laws of that Singapore in relation to securities and security tests. VSS Tokens do not provide ownership of the stocks or assets of Vault or carry any right to the revenue or profits of Vault or any other third party.

6.4 Fund Usage

Funds received by Vault from the Crowd Sale are intended for use in the development and growth of the Vault Platform. The scope of development will be determined depending on the level of funds received and development will proceed according to the proposed priorities.

In using funds, Vault plans to use crypto-currencies whenever possible, but in order to pay some of the costs below, the crypto-currency funds must be exchanged with fiat currency.

The fund usage categories below provide a rough estimate of how the funds raised during the Crowd sale will be allocated.

- 60% is reserved for project design, research and development.
- 30% is allocated for operating costs including office rentals, equipment, servers, etc.
- 5% is allocated for sales, marketing, and community management.
- 5% legal counseling / expenses, 5% administrative fee

7. RISKS

7.1 Adherence To All Legal And Regulatory Standards

The purchase of any tokens involves a high degree of risk, including but not limited to the risks described below. Before purchasing the VSS Tokens, it is recommended that each participant carefully weigh all the information and risks detailed in this White Paper, and, specifically, the following risk factors.

A. Dependence on computer infrastructure

Vault’s dependence on functioning software applications, computer hardware and the Internet implies that Vault can offer no assurances that a system failure would not adversely affect the use of your VSS Tokens.

Despite Vault’s implementation of all of our expert and reasonable network security measures, our processing center servers are to some measure still vulnerable to computer viruses, physical or electronic break-ins or other disruptions of a similar nature.

Computer viruses, break-ins or other disruptions caused by third parties may result in interruption, delay or suspension of services, which would limit the use of VSS Tokens.

B. Smart contract limitations

Smart contract technology is still in its early stages of development, and its application is of experimental nature. This may carry significant operational, technological, regulatory, reputational and financial risks.

Consequently, although the audit conducted by independent third party increases the level of security, reliability, and accuracy, this audit cannot serve as any form of warranty, including any expressed or implied warranty that the Vault Smart Contract is fit for purpose or that it contains no flaws, vulnerabilities or issues which could cause technical problems or the complete loss of VSS Tokens.

C. Regulatory risks

The blockchain technology, including but not limited to the issue of tokens, may be a new concept in some jurisdictions, which may then apply existing regulations or introduce new regulations regarding blockchain technology-based applications, and such regulations may conflict with the current VSS Token Smart Contract setup and VSS Token concept.

This may result in substantial modifications of VSS Token Smart Contract, including but not limited to its termination and the loss of VSS Tokens as well as a suspension or termination of all VSS Token functions.

D. Taxes

Token holders may be required to pay taxes associated with the transactions involving VSS Tokens. It will be a sole responsibility of the token holders to comply with the tax laws of the relevant jurisdictions and pay all required taxes.

E. Force Majeure

Vault’s performance may be interrupted, suspended or delayed due to force majeure circumstances. For the purposes of this White Paper, force majeure shall mean extraordinary events and circumstances which could not be prevented by Vault or its management and shall include: acts of nature, wars, armed conflicts, mass civil disorders, industrial actions, epidemics, lockouts, slowdowns, prolonged shortage or other failures of energy supplies or communication service, acts of municipal, state or federal governmental agencies, other circumstances beyond Vault’s control, which were not in existence at the time of token sale.

F. Disclosure of information

Personal information received from VSS Token holders, the information about the number of tokens owned, the wallet addresses used, and any other relevant information may be disclosed to law enforcement, government officials, and other third parties when Vault is required to disclose such information by law, subpoena, or court order. Vault shall at no time be held responsible for such information disclosure.

G. Value of VSS Token

Once purchased, the value of VSS Token may significantly fluctuate due to various reasons. Vault does not guarantee any specific value of VSS Token over any specific period of time. Vault shall not be held responsible for any change in the value of VSS Token. Assumptions with respect to the foregoing involve, among other things, judgments about the future economic, competitive and market conditions and business decisions, most of which are beyond the control of the Vault team and therefore difficult or impossible to accurately predict.

Although the Vault team believes that its assumptions underlying its forward-looking statements are reasonable, any of these may prove to be inaccurate. As a result, the Vault team cannot offer any assurances that the forward-looking statements contained in this White Paper will prove to be accurate.
In light of the significant uncertainties inherent in the forward-looking statements contained herein, the inclusion of such information may not be interpreted as a warranty on the part of Vault or any other entity that the objectives and plans of the Vault project will be successfully achieved.

Please note that the Vault project and or VSS Token may be subject to other risks not foreseen by its team at this time.

8. APPENDIX

8.1 References

1. Type of cryptocurrency - https://coinmarketcap.com/all/views/all/, 15.Mar.2018

2. Number of crytocurrency wallet - https://blockchain.info/charts/my-wallet-n-users

3. Cryptocurrency market size and amount of daily transaction - https://coinmarketcap.com/charts/, 15.Mar.2018

4. Number of transactions in cryptocurrency - https://data.bitcoinity.org/bitcoin/tx_count/6m?r=month&t=l, 15.Mar.2018

5. Cryptocurrency damage statistics - https://news.bitcoin.com/9-million-day-lost-cryptocurrency-scams/, Jan 2018

6. Cryptocurrency exchange hacking cases - http://fortune.com/2018/01/26/bitcoin-price-coincheck-nem-mt-gox/

7. Type and comparison of cryptocurrency wallet - https://www.cryptocompare.com/wallets/#/overview

8. Damage due to technological errors in cryptocurrency - https://www.theregister.co.uk/2017/11/10/parity_280m_ethereum_wallet_lockdown_hack/

9. List of global financial fraud and scam - http://www.pymnts.com/global-fraud-index/

10. Global cryptocurrency benchmarking study - http://www.garrickhileman.com

11. Bitcoin: A Peer-to-Peer Electronic Cash System - https://bitcoin.org/en/bitcoin-paper

12. A Byzantine Fault Tolerance Algorithm for Blockchain http://docs.neo.org/en-us/node/whitepaper.html

13. Practical Byzantine Fault Tolerance and Proactive Recovery http://www.pmg.csail.mit.edu/papers/bft-tocs.pdf, https://www.microsoft.com/en-us/research/publication/practical-byzantine-fault-tolerance-proactive-recovery/

14. The Ripple Protocol Consensus Algorithm https://ripple.com/files/ripple_consensus_whitepaper.pdf

15. The XRP Ledger Consensus Process https://ripple.com/build/xrp-ledger-consensus-process/

16. The Stellar Consensus Protocol: A Federated Model for Internet-level https://www.stellar.org/papers/stellar-consensus-protocol.pdf, https://www.stellar.org/developers/guides/concepts/scp.html

17. Ethereum whitepaper https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf

18. Daily average difficulty of the Ethereum Network https://www.etherchain.org/charts/difficulty

19. Ethereum Token Contracts https://github.com/ConsenSys/Tokens

20. ERC20 Token Standard https://theethereum.wiki/w/index.php/ERC20_Token_Standard, https://github.com/ethereum/eips/issues/20

21. ERC223 – Proposed ERC20 Upgrade https://coincentral.com/erc223-proposed-erc20-upgrade

22. 9.1Million stolen daily from crypto currency end users https://news.bitcoin.com/9-million-day-lost-cryptocurrency-scams/