VAULT

Security You Can Trust

Vault Smart Security Token Knowns as VSS Token

Last Updated: 12 December.2018

Version: 7.0 - Korean

TheVault Ltd.
(Company Registration No. 201819091D)

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

볼트 프로젝트 및 VSS 토큰 세일 관련 정보는 볼트 재단의 공식 웹사이트 (https://www.theVault.Foundation)을 통해서만 제공됩니다. 기타 피싱 사이트, 유사 사이트에 주의하세요.

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

사용자의 결제수단은 현금 통화 결제에서 신용카드 결제, 모바일기기 결제등 현금이 없는 사회(Cashless Society)로 빠르게 이동하고 있습니다. 시장조사기관인 IDC 에 따르면, 전 세계 無현금결제(Cashless Payment) 건수는 2015 년에 4 천 3 백억 달러를 돌파했으며, 그 중 디지털 결제 대금은 2020 년까지 3 조 8000 억 달러를 넘을 것으로 예측됩니다.

시장의 많은 전문가들은, 디지털 결재 시장의 급격한 성장속에서 암호화폐가 주요 지불수단이 될 것으로 전망하고 있습니다. 현재, 암호화폐 거래의 신뢰성은 기존 금융권과 비교해 현저히 낮은 수준입니다. 이러한 이유로, 암호화폐는 제한적으로 사용되고 있습니다.

볼트는 커다란 성장 잠재력을 가진 암호화폐 시장에서, 기존 금융권보다 높은 수준의 보안 정책, 업그레이드된 보안 솔루션을 제시함으로서 암호화폐거래의 보안성, 안정성 문제에 대한 새로운 대안으로 자리잡을 것입니다. 볼트 프로젝트의 장점은 다음과 같습니다.

볼트의 주요 장점

1. 안전한 거래 (Secure, Error-Free Transactions)

세계 최초 블록체인 네트워크를 위한 인공지능기반 하이브리드 이상거래탐지 시스템(이하'AI-HFDS')을 도입시, 블랙리스트, 사기행위, 이상거래행위, 사용자 전송에러를 파악할 수 있습니다. 이를 통해, 거래소, 네트워크에 적용함으로써 암호화폐 트랜잭션의 안정성을 높입니다.

2. 빠른 속도 (Increased Speed)

볼트는 빠른 처리속도를 위해 검증된 지역별 마스터노드 운영사(암호화폐 거래소, 은행, 통신사, 정부기관 등) 를 지정하며, 신뢰관계가 형성된 거래간에 빠른 거래를 제공합니다. VSS 토큰은 이러한 하이브리드 네트워크 구성과 실시간 거래에 최적화 되도록 설계되었습니다.

3. 강화된 보안 (Smart Security)

볼트는 각종 암호화폐 사기 및 해킹에 대하여, 엔드유저 보안, 모바일 보안, 웹보안, AI-HFDS 의 보안 생태계를 통해 스마트하게 사용자 및 암호화폐 업계의 보안을 한 단계 강화합니다.

4. 위험성 감소 (Reduced Fraud and Risk)

볼트의 보안 플랫폼인 AI-HFDS 는 암호화폐 업계에 최적화된 레귤레이터 프로세스를 지원하며, 블랙리스트관리, 다차원적인 사용자 검증, 딥러닝기반 이상거래징후 모델링을 통해서 거래의 위험성을 낮추게 됩니다.

5. 보안 기반 네트워크 (Security Consensus Network)

볼트의 목표는 볼트의 보안 생태계를 통해 파트너들에게 모든 엔드 포인트 보안과 네트워크 노드간 정보 분석을 통해 보안을 향상하는 것입니다.

정부기관, 은행, 통신사, 기존 결제 게이트웨이, 신용카드 회사와 같은 기존의 금융관련 조직도 볼트의 Security Consensus Network 에 참여할 수 있습니다.
볼트의 Security Consensus Network 는 마스터 노드와 운영자에게 실시간 데이타 엑세스 및 익명성을 기반한 이상 거래를 탐지하여, 적절한 조치를 할 수 있는 수단을 제공합니다.

2. INTRODUCTION

2.1 Background

볼트는 암호화폐 업계에 보안 정책과 보안 솔루션을 제공한다는 공공의 이익을 목적으로 합니다. 볼트플랫폼은 암호화폐 거래에서 일어날 수 있는 사이버범죄행위나 암호화폐 서비스 제공사의 시스템에서 발생할 수 있는 취약점등의 잠재적인 위험으로부터 암호화폐 거래 사용자 및 서비스 제공사등 모든 당사자를 보호할 수 있습니다.

2018 년 10 월 현재, 암호화폐 시장은 비트코인을 중심으로 빠르게 성장하고 있습니다. 주요 암호화폐 거래소에 등록된 암호화폐의 종류는 약 2070 여개, 암호화폐 지갑 사용자 수는 2 천 3 백만명으로 전년대비 약 100%의 성장을 했습니다.

암호화폐 시장규모는 총 약 440 조원(한화)으로 일일 평균 거래액은 약 17.5 조원(한화)이며, 최근 6 개월간 월평균 거래건수는 약 8 백 5 십만 건에 달하고 있습니다. 하지만, 이러한 기록적인 성장에도 불구하고, 다양한 종류의 잠재적인 위협요소 및 보안상의 문제점을 가지고 있습니다.

첫째, 암호화폐 지갑관리의 문제점

대다수의 개인 암호화폐 사용자(이하 '사용자')는 암호화폐 지갑을 직접 관리함에 따라 다양한 위협요소에 노출되어 있습니다.

특히, 암호화폐지갑 관리의 허점을 노린 피싱공격, 신용사기(Scam, Fraud)등의 다양한 형태의 전문적인 공격을 받고 있으며, 사용자가 이를 방지하기 위한 보안정책을 수립하고 스스로 관리를 하는 것은 현실적으로 어렵습니다.

예를 들어, 사용자 A 가 1 비트코인을 자신의 비트코인 지갑에서 사용자 B 의 비트코인 지갑(Destination Address)으로 전달을 위해 수령인의 비트코인 지갑의 주소를 혼동하거나 또는 잘못된 주소형식등의 이유로 잘 못 입력한 경우, 사용자 A 의 1 비트코인은 증발하여 회수할 수 없습니다.

사용자가 암호화폐 거래소를 통하지 않고, 직접 비트코인 지갑을 생성하여 관리하는 경우, 지갑의 개인 비밀번호(Private Key)를 분실하면 복구할 방법이 없으며, 모든 코인을 잃어버리게 됩니다.

사용자가 개인(또는 공용) PC 를 통해 자신의 비트코인 지갑에 로그인하는 경우, PC 에 미리 설치되어 있는 해커의 피싱프로그램을 통해, 사용자의 정보 (암호화폐지갑 주소, Private Key)가 유출될 경우, 해커는 사용자의 모든 비트코인을 해커의 비트코인 지갑으로 이동할 수 있습니다.

둘째, 암호화폐 거래소의 보안상 취약점

다수의 암호화폐 거래소(이하 '거래소')는 각국의 거래소 관련 법규의 미비로 인해, 비교적 자율적으로 운영되며, 거래소 자체적으로 보안 정책을 수립해 적용하고 있습니다.
하지만, 거래소가 보안상 취약점으로 해킹을 당할 경우 사용자의 직접적인 피해로 연결될 수 있습니다.

예를 들어, 거래소가 해킹을 통해 서버에 저장된 사용자 정보를 유출한 경우, 해커가 유출된 사용자 정보를 이용해 사용자의 암호화폐를 해커의 암호화폐지갑으로 전달할 수 있으며, 이 경우 사용자의 암호화폐가 손실됩니다.

거래소 내부의 허술한 보안관리로 인해, 거래소 내부 인력이 거래소 고객 정보를 유출하거나 고객의 암호화폐를 자신의 지갑으로 전달할 경우, 사용자의 암호화폐가 손실됩니다.

지난 2014 년, 세계 최대규모 거래소인 마운트곡스가 850,000 비트코인 (당시기준 약 4 억 7000 만달러)을 해킹당해 파산했고, 2018 년 1 월 일본의 거래소인 코인체크가 5 억 NEM 코인 (약 5 억 2 천 4 백만달러)을 해킹 당했습니다.

해킹의 원인은 아직도 명확하게 파악되지 않고 있으며, 큰 범주에서 허술한 보안관리를 원인으로 추측하고 있습니다.

영국 캠브리지대학의 주요 거래소 운영자를 대상으로 한 설문조사 자료에 따르면, 거래소 스스로도 IT 보안, 해킹에 따른 위험성이 가장 크며, 그 다음으로 은행권과의 관계악화, 금융거래 사기순으로 운영상 위험요소가 크다고 평가하고 있습니다.

특히, 중소규모의 거래소가 IT 보안, 해킹, 금융거래 사기에 높은 위험에 노출되어 있다고 볼 수 있습니다.

거래소 운영 위험 요소 평가표 (2017, 캠브리지 대학교)

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

셋째, 암호화폐 연관 기술의 취약점

암호화폐의 기술적인 취약점으로 사용자가 피해를 입을 경우, 사용자가 이에 따른 손실을 증명하거나, 그 피해에 상응하는 배상을 청구하기는 현실적으로 어렵습니다.
다수의 암호화폐 관련 기술은 비영리 공개 라이센스이며, 공개 기술을 사용함에 따른 피해는 고스란히 사용자가 부담하게 됩니다.

대표적인 사례로, 암호화폐 지갑 소프트웨어 관련 문제점이 있습니다.
암호화폐 지갑은 크게 하드웨어 지갑(Cold Wallet)과 소프트웨어 지갑(데스크탑용, 모바일용, 웹용) 으로 구분하며, 현재, 약 135 개의 다양한 소프트웨어 지갑이 있습니다.

대부분의 암호화폐 지갑 프로젝트는 기술적인 관점에서 많은 잠재적인 취약점을 가지고 있습니다. 사용자가 '개발 진행중'인 암호화폐 지갑 소프트웨어 사용할 경우, 소프트웨어적인 오류(Bug)로 인해 지갑에 보유하고 있는 암호화폐가 동결되거나 손실될 수 있습니다.

실제로, 2017 년 Parity technology 사의 다중서명 지갑(Multisig Wallet) 사용자는 다중서명(Multi Signature)기능의 취약점으로 인해, 약 2 억 8 천만 달러(한화 약 3200 억)의 가치의 지갑에 저장되 있던 이더리움이 동결되는 피해를 입었습니다.

위와 같이, 암호화폐거래시 발생할 수 있는 다양한 잠재적인 문제점을 극복하고, 암호화폐가 기존 화폐(Fiat Currency)를 대체할 수 있는 새로운 통화로써 역할을 하기 위해서는 거래의 신뢰성을 보장할 수 있는 솔루션이 필요한 게 현실입니다.

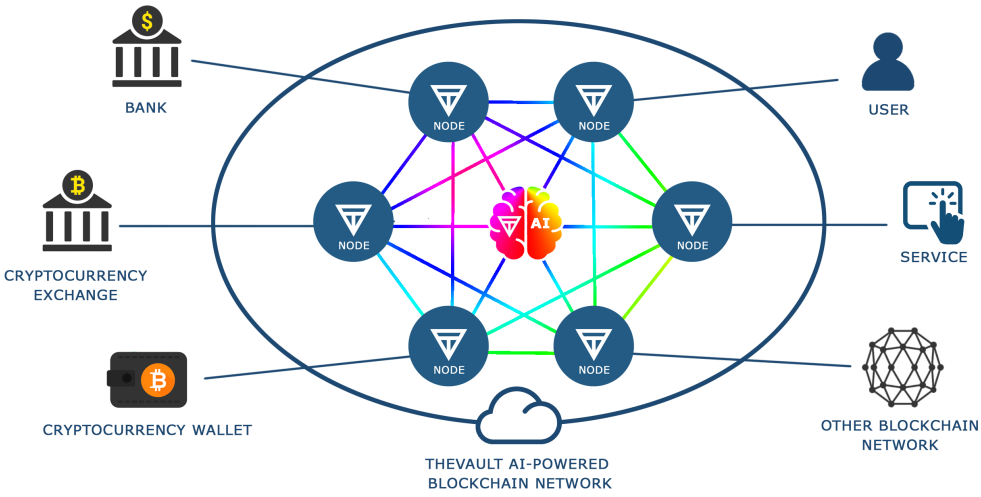
2.2 Concept

볼트는 암호화폐 업계의 문제점들을 해결하기 위해서 암호화폐 사용자(이하 '사용자'), 암호화폐 거래소(이하 '거래소') 및 암호화폐 관련 서비스 제공자를 위한 다차원적인 보안 플래폼을 제안합니다.

볼트 플랫폼은 the Vault Security Consensus Network, Vault AI-powered Hybrid Fraud Detection System and the Vault Consumer Layer 으로 구성되며, 이는 '보안 플랫폼 생태계' (이하 '보안 생태계')를 구성합니다.

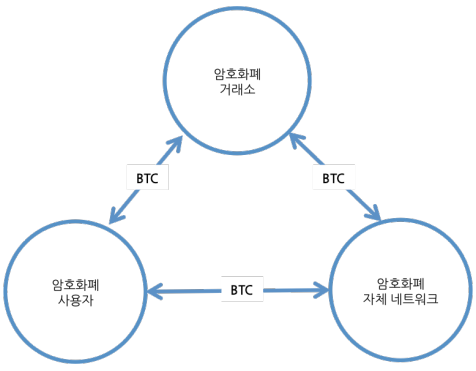
볼트의 솔루션은 볼트의 DNA 인 암호화폐 사용자와 업계간의 '신뢰의 다리'를 만들겠다 라는 철학을 기반으로 합니다.

TheVault 플랫폼 에코시스템



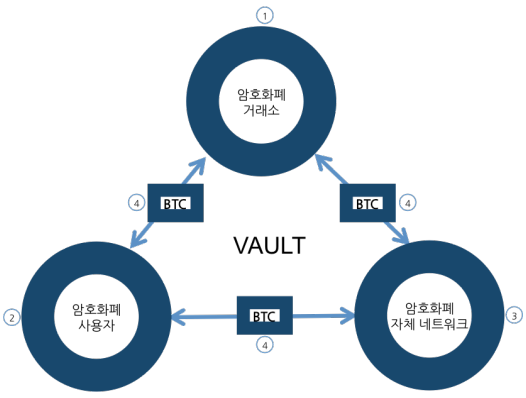
볼트의 보안 솔루션은 기존 금융권에서 입증된 보안 솔루션을 기반으로 하여 블록체인환경에 맞도록 재설계되었습니다.기존 암호화폐 트랜잭션은 볼트의 솔루션을 각각 사용자, 거래소, 기존 암호화폐 네트워크에 추가함으로서, 각 개체간 보안성이 강화된 트랜잭션이 가능합니다.

기존의 암호화폐 트랜잭션



볼트 솔루션 적용 후

볼트의 보안이 적용된 트랜잭션



볼트의 보안성 강화 트랜잭션에 대한 설명은 아래와 같습니다.
① 암호화폐 거래소는 볼트의 서버 솔루션인 'AI-HFDS'를 적용하여, 사용자간, 거래소간 트랜잭션에 대한 해킹, 이상거래의 위험으로부터 보호될 수 있습니다.

② 암호화폐 사용자는 접속환경에 따라 PC(또는 모바일, 웹)용 사용자 솔루션을 사용합니다. 사용자는 이를 통해 각종 해킹시도, 피싱공격, 개인정보유출, 이상거래의 위험으로부터 보호할 수 있습니다.

③ 비트코인, 이더리움등과 같은 암호화폐 네트워크는 볼트의 보안 솔루션이 적용된 보안 네트워크와 연결되어 사용자 거래 트랜잭션을 보호하게 됩니다. 볼트 재단은 기존 암호화폐 네트워크와 연결되는 인터페이스를 제공하며, 기존의 암호화폐 네트워크는 이를 쉽게 플러그인하여 네트워크 사용자들에게 신뢰성 높은 기술을 제공할 수 있습니다.

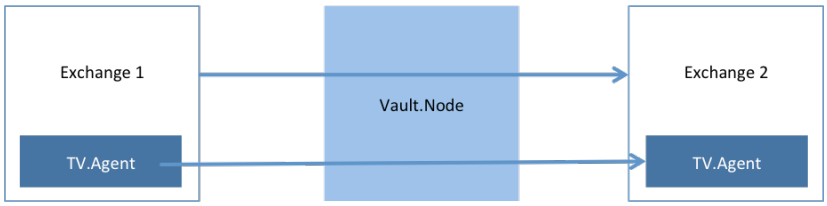
④ 거래에 사용되는 기존의 암호화폐는 볼트의 솔루션, 볼트 네트워크를 통해 신뢰성이 높은 트랜잭션을 보장받을 수 있습니다.

첫째, 암호화폐 거래소의 보안

볼트는 암호화폐 거래소(이하 '거래소')를 위한 보안 솔루션을 제안합니다.
볼트의 에이전트는 거래소를 위한 솔루션으로, 볼트 에이전트를 통해 볼트 보안 네트워크에 참여하여 거래소 사용자에게 신뢰성 있는 트랜잭션 서비스를 제공할 수 있습니다.

그림과 같이, 볼트 에이전트는 각 거래소의 시스템에 플러그인(Plug-in)되어, 거래소간의 거래시 내부 데이타베이스의 공유없이 볼트의 보안 네트워크내에서 신뢰성 있는 통신을 할 수 있도록 설계됩니다.

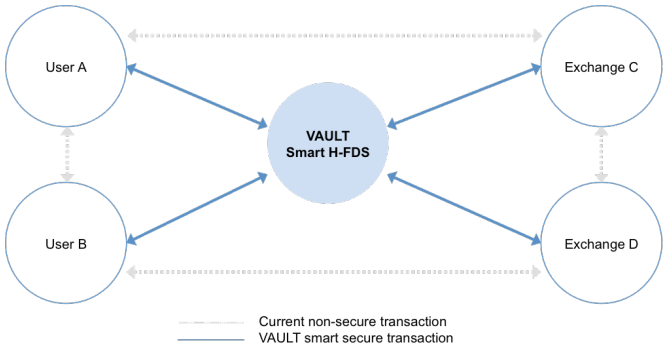
거래소간 트랜잭션 플로우



볼트 보안 에이전트는 암호화폐 지갑 주소의 무결성확인, 상대방 지갑 주소의 존재 유무 상호검증, 주소의 활성화 유무확인, 블랙리스트 등록여부확인, 거래 대상 신뢰도 측정을 위한 스마트 투표(Smart-Voting) 기능을 지원합니다.

다음 그림과 같이, 볼트의 보안 에이전트는 개인간, 거래소간 거래에 있어서 트랜잭션을 중계하는 역할을 합니다.

사용자 및 거래소 트랜잭션 플로우



1) 사용자가 자신의 거래소 A 에서 거래소 B 에 속한 지갑주소로 1 비트코인을 보낼 경우 거래소 A 는 사용자 접속시 볼트의 엔드유저 보안 솔루션의 설치 유무를 확인하고, 설치가 되 있는 경우 엔드 유저 보안솔루션이 실행됩니다. 이후, 모든 사용자와 거래소간의 트랜잭션은 볼트의 보안 솔루션을 통해 보호가 됩니다.

사용자가 전송할 비트코인지갑의 주소를 입력하고 전송할 때, 거래소 A 의 볼트 에이전트는 상대편 거래소 B 의 볼트 에이전트와 연결되어, 목적지 지갑주소의 유효성 및 존재여부, 블랙리스트 등록여부, 전자지갑 주소의 신뢰도등 거래의 신뢰성을 높일수 있는 기능을 수행합니다.

거래소 B 의 볼트 에이전트는 거래소 A 의 볼트 에이전트로 받는 사용자관련 질문들에 대해 내부의 데이타베이스를 리뷰하여 응답하게 됩니다.

거래소 B 의 전송받을 지갑주소의 유효성이 맞지 않거나, 지갑이 존재하지 않는 경우 거래소 B 의 볼트 에이전트는 거래소 A 볼트 에이전트에게 해당 메세지를 전송하고, 거래소 A 는 사용자의 비트코인 전송을 중지합니다.

거래소 A 는 사용자에게 주소가 존재하지 않음을 통지하고, 사용자는 전송받을 지갑주소를 다시 확인하는 절차를 거칩니다. 사용자는 이와 같은 과정을 통해 관리 부주의로 인한 암호화폐 분실을 방지합니다.

- 거래소 A 가 볼트 에이전트를 통해 거래소 B 의 주소가 블랙리스트에 등록된 것으로 확인되면, 거래소 B 는 해당 메세지를 거래소 A 에 공유합니다. 거래소 A 는 사용자에게 블랙리스트에 등록된 계좌임을 알리고, 사용자에게 다시한번 전송할지 묻게됩니다.

- 볼트 에이전트는 전자지갑에 대한 신뢰도를 평가하고, 그에 따른 레벨을 통해 사용자를 잠재적인 위험으로부터 보호합니다.

신뢰도가 현저히 낮은 경우, 거래소는 사용자에게 관련 잠재적인 위험요소가 있음을 알리고, 사용자가 해당 지갑주소로 암호화폐 전달시, 이메일 인증, 전화 인증등 추가 인증작업을 거치게 됩니다.

둘째, 암호화폐 사용자 보안 (Vault Consumer Protection)

볼트소비자 보호 계층 Vault Consumer Protection 계층은 다른 볼트플랫폼 구성 요소와 통합되며 디지털 결제 암호화 사용자를 위한 강력한 보안 솔루션을 제공하는 최종 사용자 보안 솔루션입니다.

사용자가 다양한 접속 환경(PC, 모바일기기, 웹)에서 암호화폐를 거래할 경우, 볼트는 각각의 환경에 최적화된 보안 기능을 제공해 각종 해킹, 피싱, 파밍등의 위협으로부터 사용자를 안전하게 보호합니다. 다음과 같은 사례에 적용할 수 있습니다.

1) 사용자의 PC 기기 사용시

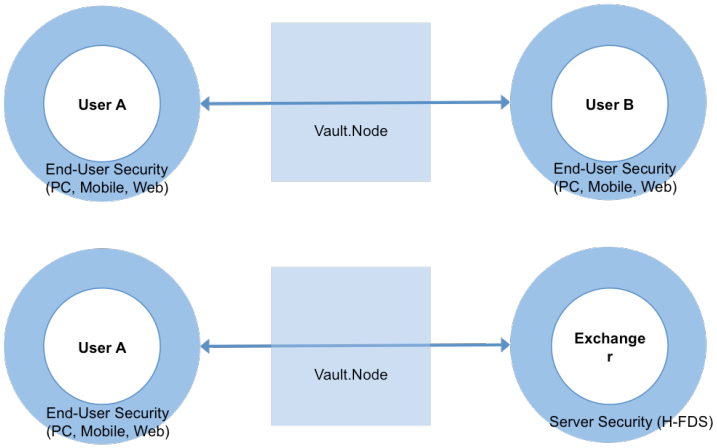
암호화폐 사용자가 PC 에 PC 용 암호화폐 지갑을 사용할 경우, 사용자는 볼트 엔드유저 보안 솔루션을 PC 에 설치합니다. 엔드유저 보안솔루션은 '안티바이러스 엔진'을 사용하여, 사용자의 PC 를 각종 바이러스로부터 보호하고, 악성코드, 스파이웨어, 랜섬웨어를 비롯한 각종 사이버위협을 차단합니다.

2) 사용자의 모바일기기 사용시

암호화폐 사용자가 휴대폰에 암호화폐 지갑 모바일 앱을 사용할 경우, 암호화폐 지갑 앱 개발사가 사용자 보호를 위해 볼트 모바일 보안 모듈을 프로그램내에 플러그인(Plug-in) 합니다.
사용자가 모바일앱을 통해 서비스 사용시, 앱에 플러그인된 볼트 보안 솔루션은 사용자 모바일의 비정상 실행 환경 탐지, 실행파일 암호화, 앱 무결성 검증, 앱 위조 변조 및 결제 우회 탐지, 해킹툴 차단등의 기능을 통해 사용자를 보호합니다.

아래의 그림과 같이 사용자는 볼트의 보안계층으로 보호되어, 사용자간, 사용자 및 거래소간 거래에 있어서 보안이 한단계 업그레이드된 신뢰성 있는 거래를 할 수가 있습니다.

엔드유저 보안방식



셋째, 금융사기로부터의 사용자 보호

볼트는 암호화폐 사용자 및 암호화폐 서비스 사업자를 위한 보안 솔루션을 제안합니다. 암호화폐 서비스 사업자 (암호화폐 지갑, 암호화폐 거래소 등)는 볼트의 AI-HFDS 를 시스템내에 도입하여, 다양한 형태의 사용자 트랜잭션상 문제점들에 대한 적절한 액션을 설정하여 대처할 수 있습니다. 인공지능기반 하이브리드 이상거래탐지 시스템(이하 'AI-HFDS')은 딥러닝 인공지능(AI) 기반 이상거래 탐지시스템을 기반으로 합니다.

볼트의 딥러닝(Deep Learning)은 최소 6 개월~1 년간 볼트 하이브리드 네트워크내의 암호화폐 사용자 및 거래소의 각종 거래 패턴을 수집합니다. 이 수집된 데이타는 인간 두뇌의 연결성 모방한 것과 같이 데이터 세트를 분류해 데이터간 상관관계를 찾는 심층신경망(Deep Neural Network)을 구성합니다. 이에 대한 다양한 예시는 아래와 같습니다.

1) 위치 정보 이용 사례

사용자가 싱가폴의 한 음식점에서 암호화폐 결제를 한 후 30 분 후, 런던의 음식점에서 결제가 된다면, 지역간 거리에 따른 이동시간보다 빠르게 타 지역에서 결제가 된 경우입니다.

암호화폐결제 서비스를 제공하는 업체는 볼트의 보안 네트워크상 해당 국가의 볼트 네트워크의 마스터 노드(Master Node) 운영사를 통해 출입국관리소의 시스템에 출국 여부를 확인하게 됩니다 (국가별로 출입국 확인 서비스 가능여부가 다름).

출국이 확인 안 될 경우 사용자에게 확인 연락을 통해 거래의 진위를 직접 확인하고, 해당 사용자 암호화폐 트랜잭션 서비스를 임시중지합니다.

2) 사용자 정보와 거래 이력 정보 이용 사례

사용자가 일 평균 10 만원 미만을 거래하다, 쇼핑센터에서 100 만원 이상 결제시, 평소의 결제 패턴과 상이한 거래로 판단이 된다면, 볼트의 AI-HFDS 는 승인을 거절 또는 본인확인을 위한 프로세스를 진행합니다.

3) 사용자 환경 정보 이용 사례

사용자는 볼트 AI-HFDS 가 적용된 암호화폐 서비스에서, 접속한 환경 (PC 및 모바일기기, 운영체제, 웹 브라우저, IP 주소) 의 분석을 통해 동시 접속 사용자 여부, 기타 사용자 환경 변경을 감지하여 이상이 확인된 경우, 사용자 재인증을 진행하거나 본인 확인 단계를 진행합니다.

2.3 Who We Are

볼트의 공동 설립자와 고위 경영진은 아시아 핀테크, 마케팅, 사이버 보안 분야의 경험있는 전문가로 구성되어 있습니다.

1) Dannie Francis: Cofounder : linkedin.com/in/danniefrancis

2) Marco Baik il Kyoung: Cofounder : linkedin.com/in/marcobaik

모든 매니지먼트팀 및 어드바이서는 볼트 공식 웹사이트 (http://www.thevault.foundation)에서 확인할 수 있습니다.

2.4 Operation Structure

볼트는 비영리 재단입니다. 그리고, 글로벌 금융 및 보안 전문가들로 구성된 재단 산하에 영리법인을 설립하여 소프트웨어 개발, 네트워크 운영을 진행합니다.

볼트는 비영리 법인으로 그 재원으로 운영되는 보증에 의해 제한된 공공 기업입니다. 이후 볼트가 소유하고 있는 글로벌 금융 및 보안 전문가로 구성된 이익창출회사를 설립하여 소프트웨어 개발과 네트워크 운영을 할 계획입니다.

각 운영주체에 대한 설명은 아래와 같습니다.

1) 볼트 비영리 법인: 볼트(TheVault Ltd, 이하 '볼트')는 싱가폴에 설립된 비영리법인으로, VSS 토큰을 발행하고 유지하는 역할을 합니다.

2) 볼트 영리 법인: 볼트 영리법인(TheVault Lab Pte Ltd)은 싱가폴에 설립되었으며, 볼트 솔루션의 개발, 볼트 네트워크 관리, 볼트의 솔루션의 사용자 배포, 소프트웨어 업데이트 등 볼트 생태계의 유지, 관리를 담당합니다.

3. AI-HFDS SOLUTION

3.1 Server-side Security 'AI-HFDS'

볼트의 인공지능기반 하이브리드 이상거래탐지 시스템(AI-HFDS, Artificial Inteligence-Hybrid Fraud Detection System)은 '인공지능 엔진'을 기반으로 합니다. AI-HFDS 는 사용자 및 거래소를 위한 가상화폐 거래 피해 예방을 위한 솔루션으로 가상화폐 거래시 단말기 정보, 접속정보, 거래정보등을 수집, 분석하여 의심되는 이상거래를 탐지하고 차단하는 시스템 입니다.

기존 금융권에서는 이용자의 PC 에 백신, 방화벽, 키보드 보안 프로그램 등의 설치를 의무화하는 등 이용자 측면에서만의 보호를 강조 했었다면, 볼트의 이상거래탐지 시스템(AI-HFDS)은 암호화폐 거래서비스를 제공하는 개인, 회사에서 다양한 정보를 수집하고 분석하여 이상거래를 탐지하고 차단하여 기존보다 더 적극적으로 트랜잭션을 보호할 수 있습니다.

현재, 암호화폐 업계이 보안규정이 부족하며, 그나마 이를 제시하는 CCSS 협회(Crypto Currency Security Standard)는 지갑 및 교환 공급 업체에 대한 보안 지침을 제공하지만, 반드시 구현하고 감사해야 하는 필수 기능이 아닙니다.

AI-HFDS 는 보안을 보다 스마트하고 안전하게 만들기 위해 이러한 지침에 정책을 추가합니다. 기존의 은행 시스템에서도 마찬가지로, 많은 전통적인 은행들이 사용자 측 보안에 대한 필요성을 강조하거나 추가적인 하드웨어 솔루션과 다단계 및 다중 인증 절차를 제공하는 하고 있지만, 해커들은 여전히 취약점을 발견해 공격하고 있습니다.

AI-HFDS 를 블록체인기반 네트워크로 구성함에 있어 장점은 아래와 같습니다.

첫째, 보안성 강화

볼트의 블록체인 네트워크는 사용자 정보수집에 필요한 데이타의 위조, 변조를 방지하여 기초 데이타의 신뢰성이 높아집니다.

둘째, 호환성 향상

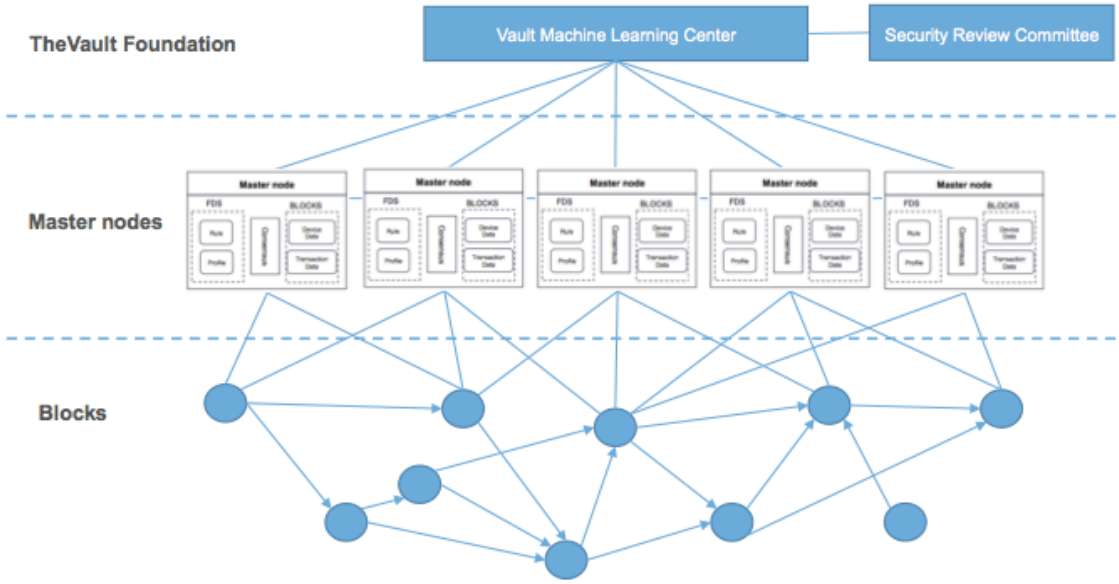
탈중앙화가 가능한 퍼블릭 플랫폼이기 때문에 미리 검증된 시스템을 일반 사용자, 암호화폐 사업자에게 제공할 수 있습니다.

셋째, 비용 및 자원의 절감효과

개별 사업자가 각각 구축, 운영하는 종속적인 시스템은 각각 검증을 해야하며, 중앙집중식 시스템 구축을 하기 때문에, 많은 비용과 자원이 필요합니다. 볼트의 블록체인 네트워크는

최소한의 리소스를 중앙에서 관리하고, 대부분의 데이타를 분산처리하기 때문에 저비용, 고효율 처리가 가능합니다.

Vault 블록체인 네트워크 다이어그램



볼트 네트워크 주요 구성요소에 대한 설명은 아래와 같습니다.

1) 볼트 러닝머신센터(Vault Machine Learning Center)

The Vault Foundation 에서 운영하는 이상 거래 탐지를 위한 머신 러닝 센터로 딥 러닝으로 거래 로그를 트레이닝 하여 이상 거래 탐지 패턴 생성합니다.

2) 보안정책심의회(Security Review Committee)

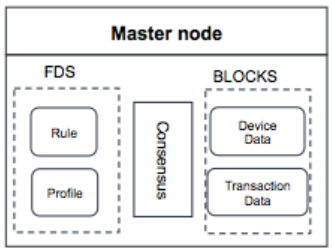
Security Review Committee 는 보안정책을 수립 및 관리하고, 블랙리스트(Black List) 및 그레이 리스트(Grey List) 단말 및 월렛 주소를 기반으로 이상 거래 탐지 패턴 정책 심의하게 됩니다.

3) 마스터노드(MasterNode)

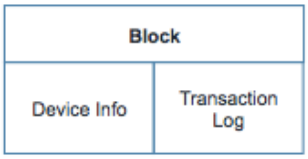
마스터노드는 이상거래 탐지 RULE 및 컨센서스로 구성되며, 컨센서스는 VCP(Vault Consensus Protocol)을 사용합니다. 볼트의 메인넷은 마스터노드 형태로 구성되며, 마스터노드에서 이상 거래 여부를 탐지합니다. 각 블록체인의 블록은 단말 정보 거래 로그 정보 저장소로 활용됩니다.

4) Blocks 단말 정보 및 거래 로그를 저장하게 됩니다.

Master Node 구조



Block 정보



이상거래 탐지방법으로는 사용자의 거래 이용환경, 거래패턴, 거래사전행위에 의해 종합적으로 결정이 되며, 각각의 거래 허용범위에 따라 이상거래 여부를 판별하고 있습니다.

이상거래탐지패턴은 Rule 과 Score 로 구성되며, 전자금융거래에 적용되어 각종 사용자 디바이스 수집정보와 거래정보를 기반으로 한 패턴에 대해 대용량엔진으로 통합 분석 후 이상징후에 대한 차단 대상 정보를 업무서버로 응답처리 합니다.

분석의 정확성을 높이기 위해서는 최소 6 개월에서 1 년간의 데이타를 축적하는 선결과정이 필요합니다. 딥러닝을 위해 기본적으로 수집되는 정보는 아래 표와 같습니다.

접속 단말기 로그정보 수집 항목

거래정보	PC	모바일 기기
사용자식별 ID	접속자 컴퓨터 로컬 IP	UUID
거래시간	Proxy IP	UUID2
송금 지갑주소	VPN IP	모바일 OS 버전
입금 계좌주소	IP 국가대역	기기 제조사
거래소 코드	MAC Address	모델명
금액	HDD Serial Number	음성통화상태
채널식별코드	CPU ID	데이터통신상태
서비스식별코드	OS 정보	단말기 ID
	브라우저 정보	단말기 전화번호
	USB Serial	네트워크 망사업자 코드
		SIM Card 국가코드
		SIM Card 일련번호
		가입자 ID
		단말 MAC Address 정보
		루팅 or 탈옥여부

3.2 User-side Security - PC

볼트의 엔드유저 솔루션은 '안티바이러스 엔진'을 기반으로 하며, 악성코드, 스파이웨어, 랜섬웨어를 비롯한 각종 사이버위협을 차단하여 암호화폐 사용자의 컴퓨터를 안전하게 보호합니다.
암호화폐 사용자는 볼트의 엔드유저 사용자 보안 프로그램을 PC 또는 모바일기기에 설치하여, 실시간 감시와 보호기능을 통해 암호화폐 사용자 시스템과 중요 정보를 안전하게 보호합니다.

암호화폐 거래소 또는 암호화폐 관련 소프트웨어 개발사는 엔드유저 사용자에게 볼트의 엔드유저 보안 프로그램 설치를 통해, 엔드유저의 디바이스에서 발생할 수 있는 잠재적인 해킹, 피싱에 대한 위험으로 부터 사용자를 보호할 수 있습니다.

볼트의 엔드유저 사용자 보안모듈은 타 서비스, 사이트에 플러그인 할 수 있도록 설계되어, 기존 암호화폐 업계에 쉽고, 빠르게 적용할 수 있습니다.

3.2 User-side Security - Mobile

볼트의 모바일 보안 솔루션은, 암호화폐 지갑등을 개발하는 모바일 앱 개발사가 프로그램내에 볼트의 보안 모듈을 플러그인 하여 보안 기능을 빠르고 쉽게 적용할 수 있도록 설계되었습니다.
개발사는 볼트의 모바일 보안 에이전트를 통해 실행파일을 암호화하고 해킹을 방지하여, 사용자에게 각종 해킹으로부터 안전한 서비스를 제공할 수 있습니다.

3.2 User-side Security - Web

볼트의 온라인 및 웹 보안 솔루션은 암호화폐 사이트를 사용하는 사용자 PC 의 정보유출, 키보드 해킹 및 각종 암호화폐사고를 방지하는 통합 온라인 보안 솔루션입니다. 다양한 운영체제 및 웹브라우저를 지원하며, HTML, Java Script 를 통해 간편하게 설치됩니다. 다양한 PC 보안 기능과 정기적인 패턴 업데이트로 안전한 PC 환경을 구현합니다.

4. VSS TOKEN

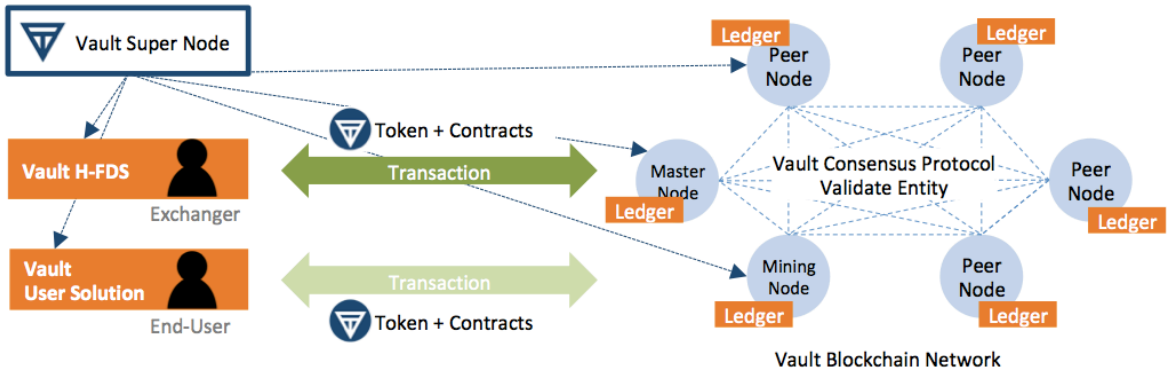
4.1 Value of the VSS Token

VSS 토큰은 볼트 비영리 법인에서 발행을 하고, 볼트 생태계내에서 다양한 방법으로 통해 VSS 토큰을 획득하고 사용할 수 있습니다. 빠른 이해를 위해, 인간의 신체와 비교할 수 있습니다. 예를 들어, VSS 토큰은 볼트 생태계 내에서, 영양소를 전달하는 피와 같은 역할을 합니다. 볼트 보안 네트워크는 이 피를 옮길 수 있는 혈관이며, 볼트 솔루션은 심장, 간과 같은 역할을 합니다.

볼트의 합의 방식은 탈 중앙화된 볼트 컨센서스 프로토콜(Vault Consensus Protocol, VCP) 입니다.
VCP 의 컨셉은 검증된 허가 받은 사업자들로 구성된 네트워크를 통해 합의가 이뤄지는 방식이며, 프랙티컬 비잔틴 장애 허용 (Practical Byzantine Fault Tolerance) 알고리즘을 개선한 모델로 설계되어 기존 블록체인 합의 방식인 PoW, PoS 의 단점인 불확실성과 성능문제를 개선하고, 네트워크에 대한 악의적인 공격(Malicious Attack)을 막을 수 있습니다.

이는, 신뢰성 높은 노드들이 블록체인에 합의하여 알고리즘에 참여하는 방식으로, 분권형의 보안성이 높은 거래시스템입니다.

볼트 보안 네트워크



볼트 보안 네트워크내에서 각각의 개체들은 다음과 같은 역할을 합니다.
1) 볼트의 솔루션은 사용자 보안(User End Security) 솔루션과 암호화폐 거래소 및 암호화폐 네트워크를 위한 서비스 제공자(Server Security)솔루션으로 구성됩니다.
사용자 보안 솔루션은 PC, Mobile, Web 등 다양한 접속환경으로부터 사용자 보안 및 보안에 필요한 정보를 수집하는 역할을 합니다.

2) 볼트 보안 네트워크내에서 암호화폐 사용자와 거래소는 새로운 블록을 생성하여, 볼트 네트워크 내에서 보안 트랜잭션에 대한 요청을 합니다. 신뢰성 서비스 사용에 대한 댓가로 VSS 토큰을 사용하여야 합니다.

3) 볼트 보안 네트워크내에서의 각 노드들은 AI-HFDS(Hybrid-Fraud Detection System)을 위한 데이타 처리의 역할을 담당합니다. 볼트 수퍼 노드는 각각의 노드들과 통신을 하며, 각 노드의 역할에 대한 인증과 검증작업을 수행하고, 네트워크의 효율적인 운영을 위한 컨트롤타워 역할을 합니다.

4.2 VSS Token Acquisition

볼트 사용자는 자신의 PC, 모바일기기, 웹에서 볼트의 보안 서비스를 이용시 VSS 토큰이 필요합니다. 사용자의 VSS 토큰은 볼트의 네트워크를 유지하기 위해 사용됩니다.
암호화폐 사용자 및 암호화폐 관련 사업자는 VSS 토큰의 획득을 위해서는 VSS 토큰 지갑을 먼저 생성하여야 하며, 아래와 같은 방법으로 볼트 지갑을 생성할 수 있습니다.

사용자가 VSS 토큰을 획득을 위해서는 볼트 지갑을 만들어야 합니다. 볼트 지갑을 만드는 방법은 아래와 같습니다.

1. 보안 사용자 프로그램을 설치한 지갑생성

볼트의 사용자 보안 프로그램 설치 후, 사용자는 볼트 계좌를 생성할 수 있으며, 이 계좌와 연결된 VSS 토큰 지갑을 만들수 있습니다.

2. 볼트 웹사이트 계좌를 통한 지갑생성

볼트 웹사이트에 회원가입 후 볼트 지갑을 생성 할 수 있습니다. 향후 볼트 웹사이트에서 제공하는 암호화폐 거래소를 통해 볼트와 기존 암호화폐의 교환을 할 수 있습니다.

3. 암호화폐 거래소를 통한 지갑생성

VSS 토큰이 상장된 암호화폐 거래소를 통해 VSS 토큰 지갑을 생성할 수 있습니다. 암호화폐 거래소에 계정을 만든 후, VSS 토큰 지갑을 생성할 수 있습니다.

계좌 생성 후 VSS 토큰의 획득 방법은 아래와 같습니다.

첫째, 암호화폐 사용자의 토큰 획득 방법

1) 기존 암호화폐를 이용한 교환

사용자는 볼트에서 제공하는 암호화폐 거래소 또는 VSS 토큰을 거래하는 외부 암호화폐 거래소 및 VSS 토큰을 보유하고 있는 개인간의 교환을 통해 기존의 가상화폐(Bitcoin, Ethereum, Litecoin 등)를 사용하여, VSS 토큰(VSS)으로 교환할 수 있습니다.

2) 볼트 보안연구에 참여

볼트는 공공의 이익을 위해, 보안관련 연구 프로젝트를 수행합니다. 소프트웨어 개발, 보안 모델 개발등 다양한 주제를 가지고 진행하는 이 프로젝트에 재능기부를 하여 VSS 토큰을 획득할 수 있습니다.

3) 볼트의 리서치, 공익광고 및 설문조사에 참여

볼트는 암호화폐 업계의 보안성 향상을 위해 사용자 및 사업자를 대상으로 한 리서치를 진행하고, 공익을 위한 광고의 전파 및 사용성 향상을 위한 설문조사를 진행합니다. 사용자는 이러한 볼트의 활동에 참여함으로서 VSS 토큰을 획득할 수 있습니다.

4) 볼트 베타 네트워크 참여

볼트는 사용자의 보안 네트워크 베타버전의 참여를 활성화하기 위해, 일정수량의 VSS 토큰을 사용자에게 배포합니다. 초기 네트워크의 안정화를 위해 볼트 솔루션을 설치하고, AI-HFDS 의 정확도를 높이기 위해 사용자 정보를 제공함으로서 VSS 토큰을 획득할 수 있습니다.

둘째, 암호화폐 사업자 (거래소, 채굴등 암호화폐 관련 사업자) 의 토큰 획득 방법

1) 기존 암호화폐를 이용해 교환

암호화폐 사업자는 사용자를 위한 보안 서비스의 원활한 제공을 위해, 충분한 VSS 토큰을 확보해야 하며, 볼트는 암호화폐 사업자에게 안정적인 서비스를 제공할 수 있도록 다양한 컨설팅을 제공합니다. 또한, 사업자는 가상화폐 거래소를 통해 기존의 가상화폐를 사용하여, VSS 토큰 (VSS)으로 교환할 수 있습니다.

2) VSS 토큰 마스터노드 운영을 통한 토큰 획득

볼트는 안정적인 서비스를 위해, 국가별, 지역별로 검증된 마스터 노드를 지정합니다. 이러한 마스터노드들은 사용자정보관리, AI-HFDS 처리에 중심적인 역할을 하게 됩니다. 마스터 노드의 역할을 함으로써 사용자가 네트워크에 지급하는 VSS 토큰 중 일정량을 네트워크에 기여한 보상으로 획득하게 됩니다.

3) VSS 토큰의 마이닝을 통한 토큰 획득

VSS 토큰의 마이닝을 하는 사업자는 볼트 네트워크내의 인공지능기반 AI-HFDS 의 분산 프로세싱의 일부분을 담당함으로써 사용자가 사용하는 VSS 토큰의 일부분을 그 보상으로 획득할 수 있습니다.

4.3 Token Use

암호화폐 사용자, 암호화폐 거래소, 기타 암호화폐 사업자가 VSS 토큰을 사용하여, 볼트의 사용자용, 서버용 솔루션을 사용할 수 있고, 거래에 있어서 신뢰성이 높은 서비스를 사용할 수 있습니다. VSS 토큰 사용 시나리오는 아래와 같습니다.

첫째, 암호화폐 사용자

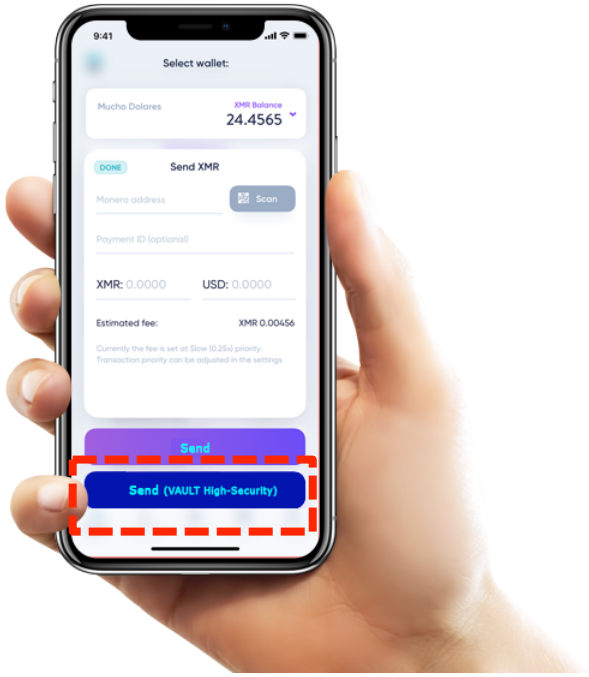
사용자가 다양한 접속환경 (PC, Mobile, Web)을 지원하는 볼트 사용자 보안 솔루션을 사용할 경우, 사용자는 자신이 보유하고 있는 VSS 토큰을 사용하여야 합니다. 솔루션은 제공되는 서비스 종류에 따라 종량제 또는 정액제로 VSS 토큰을 요청하게 됩니다.

예를 들어, 사용자 A 가 자신의 PC 에 볼트 사용자 보안 소프트에웨어를 설치할 경우, 이 소프트웨어는 안전한 암호화폐 거래를 위해 사용자의 PC 를 각종 해킹위협으로부터 보호하게 됩니다. 보안 소프트웨어의 사용을 위해서 VSS 토큰을 지급하여야 합니다. VSS 토큰은 볼트로 회수되어, 지속적인 해킹위협방어 연구 및 소프트웨어 업그레이드에 사용됩니다.

둘째, 암호화폐 거래소

사용자가 자신의 암호화폐 지갑에서 다른 지갑주소로 암호화폐를 전송할 경우, 볼트의 솔루션은 신뢰성이 높은 트랜잭션 서비스를 제공하며, 이에 대한 커미션을 VSS 토큰으로 지급하여야 합니다.

볼트 보안 전송 화면 예시



예를 들어, 사용자 A 가 암호화폐 거래소를 통해 자신의 비트코인 지갑에서 1 BTC 를 다른 비트코인 주소로 전송시, 볼트의 보안네트워크를 사용할 경우, 사용자는 VSS 토큰을 지급하게 됩니다. 여기에 지급된 VSS 토큰은 볼트 생태계의 유지를 위해 거래소 서버, 중계 서버, 볼트 비영리 법인에 지급하게 됩니다.

셋째, 기타 암호화폐 사업자

암호화폐 사업자가 볼트 AI-HFDS 를 사용할 경우, 암호화폐 사업자는 자신의 회원들에게 수준높은 보안 서비스를 제공할 수 있습니다.

특히, 볼트의 AI-HFDS 는 다양한 사용자, 트랜잭션 모델링을 통해 정확성을 높이며, 서로다른 사업자간에 독립적으로 운영이 되지만, 보안 측면에서는 각 사업자에 최적화된 보안 트랜잭션 기능을 제공하게 됩니다. 사업자는 이러한 장점을 가진 볼트의 서버용 AI-HFDS 도입을 위해 VSS 토큰을 사용할 수 있습니다.

5. ROADMAP

볼트는 2018 년 4 분기 VSS 토큰의 Token Offer 를 시작합니다.
2019 년 1 분기중 VSS 토큰을 발행하고, 아래의 표와 같이 단계적으로 보안 솔루션을 출시하게 됩니다. 아래에 계획된 개발일정은 추후 공지를 통해 변경될 수 있습니다.

5.1 Business Roadmap

일 자	내 용
2018 Q4	• Start VSS Token offer and Croud Funding
2019 Q1	• Masternode Partner application start • Roadshow - Asia, America, Europe
2019 Q2	• Open America HQ • Masternode partner appointed
2019 Q3	• Open Europe HQ • Vault partner network event
2019 Q4	• Vault stakeholder event • Global advertisement start
2020 Q4	• Vault global exhibition

5.2 Technical Roadmap

일 자	내 용
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 Sale Plan

이 백서안에는 VSS 토큰이 적용되는 방법, 토큰 사용에 대한 잠재적 이점 및 토큰 획득 방법 및 시기, 토큰 출시일과 같은 Token Offer 에 대한 기본 사항이 설명되어 있습니다.

6.2 Token Offer

우리는 볼트 보안 플랫폼와 볼트 보안 생태계의 발전을 믿는 개인 및 조직을 초대하여 VSS 토큰을 기존 가상화폐로 일정 비율에 따라 기탁(또는 교환)받게 됩니다. VSS 토큰은 볼트의 보안 생태계를 내에서 암호화폐 사용자 및 서비스 제공자의 보안 기능 사용시 사용될 것입니다.

총 발행되는 토큰은 100 억개로,

- 2,000,000,000 개의 토큰은 볼트 비영리법인의 미래에 사용을 위한 보유분임.
- 900,000,000 개 토큰은 파운더 보유분임.
- 3,100,000,000 개 토큰은 파트너, 팀원, 각종 컨설팅 서비스를 위한 보유분임.
- 4,000,000,000 개의 토큰은 크라우드 펀딩, 공공, 개인, 기업을 위한 Token Offer 수량.

토큰 배분 표

구 분	상 세
볼트 비영리법인 보유분 (20%)	각종 리워드 지급, 서비스 관리, 생태계 유지등 미래 서비스를 위해 예약된 토큰 할당량
파운더 (9%)	파운더 보유 토큰 할당량
파트너 (31%)	파트너, 컨설팅 서비스 및 팀원을 위한 토큰 할당량
Token Offer (40%)	크라우드 펀딩을 위한 토큰 할당량

6.3 Token Type

VSS 토큰은 본 백서에 명시된 바와 같이 '볼트의 플랫폼에 의한 암호화폐 트랜잭션 보안'에 사용하는 Utility Token 으로 Security Token 이 아닙니다.
VSS 토큰은 이윤투자 용도로 사용할 수 없으며, VSS 토큰은 최종 사용자가 디지털 결제 및 암호화 통화 거래의 보호를 위해 사용해야 합니다.

볼트는 토큰 판매에 앞서 싱가포르의 관할권을 기준으로 설정되며, 증권 및 보안 테스트와 관련된 싱가포르의 법률만 적용됩니다. VSS 토큰은 볼트의 주식 또는 자산, 볼트의 수익 또는 이익 또는 현재 또는 미래의 관련 엔티티에 대한 소유권을 제공하지 않습니다.
VSS 토큰은 TheVault LTD.(볼트 비영리 법인)의 주식 또는 자산의 소유권을 포함하지 않습니다.

6.4 Fund Usage

볼트 비영리 법인이 크라우드 세일로부터 받은 기금은 볼트 생태계의 발전과 볼트 플랫폼 개발을 위해 사용하기 위한 것입니다. 접수된 기금 수준에 따라, 개발의 범위를 결정할 것이며, 제안된 우선순위에 따라 개발이 진행 됩니다.

자금 사용에 있어서, 볼트 비영리법인은 가능하면 암호화 통화를 사용할 계획이지만, 아래 비용 중 일부를 지불하기 위해서는 일반 통화로 교환해야 합니다.

아래의 자금 사용 구분은 크라우스 세일 기간 동안 모금 된 기금이 어떻게 할당 될지에 대한 대략적인 추정을 제시합니다. 모집한 기금은 아래와 같이 배분되어 사용될 예정입니다.

- 60% is reserved for project design, research and development
- 30% 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/