VESvault Business White Paper

John Brixius (jb@vesvault.com)

Jim Zubov (jz@vesvault.com)

Svetlana Starkova (ss@vesvault.com)

Slava Starkov (vs@vesvault.com)

October 1, 2018

Table of Contents

1 A Global Internet Pervasive Opportunity

Encryption is un-hackable. If encryption was practical for mainstream use for data-at-rest (stored data), it would transform cyber-security. This issue touches all stored information for every user, every business, and most government agencies everywhere on the Earth: documents, photos, videos, voice messages, audio files, server stored text messages, email messages, digital assets, financial records, medical records, etc. It's a totally global, Internet pervasive issue and market. In fact, some experts have stated the future viability of the Internet itself hangs in the balance if the growing cyber-security threat it not mitigated. Yet, end-to-end encryption of data-at-rest is very rarely used, and the market remains almost completely untapped. We believe the technologies and services that solve this problem are going to have massive global market reach for all data-at-rest: everything, everywhere, for everyone. VES offers a solution to this problem.

2 The Problem and Problematic Solutions

2.1 The Cyber-Security Epidemic

By most accounts, cyber-crime is growing at epidemic rates. Economic losses are staggering and are also rapidly growing. Alarmingly, it's more likely than not that any single person will be a victim of cybercrime. More concerning, some experts say the viability of the Internet itself is at risk.

That we may soon reach a point where society can no longer trust the internet and will need to find off-line solutions to the services that are currently conducted on-line.

2.2 Suboptimal Non-Encryption Security Measures

All of the commonly used cyber security measures don't seem to be working. Authentication control, firewalls, anti-malware and other measures seem to be breached at an alarming level.

2.3 Encryption: A Perfect Record Of Security

Curiously, encryption has essentially a perfect record from being hacked, and yet its use it limited to data in transmission. Encryption is rarely used for data at-rest (stored data).

2.4 The Myth of Pervasive Encryption

Most people think that encryption is used far more than it actually is. They think their emails are encrypted. In truth, their emails are only encrypted while they are in transit, not while they sit on the server (i.e., Hillary Clinton email server scandal). Most people think backups of their encrypted text messages are safely "encrypted". If "encrypted" backups are stored on servers they are done so with the encryption key belonging to the service provider and not the same key used by the owner, meaning the service provider can access your content at any time. It also means the service provider's key may be stored somewhere in an unencrypted state (plain text), making it accessible to hacks. That's like putting the key to your front door under your doormat.

2.5 Encryption: The Flawed Perfect Solution

2.5.1 The Needle In The Haystack

The concept behind encryption is very simple. It's essentially hiding a needle in a haystack, a very, very big haystack. The needle represents a key and whoever has the key can unscramble or unlock what the key is protecting. Without the key, the information cannot be decrypted (unscrambled) and is completely safe.

Encryption doesn't stop anyone from searching and finding the key. The only protection is that the haystack is so large it is essentially impossible to find the needle – to guess what the key is. Only the proper owner knows where the needle is hidden – what the key is.

2.5.2 The Size Of The Haystack

The number of possible guesses to find the key is so large it's difficult to comprehend. But, it's helpful to try. There are about 10^{18}, or one billion, billion grains of sand on the earth and there are 100 times more atoms in a single grain of sand than there are grains of sand on the entire Earth. Then, there are more stars in the universe than there are grains of sand on Earth and stars are far, far larger than Earth. We could keep going, but suffice to say there are an estimated 10^{80} atoms in the universe.

The approximate number of possible guesses to find a private encryption key is about 10^{156} for ECDH P-521 encryption. To comprehend that number, if there were as many universes as there are atoms in our universe, the total number of atoms in all those universes would be 10^{160}. Cracking the encryption is equivalent to finding a single atom in an impossibly large number of universes.

As evidence that the haystack is so large it's impossible to find a key, there has never been a known successful brute force hack on Bitcoin. Billions of dollars of Bitcoin are available for anyone in the world to take.

There are no other security measures. All anyone needs do is find a key for a single digital wallet and use a browser to secretly enter the key and transfer someone else's hundreds of millions of dollars into another, completely anonymous wallet and walk away without leaving a trace. This could be done in seconds on a laptop in a crowded coffee shop and no one would be the wiser. The stolen money would be safely protected for use on another day. But, it simply never happens because encryption is an un-hackable security measure.

2.5.3 The Problem With Encryption

Encryption's very strength is also its Achilles heel. It is so un-hackable, that if the owner loses the key, they can never again access their encrypted content. It is lost forever. While this may not be a deal killer for some very specific applications and users – primarily blockchain, ephemeral texts and some government agencies – for most people and the vast majority of situations, the benefit is not worth the risk. Encryption is impractical for mainstream use.

3 Sub-Optimal Spare Key Solutions

The only solution to the key loss problem is to safely store one or more backup keys – copies of the original key – or the Seed that uniquely generates the key.

But having additional copies of keys results in compromises in privacy, security and convenience that either negate the benefits of encryption or render it no longer acceptable for general use.

Even if these compromises didn't exist, previous methods of storing spare keys simply haven't been reliable enough to merit their use. If the odds are only 1 out of one million that the backup method will fail, in a world with billions of online users, who wants to be the 1 out of every one

million persons who loses their priceless photos, documents or digital assets?

4 Solution Requirements

A solution is needed that:

1. doesn't compromise the security or privacy of end-to-end encryption;
2. has a high level of reliability (we estimate at no more than a 1 in 1 billion chance of failure, and preferably much less).;
3. isn't inconvenient.

Such a solution would unlock the true potential of encryption for pervasive use with all stored content and would finally enable end-to-end encryption to be practical for mainstream use.

5 The VES Solution

VES, or Viral Encrypted Security, can deliver on all three criteria and can be a significant contributor to enabling encryption for widespread use with all data-at-rest.

Through the VES APIs, *any* 3rd party service provider can integrate VES into their products and provide the benefits to their customers. VES can essentially work with everything, for everyone, everywhere.

6 Recovery is Simple and Easy

Recovering lost encrypted content is simple and easy with VES.

If Alice discovers she lost her key, she simply checks the *lost key* option and creates a new VESkey. Alice's friends are immediately alerted. By entering their own personal VESkeys and selecting the *assist* option, each friend can contribute to Alice's recovery process. When a predetermined number of friends have assisted Alice, she can then enter her new VESkey, and all of the previously lost encrypted information will be recovered. It's that simple.

Although multiple friends can help, none of them has access to any of Alice's information, ensuring the privacy and security of end-to-end encryption is maintained.

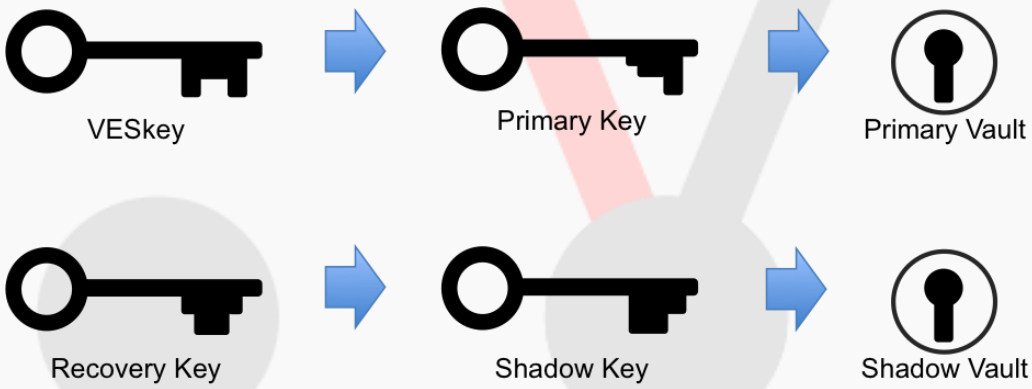
7 How VES Works

Among other innovations, VES uses a technology similar to a concept called Shamir's Secret Sharing, but with some slight changes and some very significant improvements. In particular, VES solves the ***reliability*** and ***collusion*** issues that have kept past implementations of Shamir's from being usable. To understand how VES solves the reliability and collusion issues, along with how VES address security in full, it is best to start with a general understanding of how VES works.

7.1 The Shadow Vault

Suppose Alice is a user of VESvault. A critical element to VES security is a Shadow Vault holding another encrypted copy of Alice's data. Alice's private information is duplicated with one of the two collections deposited in a Primary Vault and the second deposited in a Shadow Vault. The Primary Vault is encrypted by the Primary Vault Key while the Shadow Vault uses a different key, the Shadow Vault Key. Neither key can unlock the other vault.

On a daily basis, Alice uses her VESkey to access her Primary Vault. She does not have possession of the other key – the Recovery Key – to access the Shadow Vault, nor is the Shadow Vault ever accessed for any reason other than to recover her lost content if she loses her VESkey. It is these two sets of distinct copies of Alice's information, each only accessible through distinct encryption keys which are each used in distinct, non-overlapping ways, that makes VES unique. It allows VES to effectively address security vulnerabilities.



7.2 VESkey And App Keys

Alice's manually created VESkey is used to access the encrypted content in her Primary Vault. Alice keeps her VESkey to herself, and is encouraged not to store it on her computer.

Each VES enabled 3rd party app used by Alice creates its own App Vault, and an associated App Key to decrypt the content of the App Vault. Each App Key is stored in Alice's Primary Vault in the encrypted form. Hence, there is also a copy of each App Key stored in Alice's Shadow Vault.

When Alice manually enters her VESkey, it can decrypt all the contents in her Primary Vault, including any and all App Keys, which in turn are used to decrypt the contents of their respective App Vaults.

Each App may choose either to securely store its App Key outside the purview of VESvault, or to request Alice to retrieve the App Key using her VESkey every time she uses the app. If this is the case, the process steps would be:

a) the App invokes VESvault, which retrieves the encrypted entries from the VESvault repository and requests Alice to enter her VESkey;
b) Alice enters her VESkey, the client-side VESvault component decrypts the Primary Vault Key, uses it to decrypt the App Key and securely transfers the decrypted App Key to the App, all of which are on Alice's device;
c) the App uses the App Key to retrieve and decrypt the encrypted content in Alice's App Vault, all of which takes place on Alice's device, ensuring the entire process is end-to-end encrypted.

7.3 Recovery Key And Recovery Tokens

A randomly generated Recovery Key is needed to decrypt the Shadow Vault Key, which is used to decrypt the Shadow Vault. The Shadow Vault content is a mirror image of the content of the Primary Vault.

Borrowing from linear algebra – where to solve for the unknown variables it takes at least as many independent equations as there are variables – the Recovery Key is scrambled into multiple unique Tokens. Each individual Token is completely unusable as an encryption key and incapable of being unscrambled. Only when a pre-determined number of Tokens are combined can they be unscrambled to re-form the Recovery Key.

Each Token is allocated to one of a handful of friends who have been pre-selected by Alice, and is deposited into that friend's Primary and Shadow Vaults in an encrypted form – resulting in a secondary level of protection.

7.4 Starting The VESrecovery Process

When Alice next tries to access her encrypted content and discovers she has lost her VESkey, she simply creates a new VESkey while selecting the *lost key* option. All her friends are immediately alerted by email with a link to assist the recovery, which they can do by keying in their personal VESkeys and electing to assist Alice.

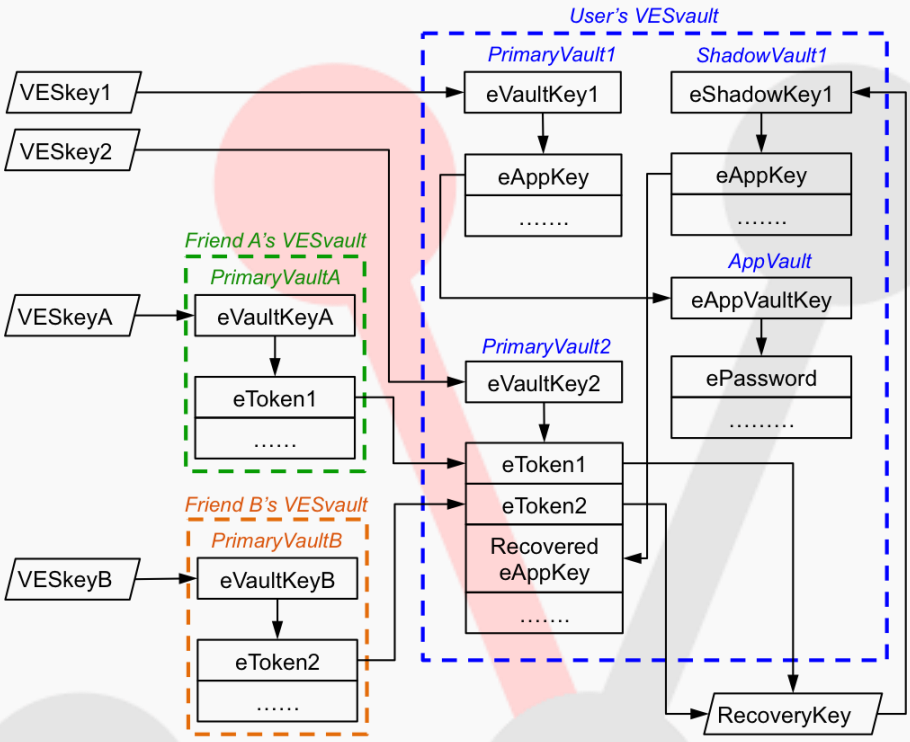
7.5 The VESrecovery Process

When Alice's friend Bob assists Alice, the recovery token in his VESvault is decrypted from his encryption by Bob entering his personal VESkey. It's then re-encrypted with Alice's new encryption, and deposited in her Primary Vault. Once the pre-defined number of friends have similarly provided assistance to Alice, she is alerted. Once Alice enters the new VESkey she recently created, the system automatically reclaims the lost encrypted content and re-encrypts everything using Alice's new VESkey. Everything is recovered and stored under Alice's new VESkey.

During the entire process, nobody, including VESvault, has access to any keys that can decrypt Alice's personal information, ensuring that end-to-end privacy and security is maintained.

8 A More Detailed VES Process Overview

(Note: This section is somewhat technical in nature. It is a more detailed version of the previous section and intended as an introduction to a technical analysis. A non-technical reader may choose to skip this section if a more detailed understanding of VES is not desired.)



8.1 Semi-Detailed Illustration Overview

The above figure is meant to show how the VES encrypted repository is organized and how VESrecovery works relative to a 3rd party App that uses the VES APIs. As such, some system components, process steps and relationships that are not critical to the explanation may be missing or simplified. All encryption and decryption steps occur on the client side, making for full end-to-end encryption.

Note that the Primary and Shadow Vaults are mainly intended for storing internal items, such as App Keys and Recovery Tokens, while secondary App Vaults are dedicated to user generated and encrypted items, such as notes, documents, photos, emails, passwords, transactions, or whatever content the individual App is storing on behalf of the user.

8.2 Illustration Conventions

- An "e" in front of any label indicates that the item has been encrypted. For example, *eVaultKey1* is the encrypted version of *VaultKey1*
- All keys in the parallelogram shapes are symmetric encryption keys – all the *VESkeys* and the *RecoveryKey*. These keys are never stored in the system: *VESkeys* are manually entered by users, and *RecoveryKey* is temporarily recreated by the descrambling process using the *Tokens*.
- Asymmetric encryption keys are shown in rectangular shapes – all *VaultKey* entries, *AppVaultKey* and *ShadowKey1*.
- All arrows originating from keys show the items that they decrypt, either directly or indirectly, as is the case with *RecoveryKey*.
- Every *PrimaryVault* normally has a *ShadowVault*, but only *ShadowVault1* is shown because it is the only *ShadowVault* used in the recovery process.
- Everything within an individual user's Vault is accessible only through either the user's *VESkey(s)* or *RecoveryKey(s)*.
- Everything within an AppVault is accessible through AppKey, which might be either stored externally by the App, or retrieved from the user's Vault on every use.

8.3 Using VESvault in Conjunction with a VES Enabled App

In most cases, a VES enabled App will invoke a VESvault Delegate process, which will interact with the user to decrypt the App Key, and then send the App Key back to the App, at which point the App can communicate with the VES API directly to deposit and retrieve items in the corresponding App Vault.

If the user's VESvault account or the App Vault is not completely set up, the Delegate process will guide the user through onboarding.

The App may choose to store the App Key indefinitely. In this case the user may keep using the App without the need to further interact with VESvault or to use the VESkey.

8.4 VESrecovery

8.4.1 Setting Up VESrecovery

VESrecovery must be set up prior to the loss of the VESkey. The User is requested to set up VESrecovery during the VESvault onboarding process, and may change the settings at any time.

The User selects a small number of friends, *N*, to call upon to assist in VESrecovery. In the illustration, *N* is not known nor is it shown. The User also selects the number of friends required, *X*, to assist the User to achieve recovery. In the illustration, it is implied but not outwardly stated that $X = 2$.

8.4.2 Recovery Tokens

With *N* and *X* established, VES creates *N* independent linear equations, each with *X* variables, and allocates a unique token pertaining to each equation to each of the *N* friends.

In this case there are two tokens, *Token1* and *Token2*. *Token1* is encrypted with the public component of *VaultKeyA* to create *eToken1*, and *Token2* is encrypted with the public component of *VaultKeyB* to create *eToken2.*

Both *eToken1* and *eToken2* are stored in the Primary Vaults and Shadow Vaults (not shown) of *Friend A* and *Friend B*, respectively.

8.4.3 Creating A New VESkey And Starting VESrecovery

The link, *I Lost My VESkey*, is available at every VESkey entry box and the User can select it when *VESkey1* becomes lost. Upon doing so, the User is required to manually create a new *VESkey2.* In doing so *PrimaryVault2* is also automatically created. Simultaneously, an alert is sent out to the User's friends.

8.4.4 Assistance From Friends

Friend A and *Friend B* can assist the User by entering *VESkeyA* and *VESkeyB*, respectively, along with selecting the *Assist* action in VESvault. *VESkeyA* and *VESkeyB* then decrypt *eVaultKeyA* and *eVaultyKeyB*, respectively, which in turn decrypt the *eToken1* and *eToken2*, respectively.

Separately, *Token1* and *Token2* are unusable as keys and are essentially as difficult to unscramble as it is to brute force hack state of the art encryption.

Token1 and *Token2* are then re-encrypted using the public component of User's new asymmetric key, *VaultKey2*, and deposited in the User's new *PrimaryVault2*.

8.4.5 Finalizing VESrecovery

The next time the User enters *VESkey2* to access the new PrimaryVault2, *VESkey2* decrypts *eToken1* and *eToken2* from *PrimaryVault2. Token1* and *Token2* are then descrambled to re-create *RecoveryKey*, which is used to decrypt *eShadowKey1* to re-create *ShadowKey1*. *ShadowKey1* is used to decrypt all the contents of *ShadowVault1*, including the backup copy of *eAppKey*. All the decrypted contents of *ShadowVault1* are then re-encrypted with the public component of *VaultKey2* and deposited into *PrimaryVault2*.

This completes the recovery process and the User can now use the new *VESkey2* to access the VESvault contents. At this point *PrimaryVault1* and *ShadowVault1* are deleted.

8.5 Security Considerations

When looking at this process, it is important to note that, unlike App Keys, user created VESkeys are never shared with any App. The VESrecovery process is unique to VESvault and cannot be conducted by the App. This provides a safeguard in that while the App can do anything it wants with the App Key and the contents of the App Vault (any 3rd party App developer can do anything they want with their own information), the App can neither decrypt any other content of VESvault, nor it is permitted to do any changes outside of its App Vault.

9 Security

9.1 VESvault Password

Alice can access her VESvault account (but not her encrypted VESvault contents – that requires her VESkey in addition to her password) either by using her VESvault password, or by authenticating with a trusted linked account, such as Google or Linkedin. While using a linked account is a convenient option to access VESvault, the password needs to be entered on every critical action – setting or changing a VESkey, setting VESrecovery friends, starting VESrecovery (*forgot VESkey* option), changing the password.

To initially set her VESvault password, or to reset a lost password, Alice must use a secret link sent to her email address, thus confirming she has access to her email inbox.

It's worth noting again that, under a proper setup, Alice's VESvault password does not give her the ability to decrypt any information stored in Alice's VESvault.

9.2 VESkey

Alice's VESkey is a master password that is used to indirectly decrypt all information in Alice's VESvault. Alice is supposed to create a strong, hard to guess VESkey, and never share it with anybody.

The importance of using a strong VESkey cannot be underestimated. Encryption only guarantees protection if the encryption key is strong enough to make it impossible to brute force hack your data.

9.2.1 Split VESkey

The **Split VESkey** feature is an important planned development because it will make the use of very strong, computer generated VESkeys more convenient.

With the split key feature, the VESkey will be securely stored on the user's device protected by the device's security means, such as fingerprint, PIN or facial scan. The user only needs to unlock the device, which in turn unlocks the full, randomly generated VESkey. This feature provides the best of both worlds – an easy and convenient access from a secure device such as Android or iPhone, along with the full benefit of encryption form a long, random VESkey.

The smart phone feature that locks out multiple attempted PIN entries complements the Split Key feature in that it is so secure that Split Key doesn't need an additional PIN with its own lockout feature. For devices without these PIN security measures, like regular laptops, PCs or tablets, VESvault employs a server side measure that simulates this access/lockout feature found in secure smart phones.

For these cases, the user's locally stored VESkey will be encrypted with a strong intermediate encryption key. The intermediate key will be randomly generated by and stored on the VESvault server, and only supplied by the server in response to the correct PIN, fingerprint or facial scan coming from the client's device. In this regard, the same PIN, fingerprint or facial scan that unlocks the phone can be used to unlock VESvault.

After a certain number of incorrect attempts – just as with a smart phone – VESvault will lock out the user's intermediate key for a certain time, or eventually forever, enabling the level of security on par with an iPhone for common unsecure devices. If the correct PIN, fingerprint or facial scan is entered, the intermediate key will be sent to the user's device, where it decrypts the VESkey to enable a VESvault session. Storing the intermediate key on the server does not create an additional vulnerability since it is useless by itself to any hacker who gains access to it. The result is the VESvault version of this feature is as secure as the local smart phone version.

The user will be able to replicate or transfer the VESkey between devices using a barcode, similar to other end-to-end encrypted services. In case if the user loses a device with a VESkey stored on it, he will need to promptly change his VESkey using another device, and the lost device will be instantly locked out from VESvault.

9.3 Two-factor Authentication

Two-factor authentication, planned to be implemented in the near future, will serve as a security barrier that protects users from hackers that try to steal users' passwords in order to gain unauthorized access to their VESvault accounts. Since bad agents attempting a hack of VES protected encrypted data will, among other things, attempt to initiate VESrecovery upon gaining access to the user's account, two-factor authentication will be a strong safeguard to prevent this from happening.

Requiring two-factor authentication means that a hacker not only needs to steal the user's password, but also has to access the user's device.

Two-factor authentication improves the security of the VESvault account comparing to using only a password, which in itself is less protected than the VESkey (recovering your password takes place by email, which is far less secure than the VESrecovery process).

This feature is intended not to be obtrusive or time consuming. The user will only be required to use a second device (for instance, to receive a text on your phone) in addition to entering the password when changing the password, or requesting VESrecovery. For any other actions, that require the user to know their current VESkey, the 2nd factor would be an unnecessary inconvenience.

9.4 Shadow Vault

All the contents of Alice's Primary Vault can be decrypted using her VESkey. The Shadow Vault is a real-time mirror copy of the Primary Vault, except that it is encrypted by a different set of keys.

9.4.1 The Recovery Key And The Shadow Vault Key

The Recovery Tokens that are shared with Alice's friends can be combined to recreate the Recovery Key, which decrypts the Shadow Vault Key, which in turn decrypts the contents of the Shadow Vault. This two-key process allows for additional security measures as opposed to using a single key. While Alice's friends might be able to recreate the Recovery Key, the system is designed so that they should never have access to Alice's encrypted Shadow Vault Key.

Access control measures are used so that only owner of the content, Alice, can get access to the encrypted Shadow Vault Key. If Alice's friends collude and build the Recovery Key, or if hackers do the same by hacking

Alice's friends' accounts, they would still need to bypass the access control measures to gain access to both Alice's Shadow Vault Key and her Shadow Vault contents.

9.4.2 Shadow Vault Key Is Only Accessed Under One Condition

The VESvault backend will not reveal the encrypted Shadow Vault Key to anyone other than Alice, and only a single time under a single condition – when VESrecovery has been triggered by a lost key event. There are no copies of the Recovery Key in existence, either in an encrypted or unencrypted state. In addition, the access to the Shadow Vault Key is restricted by the Security Time Delay, which is explained in another section.

9.5 Voice (ID) Verification

While identity verification by real human friends is currently only a voluntary part of the security measures that VES employs, it is forecasted to eventually become a mandatory part of the process. Currently, humans rely on computers as inanimate objects to prove our identities more than the consent from other humans. We rely on passports, driver's licenses, birth records to establish our identities in the real world, and our ability to access our online accounts to manage our identities in the cloud. Yet, at the same time, humans rely on the ability of other humans to identify us through visual and audio clues.

As artificial intelligence grows, the means of identifying humans in the cloud will shift from ability to access our online accounts to humans in our physical world vouching for our identity. The reason for this is that artificial intelligence, and hackers, will increasingly be able to succeed at online Identity theft. The will be able to increasingly hijack our online identity and create increasingly higher hurdles to our ability to reclaim it. Moreover, these systems will enable easier falsification of the documents we so readily rely on to establish our identity – passports, driver's licenses, etc.

While the advancement of blockchain may be one piece of the puzzle to combat this situation, another critical piece of the solution is to look backward at technology as opposed to forward. Our identity is first established by our human networks and our human networks can and will play an increasing role in maintaining our cloud-based identities as technology advances.

As such, VES stands to play an important part of ID verification. The VES network will not only become another factor of identification, but one that is less prone to hacking as it is human based and not computer based. At first, the VES ID verification will be exclusive to VESrecovery but it is a capability that could become an important stand-alone service. In essence, the VES network for ID verification is a human parallel to how blockchain nodes works to ensure the validity of the blockchain.

9.5.1 How ID Verification Works In VES

Currently, voice, video or real-world verification in VES is not a mandatory process. It is recommended that, before executing assistance, friends Voice Verify that the User is in fact the person who initiated the VESrecovery process.

In the future we see this process being made mandatory. The two barriers to doing that today are that users and their friends may not value the measure sufficiently to endure the additional time delay and that the process needs to be refined more to minimize the level of inconvenience.

There are multiple ways in which ID verification can be integrated. One possible way is to integrate a calling app that must verify that an audio or video connection has been made between a friend and Alice before this friend can provide the assistance. Another possibility would be that a PIN is given to Alice when she requests VESrecovery, then Alice must verbally convey the PIN to the friend who then keys it into the system before they can assist Alice.

9.6 Security Time Delay

When a VESrecovery event is initiated, a countdown timer starts that blocks Alice's encrypted Shadow Vault Key from being released. At the same time, an alerting email is sent to the Alice's email account informing her of the recovery event and giving the option to stop it if she didn't authorize it. At any time before the hackers complete the recovery, Alice can stop the process by entering her VESkey. The security time delay guarantees a minimum amount of time to do this.

If the Security Time Delay expires, it doesn't mean that Alice can't still enter her VESkey to prevent the hack. She can do so even if the friends have already provided the assistance, as long as the hackers have not entered the VESkey they created to complete the recovery process. After the Security Time Delay expires it becomes a race as to who enters their VESkey first.

9.6.1 Security Time Delay Options

Alice can select a security time delay from 5 minutes to 30 days to meet her personal requirements in balancing security with speed of recovery. She would want to set a time that is long enough for her to safely respond to the email alert but not so long as to make VESrecovery inconvenient for her should it be a real recovery event that she legitimately initiated. Any recovery event, regardless if rightfully or wrongly initiated, cannot be completed until the Security Time Delay expires.

9.7 Forward Secrecy

Additionally, VES will have forward secrecy to provide still another layer of protection from a back-door hack. When Alice enters her current VESkey, both her Primary and Shadow Vault contents are periodically re-encrypted with new, randomly generated Primary and Shadow Vault Keys. A new random Recovery Key will be generated to encrypt the private

Shadow Vault Key, and scrambled among the Alice's VESrecovery friends on the background. In doing so, any Recovery Key previously recreated by colluding friends, or any encrypted content stored by a backdoor hacker, is no longer usable.

10 Vulnerabilities Of VES Encrypted Content

10.1 Overview: VES vs E2E Without VES

As mentioned, the encryption used in VES is the same that is used in any other e2e service deploying state-of-the-art encryption algorithms. The only meaningful difference between the two is the inclusion of VESrecovery, where a recovery key is created and processed into the tokens that are shared with friends. Since outside of this functionality, e2e encryption is considered extremely secure and without vulnerabilities, the only assessment of vulnerability that matters is any possible increased vulnerability that results from the inclusion of the recovery key process. Specifically, does VES create additional vulnerabilities and to what extent.

The only increased vulnerability in using VESrecovery is the possibility of someone gaining unauthorized access to the recovery key. The bulk of the VES security measures, above and beyond using encryption itself, pertain to mitigating the risk that an unauthorized user can gain access to the recovery key.

It helps to break this risk down to two separate groups of people: hackers and the friends the user selects for recovery.

In terms of friends, they would need to collude to rebuild the recovery key, and then successfully execute a back-end hack to the system to steal the encrypted contents belonging to the user. Or, they'd need to steal the user's VESvault account, bypass two-factor authentication and bypass the security time delay. The possibility of successfully doing this is extremely

remote, and made exponentially more remote in that it is limited to a handful of people the user has personally selected as trustworthy, who also may not know each other.

For hackers, brute force hacking to get the tokens and rebuild the recovery key is harder than brute force hacking the encrypted content itself, because the hacker would need to do it more than once and then bypass additional steps. So there is no additional vulnerability along this path. The hacker's only viable path requires sequentially defeating multiple security barriers: getting access to the user's email account, bypassing two-factor authentication, tricking the friends into offering recovery assistance and then bypassing the security time delay. Yes, this is an additional vulnerability, but these barriers are significantly higher than those currently used on the most secure sites that don't use encryption. In particular, the security time delay alerts the user in real time that a potential hack is happening and gives the user the ability to stop it. Thus, the odds of this attack succeeding are extremely remote.

To sum it all up, the tradeoff in using VES is getting a reliable means of recovering content after key loss versus the risk that a hacker can bypass multiple independent layers of security to steal your recovery key. These layers being above and beyond the level of security that current non-encrypted services use. For most people, we believe this is an easy decision in favor of using VES.

10.2 Brute Force Vulnerability Of Encryption

As long as a strong VESkey and strong randomly generated App Keys are used, the User's data is essentially impossible to brute force hack. VES uses state-of-the-art encryption algorithms, such as ECDH P-521 and AES-256. In this way, the User's secret data is no less safe with VES than with any other encryption solution, such as Bitcoin.

Because VESkeys are manually created by Users, there is a distinct chance that Users will not use the full randomness and create short, easy to remember phrases for their VESkeys. In these cases, the encryption is not as strong as it could be and is more susceptible to being hacked than in case of apps that randomly generate strong encryption keys.

A tradeoff exists between using a short, easy to remember passphrase as the VESkey and the improved security of using a long, random passphrase. A solution that results in having the best of both worlds is the future Split VESkey technology on the product roadmap. This technology is more fully explained in "Split VESkey" section of this document.

10.3 Identity Theft Vulnerability

If a hacker gets access to the User's VESvault account, either by stealing the User's credentials or by taking control of a device with the User's VESvault session open on it, the hacker still won't have all that is needed to decrypt the information without the User's VESkey. The intent behind the VESkey is to keep it secret and not share it with anyone. However, the hacker may attempt to initiate VESrecovery on the User's behalf, and to change the User's VESvault password in the interim.

Both of those actions require the User, or the hacker, to enter the current VESvault password, which will be a problem to the hacker who stole the session and doesn't know the password.

If the hacker attempts to use the '*Forgot password?*' action, he needs to access the User's email inbox to retrieve the secret link.

Even if the hacker succeeds with all of these actions, he will then need to defeat the two-factor authentication process which requires access to User's mobile device. See the 'Two-Factor Authentication' section for more details. Otherwise, the hacker could attempt the report that the second factor device has been lost – the recovery process for a lost two-factor

device has not yet been developed at this point, and likewise neither has the security measures to protect against a hack. Security measures will be implemented for this process.

If the hacker manages to defeat two-factor authentication and then initiates VESrecovery, he will then need to defeat ID verification. Friends are strongly advised to contact the User before providing the recovery assistance, and alert the User and other friends if suspicious activity is detected. As outlined in another section, ID verification may be made mandatory in a future release.

Lastly, an additional security barrier is the Security Time Delay, which alerts the real user in real-time that their VESvault account is being hacked and gives the real user sufficient time to stop the hack by entering their VESkey. This feature is explained in the Security Time Delay section.

In summary, the shortest list of sequential security barriers that would need to be breached through an Identity theft include: 1) gaining access to the user's email account to initiate a password reset; 2) defeating 2-factor authentication to initiate VESrecovery; 3) bypassing any ID verification by the assisting friends during VESrecovery; and 4) defeating the Security Time Delay.

It should be noted that only steps 1 and 2 are all the security measures in place for most major websites, which are considered to be secure.

10.4 Malware Vulnerability

In addition to end-to-end encryption, all communications between users and the VESvault server are handled through a secure TLS connection. It mitigates possibilities of wiretapping or man-in-the-middle attack.

However, certain kinds of malware on the client-side device, such as keystroke loggers, may potentially steal VESkeys and passwords.

Appropriate malware protection measures, such as antivirus software, may be beneficial.

10.5 Backend Hack Vulnerability

If a hacker gets access to the VESvault backend server or database, the hacker still won't be able to decrypt any information without having VESkeys. Since VESvault uses end-to-end encryption, no unencrypted secret data or encryption keys are ever passed to the backend server.

The hacker might be able to initiate VESrecovery on one or more VESvault user accounts from inside the system, and additionally to bypass two-factor authentication and the security time delay. Even then the users are still safe as long as their friends contact them to verify their identity before providing the assistance.

A group of friends colluding to rebuild the Recovery Key, in conjunction with a backend hack to gain access to the content of the Shadow Vault is the single possible scenario of bypassing all the VESvault security measures to steal the User's secret information. So, it is ultimately important to protect VESvault servers from any possibility of a backend hack.

The VESvault backend implements state-of-the-art access control. In the future, the VESvault backend will receive a formal SOC 2 attestation to ensure compliance with SOC 2 security requirements.

11 Solving The Collusion Problem

The Collusion Problem is best classified as a type of Identity Theft. It merits special attention because it is so strongly associated with Shamir's Secret Sharing that any use of Shamir's is often dismissed outright without further consideration. When framed as an Identity Theft problem, and deploying additional measures that are used to mitigate Identity Theft, the Collusion problem can be appropriately mitigated.

11.1 Collusion Problem – The Misuse Of Shamir's

The byproduct of using no security other than encryption is that it makes the encryption key a single point vulnerability. Using Shamir's to create a backup of this single point vulnerability opens a path to the key no longer being private – through Collusion – and subsequently eliminates all the security of encryption in this specialized use case scenario. As such, the Collusion risk is more often seen as an Achilles' Heel when Shamir's is used with encryption than as a vulnerability created by inappropriate use.

With past implementations of Shamir's, multiple friends could collude to recreate Alice's key and without any additional security barriers, have direct access to her encrypted content. This is a result from the key that is scrambled and shared with multiple friends through the use of Shamir's is a copy of the same key Alice uses to access her encrypted content. Having the exact same key as Alice, and with no additional security measures, the colluders can simply "pretend to be Alice" and enter her key to access her content.

Even if the friends don't collude, if a hacker were to breach the accounts of Alice's friends, the hacker could recreate Alice's key and access her encrypted content. Thus, the process of using Shamir's to scramble and share the same key used by Alice, in the absence of any additional security measures, creates an unacceptable vulnerability known as the Collusion Problem.

11.2 Mitigating The Collusion Problem

Mitigating the Collusion Problem involves creating additional security measures so that if an encryption key is recreated through collusion, it cannot be used to access the User's encrypted content without also bypassing the additional security measures.

In order to use the recreated Recovery Key, the colluding friends must retrieve the Alice's encrypted Shadow Vault Key and the encrypted Shadow Vault content. They would need to do this either through identity theft of the Alice's account, or through a backend hack on the VESvault servers.

The Identity Theft Vulnerability section describes the layers of protection against stealing the secret information through the Alice's account. Even if the friends are colluding against Alice, they still need to pass 3 barriers to complete the hack – VESvault password (and/or access to Alice's email inbox), Two-Factor Authentication, and Security Time Delay.

The backend infrastructure is protected by the industry standard measures, as mentioned in the Back-Door Hack Vulnerability section.

Before even being able to begin to attempt to defeat the three security measures (account password, two-factor, security time delay), the bad actors must come from the small group of friends selected by Alice. The conditions are that: 1) the group is very small; 2) Alice likely selects people who are trustworthy, 3) Alice's friends may not have personal connections with each other, 4) the selected friends cannot find out through VESvault the identity of the other friends selected by Alice, and 5) because the pool is so small, the decision to collude will occur after the friends have been selected. All these factors dramatically mitigate the possibility that a quorum of colluders will be able to form.

Thus, with proper selection of friends, the combination of two very unlikely events – that a quorum of colluders will form and that they will defeat all the security measures – means that the collusion risk is effectively mitigated.

12 Solving The Reliability Problem

12.1 The Reliability Problem

Since the key loss problem is the reason why encryption still isn't ubiquitously used for stored data, the reliability of recovery of a lost key needs to essentially approach 100%. If the failure of recovery is anything but extremely unlikely, it isn't good enough for practical, mainstream use. Benchmarking against the use of a primary and secondary hardware devices for storage, the reliability of any key recovery methodology needs to match, and even exceed, the reliability of two hardware devices failing simultaneously.

12.2 Virally Connected Network Of Friends

To solve the reliability issue, VES uses a virally connected network of friends that can form a virtually endless interconnected network. Each friend can assist the friends to whom they are directly connected. When someone receives recovery assistance from their friends, they can in turn assist any friends to whom they are directly connected who are also in need of assistance.

The result is a human-based chain reaction of recovery that can multi-directionally ripple through the entire VES network. There is no limit to the depth of the network that can assist the user, nor to the depth of the network the user can assist.

12.3 Each Friend's VESkey Is A Security Barrier

At the same time, each friend's personal VESkey also acts as a firewall to safeguard against a chain reaction data breach resulting from a breach of any individual account in the viral network. Each link in the chain reaction requires the manual entry of a VESkey by a friend, ensuring that the system itself can't propagate recovery without the involvement of humans at every step.

12.4 Calculating The Reliability

The following recursive formula gives an estimated probability that a user will successfully recover his or her lost VESkey should they lose it:

$$p_{L+1} = p_0 \sum_{i=0}^{x-1} \left[\left(\frac{N!}{(N-i)!\, i!} \right) {p_L}^{(N-i)} (1 - p_L)^i \right]$$

Here $\boldsymbol{L}$ is the depth of your network of Friends (0 being only you), $\boldsymbol{N}$ is the number of unique Friends per person, $\boldsymbol{p_0}$ is the probability that someone loses their VESkey in the time period between unlocking VES, and $\boldsymbol{x}$ is the number of friends needed to respond to achieve VESrecovery.

We've used this formula to develop a helpful FUN MATH tool in order to give users an opportunity to appraise their recovery chances in respect to various network configurations.

12.5 Resulting Odds Of Not Recovering Lost Data

With just a very small and limited network of friends, the odds of non-recovery can easily exceed 1 in 1 billion, which seems to be about the threshold of acceptable reliability when it comes to valuable encrypted content.

For example, suppose Alice has five friends who each have 5 friends and it takes assistance from any 2 of 5 friends for anyone in the network to achieve recovery. Also, suppose the probability any single person loses their VESkey between logins is 25%. In this scenario, the calculated odds that Alice will lose her content from key loss are about 1 in 3.4 billion!

If one more level of friends is added, the odds drop to less than 1 in 112 trillion, trillion, trillions! That's with only 156 total unique people in the network and only four levels deep! As will be shown, this probability is far less than that of two solid state hard drives failing on the same week, making the human-based VESrecovery approach more reliable than a typical hardware approach.

12.6 What Odds To Look For

The main goal of building a VES network is to achieve odds of non-recovery that are so small that successful recovery is virtually guaranteed. So what determines the cutoff?

Since there are billions of people alive and certainly hundreds of millions online, if the odd of non-recovery are 1 in a million, it will result in far too many people losing their information. This is not acceptable — after all, would you want to be that 1 person in a million who loses the data? 1 in a billion brings the statistics closer to values where it becomes unlikely that even a single person loses their data.

From a different perspective, people consider the use of hardware digital wallets with a backup on another device to be sufficiently reliable. Since the probability of annual failure of a solid-state drive (SSD) is approximately one tenth of one percent, which translates to a weekly failure rate of about 1 in fifty thousand, the chance of both the primary SSD and a backup SSD both failing in the same week is approximately 1 in 2.5 billion. Since this is generally considered to be a safe situation, matching or bettering these odds should show that human recovery VES

network can be as reliable and more reliable that using two SSDs as primary and backup.

12.6.1 Facebook And LinkedIn As Reference Networks

Considering that the average Facebook user has 338 friends[1] and the average number of LinkedIn connections is 930[2], it seems very conservative that the average person can identify 10 to 15 people in their existing networks whom they can trust to become VES friends. Using the formula in our FUN MATH page, it can be estimated that if your VES network consists of 10 friends who each have 10 friends, everyone requires 3 people to provide assistance and the probability that any single person loses their key is 25%, then the risk of losing your encrypted content is less than 1 in 6,000 billion, billion billions. These odds surpass the reliability threshold.

12.6.2 BEWARE RELYING SOLELY ON VES AS A BACKUP

At the initial stages of growing the VES network, we still advice that users of VES should always maintain a copy of their VESkey somewhere safe for retrieval should they lose it, and should not rely exclusively on VESrecovery as a lone means of recovery. The consequences of key loss is simply too great to not take additional precautions. An individual's VES network may become so reliable that the risk shifts to hardware failure, natural disaster or some other condition that may limit a user's ability to use VESrecovery, and these unlikely events, or others, can happen.

13 Technical White Paper

For even more in-depth information about VES and how VES works, and a more detailed analysis of vulnerabilities, please read our Technical White Paper.

14 VES APIs

The VES APIs allow any 3rd party service providers across the digital multiverse to integrate VES into their products and extend the benefits to their user base. The APIs may be used for any individual blockchain universe, as well as the traditional Internet universe.

The APIs are currently in production. All pertinent information can be found in the VESvault Development Center – VES.host.

15 Current Use Cases

15.1 CloudDash

CloudDash is a VES-enabled cloud storage and team management tool that integrates VES with Google Drive, OneDrive and Dropbox and more. It's the one place you can see all your drives with all service providers and every user who has access, in one view. And, you can drill down to manage by **person**, as well as by **file**.

15.1.1 Origins Of CloudDash

We began work on CloudDash as a sandbox, proof-of-concept to manage the online presence for a team, to enable a team leader to see who on the team has access to which online apps. Access rights to team documents in Google Drive, Dropbox and OneDrive became a natural extension of this tool. Document management in CloudDash, in turn, became the starting point for the first integration with VES technology.

The legacy CloudDash App is live, however it is not yet the fully refined product that we envision it to be in the future. The original VES integration took place before we released the VES API's, so CloudDash uses some

legacy methods, such as server-side encryption. In the future, full end-to-end encryption – as currently available through the VES APIs – will be incorporated into the CloudDash product.

15.1.2 CloudDash Advantages

Even in its current unfinished form, the CloudDash App still provides unique advantages as a superior tool for managing document access across centralized cloud services. It gives the manager a user view as opposed to a document or app view. In a single place, it gives the manager a tool to see everyone who has access to all documents in any number of storage drives. It gives the ability to drill down to see all the individual documents and what type of access rights any specific user has, and the ability to easily change access rights to each file on the spot. It sets the benchmark in managing user access to shared documents. The demand for this kind of App clearly exists. Today, VES-enabled CloudDash has users in *104 countries* — a truly global reach, as can be seen in the map below.

Global Reach: CloudDash user base in 104 countries (shown in blue)

15.1.3 Planned Improvements To CloudDash

Future plans for CloudDash involve integrating a new wave of Blockchain based distributed storage services such as Storj, Filecoin, Sia and Maidsafe in addition to the centralized storage services that are already available. We will add end-to-end encryption to CloudDash as well.

15.2 VESwallet

15.2.1 Motivation For Building VESwallet

We wanted to do the first integration of VES API's ourselves, so we created the Ethereum-based **VESwallet** App as a proof-of-product of the APIs. We are not in the digital wallet business – rather, we released it to

showcase VES capabilities and production readiness to the crypto community in a type of product where VES can make a difference. Since the real world horror stories of losing digital wallet keys are starting to increasingly happen, a secure and reliable way to recover the key is a much-needed solution to this problem.

15.2.2 VESwallet Design

We designed **VESwallet** by using our APIs with the open source code from MyEtherWallet / MyCrypto. VESwallet improves the Keystore option to become a safe and reliable method of storing the private wallet key and gives average users a level of safety and security that previously only existed for wealthy wallet holders.

15.2.3 Advantages Of VESwallet

We envision safe and secure encryption services to be practical and affordable to everyone and we believe that integrating VES can offer significant help in this regard by improving the redundancy of wallet key recovery while simultaneously eliminating the legacy problem of single point vulnerability with most soft and hard digital wallets. We feel that VESwallet is a real improvement over current digital wallets in this regard.

In terms of real world benefit, people are starting to lose their wallet passwords, private keys and seeds on an increasing basis, so this particular integration of VES can help mitigate a real, relevant problem that causes people to lose hefty amounts of money.

15.2.4 VESwallet Improves The Keystore Option

VESwallet dramatically improves the Keystore option by providing a safe and reliable way to recover the wallet password.

It improves the security of the wallet by storing the password separately from the encrypted private key that it decrypts, eliminating any

single point vulnerability. In turn, this brings more redundancy in safe storage options of the encrypted private key. With a safe VES backup of the wallet password in the cloud and a number of safely encrypted redundant copies of the private key stored locally, such as separate USB drives, there is far less chance of either losing the wallet or it being hacked.

The password in the cloud has VES as a redundancy and the multiple USB devices is the redundancy for the encrypted wallet private key. Neither the password in the cloud nor the encrypted key on any USB drive is usable without the other. This allows multiple USB drives to be safely stored in multiple locations because it isn't a single point vulnerability.

This advantage allows the Keystore option to become a viable means of key storage when compared to legacy options of storing the encryption key in places such as bank deposit boxes or home safes. Also, in various use case scenarios that include offline operation and isolated operating systems, the VES enabled Keystore option can match and exceed the safety and security of traditional cold, hard wallets.

15.2.5 More Information On VESwallet

For more in depth information about **VES** and **VESwallet**, please read the VESwallet Overview or visit VESwallet.

16 Product Roadmap

While VES and some VES-enabled Apps are already live, they are not yet what we envision them to be. There are many improvements and products that we plan on releasing in the future in order to fully tap into the potential of VES and VES-enabled Apps to make the Internet a safer, better place.

16.1 VES Security Improvements

There are several important VES security features in the works that we plan to release in the near future, that are already mentioned in this document:

- Security Time Delay (estimated launch Dec '18)
- Forward Secrecy (estimated launch Jan '19)
- Two-factor Authentication (estimated launch Q1 2019)
- Split VESkey (estimated launch Q1 2019)

16.2 VES Strength Of Network Tool

It is important that a user be able to quickly appraise the strength and real time status of their VES network of friends in order to know just how reliably they can expect to receive assistance. We are developing a **strength of network** tool that shows the depth and breadth of a user's network, as well as the current status any individual Friend's VESkey at a glance.

This tool will be a graphic representation of a user's VES network. It will likely consist of colored dots representing each friend, with lines connecting the dots showing the viral connections. The colors will indicate the status of a friend's VESkey. The identities of secondary friends will be protected so that other than their direct friends, a user will not know the identities of any friends of friends. In this way, the identity of every friend is kept secret from anyone other than the friend who selected them.

We are looking at ways to integrate the Strength of Network tool with our already developed FUN MATH calculator. With this integration, user's will be able to enter an estimated probability that any single person loses their VESkey to generate the overall probability of recovery for the user's real network.

The estimated launch of the Strength of Network Tool is Q2 2019.

16.3 VESmail

16.3.1 VES-enabled IMAP Email Project

The Killer App that will put VES on the map and create the opportunity for rapid viral growth of VES is the integration of VES with IMAP email. We call this project VESmail and it is our highest priority developmental project for our APIs.

16.3.2 The Need For Secure Email Storage

Email has long been pervasive across the Internet. It is used by virtually everyone, everywhere, every day. Every day, approximately 266 billion email messages are sent, and this number is expected to grow to 333 billion by 2022. With 54% of the world's 7.6 billion population having Internet access, this accounts to 65 daily emails for every online user[3][4].

What most people don't know is that the vast majority of these emails are stored in an unencrypted state on incoming and outgoing mail servers. Yes, most emails use TLS, which encrypts them while they are in transit, but TLS does not encrypt the emails while they are stored on a server. In fact, very rarely are emails encrypted while stored on a server, and essentially all emails are stored on a server somewhere. Any information on these stored plain text emails is extremely vulnerable to a hack. This was the issue with the Hillary Clinton email server – it was not a government sanctioned server and did not store emails in an encrypted state.

The adoption rate of TLS over the past few years is a good indicator or the potential adoption rate of encryption-at-rest for emails, assuming a viable solution is available. After all, if emails are important enough to be protected while in transit, they are sufficiently important to encrypt while at rest. In the past few years, TLS has gone from being rarely used to being

used for approximately 90% of all emails. We believe that a viable at-rest solution for email can achieve a similar adoption level in a short period of time, resulting in an estimated 240 billion daily emails using a service or utility to encrypt the emails while at-rest.

Numerous email encryption services have been launched but they have failed to achieve significant market penetration. We believe that the primary reason for this is the risk of key loss (which VES solves). A secondary reason for this is many of these services are closed systems – both the sender and receiver of the email must have a special email account with the encryption service.

16.3.3 The VESmail Solution

VES presents an answer to the encryption problem. By hooking up IMAP email service to VES, **VESmail** will provide a viable solution to the hurdle that keeps stored email from being protected by encryption. VESmail is different from other attempts because:

1. VES solves the key loss problem with sufficient reliability
2. VES does not require a special email account or complicated key management, and can be used with any existing IMAP email account
3. A user of VESmail will be able to conveniently, selectively send encrypted and plain text messages at will, not requiring recipients to be users of VES.

We believe the combination of these three attributes will remove the barriers to widespread adoption of VES for emails at-rest.

16.3.4 Impact Of VES Enabled Email To Growth Of VES

Not only is the size of the email opportunity pervasive to the entire Internet and applicable to every user of email, but the viral nature of emails provides for a unique viral growth opportunity for VES. Every

recipient of a sent email will need a VES account to decrypt the email. And, since the sender and recipient have a personal relationship that requires sharing secret information, there is a level of trust between the users that lends itself to them being friends for VESrecovery. With so many emails being sent every day, the viral cycle time for VES growth through email is very quick. This perfect storm of conditions should provide a highly fertile method of rapid viral adoption of both VES users and the VES network of friends.

The estimated launch date for VESmail is Q2 2019, assuming sufficient funding has been achieved.

16.4 CloudDash

16.4.1 Integration Of Decentralized Storage Services

In addition to the traditional centralized cloud storage services – Google Drive, Dropbox and OneDrive – that are already integrated, we plan to integrate the new wave of Blockchain based distributed storage services such as Storj, Filecoin, Sia and Maidsafe with CloudDash as they become available. With this, CloudDash will become an ideal single source to:

- simultaneously manage document storage across all storage options for a team, company, department family or individual;
- view and manage access rights by individual users across all storage services;
- use multiple storage services, as well as local hard drives, for better redundancy and access of storage.

16.4.2 End-To-End Encryption

An overhaul of legacy CloudDash integration with VES will give CloudDash complete end-to-end encryption.

There is no estimated launch date for the revisions to CloudDash.

16.5 3rd Party Partnerships

Our primary strategic objective is partnership with 3rd party service providers through our APIs. The fastest and most extensive way to grow the VES network is to party with 3rd parties rather than compete with them. To that end we will continue to explore and promote these partnerships. If we identify a particular market need that is underserved and we cannot identity a suitable partner, we will explore launching B2C services -- such as CloudDash and VESmail – either directly ourselves or in partnership with others. A few such opportunities have already been identified and we are in the early stages of exploration.

17 VES Business Model

17.1 VES Fee Structure

VES will charge a fee based on what the end user is being charged by the third-party service integrated with VES. The fee is calculated as a small, fixed percent of the 3rd party fee, and can be billed either to the integrated third party or directly to the end user. The approach is similar to that of Mastercard and Visa. It enables a business model that generates revenue with premium services while still enabling VES to be free when used in conjunction with free third-party services, such as email. It's a business model that can be fairly deployed across all markets without conflict, and can be fairly easily managed without unnecessary overhead.

The VES fee will be in the native currency of the 3rd party service. For example, for any traditional services that charge in USD, the VES fee will

also be in USD. For any Blockchain services, the VES fee will be in the native token of the particular service. The VES fee plan makes it simple for end users to understand the cost of VES and doesn't discriminate 3rd parties based on their fee structure.

The business model also allows for rapid viral growth of the VES network through partnerships with free services, such as IMAP email, while also providing for revenues from affiliation with premium services. And since VES will charge in the native digital currency of blockchain based services, such as the upcoming decentralized storage services, it will be a big enabler to solving the key management problem for these services and unlock their true growth potential.

Like Visa and Mastercard, the business model allows for universal, consistent use with any and all 3rd parties and their customers, enabling for widespread global adoption of VES.

Before a fee can be charged, VES must be at a state that there is real benefit to the market, which requires that the VES network be sufficiently established that it can provide the necessary level of reliability of recovery. A critical mass of active VESvault users is necessary to achieve this state. Prior to critical mass, the VES network will offer a less than optimal level of reliability. For this reason, revenue generation is not expected to occur in the early stages of launch, prior to the establishment of a critical mass of users. During this fledgling time, the focus will be on growing the VES network through free services, such as IMAP email.

17.2 Market Dynamics: VES Versus Non-VES E2E Encryption

17.2.1 Current Market Use Cases And Market Information

Until now, the use of encryption for data-at-rest has largely been limited to very specific use cases and user types. One use case is some

government agencies and corporations who have the infrastructure to protect sensitive information from those who very much wish to take it. In these situations, teams of people use complicated key management systems with strict security policies and multiple redundancies.

A second use case is blockchain, which by its design, is built solely on encryption as a single security measure. If you want to dabble in Bitcoin or any other Cryptocurrency, you've got to get comfortable storing encryption keys.

The third case is that encryption is used for some ephemeral text messaging Apps. In these cases, the text messages are almost exclusively stored on the user's device. If they are backed up on a server, they are usually either not encrypted or encrypted with the service provider's encryption key and not the user's key. The widespread adoption of these services, such as Signal, WhatsApp and Facebook Messenger, is a testament to how quickly and pervasively encryption will be adopted by the global market if the key problem is solved. The key problem is solved in this use case, by the fact that users not only don't care if they lose their past text messages, in some cases they want them to disappear. Losing a key has no impact on the user's ability to re-set their account to continue using the App.

The fourth use case contrasts very nicely with the third. This use case is where a very small number of users choose to use an e2e encryption App of a service that stores data, where most people use an App without encryption. Examples include e2e encrypted email services and file storage services. Key loss is an issue with these Apps and hence why very few consumers use encrypted versions of these Apps. It seems highly plausible that if the key loss problem were resolved, then encrypted versions of these Apps would become mainstream, replacing the plain text versions, just as it grew to become widespread in the text messaging segment.

The fifth use case is that encryption is used to secure data stored locally on smart phones, tablets and computers. In these cases, the user

enters a PIN or password to gain access to a locally stored version of the encryption key, which then decrypts the locally stored content. Often, after a very few failed PIN entry attempts, the system will shut down and disallow the access of the encrypted content for certain time, or even forever. At times, service providers, such as Apple and Google, will back up some contents of the phone. But this backed up information is rarely encrypted with the user's encryption key. Without a backup, if, for any reason, the user cannot access their phone, the locally stored encrypted content is lost forever.

17.2.2 Law Enforcement's Push For A Back Door

Use cases three, ephemeral texts, and five, smart phones, are the primary reason law enforcement agencies have been pushing for a back door to encryption. A back door would be a master key that would enable anyone who possesses it to hack into any phone or text message. Obviously, creating a back door defeats the purpose of encryption by not only allowing the government to surveil every citizen, but the master key itself could be hacked and used by nefarious actors. It is for these reasons that many privacy and citizen advocacy groups are resisting these efforts.

17.2.3 VES Versus A Non-VES E2E Encrypted App

The major claim of a traditional e2e encrypted App is that only the user has the key and nobody can ever access the user's content under any circumstance without the user's cooperation. This means that not only can't the government surveil the user, they also cannot seize the user's content even if there is a valid law enforcement reason.

The only difference between VES and traditional e2e encryption is that the Recovery Tokens can re-create the Recovery Key, which would enable the key holder to decrypt the user's information in their Shadow Vault, if the key holder could also gain access to the Shadow Vault. As explained in other sections of this document, numerous additional security measures have been put in place to mitigate this possibility.

17.3 An Alternative To A Government Back Door – The Side Door

VES is similar to traditional e2e encryption in that the government cannot spy on its citizens. However, VES is different from traditional e2e encryption in that there is a "side door" that the government can use in extreme cases to get a user's encrypted content without the direct cooperation of the user. If the law enforcement suspects that there is a justification to seize a citizen's encrypted content, the agency can get a warrant from a court. With that warrant, they can force VESvault Corp. to hand over the user's encrypted content, and VESvault would be required by law to comply. But even then, the law enforcement agency could not read the encrypted content (neither can VESvault Corp.). Instead, they could seize the user's account and initiate a VESrecovery.

The law enforcement agency would also need to secure warrants from courts to approach the user's VESrecovery friends and threaten legal action if they did not enter their own VESkeys to assist law enforcement in a VESrecovery attempt on the user's account. Since the activity of a user's account can be monitored for the likely use of a VESkey, any friend that would refuse to assist the law enforcement agency, or who pretended to lose their VESkey, would also need to refrain from using their VES account at all. The friends could resist, but it would be at a big inconvenience.

This "side door" process gives law enforcement the ability to seize encrypted information when there is just cause, and proper due process of law is followed, without giving them the ability to spy on its citizens. Prior to the Internet revolution, law enforcement needed to get warrants to place wire-taps or to seize documents, and the VES side door approach is in line with this prior, and fair, protocol.

17.4 The Conspiracy Theorists Versus The Masses

The conspiracy theorists can still use VES without using VESrecovery, and eliminate the side door along with any risk of hacking or colluding to retrieve content from the Shadow Vault. However, we believe that the vast majority of the population desires to use e2e encryption for different reasons. They primarily want to use encryption for security from hackers, with the mitigation of surveillance from either the government or the service provider being a secondary benefit. We believe most people are not interested in hiding illegal activity from the government and subsequently won't see the possibility of law enforcement following due process to seize information, and in the process announce the activity to the user and/or the user's friends, as a negative. In fact, most users would want law enforcement to be able to do this because if they go as far as to involve the courts, there is probable cause that the person targeted is dangerous to the general population. It also negates the reasons for having a back door, which most users very much care about and don't want to ever happen. In summary, we feel that the legitimate side door provided by VES is not an inhibitor to mass adoption, and could even promote VES.

In terms of VESrecovery creating a vulnerability that can be exploited by nefarious friends who collude, we feel that the vast majority of users do not feel this is a risk, especially considering all the layers of protection implemented in VESvault. The conspiracy theorist may find this aspect objectionable, but we feel that the masses will not. As evidence of this, the vast majority of the population stores all of their sensitive information in plain text form, easily readable by their service providers, easily surveilled by the government, and much easier to hack than if encrypted. With the VES vulnerability being far, far less than the vulnerability of storing content in plain text form, there shouldn't be any market acceptance risk because of this condition.

17.5 Unique Market Risks

17.5.1 A Long Term Play

For multiple reasons, the adoption of VES and success of VESvault will not happen as quickly as other technology market adoptions. VES is a form of insurance and insurance is not something that users get excited about. It's more of a slow growth product. And, it's insurance that isn't at its full potential right away until the VES network starts to grow and obtains critical mass. At the point, when new users select friends who already have extensive, established VES networks, the new users will immediately have the full benefits of VES, but that won't happen in the initial stages of growth. Also, since the value of VES will grow with the VES network, the ability to charge revenues will lag the development of the network.

However, these attributes that will result in a slower initial adoption rate will reverse and later contribute to an accelerated adoption rate once a critical mass of users and VES enabled Apps have been established. As mentioned, new users will immediately tap into the benefits of established VES networks. Once established, each user will take their entire VES network with them to every new VES enabled App they use.

17.5.2 Possible Government Regulation

There is some risk that the government will create regulations that may directly inhibit the use of encryption, or require it to be altered to limit its market appeal. However, this risk is relatively low. This is especially the case in that e2e encryption is a client-side App that would be very difficult to regulate because it does not require a middle-man. Users could simply download an e2e encryption App and encrypt everything on their device and all texts, emails and phone calls. Since, in this scenario, there is no centralized service provider that participates in the encryption, and since this technology can't be erased from the Internet, it would be difficult for the government to effectively enforce a ban on e2e encryption.

18 VES Token

The VES ERC20 token – which is not to be confused with the scrambled Recovery Token – will be membership based and will have both utility and contractual attributes. As a utility token, it will work as a smart contract within the Ethereum universe. As a general contract, it will extend beyond the Ethereum universe to every other universe in which VES can function, both blockchain and non-blockchain.

Every VEStoken will entitle the holder to an indefinite 1% discount on all VES fees from all Apps used for one individual VESvault account.

The VEStokens will be additive so any user can acquire and assign up to 100 VEStokens to any single VES account. With 100 tokens, the user will have full membership and will have a 100% discount on all VES services deployed with all Apps associated with the user's VES account.

If and when users transfer VEStoken to others, the membership rights will also be transferred in full to the new owner.

References

1 https://www.chegg.com/homework-help/questions-and-answers/2014-pew-study-found-average-us-facebook-user-338-friends-study-also-found-median-us-faceb-q23924578

2 https://www.jeffbullas.com/25-linkedin-facts-and-statistics-you-need-to-share/

3 https://en.wikipedia.org/wiki/Global_Internet_usage

4 https://www.quora.com/How-many-emails-are-sent-in-the-world-every-day