FrostByte

FROSTBYTE TECHNOLOGY INC © | WHITEPAPER NOVEMBER 2022

Redefining Data Security

www.frostbyte.app

TABLE OF

Content

Executive Summary

The FrostByte mobile app allows users to set their data security risk tolerance to absolute zero. The FrostByte app allows fully customizable data security governance while providing military-grade encryption and self-sovereign cold-storage data security.

Issues in critical data management have typically led to great economic losses, most commonly due to hacks or loss of access credentials. Most of these losses could be avoided through improvements in the current standards of data security and data management.

FrostByte's customizable governance structure enables individuals and organizations alike to nominate trusted persons to access their secret encrypted data, in case of unforeseen events happening to those persons who hold the access credentials to the secret encrypted data. Loss of access credentials can cause serious economic loss at worst, and at best can be a critical hindrance. FrostByte allows an individual user to have in place trusted persons who can access the user's secret data in the event something unforeseen happens to the user. Similarly, FrostByte allows an organization to authorize a specified number of executives or other personnel to collectively access sensitive and valuable organizational data, and to rotate those authorized persons in the event that some of those authorized personnel leave the organization or something unforeseen happens to them. A flexible and secure governance framework is invaluable for organizations to ensure a smooth transition to allow authorized persons in an organization to continue to access the organization's secret data in case of personnel changes or other risk scenarios.

FrostByte, Inc. (a Delaware corporation that has developed the FrostByte mobile app) has already successfully been granted a patent in the United States in April 2022 for its innovative governance framework and encryption technology. FrostByte, Inc. has also filed several similar patents internationally to protect its novel technology.

The patented FrostByte technology has a perfect security track record to date, having secured over US$ 30 million worth of crypto assets for over 3 years. The FrostByte mobile app, which encapsulates the ground-breaking security governance technology in a user-friendly and intuitive form factor of a mobile app, is currently in a public beta and is available for download on both iOS and Android. The FrostByte mobile app will transition to a full public release in early 2023. Users will be able to access and pay for the premium subscription features conventionally in fiat currency on the Apple App Store and the Google Play Store.

The FrostByte mobile app also aims to deliver additional innovation in upcoming iterations of its development with a view to unlocking further functionality for Web 3.0.

DISCOVER US

Introduction

With the ongoing digitalization of private data and the incredible advancements in accessible technology made in recent decades, the importance of data security is greater than ever before. As a consequence of the continuously rising number of digital asset owners worldwide, imperfections and issues with the current standards of digital asset security become quickly evident.

Data theft due to malicious attacks, or loss of assets due to the improper management of data security credentials, is becoming a widely reported and serious problem that is still largely unaddressed by current standard data management practices. These can come with devastating consequences. For example, in one highly publicized case, a San Francisco- based programmer lost the password to his offline storage device leaving him without access to his fortune of **7,002 Bitcoin** (approximate worth: US$330 million).

The case of the deceased **CEO of Quadriga**, Canada&#39;s largest crypto exchange at the time (2019), also exemplifies the shortcomings of having only one individual manage an organizations' digital assets and data, as well as highlighting common problems of hardware wallets and instances where users rely on a third-party custodian. The CEO of Quadriga was reported to have unexpectedly died with approximately US$145 million worth of customers' cryptocurrencies on a hardware wallet that only he had access to, resulting in most of the crypto exchange customers' assets being forever lost. This case demonstrates the difficulties in ensuring access to data, private keys, or other sensitive information in worst-case scenarios.

Because of the rapidly growing adoption of cryptocurrencies and the ever-increasing value of sensitive personal data, providing a suitable solution for data security and governance frameworks to access that secret data is of utmost importance and urgency. Currently, with more than 200 million registered blockchain wallets and a fast-growing hardware wallet market (expected to reach US$8.9bn by 2025), users need a reliable solution to address pain points related to the safe and secure custody and management of secret data. It is, therefore, imperative to offer cryptocurrency owners, whether they are individuals or organizations, and indeed any owner of secret data, a robust yet flexible governance framework to eliminate the risks of allowing others to access that data if and when something untoward should happen to the person managing that data for themselves or others.

Even though different offerings for digital data security have been developed, each has its own shortcomings. When it comes to the management of critical data or secret data, one of the most prominent options is the self-sovereign custody of that data (i.e., putting the security of a user's data in their own hands). Even though some of the widely used hardware wallets (most commonly cold storage devices) have sophisticated encryption algorithms, proper management of cold storage data systems can be cumbersome, especially when it comes to scaling and enterprise needs. To exacerbate the issue, cold storage often results in problems when backing up the secret passphrase securely, often because of incorrect implementation of security protocols or poor security practices. Further, the access and management of the secret data is usually placed in the hands of a single person, whether that person is managing their own secret data or the secret data of an organization. This can result in a single point of failure. Such solutions make no provision for that person to authorize other individuals to access and manage that secret data in the event something unfortunate happens to that person. Even those few solutions which do allow for multi-signature by authorized persons do not allow for rotation or amendment of credentials in the event that something happens to one or more of the authorized signatories. Therefore, as a consequence of these and other shortcomings, secret data can be subject to loss or theft.

To compound the issue further, most hardware wallets are still not compatible with mobile devices and thereby unable to serve the fast-growing mobile adaption of DeFi solutions in the blockchain community.

In addition to self-custody, third-party custody services are also prominent. Here, a customer entrusts a third-party custodian (which uses their own security solution or a cloud-based service) with their data security. All third-party custodian services pose their own security risk, as data is stored on centralized platforms, making it liable to theft or lockout. A user who is reliant on a third-party data custody solution is ultimately at the mercy of that service provider, and will likely suffer serious loss as a consequence of any failure of the security protocols or brute-force hacks of that service provider, or as a consequence of any organizational-related risks (such as insolvency) or personnel-related risks (such as key personnel leaving the organization or something untoward happening to them). A prominent example of the potentially devastating implications of leaving custody of digital assets to another party is the Mt. Gox hack.

Mt. Gox, a crypto exchange and third-party custodian which utilized hot wallet storage, lost over 850,000 bitcoins during the biggest crypto exchange hack to date. Despite the risk, digital asset custody providers are known to charge high annual fees that continue to rise as asset values increase. Moreover, users often face lengthy response times when seeking to access

Similarly, password managers are third-party applications that store and manage your passwords to multiple accounts in an encrypted manner; and users only need to remember one single password to enter and manage their encrypted data vault. Many individuals and organizations rely on password manager applications to help generate and store secret data. Password managers offer superior security to storing passwords locally or in the cloud, but they still have certain disadvantages. If passwords are not encrypted (e.g., the password manager program does not require a password or biometrics to enter), then an attacker with local or remote access to the user's device can still gain access to the secret data. Likewise, if the master password is weak, it is likely to be easily guessed or algorithmically determined, obtained through phishing, or brute-forced if no 2FA is present on the account.

All the previously mentioned data solutions have their limitations and lack an adequate industry-wide standard of safety. Nevertheless, they capture significant customer traffic. This can be explained by the lack of more sophisticated alternatives. The FrostByte app is about to revolutionize the market, with FrostByte's data security offering which allows users to set their risk tolerance to absolute zero, ushering in a new standard for data security.

FrostByte offers offline military-grade encryption and a cold-storage solution by storing the data right on the user's personal device. No secret data of any FrostByte user is ever stored on any FrostByte server or in the cloud. By ensuring that no encrypted data belonging to FrostByte customers is ever kept on networks or servers, customers are protected from increasingly popular phishing attacks. Furthermore, none of the customers' personally identifiable information (PII) is ever tied to FrostByte. In this manner, FrostByte empowers the user to anonymously keep full custody of their secret data, and brings key escrow services in-house, saving the user money while reducing security risks tremendously.

In its offering, FrostByte also enables its customers to choose their bespoke governance frameworks in which users can authorize one or more persons they trust to access their encrypted secret data. (The governance framework functions like a bank account where an account holder is able to select one or more authorized signatories to access their account.) As such, a FrostByte user is able to select a of number authorized persons who will be able to access whichever of the encrypted data vaults the user may from time to time create in the FrostByte app, and thereafter, the user will also select the minimum number from those authorized persons that will be required to unencrypt one or more of the user's encrypted data vaults. The user is entirely free to choose different authorized persons and different minimum numbers from those authorized persons to access different encrypted data vaults that the user creates using the FrostByte app. This gives the user full freedom and full flexibility to design their own security governance frameworks to suit their individual or organizational needs. (The FrostByte governance schema is further explained in the functionality of the app section below.) In this manner, the app allows for secure posthumous access to and transfer of digital assets, encryption keys, account logins, and several other types of digital assets.

FrostByte's patented technology ensures authorized persons can be rotated easily, without the encrypted secret data ever having to be accessed in the process, making this offering innovative and invaluable for individuals and businesses alike, who are concerned about the security of their data (or that of their customers). As such, FrostByte provides a solution to the governance issue of crypto assets for both individuals and organizations. their digital assets which can be frustrating in cases of urgency.

By using FrostByte, even cryptocurrency exchanges or custodians of other people's data can actually provide a better and more secure service offering to their customers, thereby enhancing reliability, governance, and security for the customer and with an organizational view to increase market share and revenue.

In conclusion, FrostByte aspires to combine the best features of a hardware wallet, third-party custodians and password managers into a single product: a decentralized and truly self-sovereign data security mobile app that uses military-grade data encryption in a cold-storage solution with a governance framework.

Business Details

FrostByte has identified shortcomings in the current data security offerings and management practices and has created a superior alternative to the current industry standard. FrostByte's proprietary data security mobile app brings together the highest security standards, accessibility, and flexibility to its customers' needs in one easy to use mobile app on iOS and Android.

FrostByte's mission is to make highly sophisticated data security and governance accessible for everyone. Anyone can securely encrypt to the highest standards most formats of secret data using FrostByte. (The data formats that FrostByte can securely encrypt and allow a user to securely store include login codes, passwords, images, documents, crypto private keys, backup passphrases and others.) FrostByte even allows users to generate strong passwords in-app, which can be used as website login or other passwords by the user. FrostByte thereby also enables users to conveniently generate and use different strong passwords for each web 2 or web 3 service that a FrostByte user may use. Accordingly, FrostByte is the data security mobile app of choice for any individual, small-medium-sized business, or large enterprise. Anyone using cryptocurrencies, managing sensitive data like encryption keys, relying on passwords, providing custody for customer assets, or being involved in any other activity requiring secure and accessible storage of data can find an optimal, robust, and reliable solution in FrostByte. In its offering, FrostByte combines the best features of traditional password managers, paper or hardware wallets, and third-party crypto custodians while going well beyond those services in terms of safety, utility, and ease of use.

FrostByte's unique customer proposition also allows individuals and organizations to safeguard their secret data through the app's sophisticated military-grade encryption and user-defined governance framework, giving the owner complete control over the data and access to it. More specifically, FrostByte's solution stores and protects encrypted data using its innovative Vault tool. The Vaults allow multi-user security and access with various levels of governance applied over a singe piece of secret data or over group of secret digital assets. Vaults are totally customizable to the needs of any person or organization, and allow for easy credential management.

FrostByte is immensely scalable. By way of example, a FrostByte user is able to select up to 256 individuals to be authorized persons and can also select how many of those authorized persons must collectively come together to unlock the secure Vault containing the encrypted secret data. (Whilst it is unlikely that an individual or organization will select up to 256 authorized persons, this maximum number of 256 is referenced here to show the potential of FrostByte.) The app allows huge scalability and shared access to encrypted data. Authorized persons can be rotated easily without ever having to access the secure Vault, allowing for user-friendly and secure applicability, even in large organizations, and avoiding situations where a board may be held to ransom by a disgruntled authorized person on a secure data Vault.

This functionality solves several pain points for the crypto industry and for anyone managing secret data for themselves or for others. By way of example in the case of an individual, a FrostByte user could establish a special posthumous data Vault containing their most secret data (bank account details, crypto backup passphrases, etc.) and have the Vault act as a 'digital will'. Access to that encrypted data Vault could be shared with the user's loved ones or trusted persons, one of whom could include their attorney. Once the owner of the Vault passes away, the loved ones or trusted persons are able to access the encrypted data Vault using their respective passwords along with a password revealed after death by an attorney to unlock the encrypted data Vault.

In the context of businesses and organizations, it is important to account for changes in key personnel (e.g., managers, directors, executives, principals, etc.) due to circumstances such as retirement, termination, or accident. FrostByte provides immense utility to businesses as it allows business owners, managers, or a board of directors to select a number of authorized individuals in the organization to access the secure Vaults containing the organization's sensitive information, private keys, or other secret data belonging to the company or its customers. When a director or manager leaves the organization and new directors are appointed, FrostByte allows the authorized individuals to be changed quickly and easily without requiring the authority of the outgoing director(s) and without ever having to unlock the secure Vault. This functionality is tremendously helpful for businesses (for example crypto exchanges) that custody crypto assets or other sensitive data or digital assets and do not wish to expose these unnecessarily every time a change of authorized personnel is required.

As the fast-evolving crypto and DeFi space is very much unregulated in terms of governance, investors need to know that sophisticated governance mechanisms are in place and their investments are well protected. FrostByte's offering enables crypto start-ups and DeFi businesses to implement such governance mechanisms to provide the highest attainable security their investors deserve, and allows organizations and businesses to bring custody in-house in order to achieve a more effective and affordable alternative to 3rd party custody.

Summary of FrostByte's Key Feature Offering:

Military grade encryption	Cold storage of data	Facilitating governance which is fully customizable to the specific needs of the individual or organization for the management of secret data and digital assets
Facilitating credential management through multiple trusted individuals	Allows for change of trusted individuals without the need to unencrypt the Vault and access the secret data	Replaces the cumbersome and potentially risky use of password managers and unwieldy hardware wallets
Allows for self-sovereign security and thereby provides independence from 3rd party custodians	Can be used to protect customers' secret data and digital assets	Provision for secure offline multiple backups of all encrypted Vaults, a single Vault, or a single digital asset either electronically to another mobile device or by way of printed QR codes
App functionality through web extension		

FrostByte ensures a pleasant user experience through an easy-to-use, carefully designed user interface built mobile-first. Depending on one's needs, users can choose between different utility and pricing options. There is a free version, enabling single password backup and shared backup, providing an accessible option to manage passwords or keys for everyone.

Alternatively, users can elect paid premium features, such as adding multi-password backups and multi-authorized person Vault access. Other features such as YubiKey integration will also be made available to premium users. Furthermore, FrostByte will offer enterprise services, including localized LAN deployment and 24/7 support services. Additionally, to avoid any risks arising from incorrect user implementation, FrostByte will also offer its enterprise customers ancillary implementation services, including data encryption and security strategies, consulting about operational security best practices, and encryption schema support.

The free version of the mobile app will use the same military-grade encryption standard as the premium version, and FrostByte will also provide educational content for better security practices and protocols, so that its individual and corporate users may optimize their use of the FrostByte app and keep their secret data safe.

FrostByte also has a long continued development roadmap for its app, including crypto wallet functionality, Web 3.0 integration, improved governance features and so much more. FrostByte is excited to embark on this journey with a passionate community of users who are concerned about the safety and security of their valuable secret data.

FUNCTIONALITY OF THE

FrostByte App

To provide the aforementioned functionality, FrostByte has developed a proprietary cryptographic key-management solution, which has been successfully patented in the United States in April 2022, and in respect of which international patents in key jurisdictions have already been filed. (It is commonly understood that international jurisdictions will also grant patents to FrostByte on the basis that this has already been granted by the United States.)

The core functionality of the FrostByte app means users can create multiple secure encrypted data Vaults each containing single or several encrypted digital assets belonging to the user. Users can implement an entirely bespoke governance framework to meet their specific needs and circumstances. To ensure that the mobile app has the highest security attainable, the secret data of the user is kept fully in the hands of the user and remains on the device at all times – the secret data is never stored in the cloud or on any centralized server belonging to any third party (including FrostByte). FrostByte never has access to any user inputs or any of the user's secret data. The user is always fully and exclusively in control of their own secret data.

FrostByte also allows for recovery of the encrypted secret data in a disaster event (e.g., the user's mobile device is lot, damaged or stolen, or there has been a tragic accident of the user or an authorized person, or there has been some other access credential loss). The previously introduced multi-user governance access means that the FrostByte mobile app eliminates a common single point of failure. In order to ensure that a user is able to backup their secret data to another mobile device and/or physically, the mobile app allows for the display and printing of QR codes that represent, at the user's choice, all of the encrypted Vaults or a specific encrypted Vault or a specific set of encrypted data that is secured within a Vault. If the user generates and displays those QR codes in the FrostByte app, the user can either share by e-mail or instant messenger those QR codes to another mobile device belonging to the user (by way of electronic backup) or to another device belonging to a trusted person. The user can also print out one or more of such QR codes and keep those physical printouts in a safe place in one or more secure locations by way of redundancy.

The FrostByte app also allows automated key upgrades of completely offline data, thereby being the first software solution to address the cumbersome process of offline key management at scale. To understand how FrostByte provides these services, the following sections will deep-dive into the underlying technology of FrostByte's revolutionary software.

Creation of the Vault Key

A crucial part of the FrostByte encryption and decryption process is generating an offline Vault Key that is specific to the user's governance requirements. The user can create several Vault Keys, each having different governance requirements- that is to say: the user is free to select different authorized persons and different numbers of authorized persons for each Vault Key. The User can decide to use the same Vault Key for one or more encrypted Vaults that the user may create from time to time.

After the user first elects to perform an encryption operation, the graphical user interface of the FrostByte app requires identity credentials from either a single authorized person or multiple authorized persons (N users), depending on the user's desired selection. Once provided with that input, the app instructs the user's device to create a cryptographic Vault Key corresponding to the credentials that have been entered by that authorized person or by those authorized persons. After generating such a key, the app uses the Vault Key to encrypt the secret data (e.g., a password, a login, an image, a document, etc.). Depending on the device, the supported types of user credentials may differ, but the FrostByte app will support electronic biometric data to unlock the app, as well as passwords or passphrases and the planned YubiKey (or similar 2FA device) to unlock the encrypted data Vaults. The option to accept biometric security such as facial recognition or fingerprints to unlock the app enhances the security and ease of use of the application.

Peering under the hood and getting slightly more technical, the FrostByte user might permit a subset of the authorized individuals N (where N>2) to perform decryption operations. Such a subset will further be referred to as Nmin. The Vault Keys may be used to generate encryption keys created from the input of N identity credentials for decryption. The encryption key is configured to only require Nmin, and the sole input of such the Nmin credentials will result in the generation of the encryption key. The encryption key is generated using a cryptographically secure random number generator, generating a 256-bit array. The Vault Key is then split, using the Shamir's Secret Sharing algorithm, into different shards. The shards are encrypted with the blake2b hashes of the passwords input by the authorized individuals N. The encryption key is never entirely stored on the device - it must always be reconstructed from the Nmin required shards. Reconstituting the encryption key may then be accomplished using a secret sharing algorithm and a key derivation function (KDF). Through the FrostByte mobile app, the algorithm then generates the shares of all the N passwords/passphrases according to the subgroup Nmin. Also, the app might use the KDF to derive the Vault Key from at least one share of the passwords/passphrases. The encrypted shards together with the metadata is what forms the Vault Key which can be stored, shared by QR code, etc.

After its generation, the Vault Key may be stored in the hardware memory device for usage and later retrieval. The Vault Key itself may be retrieved and distributed from its local, on-device storage through any means of electronic or physical transfer (e.g., a printed QR code) for additional offline protection or to be shared.

Encryption of data

After creating the Vault Key, the mobile app will proceed to use the Vault Key to encrypt the secret data input by the user.

The standard free tier of the FrostByte app will have more rudimentary encryption methods but will use the same military-grade encryption as the premium feature set. In the free version, encryptions will not use a Vault Key and instead will only be capable of being single-password encrypted using either the default app specified pin code, passphrase at launch, or a user-specified unique passphrase for encryption that is specific only to that particular asset.

The Vault Key is part of the premium feature set of the FrostByte app which becomes available to the user who purchases a FrostByte subscription on the Apple App Store (for iOS) or the Google Play Store (for Android)

The Vault Key is used as a capacitive input before performing the encryption and decryption operations. Even if an undesirable third party gains access to the encrypted backup data, this will remain incomprehensible without the Vault Key.

After being encrypted, data is to be stored in the processor's cache memory or on the hardware memory of the device. Also, the encrypted data can be retrieved, displayed, or communicated from the device in any digital or physical representation of choice.

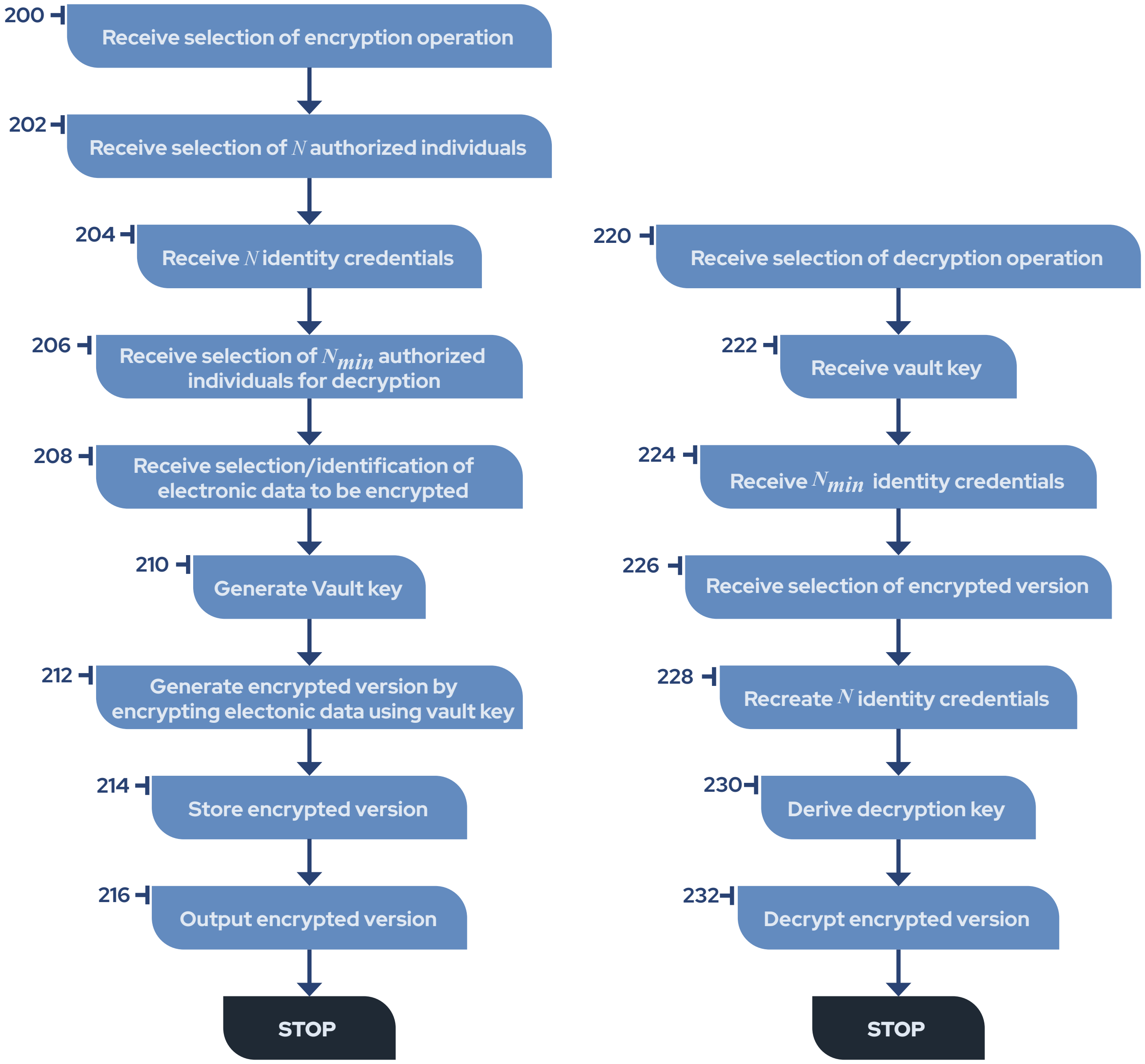
Storage

All data is stored on-device only. Even though the hardware memory may contain Vault Key, encrypted data, identity credentials or more, the information may be stored in separate hierarchical file structures and/or hardware portions. Furthermore, access will be limited strictly by hardware and/or software flags to grant access, retrieval, and usage only to the FrostByte app. The data, except for small pieces of metadata like Vault names and Vault Key names, will be stored in encrypted from on the mobile device. Such data will be easily exportable and importable for FrostByte users via QR Codes. To solve enterprise pain points with offline key management, the app allows for multi-user encryption/decryption credential management of offline assets, where the encrypted version can be stored offline, separate from the decryption credential sets. With no centralized or local database for users or passwords, FrostByte enables all the benefits of centralized credential management in a decentralized manner without conventional risks. Moreover, all credential management and data encryption can be processed offline.

Decryption of data

When any of the *N* authorized individuals desire to perform a decryption operation, the user will first need to input the Vault Key into the FrostByte mobile app. If the Vault Key is accepted, the app can proceed with the decryption process. The app collects passwords for m Vault Key shards as required, and decrypts them using the provided user passwords. Once decrypted, the shards are combined and the whole vault-key string is re-created from the m of n shards via Shamir's Secret Sharing algorithm. The re-created original 256-bit vault key string is then used to decrypt the selected secret data.

The following two flowcharts provide a graphical representation of the data encryption and decryption process.


200
Receive selection of encryption operation
202
Receive selection of N authorized individuals
204
Receive N identity credentials
206
Receive selection of N_{min} authorized individuals for decryption
208
Receive selection/identification of electronic data to be encrypted
210
Generate Vault key
212
Generate encrypted version by encrypting electonic data using vault key
214
Store encrypted version
216
Output encrypted version
STOP
220
Receive selection of decryption operation
222
Receive vault key
224
Receive N_{min} identity credentials
226
Receive selection of encrypted version
228
Recreate N identity credentials
230
Derive decryption key
232
Decrypt encrypted version
STOP

FUTURE PROPOSED BLOCKCHAIN INTEGRATION

The founders of FrostByte, Inc. are all aligned with the ideals of decentralization and Web 3.0, and as such, began the creation of FrostByte in 2018 to solve one of the biggest pain-points of the crypto community: self-sovereign custody of digital assets in a user-friendly and secure manner with a governance framework.

The value of crypto assets and other digital assets comprises seed phrases or private keys, and by adequately securing the secrecy of these, the value of crypto assets and other digital assets can be safeguarded. However, as a general principle, all secret data has value for the owner of that data, and that data must be kept secret and under the control of the owner in order to preserve the value of that data for the owner. The solution that the FrostByte founders of embarked upon to bring to the crypto industry therefore also applies equally to all valuable and secret data. As such, the application of FrostByte technology therefore has far reaching application and utility beyond the confines of the crypto industry.

Whilst our go-to-market is the crypto industry, our mobile app will be available for anyone within or outside the crypto community to download on the Apple App Store (for iOS) and the Google Play Store (for Android) because we recognize that non-crypto users will also find FrostByte tremendously useful. It becomes quickly apparent that FrostByte's innovative and patented technology has widespread application and also can replace conventional password managers. Therefore, non-crypto users who wish to use FrostByte as a password manager will be able to access the premium feature set of the FrostByte mobile app by conventionally paying a monthly or annual subscription fee using fiat currency on the Apple App Store or the Google Play Store.

Notwithstanding the above, given our roots of the founders of FrostByte Inc. and their affiliation with Web 3.0 values, it was impossible for them not to address the specific usage of the ground-breaking data security app by the global crypto community. We have therefore decided to progress the issue of a blockchain token through a non-US partner company, where it is envisaged that such token would confer additional utility to those FrostByte users who seek to access the premium feature set of the FrostByte mobile app by paying for the subscription using such tokens. Further details will follow in due course.