FrostByte

FROSTBYTE, INC. | WHITE PAPER 2022

Redefining Risk Tolerance in Data Security

www.frostbyte.app

TABLE OF

Content

Executive Summary 3

Introduction 4
- Business Details 6
- Functionality of the FrostByte App 8
  - The Vault Key 9
  - Encryption of data 10
  - Storage 10
  - Decryption of data 11

Tokenomics 12
- Staking 12
- Token Utility 12
- Token Distribution 13

FrostByte: Underlying Blockchain Technology 14

Roadmap 15

Team 16

Legal terms, Conditions, Considerations, Risks & Disclaimers 17

Executive Summary

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

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

Frostbyte's customizable governance structure enables individuals to nominate additional trusted persons to access their secret encrypted data, in case of unforeseen events where the loss of credentials could be a critical hindrance (e.g., a loved one may access the crypto assets of a deceased relative). Furthermore, a flexible and secure governance framework is invaluable for organizations to allow for smooth transferrable access to data for organization members in case of personnel changes.

This is where FrostByte delivers innovation. FrostByte will enable its community to store and access encrypted data on the blockchain using $FROST tokens. The $FROST token also enables users to unlock access to FrostByte premium in-app features, and receive staking rewards. Currently, FrostByte has filed US and international patents for its technology and has a perfect security track record to date. Following an IDO raise, FrostByte will launch its application for both iOS and Android to beta testers, and shortly after through a full public release.

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 evident.

Data theft due to malicious attacks, or loss of assets due to the improper management of credentials, is becoming a widely reported 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 such as a San Francisco-based programmer, who lost the password to his offline storage device, leaving him without access to his fortune of **7,002 Bitcoin** (approximate worth: US$330 million in 2022). Because of the rapidly growing adoption of cryptocurrencies, providing a suitable solution for data security and governance frameworks to access that secured data is of utmost 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 for these pain points.

Even though different offerings for digital data security have been developed, each has its shortcomings. When it comes to critical data management, one of the most prominent options is the self-custody of data. Even though some of the widely used hardware wallets (most commonly cold storage devices) have sophisticated encryption algorithms, proper cold storage of data 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, often because of 3 incorrect implementation of security protocols or poor security practices. Therefore, secret data can be subject to loss or theft.

To compound this 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 or a cloud server with their data security. However, these services impose security threats, as data is stored on centralized platforms, making it liable to theft or lockout. 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 in cases of urgent issues. The case of the deceased **CEO of Quadriga**, Canada's largest crypto exchange at the time (2019), exemplifies the shortcomings of both hardware wallets and third-party custody. The CEO 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 customers' assets being forever lost. That case demonstrates the difficulties in ensuring access to data, private keys, or other sensitive information in worst-case scenarios with the previously described forms of custody. It is, therefore, crucial to offer cryptocurrency owners 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.

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 vault. Many individuals and organizations rely on password manager applications to help generate secure passwords. 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 to enter), then an attacker can still gain access with local access to the machine. Likewise, if the master password is weak, it is likely to be easily guessed, 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. FrostByte is about to revolutionize the market, with FrostByte's data security offering allowing users to set their risk tolerance to absolute zero, bringing in a new standard for data security.

FrostByte offers offline military-grade encryption services by storing the data right on the user's personal device. By not keeping any encrypted data on networks or servers, customers are protected from increasingly popular phishing attacks. Furthermore, none of the customers' personally identifiable information (PII) is tied to FrostByte. Thereby, FrostByte empowers the user to anonymously keep full custody, and bring key escrow services in-house, saving the user money while reducing risks tremendously. In its offering, FrostByte 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.

After a user selects their authorized persons, they are also able to choose a minimum number from those authorized persons that will be required to unencrypt the Vault which secures the user's encrypted secret data. (This 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. 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 with data security. As such, FrostByte provides a solution to the governance issue of crypto assets for both individuals and organizations. In conclusion, FrostByte aspires to bring the best features of a hardware wallet, third-party custodians, and password managers combined in one product: A decentralized and truly self-sovereign data security mobile app.

Business Details

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

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 sensitive data using FrostByte (whether that sensitive data is a login code, a password, an image, a document, private keys, backup passphrases or other formats). 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 is allowing individuals or organizations to safeguard sensitive data through its sophisticated security service and a 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 various levels of governance applied over a set or group of 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 can 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. This allows huge scalability and shared access to encrypted data. These 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.

This functionality solves several pain points for the crypto industry. For an individual example, a FrostByte user could establish a special posthumous vault acting as a 'digital will', and share encrypted data with nominated loved ones. Once the owner of the vault is deceased, the loved ones entrusted with assets could use their passwords along with the password revealed after death by an attorney to unlock the vault. In the case of the previously mentioned crypto millionaire, had he been a FrostByte user and would have nominated his immediate family as authorized persons, his family would have been able to access his crypto wealth after his death.

In the context of businesses and organizations, it is important to account for changes in personnel in key roles (e.g., managers, directors, executives, principals, etc.) due to circumstances such as retirement, termination, or accidents. FrostByte provides immense utility to businesses as it allows business owners, managers, or a board of directors to select a number of authorized individuals to access the secure Vault containing the secret data, 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.

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

Individuals	Small-Medium sized businesses	Enterprises
Military grade encryption of any kind of data	Military grade encryption of any kind of data	Military grade encryption of any kind of data
Ease the management of digital assets	Ease the management of digital assets	Ease the management ofdigital assets
Replaces the cumbersome and potentially risky use of password managers and hardware wallets	Protecting customers digital assets	Governance adaptable to the specific needs of the organization
Facilitate credential management with trusted individuals	Self-sovereign security	Independence from 3rd party custodians

Frostbyte ensures a pleasant user experience through an easy-to-use, carefully designed user interface built mobile-first. Depending on one's needs, the 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, military-grade data security, 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.

FUNCTIONALITY OF THE

FrostByte App

To provide the aforementioned utilities, FrostByte has developed a proprietary cryptographic key management solution, which is currently patent-pending in the US and internationally.

FrostByte's app delivers a core functionality: Users can create secure encrypted multiple data Vaults each containing several encrypted digital assets belonging to the user, deposit and encrypt their secret data, and access it within a governance framework of their bespoke design. 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 – the secret data is never stored in the cloud or on any centralized server belonging to a third party. FrostByte never has access to any user inputs or any of the user's secret data. The user is in control of their own secret data, and is in full control of the encryption schema and delegation of keyholders.

FrostByte's software also allows for recovery of the encrypted secret data in a disaster event (e.g., a tragedy or team member/credential loss). The previously introduced multi-user governance access means that the FrostByte mobile app eliminates a common single point of failure. In addition, the mobile app allows for the display and printing of QR codes that represent, at the user's choice, access keys to the encrypted Vault and/or to the encrypted data itself that is secured within the Vault, being the best way to share such QR codes. The mobile 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 section will deep-dive into the underlying technology of FrostByte's software.

Firstly, if a user desires to encrypt data, one will need to access the FrostByte mobile app, which can be obtained from various online sources (available on iOS and Android). Multiple gating and security processes ensure the sophisticated utility provided by FrostByte, which is described in the following paragraphs.

The Vault Key

A crucial part of the encryption process is generating an offline Vault Key specific to the user and data. After the user first elects to perform an encryption operation, the graphical user interface of the Frostbyte mobile app requires identity credentials from either the single or multiple authorized persons (N users), depending on the user's 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. After generating such a key, the app uses the Vault Key to encrypt the secret data. 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) 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 a little more, the FrostByte user might permit a subset of the authorized individuals $N\ (N>2)$ 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. Vault Key is configured to only require $Nmin$, the sole input of such the $Nmin$ credentials will result in the generation of the Vault Key. Generating the Vault 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. 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.

Encryption of data

After creating the Vault Key, the mobile app may encrypt the data. The standard free tier will have more rudimentary encryption methods.

Here, encryptions will be single password encrypted using either the default app specified pin code, passphrase at launch, or the user can specify a unique passphrase for encryption, specific only to that particular asset. The Vault Key is part of the premium tier and can be unlocked by purchasing a subscription conventionally via app store, or by staking at least 1,000 FROST tokens, which is further elaborated on in the tokenomics section below. The Vault Key is used as a capacitive input before performing the encryption operations. In doing so, the app either requires the user to access the Vault Keys storage location on the device or physically present the Vault Key by scanning its corresponding physical representation (e.g., a QR code). Once the Vault Key is verified, the app will require that some or all the N authorized individuals provide their encryption credentials (passwords to their shards). Then, the software may call or involve an encryption algorithm, using the Vault Key as an encryption parameter. For its encryption operation, the XSalsa20 encryption algorithm may be used. Even if rogue entities gain access to backup data, such remains incomprehensible without the encryption credentials. The encryption operation may also use the scrypt algorithm to derive the encryption key from any one or more of the N or the Nmin passwords/passphrases. The scrypt algorithm is a well-known slow hashing algorithm, making it infeasible for attackers to discover the decryption key by brute force. 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.

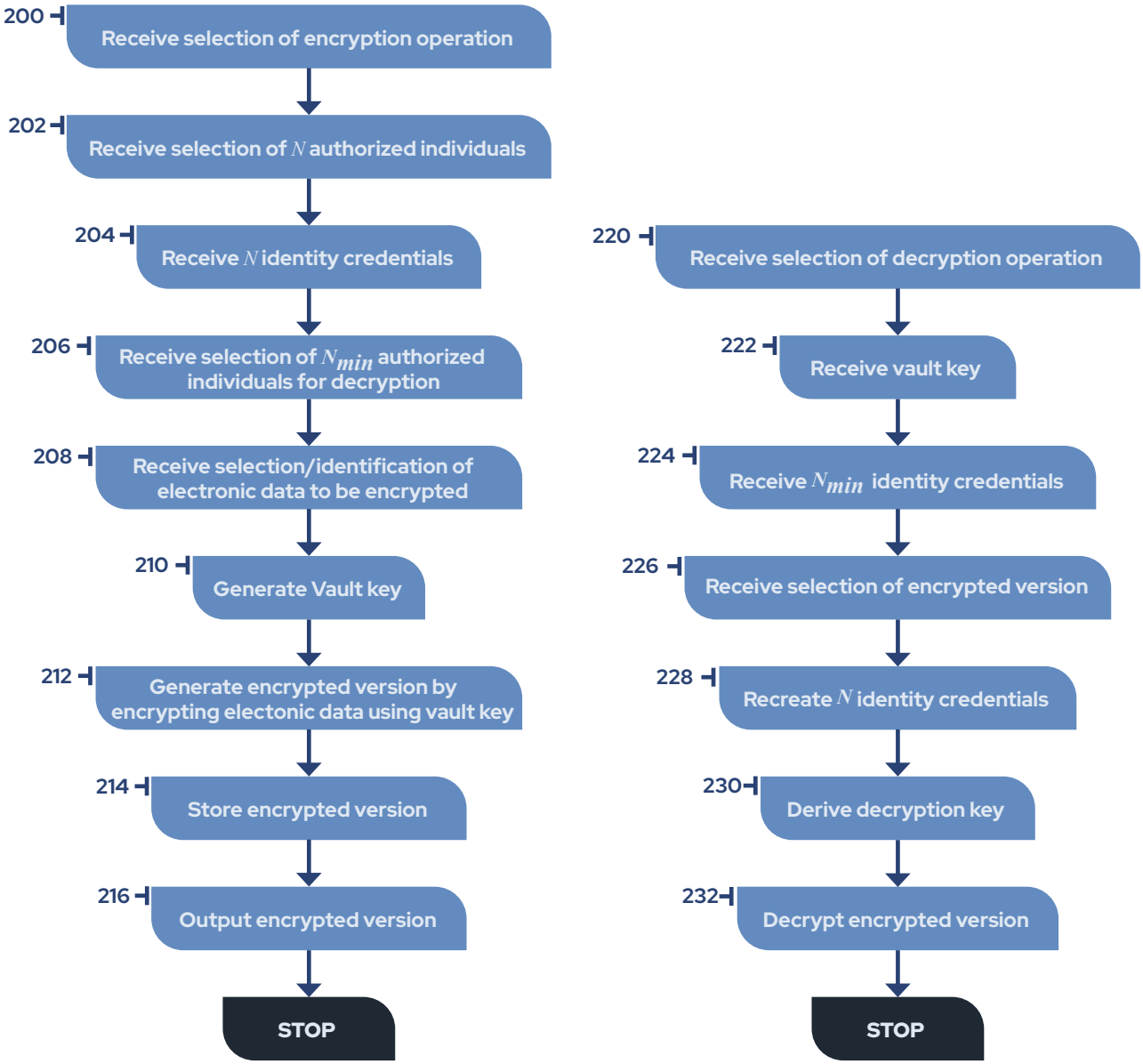
Storage

All data is stored on the device. 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 encrypted. 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, separated from the decryption credential sets. With no centralized or local database for users or passwords, FrostByte enables all the benefits of centralized credential management 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 may 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 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 asset.

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



Tokenomics

STAKING

FROST will initially be issued as an ERC-20 token on the Ethereum blockchain. Frostbyte will enable holders of its native FROST token to stake tokens to receive rewards tokens, incentivizing the long-term membership token holders in the Frost community. In the early weeks and months after the launch of the FROST token, this is especially important to support the price of the FROST token by limiting the available supply on secondary markets. Furthermore, this incentivizes ongoing long-term value appreciation.

FrostByte will allocate a total number of FROST tokens from its Community Reserves towards staking rewards. That means that a fixed number of FROST tokens will be available for each block as reward tokens at the end of each block to those users who stake FROST tokens for a continuous number of blocks. It is planned that during the early blocks after issuance of the token, the number of reward FROST tokens received by each user staking FROST tokens will be higher than later blocks as the number of users staking FROST tokens grows. Also, the algorithm distributing FROST token rewards per block will keep track of the total period for which FROST tokens have remained staked. To further reward the loyalty of our FROST token holders who continue staking their FROST tokens for longer, the algorithm will reward those users with more reward tokens.

FrostByte will, during the early days following the issuance of FROST tokens and at later stages of mobile app development and maturity of the user community, undertake a series of marketing and community building initiatives and bounty programs around the FROST token. These initiatives and programs will be designed to grow and strengthen the user community of the FrostByte mobile app and thereby ensure that a growing number of investors and holders of digital assets and sensitive data can safely and robustly secure those assets and data. At the same time, all of these initiatives will also support the utility of the FROST token.

As with all staking programmes, it is expected that staking rewards will be higher initially and will decrease over time, but given the above staking mechanics, users who stake their FROST tokens early and for onger periods of time will receive proportionally higher rewards.

TOKEN UTILITY

As a core utility of our FROST native token, the token will function as access to the premium features of our FrostByte mobile app. As stated above, the premium features include Vault creation with multiple authorized individuals, YubiKey support, and many other top-tier features.

FrostByte's innovative technology has far-reaching utility beyond the crypto industry and can replace conventional password managers. However, while our core and immediate focus is the crypto industry, our mobile app will be available for anyone to download on the Apple App Store for iOS and the Google Play Store for Android. As such, conventional users will be able to pay a monthly or annual subscription to access the premium features of the mobile app.

To give utility to the FROST token, the premium features of the mobile app will be accessible to every FROST token holder, who stakes at least 1,000 FROST tokens. (FrostByte may in due course consider changing the number of tokens to be staked in the event of price fluctuations of the FROST token.) The premium features will stay free for as long as the required number of FROST tokens remain staked. This could lead to lifetime premium-feature access. Additionally, staking will lead to holders receiving reward FROST tokens. The staking rewards can be staked to earn even more rewards or sold on the secondary market to allow new users of the FrostByte mobile app into the token economics model. We plan to make the

FROST token a core proposition around the continued growth and development of the FrostByte mobile app.

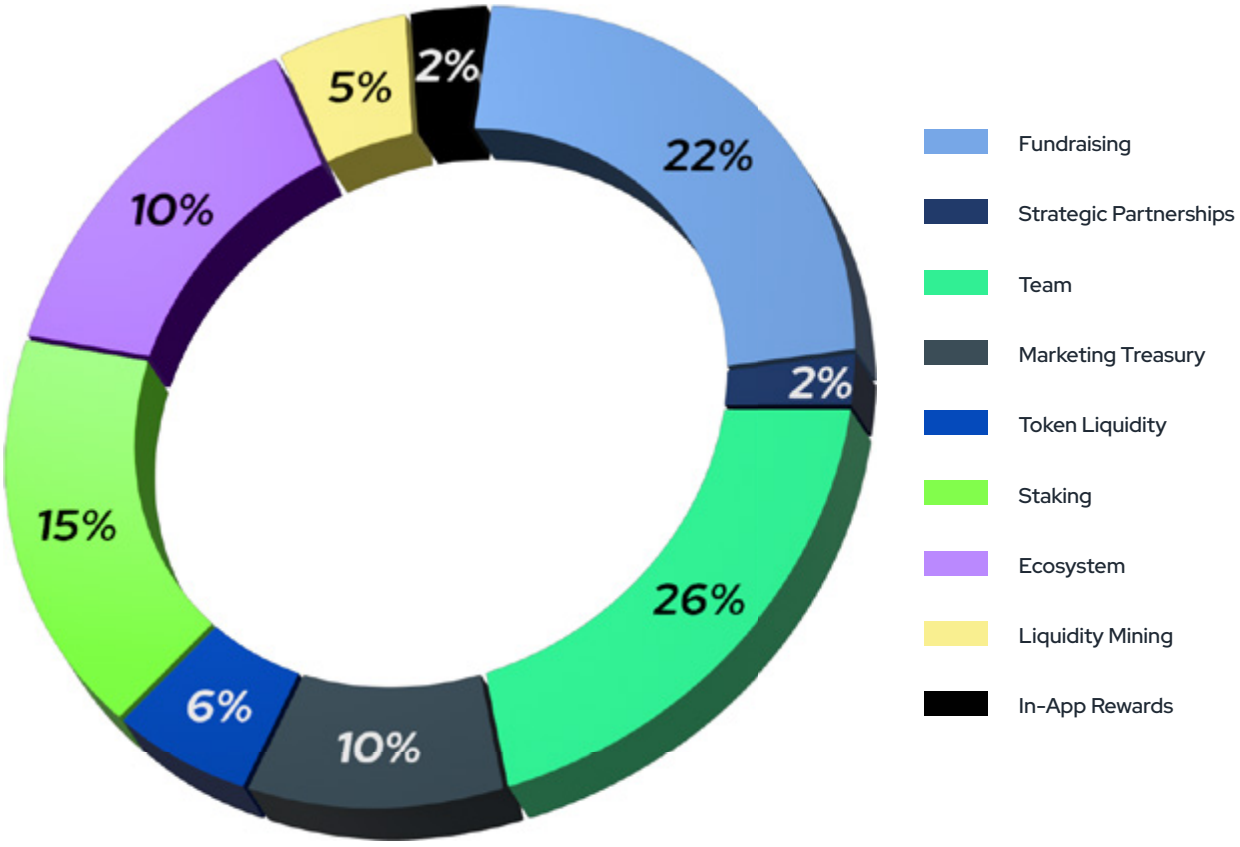
An example of the future utility of the FROST token will be to enable users to utilize the FROST tokens as a payment method for fees arising from all transactions involving FROST tokens. This utility is available on other blockchains, such as Cardano, which FrostByte may consider migrating to in the future. This would allow using native tokens as a currency for transaction fees contrary to other layer one applications.

Furthermore, the FROST token will be able to function as a payment method when users want to read or write encrypted Vault data on the blockchain, acting as a "decentralized cloud backup" of sensitive data.. FrostByte will charge a token based fee when users want to back up their encrypted secret data to or read their previously backed-up encrypted secret data from a decentralized file storage system. Part or all of the fees charged will be used to continue to reward those users who stake their FROST tokens.

TOKEN DISTRIBUTION

As demonstrated above, the FROST token is a central pillar of the FrostByte mobile app utility. To ensure a healthy and stable ecosystem, we have implemented an eighteen-month vesting period for investors and a thirty-six-month vesting period for the team. Furthermore, over one-fourth of the tokens are part of an Ecosystem-Development-Fund that will ensure that the ecosystem continues to thrive and grow in the manner set out above.

The FrostByte team will also assist liquidity pools and implement treasury management to ensure a responsible, long-lasting, and healthy token ecosystem that supports a thriving, vibrant and ever-growing community of FrostByte users.



FROSTBYTE:

Underlying Blockchain Technology

After careful consideration, FrostByte has chosen to deploy as a blockchain agnostic application, focusing on those blockchain protocols which deliver the greatest security guarantees in line with our overarching philosophy.

FROST will initially be launched as an ERC-20 token on Ethereum, and our components will be initially launched on the Ethereum blockchain—currently the most used and recognized smart contract blockchain. Eventually, Frostbyte will also explore deploying on other ecosystems, once they have smart contract functionality and have been fully proven as a viable alternative to Ethereum.

FrostByte is looking forward to building an active and engaged community. As trust and satisfaction of the community lie at the core of any Blockchain project, FrostByte is committed to ensuring the highest possible satisfaction of members in the Frost ecosystem. To do so, Frostbyte welcomes community feedback, suggestions and wishes regarding the app and services to meet the demands of its community.

Furthermore, the FROST token has the greatest benefits for the community at heart. Through the staking, premium access and token reward functionality, FrostByte stipulates organic community growth. Bringing a community centered focus, business model and token design together, FrostByte looks forward to developing an active and growing community centered around the best possible data security.

Roadmap

FrostByte has conducted an extensive research and development phase, lasting from 2018 and 2020.

FrostByte has already been used to secure over US$30 million of crypto assets and has a perfect security track record to date. FrostByte has created a technology that finally satisfies the consumer demand for combining the most advanced features of data security services bound into one convenient and easy-to-use mobile app. The FrostByte team has developed a fully functional mobile app with US and international patents pending.

The next stage of FrostByte will be its deployment of blockchain feature integration into the app. To facilitate this, Q4 of 2021 through to Q1 of 2022 will host our seed and private round for sales of the FROST token to secure funding. The initial decentralized offering (IDO) of the FROST utility token through a number of decentralized launchpads will follow in Q2 of 2022. The FrostByte source code will receive external auditing as well to ensure the highest possible security. Soon after our IDO and audit, the FrostByte mobile app for IOS and Android will become available for public use following a closed beta. FrostByte will also implement additional utilities to grow and strengthen its community through a variety of community engagement programs or incentive and bounty programs. FrostByte intends to enable its staking and liquidity mining operations very shortly after its initial token offering.

FrostByte will then roll out further utilities for their token holders like premium access, as discussed in detail in the Tokenomics section of this whitepaper. In 2023, we aspire to release a dedicated enterprise version of our mobile app, as well as white glove enterprise deployments and support services. Future builds are also planned for 2023 and beyond to bring exciting and cutting-edge functionality to the mobile app, which will enhance FrostByte's UI/UX to make it the premier go-to data security manager globally.

FROSTBYTE

The Team

CEO Co-Founder:
Saul Schwartzbach
saul@frostbyte.app

COO Co-Founder:
Nate Johnston
nathan@frostbyte.app

CSO Co-Founder:
Vikram Nagrani
vikram@frostbyte.app

CTO:
Parker McCurley
parker@decentlabs.io

Developer:
Ransom Christofferson
ransoing@gmail.com

Advisor:
Ivan Gowan
ivangowan@gmail.com

Advisor:
David Johnston
david@dltx.com

LEGAL TERMS, CONDITIONS, CONSIDERATIONS, RISKS AND DISCLAIMERS

IMPORTANT NOTICE: PLEASE READ THE ENTIRETY OF THIS WHITE PAPER, TOGETHER WITH THE LEGAL TERMS, CONDITIONS, CONSIDERATIONS, RISKS AND DISCLAIMERS DOCUMENT AVAILABLE ON https://frostbyte.app. WE RECOMMEND YOU CONSULT A LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S) OR EXPERTS FOR FURTHER GUIDANCE PRIOR TO PARTICIPATING IN THE FROSTBYTE INITIAL DECENTRALIZED TOKEN OFFERING. YOU ARE STRONGLY ADVISED TO TAKE INDEPENDENT LEGAL ADVICE IN RESPECT OF THE LEGALITY IN YOUR JURISDICTION OF YOUR PARTICIPATION IN THE FROSTBYTE INITIAL DECENTRALIZED TOKEN OFFERING. YOU SHOULD NOTE THAT YOUR YOUR PARTICIPATION IN THE FROSTBYTE INITIAL DECENTRALIZED TOKEN OFFERING SHALL BE DEEMED TO CONSTITUTE YOUR ACKNOWLEDGEMENT AND ACCEPTANCE OF THE LEGAL TERMS, CONDITIONS, CONSIDERATIONS, RISKS AND DISCLAIMERS DOCUMENT AVAILABLE ON https://frostbyte.app AND YOUR REPRESENTATION THAT YOU HAVE SOUGHT PRIOR INDEPENDENT LEGAL ADVICE.

Please note that this is a summary of the Legal Terms, Conditions, Considerations, Risks and Disclaimers Document, the full version of which can be found on: https://frostbyte.app (the "Website"), and which you must read in full before (i) making use of this White Paper and any and all information available on the website(s) of FrostByte Technology OÜ (the "Company") and/or (ii) participating in the Company's Initial Decentralized Token Offering outlined in this White Paper (the "IDO"). Any undefined capitalized terms below shall have the meaning set out in the Legal Terms, Conditions, Considerations, Risks and Disclaimers Document.

This summary should not be relied on in place of reading the Legal Considerations, Risks and Disclaimer Document in full. The contents of the Legal Terms, Conditions, Considerations, Risks and Disclaimers Document outlines, amongst other things, certain legal matters which you should consider, certain risks and disclaimers applicable to the IDO and, certain terms and conditions applicable to you in connection with: (i) your use of this White Paper and of any and all information available on the Website; and/or (ii) your participation in the IDO, in each case in addition to any other terms and conditions that we may publish from time to time relating to this White Paper, the Website and the IDO and which may be applicable to your participation in the IDO. The full Legal Terms, Conditions, Considerations, Risks and Disclaimers Document forms part of the White Paper event though it is presented as a separate paper. It is intended to and must be read in conjunction with the White Paper.

The information set forth in the Legal Terms, Conditions, Considerations, Risks and Disclaimers Document may not be exhaustive and does not imply any elements of a contractual relationship unless expressly provided. While we make every reasonable effort to ensure that all information: (i) in this White Paper; and (ii) the Available Information (as such term is defined in the Legal Terms, Conditions, Considerations, Risks and Disclaimers Document) is accurate and up to date, such material in no way constitutes professional advice.

The Company does not recommend purchasing Tokens (as such term is defined in the Legal Terms, Conditions, Considerations, Risks and Disclaimers Document) for speculative investment purposes. Tokens do not entitle you to any equity, governance, voting or similar right or entitlement in the Company or in any of its affiliated companies. Tokens are sold as digital assets, similar to downloadable software, digital music and the like. The Company does not recommend that you purchase Tokens unless you have prior experience with cryptographic tokens, blockchain-based software and distributed ledger technology and unless you have first taken independent professional advice with respect to the Available Information, Legal Terms, Conditions, Considerations, Risks and Disclaimers Document and the IDO.

Citizens, nationals, residents (tax or otherwise) and/or green card holders of each of: (i) People's Republic of China; (ii) Afghanistan; (iii) Bosnia and Herzegovina; (iv) Central African Republic; (v) Cuba; (vi) Democratic Republic of Congo; (vii) Democratic People's Republic of Korea; (viii) Eritrea; (ix) Ethiopia; (x) Guinea-(xi) Bissau; (xii) Iran; (xiii) Iraq; (xiv) Israel; (xv) Libya; (xvi) Lebanon; (xvii) Somalia; (xviii) South Sudan; (xix) Sudan; (xx) Syria; (xxi) Uganda; (xxii) United States of America; (xxiii) Vanuatu; (xxiv) Yemen; and (xxv) any other jurisdiction which prohibits or requires any supervision oversight licensing regulatory compliance legal compliance and/or prior approval from any regulatory (or similar) authority or body or form any monetary or securities body or authority for:

a. the possession, dissemination or communication of the Available Information; and/or

b. the participation in the IDO and/or the purchase of Tokens and/or the offer for sale of the Tokens or any similar activity or product,

or any other Restricted Persons (as such term is defined in the Legal Terms, Conditions, Considerations, Risks and Disclaimers Document) are not permitted to participate in the IDO.

In no event shall the Company and/or its Affiliates (as such term is defined in the Legal Terms, Conditions, Considerations, Risks and Disclaimers Document) be liable for the Excluded Liability Matters (as such term is defined in the Legal Terms, Conditions, Considerations, Risks and Disclaimers Document).

The Company does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking made or alleged to be made by the Company in any form whatsoever to any entity or person.

You should carefully consider and evaluate each of the risk factors and all other information contained in the Legal Terms, Conditions, Considerations, Risks and Disclaimers Document before deciding to participate in the IDO.

YOU MAY LOSE ALL MONIES THAT YOU SPEND PURCHASING TOKENS. IN THE EVENT THAT YOU PURCHASE TOKENS, YOUR PURCHASE CANNOT BE REFUNDED OR EXCHANGED.

THERE IS NO GUARANTEE THAT THE UTILITY OF THE TOKENS OR THE PROJECT ENVISAGED IN THIS WHITE PAPER WILL ACTUALLY BE DELIVERED OR REALIZED.

YOU ARE WAIVING YOUR RIGHTS BY AGREEING TO LEGAL TERMS, CONDITIONS, CONSIDERATIONS, RISKS AND DISCLAIMERS DOCUMENT AND PARTICIPATING IN THE IDO. BY PARTICIPATING IN THE IDO YOU ARE AGREEING TO HAVE NO RECOURSE, CLAIM, ACTION, JUDGMENT OR REMEDY AGAINST FROSTBYTE TECHNOLOGY OÜ IF THE UTILITY OF THE TOKENS OR IF THE PROJECT DESCRIBED IN THIS WHITE PAPER IS NOT DELIVERED OR REALIZED IN FULL.

IF YOU ARE UNCERTAIN AS TO ANYTHING IN THIS WHITE PAPER OR YOU ARE NOT PREPARED TO LOSE ALL MONIES THAT YOU SPEND PURCHASING TOKENS, **WE STRONGLY URGE YOU NOT TO PURCHASE ANY TOKENS.**

TOKENS ARE NOT SHARES OR SECURITIES OF ANY TYPE. THEY DO NOT ENTITLE YOU TO ANY OWNERSHIP OR OTHER INTEREST IN FROSTBYTE TECHNOLOGY OÜ. THEY ARE MERELY A MEANS BY WHICH YOU MAY BE ABLE TO UTILIZE THE PLATFORM. THERE IS NO GUARANTEE THAT THE PLATFORM WILL ACTUALLY BE DEVELOPED IN THE MANNER WHICH IS DESCRIBED IN THE AVAILABLE INFORMATION.

PLEASE READ THE ENTIRETY OF THE LEGAL TERMS, CONDITIONS, CONSIDERATIONS, RISKS AND DISCLAIMERS DOCUMENT CAREFULLY. In the event of any conflict or inconsistency between the entire Legal Terms, Conditions, Considerations, Risks and Disclaimers Document and this summary, the entire Legal Terms, Conditions, Considerations, Risks and Disclaimers Document shall prevail.