FrostByte

"Absolute zero: The new risk tolerance standard in data security"

Whitepaper

Nov 8, 2021

Table of Contents

Executive Summary

Issues in critical data management have 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 sets the risk tolerance to an absolute zero: The FrostByte app allows customizable data governance while providing military grade encryption and security. The customizable governance structure enables individuals to nominate trusted persons to access their data in case of untoward events where the loss of credentials has been a critical hindrance to this date. Furthermore, flexible and secure governance is invaluable for organizations to allow for smooth transferrable access to data for organization members in case of personnel changes.

FrostByte is offering these services with a view to fully deploying on Cardano, aligning with Cardano's mission and utility. FrostByte will enable its community to settle blockchain transactions to back up data with Frost native tokens. Also, the Frost token allows users to gain access to FrostByte premium features and to receive staking rewards. Currently, FrostBytes technology is being patented after having a perfect security track record. After securing funding and an IDO through OCCAM.fi, FrostByte will launch its application on the Cardano blockchain once the network is fully operational and tested, but only as an interim measure FrostByte may consider launching its token on another fast and low transaction network.

Introduction

With ongoing digitalization and the incredible advancements technology made in the 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 known problem that is still largely unaddressed by current standard data management practices. These can come with devastating consequences, as in the case of the 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 October 2021). 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 to their 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 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. To exacerbate the issue, cold storage often results in problems when backing up the secret passphrase, often because of incorrect implementation of security protocols or bad security practices. Therefore, secret data can be subject to loss or theft. Furthermore, 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. Besides self-custody, third-party custody services are prominent. Here, a customer entrusts a third-party custodian or a cloud server with his 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 third-party custodian who 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. Here, the case of the deceased CEO of Quadriga, Canada's largest crypto exchange at the time (2019), visualizes the shortcomings of both hardware wallets and third-party custody. The CEO unexpectedly died with approximately US$145 million worth of cryptocurrencies on a hardware wallet that only he had access to, resulting in most of the investor's assets becoming entirely inaccessible. That case exemplifies 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.

Lastly, another widely used data security service are password manager applications, which generate and store passwords and other sensitive information for users. This practice of digital asset management comes with security concerns as well. As sensitive data is most often stored in the cloud, providing more surface for attacks than cold storage options. Still, digital password managers enjoy more than 27 million users at the point of writing. All the previously mentioned data solutions certainly have their downsides 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 this market: FrostByte's data security offering sets an absolute zero risk tolerance as the new standard for data security.

FrostByte offers offline military-grade encryption services by storing the data right on the user's personal devices. 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 keep custody and key escrow services in-house, saving the user money while reducing risks tremendously. In its offering, FrostByte enables its customers to choose their governance frameworks in which users can select which authorized persons can access the encrypted secret data. After selection, a minimum number of authorized persons is going to be required to authorize the decryption of a Vault. This schema is further explained in the functionality of the app section. In doing so, 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 realised the shortcomings in the current data security offering and management practises and has created a superior alternative to the current standards. Its 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 any format of secret data using FrostByte (whether that secret data is a login code, a password, an image, a document, private keys, backup passphrases or anything else). 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 finds an optimal, robust and reliable solution in FrostByte. In its offering, FrostByte combines the best features of traditional password managers, hardware storage and third-party crypto custodians while going well beyond those services in terms of safety and utility.

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. As the app allows for multi-person access, the service is adaptable to one's personal, or any organization’s specific governance needs.

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 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 big pain points for the crypto industry. For an individual's use case, a FrostByte user can nominate family and friends to be authorized persons and select a number of them to come together and access the user's mobile phone to unlock the secure Vault and unencrypt the user's secret data (private keys, etc.). The ability for the FrostByte user to allow such access to authorized persons is invaluable if something untoward happens to the user. 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 has immense utility for businesses as it allows the business owners, managers, or board of directors to select individuals matching their use case to access the secure Vault containing the secret data, private keys, or else 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 and without ever having to unlock the secure Vault. This functionality is tremendously helpful for businesses that custody crypto assets or other sensitive data (for example crypto exchanges).

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.

Summarized Key Offering of FrostByte

Individuals

- Military grade encryption of any kind of data
- Ease management of digital assets
- Replaces the cumbersome and potentially risky use of password managers and hardware wallets
- Facilitate credential management with trusted individuals

Small-Medium sized businesses

- Military grade encryption of any kind of data
- Ease management of digital assets
- Protecting customer's digital assets
- Self-sovereign security

Enterprises

- Military grade encryption of any kind of data
- Ease management of digital assets
- Governance adaptable to specific needs of organization
- 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 and features, as well as YubiKey integration. 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.

FrostByte App Functionality

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 data Vaults, 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 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. FrostByte never has access to any user inputs or any of the user's secret data.

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 users (*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, as well as passwords or passphrases. The option to accept biometric security such as facial recognition or fingerprints enhances the security 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 N_{min}*.* 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 N_{min}*,* the sole input of such the N_{min} 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 N_{min}*.* 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 rudimental 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 tiers and can be unlocked by staking at least 1000 FROST tokens, which will be further elaborated on in the tokenomics section of the whitepaper. It is used as a capacitive input before performing the encryption operations. In doing so, the app either has the user 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 N_{min} 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

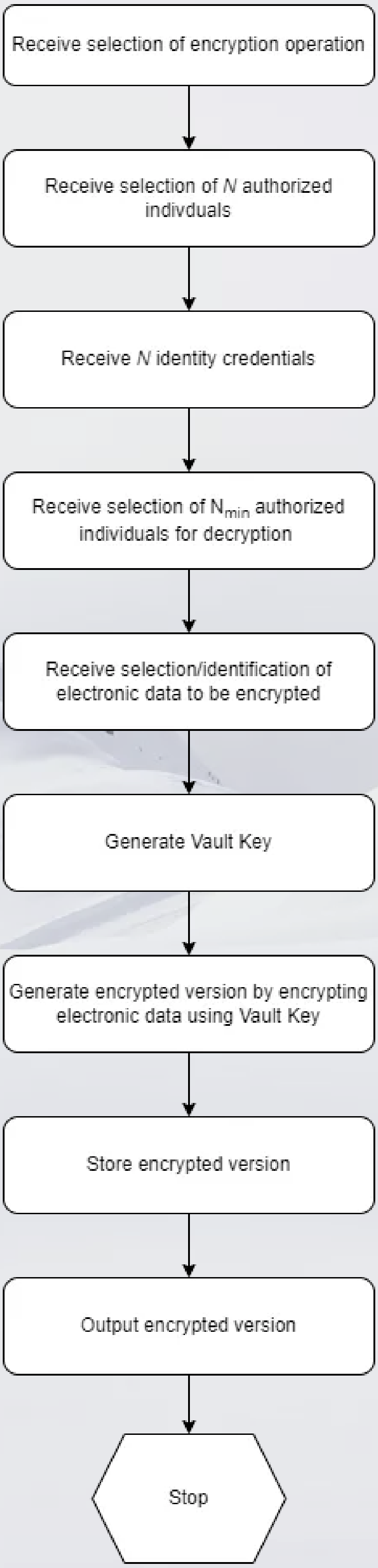
All data is stored on the device. Even though the hardware memory may contain Vault Key, encrypted data, identity credentials or more, the information may be stored in separate hierarchical file structures and/or hardware portions. Furthermore, access will be limited strictly by hardware and/or software 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. 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

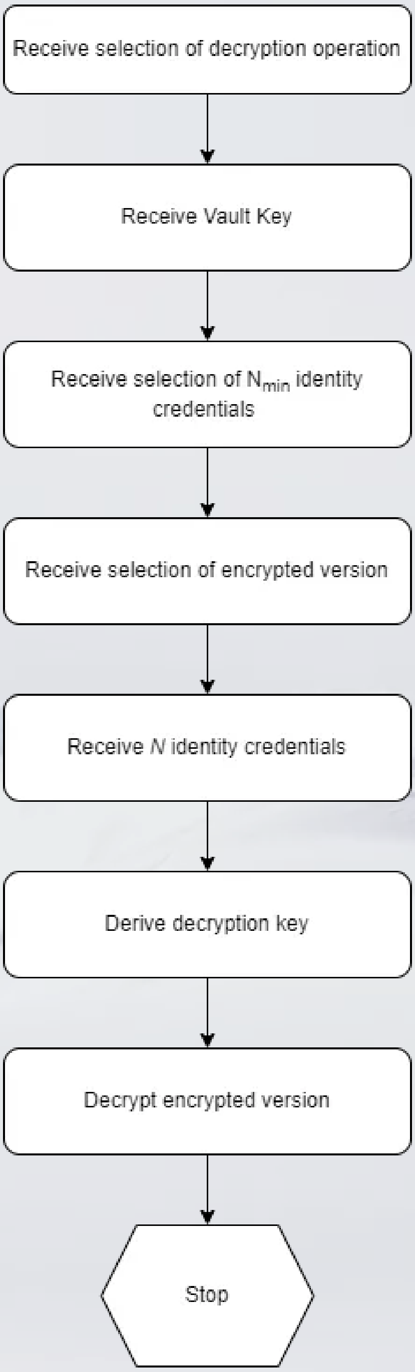
When any of the N authorized individuals desire to perform a decryption operation, the user may first need to input the Vault Key into the FrostByte mobile app. If the Vault Key is accepted, the app can proceed with the decryption process. The app collects passwords for m Vault Key shards as required, 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.

FrostByte Data Encryption


Receive selection of encryption operation
Receive selection of *N* authorized indivduals
Receive *N* identity credentials
Receive selection of N_{min} authorized individuals for decryption
Receive selection/identification of electronic data to be encrypted
Generate Vault Key
Generate encrypted version by encrypting electronic data using Vault Key
Store encrypted version
Output encrypted version
Stop

FrostByte Data Decryption


Receive selection of decryption operation
Receive Vault Key
Receive selection of N_{min} identity credentials
Receive selection of encrypted version
Receive *N* identity credentials
Derive decryption key
Decrypt encrypted version
Stop

Tokenomics

Staking

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.

The FROST token will eventually be a native token of the Cardano network, but may begin life as a token on another fast and low-cost blockchain network whilst the Cardano network works towards becoming fully smart contract functional and has been thoroughly tested. As such, reward tokens will be awarded at the end of each transaction bloch (or epoch of the Cardano network in due course) to users who stake FROST tokens (Currently, an epoch lasts five days, but this number is configurable and is changeable after an updated proposal of the Cardano network. Epochs work circularly: when one ends, another starts). 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/epoch as reward tokens at the end of each block/epoch to those users who stake FROST tokens during the entire length of that epoch or 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.

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. 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.

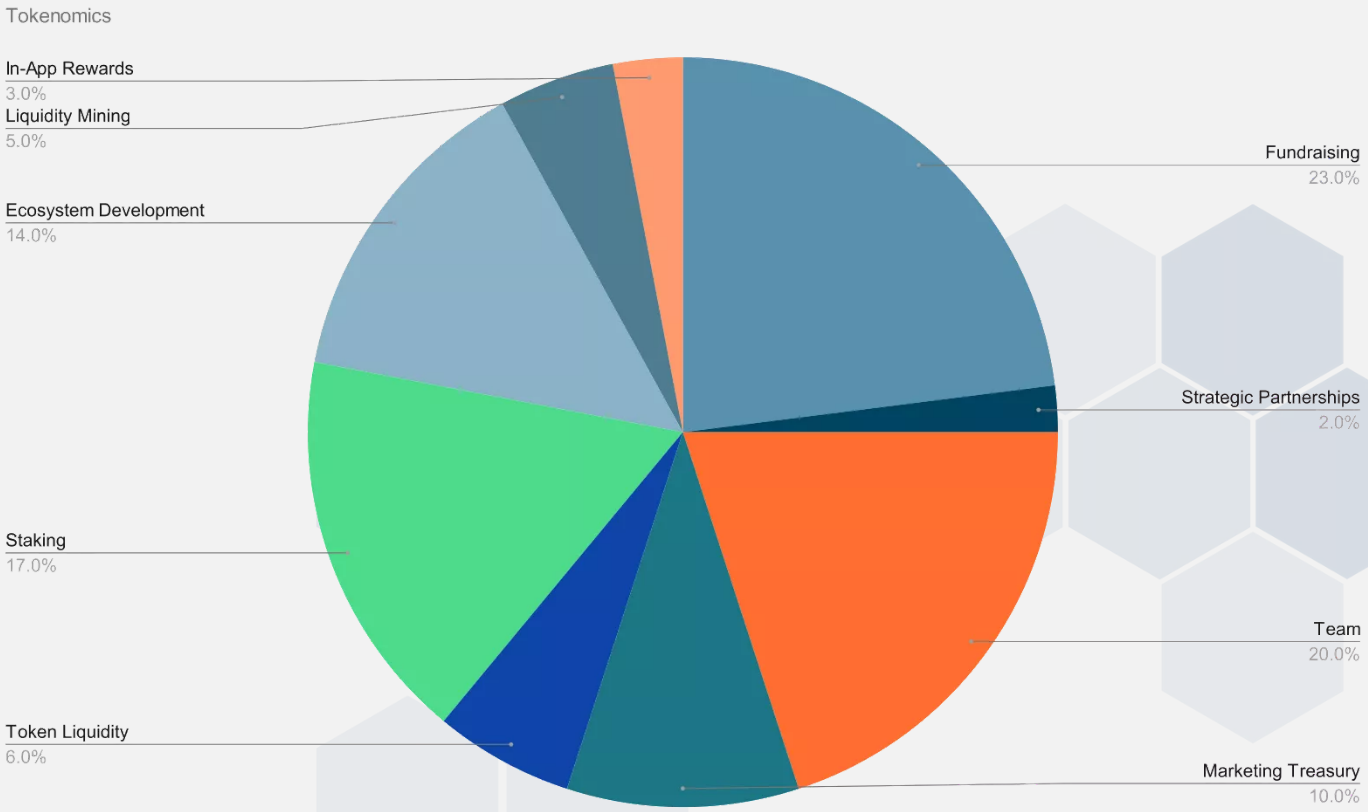
An example of the future utility of the FROST token will be to enable users to utilize the FROST tokens as a payment method for fees arising from all transactions involving FROST tokens. This utility is unique to the Cardano Network, which allows using native tokens as a currency for transaction fees contrary to other layer one applications.

Furthermore, the FROST token will be able to function as a payment method when users want to back up encrypted Vault data onto the blockchain or to access encrypted data from the blockchain. FrostByte will charge a 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 the 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 twenty-four-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.



Building on Cardano

After careful consideration, FrostByte chose to deploy its app on the Cardano ecosystem once this has full smart contract functionality and has been fully tested. We are convinced that Cardano, being a decentralized third-generation layer one solution, aligns well with the mission of the FrostByte project. Cardano itself, being built on a foundation of extensive peer-reviewed research and evidence-based development, provides the highest possible extent of security and utility for its second layer ecosystem. By combining the options to deploy smart contracts while being built on a proof-of-stake consensus (POS), Cardano positioned itself as the prime choice of a sustainable, socially responsible, and scalable blockchain. As we look to expand the capabilities of FrostByte, we may choose to add network-based features. We must choose a secure, decentralized, and efficient network to build these features. Particularly the decentralization of the Cardano network aligns perfectly with the decentralized FrostByte app. As Cardano positioned itself to become a fast-growing environment for DeFi applications, numerous mobile-first projects will launch on Cardano. Their users and investors will need to secure and store their data with sophisticated governance mechanisms, a service FrostByte is about to bring to this ecosystem.

Due to the PoS consensus, Cardano makes transactions highly efficient. Such fosters low transaction costs, tremendously benefiting the FrostByte community as well. We are very fond of the opportunity to use our native token to settle transaction costs, as this adds convenience and safety for the FrostByte users. Besides its unmatched utility, Cardano's mission of empowering the individual through technology resonates perfectly with our driving mission of empowering the individual through the best possible data security.
Furthermore, the strong and engaged Cardano community provides the backbone for its growth and the future success of the ecosystem. With the academic approach Cardano and their achievements to this point of time, driven by some of the best technologists in the field, FrostByte is convinced that they are the best possible layer one solution to partner with for the long term.

Community

FrostByte is looking forward to the build of 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.

Through its services, token offering and the outstanding Cardano community, FrostByte is confident that its ecosystem will grow exponentially. Given the unique functionality of the app and the utility of the native FROST token, FrostByte expects a vibrant and engaged 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 centred 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

Matching the Cardano mentality of achieving the highest possible quality through thoughtful development, FrostByte 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. We have 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 as an on-chain app. To facilitate this, Q4 of 2021 will host a seed and private round for sales of the FROST token to secure funding. The initial digital offering of the FROST utility token through the OCCAM Launchpad will follow in Q1 of 2022, acknowledging the quality of the FrostByte app and its valuable contribution to the Cardano ecosystem. (However, it is likely that the FROST token will first be issued on a fast and low cost blockchain and will then transition to the Cardano network once the latter is fully smart contract functional and tested.) Furthermore, the FrostByte source code will receive external auditing as well to ensure the highest possible security. Soon after this point, the mobile app for IOS and Android will become available to use. In the first half of 2022, FrostByte will 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.

In the second half of 2022, and subject to smart contract functionality being fully available and tested on the Cardano network, FrostByte plans to integrate its app onto the Cardano blockchain. Thereby, FrostByte will enable 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.

Team

Saul Schwartzbach

Co-Founder & CEO

Nate Johnston

Co-Founder & COO

Vikram Nagrani

Co-Founder & CSO

Parker McCurley

CTO

Ransom Christofferson

Developer

Advisors & Partners

Ivan Gowan

Advisor

David Johnston

Advisor

Occam.fi

Partner

DLTX

Partner

SecuX

Partner

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 HERE. 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 DECENTRALISED 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 DECENTRALISED TOKEN OFFERING. YOU SHOULD NOTE THAT YOUR YOUR PARTICIPATION IN THE FROSTBYTE INITIAL DECENTRALISED TOKEN OFFERING SHALL BE DEEMED TO CONSTITUTE YOUR ACKNOWLEDGEMENT AND ACCEPTANCE OF THE LEGAL TERMS, CONDITIONS, CONSIDERATIONS, RISKS AND DISCLAIMERS DOCUMENT AVAILABLE HERE 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 HERE, 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 https://frostbyte.app (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 which is available HERE forms part of this White Paper event though it is presented as a separate paper. It is intended to and must be read in full in conjunction with the White Paper.

The information set forth in the Legal Terms, Conditions, Considerations, Risks and Disclaimers Document (which is available HERE) may not be exhaustive. 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:
the possession, dissemination or communication of the Available Information; and/or
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 Parties (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 Parties do not make or purport to make, and hereby disclaim, any representation, warranty or undertaking made or alleged to be made by any Company Party 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 (which is available HERE) 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 REALISED.

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, JUDGEMENT 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 REALISED 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 UTILISE 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 (which is available **HERE**). 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 (which is available **HERE**) shall prevail.

*****

FrostByte

Get in Touch