VAULTAVO

VAULTAVO BIOMETRIC SMART CARD: SECURING YOUR FUTURE

VAULTAVO

ABSTRACT

Digital Custodians face the challenge of simultaneously optimizing flexibility, security, liquidity and convenience. We discuss how the Vaultavo Custody Solution solves this challenge with its unique, world-first biometric digital asset smart card. We further look at the design of the Vaultavo Card, how it works and how it improves on the digital custody technology that came before it.

INTRODUCTION

Certain products revolutionize the manner in which users interface with technology. The introduction of Google's search engine made the web accessible to the masses and the first iPhone with its intuitive touch screen technology created the blueprint for smartphones as we know them today. Neither Google nor Apple were first movers in the respective markets they revolutionized. However, each understood exactly what users needed to get the most out of a nascent technology. By creating a sophisticated, yet easy-to-use product, they rapidly advanced the adoption of a new technology. The crypto industry is on the verge of mainstream adoption, but it still lacks a key product that unlocks its potential and improves user experience. This product must be significantly better than the legacy systems which crypto seeks to supplement and, in some instances, replace. Vaultavo aims to fill this void with a custody solution, based on its world-first biometrically enabled digital asset smart card (the "Vaultavo card").

> **"WE BELIEVE THE VAULTAVO CUSTODY SOLUTION IS THE ULTIMATE ANSWER TO FURTHER ENHANCE RELIABILITY IN THE PREDOMINANTLY UNREGULATED SECTOR AND THUS SPEED UP BROADER INSTITUTIONAL ADOPTION OF CRYPTOCURRENCIES."**

In this paper we dive into the specifics of the Vaultavo card and how it facilitates a custody solution, far superior to what the competition has to offer. We will look at how it works and why the unique features of the Vaultavo card enables the Vaultavo Custody Solution to onboard the ever-expanding number of institutional players. Vaultavo's unique security technology combines the best aspects of various digital custody solutions; it solves the custody dilemma of simultaneously having high security while maintaining a high degree of liquidity and is flexible enough to fit any custody configuration. We believe the Vaultavo Custody Solution is the ultimate answer to further enhance reliability in the predominantly unregulated sector and thus speed up broader institutional adoption of cryptocurrencies.

THE CHALLENGE

There is a changing perception from Bitcoin and other cryptocurrencies functioning merely as payment rails, or mediums of exchange, to assets that can serve as store-of-value assets over longer time horizons. The industry initially had no need for bank-grade security and third-party custodians when Bitcoin was understood as an experimental new form of internet money - simple browser wallets were commonplace and deemed sufficient. However, once the value of a scarce digital asset in an increasingly connected world became evident, the necessity for secure, trustworthy third-party custodians became undeniable.

> **THE CHALLENGE THAT DIGITAL CUSTODIANS FACE TODAY LIES IN FINDING THE RIGHT BALANCE BETWEEN OFFERING HIGH LEVELS OF SECURITY WHILE SIMULTANEOUSLY MAINTAINING THE LIQUIDITY OF THE ASSETS.**

The challenge that digital custodians face today lies in finding the right balance between offering high levels of security while simultaneously maintaining the liquidity of the assets. Institutional investors are especially interested in custody technology that allows them to securely store their assets over longer periods of time while retaining the ability to quickly transfer or exchange their assets at will. No current solutions in the digital custody space convincingly solve both these problems. This is why we believe that the Vaultavo Custody Solution will be the key to unlocking the potential of the crypto world by making it both more accessible and orders of magnitude safer than existing custody solutions.

The Vaultavo Custody Solution was developed to safely on-board institutional investors such as commercial banks, centralized exchanges, and SMEs to the new blockchain asset class. Our solution is equally well-suited for high value retail investors who wish to optimize the security of their assets while enjoying the convenience that the Vaultavo Custody Solution offers. In the next section we will reveal exactly how the Vaultavo Card works, and how the Vaultavo Card, as the key component of the Vaultavo Custody Solution, facilitates the securing of your digital assets.

VAULTAVO

FIRST LOOK AT THE VAULTAVO CARD

Vaultavo's answer to the challenge of simultaneously optimizing security and liquidity lies in its unique proprietary technology; the world's first biometric-enabled digital asset smart card. The card is dimensionally proportional to a standard bank card that conveniently fits in your wallet. Upon closer inspection, three features that visually distinguish it from standard bank cards hint at the groundbreaking technology inside.

The first is a biometric fingerprint scanner which registers clients and enables them to seamlessly initiate and verify transactions by simply using their fingerprint. The second is an eInk display screen, similar to what one might find on a digital eBook reader device, that provides clear instructions to help with the registration process or navigate when transactions are done. Third, is the USB-C port which allows one to connect the device to a mobile phone, a laptop or computer. The Vaultavo Card also boasts contact, and contactless interfaces and a battery that can be recharged contactless or using a USB-C cable. The card form-factor is one most people are familiar and comfortable with, and its sleek appearance is modern, efficient, and aesthetically pleasing.

"UPON CLOSER INSPECTION, THREE FEATURES THAT VISUALLY DISTINGUISH IT FROM STANDARD BANK CARDS HINT AT THE GROUND-BREAKING TECHNOLOGY INSIDE."

The Vaultavo card is used in multiple roles in the Vaultavo Custody Solution as will be explained in more detail under "How does it work?" section below.

Although its primary function is to create and protect the private key using the unique on-card biometric fingerprint reader, it is also used as an access and control card within the Vaultavo Custody Solution custody flow.

If deployed as a Key Store it is plugged into the proprietary Vaultavo Vault and becomes the "Vaulted Card" that holds and protects the Private key. The Private key can only be accessed using the fingerprint/s that was used to create the Private key. More on the Vaulted Card in the sections below.

VAULTAVO

HOW DOES IT WORK?

Vaultavo Custody Solution Operations

To ensure complete separation of roles and responsibilities in custody operations, different roles are responsible for different functions within the Vaultavo custody flow. The programmable firmware of the Vaultavo Cards is used to change the function of the cards to fit in with the responsibilities of the five various roles.

The five main functions are:

- *Security Administrator (Security Administrator Card)*

The Security Administrator enrolls themselves onto the system with their Security Administrator Card, using their own fingerprint thus activating the security administration of the institution. The Security Administrator defines the custody rules and policies. These rules and policies can be different for each Vaulted card. The Vaulted Cards are the Vaultavo card that sits in the Vaultavo Vault and that holds the Private Key - see more below. The Security Administrator then sets up three roles and issues Vaultavo cards to the individuals in the institution who will be responsible for Account Administration, Initiation and Verification of transactions.

- *Account Administrator (Account Administrator Card)*

Using the Account Administration card and their fingerprint, the Account Administrator sets up and manages secure accounts and wallets, as well as applies the relevant rules and policies to the secure accounts. issues Vaultavo cards to the individuals in the institution who will be responsible for Account Administration, Initiation and Verification of transactions.

- *Initiator/s (Initiator Card/s)*

The Initiator/s enrolls themselves using their fingerprints and their Initiator cards and now have permission to only initiate transactions.

- *Verifier/s (Verifier Card/s)*

The Verifier/s enrolls themselves using their fingerprints and their Verifier card/s and now have permission to only verify previously initiated transactions. Depending on the rules set up by the Security Administrator, N of M verifier might have to verify an initiated transaction.

- *Crypto Owner (Client Card)*

In some of the Use Cases, the Initiation and Verification functions are done by the Crypto Owner. The cards used are then called a "Client Card".

The first notable point with the Vaultavo system is that these five roles can now be configured in multiple ways based on the crypto owner's wishes and the rules and protocols of the system will manage them accordingly.

KEY CREATION, BACKUP AND RESTORE

Institution

Three to five Vaultavo cards are issued to the three to five people that will act as Key Custodians for the institution (the "Vaultavo Custodian Cards"). Using our proprietary Vaultavo Key Management System, the key custodians enroll themselves using their own fingerprint and their Custodian Card. Each Custodian Card generates a custodian key linked to the fingerprint of the Key Custodian. The three to five Key Custodians then form a quorum to generate the Master Institutional Key which is used to generate the private keys on the Vaulted cards for that Institution.

In a similar manner, three to five 5 Key Custodians use Vaultavo Custodian Cards & the Vaultavo Key Management System to create a Master Backup Institutional Key which is used to generate unique backup keys for each of the Vaulted Cards. Each unique backup key is used to encrypt the Private Key of the Vaulted Card for Backup & Restore.

Any Key Custodian can be replaced by issuing a new Vaultavo Custodian Cards and by enrolling a new Key Custodian. Traditional financial sector merges with the rapidly developing technology.

Individual

The crypto owner uses a Vaultavo Card (the "Client Card") to enroll and register themselves with their fingerprint by using the biometric fingerprint scanner on the card. The fingerprint registration activates a random number generating process using the fingerprint, and the private key is created on the corresponding Vaulted card in the Vaultavo vault at the institution. The Client card and the corresponding vaulted card are now linked.

In a similar manner as with an Institution, three to five 5 Key Custodians appointed by the institution, use Vaultavo Custodian Cards & the Vaultavo Key Management System to create a Master Backup Institutional Key which is then used to generate unique backup keys for each of the Vaulted Cards. Each unique backup key is used to encrypt the Private Key of the Vaulted Card for Backup & Restore.

Any Key Custodian can be replaced by issuing new Vaultavo Custodian Cards and enrolling a new Key Custodian.

Use case 1*: Institutions that custodies Crypto on behalf of 3rd parties*

The Vaultavo card/s that will hold the private keys are placed in the state-of-the-art, proprietary designed and manufactured card HSM (the "Vaultavo Vault"). Each Vaultavo Vault holds up to 710 Vaultavo cards. These cards are referred to as the Vaulted cards. *(The Vaultavo Vault will be discussed in our next white paper)*

The Security Administrator of the institution defines the custody rules and policies. The Security Administrator then sets up the institution's Account Administrator, Initiator and Verifier/s roles. The Security Administrator then issues Vaultavo cards to the Account Administrator, Initiator and Verifier/s (see roll definitions above).

Similar as with multi-signature custody storage devices, using the Vaultavo cards linked to various roles, the Vaultavo Custody Solution is now configured to require multiple parties to initiate and verify transactions based on the rules defined by the Security Administrator of the institution. The Initiator/s only have permission to initiate transactions and the Verifier/s only have permission to verify previously initiated transactions done by the Initiator/s. Once a transaction/s have been successfully verified, all information is sent to the Vaulted card in the Vaultavo Vault, that verifies that all rules and policies have been met, after which it signs the transaction and pushes it onto the blockchain and send confirmation of completion back to the Vaultavo Custody Solution.

Use case 2*: Institutions act as a custody escrow agent (need to ensure that all agreed rules have been met before verifying transactions) but the client (Crypto owner) is solely responsible for the initiation of transactions*

Vaulted card/s that will hold the private keys of the crypto owner are placed in the Vaultavo Vault at the institution.

As in Use case 1, the Security Administrator of the institution defines the custody rules and policies. The Security Administrator then sets up the institution's Account Administrator and Verifier/s roles, including the Initiator role that in this Use case is the client (crypto owner). The Security Administrator then issues Vaultavo cards to the Account Administrator and Verifier/s, and the same process is followed as described in Use case 1.

A Vaultavo Card (the "Client Card") is then sent to the crypto owner. Upon receiving her Client Card, the crypto owner enrolls and registers herself with her fingerprint by using the biometric fingerprint scanner on the card. The fingerprint registration activates a random number generating process using the fingerprint, and the private key is created on the corresponding Vaulted card in the Vaultavo vault at the institution. The Client card and the corresponding vaulted card are now linked.

The Crypto Owner has the option to enroll 3rd party fingerprints for succession purposes (should Crypto Owner become incapacitated) and to enroll duress fingerprint/s that will place the card in "low balance" mode should the Crypto Owner ever be forced to relinquish his crypto assets.

As in Use case 1, the Initiator (now the crypto owner), that resides outside the institution, initiates transactions, and the transaction is verified by the Verifies that reside within the institution. Only once a transaction has been successfully verified, all information is sent to the Vaulted card in the Vaultavo Vault. The Vaulted card verifies that all rules and policies have been met, after which it signs the transaction and pushes it onto the blockchain and sends confirmation of completion back to the owner and verifiers.

Use case 3*: Institutions act as a Private Key escrow agent and the client (Crypto owner) is solely responsible for the initiation and verification of transactions.*

Vaulted card/s that will hold the private keys of the crypto owner are placed in the Vaultavo Vault controlled by the institution.

As in Use case 1, the Security Administrator of the institution defines the custody rules and policies in collaboration with the crypto owner/s. The Security Administrator then sets up the institution's Account Administrator roles as well as the Initiator/Verifier roles that in this configuration is the client (crypto owner). The Security Administrator then issues Vaultavo cards to the Account Administrator, and the same process is followed as in Use case 1.

A Vaultavo card (the "Client card") is sent to the crypto owner. Upon receiving his Vaultavo Card, the crypto owner enrolls and registers himself with his fingerprint by using the biometric fingerprint scanner on the card. The fingerprint registration activates a random number generating process using the fingerprint, and the private key is created on the corresponding Vaulted card in the Vaultavo vault at the institution. The Client card and the corresponding vaulted card are now linked.

The Crypto Owner has the option to enroll 3rd party fingerprints for succession purposes (should Crypto Owner become incapacitated) and to enroll duress fingerprint/s that will place the card in "low balance" mode should the Crypto Owner ever be forced to relinquish his crypto assets.

As in Use case 2, the crypto owner, that resides outside the institution, initiates transactions but in this Use case the crypto owner also has to verify the transactions. Only once transaction/s have been successfully verified, all information is sent to the Vaulted Card in the Vaultavo Vault, that verifies that all rules and policies have been met, after which it signs the transaction and pushes it onto the blockchain and sends confirmation of completion back to the owner.

In all configurations, the private keys are stored on the EMV6+ certified security module which is located on the Vaulted card; this security module is a smaller version of a hardware security module (HSM). It may be smaller in size but boasts the same security profile as larger modules. A feature of the Vaultavo Card technology is that the private key is completely isolated on the card's security module and is only accessible using the remote fingerprint reader, making it ultra-secure.

> THE VAULTAVO CARD HAS INDUSTRY LEADING TECHNOLOGY WITH REGARDS TO SECURITY; IT IS IMPOSSIBLE TO HACK THE SYSTEM TO RETRIEVE THE PRIVATE KEY AS BIOMETRICALLY AUTHENTICATION IS THE ONLY METHOD WHEREBY TRANSACTIONS CAN BE INITIATED AND VERIFIED.

The Vaultavo Card has industry leading technology with regards to security; it is impossible to hack the system to retrieve the private key as biometrically authentication is the only method whereby transactions can be initiated and verified. This bolsters security in two ways. If your card is lost or stolen, the card is useless to bad actors who wish to access your crypto assets. The sophisticated EMV6+ chip on the Vaultavo Card not only serves as a discrete, highly secure HSM for crypto storage, but is also certified to function as a standard Visa or Mastercard would. The interoperability between the fiat and crypto world can become a reality with the Vaultavo Card; you have a bank and crypto wallet in one accessible, easy to use card. Vaultavo technology is the culmination of the best aspects of digital custody solutions that came before it.

In the next section we review current custody solutions and why Vaultavo's novel approach is superior.

WHERE CURRENT DIGITAL CUSTODY SECURITY SOLUTIONS

Vaultavo conducted extensive market research on existing digital custody solutions to understand what drives consumer preference in the digital custody space. Even the best solutions were found wanting. No product struck the right balance between flexibility, security and liquidity. It is precisely this balance that Vaultavo achieves with its proprietary biometric smart card technology. In this section we briefly discuss the shortcomings of the solutions employed by Vaultavo's competitors to highlight the benefits this new technology offers.

Service vs. Technology Providers

A 2021 report by ULAM Labs identified 74 digital asset custody providers globally. Custodians differ substantially in the services they offer, the assets they are willing and able to secure and their target market. To understand the current landscape of digital custody it is useful to differentiate 'Service Providers' from 'Technology Providers'. Service Providers purchase the security technology they utilize from third parties. If they develop their own custody solution and offer that to the market, we refer to them as hybrid players. They often provide digital custody as a secondary service to their primary operations and thus lack expertise on the underlying technology. Usually, they utilize more general security technology and measures that may be known to hackers and bad actors. Technology Providers on the other hand are third parties that develop the security technology used by Service Providers. These developers focus on optimizing their security systems. Because they are not client facing, they tend to under-appreciate consumers' need for usability and convenience.

> **"WITH VAULTAVO ONE CAN COUNT ON EXPERT KNOWLEDGE OF THE UNDERLYING TECHNOLOGY AND EXCELLENT SAFEKEEPING AND MANAGEMENT SERVICES ALL IN ONE CONVENIENT PACKAGE - AS IT SHOULD BE."**

Vaultavo is a Technology Provider that provides its proprietary Custody Solution to Service Providers, but it's custody solution is also client facing. Vaultavo provides the perfect balance offering its certified high grade custom security technology in the form of a Biometric Smart Card and white-glove digital custody solution with its microservices architecture and plug-and-play Portals. With Vaultavo one can count on expert knowledge of the underlying technology and excellent safekeeping and management services all in one convenient package - as it should be.

Liquidity

Cryptocurrencies are increasingly recognized as store-of-value asset classes that accrue value over long time horizons despite short-term volatility. So investors opt for cold storage custody solutions in safety deposit boxes. These options are highly illiquid. This serves to discourage frantic, emotional trading based on FUD (fear, uncertainty and doubt) that is often propagated through misinformation on social media. A subset of investors prefers to HODL long term and weather the volatility of the crypto market. However, there are instances where individuals may wish to do a fast withdrawal but can't because of their cold storage structure.

We firmly believe that our clients should always be in full control of their assets and not be held hostage by external custody constructs. One mechanism that Vaultavo uses to improve security is multisig authentication of transactions which also serves to discourage emotional trading. This measure requires the consensus of multiple parties, which means that a plurality or majority of relevant parties responsible for the crypto assets must greenlight the decision before it is executed. If these requirements are met, transactions such as selling crypto or transferring assets to a different wallet can be enacted instantaneously.

"WE FIRMLY BELIEVE THAT OUR CLIENTS SHOULD ALWAYS BE IN FULL CONTROL OF THEIR ASSETS AND NOT BE HELD HOSTAGE BY EXTERNAL CUSTODY CONSTRUCTS."

Cloud Based Services

One of the more popular digital asset security solutions is cloud-based services, these services do not utilize hardware devices to secure crypto assets. Specific policies are established by the client to determine who can and cannot access the stored digital assets. Specialized lists can be created to make recurring payments to particular wallets with lower security requirements, while uncommon transaction-types must complete a more stringent authentication process. The lack of hardware devices in cloud services may initially seem appealing as safeguarding a hardware device is a responsibility and, in some circumstances, an added risk, as the device may get lost or stolen.

"SPECIFIC POLICIES ARE ESTABLISHED BY THE CLIENT TO DETERMINE WHO CAN AND CANNOT ACCESS THE STORED DIGITAL ASSETS."

Storing one's private keys on a cloud-based system does however introduce a different set of risks, chief among which is the greater attack surface compared to hardware options that are disconnected from the internet. Weak policy design and leaking passwords can lead to exploitation of the cloud security system. Cloud based digital custodians generally utilize a combination of multiparty computing (MPC) and zero-knowledge proofs to secure their system. Experts have yet to verify the effectiveness of MPC technology and in the next section we discuss why MPC technology is beginning to fall out of favor compared to hardware security module (HSM) technology.

MPC vs. HSM

In our *Custody Security Technology* paper, we discuss the virtues of hardware security modules (HSM) over multiparty computation (MPC) in detail, but here is the summary. Multiparty computation is a technology that is similar to multi-signature wallets which requires the consent of more than one party in order to execute a transaction. When an action is to be executed using MPC technology each relevant participant contributes private data to a computation, the collective inputs generate an output which, when correct, serves as authentication for transactions and management of crypto assets to take place. This prevents the single point of failure system which certain cold storage devices suffer from. MPC technology can be protected by different algorithms, though trade-offs between security, latency and efficiency need to be considered.

The issue with MPC technology is that they require third-party computers that are often multipurpose and easier to exploit. Most privacy guarantees that MPC technology offers can be replicated using zero-knowledge proofs, however the hardware is not as robust and secure as HSMs which are designed with the singular purpose of securing digital data and by extension digital assets. The Vaultavo Card benefits from the security of HSM and similarly has multi-party verification capabilities that replicate MPC security features without involving third-party computers or systems.

VAULTAVO

CONCLUSION

The crypto industry is primed for Vaultavo's biometric smart card solution which simultaneously optimizes security and liquidity. The Vaultavo Card bridges the crypto and fiat world as the EMV6+ certified micro-chip enables both crypto storage and standard VISA and Mastercard operations. Vaultavo's proprietary Vaultavo Vault technology gives it the best-in-class security profile, while zero-knowledge proofs are used to gain the added benefits of multiparty computations, or multi signature verification. A stolen or lost Vaultavo Card is of no use to bad actors who would require the cardholder's fingerprint and the consent of other designated cardholders to initiate and approve a transaction. Vaultavo's has unlocked the secret to maximizing security and liquidity while maintaining ease of use convenience, making it more effective and more widely-adoptable than any other digital custody solution out there.

> **"THE CRYPTO INDUSTRY IS PRIMED FOR VAULTAVO'S BIOMETRIC SMART CARD SOLUTION WHICH SIMULTANEOUSLY OPTIMIZES SECURITY AND LIQUIDITY."**

TO LEARN MORE VISIT
www.vaultavo.com

FOR GENERAL ENQUIRIES CONTACT
hello@vaultavo.com

FOLLOW US ON TWITTER
@vaultavo